Acronis

acronis.com

Cyber Protection

24.03

Guide de l'utilisateur

RÉVISION : 11/04/2024

Table des matières

Prise en main de Cyber Protection

Activation du compte

Lorsqu'un administrateur vous crée un compte, un e-mail vous est envoyé. Le message contient les informations suivantes :

- **Votre identifiant.** Nom d'utilisateur que vous utilisez pour vous connecter. Votre identifiant figure également sur la page d'activation du compte.
- Bouton **Activer le compte**. Cliquez sur le bouton et configurez le mot de passe de votre compte. Assurez-vous que le mot de passe contient au moins neuf caractères. Pour plus d'informations sur le mot de passe, reportez-vous à "Exigences relatives au mot de passe" (p. 19).

Si votre administrateur a activé l'authentification à deux facteurs, vous serez invité à la configurer pour votre compte. Pour plus d'informations à ce sujet, reportez-vous à "Authentification à deux facteurs" (p. 19).

Exigences relatives au mot de passe

Le mot de passe d'un compte utilisateur doit comporter au moins 9 caractèresLa complexité des mots de passe est également vérifiée et les mots de passe sont classés dans les catégories suivantes :

- Faible
- Moyenne
- Fort

Vous ne pouvez pas enregistrer un mot de passe faible, même s'il contient 9 caractères ou plus. Les mots de passe qui contiennent le nom de l'utilisateur, l'identifiant, l'adresse e-mail de l'utilisateur ou le nom du tenant auquel le compte utilisateur appartient sont toujours considérés comme faibles. La plupart des mots de passe courants sont également considérés comme faibles.

Pour renforcer un mot de passe, ajoutez-lui des caractères. L'utilisation de différents types de caractères (chiffres, majuscules, minuscules et caractères spéciaux) n'est pas obligatoire, mais permet d'obtenir des mots de passe plus forts, mais aussi plus courts.

Authentification à deux facteurs

L'authentification à deux facteurs vous protège davantage contre l'accès non autorisé à votre compte. Lorsque l'authentification à deux facteurs est configurée, vous devez saisir votre mot de passe (premier facteur) et un code unique (second facteur) pour vous connecter à la console Cyber Protect. Le code unique est généré par une application spéciale qui doit être installée sur votre téléphone mobile ou un autre terminal vous appartenant. Même si quelqu'un découvre votre identifiant et votre mot de passe, il ne pourra pas se connecter à votre compte sans avoir accès à le terminal qui applique le second facteur.

Pour configurer l'authentification à deux facteurs pour votre compte

Vous devez configurer l'authentification à deux facteurs pour votre compte si l'administrateur l'a activée pour votre organisation. Si l'administrateur active l'authentification à deux facteurs alors que vous êtes connecté à la console Cyber Protect, vous devrez la configurer à l'expiration de votre session actuelle.

Prérequis

- L'authentification à deux facteurs est activée pour votre organisation par un administrateur.

Pour configurer l'authentification à deux facteurs pour votre compte

1. Installez une application d'authentification sur votre terminal mobile.
   Exemples d'applications d'authentification :
   - Twilio Authy
   - Microsoft Authenticator
   - Google Authenticator
2. Scannez le QR code à l'aide de votre application d'authentification, puis saisissez le code à 6 chiffres affiché dans l'application d'authentification, dans la fenêtre **Configurer l'authentification à deux facteurs**.
3. Cliquez sur **Suivant**.
   Les instructions qui concernent la restauration de votre accès à votre compte (si vous perdez votre terminal avec authentification à deux facteurs ou désinstallez l'application d'authentification) s'affichent.
4. Enregistrez ou imprimez le fichier PDF.

   Remarque
   Veillez à enregistrer le fichier PDF dans un endroit sûr ou à l'imprimer pour vous y reporter ultérieurement. C'est la meilleure façon de restaurer l'accès.

5. Retournez à la page de connexion de la console Cyber Protect et saisissez le code généré.
   Un code unique est valable 30 secondes. Si vous attendez plus de 30 secondes, utilisez le code généré juste après.

Lors de votre prochaine connexion, vous pourrez cocher la case **Faire confiance à ce navigateur**. Dans ce cas, le code ne sera pas requis lors des connexions suivantes avec ce navigateur sur cet ordinateur.

Remarque
Nous vous recommandons de ne pas cocher cette case. Sinon, vous perdrez l'accès à l'authentification à deux facteurs pour votre compte.

Pour restaurer l'authentification à deux facteurs sur un nouveau terminal

Si vous avez accès à l'application d'authentification sur mobile configurée précédemment

1. Installez une application d'authentification sur votre nouveau terminal.
2. Utilisez le fichier PDF que vous avez enregistré lorsque vous avez configuré l'authentification à deux facteurs sur votre terminal. Ce fichier contient le code à 32 chiffres que vous devez saisir dans l'application d'authentification pour réassocier cette application à votre compte Acronis.

   Important
   Si le code ne fonctionne pas, veillez à ce que l'heure dans l'application d'authentification pour mobile soit synchronisée avec votre terminal.

   Si vous n'avez pas enregistré le fichier PDF pendant l'installation :

a. Cliquez sur **Réinitialiser l'authentification à deux facteurs**, puis saisissez le mot de passe à usage unique dans l'application d'authentification sur mobile.
b. Suivez les instructions affichées à l'écran.

Si vous n'avez pas accès à l'application d'authentification sur mobile configurée précédemment

1. Prenez un nouveau terminal mobile.
2. Utilisez le fichier PDF stocké pour associer un nouveau terminal (le nom par défaut du fichier est `cyberprotect-2fa-backupcode.pdf`).
3. Restaurez l'accès à votre compte depuis la sauvegarde. Assurez-vous que les sauvegardes sont prises en charge par votre application mobile.
4. Ouvrez l'application dans le même compte, depuis un autre terminal mobile s'il est pris en charge par l'application.

Paramètres de confidentialité

Les paramètres de confidentialité vous aident à indiquer si vous donnez ou non votre consentement pour la collecte, l'utilisation et la divulgation de vos informations personnelles.

En fonction du pays dans lequel vous utilisez Cyber Protect Cloud et du centre de données Cyber Protect Cloud qui vous fournit des services, lors du lancement initial de Cyber Protect Cloud vous serez peut-être invité à confirmer si vous acceptez ou non d'utiliser Google Analytics dans Cyber Protect Cloud.

Google Analytics nous aide à mieux comprendre le comportement des utilisateurs et à leur offrir une meilleure expérience dans Cyber Protect Cloud en collectant des données avec pseudonyme.

Si vous avez activé ou refusé d'activer Google Analytics lors du lancement initial de Cyber Protect Cloud, vous pouvez changer d'avis ultérieurement.

Activer ou désactiver Google Analytics

1. Dans la console Cyber Protect, cliquez sur **Gérer les comptes**.
2. Cliquez sur l'icône de compte dans l'angle supérieur droit.
3. Sélectionnez **Mes paramètres de confidentialité**. La fenêtre **Mes paramètres de confidentialité** s'affiche.

4. Dans la section **Collecte de données Google Analytics**, cliquez sur l'un des boutons suivants :
   - **Activé** pour activer Google Analytics
   - **Désactivé** pour désactiver Google Analytics

Dans la section **Comment supprimer les cookies**, vous pouvez contrôler et gérer les cookies directement dans votre navigateur.

Remarque
Si la section Google Analytics n'apparaît pas, cela signifie que Google Analytics n'est pas utilisé dans votre pays.

Dans la section **Intégration au produit et aide interactive** (affichée initialement pendant la période d'évaluation) vous pouvez choisir d'arrêter ou de continuer de recevoir les informations sur les améliorations et nouvelles fonctionnalités du programme. La fonctionnalité est activée par défaut, mais vous pouvez la désactiver en paramétrant le commutateur sur **Désactiver**.

Accès au service Cyber Protection

Une fois que vous avez activé votre compte, vous pouvez accéder au service Cyber Protection en vous connectant à la console Cyber Protect ou via le portail de gestion.

Vous connecter à la console Cyber Protect

1. Allez sur la page de connexion au service Cyber Protection.
2. Saisissez votre identifiant, puis cliquez sur **Suivant**.
3. Saisissez votre mot de passe, puis cliquez sur **Suivant**.
4. [Si vous utilisez plusieurs services Cyber Protect Cloud] Cliquez sur **Cyberprotection**.
   Les utilisateurs ayant uniquement accès au service Cyber Protection se connectent directement à la console de service Cyber Protect.
   Si le service **Cyberprotection** n'est pas le seul service auquel vous pouvez accéder, vous pouvez passer d'un service à l'autre en cliquant sur l'icône  dans l'angle supérieur droit. Les administrateurs peuvent également se servir de cette icône pour accéder au portail de gestion.

Le délai d'expiration pour la console Cyber Protect est de 24 heures pour les sessions actives et d'une heure pour les sessions inactives.

Vous pouvez modifier la langue de l'interface Web en cliquant sur l'icône de compte dans l'angle supérieur droit.

Accéder à la console Cyber Protect via le portail de gestion

1. Dans le portail de gestion, accédez à **Surveillance** > **Utilisation**.
2. Sous **Cyber Protect**, sélectionnez **Protection**, puis cliquez sur **Gérer le service**.
   Vous pouvez aussi sélectionner un client sous **Clients**, puis cliquer sur **Gérer le service**.

Vous serez alors redirigé vers la console Cyber Protect.

Important
Si le client est en mode de gestion **Libre-service**, vous ne pouvez pas gérer les services à sa place. Seuls les administrateurs clients peuvent modifier le mode client et sélectionner **Géré par le fournisseur de services**, puis gérer les services.

Pour réinitialiser votre mot de passe

1. Allez sur la page de connexion au service Cyber Protection.
2. Saisissez votre identifiant, puis cliquez sur **Suivant**.
3. Cliquez sur **Mot de passe oublié ?**
4. Confirmez que vous souhaitez obtenir plus d'instructions en cliquant sur **Envoyer**.
5. Suivez les instructions contenues dans l'e-mail que vous avez reçu.
6. Configurez votre nouveau mot de passe.

Exigences logicielles

Navigateurs Web pris en charge

La console Cyber Protect utilise le protocole TLS 1.2 et prend en charge les navigateurs Web suivants :

- Google Chrome 29 ou version ultérieure
- Mozilla Firefox 23 ou version ultérieure
- Opera 16 ou version ultérieure
- Microsoft Edge 25 ou version ultérieure
- Safari 8 ou version ultérieure s'exécutant sur les systèmes d'exploitation macOS et iOS

Il est possible que les autres navigateurs (dont les navigateurs Safari s'exécutant sur d'autres systèmes d'exploitation) n'affichent pas correctement l'interface utilisateur ou ne proposent pas certaines fonctions.

Systèmes d'exploitation et environnements pris en charge

Agent pour Windows

Cet agent inclut un composant de protection contre les virus et les malwares et de filtrage d'URL. Consultez "Fonctionnalités de protection prises en charge par système d'exploitation" (p. 45) pour en savoir plus sur les fonctionnalités prises en charge par système d'exploitation.

- Windows XP Professionnel SP1 (x64), SP2 (x64), SP3 (x86)
- Windows Server 2003 SP1/2003 R2 et versions ultérieures – éditions Standard et Enterprise (x86, x64)
- Windows Small Business Server 2003/2003 R2
- Windows Server 2008, Windows Server 2008 SP2* – éditions Standard, Enterprise, Datacenter, Foundation et Web (x86, x64)
- Windows Small Business Server 2008, Windows Small Business Server 2008 SP2*
- Windows 7 - toutes les éditions

Remarque
Pour utiliser Cyber Protection avec Windows 7, vous devez installer les mises à jour suivantes fournies par Microsoft avant d'installer l'agent de protection :

- Mises à jour de sécurité étendues (ESU) pour Windows 7
- KB4474419
- KB4490628

Pour plus d'informations sur les mises à jour requises, reportez-vous à cet article de la base de connaissances.

- Windows Server 2008 R2* – éditions Standard, Enterprise, Datacenter, Foundation et Web
- Windows Home Server 2011*
- Windows MultiPoint Server 2010*/2011*/2012
- Windows Small Business Server 2011* – toutes les éditions
- Windows 8/8.1 – toutes les éditions (x86, x64), sauf les éditions Windows RT
- Windows Server 2012/2012 R2 – toutes les éditions
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10 – éditions Famille, Professionnel, Éducation, Entreprise, IoT Entreprise et LTSC (anciennement LTSB)
- Windows Server 2016 – toutes les options d'installation, excepté Nano Server
- Windows Server 2019 – toutes les options d'installation, excepté Nano Server
- Windows 11 – toutes les éditions
- Windows Server 2022 – toutes les options d'installation, excepté Nano Server

Remarque
* Pour utiliser Cyber Protection avec cette version de Windows, vous devez installer la mise à jour du support de signature de code SHA2 de Microsoft (article KB4474419) avant d'installer l'agent de protection.

Pour plus d'informations sur les problèmes liés à la mise à jour du support de signature de code SHA2, reportez-vous à cet article de la base de connaissances.

Agent pour SQL, agent pour Active Directory, agent pour Exchange (pour la sauvegarde de bases de données et la sauvegarde reconnaissant les applications)

Chacun de ces agents peut être installé sur une machine fonctionnant sous tout système d'exploitation figurant dans la liste ci-dessus, avec une version prise en charge de l'application respective.

Agent pour empêcher les pertes de données

Contrôle des terminaux

- Microsoft Windows 7 Service Pack 1 et versions ultérieures
- Microsoft Windows Server 2008 R2 et versions ultérieures
- macOS 10.15 (Catalina)
- macOS 11.2.3 (Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)

Remarque
Agent for Data Loss Prevention pour macOS ne prend en charge que les processeurs x64. Les processeurs Apple Silicon ARM ne sont pas supportés.

Prévention des pertes de données

- Microsoft Windows 7 Service Pack 1 et versions ultérieures
- Microsoft Windows Server 2008 R2 et versions ultérieures

Remarque
Agent for Data Loss Prevention peut être installé sur des systèmes macOS non pris en charge, car il fait partie intégrante d'Agent for Mac. Dans ce cas, la console Cyber Protect indiquera que Agent for Data Loss Prevention est installé sur l'ordinateur, mais les fonctionnalités de contrôle des terminaux et de prévention des pertes de données ne fonctionneront pas. La fonctionnalité de contrôle des terminaux ne fonctionnera que sur les systèmes macOS supporté par Agent for Data Loss Prevention.

Agent pour Advanced Data Loss Prevention

- Microsoft Windows 7 Service Pack 1 et versions ultérieures
- Microsoft Windows Server 2008 R2 et versions ultérieures

Agent pour File Sync & Share

Pour obtenir la liste des systèmes d'exploitation pris en charge, consultez le Guide de l'utilisateur Cloud Cyber Files.

Agent pour Exchange (pour la sauvegarde de boîte aux lettres)

- Windows Server 2008 – éditions Standard, Enterprise, Datacenter, Foundation et Web (x86, x64)
- Windows Small Business Server 2008
- Windows 7 - toutes les éditions
- Windows Server 2008 R2 - éditions Standard, Enterprise, Datacenter, Foundation et Web
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – toutes les éditions
- Windows 8/8.1 – toutes les éditions (x86, x64), sauf les éditions Windows RT
- Windows Server 2012/2012 R2 – toutes les éditions
- Windows Storage Server 2008/2008 R2/2012/2012 R2
- Windows 10 – éditions Famille, Professionnel, Éducation et Entreprise
- Windows Server 2016 – toutes les options d'installation, excepté Nano Server
- Windows Server 2019 – toutes les options d'installation, excepté Nano Server
- Windows 11 – toutes les éditions
- Windows Server 2022 – toutes les options d'installation, excepté Nano Server

Agent pour Microsoft 365

- Windows Server 2008 – éditions Standard, Enterprise, Datacenter, Foundation et Web (x64 uniquement)
- Windows Small Business Server 2008
- Windows Server 2008 R2 - éditions Standard, Enterprise, Datacenter, Foundation et Web
- Windows Home Server 2011
- Windows Small Business Server 2011 – toutes les éditions
- Windows 8/8.1 – toutes les éditions (x64 uniquement), sauf les éditions Windows RT
- Windows Server 2012/2012 R2 – toutes les éditions
- Windows Storage Server 2008/2008 R2/2012/2012R2/2016 (x64 uniquement)
- Windows 10 – éditions Famille, Professionnel, Éducation et Entreprise (x64 uniquement)
- Windows Server 2016 – toutes les options d'installation (x64 uniquement), sauf Nano Server
- Windows Server 2019 – toutes les options d'installation (x64 uniquement), sauf Nano Server

- Windows 11 – toutes les éditions
- Windows Server 2022 – toutes les options d'installation, excepté Nano Server

Agent pour Oracle

- Windows Server 2008R2 – éditions Standard, Enterprise, Datacenter et Web (x86, x64)
- Windows Server 2012R2 – éditions Standard, Enterprise, Datacenter et Web (x86, x64)
- Linux – tout noyau ou distribution pris en charge par un agent pour Linux (répertorié ci-dessous)

Agent pour MySQL/MariaDB

- Linux – tout noyau ou distribution pris en charge par un agent pour Linux (répertorié ci-dessous)

Agent pour Linux

Cet agent inclut un composant de protection contre les virus et les malwares et de filtrage d'URL. Consultez "Fonctionnalités de protection prises en charge par système d'exploitation" (p. 45) pour en savoir plus sur les fonctionnalités prises en charge par système d'exploitation.

Les distributions Linux et les versions de noyau suivantes ont été spécifiquement testées. Toutefois, même si votre distribution Linux ou votre version de noyau n'est pas répertoriée, il est possible qu'elle fonctionne quand même correctement dans tous les scénarios nécessaires, en raison des spécificités des systèmes d'exploitation Linux.

Si vous rencontrez des problèmes lors de l'utilisation de Cyber Protection avec votre association de distribution Linux et de version de noyau, contactez l'équipe d'assistance pour une enquête approfondie.

Linux avec noyau de la version 2.6.9 à la version 5.19 et glibc 2.3.4 ou version ultérieure, y compris les distributions x86 et x86_64 suivantes :

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04, 22.10, 23.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 37, 38
- SUSE Linux Enterprise Server 10, 11, 12, 15

  Important
  Les configurations avec Btrfs ne sont pas prises en charge pour SUSE Linux Enterprise Server 12 et SUSE Linux Enterprise Server 15.

- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10, 11
- CentOS 5.x, 6.x, 7.x, 8.x*
- CentOS Stream 8*, 9*

- Oracle Linux 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2* : Unbreakable Enterprise Kernel et Red Hat Compatible Kernel

  Remarque
  Installation de l'agent de protection sur Oracle Linux 8.6 et versions ultérieures sur lesquelles Secure Boot est activé ; exige la signature manuelle des modules noyau. Pour plus d'informations sur la signature d'un module noyau, reportez-vous à cet article de la base de connaissances.

- CloudLinux 5.x, 6.x, 7.x, 8.x*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.x*,9.0*, 9.1*, 9.2*
- Rocky Linux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- ALT Linux 7.0

* À partir de la version 8.4, prise en charge uniquement avec les noyaux de 4.18 à 5.19

Agent pour Mac

Cet agent inclut un composant de protection contre les virus et les malwares et de filtrage d'URL. Consultez "Fonctionnalités de protection prises en charge par système d'exploitation" (p. 45) pour en savoir plus sur les fonctionnalités prises en charge par système d'exploitation.

Les architectures x64 et ARM (utilisées dans les processeurs Apple Silicon tels qu'Apple M1 et M2) sont toutes deux prises en charge.

Remarque
Vous ne pouvez pas restaurer les sauvegarde de disque d'ordinateurs Mac Intel sur des Mac utilisant des puces silicone Apple, et inversement. Vous pouvez restaurer des fichiers et des dossiers.

- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12
- macOS Ventura 13
- macOS Sonoma 14

Important
À partir de la version C23.07, Cyber Protect Cloud ne prend pas en charge les systèmes d'exploitation suivants : OS X Yosemite 10.10, OS X El Capitan 10.11 et macOS Sierra 10.12.

Nous vous recommandons vivement d'effectuer la mise à niveau de votre système d'exploitation vers une version prise en charge afin de garantir la compatibilité et de pouvoir utiliser toutes les fonctionnalités de Cyber Protect Cloud.

Agent pour VMware (appliance virtuelle)

Cet agent est fourni en tant qu'appliance virtuelle pour s'exécuter sur un hôte ESXi.

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

Agent pour VMware (Windows)

Cet agent est livré comme une application Windows pour s'exécuter dans tout système d'exploitation inscrit dans la liste ci-dessus pour l'agent pour Windows, avec les exceptions suivantes :

- Les systèmes d'exploitation 32 bits ne sont pas pris en charge.
- Windows XP, Windows Server 2003/2003 R2 et Windows Small Business Server 2003/2003 R2 ne sont pas pris en charge.

Agent pour Hyper-V

- Windows Server 2008 (x64 uniquement) avec rôle Hyper-V, y compris le mode d'installation de Server Core
- Windows Server 2008 R2 avec rôle Hyper-V, y compris le mode d'installation de Server Core
- Microsoft Hyper-V Server 2008/2008 R2
- Windows Server 2012/2012 R2 avec rôle Hyper-V, y compris le mode d'installation de Server Core
- Microsoft Hyper-V Server 2012/2012 R2
- Windows 8, 8.1 (x64 uniquement) avec Hyper-V
- Windows 10 – éditions Familiale, Pro, Education et Enterprise avec Hyper-V
- Rôle de Windows Server 2016 avec Hyper-V – toutes les options d'installation, excepté Nano Server
- Microsoft Hyper-V Server 2016
- Rôle de Windows Server 2019 avec Hyper-V – toutes les options d'installation, excepté Nano Server
- Microsoft Hyper-V Server 2019
- Windows Server 2022 – toutes les options d'installation, excepté Nano Server

Agent pour Virtuozzo

- Virtuozzo 6.0.10, 6.0.11, 6.0.12, 7.0.13, 7.0.14
- Virtuozzo Hybrid Server 7.5

Agent pour Virtuozzo Hybrid Infrastructure

Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0

Agent pour Scale Computing HC3

Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3

Agent pour oVirt

Red Hat Virtualization 4.2, 4.3, 4.4, 4.5

Agent pour Synology

DiskStation Manager 6.2.x, 7.x

L'agent pour Synology ne prend en charge que les NAS dotés de processeurs x86_64. Les processeurs ARM ne sont pas pris en charge.

Cyber Protect Monitor

- Windows 7 et versions ultérieures
- Windows Server 2008 R2 et versions ultérieures
- Toutes les versions de macOS qui sont prises en charge par Agent pour Mac

Versions de Microsoft SQL Server prises en charge

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

Les éditions SQL Server Express des versions de serveur SQL susmentionnées sont également prises en charge.

Remarque
La sauvegarde de Microsoft SQL n'est prise en charge que pour les bases de données fonctionnant sur les systèmes de fichiers NFTS, REFS et FAT32. ExFat n'est pas pris en charge.

Versions Microsoft Exchange Server compatibles

- Microsoft Exchange Server 2019 – toutes les éditions.
- Microsoft Exchange Server 2016 – toutes les éditions.
- Microsoft Exchange Server 2013 – toutes les éditions, mise à jour cumulative 1 (CU1) et ultérieures.
- Microsoft Exchange Server 2010 – toutes les éditions, tous les service packs. La sauvegarde et restauration granulaire pour boîte aux lettres depuis les sauvegardes de base de données sont prises en charge par le Service Pack 1 (SP1).
- Microsoft Exchange Server 2007 – toutes les éditions, tous les service packs. La sauvegarde et restauration granulaire pour boîte aux lettres depuis les sauvegardes de base de données ne sont pas prises en charge.

Versions de Microsoft SharePoint prises en charge

Cyber Protection prend en charge les versions de Microsoft SharePoint suivantes :

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1
- Microsoft SharePoint Foundation 2010 SP1
- Microsoft Office SharePoint Server 2007 SP2*
- Microsoft Windows SharePoint Services 3.0 SP2*

* Pour pouvoir utiliser SharePoint Explorer avec ces versions, il est nécessaire d'avoir une batterie de restauration SharePoint à laquelle joindre les bases de données.

Les sauvegardes ou bases de données à partir desquelles vous extrayez des données doivent provenir de la même version de SharePoint que celle sur laquelle SharePoint Explorer est installé.

Versions Oracle Database prises en charge

- Oracle Database version 11g, toutes éditions
- Oracle Database version 12c, toutes éditions
- Oracle Database version 19c, toutes éditions
- Oracle Database version 21c, toutes éditions

Prise en charge des configurations à instance unique seulement.

Versions SAP HANA prises en charge

HANA 2.0 SPS 03 installé sur RHEL 7.6 en cours d'exécution sur une machine physique ou une machine virtuelle VMware ESXi.

SAP HANA ne prend pas en charge la récupération de conteneurs de bases de données multi-tenants à l'aide d'instantanés de stockage. Par conséquent, cette solution prend en charge les conteneurs SAP HANA avec une base de données tenant uniquement.

Versions de MySQL prises en charge

- 5.5.x − Éditions Community Server, Enterprise, Standard et Classic
- 5.6.x − Éditions Community Server, Enterprise, Standard et Classic
- 5.7.x − Éditions Community Server, Enterprise, Standard et Classic
- 8.0.x − Éditions Community Server, Enterprise, Standard et Classic

Versions de MariaDB prises en charge

- 10.0.x
- 10.1.x
- 10.2.x
- 10.3.x
- 10.4.x
- 10.5.x
- 10.6.x
- 10.7.x

Plates-formes de virtualisation prises en charge

Le tableau suivant récapitule la prise en charge de diverses plates-formes de virtualisation.

Pour plus d'informations sur les différences entre les sauvegardes avec et sans agent, voir "Sauvegarde avec et sans agent" (p. 67).

Remarque
Si vous utilisez une plate-forme ou une version de virtualisation non répertoriée ci-dessous, la méthode de **sauvegarde avec agent (sauvegarde à partir d'un système d'exploitation invité)** peut encore fonctionner correctement dans tous les scénarios requis. Si vous rencontrez des problèmes avec ce type de sauvegarde, contactez l'équipe de support pour plus d'informations.

VMware

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Versions VMware vSphere : 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0 **Éditions VMware vSphere :** VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **VMware ESXi** > **Agent pour l'installation dans Windows** ou **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **VMware ESXi** > **Appliance virtuelle (OVF)**	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
VMware vSphere Hypervisor (ESXi gratuit)**	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Serveur VMware (serveur virtuel VMware) VMware Workstation VMware ACE VMware Player	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

* Dans le cas de ces éditions, le transport HotAdd pour disques virtuels est pris en charge sur vSphere 5.0 et versions ultérieures. Sur la version 4.1, il est possible que les sauvegardes soient plus lentes.

** La sauvegarde à un niveau hyperviseur n'est pas prise en charge pour vSphere Hypervisor parce que ce produit limite l'accès à l'interface de Ligne de Commande à distance (RCLI) au mode lecture seule. L'agent fonctionne pendant la période d'évaluation de l'hyperviseur vSphere tant qu'une clé de série n'est pas saisie. Une fois que vous avez saisi une clé de série, l'agent s'arrête de fonctionner.

Remarque
Cyber Protect Cloud prend officiellement en charge toute mise à jour d'une version majeure de vSphere prise en charge.

Par exemple, la prise en charge de vSphere 8.0 inclut la prise en charge de toute mise à jour de cette version, sauf indication contraire. Autrement dit, vSphere 8.0 Update 1 est également prise en charge, au même titre que la version initiale de vSphere 8.0.

La prise en charge d'une version spécifique de VMware vSphere signifie que vSAN de la version correspondante est également pris en charge. Par exemple, la prise en charge de vSphere 8.0 signifie que vSAN 8.0 est également pris en charge.

Limites

- **Machines tolérantes aux pannes**
  L'agent Pour VMware sauvegarde les machines tolérantes aux pannes uniquement si cette tolérance a été activée sur VMware vSphere 6.0 et versions ultérieures. Si vous avez effectué une mise à niveau à partir d'une ancienne version de vSphere, il vous suffit de désactiver puis d'activer la tolérance aux pannes sur chaque machine. Si vous utilisez une version antérieure de vSphere, installez un agent sur le système d'exploitation invité.
- **Disques et RDM indépendants**
  L'agent pour VMware ne sauvegarde pas les disques mappage de terminal brut (RDM) en mode de compatibilité physique ni les disques indépendants. L'agent ignore ces disques et ajoute des avertissements au journal. Vous pouvez éviter les avertissements en excluant des disques et RDM indépendants en mode de compatibilité physique à partir du plan de protection. Si vous voulez sauvegarder ces disques ou données, installez un agent sur le système d'exploitation invité.
- **Connexion iSCSI en tant qu'invité**
  L'agent pour VMware ne sauvegarde pas les volumes LUN connectés par un initiateur iSCSI qui fonctionne sous le système d'exploitation invité. Étant donné que l'hyperviseur ESXi n'a pas connaissance de ces volumes, ces derniers ne sont pas inclus dans les instantanés au niveau de l'hyperviseur et sont omis d'une sauvegarde sans avertissement. Si vous souhaitez sauvegarder ces volumes ou ces données sur ces volumes, installez un agent sur le système d'exploitation invité.
- **Machines virtuelles chiffrées** (introduites dans VMware vSphere 6.5)
  - Les machines virtuelles sont sauvegardées à l'état chiffré. Si le chiffrement est essentiel pour vous, activez le chiffrement des sauvegardes lors de la création d'un plan de protection.
  - Les machines virtuelles restaurées sont toujours chiffrées. Une fois la restauration terminée, vous pouvez activer le chiffrement manuellement.
  - Si vous sauvegardez des machines virtuelles chiffrées, nous vous recommandons de chiffrer également la machine virtuelle sur laquelle l'agent pour VMware est exécuté. Dans le cas contraire, les opérations des machines chiffrées risquent d'être plus lentes que prévu. Appliquez la **politique de chiffrement VM** à la machine de l'agent à l'aide du client vSphere Web.

- Les machines virtuelles chiffrées sont sauvegardées via LAN, même si vous configurez le mode de transport SAN pour l'agent. L'agent revient au transport NBD, car VMware ne prend pas en charge le transport SAN pour la sauvegarde de disques virtuels chiffrés.

- **Secure Boot**
  - Machines virtuelles VMware : (introduites dans VMware vSphere 6.5) **Secure Boot** est désactivé dès qu'une machine virtuelle est restaurée en tant que nouvelle machine virtuelle. Une fois la restauration terminée, vous pouvez activer cette option manuellement. Cette restriction s'applique à VMware.
  - Machines virtuelles Hyper-V : Pour toutes les MV GEN2, Secure Boot est désactivé dès qu'une machine virtuelle est restaurée vers une nouvelle machine virtuelle ou une machine virtuelle existante.
- **La sauvegarde de la configuration ESXi** n'est pas prise en charge pour VMware vSphere 7.0.
- **Opérations prises en charge pour les ordinateurs dotés de volumes logiques**
  La sauvegarde et la restauration des ressources avec volumes logiques, tels que LDM dans Windows (disques dynamiques) et LVM dans Linux, sont prises en charge avec certaines limitations. Pour plus d'informations sur ces limitations, voir "Opérations prises en charge pour les volumes logiques" (p. 59).

Microsoft

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Windows Server 2008 (x64) avec Hyper-V Windows Server 2008 R2 avec Hyper-V Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 avec Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1 (x64) avec Hyper-V Windows 10 avec Hyper-V Windows Server 2016 avec Hyper-V – toutes les options d'installation, excepté Nano Server Microsoft Hyper-V Server 2016	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Hyper-V**	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Windows Server 2019 avec Hyper-V – toutes les options d'installation, excepté Nano Server Microsoft Hyper-V Server 2019 Windows Server 2022 avec Hyper-V – toutes les options d'installation, excepté Nano Server		
Microsoft Virtual PC 2004, 2007 Windows Virtual PC	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Microsoft Virtual Server 2005	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

Remarque
Les machines virtuelles Hyper-V en cours d'exécution sur un cluster hyperconvergent avec espaces de stockage directs (S2D) sont prises en charge. Les Espaces de Stockage Directs sont également pris en charge en tant que stockage des sauvegardes.

Limites

- **Disques pass-through**
  L'agent pour Hyper-V ne sauvegarde pas les disques pass-through. Pendant la sauvegarde, l'agent ignore ces disques et ajoute des avertissements au journal. Vous pouvez éviter les avertissements en excluant des disques pass-through du plan de protection. Si vous voulez sauvegarder ces disques ou données, installez un agent sur le système d'exploitation invité.
- **Mise en cluster invité Hyper-V**
  Agent pour Hyper-V ne prend pas en charge la sauvegarde des machines virtuelles Hyper-V qui constituent des nœuds d'un cluster de basculement Windows Server. Un instantané VSS au niveau hôte peut même temporairement déconnecter le disque quorum externe du cluster. Si vous voulez sauvegarder ces machines, installez les agents dans les systèmes d'exploitation invités.

- **Connexion iSCSI en tant qu'invité**
  L'agent pour Hyper-V ne sauvegarde pas les volumes LUN connectés par un initiateur iSCSI qui fonctionne sous le système d'exploitation invité. Étant donné que l'hyperviseur Hyper-V n'a pas connaissance de ces volumes, ces derniers ne sont pas inclus dans les instantanés au niveau de l'hyperviseur et sont omis d'une sauvegarde sans avertissement. Si vous souhaitez sauvegarder ces volumes ou ces données sur ces volumes, installez un agent sur le système d'exploitation invité.
- **Secure Boot**
  Pour toutes les MV GEN2, Secure Boot est désactivé dès qu'une machine virtuelle est restaurée vers une nouvelle machine virtuelle ou une machine virtuelle existante.
- **Opérations prises en charge pour les ordinateurs dotés de volumes logiques**
  La sauvegarde et la restauration des ressources avec volumes logiques, tels que LDM dans Windows (disques dynamiques) et LVM dans Linux, sont prises en charge avec certaines limitations. Pour plus d'informations sur ces limitations, voir "Opérations prises en charge pour les volumes logiques" (p. 59).
- **Noms de fichiers VHD/VHDX avec symboles d'esperluette**
  Sur les hôtes Hyper-V exécutant Windows Server 2016 ou une version ultérieure, vous ne pouvez pas sauvegarder les machines virtuelles existantes (version 5.0) créées à l'origine avec Hyper-V 2012 R2 ou une version antérieure si le nom de leurs fichiers VHD/VHDX contient le symbole d'esperluette (&).
  Pour pouvoir sauvegarder ces machines, accédez à Hyper-V Manager, puis dissociez de la machine virtuelle le disque virtuel souhaité, modifiez le nom de fichier VHD/VHDX en supprimant le symbole esperluette, puis réassociez le disque à la machine virtuelle.
- **Dépendance à l'égard du sous-système Microsoft WMI**
  Les sauvegardes sans agent des machines virtuelles Hyper-V dépendent du sous-système Microsoft WMI, et en particulier de la classe `Msvm_VirtualSystemManagementService`. Si les requêtes WMI échouent, les sauvegardes échoueront également. Pour plus d'informations sur la classe `Msvm_VirtualSystemManagementService`, voir la documentation Microsoft.

Scale Computing

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Scale Computing HC3**	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

Limites

Opérations prises en charge pour les ordinateurs dotés de volumes logiques

La sauvegarde et la restauration des ressources avec volumes logiques, tels que LDM dans Windows (disques dynamiques) et LVM dans Linux, sont prises en charge avec certaines limitations. Pour plus d'informations sur ces limitations, voir "Opérations prises en charge pour les volumes logiques" (p. 59).

Citrix

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Citrix XenServer/Citrix Hypervisor 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 8.0, 8.1, 8.2	Non pris en charge	Pris en charge uniquement pour les invités entièrement virtualisés (également appelés HVM). Les invités paravirtualisés (également appelés PV) ne sont pas pris en charge. **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Citrix XenServer** > **Windows** ou **Linux**

Red Hat et Linux

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 Red Hat Virtualization (RHV) 4.0, 4.1	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Virtualisation Red Hat (gérée par oVirt) 4.2, 4.3, 4.4, 4.5	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Red Hat Virtualization (oVirt)**	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Machines virtuelles basées sur un noyau (KVM)	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **KVM** > **Windows** ou **Linux**
Machines virtuelles basées sur un noyau (KVM) gérées par oVirt 4.3	Pris en charge	Pris en charge

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
exécuté sur Red Hat Enterprise Linux 7.6, 7.7 ou CentOS 7.6, 7.7	**Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Red Hat Virtualization (oVirt)**	**Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Machines virtuelles basées sur un noyau (KVM) gérées par oVirt 4.4 exécuté sur Red Hat Enterprise Linux 8.x ou CentOS Stream 8.x	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Red Hat Virtualization (oVirt)**	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Machines virtuelles basées sur un noyau (KVM) gérées par oVirt 4.5 exécuté sur Red Hat Enterprise Linux 8.x ou CentOS Stream 8.x	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Red Hat Virtualization (oVirt)**	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

Limites

Opérations prises en charge pour les ordinateurs dotés de volumes logiques

La sauvegarde et la restauration des ressources avec volumes logiques, tels que LDM dans Windows (disques dynamiques) et LVM dans Linux, sont prises en charge avec certaines limitations. Pour plus d'informations sur ces limitations, voir "Opérations prises en charge pour les volumes logiques" (p. 59).

Parallels

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Parallels Workstation	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Parallels Server 4 Bare Metal	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

Oracle

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Oracle Virtualisation Manager (basé sur oVirt)* 4.3	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Red Hat Virtualization (oVirt)**	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Oracle VM Server 3.0, 3.3, 3.4	Non pris en charge	Pris en charge uniquement pour les invités entièrement virtualisés (également appelés HVM). Les invités paravirtualisés (également appelés PV) ne sont pas pris en charge. **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Oracle** > **Windows** ou **Linux**
Oracle VM VirtualBox 4.x	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Oracle** > **Windows** ou **Linux**

* Oracle Virtualisation Manager est pris en charge par l'agent pour oVirt.

Limites

Opérations prises en charge pour les ordinateurs dotés de volumes logiques

La sauvegarde et la restauration des ressources avec volumes logiques, tels que LDM dans Windows (disques dynamiques) et LVM dans Linux, sont prises en charge avec certaines limitations. Pour plus d'informations sur ces limitations, voir "Opérations prises en charge pour les volumes logiques" (p. 59).

Nutanix

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Nutanix Acropolis Hypervisor (AHV) 20160925.x à 20180425.x	Non pris en charge	Pris en charge

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
		Terminaux > **Ajouter** > **Hôtes de virtualisation** > **Nutanix AHV** > **Windows** ou **Linux**

Virtuozzo

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Virtuozzo 6.0.10, 6.0.11, 6.0.12	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Virtuozzo**	Pris en charge pour les machines virtuelles uniquement. Les conteneurs ne sont pas pris en charge. **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Virtuozzo 7.0.13, 7.0.14	Pris en charge pour les conteneurs ploop uniquement. Les machines virtuelles ne sont pas prises en charge. **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Virtuozzo**	Pris en charge pour les machines virtuelles uniquement. Les conteneurs ne sont pas pris en charge. **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Virtuozzo Hybrid Server 7.5	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Virtuozzo**	Pris en charge pour les machines virtuelles uniquement. Les conteneurs ne sont pas pris en charge. **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

Limites

Opérations prises en charge pour les ordinateurs dotés de volumes logiques

La sauvegarde et la restauration des ressources avec volumes logiques, tels que LDM dans Windows (disques dynamiques) et LVM dans Linux, sont prises en charge avec certaines limitations. Pour plus

d'informations sur ces limitations, voir "Opérations prises en charge pour les volumes logiques" (p. 59).

Vituozzo Hybrid Infrastructure

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Virtuozzo Hybrid Infrastructure 3.5, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Virtuozzo Hybrid Infrastructure**	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

Limites

- **Sauvegarde des MV sans agent avec disques sur un stockage iSCSI externe**
  Vous ne pouvez pas sauvegarder des machines virtuelles à partir de Virtuozzo Hybrid Infrastructure si les disques d'une machine virtuelle sont placés sur des volumes iSCSI externes (associés au cluster VHI).
- **Opérations prises en charge pour les ordinateurs dotés de volumes logiques**
  La sauvegarde et la restauration des ressources avec volumes logiques, tels que LDM dans Windows (disques dynamiques) et LVM dans Linux, sont prises en charge avec certaines limitations. Pour plus d'informations sur ces limitations, voir "Opérations prises en charge pour les volumes logiques" (p. 59).

Amazon

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Instances Amazon EC2	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

Microsoft Azure

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Machines virtuelles Azure	Non pris en charge	Pris en charge

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
		Terminaux > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

Compatibilité avec le logiciel de chiffrage

Les données de sauvegarde et de restauration chiffrées par le logiciel de chiffrement de *niveau de fichier* ne sont soumises à aucune limite.

Un logiciel de chiffrement de *niveau disque* chiffre à la volée. C'est la raison pour laquelle des données contenues dans la sauvegarde ne sont pas chiffrées. Un logiciel de chiffrement de niveau disque modifie généralement les zones système : secteurs de démarrage, tables de partition ou tables de système de fichiers. Ces facteurs ont une incidence sur la sauvegarde et la restauration de niveau disque, sur la possibilité du système restauré de démarrer et d'avoir accès à Secure Zone.

Vous pouvez sauvegarder les données chiffrées par les logiciels de chiffrement de niveau disque suivants :

- Microsoft BitLocker Drive Encryption
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption

Pour assurer une restauration de niveau disque fiable, suivez les règles communes et les recommandations spécifiques au logiciel.

Règle commune d'installation

Nous vous recommandons vivement d'installer le logiciel de chiffrement avant d'installer les agents de protection.

Façon d'utiliser Secure Zone

Secure Zone ne doit pas être chiffrée avec un chiffrement de niveau disque. C'est la seule façon d'utiliser Secure Zone :

1. Installez le logiciel de chiffrement, puis installez l'agent.
2. Créez Secure Zone.
3. Excluez Secure Zone lorsque vous chiffrez le disque ou ses volumes.

Règle de sauvegarde commune

Vous pouvez créer une sauvegarde de niveau disque dans le système d'exploitation.

Procédures de restauration spécifiques au logiciel

Chiffrement de lecteur BitLocker Microsoft

Pour restaurer un système qui a été chiffrée par BitLocker :

1. Démarrer à partir du support de démarrage.
2. Restaurer le système. Les données restaurées seront non chiffrées.
3. Redémarrer le système restauré.
4. Activer BitLocker.

Si vous devez restaurer seulement une partition d'un disque contenant plusieurs partitions, faites-le sous le système d'exploitation. La restauration sous un support de démarrage peut rendre la partition restaurée non détectable pour Windows.

Chiffrement McAfee Endpoint et PGP Whole Disk

Vous pouvez restaurer une partition système chiffrée en utilisant uniquement le support de démarrage.

Si le démarrage du système restauré échoue, reconstruisez le secteur de démarrage principal tel que décrit dans l'article de base de connaissances suivant : https://support.microsoft.com/kb/2622803.

Compatibilité avec les stockages Data Domain Dell EMC

Vous pouvez utiliser les terminaux Data Domain Dell EMC comme stockage des sauvegardes.

Avec ce stockage, nous vous recommandons d'utiliser un modèle de sauvegarde qui crée des sauvegardes complètes régulièrement, par exemple **Toujours complète**. Pour en savoir plus sur les modèles de sauvegarde disponibles, voir "Modèles de sauvegarde" (p. 436).

Le verrou de rétention (mode de gouvernance) est pris en charge. S'il est activé, vous devez ajouter la variable d'environnement `AR_RETENTION_LOCK_SUPPORT` à l'ordinateur avec agent de protection qui utilise ce stockage comme destination de sauvegarde.

Remarque
Les stockages Data Domain Dell EMC dont le verrou de rétention est activé ne sont pas pris en charge par l'agent pour Mac.

Pour ajouter la variable d'environnement `AR_RETENTION_LOCK_SUPPORT`

Sous Windows

1. Connectez-vous en tant qu'administrateur à l'ordinateur avec l'agent de protection.
2. Dans le **Panneau de configuration**, accédez à **Système et sécurité** > **Système** > **Paramètres système avancés**.

3. Dans l'**onglet Avancé**, cliquez sur **Variables d'environnement**.
4. Dans le panneau **Variables système**, cliquez sur **Nouveau**.
5. Dans la fenêtre **Nouvelle variable système**, ajoutez la nouvelle variable comme suit :
   - Nom de la variable : `AR_RETENTION_LOCK_SUPPORT`
   - Valeur de la variable : `1`
6. Cliquez sur **OK**.
7. Dans la fenêtre **Variables d'environnement**, cliquez sur **OK**.
8. Redémarrez la machine.

Sous Linux

1. Connectez-vous en tant qu'administrateur à l'ordinateur avec l'agent de protection.
2. Accédez au répertoire `/sbin`, puis ouvrez le fichier `acronis_mms` à modifier.
3. Ajoutez la ligne suivante au-dessus de la ligne `export LD_LIBRARY_PATH` :

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. Enregistrez le fichier `acronis_mms`.
5. Redémarrez la machine.

Dans une appliance virtuelle

1. Connectez-vous en tant qu'administrateur à l'appliance virtuelle.
2. Accédez au répertoire `/bin`, puis ouvrez le fichier `autostart` à modifier.
3. Ajoutez la ligne suivante sous la ligne `export LD_LIBRARY_PATH` :

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. Enregistrez le fichier `autostart`.
5. Redémarrez l'ordinateur de l'appliance virtuelle.

Fonctionnalités de protection prises en charge par système d'exploitation

Cette rubrique contient des informations sur les fonctionnalités de protection de Cyber Protect Cloud. Elle ne répertorie pas les fonctionnalités de sauvegarde et de restauration.

Les fonctionnalités de protection ne sont prises en charge que sur les ordinateurs sur lesquels un agent de protection est installé. Elles ne sont pas disponibles pour les machines virtuelles sauvegardées en mode sans agent, par exemple par l'agent pour Hyper-V, l'agent pour VMware, l'agent pour Virtuozzo Hybrid Infrastructure, l'agent pour Scale Computing ou l'agent pour oVirt.

Certaines fonctionnalités peuvent nécessiter une licence supplémentaire, en fonction du modèle de gestion de licences appliqué.

Systèmes d'exploitation et versions pris en charge

Windows

Sauf indication contraire pour un ensemble spécifique de fonctionnalités, les versions Windows suivantes sont prises en charge :

- Windows 7 Service Pack 1 et versions ultérieures
- Windows Server 2008 R2 Service Pack 1 et versions ultérieures

---

Remarque
Pour Windows 7, vous devez installer les mises à jour suivantes fournies par Microsoft avant d'installer l'agent de protection.

- Mises à jour de sécurité étendues (ESU) pour Windows 7
- KB4474419
- KB4490628

Pour plus d'informations sur les mises à jour requises, reportez-vous à cet article de la base de connaissances.

Linux

Les distributions Linux et leurs versions prises en charge dépendent des ensembles de fonctionnalités et sont affichées au bas de chaque tableau.

macOS

Les versions macOS prises en charge dépendent des ensembles de fonctionnalités et sont affichées au bas de chaque tableau.

Ensemble de fonctionnalités	Windows	Linux	macOS
Plans de protection par défaut			
Employés en télétravail	Oui	Non	Non
Employés de bureau (Antivirus tiers)	Oui	Non	Non
Employés de bureau (Antivirus Cyber Protect)	Oui	Non	Non
Cyber Protect Essentials (uniquement pour l'édition Cyber Protect Essentials)	Oui	Non	Non
Pour connaître les versions de Windows prises en charge, voir "Systèmes d'exploitation et versions pris en charge" (p. 46).			

Ensemble de fonctionnalités	Windows	Linux	macOS
Sauvegarde de données d'investigation			
Collecter le vidage mémoire	Oui	Non	Non
Instantané des processus en cours d'exécution	Oui	Non	Non
Notarisation de la sauvegarde d'investigation de l'image locale	Oui	Non	Non
Notarisation de la sauvegarde d'investigation de l'image Cloud	Oui	Non	Non
Pour connaître les versions de Windows prises en charge, voir "Systèmes d'exploitation et versions pris en charge" (p. 46).			

Fonctionnalités	Windows	Linux	macOS
Protection continue des données (CDP)			
Protection continue des données pour les fichiers et dossiers	Oui	Non	Non
Protection continue des données pour les fichiers modifiés via le suivi de l'application	Oui	Non	Non
Pour connaître les versions de Windows prises en charge, voir "Systèmes d'exploitation et versions pris en charge" (p. 46).			

Ensemble de fonctionnalités	Windows	Linux	macOS
Découverte automatique et installation à distance			
Découverte basée sur le réseau	Oui	Non	Non
Découverte basée sur Active Directory	Oui	Non	Non
Découverte basée sur le modèle (importer les machines depuis un fichier)	Oui	Non	Non
Ajout manuel de terminaux	Oui	Non	Non
Pour connaître les versions de Windows prises en charge, voir "Systèmes d'exploitation et versions pris en charge" (p. 46).			

Ensemble de fonctionnalités	Windows	Linux	macOS
Active Protection			
Détection d'un processus d'injection	Oui	Non	Non

Ensemble de fonctionnalités	Windows	Linux	macOS
Active Protection			
Restauration automatique de fichiers affectés depuis le cache local	Oui	Oui	Oui
Auto-défense pour les fichiers de sauvegarde Acronis	Oui	Non	Non
Auto-défense pour le logiciel Acronis	Oui	Non	Oui (Uniquement les composants Active Protection et Antimalware)
Gestion des processus fiables/bloqués	Oui	Non	Oui
Exclusions des processus/dossiers	Oui	Oui	Oui
Détection des ransomware basée sur un comportement de processus (basé sur l'IA)	Oui	Oui	Oui
Détection du cryptominage basée sur un comportement de processus	Oui	Non	Non
Protection des lecteurs externes (HDD, lecteurs flash, cartes SD)	Oui	Non	Oui
Protection du dossier réseau	Oui	Oui	Oui
Protection côté serveur	Oui	Non	Non
Protection Zoom, Cisco Webex, Citrix Workspace et Microsoft Teams	Oui	Non	Non
Pour plus d'informations sur les systèmes d'exploitation et leurs versions pris en charge, voir "Plates-formes prises en charge" (p. 860).			

Ensemble de fonctionnalités	Windows	Linux	macOS
Protection contre les virus et les malwares			
Fonctionnalité Active Protection totalement intégrée	Oui	Non	Non
Protection contre les malware en temps réel	Oui	Oui, avec le pack antimalware Advanced	Oui, avec le pack antimalware Advanced

Ensemble de fonctionnalités	Windows	Linux	macOS
Protection contre les virus et les malwares			
Fonctionnalité avancée de protection contre les malwares en temps réel avec détection basée sur la signature locale	Oui	Oui	Oui
Analyse statique pour les fichiers exécutables portables	Oui	Non	Oui*
Analyse anti-malware à la demande	Oui	Oui**	Oui
Protection du dossier réseau	Oui	Oui	Non
Protection côté serveur	Oui	Non	Non
Analyse des fichiers d'archive	Oui	Non	Oui
Analyse des lecteurs amovibles	Oui	Non	Oui
Analyse des fichiers nouveaux et modifiés uniquement	Oui	Non	Oui
Exclusions de fichier/dossier	Oui	Oui	Oui***
Exclusions des processus	Oui	Non	Oui
Moteur d'analyse du comportement	Oui	Non	Oui
Prévention des failles	Oui	Non	Non
Quarantaine	Oui	Oui	Oui
Nettoyage automatique de la zone de quarantaine	Oui	Oui	Oui
Filtrage d'URL (http/https)	Oui	Non	Non
Liste blanche à l'échelle de l'entreprise	Oui	Non	Oui
Gestion du pare-feu****	Oui	Non	Non
Gestion de l'antivirus Microsoft Defender*****	Oui	Non	Non
Gestion de Microsoft Security Essentials	Oui	Non	Non
Inscription et gestion de la protection contre les virus et les malwares via le centre de sécurité Windows	Oui	Non	Non
Pour plus d'informations sur les systèmes d'exploitation et leurs versions pris en charge, voir "Plates-			

Ensemble de fonctionnalités	Windows	Linux	macOS
Protection contre les virus et les malwares			
formes prises en charge" (p. 860).			

* L'analyse statique pour les fichiers exécutables portables est prise en charge uniquement pour les analyses planifiées sur macOS.

** Les conditions de démarrage ne sont pas prises en charge pour l'analyse à la demande sous Linux.

*** Les exclusions de fichier/dossier sont prises en charge uniquement lorsque vous spécifiez les fichiers et les dossiers qui ne seront pas analysés par la protection en temps réel ni par les analyses planifiées sur macOS.

**** La gestion du pare-feu est prise en charge sur Windows 8 et versions ultérieures.
Windows Server n'est pas compatible.

***** La gestion de l'antivirus Microsoft Defender est prise en charge sur Windows 8.1 et versions ultérieures.

Ensemble de fonctionnalités	Windows	Linux	macOS
Évaluation des vulnérabilités			
Évaluation des vulnérabilités du système d'exploitation et de ses applications natives	Oui	Oui******	Oui
Évaluation des vulnérabilités pour les applications tierces	Oui	Non	Oui
Pour plus d'informations sur les systèmes d'exploitation et leurs versions pris en charge, voir "Produits Microsoft et tiers pris en charge" (p. 1007), "Produits Linux pris en charge" (p. 1009) et "Produits Apple et tiers pris en charge" (p. 1008).			

****** L'évaluation des vulnérabilités dépend de la disponibilité des alertes de sécurité officielles pour une distribution spécifique, par exemple https://lists.centos.org/pipermail/centos-announce, https://lists.centos.org/pipermail/centos-cr-announce, entre autres.

Ensemble de fonctionnalités	Windows	Linux	macOS
Gestion des correctifs			
Approbation manuelle des correctifs	Oui	Non	Non
Installation automatique des correctifs	Oui	Non	Non
Test des correctifs	Oui	Non	Non
Installation manuelle des correctifs	Oui	Non	Non

Ensemble de fonctionnalités	Windows	Linux	macOS
Gestion des correctifs			
Programmation des correctifs	Oui	Non	Non
Mise à jour corrective sans échec : sauvegarde de machine avant l'installation de correctifs dans le cadre d'un plan de protection	Oui	Non	Non
Annulation du redémarrage d'une machine si une sauvegarde est en cours d'exécution	Oui	Non	Non
Pour connaître les versions de Windows prises en charge, voir "Systèmes d'exploitation et versions pris en charge" (p. 46).			

Fonctionnalités	Windows	Linux	macOS
Carte de la protection des données			
Définition ajustable des fichiers importants	Oui	Non	Non
Analyse des machines pour trouver des fichiers non protégés	Oui	Non	Non
Aperçu des emplacements non protégés	Oui	Non	Non
Capacité à démarrer l'action de protection depuis le widget de carte de protection des données (action **Protéger tous les fichiers**)	Oui	Non	Non
Pour connaître les versions de Windows prises en charge, voir "Systèmes d'exploitation et versions pris en charge" (p. 46).			

Ensemble de fonctionnalités	Windows	Linux	macOS
État de santé du disque			
Contrôle de l'état de santé des HDD et SSD basés sur l'IA	Oui	Non	Non
Pour connaître les versions de Windows prises en charge, voir "Systèmes d'exploitation et versions pris en charge" (p. 46).			

Fonctionnalités	Windows	Linux	macOS
Plans de protection intelligente basés sur les alertes du centre opérationnel de cyberprotection (CPOC) Acronis			
Flux de menaces	Oui	Non	Non
Assistant de réparation	Oui	Non	Non

Fonctionnalités	Windows	Linux	macOS
Plans de protection intelligente basés sur les alertes du centre opérationnel de cyberprotection (CPOC) Acronis			
Pour connaître les versions de Windows prises en charge, voir "Systèmes d'exploitation et versions pris en charge" (p. 46).			

Ensemble de fonctionnalités	Windows	Linux	macOS
Analyse de la sauvegarde			
Analyse anti-malware des sauvegardes d'images dans le cadre du plan de sauvegarde	Oui	Non	Non
Analyse des sauvegardes d'images pour détecter des malwares dans le Cloud	Oui	Non	Non
Analyse des sauvegardes chiffrées pour détecter des malware	Oui	Non	Non
Pour connaître les versions de Windows prises en charge, voir "Systèmes d'exploitation et versions pris en charge" (p. 46).			

Ensemble de fonctionnalités	Windows	Linux	macOS
Restauration sûre			
Analyse anti-malware avec protection contre les virus et les malwares lors du processus de restauration	Oui	Non	Non
Restauration sûre pour les sauvegardes chiffrées	Oui	Non	Non
Pour connaître les versions de Windows prises en charge, voir "Systèmes d'exploitation et versions pris en charge" (p. 46).			

Ensemble de fonctionnalités	Windows	Linux	macOS
Connexion à distance au bureau			
Connexion par NEAR	Oui	Oui	Oui
Connexion par RDP	Oui	Non	Non
Connexion via le Partage d'écran Apple	Non	Non	Oui
Connexion par client Web	Oui	Non	Non
Connexion par Assistance rapide	Oui	Oui	Oui
Assistance à distance	Oui	Oui	Oui

Ensemble de fonctionnalités	Windows	Linux	macOS
Connexion à distance au bureau			
Transfert de fichiers	Oui	Oui	Oui
Transmission de captures d'écran	Oui	Oui	Oui
Pour plus d'informations sur les systèmes d'exploitation et leurs versions pris en charge, voir "Plates-formes prises en charge" (p. 1049).			

Ensemble de fonctionnalités	Windows	Linux	macOS
Score #CyberFit			
Statut de score #CyberFit	Oui	Non	Non
Outil autonome de score #CyberFit	Oui	Non	Non
Recommandations du Score #CyberFit	Oui	Non	Non
Pour connaître les versions de Windows prises en charge, voir "Systèmes d'exploitation et versions pris en charge" (p. 46).			

Ensemble de fonctionnalités	Windows	Linux	macOS
Prévention des pertes de données			
Contrôle des terminaux	Oui	Non	Pris en charge sur les Mac dotés de processeurs Intel et fonctionnant sous macOS 10.15 et versions ultérieures ou macOS 11.2.3 et versions ultérieures. Non supporté par les processeurs Apple Silicon basés sur l'ARM, tels que les Apple M1 / M2.

Ensemble de fonctionnalités	Windows	Linux	macOS
Prévention des pertes de données			
Advanced Data Loss Prevention	Oui	Non	Non
Pour connaître les versions de Windows prises en charge, voir "Systèmes d'exploitation et versions pris en charge" (p. 46).			

Ensemble de fonctionnalités	Windows	Linux	macOS
Options de gestion			
Scénarios de vente incitative pour promouvoir les éditions Cyber Protect	Oui	Oui	Oui
Console d'administration centralisée et à distance basée sur le Web	Oui	Oui	Oui
Systèmes d'exploitation et versions pris en charge : Indépendance par rapport à la plate-forme.			

Ensemble de fonctionnalités	Windows	Linux	macOS
Options de protection			
Effacement à distance	Oui	Non	Non
Pris en charge pour Windows 10 et les versions ultérieures.			

Ensemble de fonctionnalités	Windows	Linux	macOS
Cyber Protect Monitor			
Application Cyber Protect	Oui	Non	Oui
Statut de protection pour Zoom	Oui	Non	Non
Statut de protection pour Cisco Webex	Oui	Non	Non
Statut de protection pour Citrix Workspace	Oui	Non	Non
Statut de protection pour Microsoft Teams	Oui	Non	Non
Pour connaître les versions de Windows prises en charge, voir "Systèmes d'exploitation et versions pris en charge" (p. 46). Sur macOS, Cyber Protect Monitor est pris en charge pour toutes les versions sur lesquelles vous pouvez installer l'agent pour Mac. Pour plus d'informations, voir "Agent pour Mac" (p. 28).			

Ensemble de fonctionnalités	Windows	Linux	macOS
Inventaire du logiciel			
Analyse de l'inventaire du logiciel	Oui	Non	Oui
Surveillance de l'inventaire du logiciel	Oui	Non	Oui
Pour connaître les versions de Windows prises en charge, voir "Systèmes d'exploitation et versions pris en charge" (p. 46). Sur macOS, l'inventaire du logiciel est pris en charge pour les versions 10.13.x à 13.x.			

Ensemble de fonctionnalités	Windows	Linux	macOS
Inventaire du matériel			
Analyse Inventaire matériel	Oui	Non	Oui
Surveillance de l'inventaire matériel	Oui	Non	Oui
Pour connaître les versions de Windows prises en charge, voir "Systèmes d'exploitation et versions pris en charge" (p. 46). Sur macOS, l'inventaire du matériel est pris en charge pour les versions 10.13.x à 13.x.			

Systèmes de fichiers pris en charge

Un agent de protection peut sauvegarder tout système de fichiers accessible depuis le système d'exploitation sur lequel l'agent en question est installé. Par exemple, l'agent pour Windows peut sauvegarder et restaurer un système de fichiers ext4 si le pilote correspondant est installé sur Windows.

Le tableau ci-dessous répertorie les systèmes de fichiers qui peuvent être sauvegardés et restaurés (le support de démarrage prend uniquement en charge la restauration). Les limites s'appliquent aux agents comme au support de démarrage.

Système de fichiers	Pris en charge par			Limites
	Agents	Support de démarrage pour Windows et Linux	Support de démarrage pour Mac	
FAT16/32	Tous les agents	+	+	Aucune limite
NTFS	Tous les	+	+	

Système de fichiers	Pris en charge par			Limites
	Agents	Support de démarrage pour Windows et Linux	Support de démarrage pour Mac	
	agents			
ext2/ext3/ext4	Tous les agents	+	-	
HFS+	Agent pour Mac	-	+	
APFS	Agent pour Mac	-	+	• Prise en charge à partir de macOS High Sierra 10.13 • La configuration du disque doit être recréée manuellement en cas de restauration vers une machine non d'origine ou à froid.
JFS	Agent pour Linux	+	-	• Les filtres de fichier (inclusions/exclusions) ne sont pas pris en charge par le support • Impossible d'activer une sauvegarde incrémentielle/différentielle
ReiserFS3	Agent pour Linux	+	-	
ReiserFS4	Agent pour Linux	+	-	• Les filtres de fichier (inclusions/exclusions) ne sont pas pris en charge par le support • Impossible d'activer une sauvegarde incrémentielle/différentielle • Il n'est pas possible de redimensionner des volumes pendant une restauration
ReFS	Tous les agents	+	+	• Les filtres de fichier (inclusions/exclusions) ne sont pas pris en charge par le support

Système de fichiers	Pris en charge par			Limites
	Agents	Support de démarrage pour Windows et Linux	Support de démarrage pour Mac	
				• Impossible d'activer une sauvegarde incrémentielle/différentielle • Il n'est pas possible de redimensionner des volumes pendant une restauration • Lors de la restauration d'un fichier à partir d'une sauvegarde ReFS, seul le contenu est restauré. Les listes de contrôle d'accès (ACL) et les autres flux ne sont pas restaurés. Les fichiers dispersés sont restaurés comme des fichiers normaux.
XFS	Tous les agents	+	+	• Les filtres de fichier (inclusions/exclusions) ne sont pas pris en charge par le support • Impossible d'activer une sauvegarde incrémentielle/différentielle • Il n'est pas possible de redimensionner des volumes pendant une restauration • Le mode de sauvegarde incrémentielle rapide n'est pas supporté pour le système de fichiers XFS. Les sauvegardes incrémentielles et différentielles de volumes XFS dans le cloud peuvent être considérablement plus lentes que des sauvegardes ext4 comparables qui utilisent le mode incrémentiel rapide.

Système de fichiers	Pris en charge par			Limites
	Agents	Support de démarrage pour Windows et Linux	Support de démarrage pour Mac	
Linux swap	Agent pour Linux	+	-	Aucune limite
exFAT	Tous les agents	+ Un support de démarrage ne peut pas être utilisé pour la reprise si la sauvegarde *est stockée sur* exFAT	+	• Seule la sauvegarde de disque/volume est prise en charge • Les filtres de fichier (inclusions/exclusions) ne sont pas pris en charge par le support • Des fichiers individuels ne peuvent pas être restaurés à partir d'une sauvegarde

Le logiciel passe automatiquement en mode secteur par secteur lorsque la sauvegarde présente des systèmes de fichiers non reconnus ou non pris en charge (par exemple, Btrfs). Il est possible d'effectuer une sauvegarde secteur par secteur pour tout système de fichiers qui :

- est basé sur des blocs ;
- n'utilise qu'un seul disque ;
- dispose d'un schéma de partitionnement MBR/GPT standard.

Si le système de fichiers ne remplit pas ces conditions, la sauvegarde échoue.

Déduplication des données

Dans Windows Server 2012 et versions ultérieures, vous pouvez activer la fonctionnalité de déduplication des données pour un volume NTFS. La déduplication des données réduit l'espace utilisé sur le volume en stockant les fragments de fichiers dupliqués du volume une fois seulement.

Vous pouvez sauvegarder et restaurer au niveau disque et sans limites un volume sur lequel la déduplication des données est activée. La sauvegarde de niveau fichier est prise en charge, sauf lors de l'utilisation du fournisseur VSS Acronis. Pour récupérer des fichiers à partir d'une sauvegarde de disque, exécutez une machine virtuelle depuis votre sauvegarde ou montez la sauvegarde sur un ordinateur exécutant Windows Server 2012 ou version ultérieure, puis copiez les fichiers à partir du volume monté.

La fonctionnalité de déduplication des données de Windows Server n'est pas liée à la fonctionnalité de déduplication Acronis Backup.

Opérations prises en charge pour les volumes logiques

La sauvegarde et la restauration des ressources avec des volumes logiques tels que LDM sous Windows (disques dynamiques) et LVM sous Linux sont prises en charge, mais avec les limitations suivantes.

Sauvegarde

La sauvegarde avec agent est une sauvegarde créée par un agent de protection installé sur la ressource ou sur un support de démarrage.

La sauvegarde sans agent n'est disponible que pour les machines virtuelles. Elle est effectuée au niveau de l'hyperviseur par un agent qui peut sauvegarder et restaurer toutes les machines virtuelles de l'environnement. Aucun agent n'est installé sur les machines virtuelles protégées.

Pour plus d'informations sur les différences entre les sauvegardes avec et sans agent, voir "Sauvegarde avec et sans agent" (p. 67).

Sauvegarde basée sur un agent	Sauvegarde sans agent
• Les volumes logiques sont sauvegardés par volume. • Les filtres de fichiers (inclusions/exclusions) sont pris en charge.	• Lorsqu'un volume logique est détecté sur un disque, ce dernier est sauvegardé en mode secteur par secteur (RAW). La structure de partition du disque n'est pas analysée et aucune image de volume n'est stockée séparément. • Les différents volumes LDM ou LVM ne peuvent pas être sélectionnés comme sources de sauvegarde, ni par sélection directe, ni par la l'utilisation de règles de politique. L'option **Ordinateur complet** est disponible dans la section **Quoi sauvegarder** d'un plan de protection. • Les filtres de fichiers (inclusions/exclusions) ne sont pas pris en charge. Les inclusions ou exclusions configurées seront ignorées.

Restauration

La restauration avec agent est effectuée par un agent installé sur la ressource ou sur un support de démarrage.

La restauration sans agent ne prend en charge que les machines virtuelles en tant que cibles. Elle est effectuée au niveau de l'hyperviseur par un agent qui peut sauvegarder et restaurer toutes les

machines virtuelles de l'environnement. Il n'est pas nécessaire de créer manuellement une machine cible vers laquelle la sauvegarde est restaurée.

	À partir d'une sauvegarde avec agent	**À partir d'une sauvegarde sans agent**
Restauration avec agent	• Une restauration par volume est possible. • La restauration de fichiers et de dossiers est possible.	• La restauration par volume n'est pas disponible. • La restauration de fichiers et de dossiers est possible.
Restauration sans agent	• La migration de machines (P2V, V2P et V2V) n'est pas prise en charge. Pour restaurer des données à partir d'une sauvegarde avec agent, utilisez un support de démarrage. • L'opération **Exécuter en tant que VM** n'est pas prise en charge. • La restauration de fichiers et de dossiers est possible.	• La restauration par volume n'est pas disponible. • La restauration de l'ensemble de la machine est possible. • La restauration de fichiers et de dossiers est possible. • L'opération **Exécuter en tant que VM** est prise en charge. Pour que la machine virtuelle soit amorçable, vous devrez peut-être modifier l'ordre d'amorçage. Pour plus d'informations, consultez cet article de la base de connaissances. • La conversion dans les types de machines virtuelles suivants est prise en charge : ◦ VMware ESXi ◦ Microsoft Hyper-V ◦ HC3 de Scale Computing

Installation et déploiement d'agents Cyber Protection

Préparation

Etape 1

Choisissez un agent en fonction de ce que vous allez sauvegarder. Pour plus d'informations sur les choix possibles, consultez De quel agent ai-je besoin ?

Etape 2

Assurez-vous que l'espace disponible sur votre disque dur est suffisant pour installer un agent. Pour des informations détaillées sur l'espace disque requis, consultez "Configuration système requise pour les agents" (p. 68).

Etape 3

Téléchargez le programme d'installation. Pour trouver les liens de téléchargement, cliquez sur **Tous les terminaux** > **Ajouter**.

La page **Ajouter des terminaux** fournit des programmes d'installation Web pour chacun des agents installés sous Windows. Un programme d'installation Web consiste en un petit fichier exécutable qui télécharge sur Internet le programme d'installation principal et le sauvegarde en tant que fichier temporaire. Ce fichier est automatiquement supprimé après l'installation.

Si vous souhaitez enregistrer les programmes d'installation localement, téléchargez un paquet comprenant tous les agents d'installation pour Windows à l'aide du lien au bas de la page **Ajouter des terminaux**. Des paquets 32 bits et 64 bits sont disponibles. Ces paquets vous permettent de personnaliser la liste des composants à installer. Ces paquets permettent également d'effectuer une installation sans assistance, par exemple via la stratégie de groupe. Ce scénario avancé est décrit dans "Déploiement des agents via la stratégie de groupe" (p. 174).

Pour télécharger le programme d'installation de l'agent pour Microsoft 365, cliquez sur l'icône de compte dans l'angle supérieur droit, puis cliquez sur **Téléchargements** > **Agent pour Microsoft 365**.

L'installation sous Linux et macOS est effectuée depuis les programmes d'installation habituels.

Tous les programmes d'installation requièrent une connexion Internet afin d'enregistrer la machine au sein du service Cyber Protection. Sans connexion Internet, l'installation ne pourra être effectuée.

Etape 4

Les fonctionnalités Cyber Protect nécessitent le package redistribuable Microsoft Visual C++ 2017. Veillez à ce qu'il soit déjà installé sur votre machine, ou installez-le avant d'installer l'agent. Après l'installation de Microsoft Visual C++, il peut être nécessaire de redémarrer l'ordinateur. Le package redistribuable Microsoft Visual C++ est disponible ici https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Etape 5

Assurez-vous que les pare-feu et les autres composants du système de sécurité de votre réseau (comme un serveur proxy) autorisent les connexions sortantes via les ports TCP suivants.

- Ports **443** et **8443**

  Ces ports permettent d'accéder à la console Cyber Protect, d'enregistrer des agents, de télécharger des certificats, d'autoriser des utilisateurs et de télécharger des fichiers depuis le stockage dans le cloud.
- Ports entre **7770** et **7800**

  Ces ports permettent aux agents de communiquer avec le serveur de gestion.
- Ports **44445** et **55556**

  Ces ports permettent aux agents de transférer des données lors du processus de sauvegarde et de restauration.

Si un serveur proxy est activé dans votre réseau, consultez la section "Configuration des paramètres de serveur proxy" (p. 75) afin de vérifier si vous avez besoin de configurer ces paramètres sur chaque ordinateur exécutant un agent de protection.

La vitesse minimale de connexion Internet requise pour gérer un agent du Cloud est 1 Mbit/s (à ne pas confondre avec le taux de transfert de données acceptable pour la sauvegarde dans le Cloud). Prenez ceci en compte si vous utilisez une technologie de connexion à faible bande passante, comme la technologie ADSL.

Ports TCP requis pour la sauvegarde et la réplication de machines virtuelles VMware

- Port **443**

  L'agent pour VMware (Windows et appliances virtuelles) se connecte à ce port sur l'hôte ESXi ou le serveur vCenter afin d'exécuter des opérations de gestion de machine virtuelle, comme la création, la mise à jour et la suppression de machines virtuelles sur vSphere lors des opérations de sauvegarde, de restauration et de réplication de MV.
- Port **902**

  L'agent pour VMware (Windows et appliances virtuelles) se connecte à ce port sur l'hôte ESXi afin d'établir des connexions NFC pour lire/écrire des données sur des disques de machine virtuelle lors des opérations de sauvegarde, de restauration et de réplication de machine virtuelle.

- Port **3333**

  Si l'agent pour VMware (appliances virtuelles) est en cours d'exécution sur le cluster/hôte ESXi qui est la cible de la réplication de machine virtuelle, le trafic de réplication de machine virtuelle ne va pas directement à l'hôte ESXi sur le port **902**. Au lieu de cela, le trafic part de l'agent pour VMware source et va jusqu'au port TCP **3333** de l'agent pour VMware (appliances virtuelles) situé sur le cluster/hôte ESXi cible.

  L'agent pour VMware source qui lit les données à partir des disques de la MV d'origine peut se trouver à n'importe quel autre emplacement et peut être de n'importe quel type : Appliance virtuelle ou Windows.

  Le service chargé d'accepter les données de réplication de MV sur l'agent pour VMware cible (appliance virtuelle) est appelé « serveur de disque de réplica ». Ce service est chargé des techniques d'optimisation WAN, comme la compression et la déduplication du trafic lors de la réplication de MV, notamment l'amorçage du réplica (voir Amorçage d'un réplica initial). Lorsqu'aucun agent pour VMware (appliance virtuelle) n'est en cours d'exécution sur l'hôte ESXi, ce service n'est pas disponible. Par conséquent, le scénario d'amorçage de réplica n'est pas pris en charge.

Ports requis par le composant Téléchargeur

Le composant Téléchargeur est chargé de délivrer des mises à jour à un ordinateur et de les distribuer à d'autres instances du Téléchargeur. Il peut s'exécuter en mode agent, qui transforme l'ordinateur en agent Téléchargeur. L'agent Téléchargeur télécharge des mises à jour depuis Internet et sert de source pour la distribution de mises à jour vers d'autres ordinateurs. Le Téléchargeur nécessite les ports suivants pour fonctionner.

- Port TCP et UDP (entrant) **6888**

  Utilisé par le protocole BitTorrent pour les mises à jour BitTorrent de pair-à-pair.
- Port UDP **6771**

  Utilisé comme port de découverte pair local. Joue également un rôle dans les mises à jour de pair-à-pair.
- Port TCP **18018**

  Utilisé pour la communication entre les programmes de mise à jour fonctionnant dans différents modes : Responsable de la mise à jour et Agent responsable de la mise à jour.
- Port TCP **18019**

  Port local, utilisé pour la communication entre le programme de mise à jour et l'agent de protection.

Étape 6

Vérifiez que les ports locaux suivants ne sont pas utilisés par d'autres processus sur l'ordinateur sur lequel vous prévoyez d'installer l'agent de protection.

- 127.0.0.1:**9999**
- 127.0.0.1:**43234**

- 127.0.0.1:**9850**

Remarque
Vous n'avez pas à les ouvrir dans le pare-feu.

Modification des ports utilisés par l'agent de protection

Il se peut que certains des ports requis par l'agent de protection soient utilisés par d'autres applications de votre environnement. Afin d'éviter les conflits, vous pouvez modifier les ports par défaut utilisés par l'agent de protection en modifiant les fichiers suivants.

- Sous Linux : `/opt/Acronis/etc/aakore.yaml`
- Sous Windows : `\ProgramData\Acronis\Agent\etc\aakore.yaml`

De quel agent ai-je besoin ?

La sélection d'un agent dépend de ce que vous allez sauvegarder. Le tableau ci-dessous regroupe les informations qui vous aideront à faire votre choix.

Sous Windows, l'agent pour Exchange, l'agent pour SQL, l'agent pour Active Directory et l'agent pour Oracle nécessitent que l'agent pour Windows soit installé. Ainsi, si vous installez l'agent pour SQL, par exemple, vous pourrez également sauvegarder la totalité de la machine sur laquelle l'agent est installé.

Nous vous recommandons également d'installer l'agent pour Windows lorsque vous installez l'agent pour VMware (Windows) et l'agent pour Hyper-V.

Sous Linux, l'agent pour Oracle, l'agent pour MySQL/MariaDB et l'agent pour Virtuozzo nécessitent l'installation de l'agent pour Linux (64 bits). Ces agents sont regroupés dans le fichier d'installation de l'agent pour Linux (64 bits).

Qu'allez-vous sauvegarder ?	Quel agent installer ?	Où dois-je l'installer ?
Machines physiques		
Machines physiques fonctionnant sous Windows	Agent pour Windows	Sur la machine qui sera sauvegardée.
Machines physiques fonctionnant sous Linux	Agent pour Linux	
Machines physiques fonctionnant sous macOS	Agent pour Mac	
Bases de données		
Bases de données SQL	Agent pour SQL	Sur une machine fonctionnant sous Microsoft SQL Server.
Bases de données MySQL	Agent pour	Sur l'ordinateur exécutant

	MySQL/MariaDB (Incluses dans le fichier d'installation de l'agent pour Linux (64 bits))	MySQL Server.
Bases de données MariaDB	Agent pour MySQL/MariaDB (Incluses dans le fichier d'installation de l'agent pour Linux (64 bits))	Sur l'ordinateur exécutant MariaDB Server.
Bases de données Exchange	Agent pour Exchange	Sur une machine exécutant le rôle de boîte aux lettres de Microsoft Exchange Server.*
Base de données Oracle	Agent pour Oracle (Sous Linux, inclus avec le fichier d'installation de l'agent pour Linux (64 bits))	Sur la machine sous Oracle Database.
Ressources de cloud à cloud		
Boîtes aux lettres Microsoft 365 (Agent cloud ou agent local)	Agent cloud (Aucune installation n'est requise)	Cette fonctionnalité est disponible avec un agent cloud déployé dans le centre de données. Pour plus d'informations, voir "Utilisation de l'agent Cloud pour Microsoft 365" (p. 638).
	Agent pour Office 365	Sur un ordinateur Windows connecté à Internet. Pour plus d'informations, voir "Utilisation de l'agent pour Office 365 installé localement" (p. 633).
Fichiers OneDrive et sites SharePoint Online Microsoft 365	Agent cloud (Aucune installation n'est requise)	Cette fonctionnalité est disponible avec un agent cloud déployé dans le centre de données. Pour plus d'informations, voir "Utilisation de l'agent Cloud pour Microsoft 365" (p. 638).
Boîtes aux lettres Gmail Google Workspace, fichiers Google Drive, et fichiers de Drive	Agent cloud	Cette fonctionnalité est disponible avec un agent

partagés	(Aucune installation n'est requise)	cloud déployé dans le centre de données. Pour plus d'informations, voir "Protection des données Google Workspace" (p. 674).
Active Directory		
Machines fonctionnant sous les services de domaine Active Directory	Agent pour Active Directory	Sur le contrôleur de domaine.
Machines virtuelles		
Machines virtuelles VMware ESXi	Agent pour VMware (Windows)	Sur une machine sous Windows possédant un accès réseau au vCenter Server et au stockage de la machine virtuelle.**
	Agent pour VMware (appliance virtuelle)	Sur l'hôte ESXi.
Les machines virtuelles Hyper-V	Agent pour Hyper-V	Sur un hôte Hyper-V.
Machines virtuelles Scale Computing HC3	Agent pour Scale Computing HC3 (appliance virtuelle)	Sur l'hôte Scale Computing HC3.
Machines virtuelles Red Hat Virtualization (gérées par oVirt)	Agent pour oVirt (appliance virtuelle)	Sur l'hôte Red Hat Virtualization
Machines virtuelles et conteneurs Virtuozzo***	Agent pour Virtuozzo (Incluses dans le fichier d'installation de l'agent pour Linux (64 bits))	Sur l'hôte Virtuozzo.
Machines virtuelles Virtuozzo Hybrid Infrastructure	Agent pour Virtuozzo Hybrid Infrastructure (Appliance virtuelle)	Sur l'hôte Virtuozzo Hybrid Infrastructure.
Les machines virtuelles hébergées sur Amazon EC2	Comme pour les machines physiques****	Sur la machine qui sera sauvegardée.
Les machines virtuelles hébergées sur Windows Azure		
Machines virtuelles Citrix XenServer		
Red Hat Virtualization (RHV/RHEV), not managed by oVirt		

Machines virtuelles basées sur un noyau (KVM), non gérées par oVirt		
Machines virtuelles Oracle, non gérées par oVirt		
Machines virtuelles Nutanix AHV		
Red Hat Virtualization (RHV/RHEV), gérées par oVirt	Agent pour oVirt (appliance virtuelle)	Sur l'hôte de virtualisation.
Machines virtuelles basées sur un noyau (KVM), gérées par oVirt		
Machines virtuelles Oracle, gérées par oVirt		
Terminaux mobiles		
Terminaux mobiles sous Android	Application mobile pour Android	Sur le terminal mobile qui sera sauvegardé.
Terminaux mobiles sous iOS	Application mobile pour iOS	

*Lors de l'installation, l'agent pour Exchange vérifie que la machine sur laquelle il sera exécuté dispose de suffisamment d'espace libre. Lors de la restauration granulaire, un espace libre égal à 15 % de la plus grosse base de données Exchange est nécessaire de manière temporaire.

**Si votre ESXi utilise un stockage rattaché à un SAN, installez l'agent sur une machine connectée au même SAN. L'agent sauvegardera les machines virtuelles directement à partir du stockage plutôt que via l'hôte ESXi et le réseau local. Pour des instructions détaillées, voir "Agent pour VMware - Sauvegarde sans réseau local" (p. 726).

***Pour Virtuozzo 7, seuls les conteneurs ploop sont pris en charge. Les machines virtuelles ne sont pas prises en charge.

****Une machine est considérée comme étant virtuelle si elle est sauvegardée via un agent externe. Si l'agent est installé dans le système invité, les opérations de sauvegarde et de restauration sont les mêmes que pour une machine physique. Cependant, si Cyber Protection peut identifier une machine virtuelle en utilisant l'instruction CPUID, un quota de service de machine virtuelle lui est attribué.Si vous utilisez l'accès direct ou une autre option qui masque l'ID de fabricant du CPU, seuls des quotas de services pour les machines physiques peuvent être attribués.

Sauvegarde avec et sans agent

Sauvegarde avec agent : requiert l'installation d'un agent de protection sur chaque machine protégée. La sauvegarde avec agent est prise en charge sur toutes les machines physiques et virtuelles. Pour plus d'informations sur l'agent dont vous avez besoin et sur son emplacement d'installation, voir "De quel agent ai-je besoin ?" (p. 64)

La sauvegarde sans agent est prise en charge par certaines plates-formes de virtualisation et n'est pas disponible pour les machines physiques. La sauvegarde sans agent ne nécessite qu'un seul agent de protection, installé sur un ordinateur dédié dans l'environnement virtuel. Cet agent sauvegarde toutes les autres machines virtuelles de cet environnement. Pour plus d'informations sur les types de sauvegarde pris en charge par plate-forme de virtualisation, voir "Plates-formes de virtualisation prises en charge" (p. 32).

Les appliances virtuelles sont disponibles pour certaines plates-formes de virtualisation. Une appliance virtuelle est une machine virtuelle prête à l'emploi contenant un agent de protection. Les appliances virtuelles sont disponibles dans un format propre à l'hyperviseur, par exemple, .ovf, .ova ou .qcow.

De quel type de sauvegarde ai-je besoin ?

Nous recommandons la sauvegarde basée sur un agent si vous avez besoin des éléments suivants :

- Fonctionnalité de protection supplémentaire : antivirus, antimalware, gestion des correctifs ou connexion au bureau à distance. Pour plus d'informations sur ces fonctionnalités, voir "Fonctionnalités de protection prises en charge par système d'exploitation" (p. 45).
- Machines virtuelles séparées au niveau du tenant, par exemple pour que les utilisateurs du tenant n'aient accès qu'à leurs propres sauvegardes.
- Sauvegardes au niveau des fichiers que vous pouvez restaurer sur les systèmes d'exploitation invités.

Nous recommandons la sauvegarde sans agent si vous avez besoin des éléments suivants :

- Il s'agit uniquement d'une sauvegarde, sans aucun dispositif de protection supplémentaire.
- Gestion simplifiée : vous pouvez sauvegarder plusieurs machines virtuelles en installant et en configurant un seul agent.
- Utilisation minimale des ressources : un agent dédié utilise moins de processeur et de mémoire RAM que plusieurs agents installés sur chaque machine virtuelle de votre environnement.
- Configurations de sauvegarde spécifiques, telles que la sauvegarde sans réseau local. Pour plus d'informations sur cette fonctionnalité, voir "Agent pour VMware - Sauvegarde sans réseau local" (p. 726).
- Moins de frais généraux de configuration. L'agent dédié sauvegarde les machines virtuelles au niveau de l'hyperviseur, indépendamment des systèmes d'exploitation invités.

Configuration système requise pour les agents

Agent	Espace disque requis pour l'installation
Agent pour Windows	1,2 Go
Agent pour Linux	2 Go

Agent pour Mac	1 Go
Agent pour SQL et Agent pour Windows	1,2 Go
Agent pour Exchange et Agent pour Windows	1,3 Go
Agent pour empêcher les pertes de données	500 Mo
Agent pour Microsoft 365	500 Mo
Agent pour Active Directory et Agent pour Windows	2 Go
Agent pour VMware et agent pour Windows	1,5 Go
Agent pour Hyper-V et agent pour Windows	1,5 Go
Agent pour Virtuozzo et agent pour Linux	1 Go
Agent pour Virtuozzo Hybrid Infrastructure	700 Mo
Agent pour Oracle et Agent pour Windows	2,2 Go
Agent pour Oracle et agent pour Linux	2 Go
Agent pour MySQL/MariaDB et agent pour Linux	2 Go

Les opérations de sauvegarde, y compris leur suppression, nécessitent environ 1 Go de mémoire RAM par To de taille de sauvegarde. La consommation de mémoire varie en fonction du volume et du type des données traitées par les agents.

Remarque
L'utilisation de la mémoire vive peut augmenter lors de la sauvegarde de très larges ensembles de sauvegarde (4 To et plus).

Dans les systèmes x64, les opérations avec support de démarrage et restauration de disque avec redémarrage nécessitent au moins 2 Go de mémoire.

Sur les ressources avec des processeurs modernes tels que les processeurs Intel Core de 11e génération ou AMD Ryzen 7, qui prennent en charge la technologie CET, certaines fonctionnalités de l'agent pour la prévention des pertes de données sont désactivées afin d'éviter les conflits. Le tableau suivant indique la disponibilité du contrôle des terminaux et des fonctionnalités Advanced DLP sur des systèmes avec des processeurs de ce type.

Fonctionnalités	Contrôle des terminaux	Advanced DLP
Canaux locaux		
Stockage amovible	N/D	Oui

Stockage amovible chiffré	Oui	N/D
Imprimantes	N/D	Non
Lecteurs mappés redirigés	N/D	Oui
Presse-papiers redirigé	N/D	Non
Communications réseau		
E-mails SMTP	N/D	Oui
Microsoft Outlook (MAPI)	N/D	Oui
IBM Notes	N/D	Non
Messageries Web	N/D	Oui
Messagerie instantanée (ICQ)	N/D	Non
Messagerie instantanée (Viber)	N/D	Non
Messagerie instantanée (IRC, Jabber, Skype, Viber)	N/D	Oui
Services de partage de fichiers	N/D	Oui
Réseaux sociaux	N/D	Oui
Partage de fichiers sur réseau local (SMB)	N/D	Oui
Accès Web (HTTP/HTTPS)	N/D	Oui
Transferts de fichiers (FTP/FTPS)	N/D	Oui
Liste d'autorisation de transfert de données		
Liste d'autorisation des types de terminaux	N/D	Oui
Liste d'autorisation des communications réseau	N/D	Oui
Liste d'autorisation des hôtes distants	N/D	Oui
Liste d'autorisation des applications	N/D	Oui
Périphériques		
Stockage amovible	Oui	Oui
Stockage amovible chiffré	Oui	Oui
Imprimantes	Non	Non
Terminaux mobiles connectés par MTP	Non	Non
Adaptateurs Bluetooth	Oui	Oui
Lecteurs optiques	Oui	Oui

Disquettes	Oui	Oui
Presse-papiers Windows	Non	Non
Capture d'écran	Non	Non
Lecteurs mappés redirigés	Oui	Oui
Presse-papiers redirigé	Non	Non
Autoprotection d'agents Cyber Protect		
Protection des utilisateurs finaux standard	Oui	Oui
Protection des administrateurs système locaux	Oui	Oui

Paquets Linux

Pour ajouter les modules nécessaires au noyau Linux, le programme d'installation a besoin des paquets Linux suivants :

- Le paquet comprenant les sources et en-têtes du noyau. La version du paquet doit correspondre à celle de la version de noyau.
- Le système de compilation GNU Compiler Collection (GCC). La version du GCC doit être celle avec laquelle le noyau a été compilé.
- L'outil Make.
- L'interpréteur Perl.
- Les bibliothèques `libelf-dev`, `libelf-devel` ou `elfutils-libelf-devel` pour créer des noyaux à partir de 4.15 et configurées avec CONFIG_UNWINDER_ORC=y. Pour certaines distributions, comme Fedora 28, elles doivent être installées séparément des fichiers en-tête du noyau.

Les noms de ces paquets peuvent varier en fonction de votre distribution Linux.

Sous Red Hat Enterprise Linux, CentOS et Fedora, les paquets sont normalement installés par le programme d'installation. Dans d'autres distributions, vous devez installer les paquets s'ils ne sont pas installés ou ne possèdent pas de la version requise.

Est-ce que les paquets requis sont déjà installés ?

Pour vérifier si les paquets sont déjà installés, effectuez les étapes suivantes :

1. Exécutez la commande suivante pour déterminer la version de noyau et la version de GCC requise :

   ```
   cat /proc/version
   ```

   Cette commande renvoie des lignes similaires aux suivantes : `Linux version 2.6.35.6` et `gcc version 4.5.1`
2. Exécutez la commande suivante pour vérifier si l'outil Make et le compilateur GCC sont installés :

```
make -v
gcc -v
```

Pour **gcc**, assurez-vous que la version renvoyée par la commande est la même que dans `gcc version` à l'étape 1. Pour **make**, assurez-vous simplement que la commande s'exécute.

3. Vérifiez si la version appropriée des paquets pour la génération des modules du noyau est installée :
   - Sous Red Hat Enterprise Linux, CentOS et Fedora, exécutez la commande suivante :
     ```
     yum list installed | grep kernel-devel
     ```
   - Sous Ubuntu, exécutez les commandes suivantes :
     ```
     dpkg --get-selections | grep linux-headers
     dpkg --get-selections | grep linux-image
     ```

   Dans un cas comme dans l'autre, assurez-vous que les versions des paquets sont les mêmes que dans `Linux version` à l'étape 1.
4. Exécutez les commandes suivantes afin de vérifier que l'interpréteur Perl est bien installé :
   ```
   perl --version
   ```

   Si les informations de la version de Perl s'affichent, cela signifie que l'interpréteur est installé.
5. Sous Red Hat Enterprise Linux, CentOS et Fedora, exécutez la commande suivante pour vérifier si `elfutils-libelf-devel` est installé :
   ```
   yum list installed | grep elfutils-libelf-devel
   ```

   Si les informations de la version de la bibliothèque s'affichent, cela signifie que cette dernière est installée.

Installation des paquets à partir de la base de données de référentiel.

Le tableau suivant indique comment installer les paquets requis dans diverses distributions Linux.

Distribution Linux	Noms des paquets	Comment installer
Red Hat Enterprise Linux	**kernel-devel gcc make elfutils-libelf-devel**	Le programme d'installation téléchargera et installera les paquets automatiquement en utilisant votre abonnement Red Hat.

	perl	Exécuter la commande suivante : `yum install perl`
CentOS Fedora	**kernel-devel gcc make elfutils-libelf-devel**	Le programme d'installation téléchargera et installera les paquets automatiquement.
	perl	Exécuter la commande suivante : `yum install perl`

Ubuntu
Debian
	linux-headers linux-image gcc make perl	Exécutez les commandes suivantes :
		`sudo apt-get update`
		`sudo apt-get install linux-headers-$(uname -r)`
		`sudo apt-get install linux-image-$(uname -r)`
		`sudo apt-get install gcc-<package version>`
		`sudo apt-get install make`
		`sudo apt-get install perl`

SUSE Linux
OpenSUSE
	kernel-source gcc make perl	`sudo zypper install kernel-source`
		`sudo zypper install gcc`
		`sudo zypper install make`
		`sudo zypper install perl`

Les paquets seront téléchargés à partir de la base de données de référentiel de la distribution et installés.

Pour d'autres distributions Linux, veuillez vous référer à la documentation de la distribution concernant les noms exacts des paquets requis et les façons de les installer.

Installation manuelle des paquets

Vous pourriez devoir installer les paquets **manuellement** si :

- La machine ne possède pas d'abonnement Red Hat actif ou ne dispose pas d'une connexion Internet.
- Le programme d'installation ne peut pas trouver les versions de **kernel-devel** ou **gcc** correspondant à la version de noyau ; Si la version disponible de **kernel-devel** est plus récente que votre noyau, vous devez soit mettre à jour le noyau ou installer la version correspondante de **kernel-devel** manuellement.

- Vous possédez les paquets requis sur le réseau local et ne voulez pas perdre de temps pour la recherche et le téléchargement automatique.

Obtenez les paquets à partir de votre réseau local ou depuis un site Web tiers auquel vous faites confiance, et installez-les de la façon suivante :

- Sous Red Hat Enterprise Linux, CentOS ou Fedora, exécutez la commande suivante en tant qu'utilisateur racine :

  ```
  rpm -ivh PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```

- Sous Ubuntu, exécutez la commande suivante :

  ```
  sudo dpkg -i PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```

Exemple : Installation manuelle des paquets sous Fedora 14

Suivez ces étapes pour installer les paquets requis dans Fedora 14 sur une machine 32 bits :

1. Exécutez la commande suivante pour déterminer la version de noyau et la version de GCC requise :

   ```
   cat /proc/version
   ```

   Les données de sortie de cette commande incluent les éléments suivants :

   ```
   Linux version 2.6.35.6-45.fc14.i686
   gcc version 4.5.1
   ```

2. Obtenez les paquets **kernel-devel** et **gcc** qui correspondent à cette version de noyau :

   ```
   kernel-devel-2.6.35.6-45.fc14.i686.rpm
   gcc-4.5.1-4.fc14.i686.rpm
   ```

3. Obtenez le paquet **make** pour Fedora 14 :

   ```
   make-3.82-3.fc14.i686
   ```

4. Installez les paquets en exécutant les commandes suivantes en tant qu'utilisateur racine :

   ```
   rpm -ivh kernel-devel-2.6.35.6-45.fc14.i686.rpm
   rpm -ivh gcc-4.5.1.fc14.i686.rpm
   rpm -ivh make-3.82-3.fc14.i686
   ```

   Vous pouvez spécifier tous ces paquets dans une seule commande `rpm`. L'installation de l'un de ces paquets peut nécessiter l'installation d'autres paquets supplémentaires pour résoudre les dépendances.

Configuration des paramètres de serveur proxy

Les agents de protection peuvent transférer des données via un serveur proxy HTTP/HTTPS. Le serveur doit passer par un tunnel HTTP sans analyser ou interférer avec le trafic HTTP. Les proxys intermédiaires ne sont pas pris en charge.

Puisque l'agent s'enregistre dans le cloud lors de l'installation, vous devez configurer les paramètres du serveur proxy lors de l'installation de l'agent ou à l'avance.

Pour Windows

Si un serveur proxy est configuré dans le **Panneau de configuration** > **Options Internet** > **Connexions**, le programme d'installation lit dans le registre les paramètres de serveur proxy et les utilise automatiquement.

Utilisez cette procédure si vous souhaitez effectuer les tâches suivantes.

- Configurez les paramètres de proxy avant l'installation de l'agent.
- Mettez à jour les paramètres de proxy après l'installation de l'agent.

Pour configurer les paramètres de proxy pendant l'installation de l'agent, voir "Installation des agents de protection sous Windows" (p. 80).

Remarque
Cette procédure n'est valable que lorsque le fichier `http-proxy.yaml` n'existe pas sur l'ordinateur. Si le fichier `http-proxy.yaml` existe sur l'ordinateur, vous devez mettre à jour les paramètres de proxy de ce fichier, car ils remplacent ceux du fichier `aakore.yaml`.

Le fichier `%programdata%\Acronis\Agent\var\aakore\http-proxy.yaml` est créé lorsque vous configurez les paramètres du serveur proxy à l'aide de Cyber Protection Monitor. Pour plus d'informations, voir "Configuration des paramètres de serveur proxy dans Cyber Protect Monitor" (p. 325).

Pour ouvrir le fichier `http-proxy.yaml`, vous devez être membre du groupe Administrateurs dans Windows.

Pour configurer les paramètres de proxy

1. Créez un nouveau document texte et ouvrez-le dans un éditeur de texte comme le Bloc-notes.
2. Copiez et collez les lignes suivantes dans le fichier.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Global\HttpProxy]
"Enabled"=dword:00000001
"Host"="proxy.company.com"
"Port"=dword:000001bb
```

```
"Login"="proxy_login"
"Password"="proxy_password"
```

3. Remplacez `proxy.company.com` par votre adresse IP/nom d'hôte de serveur proxy et `000001bb` par la valeur hexadécimale du numéro de port. Par exemple, `000001bb` est le port 443.
4. Si votre serveur proxy nécessite une authentification, remplacez `proxy_login` et `proxy_password` par les informations de connexion au serveur proxy. Dans le cas contraire, supprimez ces lignes du fichier.
5. Enregistrez le document sous `proxy.reg`.
6. Exécutez le fichier en tant qu'administrateur.
7. Confirmez que vous souhaitez modifier le registre Windows.
8. Si l'agent n'est pas encore installé sur cette ressource, installez-le maintenant. Si l'agent est déjà installé sur la ressource, passez à l'étape suivante.
9. Ouvrez le fichier `%programdata%\Acronis\Agent\etc\aakore.yaml` dans un éditeur de texte.
   Pour ouvrir ce fichier, vous devez être membre du groupe Administrateurs dans Windows.
10. Localisez la section **env** ou créez-la, puis ajoutez-y les lignes suivantes.

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

11. Remplacez `proxy_login` et `proxy_password` par les identifiants de connexion au serveur proxy, et `proxy_address:port` par l'adresse et le numéro de port du serveur proxy.
12. Dans le menu **Démarrer**, cliquez sur **Exécuter**, saisissez : **cmd**, puis cliquez sur **OK**.
13. Redémarrez le service aakore en exécutant les commandes suivantes.

```
net stop aakore
net start aakore
```

14. Redémarrez l'agent exécutant les commandes suivantes.

```
net stop mms
net start mms
```

Pour macOS

Utilisez cette procédure si vous souhaitez effectuer les tâches suivantes.

- Configurez les paramètres de proxy avant l'installation de l'agent.
- Mettez à jour les paramètres de proxy après l'installation de l'agent.

Pour configurer les paramètres de proxy pendant l'installation de l'agent, voir "Installation des agents de protection sous macOS" (p. 85).

Pour configurer les paramètres de proxy

1. Créez le fichier `/Library/Application Support/Acronis/Registry/Global.config` et ouvrez-le dans un éditeur de texte tel que TextEdit.
2. Copiez et collez les lignes suivantes dans le fichier.

```
<?xml version="1.0" ?>
<registry name="Global">
    <key name="HttpProxy">
        <value name="Enabled" type="Tdword">"1"</value>
        <value name="Host" type="TString">"proxy.company.com"</value>
        <value name="Port" type="Tdword">"443"</value>
        <value name="Login" type="TString">"proxy_login"</value>
        <value name="Password" type="TString">"proxy_password"</value>
    </key>
</registry>
```

3. Remplacez `proxy.company.com` par votre adresse IP/nom d'hôte de serveur proxy et `443` par la valeur décimale du numéro de port.
4. Si votre serveur proxy nécessite une authentification, remplacez `proxy_login` et `proxy_password` par les informations de connexion au serveur proxy. Dans le cas contraire, supprimez ces lignes du fichier.
5. Enregistrez le fichier.
6. Si l'agent n'est pas encore installé sur cette ressource, installez-le maintenant. Si l'agent est déjà installé sur la ressource, passez à l'étape suivante.
7. Ouvrez le fichier `/Library/Application Support/Acronis/Agent/etc/aakore.yaml` dans un éditeur de texte.
8. Localisez la section **env** ou créez-la, puis ajoutez-y les lignes suivantes.

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

9. Remplacez `proxy_login` et `proxy_password` par les identifiants de connexion au serveur proxy, et `proxy_address:port` par l'adresse et le numéro de port du serveur proxy.
10. Rendez-vous dans **Applications** > **Utilitaires** > **Terminal**.
11. Redémarrez le service aakore en exécutant les commandes suivantes.

```
sudo launchctl stop aakore
sudo launchctl start aakore
```

12. Redémarrez l'agent exécutant les commandes suivantes.

```
sudo launchctl stop acronis_mms
sudo launchctl start acronis_mms
```

Pour Linux

Exécutez le fichier d'installation avec les paramètres `--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN --http-proxy-password=PASSWORD`. Utilisez la procédure suivante pour mettre à jour les paramètres de proxy après l'installation de l'agent de protection.

Pour configurer les paramètres de proxy

1. Ouvrez le fichier `/etc/Acronis/Global.config` dans un éditeur de texte.
2. Effectuez l'une des actions suivantes :
   - Si les paramètres de proxy ont été précisés lors de l'installation de l'agent, localisez la section suivante.

     ```
     <key name="HttpProxy">
         <value name="Enabled" type="Tdword">"1"</value>
         <value name="Host" type="TString">"ADDRESS"</value>
         <value name="Port" type="Tdword">"PORT"</value>
         <value name="Login" type="TString">"LOGIN"</value>
         <value name="Password" type="TString">"PASSWORD"</value>
     </key>
     ```

   - Si les paramètres de proxy n'ont pas été spécifiés pendant l'installation de l'agent, copiez les lignes suivantes et collez-les dans le fichier, entre les balises `<registry name="Global">...</registry>`.

     ```
     <key name="HttpProxy">
         <value name="Enabled" type="Tdword">"1"</value>
         <value name="Host" type="TString">"ADDRESS"</value>
         <value name="Port" type="Tdword">"PORT"</value>
         <value name="Login" type="TString">"LOGIN"</value>
         <value name="Password" type="TString">"PASSWORD"</value>
     </key>
     ```

3. Remplacez `ADDRESS` par la nouvelle adresse IP/nom d'hôte de serveur proxy et `PORT` par la valeur décimale du numéro de port.
4. Si votre serveur proxy nécessite une authentification, remplacez `LOGIN` et `PASSWORD` par les informations de connexion au serveur proxy. Dans le cas contraire, supprimez ces lignes du fichier.
5. Enregistrez le fichier.
6. Ouvrez le fichier `/opt/acronis/etc/aakore.yaml` dans un éditeur de texte.
7. Trouvez la section **env** ou créez-la, puis ajoutez-y les lignes suivantes :

   ```
   env:
       http-proxy: proxy_login:proxy_password@proxy_address:port
       https-proxy: proxy_login:proxy_password@proxy_address:port
   ```

8. Remplacez `proxy_login` et `proxy_password` par les identifiants de connexion au serveur proxy, et `proxy_address:port` par l'adresse et le numéro de port du serveur proxy.
9. Redémarrez le service aakore en exécutant la commande suivante.

```
sudo service aakore restart
```

10. Redémarrez l'agent en exécutant la commande d'exécution dans n'importe quel répertoire.

```
sudo service acronis_mms restart
```

Pour un support de démarrage

En cas d'utilisation d'un support de démarrage, vous pourriez avoir besoin d'accéder au stockage dans le cloud via un serveur proxy. Pour configurer les paramètres du serveur proxy, cliquez sur **Outils** > **Serveur proxy**, puis spécifiez le nom d'hôte/l'adresse IP, le port et les identifiants du serveur proxy.

Installation des agents de protection

Vous pouvez installer les agents sur des machines exécutant l'un des systèmes d'exploitation répertoriés dans « Systèmes d'exploitation et environnements pris en charge ». Les systèmes d'exploitation qui prennent en charge les fonctionnalités Cyber Protect sont répertoriés dans « Fonctionnalités Cyber Protect prises en charges par le système d'exploitation ».

Téléchargement d'agents de protection

Avant d'installer un agent, vous devez télécharger son fichier d'installation depuis la console Cyber Protect.

Pour télécharger un agent lors de l'ajout d'une ressource à protéger

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. En haut à droite, cliquez sur **Ajouter un terminal**.
3. Dans le volet **Ajouter des terminaux**, à partir du menu déroulant **Canal de publication**, sélectionnez une version d'agent.
   - **Version précédente** : télécharger la version d'agent de la version précédente.
   - **Actuelle** : télécharger la version la plus récente de l'agent.
4. Sélectionnez l'agent correspondant au système d'exploitation de la ressource que vous ajoutez. La boîte de dialogue **Enregistrer sous** s'affiche.
5. [Uniquement pour les Mac avec des processeurs Apple silicon (comme Appli M1)] Cliquez sur **Annuler**. Dans le volet **Ajouter un ordinateur Mac** qui s'affiche, cliquez sur le lien **Télécharger ARM installateur**.
6. Sélectionnez un emplacement pour enregistrer le fichier d'agent d'installation et cliquez sur **Enregistrer**.

Pour télécharger un agent pour un usage ultérieur

1. Cliquez sur l'icône **Utilisateur** dans l'angle supérieur droit de la console Cyber Protect.
2. Cliquez sur **Téléchargements**.

3. Dans la boîte de dialogue **Téléchargements**, à partir du menu déroulant **Canal de publication**, sélectionnez une version d'agent.
   - **Version précédente** : télécharger la version d'agent de la version précédente.
   - **Actuelle** : télécharger la version la plus récente de l'agent.
4. Parcourez la liste des installateurs disponibles pour trouver l'installateur d'agent dont vous avez besoin et cliquez sur l'icône de téléchargement au bout de la ligne correspondante.
   La boîte de dialogue **Enregistrer sous** s'affiche.
5. Sélectionnez un emplacement pour enregistrer le fichier d'agent d'installation et cliquez sur **Enregistrer**.

Installation des agents de protection sous Windows

Prérequis

Installez l'agent requis sur la ressource que vous souhaitez protéger. Consultez "Téléchargement d'agents de protection" (p. 79).

Pour installer l'agent pour Windows

1. Assurez-vous que la machine est connectée à Internet.
2. Connectez-vous en tant qu'administrateur, puis exécutez l'installateur.
3. [Facultatif] Cliquez sur **Personnaliser les paramètres d'installation** et procédez aux changements désirés :
   - Pour modifier les composants à installer (par exemple, pour désactiver l'installation de Cyber Protection Monitor ou de l'outil en ligne de commande, ou pour installer l'agent de protection antimalware ou l'agent de filtrage d'URL).

     Remarque
     Sur les ordinateurs Windows, la fonction de protection antimalware nécessite l'installation de l'agent pour la protection antimalware, et la fonction de filtrage d'URL nécessite l'installation de l'agent pour le filtrage d'URL. Ces agents sont installés automatiquement pour les ressources protégées si la **Protection antivirus et antimalware** et/ou les modules de **Filtrage d'URL** sont activés dans leurs plans de protection.

   - Pour modifier la méthode d'enregistrement de la ressource au sein du service Cyber Protection. Vous pouvez passer de l'option **Utiliser la console de service** (par défaut) à **Utiliser les informations d'identification** ou **Utiliser un jeton d'enregistrement**.
   - Pour modifier le chemin d'installation.
   - Pour modifier le compte utilisateur sous lequel le service de l'agent sera exécuté. Pour plus d'informations, veuillez consulter l'article "Changer le compte de connexion sur les machines Windows" (p. 88).
   - Pour vérifier ou modifier le nom d'hôte/l'adresse IP, le port et les informations d'identification du serveur proxy. Si un serveur proxy est activé dans Windows, il est détecté et utilisé automatiquement.

4. Cliquez sur **Installer**.
5. [Lors de l'installation de l'agent pour VMware uniquement] Indiquez l'adresse et les identifiants de vCenter Server ou de l'hôte ESXi autonome dont vous souhaitez sauvegarder et restaurer les machines virtuelles, puis cliquez sur **Terminé**.

   Au lieu d'utiliser un compte existant avec le rôle Administrateur, nous vous recommandons d'utiliser un compte dédié à l'accès à vCenter Server ou à l'hôte ESXi. Pour en savoir plus sur les privilèges nécessaires pour le compte dédié, voir "Agent pour VMware – privilèges nécessaires" (p. 736).
6. [Lors d'une installation sur un contrôleur de domaine uniquement] Spécifiez le compte d'utilisateur depuis lequel l'agent sera exécuté, puis cliquez sur **Terminé**. Pour des raisons de sécurité, le programme d'installation ne crée pas automatiquement de nouveaux comptes sur un contrôleur de domaine.

   Remarque
   Le compte utilisateur que vous indiquez doit disposer du droit `Se connecter en tant que service`. Ce compte doit avoir déjà été utilisé dans le contrôleur de domaine pour que son dossier de profil soit créé sur cet ordinateur.

   Pour plus d'informations sur l'installation de l'agent sur un contrôleur de domaine en lecture seule, consultez cet article de la base de connaissances.
7. Si vous avez conservé la méthode d'enregistrement par défaut **Utiliser la console de service** à l'étape 3, attendez que l'écran d'enregistrement apparaisse, puis passez à l'étape suivante. Sinon, aucune autre action n'est requise.
8. Effectuez l'une des actions suivantes :
   - Si vous vous connectez à l'aide d'un compte administrateur d'entreprise, enregistrez les ressources pour votre société :
     a. Cliquez sur **Enregistrer la ressource**.
     b. Dans la fenêtre de navigateur qui s'affiche, connectez-vous à la console Cyber Protect et consultez les informations d'inscription.
     c. Dans la liste **S'inscrire au compte**, sélectionnez le compte utilisateur avec lequel vous souhaitez enregistrer la ressource.
     d. Cliquez sur **Vérifier le code**, puis sur **Confirmer l'enregistrement**.
   - Si vous vous connectez à l'aide d'un compte administrateur de partenaire, enregistrez les ressources pour vos clients :
     a. Cliquez sur **Enregistrer la ressource**.
     b. Dans la fenêtre de navigateur qui s'affiche, connectez-vous à la console Cyber Protect et consultez les informations d'inscription.
     c. Dans la liste **S'inscrire au compte**, sélectionnez le compte utilisateur de votre client avec lequel vous souhaitez enregistrer la ressource.
     d. Cliquez sur **Vérifier le code**, puis sur **Confirmer l'enregistrement**.

- Cliquez sur **Afficher les informations d'enregistrement**. Le programme d'installation affiche le lien et le code d'enregistrement. Si vous ne pouvez pas terminer l'inscription de la ressource sur l'ordinateur actuel, copiez le lien et le code d'inscription ici, puis suivez les étapes d'inscription sur un autre ordinateur. Dans ce cas, vous devrez saisir le code d'enregistrement dans le formulaire d'enregistrement. Le code d'enregistrement n'est valable qu'une heure.
  Sinon, vous pouvez accéder au formulaire d'enregistrement en cliquant sur **Tous les terminaux** > **Ajouter**, en cherchant **Enregistrement par code**, puis en cliquant sur **Enregistrer**.

  Remarque
  Ne quittez pas le programme d'installation avant d'avoir confirmé l'enregistrement. Pour lancer de nouveau l'enregistrement, vous devrez redémarrer le programme d'installation et répéter la procédure d'installation.

  En conséquence, la ressource sera affectée au compte utilisé pour la connexion à la console Cyber Protect.
- Enregistrez la ressource manuellement à l'aide de la ligne de commande. Pour en savoir plus sur la façon de procéder, reportez-vous à "Inscription et désinscription manuelles des ressources" (p. 125).

9. [Si l'agent est enregistré sous un compte dont le tenant est en mode Conformité] Définissez le mot de passe de chiffrement.

Installation des agents de protection sous Linux

Préparation

- Installez l'agent requis sur l'ordinateur que vous souhaitez protéger. Consultez "Téléchargement d'agents de protection" (p. 79).
- Assurez-vous que les packages Linux nécessaires sont installés sur la machine.
- Lors de l'installation de l'agent dans SUSE Linux, vérifiez que vous utilisez `su -` au lieu de `sudo`. Dans le cas contraire, l'erreur suivante se produit lorsque vous essayez d'inscrire l'agent par l'intermédiaire de la console Cyber Protect : `Échec de lancement du navigateur Web. Aucun affichage disponible.`
  Certaines distributions Linux telles que SUSE ne transmettent pas la variable DISPLAY lors de l'utilisation de sudo et le programme d'installation ne peut pas ouvrir le navigateur dans l'interface graphique.

Installation

Pour installer l'agent pour Linux, vous avez besoin d'au moins 2 Go d'espace disque libre.

Pour installer l'agent pour Linux

1. Assurez-vous que la machine est connectée à Internet.
2. En tant qu'utilisateur root (superutilisateur), accédez au répertoire dans lequel est stocké le fichier d'installation, définissez-le comme fichier exécutable, puis exécutez-le.

   ```
   chmod +x <installation file name>
   ```

   ```
   ./<installation file name>
   ```

   Si un serveur proxy est activé sur votre réseau, lorsque vous exécutez le fichier d'installation, spécifiez le nom d'hôte/l'adresse IP et le port du serveur au format suivant : `--http-proxy-host=ADDRESS` `--http-proxy-port=PORT` `--http-proxy-login=LOGIN` `--http-proxy-password=PASSWORD`.

   Si vous souhaitez modifier la méthode par défaut d'enregistrement de la machine dans le service Cyber Protection, exécutez le fichier d'installation avec l'un des paramètres suivants :
   - `--register-with-credentials` : pour demander un nom d'utilisateur et un mot de passe lors de l'installation
   - `--token=STRING` : pour utiliser un jeton d'enregistrement
   - `--skip-registration` : pour ignorer l'enregistrement
3. Sélectionnez les cases à cocher correspondant aux agents que vous voulez installer. Les agents suivants sont disponibles :
   - Agent pour Linux
   - Agent pour Virtuozzo
   - Agent pour Oracle
   - Agent pour MySQL/MariaDB

   L'agent pour Oracle et l'agent pour Virtuozzo et l'agent pour MySQL/MariaDB nécessitent que l'agent pour Linux (64 bits) soit également installé.
4. Si vous avez conservé la méthode d'enregistrement par défaut à l'étape 2, passez à l'étape suivante. Sinon, saisissez le nom d'utilisateur et le mot de passe du service Cyber Protection, ou attendez que la machine soit enregistrée à l'aide du jeton.
5. Effectuez l'une des actions suivantes :
   - Si vous vous connectez à l'aide d'un compte administrateur d'entreprise, enregistrez les ressources pour votre société :
     a. Cliquez sur **Enregistrer la ressource**.
     b. Dans la fenêtre de navigateur qui s'affiche, connectez-vous à la console Cyber Protect et consultez les informations d'inscription.
     c. Dans la liste **S'inscrire au compte**, sélectionnez le compte utilisateur avec lequel vous souhaitez enregistrer la ressource.
     d. Cliquez sur **Vérifier le code**, puis sur **Confirmer l'enregistrement**.
   - Si vous vous connectez à l'aide d'un compte administrateur de partenaire, enregistrez les ressources pour vos clients :

a. Cliquez sur **Enregistrer la ressource**.

b. Dans la fenêtre de navigateur qui s'affiche, connectez-vous à la console Cyber Protect et consultez les informations d'inscription.

c. Dans la liste **S'inscrire au compte**, sélectionnez le compte utilisateur de votre client avec lequel vous souhaitez enregistrer la ressource.

d. Cliquez sur **Vérifier le code**, puis sur **Confirmer l'enregistrement**.

- Cliquez sur **Afficher les informations d'enregistrement**. Le programme d'installation affiche le lien et le code d'enregistrement. Si vous ne pouvez pas terminer l'inscription de la ressource sur l'ordinateur actuel, copiez le lien et le code d'inscription ici, puis suivez les étapes d'inscription sur un autre ordinateur. Dans ce cas, vous devrez saisir le code d'enregistrement dans le formulaire d'enregistrement. Le code d'enregistrement n'est valable qu'une heure.

  Sinon, vous pouvez accéder au formulaire d'enregistrement en cliquant sur **Tous les terminaux** > **Ajouter**, en cherchant **Enregistrement par code**, puis en cliquant sur **Enregistrer**.

  Remarque
  Ne quittez pas le programme d'installation avant d'avoir confirmé l'enregistrement. Pour lancer de nouveau l'enregistrement, vous devrez redémarrer le programme d'installation et répéter la procédure d'installation.

  En conséquence, la ressource sera affectée au compte utilisé pour la connexion à la console Cyber Protect.
- Enregistrez la ressource manuellement à l'aide de la ligne de commande. Pour en savoir plus sur la façon de procéder, reportez-vous à "Inscription et désinscription manuelles des ressources" (p. 125).

6. [Si l'agent est enregistré sous un compte dont le tenant est en mode Conformité] Définissez le mot de passe de chiffrement.
7. Si UEFI Secure Boot est activé sur l'ordinateur, vous êtes informé que vous devez redémarrer le système après l'installation. Veillez à vous rappeler le mot de passe (celui de l'utilisateur racine ou « acronis ») qui doit être utilisé.

   Remarque
   L'installation génère une nouvelle clé utilisée pour la signature des modules noyau. Vous devez inscrire cette nouvelle clé dans la liste MOK (Machine Owner Key) en redémarrant l'ordinateur. Sans l'inscription de cette clé, votre agent ne sera pas opérationnel. Si vous activez UEFI Secure Boot après l'installation de l'agent, vous devez réinstaller l'agent.

8. Une fois l'installation terminée, effectuez l'une des actions suivantes :
   - Cliquez sur **Redémarrer**, si vous avez été invité à redémarrer le système à l'étape précédente.

Lors du redémarrage du système, choisissez la gestion de clé MOK (Machine Owner Key), sélectionnez **Enroll MOK**, puis inscrivez la clé à l'aide du mot de passe recommandé à l'étape précédente.

- Sinon, cliquez sur **Quitter**.

Les informations concernant le dépannage sont fournies dans le fichier :
`/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL`

Installation des agents de protection sous macOS

Prérequis

Installez l'agent requis sur la ressource que vous souhaitez protéger. Consultez "Téléchargement d'agents de protection" (p. 79).

Pour installer l'agent pour Mac (x64 ou ARM64)

1. Assurez-vous que la machine est connectée à Internet.
2. Double-cliquez sur le fichier d'installation (.dmg).
3. Patientez pendant que le système d'exploitation monte l'image du disque d'installation.
4. Double-cliquez sur **Installer**.
5. Si un serveur proxy est activé dans votre réseau, cliquez sur **Agent de protection** dans la barre de menu, puis sur **Paramètres de serveur proxy**. Spécifiez ensuite l'adresse IP/nom de l'hôte, le port et les informations d'identification de serveur proxy.
6. Si vous y êtes invité, fournissez les informations d'identification de l'administrateur.
7. Cliquez sur **Continuer**.
8. Attendez l'apparition de l'écran d'enregistrement.
9. Effectuez l'une des actions suivantes :
   - Si vous vous connectez à l'aide d'un compte administrateur d'entreprise, enregistrez les ressources pour votre société :
     a. Cliquez sur **Enregistrer la ressource**.
     b. Dans la fenêtre de navigateur qui s'affiche, connectez-vous à la console Cyber Protect et consultez les informations d'inscription.
     c. Dans la liste **S'inscrire au compte**, sélectionnez le compte utilisateur avec lequel vous souhaitez enregistrer la ressource.
     d. Cliquez sur **Vérifier le code**, puis sur **Confirmer l'enregistrement**.
   - Si vous vous connectez à l'aide d'un compte administrateur de partenaire, enregistrez les ressources pour vos clients :
     a. Cliquez sur **Enregistrer la ressource**.
     b. Dans la fenêtre de navigateur qui s'affiche, connectez-vous à la console Cyber Protect et consultez les informations d'inscription.

c. Dans la liste **S'inscrire au compte**, sélectionnez le compte utilisateur de votre client avec lequel vous souhaitez enregistrer la ressource.
d. Cliquez sur **Vérifier le code**, puis sur **Confirmer l'enregistrement**.

- Cliquez sur **Afficher les informations d'enregistrement**. Le programme d'installation affiche le lien et le code d'enregistrement. Si vous ne pouvez pas terminer l'inscription de la ressource sur l'ordinateur actuel, copiez le lien et le code d'inscription ici, puis suivez les étapes d'inscription sur un autre ordinateur. Dans ce cas, vous devrez saisir le code d'enregistrement dans le formulaire d'enregistrement. Le code d'enregistrement n'est valable qu'une heure.

  Sinon, vous pouvez accéder au formulaire d'enregistrement en cliquant sur **Tous les terminaux** > **Ajouter**, en cherchant **Enregistrement par code**, puis en cliquant sur **Enregistrer**.

  Remarque
  Ne quittez pas le programme d'installation avant d'avoir confirmé l'enregistrement. Pour lancer de nouveau l'enregistrement, vous devrez redémarrer le programme d'installation et répéter la procédure d'installation.

  En conséquence, la ressource sera affectée au compte utilisé pour la connexion à la console Cyber Protect.
- Enregistrez la ressource manuellement à l'aide de la ligne de commande. Pour en savoir plus sur la façon de procéder, reportez-vous à "Inscription et désinscription manuelles des ressources" (p. 125).

10. [Si l'agent est enregistré sous un compte dont le tenant est en mode Conformité] Définissez le mot de passe de chiffrement.
11. Si votre version de macOS est Mojave 10.14.x ou une version supérieure, accordez un accès complet au disque à l'agent de protection pour permettre les opérations de sauvegarde.
    Pour les instructions, consultez l'article Grant the 'Full Disk Access' permission to the Cyber Protection agent (64657).
12. Pour utiliser la fonctionnalité Bureau à distance, accordez les autorisations système requises à Agent Connect. Pour plus d'informations, voir "Attribution des autorisations système requises à Agent Connect" (p. 86).

Attribution des autorisations système requises à Agent Connect

Pour activer toutes les caractéristiques de la fonctionnalité Bureau à distance sur les ressources macOS, vous devez autoriser l'accès complet au disque et également affecter les autorisations suivantes à Agent Connect :

- Enregistrement d'écran : permet l'enregistrement d'écran de la ressource macOS via NEAR. Jusqu'à ce que cette autorisation soit accordée, toutes les connexions de contrôle à distance seront refusées.
- Accessibilité : permet d'établir des connexions à distance en mode de contrôle via NEAR

- Microphone : permet la redirection du son d'une ressource macOS distante vers la ressource locale via NEAR. Pour activer la fonctionnalité de redirection du son, vous devez installer un pilote de capture sur la ressource. Pour plus d'informations, voir "Redirection du son à distance" (p. 1051).
- Automatisation : active le vider la corbeille

Une fois l'agent démarré sur la ressource macOS, le système vérifie si cet agent dispose de ces droits et vous demande d'accorder les autorisations le cas échéant.

Pour accorder l'autorisation d'enregistrement de l'écran

1. Dans la zone **Accorder les autorisations système requises** de la boîte de dialogue de l'agent Cyber Protect, cliquez sur **Configurer les autorisations système**.
2. Dans la boîte de dialogue **Autorisations système**, cliquez sur **Demander l'autorisation d'enregistrement de l'écran**.
3. Cliquez sur **Ouvrir les préférences système**.
4. Sélectionnez **Agent Connect**.

Si l'agent ne dispose pas de l'autorisation correspondante lorsque vous essayez d'accéder à distance à la ressource, une boîte de dialogue demandant l'autorisation d'enregistrement d'écran s'affiche. Seul l'utilisateur local peut répondre à cette demande.

Pour accorder l'autorisation d'accessibilité

1. Dans la zone **Accorder les autorisations système requises** de la boîte de dialogue de l'agent Cyber Protect, cliquez sur **Configurer les autorisations système**.
2. Dans la boîte de dialogue **Autorisations système**, cliquez sur **Demander l'autorisation d'accessibilité**.
3. Cliquez sur **Ouvrir les préférences système**.
4. Cliquez sur l'icône en forme de cadenas, en bas à gauche de la fenêtre, afin qu'elle change et affiche un cadenas déverrouillé. Pour que vous puissiez effectuer les modifications, le système vous demande un mot de passe d'administrateur.
5. Sélectionnez **Agent Connect**.

Pour accorder l'autorisation de microphone

1. Dans la zone **Accorder les autorisations système requises** de la boîte de dialogue de l'agent Agent Connect, cliquez sur **Configurer les autorisations système**.
2. Dans la boîte de dialogue **Autorisations système**, cliquez sur **Demander l'autorisation de microphone**.
3. Cliquez sur **OK**.

Remarque
Vous devez également installer un pilote de capture d'écran sur la ressource macOS pour que l'agent puisse utiliser l'autorisation accordée et rediriger le son de la ressource. Pour plus d'informations, voir "Redirection du son à distance" (p. 1051).

Pour accorder l'autorisation d'automatisation

1. Dans la zone **Accorder les autorisations système requises** de la boîte de dialogue de l'agent Agent Connect, cliquez sur **Configurer les autorisations système**.
2. Dans la boîte de dialogue **Autorisations système**, cliquez sur **Demander l'autorisation d'automatisation**.

Changer le compte de connexion sur les machines Windows

À l'écran **Sélectionner les composants**, définissez le compte sous lequel les services seront exécutés en remplissant le champ **Compte d'ouverture de session pour le service de l'agent**. Vous pouvez sélectionner l'une des options suivantes :

- **Utiliser des comptes d'utilisateur du service** (par défaut pour l'agent de service)
  Les comptes d'utilisateur du service sont des comptes système Windows utilisés pour exécuter des services. Ce paramètre présente l'avantage suivant : les politiques de sécurité du domaine n'affectent pas les droits d'utilisateur de ces comptes. Par défaut, l'agent est exécuté sous le compte **Système Local**.
- **Créer un nouveau compte**
  Le nom de compte pour l'agent sera Agent User.
- **Utiliser le compte suivant**
  Si vous installez l'agent sur un contrôleur de domaine, le système vous invite à spécifier des comptes existants (ou le même compte) pour l'agent. Pour des raisons de sécurité, le système ne crée pas automatiquement de nouveaux comptes sur un contrôleur de domaine.
  Le compte utilisateur que vous indiquez lorsque le programme d'installation est exécuté sur un contrôleur de domaine doit disposer du droit `Se connecter en tant que service`. Ce compte doit avoir déjà été utilisé dans le contrôleur de domaine pour que son dossier de profil soit créé sur cet ordinateur.
  Pour plus d'informations sur l'installation de l'agent sur un contrôleur de domaine en lecture seule, consultez cet article de la base de connaissances.

Si vous choisissez de **Créer un nouveau compte** ou choisissez l'option **Utiliser le compte suivant**, assurez-vous que les politiques de sécurité du domaine n'affectent pas les droits d'utilisateur des comptes liés. Si un compte est privé des droits d'utilisateur attribués lors de l'installation, le composant pourrait ne pas fonctionner correctement ou ne pas fonctionner.

Privilèges requis pour le compte de connexion

Un agent de protection est exécuté en tant que service de la machine gérée (MMS) sur une machine Windows. Le compte sous lequel l'agent s'exécutera doit avoir des droits spécifiques pour que

l'agent fonctionne correctement. Ainsi, l'utilisateur du MMS doit se voir attribuer les privilèges suivants :

1. Inclus dans les groupes **Opérateurs de sauvegarde** et **Administrateurs**. Sur un contrôleur de domaine, l'utilisateur doit être inclus dans le groupe **Domaine Admins**.
2. Dispose de la permission **Contrôle complet** sur le dossier `%PROGRAMDATA%\Acronis` (sous Windows XP et Server 2003, `%ALLUSERSPROFILE%\Application Data\Acronis`) et ses sous-dossiers.
3. Dispose de la permission **Contrôle complet** sur certaines clés de registre pour la clé suivante : `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`.
4. Dispose des droits d'utilisateur suivants :
   - Connexion en tant que service
   - Ajuster les quotas de mémoire pour un processus
   - Remplacer un jeton de niveau processus
   - Modifier les valeurs d'environnement du firmware

Comment attribuer les droits d'utilisateur

Suivez les instructions ci-dessous pour attribuer les droits d'utilisateur (cet exemple utilise le droit d'utilisateur **Connexion en tant que service**, la procédure est la même que pour les autres droits d'utilisateur) :

1. Connectez-vous à l'ordinateur en utilisant un compte avec des privilèges d'administration.
2. Ouvrez **Outils administratifs** depuis le **Panneau de configuration** (ou cliquez sur Win+R, saisissez **control admintools**, et appuyez sur Entrée), puis ouvrez **Stratégie de sécurité locale**.
3. Développez **Stratégies locales** et cliquez sur **Attribution des droits d'utilisateur.**
4. Dans le panneau de droite, cliquez avec le bouton droit sur **Connexion en tant que service**, puis sélectionnez **Propriétés**.
5. Cliquez sur le bouton **Ajouter un utilisateur ou un groupe...** pour ajouter un nouvel utilisateur.
6. Dans la fenêtre **Sélectionner des utilisateurs, ordinateurs, comptes de service ou groupes**, trouvez l'utilisateur que vous souhaitez saisir et cliquez sur **OK**.
7. Cliquez sur **OK** dans **les propriétés de Connexion en tant que service** afin d'enregistrer les modifications.

Important
Assurez-vous que l'utilisateur que vous avez ajouté au droit d'utilisateur **Connexion en tant que service** n'est pas répertorié dans la stratégie **Refuser la connexion en tant que service** sous **Stratégie de sécurité locale**.

Notez que nous vous recommandons de ne pas de modifier manuellement les comptes de connexion une fois l'installation terminée.

Installation et désinstallation dynamiques de composants

Pour les ressources Windows protégées par l'agent version 15.0.26986 (publiée en mai 2021) ou versions ultérieures, les composants suivants sont installés de façon dynamique, c'est-à-dire uniquement lorsqu'ils sont requis par un plan de protection :

- Agent de filtrage d'URL : nécessaire aux fonctionnalités de filtrage d'URL.
- Agent de protection antimalware : nécessaire aux fonctionnalités de protection antimalware.
- Agent de prévention des pertes de données : nécessaire aux fonctionnalités de contrôle des terminaux.

Par défaut, ces composants ne sont pas installés. Le composant respectif est automatiquement installé si une ressource devient protégée par un plan dans lequel l'un des modules suivants est activé :

- Protection contre les virus et les malwares
- Filtrage d'URL
- Contrôle des terminaux

De même, si aucun plan de protection n'a encore besoin des fonctionnalités de protection contre les malwares, de filtrage d'URL ou de contrôle des terminaux, le composant respectif est automatiquement désinstallé.

L'installation ou la désinstallation dynamique de composants prend jusqu'à 10 minutes à compter de la modification du plan de protection. Toutefois, si l'une des opérations suivantes est en cours d'exécution, l'installation ou la désinstallation dynamique démarrera une fois cette opération terminée :

- Sauvegarde
- Restauration
- Réplication de sauvegarde
- Réplication de machine virtuelle
- Test d'un réplica
- Exécution d'une machine virtuelle à partir d'une sauvegarde (y compris finalisation)
- Basculement pour reprise d'activité après sinistre
- Restauration automatique pour reprise d'activité après sinistre
- Exécution d'un script (pour la fonctionnalité de création de cyber-scripts)
- Installation des correctifs
- Sauvegarde de la configuration ESXi

Installation ou désinstallation sans assistance

Installation ou désinstallation sans assistance sous Windows

Dans Windows, vous pouvez effectuer une installation ou une désinstallation sans assistance en procédant comme suit :

- En utilisant le fichier EXE du programme d'installation et en indiquant les paramètres d'installation dans la ligne de commande.
- En utilisant un fichier MSI que vous extrayez du programme d'installation et en indiquant les paramètres d'installation de l'une des manières suivantes :
  - Dans un fichier MST
  - Directement dans la ligne de commande

Installation et désinstallation sans assistance à l'aide d'un fichier EXE

Pour ce type d'installation sans assistance, téléchargez le programme d'installation, puis démarrez-le à partir de la ligne de commande avec les paramètres d'installation requis. Pour afficher les paramètres que vous pouvez utiliser, reportez-vous à "Paramètres d'une installation sans assistance (EXE)" (p. 93).

Vous n'avez pas besoin d'extraire à l'avance les packages d'installation et les fichiers MSI et MST.

Installation et désinstallation des agents et des composants (EXE)

Pour effectuer une installation sans assistance avec un fichier EXE, exécutez le programme d'installation et spécifiez les paramètres d'installation dans la ligne de commande.

Pour télécharger le Pour télécharger le programme d'installation, cliquez dans la console Cyber Protect sur l'icône de compte en haut à droite, puis sur **Téléchargements**. Le lien de téléchargement est également disponible dans le panneau **Ajouter des terminaux**.

Pour installer les agents et les composants

1. Démarrez l'interface de ligne de commande en tant qu'administrateur, puis accédez au fichier EXE du programme d'installation.
2. Pour démarrer le programme d'installation et spécifier les paramètres d'installation, exécutez la commande suivante :

   ```
   <file path>/<EXE file><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
   ```

   Utilisez des espaces pour séparer les paramètres, ainsi que des virgules sans espace pour séparer les valeurs des paramètres. Par exemple :

   ```
   C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
   components=agentForWindows,agentForSql,commandLine --install-dir="C:\Program
   ```

```
Files\BackupClient" --reg-address=https://eu2-cloud.company.com --reg-token=34F6-
8C39-4A5C --quiet
```

Pour connaître les paramètres disponibles et leurs valeurs, reportez-vous à "Paramètres d'une installation sans assistance (EXE)" (p. 93).

Exemples

- Installation de l'agent pour Windows, de l'agent de protection contre les malwares, de l'agent pour le filtrage d'URL, de l'outil en ligne de commande et de Cyber Protect Monitor. Enregistrement de la ressource dans le service Cyber Protection à l'aide d'un nom d'utilisateur et d'un mot de passe.

  ```
  C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
  components=agentForWindows,agentForAmp,commandLine,trayMonitor --install-
  dir="C:\Program Files\BackupClient" --agent-account=system --reg-
  address=https://cloud.company.com --reg-login=johndoe --reg-password=johnspassword
  ```

- Installation de l'agent pour Windows, de l'outil de ligne de commande et de Cyber Protect Monitor. Création d'un compte de connexion pour le service de l'agent dans Windows. Enregistrement de la ressource dans le service Cyber Protection à l'aide d'un jeton.

  ```
  C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
  components=agentForWindows,commandLine,trayMonitor --install-dir="C:\Program
  Files\BackupClient" --agent-account=new --reg-address=https://eu2-cloud.company.com -
  -reg-token=34F6-8C39-4A5C
  ```

- Installation de l'agent pour Windows, de l'outil de ligne de commande, de l'agent pour Oracle et de Cyber Protect Monitor. Enregistrement de la machine dans le service Cyber Protection à l'aide d'un nom d'utilisateur et d'un mot de passe.

  ```
  C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
  components=agentForWindows,commandLine,agentForOracle,trayMonitor --install-
  dir="C:\Program Files\BackupClient" --language=en --agent-account=system --reg-
  address=https://cloud.company.com --reg-login=johndoe --reg-password=johnspassword
  ```

- Installation de l'agent pour Windows, de l'outil de ligne de commande et de Cyber Protect Monitor. Définition de la langue de l'interface utilisateur sur Allemand. Enregistrement de la machine dans le service Cyber Protection à l'aide d'un jeton. Définir un proxy HTTP.

  ```
  C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
  components=agentForWindows,commandLine,agentForOracle,trayMonitor --install-
  dir="C:\Program Files\BackupClient"--language=de --agent-account=system --reg-
  address=https://eu2-cloud.company.com --reg-token=34F6-8C39-4A5C --http-proxy-
  address=https://my-proxy.company.com:80 --http-proxy-login=tomsmith --http-proxy-
  password=tomspassword
  ```

Pour supprimer un composant installé

1. Lancez l'interface de ligne de commande en tant qu'administrateur, puis accédez à `%ProgramFiles%\BackupClient\RemoteInstall`.
2. Exécuter la commande suivante :

   ```
   web_installer.exe --remove-components=<value 1>,<value 2> --quiet
   ```

   Pour connaître les paramètres disponibles et leurs valeurs, reportez-vous à "Paramètres d'une installation sans assistance (EXE)" (p. 93).

Exemple

- Désinstallation de Cyber Protect Monitor.

  ```
  C:\Program Files\BackupClient\RemoteInstall\web_installer.exe --remove-components=trayMonitor --quiet
  ```

Pour désinstaller un agent

1. Lancez l'interface de ligne de commande en tant qu'administrateur, puis accédez à `%Program Files%\Common Files\Acronis\BackupAndRecovery`.
2. Exécuter la commande suivante :

   ```
   Uninstaller.exe --quiet --delete-all-settings
   ```

   Pour connaître les paramètres disponibles et leurs valeurs, reportez-vous à "Paramètres d'une installation sans assistance (EXE)" (p. 93).

Exemples

- Désinstallation de l'agent pour Windows et de tous ses composants. Suppression de tous les journaux, tâches et paramètres de configuration.

  ```
  C:\Program Files\Common Files\Acronis\BackupAndRecovery\Uninstaller.exe --quiet --delete-all-settings
  ```

- Désinstallation d'un agent pour Windows protégé par mot de passe et de tous ses composants. Suppression de tous les journaux, tâches et paramètres de configuration.

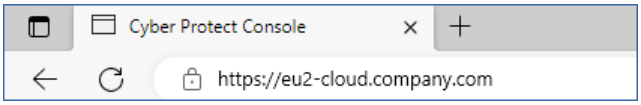
  ```
  C:\Program Files\Common Files\Acronis\BackupAndRecovery\Uninstaller.exe --anti-tamper-password=<password> --quiet --delete-all-settings
  ```

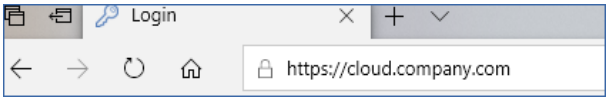
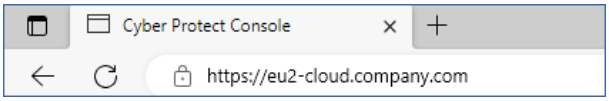
Paramètres d'une installation sans assistance (EXE)

Le tableau suivant récapitule les paramètres de l'installation sans assistance avec un fichier EXE.

Paramètres	Description
Paramètres généraux	

Paramètres	Description
`--add-components=`<component1,component2,...,componentN>	Les composants à installer. Vous trouverez la liste complète des composants disponibles dans "Composants d'une installation sans assistance (EXE)" (p. 98). Lorsque vous spécifiez plusieurs composants, séparez-les par des virgules. N'ajoutez pas d'espaces avant ou après la virgule. Si vous spécifiez des composants déjà installés, ces composants sont réparés ou mis à jour, selon leur version et celle du programme d'installation. Si vous ne spécifiez pas ce paramètre, un ensemble de composants sera installé, selon l'ordinateur sur lequel vous effectuez l'installation. Par exemple, l'agent pour SQL n'est installé que sur les ordinateurs qui exécutent MS SQL Server.
`--install-dir=`<path>	Dossier dans lequel les composants sélectionnés seront installés. Si le dossier spécifié n'existe pas, il sera créé. Si vous ne spécifiez pas ce paramètre, un dossier par défaut est utilisé : `C:\Program Files\BackupClient`.
`--log-dir=`<path>	Le dossier dans lequel les journaux d'installation seront enregistrés. Si vous ne spécifiez pas ce paramètre, un dossier par défaut est utilisé : `%ProgramData%\Acronis\InstallationLogs`.
`--language=`<code>	La langue du produit. Les valeurs suivantes sont disponibles : en, bn, bg, cs, da, de, es, fr, ko, id, it, hi, hu, ms, nl, ja, nb, pl, pt, pt_BR, ru, fi, sr, sv, th, tr, vi, zh, zh_TW. Si vous ne spécifiez pas ce paramètre et que le langage système de l'ordinateur sur lequel vous effectuez l'installation figure dans la liste ci-dessus, le langage système est utilisé. Dans tous les autres cas, la valeur est définie sur en.
`--quiet`	Utilisez ce paramètre pour exécuter le programme d'installation sans afficher l'interface graphique. Ne l'utilisez pas avec le paramètre `--register-only`.
`--help`	Utilisez ce paramètre pour voir la liste de tous les paramètres disponibles que vous pouvez utiliser dans la

Paramètres	Description
	ligne de commande et dans leurs descriptions.
`--fss-onboarding-auto-start`	Utilisez ce paramètre avec le paramètre `--quiet` pour afficher l'assistant d'intégration File Sync & Share après une installation sans assistance.
Paramètres d'enregistrement	
`--registration={skip | by-credentials | by-token | device-flow}`	Utilisez ce paramètre pour choisir le mode d'inscription de l'agent après l'installation. Pour passer l'enregistrement, spécifiez `skip`. Vous pouvez enregistrer l'agent ultérieurement à l'aide du paramètre `--register-only`. Pour enregistrer l'agent à l'aide d'identifiants, spécifiez `by-credentials`, puis utilisez les paramètres `--reg-login` et `--reg-password`. De la même manière, vous pouvez également utiliser uniquement les paramètres `--reg-login` et `--reg-password` ; dans ce cas, la spécification de `--registration=by-credentials` est facultative. Pour enregistrer l'agent avec un jeton d'enregistrement, spécifiez `by-token`, puis utilisez le paramètre `--reg-token`. De la même manière, vous pouvez utiliser uniquement le paramètre `--reg-token` ; dans ce cas, la spécification de `--registration=by-token` est facultative. Pour enregistrer l'agent à l'aide du protocole OAuth 2.0, spécifiez `device-flow`. Une fois l'installation terminée, la page d'inscription s'ouvre automatiquement. Lorsque vous utilisez `--registration=device-flow`, spécifiez l'adresse exacte du centre de données en tant que valeur du paramètre `--reg-address`. Il s'agit de l'URL que vous voyez **une fois que vous êtes connecté** au service Cyber Protection. Par exemple, `https://eu2-cloud.company.com`.  N'utilisez pas `--registration=device-flow` avec le paramètre `--quiet`.
`--reg-address=<url>`	L'URL du service Cyber Protection. Vous pouvez utiliser ce paramètre avec les paramètres `--reg-login` et `--reg-password`, ou avec le paramètre `--reg-token`. • Lorsque vous l'utilisez avec les paramètres `--reg-`

Paramètres	Description
	`login` et `--reg-password`, indiquez l'adresse que vous utilisez **pour vous connecter** au service Cyber Protection. Par exemple, `https://cloud.company.com` :  • Lorsque vous l'utilisez avec le paramètre `--reg-token`, précisez l'adresse exacte du centre de données. Il s'agit de l'URL que vous voyez **une fois que vous êtes connecté** au service Cyber Protection. Par exemple, `https://eu2-cloud.company.com`.  N'utilisez pas `https://cloud.company.com` avec le paramètre `--reg-token`.
`--reg-login=`<login> `--reg-password=`<password>	Les identifiants du compte sous lequel l'agent sera enregistré dans le service Cyber Protection. Il ne peut pas s'agir d'un compte administrateur partenaire. Lorsque vous utilisez ces paramètres, la spécification du paramètre `--registration` est facultative. N'utilisez pas ces paramètres avec le paramètre `--reg-token`.
`--reg-token=`<token>	Le jeton d'enregistrement. Le jeton d'enregistrement est une série de 12 caractères, séparés en trois segments par des traits d'union. Pour plus d'informations sur sa génération, voir "Génération d'un jeton d'enregistrement" (p. 175). Lorsque vous utilisez ce paramètre, la spécification du paramètre `--registration` est facultative. N'utilisez pas ce paramètre avec les paramètres `--reg-login` et `--reg-password`.
`--register-only`	Utilisez ce paramètre pour ignorer l'installation et enregistrer l'agent à l'aide du protocole OAuth 2.0 (device-flow). Une fois l'installation terminée, la page d'inscription s'ouvre automatiquement. N'utilisez pas `--register-only` avec le paramètre `--quiet`.
Compte d'ouverture de session pour le service de l'agent	

Paramètres	Description
`--agent-account`={system | new | custom} ou `--agent-account-login`=<login> `--agent-account-password`=<password>	Utilisez ce paramètre pour indiquer le compte de connexion sous lequel le service de l'agent sera exécuté. Pour plus d'informations sur les comptes de connexion, voir "Changer le compte de connexion sur les machines Windows" (p. 88). Pour utiliser le compte **Système local**, spécifiez `--agent-account=system` ou n'utilisez pas le paramètre `--agent-account` dans votre commande. Pour que le service de l'agent s'exécute sous un nouveau compte de connexion, **Acronis Agent User**, qui est créé automatiquement, spécifiez `new`. Pour que le service de l'agent s'exécute sous un compte existant, spécifiez les identifiants de ce compte à l'aide des paramètres `--agent-account-login` et `--agent-account-password`. Dans ce cas, la spécification du paramètre `--agent-account=custom` est facultative.
Paramètres vCenter/ESXi	
`--esxi-address`=<host>	Le nom d'hôte ou l'adresse IP de vCenter Server ou de l'hôte ESXi. Utilisez ce paramètres lorsque vous installez l'agent pour VMware.
`--esxi-login`=<login> `--esxi-password`=<password>	Les identifiants d'accès à vCenter Server ou à l'hôte ESXi. Utilisez ces paramètres lorsque vous installez l'agent pour VMware.
Paramètres du proxy	
`--http-proxy`={none | system | custom}	Utilisez ce paramètre pour spécifier le serveur proxy HTTP que vous souhaitez utiliser pour la sauvegarde vers le stockage Cloud et pour la restauration à partir de ce stockage. Si vous désactivez les connexions du serveur proxy, spécifiez `--http-proxy=none`. Pour utiliser un serveur proxy à l'échelle du système, spécifiez `--http-proxy=system` ou n'utilisez pas le paramètre `--http-proxy` dans votre commande. Pour utiliser un autre serveur proxy, spécifiez l'adresse du serveur proxy et les identifiants à l'aide des paramètres `--http-proxy-address`, `--http-proxy-login` et `--http-proxy-password`. Dans ce cas, la spécification du

Paramètres	Description
	paramètre `--http-proxy=custom` est facultative.
`--http-proxy-address=`<host>:<port>	Le nom d'hôte ou l'adresse IP, ainsi que le port du serveur proxy HTTP personnalisé.
`--http-proxy-login=`<login>	Identifiant du serveur proxy HTTP personnalisé.
`--http-proxy-password=`<password>	Mot de passe du serveur proxy HTTP personnalisé.
Paramètres de désinstallation	
`--remove-components=`<component1,component2,...,componentN>	Les composants à désinstaller. Vous trouverez la liste complète des composants disponibles dans "Composants d'une installation sans assistance (EXE)" (p. 98). Lorsque vous spécifiez plusieurs composants, séparez-les par des virgules. N'ajoutez pas d'espaces avant ou après la virgule. **Important** En utilisant ce paramètre, vous pouvez désinstaller uniquement les composants. Pour désinstaller le produit complètement, accédez au Panneau de configuration de Windows > Programmes et fonctionnalités, sélectionnez le produit, puis cliquez sur **Désinstaller**.
`--delete-all-settings`	Utilisez ce paramètre facultatif lorsque vous utilisez le paramètre `--remove-components` pour supprimer tous les journaux du produit, les tâches et les paramètres de configuration.
`--anti-tamper-password=`<password>	Le mot de passe requis pour désinstaller un Agent pour Windows protégé par mot de passe ou modifier ses composants.

Composants d'une installation sans assistance (EXE)

Le tableau ci-dessous récapitule les composants que vous pouvez utiliser pour une installation sans assistance par l'intermédiaire d'un fichier EXE. Utilisez les noms de valeurs afin de spécifier des valeurs pour le paramètre `--add-components`.

Pour plus d'informations, voir "Paramètres d'une installation sans assistance (EXE)" (p. 93)"Paramètres d'une installation sans assistance (MSI)" (p. 103)

Nom de la valeur	Description du composant
`agentForWindows`	Agent pour Windows
`agentForSas`	Agent pour Files Sync & Share
`agentForAd`	Agent pour Active Directory
`agentForAmp`	Agent de protection contre les malwares et agent pour de filtrage d'URL
`agentForDlp`	Agent pour empêcher les pertes de données
`agentForEsx`	Agent pour VMware (Windows)
`agentForExchange`	Agent pour Exchange
`agentForHyperV`	Agent pour Hyper-V
`agentForOffice365`	Agent pour Office 365
`agentForOracle`	Agent pour Oracle
`agentForSql`	Agent pour SQL
`commandLine`	Outil de ligne de commande
`mediaBuilder`	Bootable Media Builder
`trayMonitor`	Cyber Protect Monitor
`all`	Cette valeur associe tous les composants.
`allAgents`	Cette valeur associe tous les agents.

Installation et désinstallation sans assistance à l'aide d'un fichier MSI

Pour ce type d'installation sans assistance, utilisez le programme d'installation Windows (programme `Msiexec`). Extrayez les packages d'installation et le fichier MSI à l'avance à l'aide de l'interface graphique du programme d'installation.

Lorsque vous installez les composants avec un fichier MSI, vous pouvez utiliser un fichier de transformation MST pour personnaliser les paramètres d'installation. Pour en savoir plus sur l'utilisation de la combinaison des fichiers MSI et MST, reportez-vous à "Installation des agents et des composants (combinaison MSI et MST)" (p. 100). Vous pouvez utiliser cette méthode d'installation dans un domaine Active Directory pour installer les agents de protection à l'aide de la stratégie de groupe Windows. Pour plus d'informations, voir "Déploiement des agents via la stratégie de groupe" (p. 174).

Vous pouvez également spécifier les paramètres d'installation manuellement dans la ligne de commande. Dans ce cas, vous n'avez pas besoin de fichier MST. Pour plus d'informations, voir "Exemples" (p. 101).

Extraction des fichiers MSI, MST et CAB

Extrayez les fichiers MSI, MST et CAB avec les packages d'installation en exécutant l'interface graphique du programme d'installation.

Pour extraire les fichiers MSI, MST et CAB

1. Exécutez l'interface graphique du programme d'installation, puis cliquez sur **Créer des fichiers .mst et .msi pour une installation sans assistance**.
2. Dans **Que faut-il installer**, sélectionnez les composants que vous souhaitez installer, puis cliquez sur **Terminé**.

   Les packages d'installation de ces composants seront extraits du programme d'installation sous forme de fichiers CAB.
3. Dans **Paramètres d'enregistrement**, sélectionnez **Utiliser les informations d'identification** ou **Utiliser un jeton d'enregistrement**. Selon votre choix, spécifiez les identifiants ou le jeton d'enregistrement, puis cliquez sur **Terminé**.

   Pour plus d'informations sur la génération d'un jeton d'enregistrement, voir "Génération d'un jeton d'enregistrement" (p. 175).
4. [Lors d'une installation sur un contrôleur de domaine uniquement] Dans **Compte d'ouverture de session pour le service de l'agent**, sélectionnez **Utiliser le compte suivant**. Spécifiez le compte utilisateur depuis lequel le service de l'agent sera exécuté, puis cliquez sur **Terminé**. Pour des raisons de sécurité, le programme d'installation ne crée pas automatiquement de nouveaux comptes sur un contrôleur de domaine.

   Remarque
   Le compte utilisateur que vous indiquez doit disposer du droit `Se connecter en tant que service`. Ce compte doit avoir déjà été utilisé dans le contrôleur de domaine pour que son dossier de profil soit créé sur cet ordinateur.

   Pour plus d'informations sur l'installation de l'agent sur un contrôleur de domaine en lecture seule, consultez cet article de la base de connaissances.
5. Vérifiez ou modifiez les autres paramètres d'installation qui seront ajoutés au fichier MST, puis cliquez sur **Poursuivre**.
6. Sélectionnez le dossier dans lequel les fichiers MSI, MST et CAB seront extraits, puis cliquez sur **Générer**.

Installation des agents et des composants (combinaison MSI et MST)

Utilisez le fichier MST pour personnaliser le paramètre d'installation du fichier MSI. Utilisez la combinaison de fichiers MSI et MST lorsque vous installez des agents sur plusieurs ordinateurs par l'intermédiaire d'une stratégie de groupe Windows. Pour plus d'informations, voir "Déploiement des agents via la stratégie de groupe" (p. 174).

Pour installer des composants avec des fichiers MSI et MST

1. Extrayez les fichiers MSI et MST en suivant les indications de "Extraction des fichiers MSI, MST et CAB" (p. 100).
2. Dans l'interface de ligne de commande de l'ordinateur sur lequel vous souhaitez installer des composants, exécutez la commande suivante :

   ```
   msiexec /i <MSI file> TRANSFORMS=<MST file>
   ```

   Par exemple :

   ```
   msiexec /i BackupClient64.msi TRANSFORMS=BackupClient64.msi.mst
   ```

Installation et désinstallation d'agents et de composants (MSI et sélection directe)

Exécutez le fichier MSI, sélectionnez manuellement les composants à installer, puis spécifiez leurs paramètres d'installation dans la ligne de commande. Dans ce cas, vous n'avez pas besoin du fichier MST.

Pour installer les agents et les composants

1. Extrayez le fichier MSI et les packages d'installation (fichiers CAB) en suivant les indications de "Extraction des fichiers MSI, MST et CAB" (p. 100).

   Pour cette méthode d'installation, vous n'avez besoin que des fichiers MSI et CAB. Vous n'avez pas besoin du fichier MST.
2. Dans l'interface de ligne de commande de la machine, exécutez la commande suivante :

   ```
   msiexec /i <MSI file><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
   ```

   Utilisez des espaces pour séparer les paramètres, ainsi que des virgules sans espace pour séparer les valeurs des paramètres. Par exemple :

   ```
   msiexec.exe /i BackupClient64.msi
   ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
   TARGETDIR="C:\Program Files\BackupClient" REGISTRATION_ADDRESS=https://eu2-
   cloud.company.com REGISTRATION_TOKEN=34F6-8C39-4A5C
   ```

   Pour connaître les paramètres disponibles et leurs valeurs, reportez-vous à "Paramètres d'une installation sans assistance (MSI)" (p. 103).

Exemples

- Installation de l'agent pour Windows, de l'agent de protection contre les malwares, de l'agent pour le filtrage d'URL, de l'outil en ligne de commande et de Cyber Protect Monitor. Enregistrement de la ressource dans le service Cyber Protection à l'aide d'un nom d'utilisateur et d'un mot de passe.

  ```
  msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
  ```

```
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,AmpAgentFeature,CommandLineTool,Tray
Monitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_USE_
SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com REGISTRATION_
LOGIN=johndoe REGISTRATION_PASSWORD=johnspassword
```

- Installation de l'agent pour Windows, de l'outil de ligne de commande et de Cyber Protect Monitor. Création d'un compte de connexion pour le service de l'agent dans Windows. Enregistrement de la ressource dans le service Cyber Protection à l'aide d'un jeton.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_CREATE_NEW_
ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com REGISTRATION_TOKEN=34F6-
8C39-4A5C
```

- Installation de l'agent pour Windows, de l'outil de ligne de commande, de l'agent pour Oracle et de Cyber Protect Monitor. Enregistrement de la machine dans le service Cyber Protection à l'aide d'un nom d'utilisateur et encodé dans un mot de passe base64. Vous devrez peut-être encoder votre mot de passe s'il contient des caractères spéciaux ou des espaces vides. Pour plus d'informations sur l'encodage d'un mot de passe, voir "Mots de passe contenant des caractères spéciaux ou des espaces vides" (p. 129).

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,OracleAgentFeature,T
rayMonitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_
LANGUAGE=en MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com
REGISTRATION_LOGIN=johndoe REGISTRATION_PASSWORD_ENCODED=am9obnNwYXNzd29yZA==
```

- Installation de l'agent pour Windows, de l'outil de ligne de commande et de Cyber Protect Monitor. Enregistrement de la machine dans le service Cyber Protection à l'aide d'un jeton. Définir un proxy HTTP.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_LANGUAGE=en
MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com
REGISTRATION_TOKEN=34F6-8C39-4A5C HTTP_PROXY_ADDRESS=https://my-proxy.company.com
HTTP_PROXY_PORT=80 HTTP_PROXY_LOGIN=tomsmith HTTP_PROXY_PASSWORD=tomspassword
```

Pour supprimer un composant installé

1. Extrayez le fichier MSI et les packages d'installation (fichiers CAB) en suivant les indications de "Extraction des fichiers MSI, MST et CAB" (p. 100).

   Pour cette méthode d'installation, vous n'avez besoin que des fichiers MSI et CAB. Vous n'avez pas besoin du fichier MST.
2. Dans l'interface de ligne de commande de la machine, exécutez la commande suivante :

```
msiexec /i <MSI file><REMOVE>=<value 1>,<value 2> REBOOT=ReallySuppress /qn
```

Pour connaître les paramètres disponibles et leurs valeurs, reportez-vous à "Paramètres d'une installation sans assistance (MSI)" (p. 103).

Exemple

- Suppression de Cyber Protect Monitor.

```
msiexec.exe /i BackupClient64.msi /l*v uninstall_log.txt REMOVE=TrayMonitor
REBOOT=ReallySuppress /qn
```

Pour désinstaller un agent

1. Extrayez le fichier MSI et les packages d'installation (fichiers CAB) en suivant les indications de "Extraction des fichiers MSI, MST et CAB" (p. 100).

   Pour cette méthode d'installation, vous n'avez besoin que des fichiers MSI et CAB. Vous n'avez pas besoin du fichier MST.
2. Dans l'interface de ligne de commande de la machine, exécutez la commande suivante :

   ```
   msiexec /x <MSI file> /l*v uninstall_log.txt DELETE_ALL_SETTINGS=1
   REBOOT=ReallySuppress /qn
   ```

   Pour connaître les paramètres disponibles et leurs valeurs, reportez-vous à "Paramètres d'une installation sans assistance (MSI)" (p. 103).

Exemples

- Désinstallation de l'agent pour Windows et de tous ses composants. Suppression de tous les journaux, tâches et paramètres de configuration.

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt DELETE_ALL_SETTINGS=1
REBOOT=ReallySuppress /qn
```

- Désinstallation d'un agent pour Windows protégé par mot de passe et de tous ses composants. Suppression de tous les journaux, tâches et paramètres de configuration.

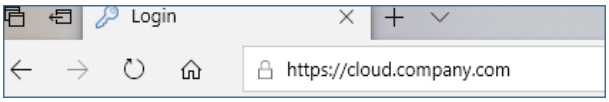
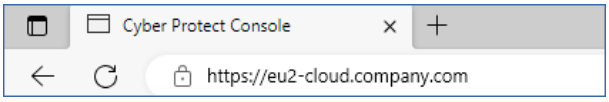
```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt ANTI_TAMPER_
PASSWORD=<password> DELETE_ALL_SETTINGS=1 REBOOT=ReallySuppress /qn
```

Paramètres d'une installation sans assistance (MSI)

Le tableau suivant récapitule les paramètres de l'installation sans assistance lorsque vous utilisez un fichier MSI.

Vous pouvez également utiliser d'autres paramètres `msiexec`. Par exemple, utilisez la commande `/qn` pour empêcher l'affichage des éléments de l'interface utilisateur graphique. Pour en savoir plus sur les paramètres `msiexec`, consultez la documentation Microsoft.

Paramètres	Description
Paramètres généraux	
ADDLOCAL= <component1,component2,...,componentN>	Les composants à installer. Vous trouverez la liste complète des composants disponibles dans "Composants d'une installation sans assistance (MSI)" (p. 107). Lorsque vous spécifiez plusieurs composants, séparez-les par des virgules. N'ajoutez pas d'espaces avant ou après la virgule. **Remarque** Vous devez extraire les fichiers d'installation de tous les composants que vous souhaitez installer. Pour plus d'informations sur l'extraction, voir "Extraction des fichiers MSI, MST et CAB" (p. 100).
TARGETDIR=<path>	Dossier dans lequel les composants sélectionnés seront installés. Si le dossier spécifié n'existe pas, il sera créé. Si vous ne spécifiez pas ce paramètre, un dossier par défaut est utilisé : `C:\Program Files\BackupClient`.
REBOOT=ReallySuppress	Spécifiez ce paramètre si vous souhaitez installer des composants sans redémarrer l'ordinateur.
/l*v <log file>	Spécifiez ce paramètre pour enregistrer un journal détaillé. Ce journal est nécessaire si vous souhaitez enquêter sur des problèmes d'installation.
CURRENT_LANGUAGE=<language ID>	La langue du produit. Les valeurs suivantes sont disponibles : en, bn, bg, cs, da, de, es, fr, ko, id, it, hi, hu, ms, nl, ja, nb, pl, pt, pt_BR, ru, fi, sr, sv, th, tr, vi, zh, zh_TW. Si vous ne spécifiez pas ce paramètre et que le langage système de l'ordinateur sur lequel vous effectuez l'installation figure dans la liste ci-dessus, le langage système est utilisé. Dans tous les autres cas, la valeur est définie sur en.
SKIP_SHA2_KB_CHECK={0,1}	Utilisez ce paramètre lorsque vous souhaitez vérifier si la mise à jour de support de signature du code SHA2 de Microsoft (KB4474419) est installé sur l'ordinateur. La vérification ne s'exécute que sur les systèmes d'exploitation qui nécessitent cette mise à jour. Pour vérifier si elle est nécessaire sur votre système d'exploitation, voir "Systèmes d'exploitation et

Paramètres	Description
	environnements pris en charge" (p. 23). Utilisez ce paramètre avec la valeur définie sur `1` pour ignorer la vérification. Si vous n'indiquez pas ce paramètre ou définissez sa valeur sur `0`, et si la mise à jour du support de signature du code SHA2 est introuvable sur l'ordinateur, l'installation échoue.
`FSS_ONBOARDING_AUTO_START={0,1}`	Utilisez ce paramètre avec la valeur définie sur `1` pour afficher l'assistant d'intégration File Sync & Share après une installation sans assistance. Si vous n'indiquez pas ce paramètre ou définissez sa valeur sur `0`, l'assistant d'intégration ne s'affiche pas.
Paramètres d'enregistrement	
`REGISTRATION_ADDRESS`	L'URL du service Cyber Protection. Vous pouvez utiliser ce paramètre avec les paramètres `REGISTRATION_LOGIN` et `REGISTRATION_PASSWORD`, ou avec `REGISTRATION_TOKEN`. • Lorsque vous l'utilisez avec les paramètres `REGISTRATION_LOGIN` et `REGISTRATION_PASSWORD`, indiquez l'adresse que vous utilisez **pour vous connecter** au service Cyber Protection. Par exemple, `https://cloud.company.com` :  • Lorsque vous l'utilisez avec le paramètre `REGISTRATION_TOKEN`, précisez l'adresse exacte du centre de données. Il s'agit de l'URL que vous voyez **une fois que vous êtes connecté** au service Cyber Protection. Par exemple, `https://eu2-cloud.company.com`.  N'utilisez pas `https://cloud.company.com` avec le paramètre `REGISTRATION_TOKEN`.

`REGISTRATION_LOGIN`
 	
`REGISTRATION_PASSWORD`
	Les identifiants du compte sous lequel l'agent sera enregistré dans le service Cyber Protection. Il ne peut pas s'agir d'un compte administrateur partenaire.
	
	N'utilisez pas ces paramètres avec le paramètre `REGISTRATION_TOKEN`.

Paramètres	Description
REGISTRATION_PASSWORD_ENCODED	Le mot de passe du compte sous lequel l'agent sera enregistré dans le service Cyber Protection, encodé en base64. Pour plus d'informations sur l'encodage de votre mot de passe, voir "Mots de passe contenant des caractères spéciaux ou des espaces vides" (p. 129).
REGISTRATION_TOKEN	Le jeton d'enregistrement. Le jeton d'enregistrement est une série de 12 caractères, séparés en trois segments par des traits d'union. Pour plus d'informations sur sa génération, voir "Génération d'un jeton d'enregistrement" (p. 175). N'utilisez pas ce paramètre avec les paramètres REGISTRATION_LOGIN et REGISTRATION_PASSWORD.
REGISTRATION_REQUIRED={0,1}	Utilisez ce paramètre pour choisir les événements qui se produisent en cas d'échec de l'inscription. Si vous définissez la valeur sur 1, l'installation échoue également. Si vous définissez la valeur sur 0 ou ne spécifiez pas le paramètre, l'installation se déroule correctement, même si l'inscription échoue.
Compte d'ouverture de session pour le service de l'agent	
MMS_USE_SYSTEM_ACCOUNT={0,1}	Utilisez ce paramètre avec la valeur 1 pour que le service s'exécute sous le compte de connexion **Système local**. Pour plus d'informations sur les comptes de connexion, voir "Changer le compte de connexion sur les machines Windows" (p. 88).
MMS_CREATE_NEW_ACCOUNT={0,1}	Utilisez ce paramètre avec la valeur 1 pour que le service de l'agent s'exécute sous le nouveau compte de connexion **Acronis Agent User** qui est créé automatiquement.
MMS_SERVICE_USERNAME=<user name> MMS_SERVICE_PASSWORD=<password>	Utilisez ces paramètres pour indiquer un compte de connexion existant sous lequel le service de l'agent sera exécuté.
Paramètres vCenter/ESXi	
SET_ESX_SERVER={0,1}	Utilisez ce paramètres lorsque vous installez l'agent pour VMware. Si vous définissez la valeur sur 0, l'agent pour VMware ne sera pas connecté à vCenter Server ou à un hôte ESXi. Si vous définissez la valeur sur 1, spécifiez les

Paramètres	Description
	paramètres suivants : ESX_HOST, EXI_USER, ESX_PASSWORD.
ESX_HOST=<nom d'hôte>	Le nom d'hôte ou l'adresse IP de vCenter Server ou de l'hôte ESXi.
ESX_USER=<user name> ESX_PASSWORD=<password>	Les identifiants d'accès à vCenter Server ou à l'hôte ESXi.
Paramètres du proxy	
HTTP_PROXY_ADDRESS=<IP address> HTTP_PROXY_PORT=<port>	Utilisez ces paramètres pour indiquer le serveur proxy HTTP que l'agent utilisera. Si vous n'utilisez pas de serveur proxy, ne spécifiez pas ces paramètres.
HTTP_PROXY_LOGIN=<login> HTTP_PROXY_PASSWORD=<password>	Les accréditations pour le serveur proxy HTTP. Utilisez ces paramètres si le serveur proxy exige une authentification.
Paramètres de désinstallation	
REMOVE={<list of components>|ALL}	Les composants à désinstaller. Lorsque vous spécifiez plusieurs composants, séparez-les par des virgules. N'ajoutez pas d'espaces avant ou après la virgule. Pour supprimer tous les composants de produit, définissez la valeur sur ALL.
DELETE_ALL_SETTINGS={0, 1}	Pour supprimer tous les journaux du produit, les tâches et les paramètres de configuration, définissez la valeur sur 1. Utilisez ce paramètre facultatif lorsque vous utilisez le paramètre REMOVE.
ANTI_TAMPER_PASSWORD=<mot de passe>	Le mot de passe requis pour désinstaller un Agent pour Windows protégé par mot de passe ou modifier ses composants.

Composants d'une installation sans assistance (MSI)

Le tableau ci-dessous récapitule les composants que vous pouvez utiliser pour une installation sans assistance par l'intermédiaire d'un fichier MSI. Utilisez les noms de valeurs afin de spécifier des valeurs pour le paramètre ADDLOCAL. Pour plus d'informations, voir "Paramètres d'une installation sans assistance (MSI)" (p. 103).

Nom de la valeur	Description du composant	Doit être installé avec	Nombre de bits
AgentFeature	Composants clés pour les agents		32 bits/64 bits
MmsMspComponents	Composants clés pour la sauvegarde	AgentFeature	32 bits/64 bits
BackupAndRecoveryAgent	Agent pour Windows	MmsMspComponents	32 bits/64 bits
AmpAgentFeature	Agent for Antimalware protection	BackupAndRecoveryAgent	32 bits/64 bits
UrlFilteringAgentFeature	Agent for URL Filtering	BackupAndRecoveryAgent	32 bits/64 bits
DlpAgentFeature	Agent pour empêcher les pertes de données	BackupAndRecoveryAgent	32 bits/64 bits
SasAgentFeature	Agent pour File Sync & Share	TrayMonitor	32 bits/64 bits
ArxAgentFeature	Agent pour Exchange	MmsMspComponents	32 bits/64 bits
ArsAgentFeature	Agent pour SQL	BackupAndRecoveryAgent	32 bits/64 bits
ARADAgentFeature	Agent pour Active Directory	BackupAndRecoveryAgent	32 bits/64 bits
ArxOnlineAgentFeature	Agent pour Microsoft 365	MmsMspComponents	32 bits/64 bits
OracleAgentFeature	Agent pour Oracle	BackupAndRecoveryAgent	32 bits/64 bits
AcronisESXSupport	Agent pour VMware ESX(i) (Windows)	BackupAndRecoveryAgent	64 bits
HyperVAgent	Agent pour Hyper-V	BackupAndRecoveryAgent	32 bits/64 bits
CommandLineTool	Outil de ligne de commande		32 bits/64 bits

TrayMonitor	Cyber Protect Monitor	AgentFeature	32 bits/64 bits
BackupAndRecoveryBootableComponents	Bootable Media Builder		32 bits/64 bits

Installation ou désinstallation sans assistance sous Linux

Cette section décrit l'installation ou la désinstallation d'agents de protection sans assistance sur une machine sous Linux via la ligne de commande.

Pour installer un agent

1. Ouvrir l'application Terminal.

2. Effectuez l'une des actions suivantes :

- Pour commencer l'installation en précisant les paramètres dans la ligne de commande, exécutez la commande suivante :

  ```
  <package name> -a <parameter 1> ... <parameter N>
  ```

  Ici, `<package name>` est le nom du paquet d'installation (un fichier .i686 ou .x86_64). Tous les paramètres disponibles et leurs valeurs sont décrits dans "Paramètres d'installation ou de désinstallation sans assistance" (p. 110).
- Pour démarrer l'installation avec des paramètres indiqués dans un fichier texte séparé, exécutez la commande suivante :

  ```
  <package name> -a --options-file=<path to the file>
  ```

  Cette approche peut s'avérer utile si vous ne souhaitez pas saisir d'informations sensibles sur la ligne de commande. Dans ce cas, vous pouvez spécifier les paramètres de configuration dans un fichier texte séparé et vous assurer que vous êtes le seul à pouvoir y accéder. Placez chaque paramètre sur une nouvelle ligne, suivi de la valeur de ce paramètre, par exemple :

  ```
  --rain=https://cloud.company.com
  --login=johndoe
  --password=johnspassword
  --auto
  ```

  ou

  ```
  -C
  https://cloud.company.com
  -g
  johndoe
  -w
  johnspassword
  -a
  ```

```
--language
en
```

Si le même paramètre est indiqué aussi bien dans la ligne de commande que dans le fichier texte, la valeur de la ligne de commande le précède.

3. Si l'option UEFI Secure Boot est activée sur l'ordinateur, vous êtes informé que vous devez redémarrer le système après l'installation. Assurez-vous de vous souvenir du mot de passe à utiliser (celui de l'utilisateur root ou « acronis »). Au cours du redémarrage du système, optez pour la gestion de la MOK (Machine Owner Key), choisissez **Enroll MOK**, puis enregistrez la clé en utilisant le mot de passe recommandé.

Si vous activez UEFI Secure Boot après l'installation de l'agent, répétez l'installation en incluant l'étape 3. Dans le cas contraire, les sauvegardes échoueront.

Pour désinstaller un agent

1. Ouvrir l'application Terminal.
2. Effectuez l'une des actions suivantes :
   - Pour désinstaller l'agent et supprimer tous les journaux, tâches et paramètres de configuration, exécutez la commande suivante :

     ```
     /usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall -a
     ```

   - Pour désinstaller l'agent tout en conservant son identifiant (par exemple, si vous prévoyez d'installer l'agent ultérieurement), exécutez la commande suivante :

     ```
     /usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall -a --no-purge
     ```

   - Pour désinstaller l'agent à l'aide du fichier d'installation, exécutez la commande suivante :

     ```
     <package name> -a -u
     ```

     Ici, `<package name>` est le nom du paquet d'installation (un fichier .i686 ou .x86_64). Tous les paramètres disponibles et leurs valeurs sont décrits dans "Paramètres d'installation ou de désinstallation sans assistance" (p. 110).

     Remarque
     Utilisez cette commande uniquement lorsque le package d'installation est la même version que l'agent installé et si `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall` est corrompu ou inaccessible.

Paramètres d'installation ou de désinstallation sans assistance

Cette section décrit les paramètres d'installation ou de désinstallation sans assistance sous Linux.

La configuration minimale pour une installation sans assistance inclut les paramètres et d'enregistrement (par exemple, paramètres `--login` et `--password` ; `--rain` et paramètres `--token`). Vous pouvez utiliser d'autres paramètres pour personnaliser votre installation.

Paramètres d'installation

Paramètres de base

`{-i |--id=}<list of components>`

Les composants à installer, séparés par des virgules et sans caractères d'espace. Les composants suivants sont disponibles pour le package d'installation .x86_64 :

Composant	Description du composant
BackupAndRecoveryAgent	Agent pour Linux
AgentForPCS	Agent pour Virtuozzo
OracleAgentFeature	Agent pour Oracle
MySQLAgentFeature	Agent pour MySQL/MariaDB

Sans ce paramètre, tous les composants ci-dessus seront installés.

L'agent pour Oracle et l'agent pour Virtuozzo et l'agent pour MySQL/MariaDB nécessitent que l'agent pour Linux soit également installé.

Le package d'installation .i686 contient uniquement BackupAndRecoveryAgent.

`{-a|--auto}`

Le processus d'installation et d'enregistrement s'achèvera sans autre intervention de l'utilisateur. Lorsque vous utilisez ce paramètre, vous devez préciser le compte sous lequel l'agent sera enregistré dans le service Cyber Protection, soit à l'aide du paramètre `--token`, soit à l'aide des paramètres `--login` et `--password`.

`{-t|--strict}`

Si le paramètre est spécifié, tous les avertissements pendant l'installation conduiront à un échec de l'installation. Sans ce paramètre, l'installation se termine avec succès même en cas d'avertissement.

`{-n|--nodeps}`

L'absence des packages Linux requis sera ignorée pendant l'installation.

`{-d|--debug}`

Rédige le journal d'installation en mode détaillé.

`--options-file=<emplacement>`

Les paramètres d'installation seront lus depuis un texte source plutôt que depuis la ligne de commande.

`--language=<identifiant de la langue>`

La langue du produit. Les valeurs disponibles sont les suivantes : `en, bg, cs, da, de, es, fr, hu, id, it, ja, ko, ms, nb, nl, pl, pt, pt_BR, ru, fi, sr, sv, tr, zh, zh_TW`.
Si ce paramètre n'est pas précisé, la langue du produit sera définie par la langue de votre système, à condition qu'elle se trouve dans la liste ci-dessus. Sinon, la langue du produit sera définie sur Anglais (`en`).

Paramètres d'enregistrement

Spécifiez l'un des paramètres suivants :

- `{-g|--login=}<nom d'utilisateur>` et `{-w|--password=}<mot de passe>`

  Les identifiants du compte sous lequel l'agent sera enregistré dans le service Cyber Protection. Il ne peut pas s'agir d'un compte administrateur partenaire.

- `--token=<jeton>`

  Le jeton d'enregistrement est une série de 12 caractères, séparés par des traits d'union en trois segments. Vous pouvez en générer un dans la console Cyber Protect, comme décrit dans Déploiement des agents via la stratégie de groupe.

  Vous ne pouvez pas utiliser le paramètre `--token` en plus des paramètres `--login`,`--password` et `--register-with-credentials`.

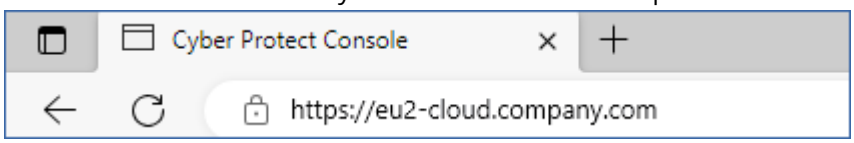
  - `{-C|--rain=}<adresse du service>`

    L'URL du service Cyber Protection.

    Vous n'avez pas à inclure ce paramètre de façon explicite lorsque vous utilisez les paramètres `--login` et `--password` pour l'enregistrement, car l'installateur utilise la bonne adresse par défaut, c'est-à-dire l'adresse que vous utilisez pour **vous connecter** au service Cyber Protection. Par exemple :

    Toutefois, lorsque vous utilisez `{-C|--rain=}` avec le paramètre `--token`, vous devez préciser l'adresse exacte du centre de données. Il s'agit de l'URL que vous voyez **une fois que vous êtes connecté** au service Cyber Protection. Par exemple :

- `--register-with-credentials`

  Si ce paramètre est indiqué, l'interface graphique de l'installateur démarrera. Pour terminer l'enregistrement, saisissez le nom d'utilisateur et le mot de passe du compte sous lequel l'agent sera

enregistré dans le service Cyber Protection. Il ne peut pas s'agir d'un compte administrateur partenaire.

- `--skip-registration`

  Utilisez ce paramètre si vous avez besoin d'installer l'agent, mais que vous avez l'intention de l'enregistrer dans le service Cyber Protection ultérieurement. Pour en savoir plus sur la façon de procéder, reportez-vous à « Enregistrement manuel de machines ».

Paramètres supplémentaires

`--http-proxy-host=<Adresse IP>` and `--http-proxy-port=<port>`

Le serveur proxy HTTP que l'agent utilisera pour la sauvegarde et la reprise depuis le Cloud, ainsi que pour la connexion au serveur de gestion. Sans ces paramètres, aucun serveur proxy ne sera utilisé.

`--http-proxy-login=<identifiant>` and `--http-proxy-password=<mot de passe>`

Les accréditations pour le serveur proxy HTTP. Utilisez ces paramètres si le serveur exige une authentification.

`--tmp-dir=<emplacement>`

Indique le dossier dans lequel les fichiers temporaires sont stockés lors de l'installation. Le dossier par défaut est **/var/tmp**.

`{-s|--disable-native-shared}`

Les bibliothèques redistribuables seront utilisées lors de l'installation, même s'il se peut qu'elles soient déjà présentes dans votre système.

`--skip-prereq-check`

Aucune vérification de l'installation des packages nécessaires à la compilation du module snapapi ne sera effectuée.

`--force-weak-snapapi`

L'installateur ne compilera pas de module snapapi. Il utilisera plutôt un module tout prêt qui peut ne pas correspondre exactement au noyau Linux. Nous ne recommandons pas d'utiliser cette option.

`--skip-svc-start`

Les services ne démarreront pas automatiquement après l'installation. La plupart du temps, ce paramètre est utilisé avec `--skip-registration`.

Paramètres d'information

`{-?|--help}`

Affiche la description des paramètres.

`--usage`

Affiche une brève description de la syntaxe de la commande.

`{-v|--version}`

Affiche la version du package d'installation.

`--product-info`

Affiche le nom du produit et la version du package d'installation.

`--snapapi-list`

Affiche les modules snapapi tout prêts disponibles.

`--components-list`

Affiche les composants de l'installateur.

Paramètres pour les fonctionnalités héritées

Ces paramètres se rapportent à un composant hérité, agent.exe.

`{-e|--ssl=}<chemin d'accès>`

Précise le chemin d'accès à un fichier de certificat personnalisé pour la communication SSL.

`{-p|--port=}<port>`

Précise le port qu'agent.exe utilise pour les connexions. Le port par défaut est 9876.

Paramètres de désinstallation

`{-u|--uninstall}`

Désinstalle le produit.

`--purge`

Désinstalle le produit et supprime ses journaux, ses tâches et ses paramètres de configuration. Il est inutile d'indiquer le paramètre `--uninstall` de façon explicite lorsque vous utilisez le paramètre `--purge`.

Exemples

- Installation de l'agent pour Linux sans l'enregistrer.

  ```
  ./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent -a --skip-registration
  ```

- Installation de l'agent pour Linux, de l'agent pour Virtuozzo et de l'agent pour Oracle, et enregistrement à l'aide des identifiants.

  ```
  ./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --login=johndoe --password=johnspassword
  ```

- Installation de l'agent pour Oracle et de l'agent pour Linux, et enregistrement à l'aide d'un jeton d'enregistrement.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i
BackupAndRecoveryAgent,OracleAgentFeature -a --rain=https://eu2-cloud.company.com --
token=34F6-8C39-4A5C
```

- Installation de l'agent pour Linux, de l'agent pour Virtuozzo et de l'agent pour Oracle, avec des paramètres de configuration dans un fichier texte séparé.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --options-
file=/home/mydirectory/configuration_file
```

- Désinstallation de l'agent pour Linux, de l'agent pour Virtuozzo et de l'agent pour Oracle, et suppression de tous leurs journaux, tâches et paramètres de configuration.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --purge
```

Installation et désinstallation sans assistance sous macOS

Cette section décrit l'installation, l'enregistrement et la désinstallation de l'agent de protection en mode sans assistance sur un ordinateur sous macOS via la ligne de commande.

Autorisations requises

Avant de lancer une installation sans assistance sur une ressource Mac, vous devez modifier le contrôle des préférences de la politique de confidentialité afin d'autoriser l'accès aux applications et les extensions du noyau et du système dans la ressource macOS pour permettre l'installation de l'agent Cyber Protection. Voir "Autorisations nécessaires à l'installation sans assistance sous macOS" (p. 117).

Après avoir déployé la charge active PPPC, vous pouvez passer aux procédures ci-dessous.

Pour télécharger le fichier d'installation (.dmg)

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur **Ajouter**, puis cliquez sur **Mac**.

Pour installer un agent

1. Ouvrir l'application Terminal.
2. Créez un répertoire temporaire dans lequel vous monterez le fichier d'installation (.dmg).

   ```
   mkdir <dmg_root>
   ```

   Remplacez `<dmg_root>` par le nom de répertoire de votre choix.
3. Montez le fichier .dmg.

   ```
   hdiutil attach <dmg_file> -mountpoint <dmg_root>
   ```

Remplacez `<dmg_file>` par le nom du fichier d'installation. Par exemple, **Cyber_Protection_Agent_for_MAC_x64.dmg**.

4. Exécutez le programme d'installation.
   - Si vous utilisez un programme d'installation complet pour Mac, comme `CyberProtect_AgentForMac_x64.dmg` ou `CyberProtect_AgentForMac_arm64.dmg`, exécutez la commande suivante.

     ```
     sudo installer -pkg <dmg_root>/Install.pkg -target LocalSystem
     ```

     Remarque
     Si vous devez activer l'intégration automatique pour File Sync & Share, exécutez plutôt la commande suivante. Cette option demande le mot de passe de l'administrateur.

     ```
     open <dmg_root>/Install.app --args --unattended --fss-onboarding-auto-start
     ```

   - Si vous utilisez un programme d'installation universel pour Mac, comme `CyberProtect_AgentForMac_web.dmg`, exécutez la commande suivante.

     ```
     sudo <dmg_root>/Install.app/Contents/MacOS/cyber_installer -a
     ```

5. Détachez le fichier d'installation (.dmg).

   ```
   hdiutil detach <dmg_root>
   ```

Exemple

```
mkdir mydirectory
```

```
hdiutil attach /Users/JohnDoe/Cyber_Protection_Agent_for_MAC_x64.dmg -mountpoint
mydirectory
```

```
sudo installer -pkg mydirectory/Install.pkg -target LocalSystem
```

```
hdiutil detach mydirectory
```

Pour désinstaller un agent

1. Ouvrir l'application Terminal.
2. Effectuez l'une des actions suivantes :
   - Pour désinstaller l'agent, exécutez la commande suivante :

     ```
     sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
     Uninstall.app/Contents/MacOS/AgentUninstall /confirm
     ```

- Pour désinstaller l'agent et supprimer tous les journaux, tâches et paramètres de configuration, exécutez la commande suivante :

```
sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
Uninstall.app/Contents/MacOS/AgentUninstall /confirm /purge
```

Autorisations nécessaires à l'installation sans assistance sous macOS

Avant de lancer une installation sans assistance sur une ressource Mac, vous devez modifier le contrôle des préférences de la politique de confidentialité afin d'autoriser l'accès aux applications et les extensions du noyau et du système dans la ressource macOS pour permettre l'installation de l'agent Cyber Protection. Vous pouvez effectuer cette opération en déployant une charge active PPPC personnalisée ou en configurant les préférences dans l'interface graphique de la ressource. Les autorisations suivantes sont nécessaires.

Configuration requise pour macOS 11 (Big Sur) ou versions ultérieures

Onglet	Section	Champs	Valeur

Contrôle de la stratégie concernant les préférences de confidentialité	Accès à l'application	Identifiant	com.acronis.backup

		Type d'identifiant	Identifiant du pack
		Exigence de code	identifier "com.acronis.backup" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APPLICATION OU SERVICE	SystemPolicyAllFiles
		ACCESS	Autoriser
	Accès à l'application	Identifiant	com.acronis.backup.aakore
		Type d'identifiant	Identifiant du pack
		Exigence de code	identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APPLICATION OU SERVICE	SystemPolicyAllFiles
		ACCESS	Autoriser
	Accès à l'application	Identifié	com.acronis.backup.activeprotection
		Type d'identifiant	Identifiant du pack
		Exigence de code	identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APPLICATION OU SERVICE	SystemPolicyAllFiles
		ACCESS	Autoriser

	Accès à l'application	Identifiant	cyber-protect-service
		Type d'identifiant	Identifiant du pack
		Exigence de code	`identifier "cyber-protect-service" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		APPLICATION OU SERVICE	SystemPolicyAllFiles
		ACCESS	Autoriser
Extensions système		Autoriser les utilisateurs à approuver des extensions système	Activé
	Identifiants d'équipe et extensions système autorisés	Nom affiché	Extensions système de l'agent Acronis Cyber Protect
		Types d'extensions système	Identifiants d'équipe autorisés
		Identifiant d'équipe	ZU2TV78AA6

Configuration requise pour les versions macOS antérieures à la version 11

Onglet	Section	Champs	Valeur

Contrôle de la stratégie concernant les préférences de confidentialité	Accès à l'application	Identifiant	com.acronis.backup

		Type d'identifiant	Identifiant du pack

		Exigence de code	identifier "com.acronis.backup" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APPLICATION OU SERVICE	SystemPolicyAllFiles
		ACCESS	Autoriser
	Accès à l'application	Identifiant	com.acronis.backup.aakore
		Type d'identifiant	Identifiant du pack
		Exigence de code	identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APPLICATION OU SERVICE	SystemPolicyAllFiles
		ACCESS	Autoriser
	Accès à l'application	Identifié	com.acronis.backup.activeprotection
		Type d'identifiant	Identifiant du pack
		Exigence de code	identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APPLICATION OU SERVICE	SystemPolicyAllFiles
		ACCESS	Autoriser

	Accès à l'application	Identifiant	cyber-protect-service
		Type d'identifiant	Identifiant du pack
		Exigence de code	identifier "cyber-protect-service" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APPLICATION OU SERVICE	SystemPolicyAllFiles
		ACCESS	Autoriser
Extensions du noyau approuvées		Autoriser les utilisateurs à approuver des extensions du noyau	Activé
		Autoriser les utilisateurs standard à approuver les extensions du noyau (macOS 11 ou versions ultérieures)	Activé
	Identifiants d'équipe et Extensions du noyau approuvés	Identifiant de l'équipe approuvé - Nom affiché	Extensions du noyau de l'agent Acronis Cyber Protect
		Identifiant de l'équipe	ZU2TV78AA6
		Identifiants de l'offre groupée des extensions du noyau	• com.acronis.systeminterceptors • com.acronis.ngscan • com.acronis.notifyframework
Extensions système		Autoriser les utilisateurs à approuver des extensions système	Activé
	Identifiants d'équipe et extensions	Nom affiché	Extensions système de l'agent Acronis Cyber Protect

	système autorisés		
		Types d'extensions système	Identifiants d'équipe autorisés
		Identifiant d'équipe	ZU2TV78AA6

Inscription et désinscription manuelles des ressources

Les ressources sont inscrites automatiquement dans le service Cyber Protection lorsque vous y installez l'agent de protection. Lorsque vous désinstallez l'agent de protection, les ressources sont désinscrites automatiquement et disparaissent de la console Cyber Protect.

Vous pouvez également inscrire une ressource manuellement à l'aide de l'interface de ligne de commande. Vous devrez peut-être utiliser l'inscription manuelle, par exemple en cas d'échec de l'inscription automatique ou si vous souhaitez déplacer une ressource vers un nouveau tenant ou sous un nouveau compte utilisateur.

Pour inscrire une ressource à l'aide d'un nom d'utilisateur et d'un mot de passe

Sous Windows

Dans la ligne de commande, exécutez la commande suivante :

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> -u <user name> -p <password>
```

Par exemple :

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -p johnspassword
```

Sous Linux

Dans la ligne de commande, exécutez la commande suivante :

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a <service
address> -u <user name> -p <password>
```

Par exemple :

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://cloud.company.com -u johndoe -p johnspassword
```

Sous macOS

Dans la ligne de commande, exécutez la commande suivante :

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a <service address> -u <user name> -p <password>
```

Par exemple :

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a https://cloud.company.com -u johndoe -p johnspassword
```

Remarque
Utilisez le nom d'utilisateur et le mot de passe du compte sous lequel vous souhaitez inscrire la ressource. Il ne peut pas s'agir d'un compte administrateur partenaire.

L'adresse du service est l'URL que vous utilisez **pour vous connecter** au service Cyber Protection. Par exemple, `https://cloud.company.com`.

Important
Si votre mot de passe contient des caractères spéciaux ou des espaces vides, reportez-vous à "Mots de passe contenant des caractères spéciaux ou des espaces vides" (p. 129).

Important
Si vous utilisez macOS 10.14 ou une version ultérieure, accordez un accès complet au disque à l'agent de protection. Pour ce faire, allez dans **Applications** >**Utilitaires**, puis exécutez **Assistant Cyber Protect Agent**. Suivez ensuite les instructions de la fenêtre de l'application.

Pour inscrire une ressource à l'aide d'un jeton d'enregistrement

Sous Windows

Dans la ligne de commande, exécutez la commande suivante :

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> --token <registration token>
```

Par exemple :

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://au1-cloud.company.com --token 3B4C-E967-4FBD
```

Sous Linux

Dans la ligne de commande, exécutez la commande suivante :

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a <service
address> --token <registration token>
```

Par exemple :

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://eu2-cloud.company.com --token 34F6-8C39-4A5C
```

Sous macOS

Dans la ligne de commande, exécutez la commande suivante :

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a <service address> --token <registration token>
```

Par exemple :

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a https://us5-cloud.company.com --token 9DBF-3DA9-4DAB
```

Important
Si vous utilisez macOS 10.14 ou une version ultérieure, accordez un accès complet au disque à l'agent de protection. Pour ce faire, allez dans **Applications** >**Utilitaires**, puis exécutez **Assistant Cyber Protect Agent**. Suivez ensuite les instructions de la fenêtre de l'application.

Appliance virtuelle

1. Dans la console de l'appliance virtuelle, appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.
2. À l'invite de commandes, exécutez la commande suivante :

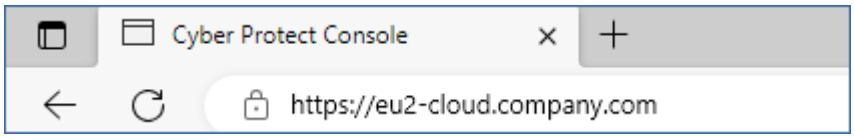
   ```
   register_agent -o register -t cloud -a <service address> --token <registration token>
   ```

   Par exemple :

   ```
   register_agent -o register -t cloud -a https://eu2-cloud.company.com --token 34F6-
   8C39-4A5C
   ```

3. Pour revenir à l'interface graphique de l'appliance, appuyez sur ALT+F1.

Remarque
Lorsque vous utilisez un jeton d'enregistrement, vous devez préciser l'adresse exacte du centre de données. Il s'agit de l'URL que vous voyez **une fois que vous êtes connecté** au service Cyber Protection. Par exemple, `https://eu2-cloud.company.com`.



Ne pas utiliser `https://cloud.company.com` ici.

Le jeton d'enregistrement est une série de 12 caractères, séparés par des traits d'union en trois segments. Pour plus d'informations sur sa génération, reportez-vous à "Génération d'un jeton d'enregistrement" (p. 175).

Pour désinscrire une ressource

Sous Windows

Dans la ligne de commande, exécutez la commande suivante :

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

Par exemple :

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

Sous Linux

Dans la ligne de commande, exécutez la commande suivante :

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

Sous macOS

Dans la ligne de commande, exécutez la commande suivante :

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o unregister
```

Appliance virtuelle

1. Dans la console de l'appliance virtuelle, appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.
2. À l'invite de commandes, exécutez la commande suivante :

   ```
   register_agent -o unregister
   ```

3. Pour revenir à l'interface graphique de l'appliance, appuyez sur ALT+F1.

Déplacement d'une ressource vers un autre tenant

Le déplacement d'une ressource vers un autre tenant n'est pas pris en charge de manière native. Vous pouvez dans ce cas annuler l'enregistrement de la ressource, puis l'enregistrer dans un autre tenant. Tous les plans de protection appliqués sont révoqués de cette ressource et perdent l'accès à ses sauvegardes enregistrées dans le stockage dans le cloud du tenant d'origine.

Pour plus d'informations sur l'enregistrement d'une ressource dans un nouveau tenant ou sous un nouveau compte utilisateur, voir "Modification de l'inscription d'une ressource" (p. 129).

Mots de passe contenant des caractères spéciaux ou des espaces vides

Si votre mot de passe contient des caractères spéciaux ou des espaces vides, entourez-le de guillemets lorsque vous le saisissez dans la ligne de commande.

Par exemple, sous Windows, exécutez cette commande :

Modèle de commande :

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> -u <user name> -p <"password">
```

Exemple de commande :

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -p "johns password"
```

En cas d'échec de la commande, chiffrez votre mot de passe au format base64 sur https://www.base64encode.org/. Indiquez ensuite, dans la ligne de commande, le mot de passe chiffré à l'aide du paramètre -b ou --base64.

Par exemple, sous Windows, exécutez cette commande :

Modèle de commande :

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> -u <user name> -b -p <encoded password>
```

Exemple de commande :

```
"C:\ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud -a https://cloud.company.com -u johndoe -b -p am9obnNwYXNzd29yZA==
```

Modification de l'inscription d'une ressource

Vous pouvez modifier l'inscription actuelle d'une ressource en l'inscrivant dans un nouveau tenant ou sous un nouveau compte utilisateur.

Important
Lorsque vous modifiez l'inscription d'une ressource, tous les plans de protection qui lui sont appliqués sont révoqués. Pour continuer à protéger la ressource, appliquez-lui un nouveau plan de protection.

Si vous inscrivez la ressource dans un nouveau tenant, cette ressource perd l'accès aux sauvegardes enregistrées dans le stockage dans le cloud du tenant d'origine. Les sauvegardes enregistrées ailleurs que dans des stockages dans le cloud restent accessibles.

Vous pouvez modifier l'inscription d'une ressource à l'aide de la ligne de commande ou du programme d'installation de l'interface utilisateur graphique. Lorsque vous utilisez la ligne de commande, vous n'avez pas besoin de désinstaller l'agent.

Pour modifier l'inscription d'une ressource

À l'aide de la ligne de commande

1. Désinscrivez l'agent de protection en suivant les indications figurant dans "Pour désinscrire une ressource" (p. 128).
2. Inscrivez l'agent de protection dans le nouveau tenant ou sous le nouveau compte utilisateur en suivant les indications de "Pour inscrire une ressource à l'aide d'un nom d'utilisateur et d'un mot de passe" (p. 125) ou de "Pour inscrire une ressource à l'aide d'un jeton d'enregistrement" (p. 126).

À l'aide du programme d'installation de l'interface utilisateur graphique

1. Désinstallez l'agent de protection.
2. Installez l'agent de protection, puis inscrivez-le dans le nouveau tenant ou sous le nouveau compte utilisateur.

Pour plus d'informations sur l'installation et l'inscription d'un agent, reportez-vous à "Installation des agents de protection" (p. 79).

Découverte automatique des machines

La découverte automatique vous permet d'effectuer les actions suivantes :

- Automatiser l'installation des agents de protection ainsi que l'inscription des ordinateurs en détectant les ordinateurs dans votre domaine Active Directory ou votre réseau local.
- Installer et mettre à jour des agents de protection sur plusieurs machines.
- Grâce à la synchronisation avec Active Directory, facilitez le provisionnement de ressources et la gestion des ordinateurs dans un domaine Active Directory important.

Prérequis

Pour exécuter la découverte automatique, vous avez besoin d'au moins un ordinateur sur lequel est installé un agent de protection dans votre réseau local ou votre domaine Active Directory. Cet agent

est utilisé comme agent de découverte.

Important
Seuls les agents installés sur des ordinateurs Windows peuvent être des agents de découverte. S'il n'existe aucun agent de découverte dans votre environnement, vous ne pourrez pas utiliser l'option **Terminaux multiples** du panneau **Ajouter des terminaux**.

L'installation à distance des agents est prise en charge uniquement pour les ordinateurs exécutant Windows (Windows XP n'est pas pris en charge). Pour l'installation à distance sur une machine exécutant Windows Server 2012 R2, vous devez avoir la mise à jour Windows KB2999226 installée sur cet ordinateur.

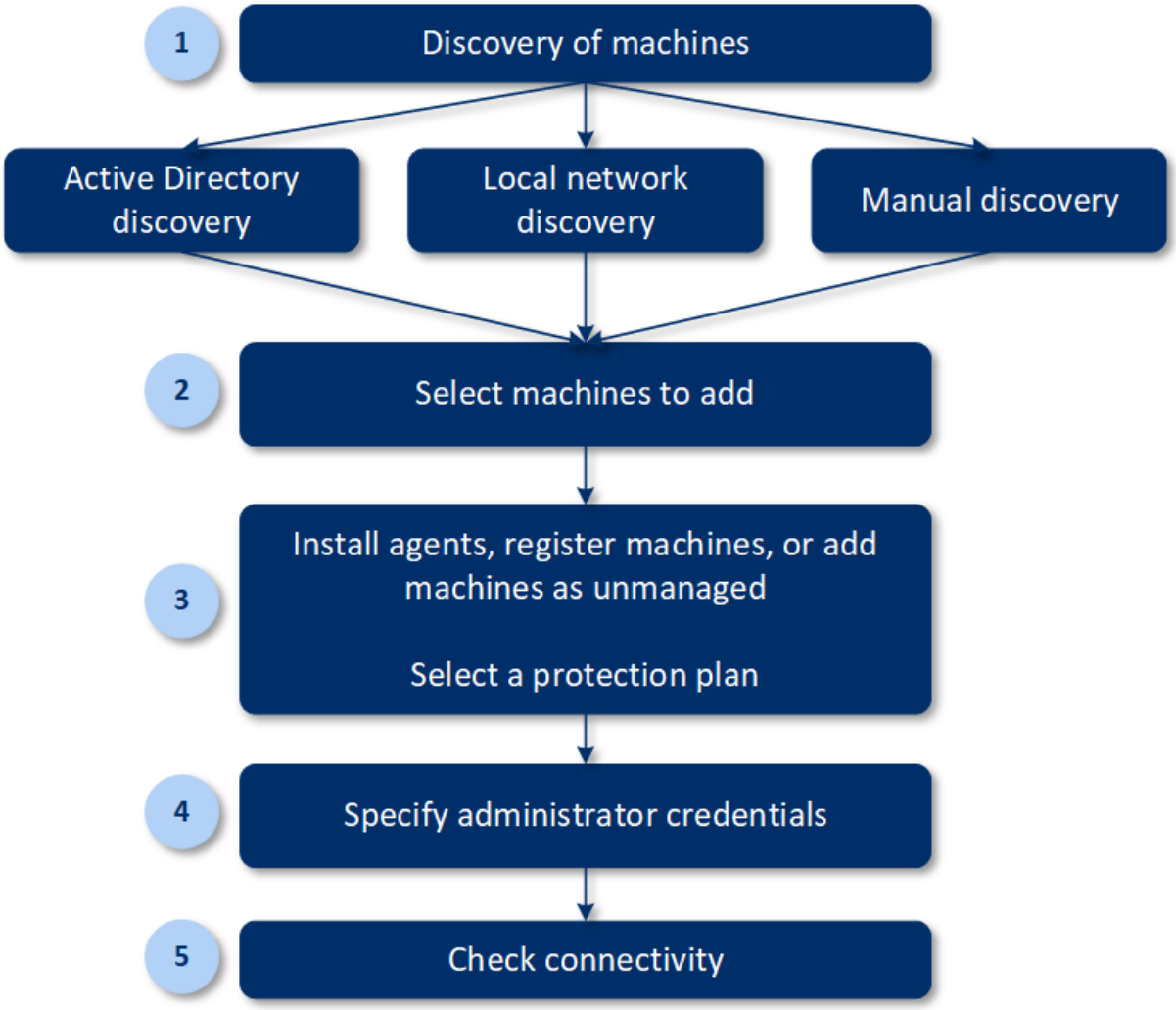
Fonctionnement de la découverte automatique

Lors d'une découverte sur le réseau local, l'agent de découverte collecte les informations suivantes pour chaque ordinateur du réseau à l'aide de la découverte NetBIOS, de Web Service Discovery (WSD) et du tableau ARP (Address Resolution Protocol) :

- Nom (nom d'hôte court/NetBIOS)
- Nom de domaine pleinement qualifié (FQDN)
- Domaine/Groupe de travail
- Adresses IPv4/IPv6
- Adresses MAC
- Système d'exploitation (nom/version/famille)
- Catégorie de machine (poste de travail, serveur, contrôleur de domaine)

Lors d'une découverte dans Active Directory, l'agent de découverte, en sus de la liste ci-dessus, collecte des informations concernant l'unité d'organisation (UO) des ordinateurs ainsi que des informations plus détaillées concernant leur nom et leur système d'exploitation. Toutefois, les adresses IP et MAC ne sont pas collectées.

Le diagramme suivant résume le processus de découverte automatique.



1. Sélectionnez la méthode de découverte :
   - Découverte dans Active Directory
   - Découverte sur le réseau local
   - Découverte manuelle : en utilisant l'adresse IP ou le nom d'hôte d'un ordinateur, ou en important une liste d'ordinateurs à partir d'un fichier

   Les résultats d'une découverte dans Active Directory ou d'une découverte sur le réseau local excluent les ordinateurs sur lesquels des agents de protection sont installés.

   Lors d'une découverte manuelle, les agents de protection existants sont mis à jour et réinscrits. Si vous exécutez la découverte automatique en utilisant le même compte que celui sur lequel un agent est inscrit, l'agent ne sera mis à jour que vers la version la plus récente. Si vous utilisez la découverte automatique à l'aide d'un autre compte, l'agent sera mis à jour vers la dernière version et réinscrit sous le tenant auquel le compte appartient.
2. Sélectionnez les ordinateurs que vous souhaitez ajouter à votre tenant.
3. Sélectionnez comment ajouter ces ordinateurs :
   - Installez un agent de protection et des composants supplémentaires sur les ordinateurs, et inscrivez-les dans la console Cyber Protect.

- Inscrivez les ordinateurs dans la console Cyber Protect (si un agent de protection était déjà installé).
- Ajoutez les ordinateurs à la console Cyber Protect en tant qu'**Machines non gérées**, sans installer d'agent de protection.

Vous pouvez également appliquer un plan de protection existant aux ordinateurs sur lesquels vous installez un agent de protection ou que vous inscrivez dans la console Cyber Protect.

4. Fournissez les identifiants administrateur pour les ordinateurs sélectionnés.
5. Vérifiez que vous pouvez vous connecter aux ordinateurs à l'aide des identifiants fournis.

Les ordinateurs qui s'affichent dans la console Cyber Protect entrent dans les catégories suivantes :

- **Découvert** : ordinateurs qui sont découverts, mais sur lesquels l'agent de protection n'est pas installé.
- **Géré** : ordinateurs sur lesquels l'agent de protection est installé.
- **Non protégé** : ordinateurs auxquels le plan de protection n'est pas appliqué. Les ordinateurs non protégés sont des ordinateurs découverts et des machines gérées auxquels aucun plan de protection n'est appliqué.
- **Protégé** : ordinateurs auxquels un plan de protection est appliqué.

Fonctionnement de l'installation à distance des agents

1. L'agent de découverte se connecte aux ordinateurs cibles à l'aide du nom d'hôte, de l'adresse IP et des identifiants administrateur indiqués dans l'assistant de découverte, puis transfère le fichier `web_installer.exe` vers ces ordinateurs.
2. Le fichier `web_installer.exe` s'exécute sur l'ordinateur cible en mode sans assistance.
3. Le programme d'installation Web récupère des packages d'installation supplémentaires depuis le cloud, puis les installe sur les machines cibles via la commande `msiexec`.
4. Une fois l'installation terminée, les composants sont inscrits dans le cloud.

Remarque
L'installation à distance des agents n'est pas prise en charge pour les contrôleurs de domaine en raison des autorisations supplémentaires requises pour l'exécution du service de l'agent.

Effectuer une découverte automatique et découverte manuelle

Avant de démarrer la découverte, assurez-vous de respecter les Prérequis.

Remarque
La découverte automatique n'est pas prise en charge pour l'ajout de contrôleurs de domaine en raison des autorisations supplémentaires requises pour l'exécution du service de l'agent.

Découvrir des machines

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur **Ajouter**.
3. Dans **Terminaux multiples**, cliquez sur **Windows uniquement**. L'assistant de découverte s'ouvre.
4. [Si votre organisation comporte des unités] Sélectionnez une unité. Ensuite, dans **Agent de découverte**, vous pourrez sélectionner les agents associés à l'unité sélectionnée et à ses unités enfant.
5. Sélectionnez l'agent de découverte qui exécutera l'analyse pour détecter les machines.
6. Sélectionnez la méthode de découverte :
   - **Rechercher dans Active Directory**. Assurez-vous que la machine sur laquelle l'agent de découverte est installé est membre du domaine Active Directory.
   - **Analyser le réseau local**. Si l'agent de découverte sélectionné ne trouve aucune machine, sélectionnez un autre agent de découverte.
   - **Spécifier manuellement ou importer à partir d'un fichier**. Définissez manuellement les machines à ajouter, ou importez-les à partir d'un fichier texte.
7. [Si la méthode de découverte sur Active Directory est sélectionnée] Sélectionnez comment rechercher des machines :
   - **Dans une liste d'unités organisationnelles**. Sélectionnez le groupe de machines à ajouter.
   - **Par demande de dialecte LDAP**. Servez-vous d'une demande de dialecte LDAP pour sélectionner les machines. **Base de recherche** définit où chercher, alors que **Filtre** vous permet de spécifier les critères pour la sélection de la machine.
8. En fonction de la méthode de découverte que vous avez sélectionnée, effectuez l'une des actions suivantes :

Méthode de découverte	Action
Recherche dans Active Directory	Dans la liste des ordinateurs découverts, sélectionnez les ordinateurs que vous souhaitez ajouter.
Analyse du réseau local	Dans la liste des ordinateurs découverts, sélectionnez les ordinateurs que vous souhaitez ajouter.

Spécifier manuellement ou importer à partir d'un fichier	Indiquez les adresses IP ou les noms d'hôte des ordinateurs, ou importez la liste des ordinateurs à partir d'un fichier texte. Le fichier doit contenir les adresses IP/noms d'hôtes, un élément par ligne. Voici un exemple de fichier :
	`156.85.34.10`
	`156.85.53.32`
	`156.85.53.12`
	`EN-L00000100`
	`EN-L00000101`
	Après l'ajout manuel ou l'importation de machines à partir d'un fichier, l'agent essaie d'effectuer un ping des machines ajoutées et de définir leur disponibilité.

9. Sélectionnez les actions à effectuer après la découverte :

Option	Description
Installer des agents et enregistrer des ordinateurs	Vous pouvez sélectionner les composants à installer sur les ordinateurs en cliquant sur **Sélectionner les composants**. Pour plus de détails, voir "Sélection des composants à installer" (p. 138).
Compte de connexion pour le service de l'agent	Ce paramètre est disponible dans l'écran **Sélectionner des composants**. Ce paramètre définit le compte sous lequel les services seront exécutés. Vous pouvez sélectionner l'une des options suivantes : • **Utiliser des comptes d'utilisateur du service** (par défaut pour l'agent de service) Les comptes d'utilisateur du service sont des comptes système Windows utilisés pour exécuter des services. Ce paramètre présente l'avantage suivant : les politiques de sécurité du domaine n'affectent pas les droits d'utilisateur de ces comptes. Par défaut, l'agent est exécuté sous le compte **Système Local**. • **Créer un nouveau compte** Le nom de compte pour l'agent sera Agent User. • **Utiliser le compte suivant** Si vous installez l'agent sur un contrôleur de domaine, le système vous invite à spécifier des comptes existants (ou le même compte) pour l'agent. Pour des raisons de sécurité, le système ne crée pas automatiquement de nouveaux comptes sur un contrôleur de domaine. Si vous avez choisi l'option **Créer un nouveau compte** ou **Utiliser le compte suivant**, assurez-vous que les politiques de sécurité du domaine n'affectent pas les droits des comptes associés. Si un compte est privé des droits d'utilisateur attribués lors de l'installation, le composant peut fonctionner de manière incorrecte ou ne pas fonctionner du tout.
Enregistrer les ordinateurs avec les agents installés	Utilisez cette option si l'agent est déjà installé sur les ordinateurs et qu'il vous suffit de les enregistrer sur Cyber Protection. Si aucun agent n'est trouvé sur les ordinateurs, ces derniers sont ajoutés en tant qu'ordinateurs **Non gérés**.
Ajouter en tant qu'ordinateurs non gérés	Si vous sélectionnez cette option, l'agent ne sera pas installé sur les ordinateurs. Vous pourrez les visualiser dans la console, et installer ou enregistrer l'agent ultérieurement.
Redémarrer l'ordinateur, si nécessaire	Cette option apparaît lorsque l'option **Installer les agents et enregistrer les ordinateurs** est sélectionnée. Si vous sélectionnez cette option, l'ordinateur est redémarré autant de fois que nécessaire pour terminer l'installation. Le redémarrage de la machine peut être nécessaire dans l'un des cas suivants : • L'installation des prérequis est terminée et un redémarrage est nécessaire pour que l'installation puisse se poursuivre.

Option	Description
	• L'installation est terminée, mais un redémarrage est nécessaire, car certains fichiers sont bloqués pendant l'installation. • L'installation est terminée, mais un redémarrage est nécessaire pour les autres logiciels précédemment installés.
Ne pas redémarrer si l'utilisateur s'est connecté	Cette option apparaît lorsque l'option **Redémarrer l'ordinateur si nécessaire** est sélectionné. Si vous sélectionnez cette option, l'ordinateur ne sera pas redémarré automatiquement si l'utilisateur est connecté au système. Par exemple, si un utilisateur travaille pendant que l'installation nécessite un redémarrage, le système n'est pas redémarré. Si les prérequis ont été installés, mais que l'ordinateur n'a pas été redémarré parce qu'un utilisateur était connecté, vous devez redémarrer l'ordinateur et recommencer l'installation pour la terminer. Si l'agent a été installé, mais que l'ordinateur n'a pas été redémarré, vous devez redémarrer l'ordinateur.
Utilisateur pour lequel enregistrer les ordinateurs	[Si votre organisation comporte des unités] Sélectionnez le compte utilisateur de l'unité ou des unités subordonnées sous lesquelles vous voulez enregistrer les ordinateurs. [Lors de la découverte automatique au niveau tenant partenaire] Dans la liste des tenants clients que vous gérez, développez l'arborescence, puis sélectionnez le compte utilisateur sous lequel vous souhaitez enregistrer les ordinateurs. [Lors de la découverte automatique en tant qu'administrateur du client] Si vous avez sélectionné **Installer les agents et enregistrer les ordinateurs** ou **Enregistrer les ordinateurs avec les agents installés**, vous avez également la possibilité d'appliquer le plan de protection aux ordinateurs. Si vous disposez de plusieurs plans de protection, vous pouvez sélectionner celui que vous souhaitez utiliser.

10. Fournissez les identifiants de l'utilisateur qui dispose de droits d'administrateur pour toutes les machines.

Important
Notez que l'installation à distance d'agents fonctionne sans aucune préparation uniquement si vous spécifiez les identifiants du compte d'administrateur intégré (le premier compte créé lors de l'installation du système d'exploitation). Si vous souhaitez définir des identifiants d'administrateur personnalisés, vous devrez effectuer des préparatifs manuels supplémentaires, décrits dans "Préparer un ordinateur pour l'installation à distance" (p. 137).

11. Le système vérifie la connectivité à toutes les machines. En cas d'échec de connexion à certaines des machines, vous pouvez modifier leurs identifiants.

Une fois la découverte des machines démarrée, vous trouverez la tâche correspondante dans l'activité **Surveillance** > **Activités** > **Découverte de machines**.

Préparer un ordinateur pour l'installation à distance

- Pour une installation réussie sur une machine distante exécutant Windows 7 ou version ultérieure, l'option **Panneau de configuration** > **Options des dossiers** > **Affichage** > **Utiliser l'assistant de partage** doit être *désactivée* sur cet ordinateur.
- Pour réussir l'installation sur une machine distante qui n'est *pas* membre d'un domaine Active Directory, le contrôle de compte utilisateur (CCU) doit être *désactivé* sur cette machine. Pour plus d'informations sur sa désactivation, consultez « Exigences pour le contrôle de compte utilisateur (CCU)" > Pour désactiver le CCU.
- Par défaut, les identifiants du compte administrateur intégré sont requis pour l'installation à distance sur toute machine Windows. Pour effectuer l'installation à distance en utilisant les identifiants d'un autre compte administrateur, les restrictions à distance de contrôle de compte utilisateur (CCU) doivent être *désactivées*. Pour plus d'informations sur la manière dont les désactiver, consultez « Exigences pour le contrôle de compte utilisateur (CCU)" > Pour désactiver les restrictions à distance de CCU.
- Le partage des fichiers et d'imprimantes doit être *activé* sur la machine distante. Pour accéder à cette option :
  - Sur un ordinateur exécutant Windows 2003 Server : accédez au **Panneau de configuration** > **Pare-feu Windows** > **Exceptions** > **Partage de fichiers et d'imprimantes**.
  - Sur un ordinateur exécutant Windows Server 2008, Windows 7 ou une version ultérieure : accédez au **Panneau de configuration** > **Pare-feu Windows** > **Centre de réseau et de partage** > **Modifier les paramètres de partage avancés**.
- Cyber Protection utilise les ports TCP 445, 25001 et 43234 pour l'installation à distance.

  Le port 445 s'ouvre automatiquement lorsque vous activez le partage de fichiers et d'imprimantes. Les ports 43234 et 25001 s'ouvrent automatiquement dans le pare-feu Windows. Si vous utilisez un autre pare-feu, assurez-vous que ces trois ports sont ouverts (ajoutés aux exceptions) pour les demandes entrantes et sortantes.

  Une fois l'installation à distance terminée, le port 25001 est fermé automatiquement par le pare-feu Windows. Les ports 445 et 43234 doivent rester ouverts si vous souhaitez mettre à jour l'agent à distance à l'avenir. Le port 25001 est ouvert et fermé automatiquement par le pare-feu Windows lors de chaque mise à jour. Si vous utilisez un pare-feu différent, laissez les trois ports ouverts.

Exigences pour le contrôle de compte d'utilisateur (UAC)

Sur un ordinateur qui exécute Windows 7 ou une version ultérieure et qui n'est pas membre d'un domaine Active Directory, les opérations de gestion centralisée (y compris l'installation à distance) nécessitent que le contrôle de compte utilisateur (UAC) et ses restrictions à distance soient désactivés.

Pour désactiver l'UAC

Effectuez l'une des opérations suivantes en fonction du système d'exploitation :

- **Pour un système d'exploitation Windows antérieur à Windows 8 :**
  Accédez à **Panneau de configuration > Afficher par : Petites icônes > Comptes d'utilisateur > Modifier les paramètres du Contrôle de compte d'utilisateur**, puis déplacez le curseur sur **Ne jamais m'avertir**. Ensuite, redémarrez la machine.
- **Pour tout système d'exploitation Windows** :
  1. Ouvrez l'Éditeur du Registre
  2. Localisez la clé de registre suivante : **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**
  3. Pour la valeur **EnableLUA**, modifiez la valeur du paramètre à **0**.
  4. Redémarrez la machine.

Pour désactiver les restrictions à distance UAC

1. Ouvrez l'Éditeur du Registre
2. Localisez la clé de registre suivante : **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
3. Pour la valeur **LocalAccountTokenFilterPolicy**, modifiez la valeur du paramètre sur **1**.
   Si la valeur **LocalAccountTokenFilterPolicy** n'existe pas, créez-en une en DWORD (32 bits). Pour plus d'informations sur cette valeur, reportez-vous à la documentation de Microsoft : https://support.microsoft.com/fr-fr/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.

Remarque
Pour des raisons de sécurité, nous vous recommandons de rétablir l'état d'origine des deux paramètres après la fin d'une opération de gestion (par exemple, une installation à distance) : **EnableLUA**=**1** et **LocalAccountTokenFilterPolicy** = **0**

Sélection des composants à installer

Vous trouverez la description des composants obligatoires et supplémentaires dans le tableau suivant :

Composant	Description
Composant obligatoire	
Agent pour Windows	Cet agent sauvegarde des disques, volumes et fichiers, et sera installé sur des machines Windows. Il sera toujours installé. Vous ne pouvez pas le sélectionner.
Composants supplémentaires	
Agent pour empêcher les pertes de données	Cet agent vous permet de limiter l'accès des utilisateurs à des périphériques, ports et presse-papiers locaux et redirigés sur des ordinateurs sur lesquels des plans de protection sont appliqués. Il sera installé s'il est sélectionné.

Protection contre les malwares et filtrage d'URL	Ce composant active le module de protection antivirus et antimalware et le module de filtrage d'URL dans les plans de protection. Même si vous choisissez de ne pas l'installer, il sera automatiquement installé ultérieurement si l'un de ces modules est activé dans un plan de protection pour l'ordinateur.
Agent pour Hyper-V	Cet agent sauvegarde des machines virtuelles Hyper-V et sera installé sur des hôtes Hyper-V. Il sera installé s'il est sélectionné et si un rôle Hyper-V est détecté sur une machine.
Agent pour SQL	Cet agent sauvegarde des bases de données SQL Server et sera installé sur des machines exécutant Microsoft SQL Server. Il sera installé s'il est sélectionné et si une application est détectée sur une machine.
Agent pour Exchange	Cet agent sauvegarde des bases de données et boîtes aux lettres Exchange, et sera installé sur des machines exécutant le rôle de boîte aux lettres de Microsoft SQL Server. Il sera installé s'il est sélectionné et si une application est détectée sur une machine.
Agent pour Active Directory	Cet agent sauvegarde les données des services de domaine Active Directory et sera installé sur des contrôleurs de domaine. Il sera installé s'il est sélectionné et si une application est détectée sur une machine.
Agent pour VMware (Windows)	Cet agent sauvegarde des machine virtuelles VMware et sera installé sur des machines Windows ayant un accès réseau à vCenter Server. Il sera installé s'il est sélectionné.
Agent pour Microsoft 365	Cet agent sauvegarde des boîtes aux lettres Microsoft 365 vers une destination locale, et sera installé sur des machines Windows. Il sera installé s'il est sélectionné.
Agent pour Oracle	Cet agent sauvegarde des bases de données Oracle et sera installé sur des machines exécutant Oracle Database. Il sera installé s'il est sélectionné.
Cyber Protection Moniteur	Ce composant permet à un utilisateur de contrôler l'exécution des tâches en cours dans la zone de notification, et sera installé sur des machines Windows. Il sera installé s'il est sélectionné. Pris en charge sur Windows 7 Service Pack 1 et versions ultérieures et Windows Server 2008 R2 Service Pack 1 et versions ultérieures.

Gestion des machines découvertes

Une fois le processus de découverte effectué, vous trouverez toutes les machines découvertes dans **Terminaux** > **Machines non gérées**.

Cette section est divisée en sous-sections en fonction de la méthode de découverte utilisée. La liste complète des paramètres de machine s'affiche ci-dessous (elle peut varier en fonction de la méthode de découverte) :

Nom	Description
Nom	Le nom de la machine. L'adresse IP s'affichera si le nom de la machine ne peut pas être découvert.

Adresse IP	L'adresse IP de la machine.
Type de découverte	La méthode de découverte utilisée pour détecter la machine.
Unité d'organisation	L'unité d'organisation à laquelle appartient la machine dans Active Directory. Cette colonne s'affiche si vous consultez la liste des machines dans **Machines non gérées** > **Active Directory**.
Système d'exploitation	Le système d'exploitation installé sur la machine.

Il existe une section **Exceptions**, où vous pouvez ajouter les machines à ignorer lors du processus de découverte. Par exemple, si vous ne souhaitez pas que des machines spécifiques soient découvertes, vous pouvez les ajouter à la liste.

Pour ajouter une machine à la section **Exceptions**, sélectionnez-la dans la liste, puis cliquez sur **Ajouter aux exceptions**. Pour retirer une machine de la section **Exceptions**, accédez à **Machines non gérées** > **Exceptions**, sélectionnez la machine, puis cliquez sur **Retirer des exceptions**.

Vous pouvez installer l'agent de protection et enregistrer un lot de machines découvertes dans Cyber Protection en les sélectionnant dans la liste et en cliquant sur **Installer et enregistrer**. L'assistant ouvert vous permet aussi d'assigner le plan de protection à un lot de machines.

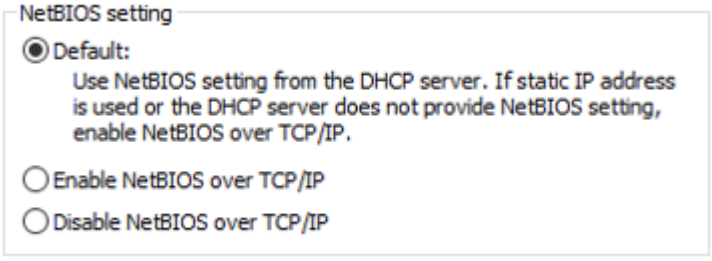
Une fois l'agent de protection installé sur des machines, ces machines s'affichent dans la section **Terminaux** > **Machines avec des agents**.

Pour vérifier l'état de la protection, accédez à **Surveillance** > **Vue d'ensemble** et ajoutez le widget **Statut de protection** ou **Machines découvertes**.

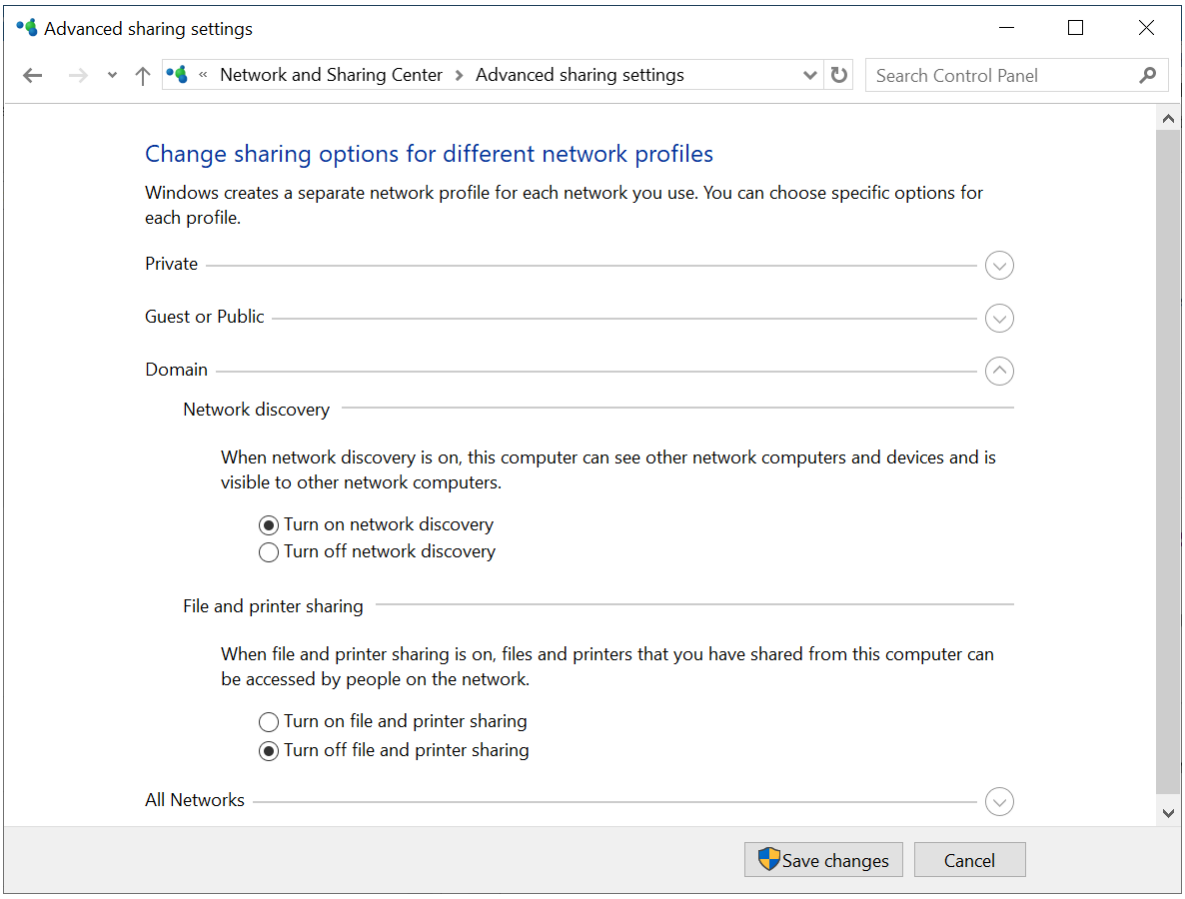
Dépannage

Si vous rencontrez le moindre problème avec la fonctionnalité de découverte automatique, essayez de procéder aux vérifications suivantes :

- Vérifiez que l'option NetBIOS par-dessus TCP/IP est activée ou configurée par défaut.



- Dans « Panneau de configuration\Centre Réseau et partage\Paramètres de partage avancés », activez la découverte du réseau.



- Vérifiez que le service Hôte du fournisseur de découverte de fonctions est en cours d'exécution sur la machine qui se charge de la découverte, ainsi que sur les machines à découvrir.
- Vérifiez que le service Publication des ressources de découverte de fonctions est en cours d'exécution sur les machines à découvrir.

Déploiement de l'agent pour VMware (appliance virtuelle)

Avant de commencer

Configuration système requise pour l'agent

Par défaut, 4 Go de RAM et 2 vCPU sont attribués à l'appliance virtuelle, ce qui est optimal et suffisant pour la plupart des opérations.

Pour améliorer les performances de sauvegarde et éviter les défaillances liées à une mémoire RAM insuffisante, nous vous recommandons d'augmenter ces ressources à 16 Go de RAM et 4 vCPU dans les situations les plus exigeantes. Par exemple, augmentez les ressources affectées lorsque vous vous attendez à un trafic de sauvegarde supérieur à 100 Mo par seconde (par exemple, sur les réseaux 10 Gigabits) ou si vous sauvegardez simultanément plusieurs machines virtuelles avec des disques durs de grande capacité (500 Go ou plus).

Les propres disques virtuels de l'appliance n'occupent pas plus de 6 Go de stockage. Le format du disque (dynamique ou statique) n'a pas d'importance et n'affecte pas les performances du matériel.

De combien d'agents ai-je besoin ?

Même si une appliance virtuelle est capable de protéger un environnement vSphere tout entier, une bonne pratique consiste à déployer une appliance virtuelle par cluster vSphere (ou par hôte s'il n'y a pas de clusters). Cela rend les sauvegardes plus rapides, car le matériel peut attacher les disques sauvegardés via le transport HotAdd. Par conséquent, le trafic de sauvegarde est dirigé d'un disque local à l'autre.

Il est normal d'utiliser simultanément l'appliance virtuelle et l'agent pour VMware (Windows), à condition qu'ils soient connectés au même vCenter Server *ou* qu'ils soient connectés à des hôtes ESXi différents. Évitez les situations pendant lesquelles un agent est connecté directement à un ESXi et un autre agent est connecté au vCenter Server qui gère ce même ESXi.

Si vous avez plusieurs agents, nous vous déconseillons d'utiliser un stockage attaché localement (c.-à-d. de stocker des sauvegardes sur des disques virtuels ajoutés à l'appliance virtuelle). Pour plus d'informations importantes à prendre en compte, voir "Utilisation d'un stockage attaché localement" (p. 729).

Désactiver le planificateur de ressources partagées (PRP) automatique pour l'agent

Si l'appliance virtuelle est déployée sur un cluster vSphere, veillez à désactiver le vMotion automatique pour celle-ci. Dans les paramètres RPR du cluster, activez des niveaux d'automatisation de machine virtuelle individuels, puis définissez **Niveau d'automatisation** de l'appliance virtuelle sur **Désactivé**.

Déploiement du modèle OVF

1. Cliquez sur **Tous les terminaux** > **Ajouter** > **VMware ESXi** > **Appliance virtuelle (OVF)**. L'archive ZIP est téléchargée sur votre machine.
2. Décompressez l'archive ZIP. Le dossier contient un fichier .ovf et deux fichiers .vmdk.
3. Assurez-vous que ces fichiers sont accessibles à partir de la machine exécutant vSphere Client.
4. Lancez vSphere Client et connectez-vous à vCenter Server.
5. Déployez le modèle OVF.
   - Lors de la configuration du stockage, sélectionnez le magasin de données partagé, s'il existe. Le format du disque (dynamique ou statique) n'a pas d'importance et n'affecte pas les performances du matériel.
   - Lors de la configuration de connexions réseau, assurez-vous de sélectionner un réseau qui autorise une connexion Internet, afin que l'agent puisse s'enregistrer correctement dans le Cloud.

Configuration de l'appliance virtuelle

Après avoir déployé l'appliance virtuelle, vous devez la configurer afin qu'elle puisse accéder à vCenter Server ou à l'hôte ESXi, ainsi qu'au service Cyber Protection.

Pour configurer l'appliance virtuelle

1. Dans vSphere Client, ouvrez la console de l'appliance virtuelle.
2. Vérifiez que la connexion réseau est configurée.

   La connexion est configurée automatiquement par l'intermédiaire du protocole DHCP (Dynamic Host Configuration Protocol).

   Pour modifier la configuration par défaut, sous **Options de l'agent**, dans le champ **eth0**, cliquez sur **Modifier** et spécifiez les paramètres réseau.
3. Connectez l'appliance virtuelle à vCenter Server ou à l'hôte ESXi.
   a. Sous **Options de l'agent**, dans le champ **vCenter/ESX(i)**, cliquez sur **Modifier** et spécifiez les informations suivantes.
      - [Si vous utilisez vCenter Server] Nom ou adresse IP de vCenter Server.
      - [Si vous n'utilisez pas vCenter Server] Nom ou adresse IP de l'hôte ESXi sur lequel vous souhaitez sauvegarder et restaurer les machines virtuelles. Pour accélérer les sauvegardes, déployez l'appliance virtuelle sur le même hôte.
      - Identifiants requis pour que l'appliance se connecte à vCenter Server ou à l'hôte ESXi.

        Au lieu d'utiliser un compte existant avec le rôle Administrateur, nous vous recommandons d'utiliser un compte dédié à l'accès à vCenter Server ou à l'hôte ESXi. Pour en savoir plus sur les privilèges nécessaires pour le compte dédié, voir "Agent pour VMware – privilèges nécessaires" (p. 736).

   b. Cliquez sur **Vérifier la connexion** pour vous assurer que les paramètres sont corrects.

   c. Cliquez sur **OK**.
4. Enregistrez l'appliance dans le service Cyber Protection à l'aide de l'une des méthodes suivantes.
   - [Uniquement pour les tenants sans authentification à deux facteurs] Enregistrez l'appliance dans son interface graphique.
     a. Sous **Options de l'agent**, dans le champ **Serveur de gestion**, cliquez sur **Modifier**.

     b. Dans le champ **Nom/IP du serveur**, sélectionnez **Cloud**.

        L'adresse du service Cyber Protection apparaît. Sauf indication contraire, ne modifiez pas cette adresse.

     c. Dans les champs **Nom d'utilisateur** et **Mot de passe**, spécifiez les identifiants du compte dans le service Cyber Protection. L'appliance virtuelle et les machines virtuelles gérées par cette appliance sont enregistrées dans ce compte.

     d. Cliquez sur **OK**.
   - Enregistrez l'appliance dans l'interface de ligne de commande.

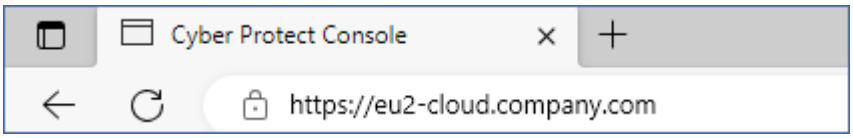
Remarque
Avec cette méthode, vous avez besoin d'un jeton d'enregistrement. Pour plus d'informations sur sa génération, reportez-vous à "Génération d'un jeton d'enregistrement" (p. 175).

a. Appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.

b. Exécuter la commande suivante :

```
register_agent -o register -t cloud -a <service address> --token <registration token>
```

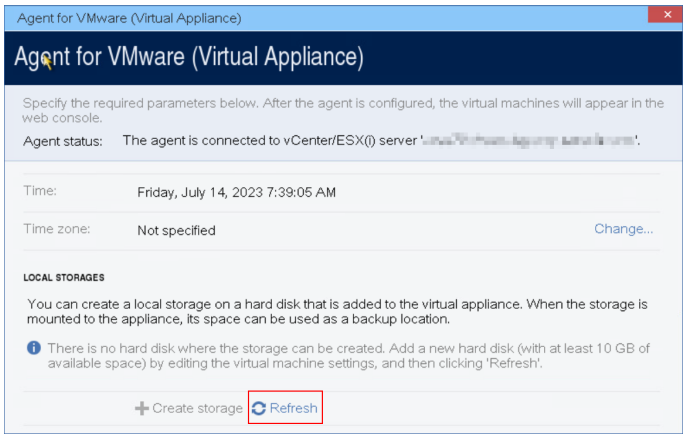
Remarque
Lorsque vous utilisez un jeton d'enregistrement, vous devez préciser l'adresse exacte du centre de données. Il s'agit de l'URL que vous voyez **une fois que vous êtes connecté** à la console Cyber Protect. Par exemple, `https://eu2-cloud.company.com`.



Ne pas utiliser `https://cloud.company.com` ici.

c. Pour revenir à l'interface graphique de l'appliance, appuyez sur ALT+F1.

5. [Facultatif] Ajoutez un stockage local.
   a. Dans vSphere Client, joignez un disque virtuel à l'appliance virtuelle. Le disque virtuel doit avoir au moins 10 Go d'espace libre.
   b. Dans l'interface graphique de l'appliance, cliquez sur **Actualiser**.



   Le bouton **Créer un stockage** devient actif.
   c. Cliquez sur **Créer un stockage**.
   d. Spécifiez un libellé pour le stockage, puis cliquez sur **OK**.
   e. Confirmez votre choix en cliquant sur **Oui**.
6. [Si un serveur proxy est activé sur votre réseau] Configurez le serveur proxy.

a. Appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.

b. Ouvrez le fichier **/etc/Acronis/Global.config** dans un éditeur de texte.

c. Effectuez l'une des actions suivantes :
   - Si les paramètres de proxy ont été précisés lors de l'installation de l'agent, recherchez la section suivante :

     ```
     <key name="HttpProxy">
         <value name="Enabled" type="Tdword">"1"</value>
         <value name="Host" type="TString">"ADDRESS"</value>
         <value name="Port" type="Tdword">"PORT"</value>
         <value name="Login" type="TString">"LOGIN"</value>
         <value name="Password" type="TString">"PASSWORD"</value>
     </key>
     ```

   - Autrement, copiez les lignes ci-dessus et collez-les dans le fichier entre les balises `<registry name="Global">...</registry>`.

d. Remplacez `ADDRESS` par la nouvelle adresse IP/nom d'hôte de serveur proxy et `PORT` par la valeur décimale du numéro de port.

e. Si votre serveur proxy nécessite une authentification, remplacez `LOGIN` et `PASSWORD` par les informations de connexion au serveur proxy. Dans le cas contraire, supprimez ces lignes du fichier.

f. Enregistrez le fichier.

g. Ouvrez le fichier **/opt/acronis/etc/aakore.yaml** dans un éditeur de texte.

h. Trouvez la section **env** ou créez-la, puis ajoutez-y les lignes suivantes :

   ```
   env:
       http-proxy: proxy_login:proxy_password@proxy_address:port
       https-proxy: proxy_login:proxy_password@proxy_address:port
   ```

i. Remplacez `proxy_login` et `proxy_password` par les identifiants de connexion au serveur proxy, et `proxy_address:port` par l'adresse et le numéro de port du serveur proxy.

j. Exécutez la commande `reboot`.

Remarque

Pour pouvoir mettre à jour une appliance virtuelle déployée derrière un proxy, modifiez le fichier `config.yaml` de l'appliance (`/opt/acronis/etc/va-updater/config.yaml`) en ajoutant la ligne suivante à la fin du fichier et en saisissant les valeurs propres à votre environnement :

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Par exemple :

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Déploiement de l'agent pour Scale Computing HC3 (appliance virtuelle)

Avant de commencer

Cette appliance est une machine virtuelle préconfigurée que vous déployez dans un cluster Scale Computing HC3. Elle contient un agent de protection qui vous permet d'administrer la cyberprotection pour toutes les machines virtuelles du cluster.

Configuration système requise pour l'agent

Par défaut, la machine virtuelle avec l'agent utilise 2 vCPU et 4 Gio de RAM. Ces paramètres sont suffisants pour la plupart des opérations, mais vous pouvez les modifier en éditant la machine virtuelle dans l'interface web Scale Computing HC3.

Pour améliorer les performances de sauvegarde et éviter les défaillances liées à une mémoire RAM insuffisante, nous vous recommandons d'augmenter ces ressources à 4 vCPU et 8 Gio de RAM dans les situations les plus exigeantes. Par exemple, augmentez les ressources affectées lorsque vous vous attendez à un trafic de sauvegarde supérieur à 100 Mo par seconde (par exemple, sur les réseaux 10 Gigabits) ou si vous sauvegardez simultanément plusieurs machines virtuelles avec des disques durs de grande capacité (500 Go ou plus).

La taille du disque virtuel de l'appliance est d'environ 9 Gio.

De combien d'agents ai-je besoin ?

Un seul agent peut protéger l'intégralité du cluster. Vous pouvez cependant avoir plus d'un agent dans le cluster si vous devez distribuer la bande passante du trafic de sauvegarde.

Si vous avez plus d'un agent dans un cluster, les machines virtuelles sont automatiquement distribuées de manière égale entre les agents, afin que chacun d'entre eux gère un nombre similaire de machines.

La redistribution automatique a lieu lorsque le déséquilibre de charge entre les agents atteint 20 %. Cela peut se produire, par exemple, lorsque vous ajoutez ou supprimez une machine ou un agent. Par exemple, vous réalisez que vous avez besoin de plus d'agents pour prendre en charge le débit et vous déployez une appliance virtuelle supplémentaire dans le cluster. Le serveur de gestion assignera les machines les plus appropriées au nouvel agent. La charge des anciens agents sera réduite. Lorsque vous supprimez un agent du serveur de gestion, les machines assignées à l'agent sont redistribuées parmi les agents restants. Cependant, cela ne se produira pas si un agent est endommagé ou est supprimé manuellement du cluster Scale Computing HC3. La redistribution démarrera seulement après que vous avez supprimé cet agent de la console Cyber Protect.

Pour vérifier quel agent gère une machine spécifique

1. Dans la console Cyber Protect, cliquez sur **Terminaux**, puis sélectionnez **Scale Computing**.
2. Cliquez sur l'icône en forme d'engrenage en haut à droite du tableau, puis, sous **Système** cochez la case **Agent**.
3. Cochez le nom de l'agent dans la colonne qui apparaît.

Déploiement du modèle QCOW2

1. Connectez-vous à votre compte Cyber Protection.
2. Cliquez sur **Terminaux** > **Tous les terminaux** > **Ajouter** > **Scale Computing HC3**.
   L'archive ZIP est téléchargée sur votre machine.
3. Décompressez l'archive ZIP, puis enregistrez le fichier .qcow2 et le fichier .xml dans un dossier appelé **ScaleAppliance**.
4. Transférez le dossier **ScaleAppliance** vers un partage réseau, puis assurez-vous que le cluster Scale Computing HC3 peut y accéder.
5. Connectez-vous au cluster Scale Computing HC3 en tant qu'administrateur disposant du rôle **Création/Modification de MV**. Pour plus d'informations sur les rôles requis pour les opérations avec les machines virtuelles Scale Computing HC3, reportez-vous à "Agent pour Scale Computing HC3 – Rôles requis" (p. 150).
6. Dans l'interface web de Scale Computing HC3, importez le modèle de machine virtuelle depuis le dossier **ScaleAppliance**.
   a. Cliquez sur l'icône **Importer MV HC3**.
   b. Dans la fenêtre **Importer MV HC3**, indiquez les informations suivantes :
      - Un nom pour la nouvelle machine virtuelle.
      - Le partage réseau sur lequel se trouve le dossier **ScaleAppliance**.
      - Le nom d'utilisateur et le mot de passe requis pour accéder à ce partage réseau.
      - [Facultatif] Un libellé de domaine pour la nouvelle machine virtuelle.
      - Le chemin d'accès au dossier **ScaleAppliance** sur le partage réseau.
   c. Cliquez sur **Importer**.

Une fois le déploiement terminé, vous devez configurer l'appliance virtuelle. Pour en savoir plus sur sa configuration, reportez-vous à "Configuration de l'appliance virtuelle" (p. 147).

Remarque
Si vous avez besoin de plus d'une appliance virtuelle dans votre cluster, répétez les étapes ci-dessus et déployez d'autres appliances virtuelles. Ne clonez pas une appliance virtuelle existante à l'aide de l'option **Cloner MV** dans l'interface web de Scale Computing HC3.

Configuration de l'appliance virtuelle

Après avoir déployé l'appliance virtuelle, vous devez la configurer afin qu'elle puisse atteindre aussi bien le cluster Scale Computing HC3 qu'elle protégera que le service Cyber Protection.

Pour configurer l'appliance virtuelle

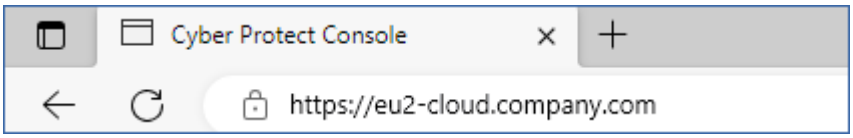
1. Connectez-vous à votre compte Scale Computing HC3.
2. Sélectionnez l'appliance virtuelle que vous souhaitez configurer, puis cliquez sur l'icône **Console**.
3. Dans le champ **eth0**, configurez les interfaces réseau de l'appliance.
   Assurez-vous que les adresses DHCP attribuées automatiquement (s'il y en a) sont valides au sein des réseaux que votre machine virtuelle utilise, ou attribuez-les manuellement. Selon le nombre de réseaux que l'appliance utilise, vous aurez peut-être une ou plusieurs interfaces à configurer.
4. Dans le champ **Scale Computing**, cliquez sur **Modifier** pour indiquer l'adresse et les identifiants du cluster Scale Computing HC3 afin d'y accéder.
   a. Dans le champ **Nom/IP du serveur**, entrez le nom DNS ou l'adresse IP du cluster.
   b. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les identifiants du compte administrateur Scale Computing HC3.
      Assurez-vous que ce compte administrateur dispose des rôles requis pour effectuer des opérations avec des machines virtuelles Scale Computing HC3. Pour plus d'informations sur ces rôles, reportez-vous à "Agent pour Scale Computing HC3 – Rôles requis" (p. 150).
   c. Cliquez sur **Vérifier la connexion** pour vous assurer que les paramètres sont corrects.
   d. Cliquez sur **OK**.
5. Enregistrez l'appliance dans le service Cyber Protection à l'aide de l'une des méthodes suivantes.
   - [Uniquement pour les tenants sans authentification à deux facteurs] Enregistrez l'appliance dans son interface graphique.
     a. Sous **Options de l'agent**, dans le champ **Serveur de gestion**, cliquez sur **Modifier**.
     b. Dans le champ **Nom/IP du serveur**, sélectionnez **Cloud**.
        L'adresse du service Cyber Protection apparaît. Sauf indication contraire, ne modifiez pas cette adresse.
     c. Dans les champs **Nom d'utilisateur** et **Mot de passe**, spécifiez les identifiants du compte dans le service Cyber Protection. L'appliance virtuelle et les machines virtuelles gérées par cette appliance sont enregistrées dans ce compte.
     d. Cliquez sur **OK**.
   - Enregistrez l'appliance dans l'interface de ligne de commande.

     Remarque
     Avec cette méthode, vous avez besoin d'un jeton d'enregistrement. Pour plus d'informations sur sa génération, reportez-vous à "Génération d'un jeton d'enregistrement" (p. 175).

     a. Appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.
     b. Exécuter la commande suivante :

     ```
     register_agent -o register -t cloud -a <service address> --token <registration
     token>
     ```


Remarque
Lorsque vous utilisez un jeton d'enregistrement, vous devez préciser l'adresse exacte du centre de données. Il s'agit de l'URL que vous voyez **une fois que vous êtes connecté** à la console Cyber Protect. Par exemple, `https://eu2-cloud.company.com`.



Ne pas utiliser `https://cloud.company.com` ici.

c. Pour revenir à l'interface graphique de l'appliance, appuyez sur ALT+F1.

6. [Facultatif] Dans le champ **Nom**, cliquez sur **Modifier** pour modifier le nom par défaut de l'appliance virtuelle, qui est **localhost**. Ce nom s'affiche dans la console Cyber Protect.
7. [Facultatif] Dans le champ **Heure**, cliquez sur **Modifier**, puis sélectionnez le fuseau horaire de votre emplacement afin de vous assurer que les opérations planifiées sont exécutées au bon moment.
8. [Si un serveur proxy est activé sur votre réseau] Configurez le serveur proxy.
   a. Appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.
   b. Ouvrez le fichier **/etc/Acronis/Global.config** dans un éditeur de texte.
   c. Effectuez l'une des actions suivantes :
      - Si les paramètres de proxy ont été précisés lors de l'installation de l'agent, recherchez la section suivante :

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

      - Autrement, copiez les lignes ci-dessus et collez-les dans le fichier entre les balises `<registry name="Global">...</registry>`.
   d. Remplacez `ADDRESS` par la nouvelle adresse IP/nom d'hôte de serveur proxy et `PORT` par la valeur décimale du numéro de port.
   e. Si votre serveur proxy nécessite une authentification, remplacez `LOGIN` et `PASSWORD` par les informations de connexion au serveur proxy. Dans le cas contraire, supprimez ces lignes du fichier.
   f. Enregistrez le fichier.
   g. Ouvrez le fichier **/opt/acronis/etc/aakore.yaml** dans un éditeur de texte.
   h. Trouvez la section **env** ou créez-la, puis ajoutez-y les lignes suivantes :

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

i. Remplacez `proxy_login` et `proxy_password` par les identifiants de connexion au serveur proxy, et `proxy_address:port` par l'adresse et le numéro de port du serveur proxy.

j. Exécutez la commande `reboot`.

Remarque

Pour pouvoir mettre à jour une appliance virtuelle déployée derrière un proxy, modifiez le fichier `config.yaml` de l'appliance (`/opt/acronis/etc/va-updater/config.yaml`) en ajoutant la ligne suivante à la fin du fichier et en saisissant les valeurs propres à votre environnement :

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Par exemple :

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Pour protéger des machines virtuelles dans le cluster Scale Computing HC3

1. Connectez-vous à votre compte Cyber Protection.
2. Accédez à **Terminaux** > **Scale Computing HC3**> <votre cluster>, ou recherchez vos ordinateurs dans **Terminaux** > **Tous les terminaux**.
3. Sélectionnez les ordinateurs et appliquez-leur un plan de protection.

Agent pour Scale Computing HC3 – Rôles requis

Cette section décrit les rôles nécessaires pour les opérations avec les machines virtuelles Scale Computing HC3.

Opération	Rôle
Sauvegarder une machine virtuelle	Sauvegarde Création/Modification de MV Suppression de MV
Restaurer sur une machine virtuelle existante	Sauvegarde Création/Modification de MV Contrôle de l'alimentation des MV Suppression de MV Paramètres de cluster
Récupérer sur une nouvelle machine virtuelle	Sauvegarde

	Création/Modification de MV Contrôle de l'alimentation des MV Suppression de MV Paramètres de cluster

Déploiement de l'agent pour Virtuozzo Hybrid Infrastructure (appliance virtuelle)

Avant de commencer

Cette appliance est une machine virtuelle préconfigurée que vous déployez dans Virtuozzo Hybrid Infrastructure. Elle contient un agent de protection qui vous permet d'administrer la cyber protection pour toutes les machines virtuelles d'un cluster Virtuozzo Hybrid Infrastructure.

Remarque
Pour vous assurer que les sauvegardes sur lesquelles l'option de sauvegarde **Service de cliché instantané des volumes (VSS) pour les machines virtuelles** est activée s'exécutent correctement et capturent les données dans un état cohérent avec les applications, vérifiez que les outils invités de Virtuozzo sont installés et à jour sur les machines virtuelles protégées.

Configuration système requise pour l'agent

Lorsque vous déployez l'appliance virtuelle, vous pouvez choisir parmi différentes combinaisons prédéfinies de vCPUs et RAM (variétés). Vous pouvez également créer vos propres variétés.

2 vCPU et 4 Go de RAM (variété moyenne) sont optimaux et suffisants pour la plupart des opérations. Pour améliorer les performances de sauvegarde et éviter les défaillances liées à une mémoire RAM insuffisante, nous vous recommandons d'augmenter ces ressources à 4 vCPU et 8 Go de RAM dans les situations les plus exigeantes. Par exemple, augmentez les ressources affectées lorsque vous vous attendez à un trafic de sauvegarde supérieur à 100 Mo par seconde (par exemple, sur les réseaux 10 Gigabits) ou si vous sauvegardez simultanément plusieurs machines virtuelles avec des disques durs de grande capacité (500 Go ou plus).

De combien d'agents ai-je besoin ?

Un seul agent peut protéger l'intégralité du cluster. Vous pouvez cependant avoir plus d'un agent dans le cluster si vous devez distribuer la bande passante du trafic de sauvegarde.

Si vous avez plus d'un agent dans un cluster, les machines virtuelles sont automatiquement distribuées de manière égale entre les agents, afin que chacun d'entre eux gère un nombre similaire de machines.

La redistribution automatique a lieu lorsque le déséquilibre de charge entre les agents atteint 20 %. Cela peut se produire, par exemple, lorsque vous ajoutez ou supprimez une machine ou un agent. Par exemple, vous réalisez que vous avez besoin de plus d'agents pour prendre en charge le débit et vous déployez une appliance virtuelle supplémentaire dans le cluster. Le serveur de gestion assignera les machines les plus appropriées au nouvel agent. La charge des anciens agents sera réduite. Lorsque vous supprimez un agent du serveur de gestion, les machines assignées à l'agent sont redistribuées parmi les agents restants. Cependant, cela ne se produira pas si un agent est endommagé ou est supprimé manuellement du nœud de Virtuozzo Hybrid Infrastructure. La redistribution démarrera seulement après que vous avez supprimé cet agent de l'interface Web Cyber Protection.

Pour vérifier quel agent gère une machine spécifique

1. Dans la console Cyber Protect, cliquez sur **Terminaux**, puis sélectionnez **Virtuozzo Hybrid Infrastructure**.
2. Cliquez sur l'icône en forme d'engrenage en haut à droite du tableau, puis, sous **Système** cochez la case **Agent**.
3. Cochez le nom de l'agent dans la colonne qui apparaît.

Limites

- L'appliance de Virtuozzo Hybrid Infrastructure ne peut pas être déployée à distance.
- La sauvegarde reconnaissant les applications des machines virtuelles n'est pas prise en charge.

Configurations de réseaux dans Virtuozzo Hybrid Infrastructure

Avant de déployer et de configurer l'appliance virtuelle, vous devez avoir configuré vos réseaux dans Virtuozzo Hybrid Infrastructure.

Configuration réseau requise pour Agent pour Virtuozzo Hybrid Infrastructure (appliance virtuelle)

- L'appliance virtuelle nécessite deux adaptateurs réseau.
- L'appliance virtuelle doit être connecté aux réseaux Virtuozzo avec les types de trafic réseau suivants :
  - API de calcul
  - Sauvegarde de MV
  - ABGW Public
  - MV publique

Pour plus d'informations sur la configuration des réseaux, voir Exigences relatives au cluster de calcul dans la documentation Virtuozzo.

Configurations de comptes utilisateur dans Virtuozzo Hybrid Infrastructure

Pour configurer l'appliance virtuelle, vous avez besoin d'un compte utilisateur Virtuozzo Hybrid Infrastructure. Ce compte doit disposer du rôle **Administrateur** dans le domaine **Défaut**. Pour en savoir plus sur les utilisateurs, veuillez consulter la section Gestion de vos utilisateurs du panneau d'administration dans la documentation de Virtuozzo Hybrid Infrastructure. Assurez-vous d'avoir accordé à ce compte l'accès à tous les projets du domaine **Défaut**.

Pour accorder l'accès à tous les projets du domaine Défaut

1. Créez un fichier d'environnement pour l'administrateur système. Pour cela, exécutez le script suivant dans le cluster Virtuozzo Hybrid Infrastructure via l'interface de ligne de commande OpenStack. Pour en savoir plus sur la connexion à cette interface, reportez-vous à Connexion à l'interface de ligne de commande OpenStack dans la documentation de Virtuozzo Hybrid Infrastructure.

   ```
   su - vstoradmin
   kolla-ansible post-deploy
   exit
   ```

2. Utilisez le fichier d'environnement pour autoriser davantage de commandes OpenStack :

   ```
   . /etc/kolla/admin-openrc.sh
   ```

3. Exécutez les commandes suivantes :

   ```
   openstack --insecure user set --project admin --project-domain Default --domain
   Default <username>
   openstack --insecure role add --domain Default --user <username> --user-domain
   Default compute --inherited
   ```

   Remplacez <username> par le compte Virtuozzo Hybrid Infrastructure disposant du rôle **Administrateur** dans le domaine **Défaut**. L'appliance virtuelle se servira de ce compte pour sauvegarder et restaurer les machines virtuelles dans tout projet enfant dans le domaine **Défaut**.

Exemple

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.sh
openstack --insecure user set --project admin --project-domain Default --domain Default
johndoe
openstack --insecure role add --domain Default --user johndoe --user-domain Default
compute --inherited
```

Pour gérer les sauvegardes pour les machines virtuelles dans un domaine autre que le domaine **Défaut**, exécutez également la commande suivante.

Pour accorder l'accès à tous les projets dans un domaine différent

```
openstack --insecure role add --domain <domain name> --inherited --user <username> --
user-domain Default admin
```

Remplacez <domain name> par le nom du domaine des projets dans lesquels le compte <username> aura accès.

Exemple

```
openstack --insecure role add --domain MyNewDomain --inherited --user johndoe --user-
domain Default admin
```

Après avoir accordé l'accès aux projets, vérifiez les rôles attribués au compte.

Pour vérifier les rôles attribués

```
openstack --insecure role assignment list --user <username> --names
```

Ici, <nomd'utilisateur> est le compte Virtuozzo Hybrid Infrastructure.

Exemple

```
openstack --insecure role assignment list --user johndoe --names -c Role -c User -c
Project -c Domain
+--------------+-----------------+---------+-------------+
| Role         | User            | Project | Domain      |
+--------------+-----------------+---------+-------------+
| admin        | johndoe@Default |         | MyNewDomain |
| compute      | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
+--------------+-----------------+---------+-------------+
```

Dans cet exemple, les options `Rôle -c`, `Utilisateur -c`, `Projet -c` et `Domaine -c` servent à abréger la sortie de commande pour s'adapter à la page.

Pour vérifier les véritables rôles attribués au compte dans tous les projets, exécutez également la commande suivante.

Pour vérifier les véritables rôles dans tous les projets

```
openstack --insecure role assignment list --user <username> --names --effective
```

Ici, <nomd'utilisateur> est le compte Virtuozzo Hybrid Infrastructure.

Exemple

```
openstack --insecure role assignment list --user johndoe --names --effective  -c Role -c
User -c Project -c Domain
+--------------+-----------------+-----------------+---------+
| Role         | User            | Project         | Domain  |
+--------------+-----------------+-----------------+---------+
| domain_admin | johndoe@Default |                 | Default |
| compute      | johndoe@Default | admin@Default   |         |
| compute      | johndoe@Default | service@Default |         |
| domain_admin | johndoe@Default | admin@Default   |         |
| domain_admin | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | service@Default |         |
| member       | johndoe@Default | service@Default |         |
| reader       | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | admin@Default   |         |
| member       | johndoe@Default | admin@Default   |         |
| reader       | johndoe@Default | admin@Default   |         |
| project_user | johndoe@Default |                 | Default |
| member       | johndoe@Default |                 | Default |
| reader       | johndoe@Default |                 | Default |
+--------------+-----------------+-----------------+---------+
```

Dans cet exemple, les options `Rôle -c`, `Utilisateur -c`, `Projet -c` et `Domaine -c` servent à abréger la sortie de commande pour s'adapter à la page.

Déploiement du modèle QCOW2

1. Connectez-vous à votre compte Cyber Protection.
2. Cliquez sur **Terminaux** > **Tous les terminaux** > **Ajouter** > **Virtuozzo Hybrid Infrastructure**. L'archive ZIP est téléchargée sur votre machine.
3. Décompressez l'archive ZIP. Elle contient un fichier image .qcow2.
4. Connectez-vous à votre compte sur Virtuozzo Hybrid Infrastructure.
5. Ajoutez le fichier image .qcow2 au cluster de calcul de Virtuozzo Hybrid Infrastructure, comme suit :
   - Dans l'onglet **Calcul** > **Machines virtuelles** > **Images**, cliquez sur **Ajouter une image**.
   - Dans la fenêtre **Ajouter une image**, cliquez sur **Parcourir**, puis sélectionnez le fichier .qcow2.
   - Indiquez le nom de l'image, sélectionnez le type **OS Linux générique**, puis cliquez sur **Ajouter**.
6. Dans l'onglet **Calcul** > **Machines virtuelles** > **Machines virtuelles**, cliquez sur **Créer une machine virtuelle**. Une fenêtre s'ouvrira, dans laquelle vous devez indiquer les paramètres suivants :
   - Un nom pour la nouvelle machine virtuelle.
   - Dans **Déployer à partir de**, choisissez **Image**.

- Dans la fenêtre **Images**, sélectionnez le fichier image .qcow2 de l'appliance, puis cliquez sur **Terminé**.
- Dans la fenêtre **Volumes**, vous n'avez pas besoin d'ajouter de volumes. Le volume ajouté automatiquement pour le disque système est suffisant.
- Dans la fenêtre **Variété**, choisissez votre combinaison souhaitée de vCPU et RAM, puis cliquez sur **Terminé**. 2 vCPU et 4 Go de RAM sont généralement suffisants.
- Dans la fenêtre **Interfaces réseau**, cliquez sur **Ajouter**, sélectionnez le réseau virtuel de type *public*, puis cliquez sur **Ajouter**. Il apparaîtra dans la liste **Interfaces réseau**.
  Si vous utilisez une configuration possédant plus d'un réseau physique (et donc avec plus d'un réseau virtuel de type public), répétez cette étape et sélectionnez les réseaux virtuels dont vous avez besoin.

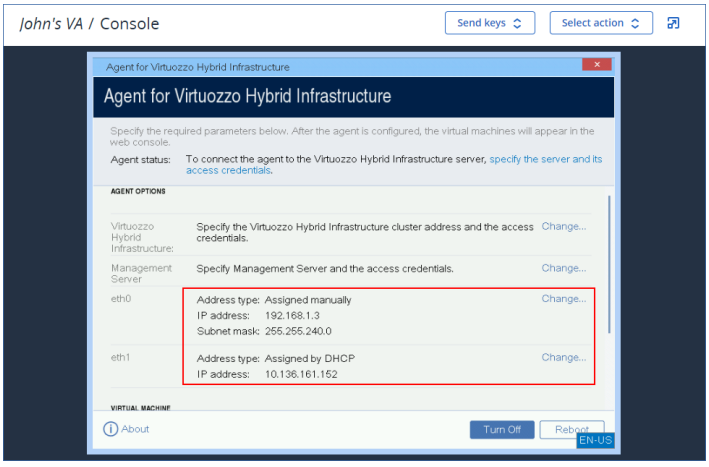
7. Cliquez sur **Valider**.
8. De nouveau, dans la fenêtre **Créer une machine virtuelle**, cliquez sur **Déployer** pour créer et démarrer la machine virtuelle.

Configuration de l'appliance virtuelle

Après avoir déployé l'agent pour Virtuozzo Hybrid Infrastructure (appliance virtuelle), vous devez configurer l'appliance virtuelle afin qu'elle puisse atteindre le cluster Virtuozzo Hybrid Infrastructure qu'elle protègera, mais aussi le service cloud Cyber Protection.

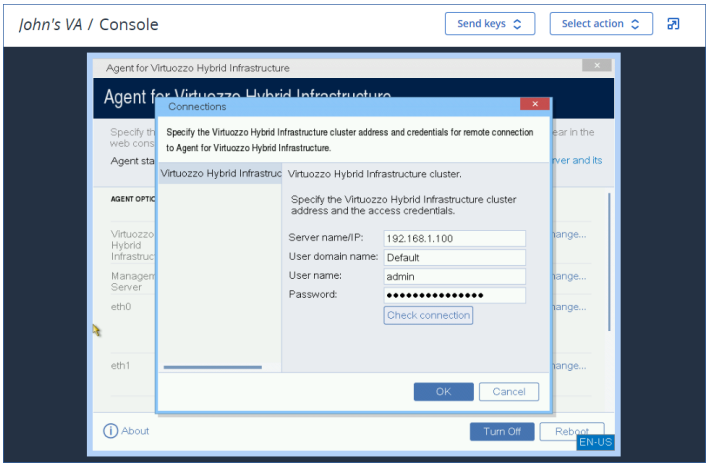
Pour configurer l'appliance virtuelle

1. Connectez-vous à votre compte sur Virtuozzo Hybrid Infrastructure.
2. Dans l'onglet **Calcul** > **Machines virtuelles** > **Machines virtuelles**, sélectionnez la machine virtuelle que vous avez créée. Cliquez ensuite sur **Console**.
3. Configurez les interfaces réseau de l'appliance. Il se peut qu'il y ait une interface ou plus à configurer ; cela dépend du nombre de réseaux virtuels que l'appliance utilise. Assurez-vous que les adresses DHCP attribuées automatiquement (s'il y en a) sont valides au sein des réseaux que votre machine virtuelle utilise, ou attribuez-les manuellement.



4. Indiquez l'adresse et les identifiants du cluster Virtuozzo :

- Nom de DNS ou adresse IP du cluster de Virtuozzo Hybrid Infrastructure – il s'agit de l'adresse du nœud de gestion du cluster. Le port par défaut 5000 sera automatiquement configuré. Si vous utilisez un port différent, vous devez l'indiquer manuellement.
- Dans le champ **Nom de domaine de l'utilisateur**, indiquez votre domaine dans Virtuozzo Hybrid Infrastructure. Par exemple, **Défaut**.
  Le nom de domaine est sensible à la casse.
- Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les identifiants du compte Virtuozzo Hybrid Infrastructure qui possède le rôle **Administrateur** du domaine indiqué.
  Pour en savoir plus sur les utilisateurs, les rôles et les domaines, reportez-vous à Configurations de comptes utilisateur dans Virtuozzo Hybrid Infrastructure.



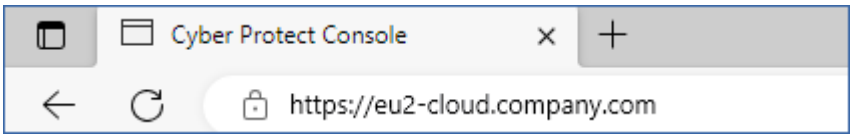
5. Enregistrez l'appliance dans le service Cyber Protection à l'aide de l'une des méthodes suivantes.
   - [Uniquement pour les tenants sans authentification à deux facteurs] Enregistrez l'appliance dans son interface graphique.
     a. Sous **Options de l'agent**, dans le champ **Serveur de gestion**, cliquez sur **Modifier**.
     b. Dans le champ **Nom/IP du serveur**, sélectionnez **Cloud**.
        L'adresse du service Cyber Protection apparaît. Sauf indication contraire, ne modifiez pas cette adresse.
     c. Dans les champs **Nom d'utilisateur** et **Mot de passe**, spécifiez les identifiants du compte dans le service Cyber Protection. L'appliance virtuelle et les machines virtuelles gérées par cette appliance sont enregistrées dans ce compte.
     d. Cliquez sur **OK**.
   - Enregistrez l'appliance dans l'interface de ligne de commande.

     Remarque
     Avec cette méthode, vous avez besoin d'un jeton d'enregistrement. Pour plus d'informations sur sa génération, reportez-vous à "Génération d'un jeton d'enregistrement" (p. 175).

     a. Appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.
     b. Exécuter la commande suivante :

```
register_agent -o register -t cloud -a <service address> --token <registration
token>
```

Remarque
Lorsque vous utilisez un jeton d'enregistrement, vous devez préciser l'adresse exacte du centre de données. Il s'agit de l'URL que vous voyez **une fois que vous êtes connecté** à la console Cyber Protect. Par exemple, `https://eu2-cloud.company.com`.



Ne pas utiliser `https://cloud.company.com` ici.

c. Pour revenir à l'interface graphique de l'appliance, appuyez sur ALT+F1.

6. [Si un serveur proxy est activé sur votre réseau] Configurez le serveur proxy.
   a. Appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.
   b. Ouvrez le fichier **/etc/Acronis/Global.config** dans un éditeur de texte.
   c. Effectuez l'une des actions suivantes :
      - Si les paramètres de proxy ont été précisés lors de l'installation de l'agent, recherchez la section suivante :

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

      - Autrement, copiez les lignes ci-dessus et collez-les dans le fichier entre les balises `<registry name="Global">...</registry>`.
   d. Remplacez `ADDRESS` par la nouvelle adresse IP/nom d'hôte de serveur proxy et `PORT` par la valeur décimale du numéro de port.
   e. Si votre serveur proxy nécessite une authentification, remplacez `LOGIN` et `PASSWORD` par les informations de connexion au serveur proxy. Dans le cas contraire, supprimez ces lignes du fichier.
   f. Enregistrez le fichier.
   g. Ouvrez le fichier **/opt/acronis/etc/aakore.yaml** dans un éditeur de texte.
   h. Trouvez la section **env** ou créez-la, puis ajoutez-y les lignes suivantes :

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

i. Remplacez `proxy_login` et `proxy_password` par les identifiants de connexion au serveur proxy, et `proxy_address:port` par l'adresse et le numéro de port du serveur proxy.

j. Exécutez la commande `reboot`.

Remarque

Pour pouvoir mettre à jour une appliance virtuelle déployée derrière un proxy, modifiez le fichier `config.yaml` de l'appliance (`/opt/acronis/etc/va-updater/config.yaml`) en ajoutant la ligne suivante à la fin du fichier et en saisissant les valeurs propres à votre environnement :

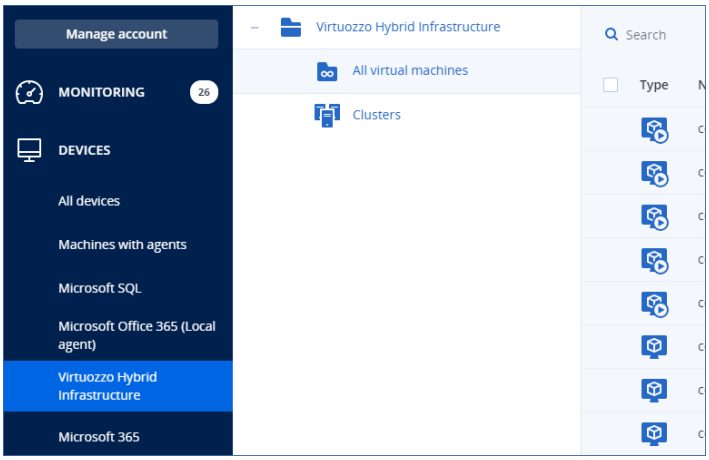
```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Par exemple :

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Pour protéger les machines virtuelles du cluster de Virtuozzo Hybrid Infrastructure

1. Connectez-vous à votre compte Cyber Protection.
2. Accédez à **Terminaux** > **Virtuozzo Hybrid Infrastructure**> <votre cluster> > **Projet par défaut** > **admin**, ou cherchez vos machines dans **Terminaux** > **Tous les terminaux**.
3. Sélectionnez les ordinateurs et appliquez-leur un plan de protection.



Déploiement de l'agent pour oVirt (appliance virtuelle)

Avant de commencer

Cette appliance est une machine virtuelle préconfigurée que vous déployez dans un centre de données Red Hat Virtualization/oVirt. Elle contient un agent de protection qui vous permet d'administrer la cyberprotection pour toutes les machines virtuelles du centre de données.

Configuration système requise pour l'agent

Par défaut, la machine virtuelle avec l'agent utilise 2 vCPU et 4 Gio de RAM. Ces paramètres sont suffisants pour la plupart des opérations, mais vous pouvez les modifier dans le portail d'administration Red Hat Virtualization/oVirt.

Pour améliorer les performances de sauvegarde et éviter les défaillances liées à une mémoire RAM insuffisante, nous vous recommandons d'augmenter ces ressources à 4 vCPU et 8 Gio de RAM dans les situations les plus exigeantes. Par exemple, augmentez les ressources affectées lorsque vous vous attendez à un trafic de sauvegarde supérieur à 100 Mo par seconde (par exemple, sur les réseaux 10 Gigabits) ou si vous sauvegardez simultanément plusieurs machines virtuelles avec des disques durs de grande capacité (500 Go ou plus).

La taille du disque virtuel de l'appliance est de 8 Gio.

De combien d'agents ai-je besoin ?

Un seul agent peut protéger l'intégralité du centre de données. Vous pouvez cependant avoir plus d'un agent dans le centre de données si vous devez distribuer la bande passante du trafic de sauvegarde.

Si vous avez plus d'un agent dans le centre de données, les machines virtuelles sont automatiquement distribuées entre les agents, afin que chacun d'entre eux gère un nombre similaire de machines.

La redistribution automatique a lieu lorsque le déséquilibre de charge entre les agents atteint 20 %. Cela peut se produire, par exemple, lorsque vous ajoutez ou supprimez une machine ou un agent. Par exemple, vous réalisez que vous avez besoin de plus d'agents pour prendre en charge le débit et vous déployez une appliance virtuelle supplémentaire dans le centre de données. Le serveur de gestion assignera les machines les plus appropriées au nouvel agent. La charge des anciens agents sera réduite. Lorsque vous supprimez un agent, les machines assignées à l'agent sont redistribuées parmi les agents restants. Cependant, cela ne se produira pas si un agent est endommagé ou est supprimé manuellement à partir du portail d'administration Red Hat Virtualization/oVirt. La redistribution démarrera seulement après que vous avez supprimé cet agent de la console Cyber Protect.

Pour vérifier quel agent gère une machine spécifique

1. Dans la console Cyber Protect, cliquez sur **Terminaux**, puis sélectionnez **oVirt**.
2. Cliquez sur l'icône en forme d'engrenage en haut à droite du tableau, puis, sous **Système** cochez la case **Agent**.
3. Cochez le nom de l'agent dans la colonne qui apparaît.

Limites

Les opérations suivantes ne sont pas prises en charge pour les machines virtuelles Red Hat Virtualization/oVirt.

- Sauvegarde reconnaissant les applications
- Exécution d'une machine virtuelle à partir d'une sauvegarde
- Réplication de machines virtuelles
- Suivi des blocs modifiés

Déploiement du modèle OVA

1. Connectez-vous à votre compte Cyber Protection.
2. Cliquez sur **Terminaux** > **Tous les terminaux** > **Ajouter** > **Red Hat Virtualization (oVirt)**.
   L'archive ZIP est téléchargée sur votre machine.
3. Décompressez l'archive ZIP. Elle contient un fichier .ova.
4. Transférez le fichier .ova vers un hôte dans le centre de données Red Hat Virtualisation/oVirt que vous souhaitez protéger.
5. Connectez-vous au portail d'administration Red Hat Virtualization/oVirt en tant qu'administrateur. Pour plus d'informations sur les rôles requis pour les opérations avec les machines virtuelles, reportez-vous à "Agent pour oVirt - Rôles et ports requis" (p. 165).
6. Dans le menu de navigation, sélectionnez **Calcul** > **Machines virtuelles**.
7. Cliquez sur l'icône représentant trois points verticaux  au-dessus du tableau principal, puis cliquez sur **Importer**.
8. Dans la fenêtre **Importer machine(s) virtuelle(s)**, procédez comme suit :
   a. Dans **Centre de données**, sélectionnez le centre de données que vous souhaitez protéger.
   b. Dans **Source**, sélectionnez **Appliance virtuelle (OVA)**.
   c. Dans **Hôte**, sélectionnez l'hôte sur lequel vous avez transféré le fichier .ova.
   d. Dans **Chemin d'accès au fichier**, indiquez le chemin d'accès au répertoire qui contient le fichier .ova.
   e. Cliquez sur **Charger**.
      Le modèle d'appliance virtuelle oVirt du fichier .ova apparaît dans le panneau **Machines virtuelles dans la source**.
      Si le modèle n'apparaît pas dans ce panneau, assurez-vous que vous avez indiqué le bon chemin d'accès au fichier, que le fichier n'est pas endommagé et qu'il est possible d'accéder à l'hôte.
   f. Dans **Machines virtuelles dans la source**, sélectionnez le modèle d'appliance virtuelle oVirt, puis cliquez sur la flèche de droite.
      Le modèle apparaît dans le panneau **Machines virtuelles à importer**.
   g. Cliquez sur **Suivant**.
9. Dans la nouvelle fenêtre, cliquez sur le nom de l'appliance, puis configurez les paramètres suivants :

- Dans l'onglet **Interfaces réseau**, configurez les interfaces réseau.
- [Facultatif] Dans l'onglet **Général**, modifiez le nom par défaut de la machine virtuelle avec l'agent

Le déploiement est maintenant terminé. Vous devez ensuite configurer l'appliance virtuelle. Pour en savoir plus sur sa configuration, reportez-vous à "Configuration de l'appliance virtuelle" (p. 162).

Remarque
Si vous avez besoin de plus d'une appliance virtuelle dans votre centre de données, répétez les étapes ci-dessus et déployez d'autres appliances virtuelles. Ne clonez pas une appliance virtuelle existante à l'aide de l'option **Cloner MV** dans le portail d'administration Red Hat Virtualization/oVirt.

Pour exclure l'appliance virtuelle de sauvegardes de groupe dynamique, vous devez aussi l'exclure de la liste des machines virtuelles dans la console Cyber Protect. Pour l'exclure, dans le portail d'administration Red Hat Virtualization/oVirt, sélectionnez la machine virtuelle avec l'agent, puis attribuez-lui le libellé `acronis_virtual_appliance`.

Configuration de l'appliance virtuelle

Après avoir déployé l'appliance virtuelle, vous devez la configurer afin qu'elle puisse atteindre aussi bien le moteur oVirt que le service Cyber Protection.

Pour configurer l'appliance virtuelle

1. Connectez-vous au portail d'administration Red Hat Virtualization/oVirt.
2. Sélectionnez l'appliance virtuelle que vous souhaitez configurer, puis cliquez sur l'icône **Console**.
3. Dans le champ **eth0**, configurez les interfaces réseau de l'appliance.
   Assurez-vous que les adresses DHCP attribuées automatiquement (s'il y en a) sont valides au sein des réseaux que votre machine virtuelle utilise, ou attribuez-les manuellement. Selon le nombre de réseaux que l'appliance utilise, vous aurez peut-être une ou plusieurs interfaces à configurer.
4. Dans le champ **oVirt**, cliquez sur **Modifier** pour indiquer l'adresse et les identifiants du moteur oVirt afin d'y accéder :
   a. Dans le champ **Nom/IP du serveur**, entrez le nom DNS ou l'adresse IP du moteur.
   b. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les identifiants d'administrateur pour ce moteur.
      Assurez-vous que ce compte administrateur dispose des rôles requis pour effectuer des opérations avec des machines virtuelles Red Hat Virtualization/oVirt. Pour plus d'informations sur ces rôles, reportez-vous à "Agent pour oVirt - Rôles et ports requis" (p. 165).
      Si le fournisseur d'authentification unique pour le moteur oVirt est Keycloak (par défaut dans oVirt 4.5.1), utilisez le format Keycloak lorsque vous indiquez le nom d'utilisateur. Par exemple, indiquez comme compte administrateur par défaut le compte `admin@ovirt@internalsso` au lieu d'`admin@internal`.

c. [Facultatif] Cliquez sur **Vérifier la connexion** pour vous assurer que les identifiants fournis sont corrects.

d. Cliquez sur **OK**.

5. Enregistrez l'appliance dans le service Cyber Protection à l'aide de l'une des méthodes suivantes.

- [Uniquement pour les tenants sans authentification à deux facteurs] Enregistrez l'appliance dans son interface graphique.

  a. Sous **Options de l'agent**, dans le champ **Serveur de gestion**, cliquez sur **Modifier**.

  b. Dans le champ **Nom/IP du serveur**, sélectionnez **Cloud**.

  L'adresse du service Cyber Protection apparaît. Sauf indication contraire, ne modifiez pas cette adresse.

  c. Dans les champs **Nom d'utilisateur** et **Mot de passe**, spécifiez les identifiants du compte dans le service Cyber Protection. L'appliance virtuelle et les machines virtuelles gérées par cette appliance sont enregistrées dans ce compte.

  d. Cliquez sur **OK**.

- Enregistrez l'appliance dans l'interface de ligne de commande.

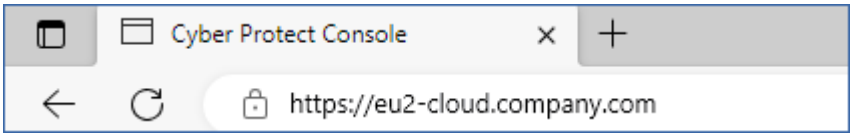
  Remarque
  Avec cette méthode, vous avez besoin d'un jeton d'enregistrement. Pour plus d'informations sur sa génération, reportez-vous à "Génération d'un jeton d'enregistrement" (p. 175).

  a. Appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.

  b. Exécuter la commande suivante :

  ```
  register_agent -o register -t cloud -a <service address> --token <registration token>
  ```

  Remarque
  Lorsque vous utilisez un jeton d'enregistrement, vous devez préciser l'adresse exacte du centre de données. Il s'agit de l'URL que vous voyez **une fois que vous êtes connecté** à la console Cyber Protect. Par exemple, `https://eu2-cloud.company.com`.

  Ne pas utiliser `https://cloud.company.com` ici.

  c. Pour revenir à l'interface graphique de l'appliance, appuyez sur ALT+F1.

6. [Facultatif] Dans le champ **Nom**, cliquez sur **Modifier** pour modifier le nom par défaut de l'appliance virtuelle, qui est **localhost**. Ce nom s'affiche dans la console Cyber Protect.
7. [Facultatif] Dans le champ **Heure**, cliquez sur **Modifier**, puis sélectionnez le fuseau horaire de votre emplacement afin de vous assurer que les opérations planifiées sont exécutées au bon moment.
8. [Facultatif] [Si un serveur proxy est activé sur votre réseau] Configurez le serveur proxy.

a. Appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.

b. Ouvrez le fichier **/etc/Acronis/Global.config** dans un éditeur de texte.

c. Effectuez l'une des actions suivantes :
   - Si les paramètres de proxy ont été précisés lors de l'installation de l'agent, recherchez la section suivante :

     ```
     <key name="HttpProxy">
         <value name="Enabled" type="Tdword">"1"</value>
         <value name="Host" type="TString">"ADDRESS"</value>
         <value name="Port" type="Tdword">"PORT"</value>
         <value name="Login" type="TString">"LOGIN"</value>
         <value name="Password" type="TString">"PASSWORD"</value>
     </key>
     ```

   - Autrement, copiez les lignes ci-dessus et collez-les dans le fichier entre les balises `<registry name="Global">...</registry>`.

d. Remplacez `ADDRESS` par la nouvelle adresse IP/nom d'hôte de serveur proxy et `PORT` par la valeur décimale du numéro de port.

e. Si votre serveur proxy nécessite une authentification, remplacez `LOGIN` et `PASSWORD` par les informations de connexion au serveur proxy. Dans le cas contraire, supprimez ces lignes du fichier.

f. Enregistrez le fichier.

g. Ouvrez le fichier **/opt/acronis/etc/aakore.yaml** dans un éditeur de texte.

h. Trouvez la section **env** ou créez-la, puis ajoutez-y les lignes suivantes :

   ```
   env:
       http-proxy: proxy_login:proxy_password@proxy_address:port
       https-proxy: proxy_login:proxy_password@proxy_address:port
   ```

i. Remplacez `proxy_login` et `proxy_password` par les identifiants de connexion au serveur proxy, et `proxy_address:port` par l'adresse et le numéro de port du serveur proxy.

j. Exécutez la commande `reboot`.

Remarque

Pour pouvoir mettre à jour une appliance virtuelle déployée derrière un proxy, modifiez le fichier `config.yaml` de l'appliance (`/opt/acronis/etc/va-updater/config.yaml`) en ajoutant la ligne suivante à la fin du fichier et en saisissant les valeurs propres à votre environnement :

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Par exemple :

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Pour protéger des machines virtuelles dans le centre de données Red Hat Virtualisation/oVirt

1. Connectez-vous à votre compte Cyber Protection.
2. Accédez à **Terminaux** > **oVirt** > <votre cluster>, ou recherchez vos ordinateurs dans **Terminaux** > **Tous les terminaux**.
3. Sélectionnez les ordinateurs et appliquez-leur un plan de protection.

Agent pour oVirt - Rôles et ports requis

Rôles requis

Pour son déploiement et son fonctionnement, l'agent pour oVirt nécessite un compte administrateur avec les rôles suivants attribués.

oVirt/Red Hat Virtualization 4.2 et 4.3/Oracle Virtualization Manager 4.3

- DiskCreator
- UserVmManager
- TagManager
- UserVmRunTimeManager
- VmCreator

oVirt/Red Hat Virtualization 4.4, 4.5

- SuperUser

Ports requis

L'agent pour oVirt se connecte au moteur oVirt à l'aide de l'URL que vous spécifiez lors de la configuration de l'appliance virtuelle. Généralement, l'URL du moteur possède le format suivant : `https://ovirt.entreprise.com`.Dans ce cas, le protocole HTTPS et le port 443 sont utilisés.

Les paramètres oVirt différents des paramètres par défaut peuvent nécessiter d'autres ports. Vous pouvez déterminer le port exact en analysant le format de l'URL.Par exemple :

URL du moteur oVirt	Port	Protocole
`https://ovirt.entreprise.com/`	443	HTTPS
`http://ovirt.entreprise.com/`	80	HTTP
`https://ovirt.entreprise.com:1234/`	1234	HTTPS

Aucun port supplémentaire n'est requis pour les opérations de lecture/écriture de disque, car la sauvegarde est effectuée en mode HotAdd.

Déploiement de l'agent pour Synology

Avant de commencer

Avec l'agent pour Synology, vous pouvez sauvegarder des fichiers et des dossiers depuis et vers un NAS Synology. Les propriétés du NAS et les autorisations d'accès des partages, dossiers et fichiers sont conservées.

L'agent pour Synology s'exécute sur le NAS. Par conséquent, vous pouvez utiliser les ressources du terminal pour les opérations de traitement des données hors hôte, comme la réplication de sauvegarde, la validation et le nettoyage. Pour en savoir plus sur ces opérations, reportez-vous à "Traitement des données hors hôte" (p. 204).

Remarque
L'agent pour Synology ne prend en charge que les NAS dotés de processeurs x86_64. Les processeurs ARM ne sont pas pris en charge.

Vous pouvez restaurer une sauvegarde dans son emplacement d'origine ou dans un nouvel emplacement sur le NAS, et dans un dossier réseau accessible par ce terminal. Les sauvegardes dans le stockage dans le cloud peuvent également être restaurées sur un NAS non d'origine sur lequel est installé l'agent pour Synology.

Le tableau ci-dessous récapitule les sources et destinations de sauvegarde disponibles.

Que sauvegarder	Éléments à sauvegarder (Source de sauvegarde)	Où sauvegarder (Destination de sauvegarde)
Fichiers/dossiers	Dossier local*	Stockage dans le Cloud
		Dossier local*
	Dossier réseau (SMB)**	Dossier réseau (SMB)**
		Dossier NFS

* Comprend les clés USB insérées dans le NAS.

Remarque
Les dossiers chiffrés ne sont pas pris en charge. Ces dossiers ne sont pas affichés dans l'interface graphique Cyber Protection.

** L'utilisation de partages réseau externes en tant que source ou destination de la sauvegarde par l'intermédiaire du protocole SMB n'est disponible que pour les agents qui s'exécutent sur Synology DiskStation Manager 6.2.3 et les versions ultérieures. Les données hébergées sur le NAS

Synology proprement dit, y compris dans les partages réseau hébergés, peuvent être sauvegardées sans limites.

Limites

- L'agent pour Synology ne prend en charge que les NAS dotés de processeurs x86_64. Les processeurs ARM ne sont pas pris en charge.
- Les partages chiffrés et sauvegardés sont restaurés comme partages non chiffrés.
- Les partages sauvegardés pour lesquels l'option **Compression de fichier** est activée sont restaurés avec cette option désactivée.
- Vous ne pouvez restaurer sur un terminal Synology NAS que les sauvegardes créées par l'Agent for Synology.

Téléchargement du programme d'installation

Le programme d'installation de l'agent pour Synology est disponible sous forme de fichier SPK.

Agent pour Synology 7.x

Pour télécharger le programme d'installation

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Dans l'angle supérieur droit, cliquez sur **Ajouter**.
3. Dans **Périphériques de stockage en réseau (NAS)**, cliquez sur **Synology**.
   Le programme d'installation est téléchargé sur votre ordinateur.

Agent pour Synology 6.x

Pour télécharger le programme d'installation

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Dans l'angle supérieur droit, cliquez sur **Ajouter**.
3. Dans **Périphériques de stockage en réseau (NAS)**, cliquez sur **Synology**.
   Le programme d'installation de l'agent pour Synology 7.x est téléchargé sur votre ordinateur.
   Vous pouvez arrêter en toute sécurité le processus de téléchargement ou ignorer le fichier téléchargé.
4. Cliquez sur **Télécharger l'agent pour Synology 6.x**.
   Le programme d'installation de l'agent pour Synology 6.x est téléchargé sur votre ordinateur.

Installation de l'agent pour Synology

Pour installer l'agent pour Synology, exécutez le fichier SPK dans Synology DiskStation Manager.

Remarque
L'agent pour Synology ne prend en charge que les NAS dotés de processeurs x86_64. Les processeurs ARM ne sont pas pris en charge.

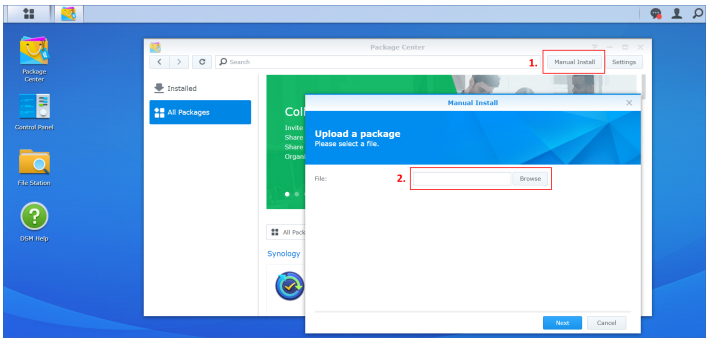
Agent pour Synology 7.x

Prérequis

- Le terminal NAS exécute DiskStation Manager 7.x.
- Vous êtes membre du groupe d'**administrateurs** sur le terminal NAS.
- Le volume du NAS sur lequel vous souhaitez installer l'agent dispose d'au moins 200 Mo d'espace libre.
- Un client SSH est disponible sur votre ordinateur. Ce document utilise Putty comme exemple.

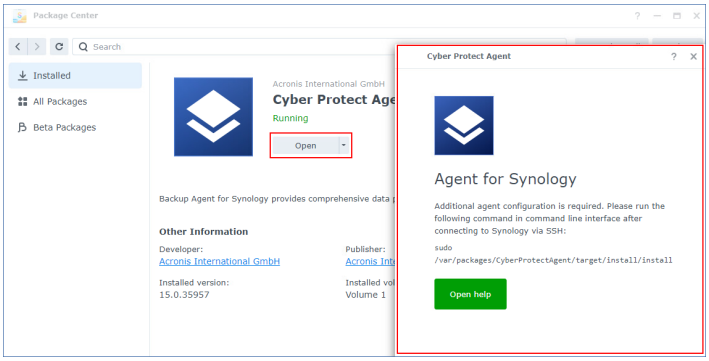
Pour installer l'agent pour Synology

1. Connectez-vous à Synology DiskStation Manager.
2. Ouvrez le **Package Center**.
3. Cliquez sur **Installation manuelle**, puis sur **Parcourir**.



4. Sélectionnez le fichier SPK que vous avez téléchargé à partir de la console Cyber Protect, puis cliquez sur **Suivant**.

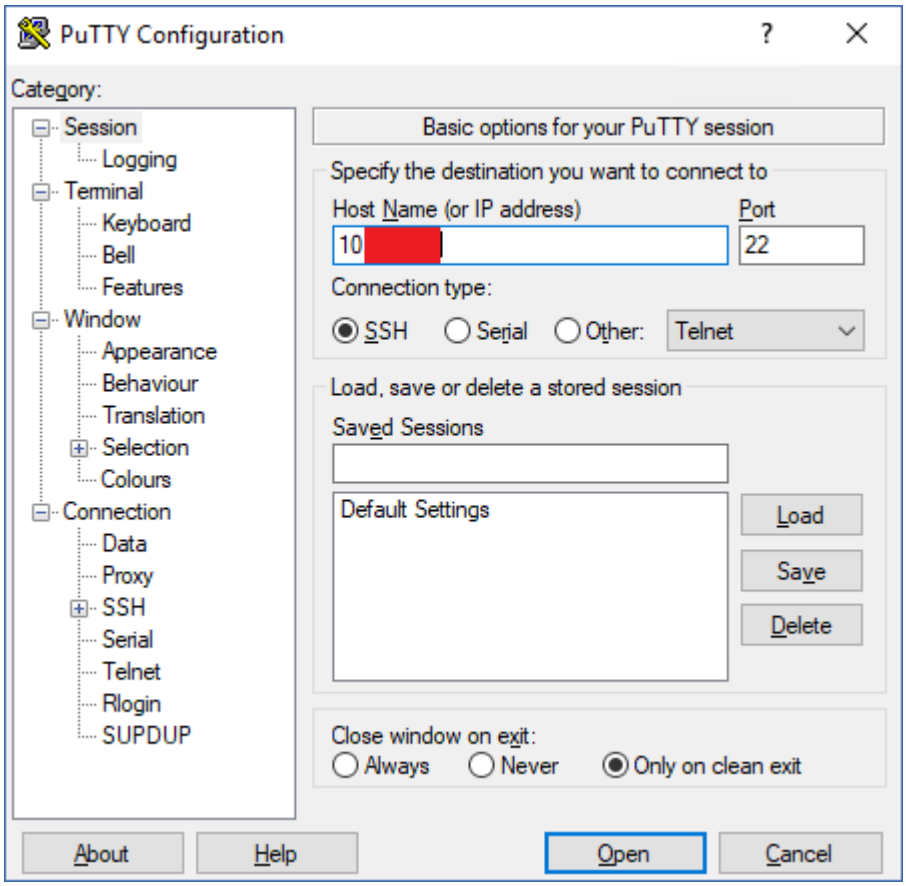
   Un avertissement s'affiche pour indiquer que vous allez installer un package logiciel tiers. Ce message fait partie de la procédure d'installation standard.
5. Pour confirmer que vous souhaitez installer le package, cliquez sur **Accepter**.
6. Sélectionnez le volume sur lequel vous souhaitez installer l'agent, puis cliquez sur **Suivant**.
7. Vérifiez les paramètres, puis cliquez sur **Terminé**.
8. Dans le **Package Center** de Synology DiskStation Manager, ouvrez l'agent Cyber Protect pour Synology, puis vérifiez que vous voyez l'écran suivant.



9. Dans le **Panneau de configuration** de Synology DiskStation Manager, accédez à **Terminal & SNMP**, puis activez l'accès SSH au terminal NAS.
10. Exécutez le script d'`installation` sur le terminal NAS à l'aide d'un client SSH (dans cet exemple, Putty).

    Le script permet l'accès root (superutilisateur) à DSM 7.0 ou à une version ultérieure, qui est l'accès nécessaire à la configuration de l'agent.

    a. Démarrez Putty, puis spécifiez l'adresse IP ou le nom d'hôte du terminal Synology NAS.



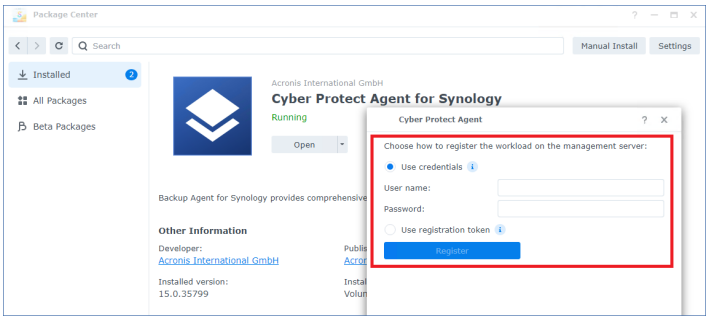
    b. Cliquez sur **Ouvrir**, puis connectez-vous en tant qu'administrateur Synology DSM.

    c. Exécutez la commande suivante.

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

    Après le démarrage du script, attendez 15 secondes pendant lesquelles les services Cyber Protection s'initialisent.

11. Dans le **Panneau de configuration** de Synology DiskStation Manager, accédez à **Terminal & SNMP**, puis désactivez l'accès SSH au terminal NAS. L'accès SSH n'est plus nécessaire.
12. Dans le **Package Center** de Synology DiskStation Manager, ouvrez l'agent Cyber Protect pour Synology.
13. Sélectionnez la méthode d'inscription.



- [Pour enregistrer l'agent en utilisant les informations d'identification].
  - Dans les champs **Nom d'utilisateur** et **Mot de passe**, indiquez les identifiants du compte sous lequel l'agent sera enregistré. Ce compte ne peut pas être un compte administrateur partenaire.
- [Pour enregistrer l'agent à l'aide d'un jeton d'enregistrement]
  - Dans **Adresse d'enregistrement**, indiquez l'adresse exacte du centre de données. Il s'agit de l'URL que vous voyez après vous être connecté à la console Cyber Protect. Par exemple, `https://us5-cloud.acronis.com`.

    Remarque
    N'utilisez pas un format d'URL sans adresse de centre de données. Par exemple, n'utilisez pas `https://cloud.acronis.com`.

  - Dans le champ **Jeton**, indiquez le jeton d'enregistrement.

    Pour plus d'informations sur la génération d'un jeton d'enregistrement, voir "Génération d'un jeton d'enregistrement" (p. 175).

14. Cliquez sur **Enregistrer**.

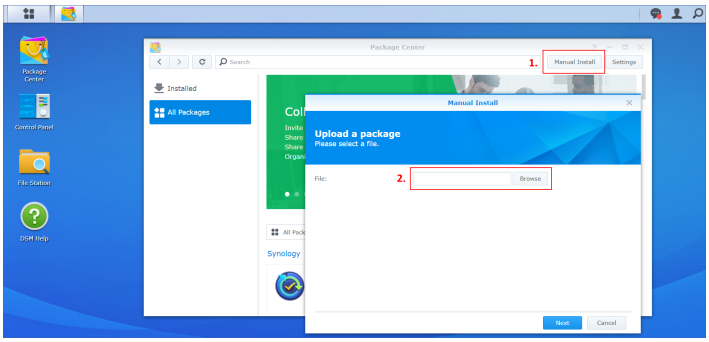
Agent pour Synology 6.x

Prérequis

- Le terminal NAS exécute DiskStation Manager 6.2.x.
- Vous êtes membre du groupe d'**administrateurs** sur le terminal NAS.
- Le volume du NAS sur lequel vous souhaitez installer l'agent dispose d'au moins 200 Mo d'espace libre.

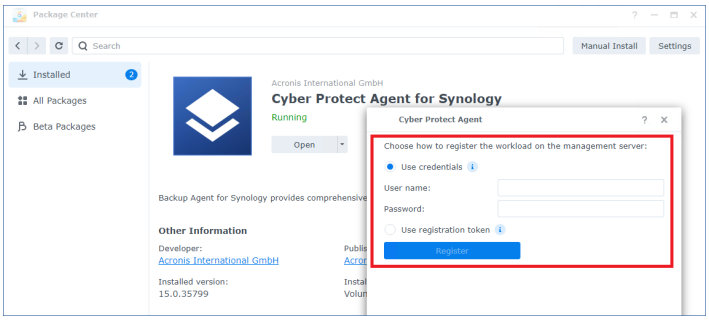
Pour installer l'agent pour Synology

1. Connectez-vous à Synology DiskStation Manager.
2. Ouvrez le **Package Center**.
3. Cliquez sur **Installation manuelle**, puis sur **Parcourir**.



4. Sélectionnez le fichier SPK que vous avez téléchargé à partir de la console Cyber Protect, puis cliquez sur **Suivant**.

   Un avertissement s'affiche pour indiquer que vous allez installer un package sans signature numérique. Ce message fait partie de la procédure d'installation standard.
5. Pour confirmer que vous souhaitez installer le package, cliquez sur **Oui**.
6. Sélectionnez le volume sur lequel vous souhaitez installer l'agent, puis cliquez sur **Suivant**.
7. Vérifiez les paramètres, puis cliquez sur **Appliquer**.
8. Dans le **Package Center** de Synology DiskStation Manager, ouvrez l'agent Cyber Protect pour Synology.
9. Sélectionnez la méthode d'inscription.



- [Pour enregistrer l'agent en utilisant les informations d'identification].
  - Dans les champs **Nom d'utilisateur** et **Mot de passe**, indiquez les identifiants du compte sous lequel l'agent sera enregistré. Ce compte ne peut pas être un compte administrateur partenaire.
- [Pour enregistrer l'agent à l'aide d'un jeton d'enregistrement]
  - Dans **Adresse d'enregistrement**, indiquez l'adresse exacte du centre de données. Il s'agit de l'URL que vous voyez après vous être connecté à la console Cyber Protect. Par exemple, `https://us5-cloud.acronis.com`.

    Remarque
    N'utilisez pas un format d'URL sans adresse de centre de données. Par exemple, n'utilisez pas `https://cloud.acronis.com`.
  - Dans le champ **Jeton**, indiquez le jeton d'enregistrement.

Pour plus d'informations sur la génération d'un jeton d'enregistrement, voir "Génération d'un jeton d'enregistrement" (p. 175).

10. Cliquez sur **Enregistrer**.

Après l'inscription, le terminal NAS Synology apparaît dans la console Cyber Protect, dans l'onglet **Terminaux** > **NAS**.

Pour sauvegarder les données sur ce terminal NAS, appliquez un plan de protection.

Mise à jour de l'agent pour Synology

Vous pouvez mettre à jour l'agent pour Synology 6.x vers une nouvelle version de l'agent pour Synology 6.x. De la même manière, vous pouvez mettre à jour l'agent pour Synology 7.x vers une nouvelle version de l'agent pour Synology 7.x.

Pour mettre à jour l'agent, exécutez la dernière version du programme d'installation dans Synology DiskStation Manager. L'inscription d'origine de l'agent, ses paramètres et les plans appliqués aux ressources protégées seront conservés.

Remarque
Vous ne pouvez pas mettre l'agent à jour depuis la console Cyber Protect.

La mise à niveau de l'agent pour Synology 6.x vers l'agent pour Synology 7.x n'est prise en charge que par la désinstallation de l'ancien agent et l'installation du nouvel agent. Dans ce cas, tous les plans de protection sont révoqués et vous devez les réappliquer manuellement.

Agent pour Synology 7.x

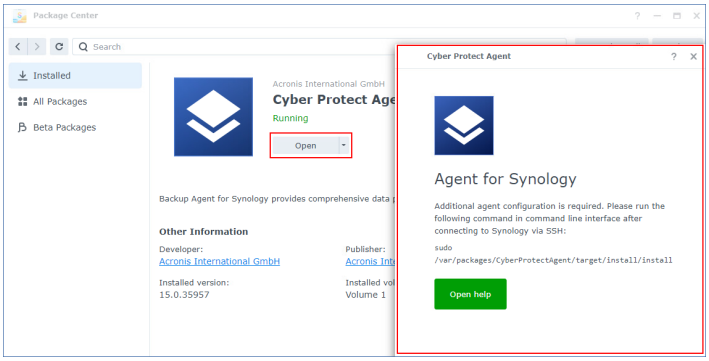
Prérequis

- Vous êtes membre du groupe d'**administrateurs** sur le terminal NAS.
- Le volume du NAS sur lequel vous souhaitez installer l'agent dispose d'au moins 200 Mo d'espace libre.
- Un client SSH est disponible sur votre ordinateur. Ce document utilise Putty comme exemple.

Pour mettre à jour l'agent pour Synology

1. Dans DiskStation Manager, ouvrez le **Package Center**.
2. Cliquez sur **Installation manuelle**, puis sur **Parcourir**.
3. Sélectionnez le dernier fichier SPK de l'agent pour Synology 7.x que vous avez téléchargé depuis la console Cyber Protect, puis cliquez sur **Suivant**.
   Un avertissement s'affiche pour indiquer que vous allez installer un package logiciel tiers. Ce message fait partie de la procédure d'installation standard.
4. Pour confirmer que vous souhaitez installer le package, cliquez sur **Accepter**.
5. Vérifiez les paramètres, puis cliquez sur **Terminé**.

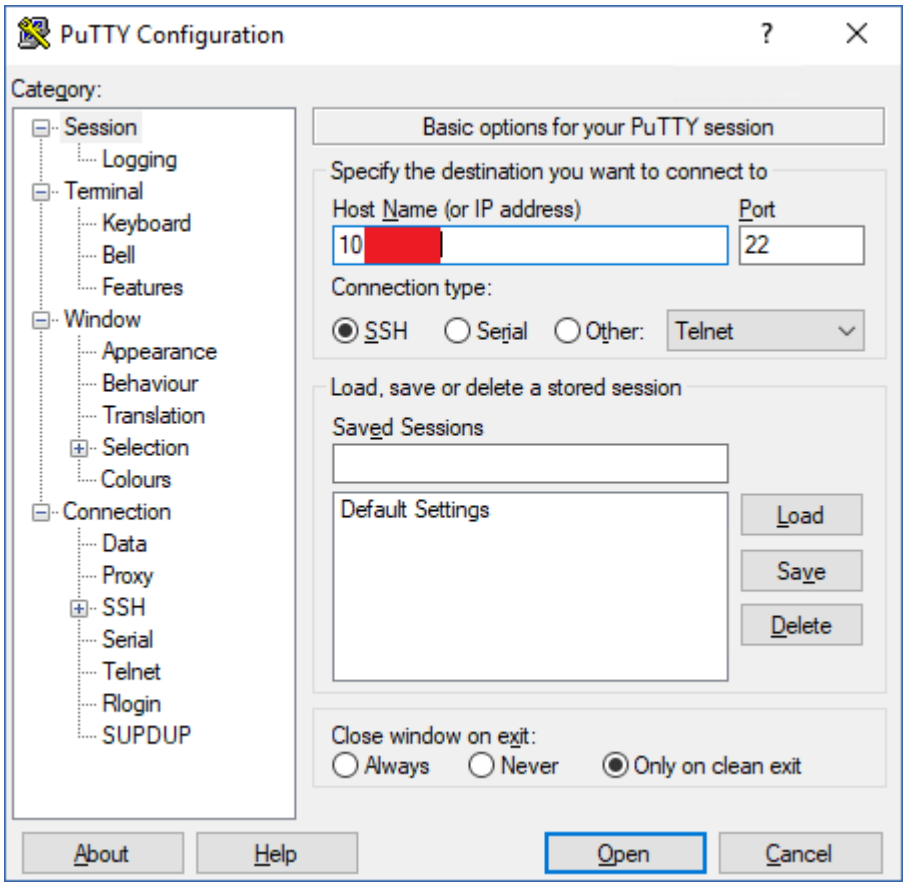
6. Dans le **Package Center** de Synology DiskStation Manager, ouvrez l'agent Cyber Protect pour Synology, puis vérifiez que vous voyez l'écran suivant.



7. Dans le **Panneau de configuration** de Synology DiskStation Manager, accédez à **Terminal & SNMP**, puis activez l'accès SSH au terminal NAS.
8. Exécutez le script d'`installation` sur le terminal NAS à l'aide d'un client SSH (dans cet exemple, Putty).

   Le script permet l'accès root (superutilisateur) à DSM 7.0 ou à une version ultérieure, qui est l'accès nécessaire à la configuration de l'agent.

   a. Démarrez Putty, puis spécifiez l'adresse IP ou le nom d'hôte du terminal Synology NAS.



   b. Cliquez sur **Ouvrir**, puis connectez-vous en tant qu'administrateur Synology DSM.

c. Exécutez la commande suivante.

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

9. Dans le **Panneau de configuration** de Synology DiskStation Manager, accédez à **Terminal & SNMP**, puis désactivez l'accès SSH au terminal NAS. L'accès SSH n'est plus nécessaire.

Agent pour Synology 6.x

Prérequis

- Vous êtes membre du groupe d'**administrateurs** sur le terminal NAS.
- Le volume du NAS sur lequel vous souhaitez installer l'agent dispose d'au moins 200 Mo d'espace libre.

Pour mettre à jour l'agent pour Synology

1. Dans DiskStation Manager, ouvrez le **Package Center**.
2. Cliquez sur **Installation manuelle**, puis sur **Parcourir**.
3. Sélectionnez le dernier fichier SPK de l'agent pour Synology 6.x que vous avez téléchargé depuis la console Cyber Protect, puis cliquez sur **Suivant**.
   Un avertissement s'affiche pour indiquer que vous allez installer un package sans signature numérique. Ce message fait partie de la procédure d'installation standard.
4. Pour confirmer que vous souhaitez installer le package, cliquez sur **Oui**.
5. Vérifiez les paramètres, puis cliquez sur **Appliquer**.

Déploiement des agents via la stratégie de groupe

Vous pouvez installer (ou déployer) de manière centralisée l'agent pour Windows sur des ordinateurs membres d'un domaine Active Directory à l'aide de la stratégie de groupe de Windows.

Dans cette section, vous apprendrez comment configurer un objet de stratégie de groupe pour déployer des agents sur les machines d'un domaine entier ou dans son unité organisationnelle.

Chaque fois qu'une machine se connecte au domaine, l'objet de stratégie de groupe obtenu garantit que l'agent est installé et enregistré.

Prérequis

- Domaine Active Directory avec contrôleur de domaine exécutant Microsoft Windows Server 2003 ou une version ultérieure.
- Vous devez être membre du groupe **Admins du domaine** dans ce domaine.
- Vous avez téléchargé le programme d'installation **Tous les agents pour Windows**.
  Pour télécharger le Pour télécharger le programme d'installation, cliquez dans la console Cyber Protect sur l'icône de compte en haut à droite, puis sur **Téléchargements**. Le lien de téléchargement est également disponible dans le panneau **Ajouter des terminaux**.

Pour déployer des agents via la stratégie de groupe

1. Générez un jeton d'enregistrement en suivant les indications de "Génération d'un jeton d'enregistrement" (p. 175).
2. Créez le fichier .mst, le fichier .msi et les fichiers .cab en suivant les indications de "Création du fichier de transformation et extraction des packages d'installation" (p. 178).
3. Configurez l'objet de stratégie de groupe en suivant les indications de "Configuration de l'objet de stratégie de groupe" (p. 179).

Génération d'un jeton d'enregistrement

Un jeton d'enregistrement transmet l'identité d'un utilisateur au programme d'installation de l'agent sans stocker ses identifiants de l'utilisateur pour la console Cyber Protect. Par conséquent, les utilisateurs peuvent enregistrer autant d'ordinateurs qu'ils le souhaitent dans leur compte ou appliquer des plans de protection à leurs ressources sans besoin de se connecter.

Remarque
Les plans de protection ne sont pas appliqués automatiquement lors de l'enregistrement de l'ordinateur. L'application d'un plan de protection est une tâche distincte.

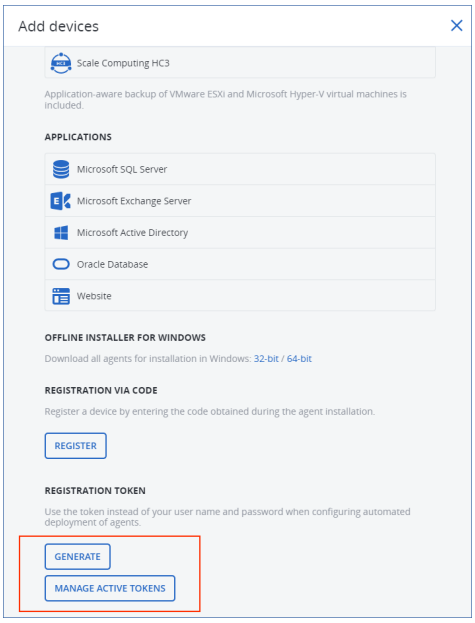
Pour des raisons de sécurité, la durée de vie des jetons est limitée, mais elle peut être modifiée. La durée de vie par défaut est de trois jours.

Les utilisateurs peuvent générer des jetons d'enregistrement uniquement pour leur propre compte. Les administrateurs peuvent générer des jetons d'enregistrement pour tous les comptes utilisateur du tenant qu'ils gèrent.

Générer un jeton d'enregistrement

En tant qu'utilisateur

1. Connectez-vous à la console Cyber Protect.
2. Cliquez sur **Terminaux** > **Tous les terminaux** > **Ajouter**.
   Le panneau **Ajouter des terminaux** s'ouvre à droite.
3. Cherchez **Jeton d'enregistrement**, puis cliquez sur **Générer**.



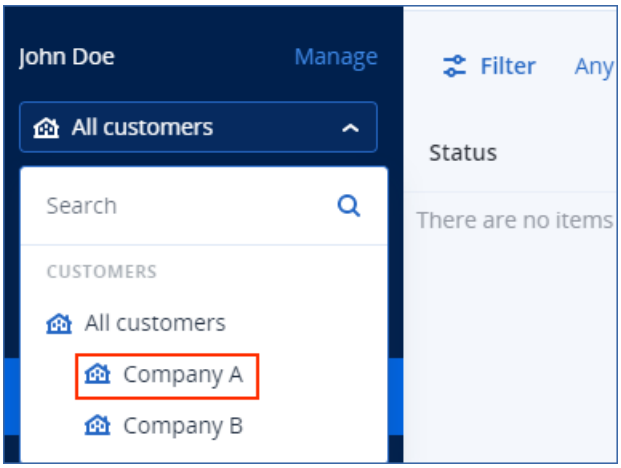
4. Spécifiez la durée de vie du jeton.
5. Cliquez sur **Générer le jeton**.
6. Cliquez sur **Copier** pour copier le jeton dans le Presse-papiers de votre terminal ou notez le jeton manuellement.

En tant qu'administrateur

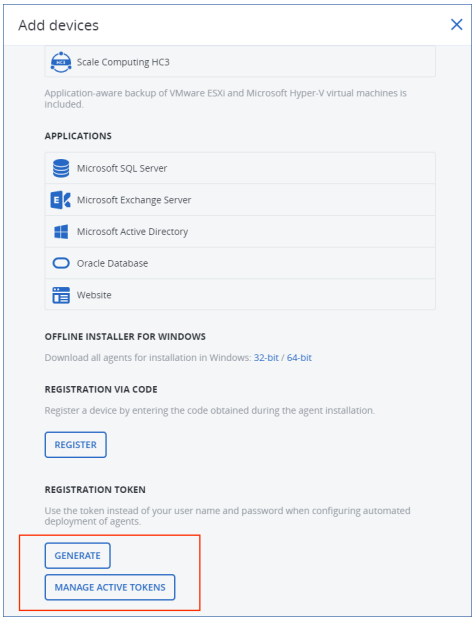
1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
   Si vous êtes déjà connecté au portail de gestion, vous pouvez accéder à la console Cyber Protect en sélectionnant **Surveillance** > **Utilisation**, puis en cliquant dans l'onglet **Protection** sur **Gérer le service**.

   [Pour les administrateurs partenaires qui gèrent les tenants des clients] Dans la console Cyber Protect, sélectionnez le tenant comportant l'utilisateur pour lequel vous souhaitez générer un jeton. Vous ne pouvez pas générer de jeton au niveau **Tous les clients**.



2. Sous **Terminaux**, cliquez sur **Tous les terminaux** > **Ajouter**.
   Le panneau **Ajouter des terminaux** s'ouvre à droite.
3. Cherchez **Jeton d'enregistrement**, puis cliquez sur **Générer**.



4. Spécifiez la durée de vie du jeton.
5. Sélectionnez l'utilisateur pour qui vous souhaitez générer un jeton.

   Remarque
   Lorsque vous utilisez le jeton, les ressources sont inscrites dans le compte utilisateur sélectionné ici.

6. [Facultatif] Pour permettre à l'utilisateur du jeton d'appliquer ou de révoquer un plan de protection sur les ressources ajoutées, sélectionnez le plan dans la liste déroulante.
   Veuillez noter que vous devrez exécuter un script qui appliquera ou révoquera un plan de protection sur les ressources ajoutées. Pour plus d'informations, reportez-vous à cet article de la base de connaissances.
7. Cliquez sur **Générer le jeton**.

8. Cliquez sur **Copier** pour copier le jeton dans le Presse-papiers de votre terminal ou notez le jeton manuellement.

Pour afficher ou supprimer des jetons d'enregistrement

1. Connectez-vous à la console Cyber Protect.
2. Cliquez sur **Terminaux** > **Tous les terminaux** > **Ajouter**.
3. Cherchez **Jeton d'enregistrement**, puis cliquez sur **Gérer les jetons actifs**.
   La liste des jetons actifs qui sont générés pour le tenant s'ouvre à droite.

   Remarque
   Pour des raisons de sécurité, seuls les deux premiers caractères de la valeur de jeton sont affichés dans la colonne **Jeton**.

4. [Pour supprimer un jeton] Sélectionnez le jeton, puis cliquez sur **Supprimer**.

Création du fichier de transformation et extraction des packages d'installation

Pour déployer des agents de protection via la stratégie de groupe de Windows, vous avez besoin d'un fichier de transformation (.mst) et des packages d'installation (fichiers .msi et .cab).

Remarque
La procédure ci-dessous utilise l'option d'inscription par défaut, c'est-à-dire l'inscription par jeton. Pour en savoir plus sur la génération d'un jeton d'enregistrement, reportez-vous à "Génération d'un jeton d'enregistrement" (p. 175).

Pour créer le fichier .mst et extraire les packages d'installation (fichiers .msi et .cab)

1. Connectez-vous en tant qu'administrateur sur n'importe quel ordinateur du domaine Active Directory.
2. Créez un dossier partagé contenant les paquets d'installation. Assurez-vous que les utilisateurs du domaine peuvent accéder au dossier partagé — par exemple, en laissant les paramètres de partage par défaut sur **Tout le monde**.
3. Exécutez le programme d'installation de l'agent.
4. Cliquez sur **Créer des fichiers .mst et .msi pour une installation sans assistance**.
5. Dans **Que faut-il installer**, sélectionnez les composants que vous souhaitez inclure dans l'installation, puis cliquez sur **Terminé**.
6. Dans **Paramètres d'Inscription**, cliquez sur **Spécifier**, saisissez un jeton d'enregistrement, puis acliquez sur **Terminé**.
   Vous pouvez modifier la méthode d'inscription en passant de **Utiliser un jeton d'enregistrement** (par défaut) à **Utiliser les identifiants** ou à **Ignorer l'inscription**. L'option **Ignorer l'inscription** suppose que vous enregistrerez manuellement les ressources ultérieurement.

7. Vérifiez ou modifiez les paramètres d'installation qui seront ajoutés au fichier .mst, puis cliquez sur **Poursuivre**.
8. Dans **Enregistrer les fichiers dans**, spécifiez le chemin d'accès au dossier partagé que vous avez créé.
9. Cliquez sur **Générer**.

Le fichier .mst, le fichier .msi et les fichiers .cab sont créés et copiés dans le dossier partagé que vous avez spécifié.

Configurez ensuite l'objet de stratégie de groupe Windows. Pour savoir comment procéder, voir "Configuration de l'objet de stratégie de groupe" (p. 179).

Configuration de l'objet de stratégie de groupe

Dans cette procédure, vous utilisez les packages d'installation que vous avez créés dans "Création du fichier de transformation et extraction des packages d'installation" (p. 178) pour configurer un objet de stratégie de groupe (GPO). L'objet de stratégie de groupe déploiera les agents sur les ordinateurs de votre domaine.

Pour configurer l'objet de stratégie de groupe

1. Connectez-vous au contrôleur de domaine en tant qu'administrateur de domaine.
   Si le domaine possède plusieurs contrôleurs de domaine, connectez-vous à l'un d'eux en tant qu'administrateur de domaine.
2. [Si vous déployez des agents dans une unité d'organisation] Assurez-vous que l'unité d'organisation dans laquelle vous souhaitez déployer les agents existe dans ce domaine.
3. Dans le menu **Démarrer** de Windows, pointez sur **Outils d'administration**, puis cliquez sur **Gestion des stratégies de groupe** (ou **Utilisateurs et ordinateurs Active Directory** sous Windows Server 2003).
4. [Pour Windows Server 2008 ou versions ultérieures] Cliquez avec le bouton droit sur le nom du domaine ou de l'unité d'organisation, puis cliquez sur **Créer un objet GPO dans ce domaine, et le lier ici**.
5. [Pour Windows Server 2003] Cliquez avec le bouton droit sur le nom du domaine ou de l'unité d'organisation, puis cliquez sur **Propriétés**. Dans la boîte de dialogue, cliquez sur l'onglet **Stratégie de groupe**, puis cliquez sur **Nouvelle**.
6. Nommez le nouvel objet de la Stratégie de groupe **Agent pour Windows.**
7. Ouvrez l'objet de stratégie de groupe **Agent pour Windows** pour le modifier :
   - [Dans Windows Server 2008 ou versions ultérieures] Sous **Objets de stratégie de groupe**, cliquez avec le bouton droit sur l'objet stratégie de groupe, puis cliquez sur **Modifier**.
   - [Dans Windows Server 2003], cliquez sur l'objet de stratégie de groupe, puis cliquez sur **Modifier**.
8. Dans le composant logiciel enfichable de l'Editeur d'objet Stratégie de groupe, développez **Configuration de l'ordinateur**.

9. [Pour Windows Server 2012 ou versions ultérieures] Développez **Stratégies** > **Paramètres du logiciel**.
10. [Pour Windows Server 2003 et Windows Server 2008] Développez **Paramètres du logiciel**.
11. Cliquez avec le bouton droit sur **Installation du logiciel**, pointez sur **Nouveau**, puis cliquez sur **Package**.
12. Sélectionnez le package .msi d'installation de l'agent dans le dossier partagé que vous avez créé, puis cliquez sur **Ouvrir**.
13. Dans la boîte de dialogue **Déployer le logiciel**, cliquez sur **Avancées**, puis sur **OK**.
14. Dans l'onglet **Modifications**, cliquez sur **Ajouter**, puis sélectionnez le fichier .mst dans le dossier partagé que vous avez créé.
15. Cliquez sur **OK** pour fermer la boîte de dialogue **Déployer le logiciel**.

Connexions SSH à une appliance virtuelle

Utilisez une connexion SSH (Secure Socket Shell) lorsque vous accédez à distance à une appliance virtuelle à des fins de maintenance.

Démarrage du démon Secure Shell

Pour permettre les connexions SSH à une appliance virtuelle, démarrez le démon Secure Shell (sshd) sur l'appliance.

Pour démarrer le démon Secure Shell

1. Dans le logiciel hyperviseur, ouvrez la console de l'appliance virtuelle.
2. Dans l'interface graphique de l'appliance, appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.
3. Exécuter la commande suivante :

   ```
   /bin/sshd
   ```

4. [Uniquement lors de la première connexion à l'appliance] Définissez le mot de passe de l'utilisateur `root` (superutilisateur).

   Pour savoir comment définir le mot de passe, voir "Définition du mot de passe root sur une appliance virtuelle" (p. 180).

Remarque
Nous vous recommandons d'arrêter le démon Secure Shell lorsque vous n'utilisez pas la connexion SSH.

Définition du mot de passe root sur une appliance virtuelle

Avant d'établir la première connexion SSH à une appliance virtuelle, vous devez définir le mot de passe root sur l'appliance.

Pour définir le mot de passe root (superutilisateur)

1. Dans le logiciel hyperviseur, ouvrez la console de l'appliance virtuelle.
2. Dans l'interface graphique de l'appliance, appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.
3. Exécuter la commande suivante :

   ```
   passwd
   ```

4. Spécifiez un mot de passe, puis appuyez sur Entrée.
   Le mot de passe doit contenir au moins neuf caractères et doit avoir un score de complexité d'au moins trois. Le score de complexité est calculé automatiquement. Pour atteindre un score plus élevé, utilisez une combinaison de caractères spéciaux, de caractères en majuscules et en minuscules, et de chiffres.
5. Confirmez le mot de passe, puis appuyez sur Entrée.

Accéder à une appliance virtuelle via un client SSH

Prérequis

- Un client SSH doit être disponible sur la machine distante. La procédure ci-dessous utilise le client WinSCP comme exemple. Vous pouvez utiliser n'importe quel client SSH, en adaptant les étapes en conséquence.
- Le démon Secure Shell (sshd) doit être démarré sur l'appliance virtuelle. Pour plus d'informations, voir "Démarrage du démon Secure Shell" (p. 180).

Pour accéder à une appliance virtuelle via WinSCP

1. Sur la machine distante, ouvrez WinSCP.
2. Cliquez sur **Session** > **Nouvelle session**.
3. Dans **Protocole de fichier**, sélectionnez **SCP**.
4. Dans **Nom d'hôte**, spécifiez l'adresse IP de votre appliance virtuelle.
5. Dans **Nom d'utilisateur** et **Mot de passe**, spécifiez `root` et le mot de passe de l'`root`.
6. Cliquez sur **Connexion**.

La liste de tous les répertoires de l'appliance virtuelle s'affiche.

Mise à jour des agents

Vous pouvez mettre à jour manuellement tous les agents à l'aide de la console Cyber Protect ou en téléchargeant et en exécutant le fichier d'installation.

Vous pouvez configurer les mises à jour automatiques pour les agents suivants :

- Agent pour Windows
- Agent pour Linux
- Agent pour Mac
- Agent Cloud Cyber Files pour File Sync & Share

Pour mettre à jour un agent automatiquement, ou manuellement via la console Cyber Protect, 4,2 Go d'espace libre sont requis dans l'emplacement suivant :

- Linux : répertoire racine
- Windows : volume sur lequel l'agent est installé

Pour mettre à jour un agent sous macOS, dans le répertoire racine, 5 Go d'espace libre sont requis.

Remarque
[Pour tous les agents fournis sous la forme d'une appliance virtuelle, y compris Agent pour VMware, Agent pour Scale Computing, Agent pour Virtuozzo Hybrid Infrastructure, Agent pour RHV (oVirt)]

Pour effectuer une mise à jour automatique ou manuelle d'une appliance virtuelle située derrière un proxy, vous devez configurer le serveur proxy sur chaque appliance comme suit.

Dans le fichier `/opt/acronis/etc/va-updater/config.yaml`, ajoutez la ligne suivante en bas du fichier, puis saisissez les valeurs correspondant à votre environnement :

```
httpProxy : http://proxy_login:proxy_password@proxy_address:port
```

Mise à jour manuelle des agents

Vous pouvez mettre à jour les agents à l'aide de la console Cyber Protect ou en téléchargeant et en exécutant le fichier d'installation.

Les appliances virtuelles avec les versions suivantes doivent être mises à jour uniquement à l'aide de la console Cyber Protect :

- Agent pour VMware (appliance virtuelle) : version 12.5.23094 et ultérieures.
- Agent pour Virtuozzo Hybrid Infrastructure (appliance virtuelle) : version 12.5.23094 et ultérieures.

Les versions suivantes des agents peuvent aussi être mises à jour via la console Cyber Protect :

- Agent pour Windows, agent pour VMware (Windows), agent pour Hyper-V : version 12.5.21670 et ultérieures.
- Agent pour Linux : version 12.5.23094 et ultérieures.
- Autres agents : version 12.5.23094 et ultérieures.

Pour trouver la version de l'agent, dans la console Cyber Protect, sélectionnez l'ordinateur, puis cliquez sur **Détails**.

Pour effectuer une mise à jour des agents à partir de versions antérieures, téléchargez et installez manuellement la version la plus récente. Pour trouver les liens de téléchargement, cliquez sur **Tous les terminaux** > **Ajouter**.

Prérequis

Sur les machines Windows, les fonctionnalités Cyber Protect nécessitent le package redistribuable Microsoft Visual C++ 2017. Veillez à ce qu'il soit déjà installé sur votre ordinateur, ou installez-le avant de mettre l'agent à jour. Après l'installation, il peut être nécessaire de redémarrer l'ordinateur. Le package redistribuable Microsoft Visual C++ est disponible sur le site Web de Microsoft : https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Pour mettre à jour un agent via la console Cyber Protect

1. Cliquez sur **Paramètres** > **Agents**.
   Le logiciel affiche la liste des machines. Les machines dont la version des agents est obsolète sont marquées d'un point d'exclamation orange.
2. Sélectionnez les machines sur lesquelles vous souhaitez effectuer une mise à jour des agents. Ces machines doivent être en ligne.
3. Cliquez sur **Mise à jour de l'agent**.

Remarque
Lors de la mise à jour, toute sauvegarde en cours échouera.

Pour mettre à jour l'agent pour VMware (appliance virtuelle) dont la version est antérieure à 12.5.23094

1. Cliquez sur **Paramètres** > **Agents** > l'agent que vous souhaitez mettre à jour > **Détails**, puis examinez la section **Machines virtuelles attribuées**. Vous devrez de nouveau saisir ces paramètres après la mise à jour.
   a. Notez bien la position du commutateur **Attribution automatique**.
   b. Pour savoir quelles machines virtuelles sont attribuées manuellement à l'agent, cliquez sur le lien **Attribué :**. Le logiciel affiche la liste des machines virtuelles attribuées. Notez bien quelles machines ont `(M)` après le nom de l'agent dans la colonne **Agent**.
2. Supprimez l'agent pour VMware (appliance virtuelle), comme décrit dans « Désinstallation d'agents ». À l'étape 5, supprimez l'agent depuis **Paramètres** > **Agents**, même si vous prévoyez de réinstaller l'agent ultérieurement.
3. Déployez l'agent pour VMware (appliance virtuelle) comme décrit dans « Déploiement du modèle OVF ».
4. Configurez l'agent pour VMware (appliance virtuelle), comme décrit dans « Configuration de l'appliance virtuelle ».
   Si vous souhaitez reconstruire le stockage connecté localement, procédez comme suit à l'étape 7 :

a. Ajoutez à l'appliance virtuelle le disque contenant le stockage local.

b. Cliquez sur **Actualiser** > **Créer le stockage** > **Monter**.

c. Le logiciel affiche la **Lettre** et le **Libellé** d'origine du disque. Ne les changez pas.

d. Cliquez sur **OK**.

5. Cliquez sur **Paramètres** > **Agents** > l'agent que vous souhaitez mettre à jour > **Détails**, puis redéfinissez les paramètres que vous avez notés à l'étape 1. Si certaines machines virtuelles ont été manuellement attribuées à l'agent, attribuez-les de nouveau comme décrit dans « Liaison de machine virtuelle ».

   Une fois la configuration de l'agent terminée, les plans de protection appliqués à l'ancien agent sont réappliqués automatiquement au nouvel agent.
6. Les plans pour lesquels la sauvegarde reconnaissant les applications est activée nécessitent de saisir de nouveau les informations d'identification. Modifiez ces plans et saisissez de nouveau les informations d'identification.
7. Les plans qui sauvegardent la configuration ESXi nécessitent de saisir de nouveau le mot de passe « racine ». Modifiez ces plans et saisissez de nouveau le mot de passe.

Pour mettre à jour les définitions de cyberprotection sur une machine

1. Cliquez sur **Paramètres** > **Agents**.
2. Sélectionnez la machine sur laquelle vous souhaitez effectuer une mise à jour des définitions de cyberprotection, puis cliquez sur **Mettre les définitions à jour**. La machine doit être en ligne.

Pour attribuer le rôle Responsable de la mise à jour à un agent

1. Cliquez sur **Paramètres** > **Agents**.
2. Sélectionnez l'ordinateur auquel vous souhaitez affecter le rôle Responsable de la mise à jour, cliquez sur **Détails**, puis activez dans la section **Définitions de la cyberprotection** l'option **Utilisez cet agent pour télécharger et distribuer des correctifs et des mises à jour**.

Remarque
Un agent avec le rôle Responsable de la mise à jour ne peut télécharger et distribuer des correctifs que pour les produits tiers Windows. Pour les produits Microsoft, la distribution des correctifs n'est pas prise en charge par l'agent Responsable de la mise à jour.

Pour effacer les données en cache sur un agent

1. Cliquez sur **Paramètres** > **Agents**.
2. Sélectionnez la machine dont vous souhaitez effacer les données en cache (fichiers de mise à jour et données de gestion des correctifs obsolètes), puis cliquez sur **Vider le cache**.

Mise à jour automatique des agents

Pour faciliter la gestion de plusieurs ressources, vous pouvez configurer la mise à jour automatique de l'agent pour Windows, de l'agent pour Linux et de l'agent pour Mac. Les mises à jour

automatiques sont disponibles pour les agents version 15.0.26986 (publiée en mai 2021) ou versions ultérieures. Pour les agents plus anciens, vous devez d'abord effectuer une mise à jour à la dernière version.

Les mises à jour automatiques sont prises en charge sur les ordinateurs exécutant l'un des systèmes d'exploitation suivants :

- Windows XP SP 3 et versions ultérieures
- Red Hat Enterprise Linux 6 et versions ultérieures, CentOS 6 et versions ultérieures
- OS X 10.9 Mavericks et versions ultérieures

Les paramètres de mise à jour automatique sont préconfigurés au niveau du centre de données. Un administrateur d'entreprise peut personnaliser ces paramètres, pour tous les ordinateurs d'une entreprise ou d'une unité, ou pour des machines individuelles. Si aucun paramètre personnalisé n'est appliqué, les paramètres du niveau supérieur sont utilisés, dans cet ordre :

1. Centre de données Cyber Protection
2. Entreprise (tenant client)
3. Unité
4. Machine

Par exemple, un administrateur d'unité peut configurer des paramètres de mise à jour automatique pour tous les ordinateurs de l'unité, qui peuvent être différents des paramètres appliqués aux ordinateurs au niveau de l'entreprise. L'administrateur peut aussi configurer différents paramètres pour un ou plusieurs ordinateurs individuels de l'unité, sur lesquels les paramètres au niveau de l'unité et de l'entreprise ne seront pas appliqués.

Après l'activation des mises à jour automatiques, vous pouvez configurer les options suivantes :

- **Mise à jour du canal**
  Cette option définit quelle version des agents sera utilisée (la plus récente ou la dernière version par rapport à la version précédente).
- **Fenêtre de maintenance**
  Cette option définit à quel moment les mises à jour peuvent être installées. Si la fenêtre de maintenance est désactivée, les mises à jour peuvent être effectuées à tout moment.
  Même lors de la fenêtre de maintenance activée, les mises à jour ne seront pas installées tant que l'agent exécutera l'une des opérations suivantes :
  - Sauvegarde
  - Restauration
  - Réplication de sauvegarde
  - Réplication de machine virtuelle
  - Test d'un réplica
  - Exécution d'une machine virtuelle à partir d'une sauvegarde (y compris finalisation)

- Basculement pour reprise d'activité après sinistre
- Restauration automatique pour reprise d'activité après sinistre
- Exécution d'un script (pour la fonctionnalité de création de cyber-scripts)
- Installation des correctifs
- Sauvegarde de la configuration ESXi

Personnaliser les paramètres de mise à jour automatique

1. Dans la console Cyber Protect, accédez à **Paramètres** > **Agents**.
2. Sélectionner la portée des paramètres :
   - Pour modifier les paramètres pour tous les ordinateurs, cliquez sur **Modifier les paramètres de mise à jour d'agent par défaut**.
   - Pour modifier les paramètres pour des ordinateurs spécifiques, sélectionnez les ordinateurs souhaités, puis cliquez sur **Paramètres de mise à jour d'agent**.
3. Configurez les paramètres selon vos besoins, puis cliquez sur **Appliquer**.

Supprimer les paramètres de mise à jour automatique personnalisés

1. Dans la console Cyber Protect, accédez à **Paramètres** > **Agents**.
2. Sélectionner la portée des paramètres :
   - Pour supprimer les paramètres personnalisés pour tous les ordinateurs, cliquez sur **Modifier les paramètres de mise à jour d'agent par défaut**.
   - Pour supprimer les paramètres pour des ordinateurs spécifiques, sélectionnez les ordinateurs souhaités, puis cliquez sur **Paramètres de mise à jour d'agent**.
3. Cliquez sur **Réinitialiser au défaut**, puis sur **Appliquer**.

Vérifier le statut de mise à jour automatique

1. Dans la console Cyber Protect, accédez à **Paramètres** > **Agents**.
2. Cliquez sur l'icône en forme d'engrenage en haut à droite du tableau, puis assurez-vous que la case **Mise à jour automatique** est cochée.
3. Consultez le statut qui s'affiche dans la colonne **Mise à jour automatique**.

Mise à jour des agents sur les ressources protégées par BitLocker

Les mises à jour d'agents qui introduisent des changements sur Startup Recovery Manager interfèrent avec BitLocker sur les ressources sur lesquelles BitLocker et Startup Recovery Manager sont activés. Dans ce cas, après un redémarrage, la clé de restauration BitLocker est requise. Pour atténuer ce problème, suspendez ou désactivez BitLocker avant de mettre à jour l'agent.

Versions de l'agent concernées :

- 23.12.36943, sortie en décembre 2023

Vous pouvez également vérifier dans les notes de publication de l'agent de protection si la mise à jour apporte des modifications à Startup Recovery Manager.

Pour mettre à jour l'agent sur une ressource avec BitLocker et Startup Recovery Manager activés

1. Sur la ressource sur laquelle vous voulez mettre à jour l'agent, suspendez ou désactivez BitLocker.
2. Mettre à jour l'agent.
3. Redémarrez la ressource.
4. Activer BitLocker.

Empêcher la désinstallation ou la modification non autorisée d'agents

Vous pouvez protéger l'agent pour Windows contre l'installation ou la modification non autorisée, en activant le paramètre **Protection par mot de passe** dans un plan de protection. Ce paramètre est disponible uniquement si le paramètre **Autoprotection** est activé.

Activer la protection par mot de passe

1. Dans un plan de protection, développez le module **Protection contre les virus et les malwares** (module **Active Protection** pour les éditions Cyber Backup).
2. Cliquez sur **Autoprotection** et assurez-vous que l'interrupteur **Autoprotection** est activé.
3. Activez l'interrupteur **Protection par mot de passe**.
4. Dans la fenêtre qui s'ouvre, copiez le mot de passe dont vous avez besoin pour désinstaller ou modifier les composants d'un Agent pour Windows protégé.

   Ce mot de passe est unique et vous ne serez pas en mesure de le récupérer si vous fermez cette fenêtre. Si vous perdez ou oubliez ce mot de passe, vous pouvez modifier le plan de protection et créer un nouveau mot de passe.
5. Cliquez sur **Fermer**.
6. Dans le volet **Autoprotection**, cliquez sur **Terminé**.
7. Enregistrez le plan de protection.

La protection par mot de passe sera activée pour les machines auxquelles ce plan de protection sera appliqué. La protection par mot de passe est uniquement disponible pour Agent pour Windows version *15.0.25851* ou ultérieure. Ces machines doivent être en ligne.

Vous pouvez appliquer un plan de protection avec protection par mot de passe activée à une machine exécutant macOS, mais aucune protection ne sera fournie. Vous ne pouvez pas appliquer un tel plan à une machine fonctionnant sous Linux.

Par ailleurs, vous ne pouvez pas appliquer plus d'un plan de protection avec protection par mot de passe activée à la même machine Windows. Pour apprendre à résoudre un conflit potentiel, consultez Résolution des conflits de plan.

Modifier le mot de passe dans un plan de protection existant

1. Dans le plan de protection, développez le module **Protection contre les virus et les malwares** (module **Active Protection** pour l'édition Cyber Backup).
2. Cliquez sur **Autoprotection**.
3. Cliquez sur **Créer un mot de passe**.
4. Dans la fenêtre qui s'ouvre, copiez le mot de passe dont vous avez besoin pour désinstaller ou modifier les composants d'un Agent pour Windows protégé.
   Ce mot de passe est unique et vous ne serez pas en mesure de le récupérer si vous fermez cette fenêtre. Si vous perdez ou oubliez ce mot de passe, vous pouvez modifier le plan de protection et créer un nouveau mot de passe.
5. Cliquez sur **Fermer**.
6. Dans le volet **Autoprotection**, cliquez sur **Terminé**.
7. Enregistrez le plan de protection.

Désinstallation d'agents

Lorsque vous désinstallez un agent d'une ressource, cette ressource est supprimée automatiquement de la console Cyber Protect. Si la ressource reste affichée après que vous avez désinstallé l'agent, en raison d'un problème réseau, par exemple, supprimez cette ressource manuellement de la console. Pour en savoir plus sur la procédure à suivre, reportez-vous à "Suppression de ressources de la console Cyber Protect" (p. 349).

Remarque
La désinstallation d'un agent ne supprime aucun plan ni sauvegarde.

Pour désinstaller un agent

Windows

1. Connectez-vous en tant qu'administrateur à l'ordinateur avec l'agent.
2. Dans le **Panneau de configuration**, accédez à **Programmes et fonctionnalités** (**Ajout ou suppression de programmes** sous Windows XP).
3. Cliquez avec le bouton droit sur **Acronis Cyber Protect**, puis sélectionnez **Désinstaller**.
4. [Pour les agents protégés par mot de passe] Spécifiez le mot de passe dont vous avez besoin pour désinstaller l'agent, puis cliquez sur **Suivant**.
5. [Facultatif] Cochez la case **Supprimer les journaux et les paramètres de configuration**.
   Ne cochez pas cette case si vous prévoyez de réinstaller le produit ultérieurement. Si vous cochez cette case, puis réinstallez l'agent, cette ressource pourrait être dupliquée dans la console Cyber Protect et ses anciennes sauvegardes risqueraient de ne pas lui être associée.
6. Cliquez sur **Désinstaller**.

Linux

1. Sur l'ordinateur avec l'agent, exécutez `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall` en tant qu'utilisateur root.
2. [Facultatif] Cochez la case **Nettoyer toutes traces de produit (supprimer les paramètres de configuration, d'emplacements de stockage, de tâches, de journaux des produits)**.
   Ne cochez pas cette case si vous prévoyez de réinstaller le produit ultérieurement. Si vous cochez cette case, puis réinstallez l'agent, cette ressource pourrait être dupliquée dans la console Cyber Protect et ses anciennes sauvegardes risqueraient de ne pas lui être associée.
3. Confirmez votre choix.

macOS

1. Sur l'ordinateur avec l'agent, double-cliquez sur le fichier .dmg d'installation.
2. Patientez jusqu'à ce que le système d'exploitation monte l'image du disque d'installation.
3. Dans l'image, double-cliquez sur **Désinstaller**.
4. Si vous y êtes invité, fournissez les informations d'identification de l'administrateur.
5. Confirmez votre choix.

Pour désinstaller les composants fournis avec l'agent pour Windows

Vous pouvez désinstaller des composants fournis avec l'agent pour Windows tels que Cyber Protect Monitor, l'agent pour la prévention des pertes de données ou Bootable Media Builder sans désinstaller l'agent pour Windows.

1. Connectez-vous en tant qu'administrateur à l'ordinateur avec l'agent.
2. Exécutez le programme d'installation, puis cliquez sur **Modifier les composants installés**.
3. Désélectionnez les cases situées à côté des composants que vous souhaitez désinstaller, puis cliquez sur **Terminé**.

Pour supprimer l'agent pour VMware (appliance virtuelle)

1. Connectez-vous à vCenter Server à l'aide de vSphere Client.
2. [Si l'appliance virtuelle est sous tension] Cliquez avec le bouton droit sur l'appliance virtuelle, puis cliquez sur **Alimentation** > **Mise hors tension**. Confirmez votre choix.
3. [Si l'appliance virtuelle utilise un stockage attaché localement sur un disque virtuel et que vous souhaitiez conserver les données sur ce disque] Supprimez le stockage virtuel de l'appliance virtuelle.
   a. Cliquez avec le bouton droit de la souris sur l'appliance virtuelle, puis cliquez sur **Modifier les paramètres**.
   b. Sélectionnez le disque avec le stockage, puis cliquez sur **Supprimer**.
   c. Sous **Options de suppression**, cliquez sur **Supprimer de la machine virtuelle**.
   d. Cliquez sur **OK**.

   En conséquence, le disque reste dans la banque de données. Vous pouvez attacher le disque à un autre appliance virtuelle.

4. Cliquez avec le bouton droit de la souris sur l'appliance virtuelle, puis cliquez sur **Supprimer du disque**. Confirmez votre choix.
5. [Facultatif] [Si vous n'envisagez pas de réutiliser cette appliance] Dans la console Cyber Protect, accédez à **Stockage de sauvegarde** > **Emplacements**, puis supprimez l'emplacement correspondant au stockage attaché localement.

Paramètres de protection

Pour configurer les paramètres généraux de protection pour Cyber Protection, accédez depuis la console Cyber Protect à **Paramètres** > **Protection**.

Mises à jour automatiques pour les composants

Par défaut, tous les agents peuvent se connecter à Internet et télécharger les mises à jour.

Un administrateur peut réduire le trafic sur la bande passante réseau en sélectionnant un ou plusieurs agents dans l'environnement et en leur attribuant le rôle Responsable de la mise à jour. Les agents dédiés se connecteront donc à Internet et téléchargeront les mises à jour. Tous les autres agents se connecteront aux agents dédiés responsables de la mise à jour à l'aide d'une technologie de pair à pair, et téléchargeront les mises à jour auprès d'eux.

Les agents ne disposant pas du rôle Responsable de la mise à jour se connecteront à Internet s'il n'y a pas d'autre agent dédié responsable de la mise à jour dans l'environnement, ou si aucune connexion à un tel agent ne peut être établie au bout de cinq minutes.

L'agent responsable de la mise à jour distribue les mises à jour et les correctifs pour la protection antivirus et antimalware, l'évaluation des vulnérabilités et la gestion des correctifs, mais il n'inclut pas les mises à jour de la version de l'agent.

Remarque
Un agent avec le rôle Responsable de la mise à jour ne peut télécharger et distribuer des correctifs que pour les produits tiers Windows. Pour les produits Microsoft, la distribution des correctifs n'est pas prise en charge par l'agent Responsable de la mise à jour.

Avant d'attribuer le rôle Responsable de la mise à jour à un agent, vérifiez que l'ordinateur sur lequel l'agent est exécuté est assez puissant et dispose d'une connexion Internet haute vitesse et d'assez d'espace disque.

Pour préparer un ordinateur pour le rôle Responsable de la mise à jour

1. Sur l'ordinateur agent sur lequel vous prévoyez d'activer le rôle Responsable de la mise à jour, appliquez les règles de pare-feu suivantes :
   - Entrant «updater_incoming_tcp_ports» : autoriser la connexion aux ports TCP 18018 et 6888 pour tous les profils de pare-feu (public, privé et domaine).
   - Entrant «updater_incoming_udp_ports» : autoriser la connexion aux ports UDP 6888 pour tous les profils de pare-feu (public, privé et domaine).

2. Redémarrez Acronis Agent Core Service.
3. Redémarrez le service de pare-feu.

Si vous n'appliquez pas ces règles et que le pare-feu est activé, les autres agents téléchargeront les mises à jour depuis le Cloud.

Attribuer le rôle Responsable de la mise à jour à un agent de protection

1. Dans la console Cyber Protect, accédez à **Paramètres** > **Agents**.
2. Sélectionnez l'ordinateur comportant l'agent auquel vous souhaitez attribuer le rôle Responsable de la mise à jour.
3. Cliquez sur **Détails**, puis activez l'interrupteur **Utilisez cet agent pour télécharger et distribuer des correctifs et des mises à jour**.

La mise à jour de pair à pair fonctionne comme suit.

1. De façon planifiée, l'agent possédant le rôle Responsable de la mise à jour vérifie le fichier d'index mis à disposition par le fournisseur de services afin de mettre à jour les principaux composants.
2. L'agent possédant le rôle Responsable de la mise à jour commence à télécharger et à distribuer les mises à jour à tous les agents.

Vous pouvez attribuer le rôle Responsable de la mise à jour à plusieurs agents dans l'environnement. Ainsi, si un agent avec le rôle Responsable de la mise à jour est hors ligne, d'autres agents possédant ce rôle peuvent servir de source pour les mises à jour des définitions.

Mise à jour des définitions de Cyber Protection de façon planifiée

Dans l'onglet **Planification**, vous pouvez configurer le planning de mise à jour automatique des définitions de Cyber Protection pour chacun des composants suivants :

- Anti-malware
- Évaluation des vulnérabilités
- Gestion des correctifs

Pour modifier le paramètre de mise à jour des définitions, naviguez vers **Paramètres** > **Protection** > **Mise à jour des définitions de protection** > **Planification**.

Type de planification :

- **Par jour** : définissez les jours de la semaine pour la mise à jour des définitions.
  Débuter à : sélectionnez l'heure à laquelle mettre à jour les définitions.
- **Par heure** : définissez un planning horaire plus granulaire pour les mises à jour.
  Exécution chaque : définissez la périodicité des mises à jour.
  À partir de ... **Jusqu'à** : définissez une plage de temps spécifique pour les mises à jour.

Mise à jour des définitions de Cyber Protection à la demande

Pour mettre à jour les définitions de Cyber Protection à la demande, pour un ordinateur en particulier

1. Dans la console Cyber Protect, accédez à **Paramètres** > **Agents**.
2. Sélectionnez les machines sur lesquelles vous souhaitez mettre à jour les définitions de protection, puis cliquez sur **Mettre les définitions à jour**.

Mémoire en cache

L'emplacement des données en cache est le suivant :

- Sur les machines Windows : `C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache`
- Sur les machines Linux : `/opt/acronis/var/atp-downloader/Cache`
- Sur les ordinateurs macOS : `/Library/Application Support/Acronis/Agent/var/atp-downloader/Cache`

Pour modifier le paramètre de stockage du cache, accédez à **Paramètres** > **Protection** > **Mise à jour des définitions de protection** > **Stockage du cache**.

Dans **Fichiers de mise à jour et données de gestion des correctifs obsolètes**, indiquez au bout de combien de temps supprimer les données en cache.

Taille maximum de la mémoire en cache (Go) pour les agents :

- **Rôle Responsable de la mise à jour :** définissez la taille du stockage pour le cache sur les machines ayant le rôle Responsable de la mise à jour.
- **Autres rôles :** définissez la taille du stockage pour le cache sur les autres machines.

Remarque
Cyber Protection collecte des échantillons de malware détectés en vue d'une analyse supplémentaire qui nous permettra d'améliorer notre logiciel. Vous pouvez modifier ce paramètre à tout moment dans l'onglet **Protection**, en désactivant l'option **Collecter et transférer des échantillons de malware vers le CPOC**.

Modification du quota de service des ordinateurs

Un quota de service est affecté automatiquement lorsqu'un plan de protection est appliqué à une machine pour la première fois.

Le quota le plus approprié est attribué, en fonction du type de la machine protégée, de son système d'exploitation, du niveau de protection requis et de la disponibilité du quota. Si le quota le plus approprié n'est pas disponible dans votre organisation, le quota suivant dans la classification est attribué. Par exemple, si le quota le plus approprié est **Serveur d'hébergement Web**, mais n'est pas disponible, le quota **Serveur** est attribué.

Exemples d'affectation de quota :

- Une machine physique qui exécute un serveur Windows ou un système d'exploitation serveur Linux (comme Ubuntu Server) se voit attribuer le quota **Serveur**.
- Une machine physique qui exécute un système d'exploitation Windows ou Linux (comme Ubuntu Desktop) se voit attribuer le quota **Poste de travail**.
- Une machine physique exécutant Windows 10 avec rôle Hyper-V activé reçoit le quota **Poste de travail**.
- Un ordinateur s'exécutant sur une infrastructure de poste de travail virtuel et dont l'agent de protection est installé à l'intérieur du système d'exploitation invité (par exemple, agent pour Windows), reçoit le quota **Machine virtuelle**. Ce type d'ordinateur peut également utiliser le quota **Poste de travail** si le quota **Machine virtuelle** n'est pas disponible.
- Un ordinateur s'exécutant sur une infrastructure de poste de travail virtuel et qui est sauvegardé en mode sans agent (par exemple, par l'agent pour VMware ou pour Hyper-V) reçoit le quota **Machine virtuelle**.
- Un serveur Hyper-V ou vSphere reçoit le quota **Serveur**.
- Un serveur avec cPanel ou Plesk reçoit le quota **Serveur d'hébergement Web**. Si le quota Serveur d'hébergement Web n'est pas disponible, il peut également utiliser le quota **Machine virtuelle** ou **Serveur** selon le type d'ordinateur sur lequel s'exécute le serveur Web.
- La sauvegarde reconnaissant les applications nécessite le quota **Serveur**, même pour un poste de travail.

Vous pourrez modifier manuellement l'attribution originale ultérieurement. Par exemple, pour appliquer un plan de protection plus avancé au même ordinateur, vous devez mettre à niveau le quota de service de l'ordinateur. Si les fonctionnalités requises par ce plan de protection ne sont pas prises en charge par le quota de service actuellement affecté, le plan de protection échouera.

Vous pouvez également modifier le quota de service si vous faites l'acquisition d'un quota plus approprié après l'affectation de celui d'origine. Par exemple, le quota **Poste de travail** est attribué à une machine virtuelle. Après l'achat d'un quota **Machines virtuelles**, vous pouvez l'attribuer manuellement à cet ordinateur à la place du quota **Poste de travail** d'origine.

Vous pouvez également libérer le quota de service attribué, puis l'attribuer à un autre ordinateur.

Vous pouvez modifier le quota de service d'un ordinateur ou d'un groupe d'ordinateurs.

Pour changer le quota de service d'un ordinateur

1. Dans la console Cyber Protect, accédez à **Terminaux**.
2. Sélectionnez la machine souhaitée, puis cliquez sur **Détails**.
3. Dans la section **Quota de service**, cliquez sur **Modifier**.
4. Dans la fenêtre **Modifier le quota**, sélectionnez le quota de service souhaité ou **Aucun quota**, puis cliquez sur **Modifier**.

Pour modifier le quota de service d'un groupe d'ordinateurs

1. Dans la console Cyber Protect, accédez à **Terminaux**.
2. Sélectionnez plusieurs ordinateurs, puis cliquez sur **Attribuer un quota**.
3. Dans la fenêtre **Modifier le quota**, sélectionnez le quota de service souhaité ou **Aucun quota**, puis cliquez sur **Modifier**.

Services Cyber Protection installés dans votre environnement

Cyber Protection installe certains des services suivants, en fonction des options Cyber Protection que vous utilisez.

Services installés sous Windows

Nom du service	Objectif
Acronis Managed Machine Service	Fonctionnalités de sauvegarde, récupération, réplication, rétention, validation
Acronis Scheduler2 Service	Exécute les tâches planifiées pour certains événements
Acronis Active Protection Service	Offre une protection contre les ransomware
Acronis Cyber Protection Service	Offre une protection contre les malwares

Services installés sous macOS

Nom du service et emplacement	Objectif
`/Library/LaunchDaemons/com.acronis.aakore.plist`	Sert à la communication entre l'agent et les composants de gestion
`/Library/LaunchDaemons/com.acronis.cyber-protect-service.plist`	Permet de détecter les malwares
`/Library/LaunchDaemons/com.acronis.mms.plist`	Offre une fonctionnalité de sauvegarde et de restauration
`/Library/LaunchDaemons/com.acronis.schedule.plist`	Exécute les tâches planifiées

Enregistrement d'un journal fichier d'agent

Vous pouvez enregistrer un journal d'agent dans un fichier .zip. Si une sauvegarde échoue pour une raison inconnue, ce fichier aidera le personnel du support technique à identifier le problème.

Par défaut, les informations contenues dans le journal sont optimisées pour les trois derniers jours, mais vous pouvez modifier cette période.

Pour collecter les journaux des agents

1. Effectuez l'une des actions suivantes :
   - Sous **Terminaux**, sélectionnez l'ordinateur dont vous souhaitez collecter les journaux, puis cliquez sur **Activités**.
   - Sous **Paramètres** > **Agents**, sélectionnez l'ordinateur dont vous souhaitez collecter les journaux, puis cliquez sur **Détails**.
2. [Facultatif] Pour modifier la période par défaut pour laquelle les informations système sont incluses, cliquez sur la flèche située à côté du bouton **Collecter les informations système**, puis sélectionnez la période.
3. Cliquez sur **Collecter les informations système**.
4. Si vous y êtes invité par votre navigateur Web, indiquez où enregistrer le fichier.

OpenVPN de site à site – Informations complémentaires

Quand vous créez un serveur de restauration, vous configurez son **adresse IP dans le réseau de production** et son **Adresse IP test**.

Quand vous aurez réalisé le basculement (exécuté la machine virtuelle dans le Cloud), et que vous vous serez connecté à la machine virtuelle pour consulter l'adresse IP du serveur, vous verrez l'**adresse IP dans le réseau de production**.

Quand vous réalisez le basculement test, vous pouvez joindre le serveur de test uniquement en utilisant l'**adresse IP test**, visible uniquement dans la configuration du serveur de restauration.

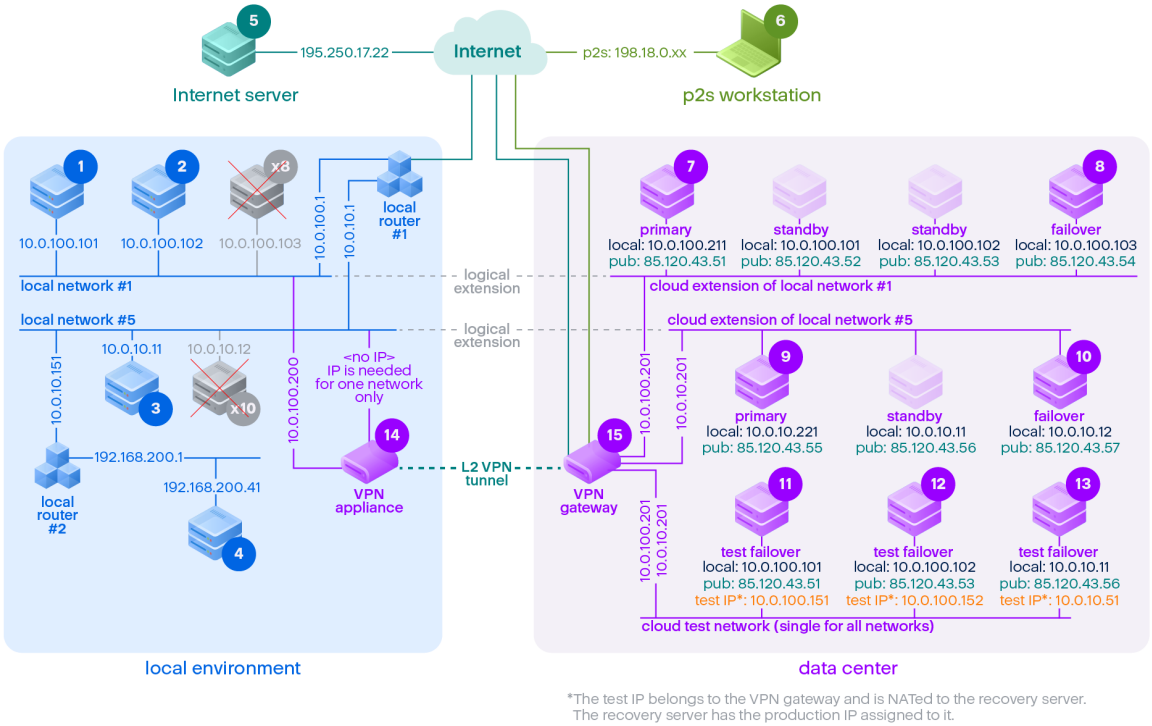
Pour accéder à un serveur de test depuis votre site local, vous devez utiliser l'**adresse IP de test**.

Remarque
La configuration réseau du serveur montre toujours l'**adresse IP dans le réseau de production** (car le serveur de test montre à quoi ressemblerait le serveur de production). En effet, l'adresse IP test n'appartient pas au serveur de test mais à la passerelle VPN, et elle est traduite en adresse IP de production à l'aide d'un NAT.

Le diagramme ci-dessous montre un exemple de configuration Open VPN de site à site. Certains serveurs de l'environnement local sont restaurés dans le Cloud au moyen du basculement (tandis que l'infrastructure réseau est OK).

1. Le client a activé la reprise d'activité après sinistre :
   a. en configurant l'appliance VPN (14) et en la connectant au serveur VPN Cloud dédié (15)
   b. en protégeant certains des serveurs locaux à l'aide de Disaster Recovery (1, 2, 3, x8 et x10)
   Certains serveurs sur le site local (comme le 4) sont connectés à des réseaux qui ne sont pas connectés à l'appliance VPN. Ces serveurs ne sont pas protégés par Disaster Recovery.

2. Une partie des serveurs (connectés à des réseaux différents) fonctionne sur le site local : (1, 2, 3 et 4)
3. Les serveurs protégés (1, 2 et 3) sont testés au moyen d'un basculement test (11, 12 et 13)
4. Certains serveurs sur le site local sont indisponibles (x8, x10). Après le basculement, ils deviennent disponibles dans le Cloud (8 et 10)
5. Certains serveurs primaires (7 et 9), connectés à des réseaux différents, sont disponibles dans l'environnement Cloud
6. Le (5) est un serveur sur Internet avec une adresse IP publique
7. Le (6) est un poste de travail connecté au Cloud à l'aide d'une connexion VPN de point à site (p2s)



Dans cet exemple, la configuration de connexion suivante est disponible (par exemple, « ping ») depuis un serveur de la rangée **De :** vers un serveur de la colonne **À :**.

	À :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
De :		locale	locale	locale	locale	internet	p2s	primaire	basculement	primaire	basculement	basculement test	basculement test	basculement test	application VPN	serveur VPN
1	locale		direct	via routuer	via routuer	via router loc	non	via tunnel : loc	via tunnel : local via	via tunnel : loc	via tunnel : local via	via tunnel : NAT (serv	via tunnel : NAT (serv	via local router 1 et tunn	direct	non

	À :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
				local 1	local 2	al 1 et Internet		al via routerlocal 1 et Internet : pub	router local 1 et Internet : pub	al via routerlocal 1 et Internet : pub	router local 1 et Internet : pub	eur VPN) via router local 1 et Internet : pub	eur VPN) via router local 1 et Internet : pub	el : NAT (serveur VPN) via router local 1 et Internet : pub		
2	locale	direct		via routerlocal 1	via routerlocal 2	via routerlocal 1 et Internet	non	via tunnel : local via routerlocal 1 et Internet : pub	via tunnel : local via router local 1 et Internet : pub	via tunnel : local via routerlocal 1 et Internet : pub	via tunnel : local via router local 1 et Internet : pub	via tunnel : NAT (serveur VPN) via router local 1 et Internet : pub	via tunnel : NAT (serveur VPN) via router local 1 et Internet : pub	via local router 1 et tunnel : NAT (serveur VPN) via router local 1 et Internet : pub	direct	non
3	locale	via routerlocal 1	via routerlocal 1		via routerlocal 2	via routerlocal 1 et Internet	non	via tunnel : local via routerlocal 1	via tunnel : local via router local 1 et Internet : pub	via tunnel : local via routerlocal 1	via tunnel : local via router local 1 et Internet : pub	via tunnel : NAT (serveur VPN) via router local	via tunnel : NAT (serveur VPN) via router local	via local router 1 et tunnel : NAT (serveur VPN) via	via routerlocal	non

	À :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								et Internet : pub		et Internet : pub		1 et Internet : pub	1 et Internet : pub	routeur local 1 et Internet : pub		
4	locale	via routeur local 2 et routeur 1	via routeur local 2 et routeur 1	via routeur local 2		via routeur local 2, routeur 1 et Internet	non	via routeur local 2 et tunnel : local via routeur local 2, routeur local 1 et Internet : pub	via routeur local 2 et tunnel : local via routeur local 2, routeur local 1 et Internet : pub	via routeur local 2 et tunnel : local via routeur local 2, routeur local 1 et Internet : pub	via routeur local 2 et tunnel : local via routeur local 2, routeur local 1 et Internet : pub	via tunnel : NAT (serveur VPN) via routeur local 2, routeur 1 et Internet : pub	via tunnel : NAT (serveur VPN) via routeur local 2, routeur 1 et Internet : pub	via tunnel : NAT (serveur VPN) via routeur local 2, routeur 1 et Internet : pub	via routeur local 2	non
5	internet	non	non	non	non		N/D	via Internet : pub	via Internet : pub	via Internet : pub	via Internet : pub	via Internet : pub	via Internet : pub	via Internet : pub	non	non
6	p2s	non	non	non	non	via Internet		via VPN p2s (ser	via VPN p2s (serveur	via VPN p2s (ser	via VPN p2s (serveur	via VPN p2s – NAT (serv	via VPN p2s – NAT (serv	via VPN p2s – NAT (serv	non	non

	À :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								veur VPN) : local via Internet : pub	VPN) : local via Internet : pub	veur VPN) : local via Internet : pub	VPN) : local via Internet : pub	eur VPN) via Internet : pub	eur VPN) via Internet : pub	eur VPN) via Internet : pub		
7	primaire	via tunnel	via tunnel	via tunnel et routerlocal 1	via tunnel et routerlocal 1 et 2	via Internet (via serveur VPN)	non		direct dans le Cloud : local	via tunnel et routerlocal 1 : local	via tunnel et routerlocal 1 : local	via serveur VPN : NAT	via serveur VPN : NAT	via tunnel et routerlocal 1 : NAT	non	Protocoles DHCP et DNS seulement
8	basculement	via tunnel	via tunnel	via tunnel et routerlocal 1	via tunnel et routerlocal 1 et 2	via Internet (via serveur VPN)	non	direct dans le Cloud : local		via tunnel et routerlocal 1 : local	via tunnel et routerlocal 1 : local	via serveur VPN : NAT	via serveur VPN : NAT	via tunnel et routerlocal 1 : NAT	non	Protocoles DHCP et DNS seulement
9	primaire	via tu	via tu	via tunn	via tunn	via Internet	non	via tunnel	via tunnel et route		direct dans le Clou	via tunnel et route	via tunnel et route	via serveur VPN :	non	Protocoles DHC

	À :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		nnel et routerlocal 1	nnel et routerlocal 1	el	el	(via serveur VPN)		et routerlocal 1 : local	r local 1 : local		d : local	r local 1 : NAT	r local 1 : NAT	NAT		P et DNS seulement
10	basculement	via tunnel et routerlocal 1	via tunnel et routerlocal 1	via tunnel	via tunnel	via Internet (via serveur VPN)	non	via tunnel et routerlocal 1 : local	via tunnel et router local 1 : local	direct dans le Cloud : local		via tunnel et router local 1 : NAT	via tunnel et router local 1 : NAT	via serveur VPN : NAT	non	Protocoles DHCP et DNS seulement
11	basculement test	non	non	non	non	via Internet (via serveur VPN)	non	non	non	non	non		direct dans le Cloud : local	via serveur VPN : local (routage)	non	Protocoles DHCP et DNS seulement
12	basculement test	non	non	non	non	via Internet (via serveur VPN)	non	non	non	non	non	direct dans le Cloud : local		via serveur VPN : local (routage)	non	Protocoles DHCP et DNS seulement
13	basculem	non	non	non	non	via	no	non	non	non	non	via	via		non	Prot

	À :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	ent test					Internet (via serveur VPN)	n					serveur VPN : local (routage)	serveur VPN : local (routage)			ocoles DHCP et DNS seulement
14	application VPN	direct	direct	via routerlocal1	via routerlocal2	via Internet (routeur local 1)	non	non	non	non	non	non	non	non		non
15	serveur VPN	non	non	non	non	non	non	non	non	non	non	non	non	non	non	

Gestion des licences pour les serveurs de gestion sur site

Pour des informations détaillées sur la façon d'activer un serveur de gestion sur site ou d'y allouer des licences, reportez-vous dans la section Licences du Guide de l'utilisateur Cyber Protect.

Définition de la méthode de protection et des éléments à protéger

Onglet Gestion

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Tous les plans que vous avez créés sont disponibles dans l'onglet **Gestion** de la console Cyber Protect.

Les sections suivantes sont disponibles :

- **Plans de protection**
- **Plans de gestion à distance**
- **Plans de création de scripts**
- **Plans de surveillance**
- **Référentiel de scripts**
- **Sauvegarde d'applications dans le Cloud**
- **Analyse de la sauvegarde**
- **Réplication de sauvegarde**
- **Validation**
- **Nettoyage**
- **Conversion en MV**
- **Réplication de MV**

Statuts du plan

Pour les plans de protection et de réplication de machines virtuelles, une barre d'état affiche les statuts suivants selon un code couleur :

- OK (verte)
- Avertissement (orange)
- Erreur (orange foncé)
- Critique (rouge)
- Le plan est en cours d'exécution (bleu)
- Le plan est désactivé (gris)

Cliquez sur la barre d'état pour obtenir des détails sur les statuts du plan pour toutes les ressources auxquelles le plan est appliqué.

Cliquez sur un statut spécifique pour afficher la liste de toutes les ressources ayant ce statut.

Plans de protection

Dans l'onglet **Gestion** > **Plans de protection**, vous pouvez voir les informations concernant vos plans de protection existants, effectuer des opérations à l'aide de ces plans et créer de nouveaux plans.

Pour plus d'informations sur les plans de protection, reportez-vous à "Plans et modules de protection" (p. 222).

Plans de sauvegarde pour les applications dans le Cloud

L'onglet **Gestion** > **Sauvegarde d'applications dans le Cloud** affiche les plans de sauvegarde cloud à cloud. Ces plans sauvegardent les applications qui s'exécutent au moyen d'agents qui s'exécutent eux-mêmes dans le Cloud, et utilisent l'espace de stockage dans le Cloud en tant qu'emplacement de sauvegarde.

Dans cette section, vous pouvez exécuter les opérations suivantes :

- Créer, afficher, exécuter, stopper, modifier et supprimer un plan de sauvegarde
- Afficher les activités associées à chaque plan de sauvegarde
- Afficher les alertes associées à chaque plan de sauvegarde

Pour en savoir plus sur la sauvegarde d'applications Cloud, consultez les sections suivantes :

- Protection des données Microsoft 365
- Protection des données Google Workspace

Exécution manuelle de sauvegardes de Cloud à Cloud

Pour éviter l'interruption du service Cyber Protection, le nombre d'exécutions de sauvegardes Cloud à Cloud est limité à 10 par heure et par organisation Microsoft 365 ou Google Workspace. Après avoir atteint ce nombre, le nombre d'exécutions autorisé est réinitialisé à un par heure, puis une exécution supplémentaire est alors disponible chaque heure par la suite (par exemple heure 1, 10 exécutions ; heure 2, 1 exécution ; heure 3, 2 exécutions) jusqu'à ce qu'un total de 10 exécutions par heure soit atteint.

Les plans de sauvegarde appliqués aux groupes de terminaux (boîtes aux lettres, Drive, sites) ou contenant plus de 10 terminaux ne peuvent pas être exécutés manuellement.

Plan d'analyse des sauvegardes

Pour analyser des sauvegardes à la recherche de malwares (y compris les ransomware), créez un plan d'analyse de sauvegarde.

Important
Les plans d'analyse des sauvegardes ne sont pas pris en charge pour tous les stockages des sauvegardes et les ressources. Pour plus d'informations, veuillez consulter l'article "Limites" (p. 910).

Créer un plan d'analyse de sauvegarde

1. Dans la console Cyber Protect, accédez à **Gestion** > **Analyse de la sauvegarde**.
2. Cliquez sur **Création d'un plan**.
3. Spécifiez le nom du plan, ainsi que les paramètres suivants :
   - **Type d'analyse** :
     - **Cloud** : cette option ne peut pas être modifiée. Un agent cloud sélectionné automatiquement effectue l'analyse de la sauvegarde.
   - **Sauvegardes vers l'analyse** :
     - **Emplacements** : sélectionnez les emplacements des ensembles de sauvegardes que vous souhaitez analyser.
     - **Sauvegardes** : sélectionnez les ensembles de sauvegardes que vous souhaitez analyser.
   - **Analyser** :
     - **Malware** : cette option ne peut pas être modifiée. L'analyse vérifie les ensembles de sauvegardes sélectionnés à la recherche de malware (y compris les ransomware).
   - **Chiffrement** : pour analyser des ensembles de sauvegardes chiffrés, indiquez le mot de passe de chiffrement. Si vous sélectionnez un emplacement ou plusieurs ensembles de sauvegardes, et que le mot de passe spécifié ne correspond à aucun ensemble de sauvegardes, une alerte est créée.
   - **Planification** : cette option ne peut pas être modifiée. Dans le stockage dans le cloud, l'analyse démarre automatiquement.
4. Cliquez sur **Créer**.

En conséquence, un plan d'analyse de la sauvegarde est créé et un agent dans le cloud recherche les malware dans les emplacements ou les ensembles de sauvegardes que vous avez indiqués.

Traitement des données hors hôte

Remarque
Cette fonctionnalité est disponible pour les tenants clients pour lesquels le quota **Advanced Backup - Serveurs** ou **Advanced Backup - NAS** est activé dans le cadre du pack Advanced Backup.

La réplication, la validation et le nettoyage sont généralement effectués par l'agent de protection qui effectue la sauvegarde. Cela représente une charge supplémentaire pour l'ordinateur sur lequel l'agent s'exécute, même après la fin du processus de sauvegarde. Pour décharger l'ordinateur, vous

pouvez créer des plans de protection des données hors hôte, c'est-à-dire des plans distincts pour la réplication, la validation, le nettoyage et la conversion en machine virtuelle.

Les plans de protection des données hors hôte permettent d'effectuer les opérations suivantes :

- Choisir des agents différents pour les opérations de sauvegarde et de protection des données hors hôte
- Programmez les opérations de traitement des données hors hôte pendant les heures creuses afin de minimiser la consommation de la bande passante du réseau.
- Si vous ne souhaitez pas installer un agent dédié au traitement des données hors hôte, planifiez les opérations de traitement des données hors hôte en dehors des heures de bureau.

Remarque
Les plans de traitement des données hors hôte s'exécutent en fonction des paramètres temporels (y compris le fuseau horaire) de l'ordinateur sur lequel l'agent de protection est installé. Pour une appliance virtuelle (par exemple, Agent for VMware ou Agent for Scale Computing HC3), vous pouvez configurer le fuseau horaire dans l'interface utilisateur graphique de l'agent.

Réplication de sauvegarde

Remarque
Cette fonctionnalité est disponible pour les tenants clients pour lesquels le quota **Advanced Backup - Serveurs** ou **Advanced Backup - NAS** est activé dans le cadre du pack Advanced Backup.

La réplication de sauvegarde copie une sauvegarde vers un autre emplacement. En tant qu'opération de traitement des données hors hôte, elle est configurée dans un plan de réplication de sauvegarde.

La réplication de sauvegarde peut également faire partie d'un plan de protection. Pour plus d'informations sur cette option, reportez-vous à "Réplication" (p. 460).

Création d'un plan de réplication de sauvegarde

Pour répliquer les sauvegardes en tant qu'opération de traitement des données hors hôte, vous créez un plan de réplication des sauvegardes.

Pour créer un plan de réplication de sauvegarde

1. Dans la console Cyber Protect, cliquez sur **Gestion** > **Réplication des sauvegardes**.
2. Cliquez sur **Création d'un plan**.
3. Dans **Agent**, sélectionnez l'agent qui effectuera la réplication.
   Vous pouvez sélectionner n'importe quel agent ayant accès à la fois à l'emplacement source et aux emplacements de réplication.
4. Dans **Éléments à répliquer**, sélectionnez les archives ou les emplacements de sauvegarde à répliquer.

Pour naviguer entre les archives et les emplacements, utilisez le commutateur **Emplacements** / **Sauvegardes** dans le coin supérieur droit.

Si vous sélectionnez plusieurs archives chiffrées, leur mot de passe de cryptage doit être identique. Pour les archives qui utilisent des mots de passe de cryptage différents, créez des plans distincts.

5. Dans **Destination**, indiquez l'emplacement de réplication.
6. Dans **Comment répliquer**, sélectionnez les sauvegardes (également appelées points de restauration) à répliquer.

   Les options suivantes sont disponibles :

   - **Toutes les sauvegardes**
   - **Sauvegardes complètes uniquement**
   - **Dernière sauvegarde uniquement**

   Pour plus d'informations sur ces options, reportez-vous à "Que répliquer" (p. 207).
7. Dans **Planification**, configurez la planification de réplication.

   Lors de la configuration de la planification de la réplication des sauvegardes, assurez-vous que la dernière sauvegarde répliquée sera toujours disponible à son emplacement d'origine lorsque la réplication des sauvegardes commencera. Si cette sauvegarde n'est pas disponible à l'emplacement d'origine, par exemple parce qu'elle a été supprimée par une règle de conservation, l'archive entière sera répliquée en tant que sauvegarde complète. Cela peut prendre beaucoup de temps et utiliser de l'espace de stockage supplémentaire.
8. Dans **Règles de rétention**, spécifiez les règles de rétention pour l'emplacement cible.

   Les options suivantes sont disponibles :

   - **Par nombre de sauvegardes**
   - **Par âge des sauvegardes** (paramètres distincts pour les sauvegardes mensuelles, hebdomadaires, quotidiennes et horaires)
   - **Par volume total de sauvegardes**
   - **Conserver les sauvegardes indéfiniment**

   Remarque
   La sélection de cette option entraînera une augmentation de l'utilisation de l'espace de stockage. Vous devez supprimer manuellement les sauvegardes inutiles.
9. [Si vous avez sélectionné des archives cryptées dans les **Éléments à répliquer**] Activez le commutateur **Mot de passe de sauvegarde**, puis fournissez le mot de passe de chiffrement.
10. [Facultatif] Pour modifier les options du plan, cliquez sur l'icône engrenage, puis configurez les options selon vos besoins.
11. Cliquez sur **Créer**.

Que répliquer

Remarque
Certaines opérations de réplication telles que la réplication d'un emplacement complet ou la réplication de toutes les sauvegardes d'un ensemble de sauvegardes peuvent être longues.

Vous pouvez répliquer des ensembles de sauvegardes ou des emplacements de sauvegarde complets. Lorsque vous répliquez un emplacement de sauvegarde, tous les ensembles de sauvegardes sont répliqués.

Les ensembles de sauvegardes sont composés de sauvegardes (appelés également points de reprise). Vous devez sélectionner les sauvegardes à répliquer.

Les options suivantes sont disponibles :

- **Toutes les sauvegardes**
  Toutes les sauvegardes de l'ensemble de sauvegardes sont répliquées à chaque exécution d'un plan de réplication.
- **Sauvegardes complètes uniquement**
  Seules les sauvegardes complètes de l'ensemble de sauvegardes sont répliquées.
- **Dernière sauvegarde uniquement**
  Seule la dernière sauvegarde de l'ensemble est répliquée, quel que soit son type (complète, différentielle ou incrémentielle).

Sélectionnez une option adaptée à vos besoins, ainsi que le modèle de sauvegarde que vous utilisez. Par exemple, si vous utilisez le modèle de sauvegarde **Toujours incrémentielle (fichier unique)** et souhaitez répliquer uniquement la dernière sauvegarde incrémentielle, sélectionnez **Dernière sauvegarde uniquement** dans le plan de réplication de sauvegarde.

Le tableau suivant récapitule les sauvegardes qui seront répliquées en fonction des différents modèles de sauvegarde.

	Toujours incrémentielle (fichier unique)	**Toujours complète**	**Complète hebdomadaire, incrémentielle journalière**	**Complète mensuelle, différentielle hebdomadaire, incrémentielle journalière (GFS)**
Toutes les sauvegardes	Toutes les sauvegardes de l'ensemble de sauvegarde	Toutes les sauvegardes de l'ensemble de sauvegarde	Toutes les sauvegardes de l'ensemble de sauvegarde	Toutes les sauvegardes de l'ensemble de sauvegarde
Sauvegardes complètes uniquement	Uniquement la première sauvegarde	Toutes les sauvegardes	Une sauvegarde par semaine*	Une sauvegarde par mois*

	Toujours incrémentielle (fichier unique)	Toujours complète	Complète hebdomadaire, incrémentielle journalière	Complète mensuelle, différentielle hebdomadaire, incrémentielle journalière (GFS)
	complète			
Dernière sauvegarde uniquement	La dernière sauvegarde de l'ensemble de sauvegardes uniquement*	La dernière sauvegarde de l'ensemble de sauvegardes uniquement*	La dernière sauvegarde de l'ensemble de sauvegardes uniquement, quel que soit son type*	La dernière sauvegarde de l'ensemble de sauvegardes uniquement, quel que soit son type*

*Lors de la configuration de la planification de la réplication des sauvegardes, assurez-vous que la dernière sauvegarde répliquée sera toujours disponible à son emplacement d'origine lorsque la réplication des sauvegardes commencera. Si cette sauvegarde n'est pas disponible à l'emplacement d'origine, par exemple parce qu'elle a été supprimée par une règle de conservation, l'archive entière sera répliquée en tant que sauvegarde complète. Cela peut prendre beaucoup de temps et utiliser de l'espace de stockage supplémentaire.

Emplacements pris en charge

Le tableau suivant récapitule les emplacements de sauvegarde pris en charge par les plans de réplication de sauvegarde.

Emplacement de sauvegarde	Pris en charge comme source	Pris en charge comme cible
Stockage dans le Cloud	+	+
Dossier local	+	+
Dossier réseau	+	+
Cloud public	+	+
Dossier NFS	–	–
Secure Zone	–	–

Validation

Remarque
Cette fonctionnalité est disponible pour les tenants clients pour lesquels le quota **Advanced Backup - Serveurs** ou **Advanced Backup - NAS** est activé dans le cadre du pack Advanced Backup.

En validant une sauvegarde, vous vérifiez que vous pouvez en restaurer les données.

Pour valider une sauvegarde en tant qu'opération de traitement des données hors hôte, vous pouvez créer un plan de validation. Pour plus d'informations sur cette création, reportez-vous à "Création d'un plan de validation" (p. 210).

Les méthodes de validation suivantes sont disponibles :

- Vérification de la somme de contrôle
- Exécuter en tant que machine virtuelle
  - Pouls de la MV
  - Validation de l'instantané

Vous pouvez sélectionner une ou plusieurs de ces méthodes. Lorsque plusieurs méthodes sont sélectionnées, les opérations pour chaque méthode de validation s'exécutent de manière consécutive. Pour en savoir plus sur les méthodes, reportez-vous à "Pouls de la MV" (p. 213).

Vous pouvez valider les ensembles de sauvegarde ou les emplacements de sauvegarde. La validation d'un emplacement de sauvegarde valide tous les ensembles de sauvegardes qu'il contient.

Emplacements pris en charge

Le tableau suivant répertorie les méthodes de validation et les emplacements de sauvegarde pris en charge.

Remarque
L'option de validation n'est pas disponible pour les sauvegardes dans le cloud public en raison des coûts prohibitifs de lecture d'une archive complète depuis un cloud public.

Emplacement de sauvegarde	Vérification de la somme de contrôle	Exécuter en tant que machine virtuelle	
		Pouls de la MV	Validation de l'instantané
Stockage dans le Cloud	+	+	+
Dossier local	+	+	+
Dossier réseau	+	+	+
Dossier NFS	–	–	–
Secure Zone	–	–	–

Statut de validation

Lorsqu'une validation est réussie, la sauvegarde est marquée d'un point vert et le libellé indique **Validé**.

Si la validation échoue, la sauvegarde est marquée d'un point rouge. La validation échoue même lorsqu'une seule des méthodes de validation utilisées échoue. Dans certains cas, cela peut être le résultat d'une erreur de configuration du plan de validation, par exemple l'utilisation de la méthode **Pouls de la MV** pour les machines virtuelles sur un hôte erroné.

Le statut de validation d'une sauvegarde est mis à jour avec chaque nouvelle opération de validation. Le statut de chaque méthode de validation est mis à jour séparément. C'est la raison pour laquelle la validation d'une sauvegarde dans laquelle une méthode a échoué est indiquée comme ayant échoué jusqu'à ce que la même méthode de validation réussisse, même si les dernières opérations de validation n'utilisent pas la méthode ayant échoué et se terminent avec succès.

Pour plus d'informations sur la vérification du statut de validation, reportez-vous à "Vérification du statut de validation d'une sauvegarde" (p. 216).

Création d'un plan de validation

Pour valider un ensemble de sauvegardes en tant qu'opération de traitement des données hors hôte, créez un plan de validation.

Pour créer un plan de validation

1. Dans la console Cyber Protect, cliquez sur **Gestion** > **Validation**.
2. Cliquez sur **Création d'un plan**.
   Le modèle de nouveau plan de validation s'ouvre.
3. [Facultatif] Pour modifier le nom du plan, cliquez sur le nom par défaut.
4. Dans **Agent**, sélectionnez l'agent qui exécutera la validation, puis cliquez sur **OK**.
   Si vous souhaitez effectuer une validation en exécutant une machine virtuelle depuis une sauvegarde, sélectionnez un ordinateur avec agent pour VMware ou agent pour Hyper-V. Sinon, sélectionnez n'importe quel ordinateur ayant accès à l'emplacement de sauvegarde.
5. Dans **Éléments à valider**, sélectionnez les ensembles de sauvegardes que vous souhaitez valider.
   a. Sélectionnez le champ d'application du plan (ensembles de sauvegardes ou emplacements complets) en cliquant sur **Emplacements** ou **Sauvegardes** en haut à droite.
      Si les sauvegardes sélectionnées sont chiffrées, elles doivent toutes utiliser le même mot de passe de chiffrement. Pour les sauvegardes qui utilisent différents mots de passe de chiffrement, créez des plans séparés.
   b. Cliquez sur **Ajouter**.
   c. Selon le champ d'application du plan de validation, sélectionnez des emplacements, ou un emplacement et des ensembles de sauvegardes, puis cliquez sur **Terminé**.
   d. Cliquez sur **Valider**.

6. Dans **Que valider**, sélectionnez les sauvegardes (connues également sous le nom de points de reprise) dans les ensembles de sauvegarde sélectionnés à valider. Les options suivantes sont disponibles :
   - **Toutes les sauvegardes**
   - **Dernière sauvegarde uniquement**
7. Dans **Comment valider**, sélectionnez la méthode de validation.
   Vous pouvez sélectionner une des options suivantes, ou les deux :
   - **Vérification de la somme de contrôle**
   - **Exécuter en tant que machine virtuelle**

   Pour en savoir plus sur les méthodes, reportez-vous à "Pouls de la MV" (p. 213).
8. [Si vous avez sélectionné **Vérification de la somme de contrôle**] Cliquez sur **Terminé**.
9. [Si vous avez sélectionné **Exécuter en tant que machine virtuelle**]. Configurez les paramètres de cette méthode.
   a. Dans **Machine cible**, sélectionnez le type de machine virtuelle (ESXi ou Hyper-V), l'hôte et le modèle de nom de l'ordinateur, puis cliquez sur **OK**.
      Par défaut, le nom est **[Nom de la Machine]_validate**.
   b. Dans **Magasin de données** (pour ESXi) ou **Chemin d'accès** (pour Hyper-V), sélectionnez le magasin de données pour la machine virtuelle.
   c. Sélectionnez l'une des méthodes de validation fournies par **Exécuter en tant que machine virtuelle**, ou les deux :
      - **Pouls de la MV**
      - **Validation de l'instantané**
   d. [Facultatif] Cliquez sur **Paramètres de MV** pour modifier la taille de la mémoire et les connexions réseau de la machine virtuelle.
      Par défaut, la machine virtuelle n'est pas connectée à un réseau et la taille de la mémoire de la machine virtuelle est équivalente à celle de la machine d'origine.
   e. Cliquez sur **Valider**.
10. [Facultatif] Dans le modèle de plan de validation, cliquez sur **Planification**, puis configurez-le.
11. [Si les ensembles de sauvegardes sélectionnés dans **Éléments à valider** sont chiffrés] Activez l'option **Mot de passe de la sauvegarde**, puis indiquez le mot de passe de chiffrement.
12. [Facultatif] Pour modifier les options du plan, cliquez sur l'icône en forme d'engrenage.
13. Cliquez sur **Créer**.

En conséquence, votre plan de validation est prêt et s'exécutera conformément à la planification que vous avez configurée. Pour exécuter le plan immédiatement, sélectionnez-le dans **Gestion** > **Validation**, puis cliquez sur **Exécuter maintenant**.

Une fois le plan démarré, vous pouvez vérifier les activités en cours et en explorer les détails dans la console Cyber Protect, dans **Surveillance** > **Activités**.

Un plan de validation peut inclure de nombreuses sauvegardes et une sauvegarde peut être validée par de nombreux plans de validation.

Remarque
Toutes les sauvegardes sont traitées séquentiellement, une par une, par une seule tâche de validation.

Une seule tâche de validation à la fois peut être exécutée sur un agent donné. Plusieurs tâches de validation peuvent être exécutées en parallèle si elles sont exécutées par différents agents : deux tâches simultanées nécessitent deux agents, trois tâches requièrent trois agents, etc.

Le tableau suivant résume les statuts possibles de l'activité de validation.

Résultat de l'activité	Plan avec une sauvegarde	Plan avec plusieurs sauvegardes
Réussi	Toutes les méthodes de validation ont réussi	Toutes les méthodes de validation ont réussi dans toutes les sauvegardes
Succès avec avertissements	Sans Objet	Une méthode de validation au moins a échoué dans au moins une sauvegarde
Faire échouer	Une méthode de validation au moins a échoué	Une méthode de validation au moins a échoué dans toutes les sauvegardes

Méthodes de validation

Dans un plan de validation, les méthodes de validation suivantes sont disponibles :

- Vérification de la somme de contrôle
- Exécuter en tant que machine virtuelle
  - Pouls de la MV
  - Validation de l'instantané

Vérification de la somme de contrôle

La validation via la vérification de la somme de contrôle calcule une somme de contrôle pour chaque bloc de données restauré depuis la sauvegarde, puis la compare à la somme de contrôle d'origine pour ce bloc de données qui a été écrite pendant la sauvegarde. La seule exception est la validation des sauvegardes de niveau fichier se trouvant dans le stockage sur le Cloud. Ces sauvegardes sont validées en vérifiant la cohérence des métadonnées enregistrées dans la sauvegarde.

La validation par vérification de la somme de contrôle est un processus très long, même pour les petites sauvegardes incrémentielles ou différentielles. Cela s'explique par le fait que l'opération de validation vérifie non seulement les données contenues physiquement dans une sauvegarde spécifique, mais également toutes les données qui doivent être restaurées, ce qui peut nécessiter la validation des sauvegardes précédentes.

Une validation réussie par vérification de la somme de contrôle indique une forte probabilité de restauration de données. Toutefois, la validation par cette méthode ne vérifie pas tous les facteurs qui influencent le processus de reprise.

Si vous sauvegardez un système d'exploitation, nous vous recommandons d'utiliser certaines des opérations supplémentaires suivantes :

- Testez la reprise du support de démarrage vers un disque dur de secours.
- Exécution d'une machine virtuelle à partir de la sauvegarde dans un environnement ESXi ou Hyper-V.
- Exécution d'un plan de validation dans lequel la méthode de validation **Exécuter en tant que machine virtuelle** est activée.

Exécuter en tant que machine virtuelle

Cette méthode fonctionne uniquement pour les sauvegardes de niveau disque contenant un système d'exploitation. Pour l'utiliser, vous avez besoin d'un hôte ESXi ou Hyper-V et d'un agent de protection (agent pour VMware ou agent pour Hyper-V) qui gère cet hôte.

La méthode de validation **Exécuter en tant que machine virtuelle** est disponible dans les variantes suivantes :

- Pouls de la MV
- Validation de l'instantané

Vous devez sélectionner au moins l'une d'elles.

Pouls de la MV

Avec cette méthode de validation, l'agent exécute une machine virtuelle à partir de la sauvegarde, la connecte à des services d'intégration VMware Tools ou Hyper-V, puis vérifie la réponse de pouls afin de garantir que le système d'exploitation a démarré avec succès. Si la connexion échoue, l'agent essaie de se connecter toutes les deux minutes pour un total de cinq tentatives. Si aucune des tentatives n'est fructueuse, la validation échoue.

Quel que soit le nombre de plans de validation et de sauvegardes validées, l'agent qui effectue la validation exécute une seule machine virtuelle à la fois. Dès que le résultat de la validation est tangible, l'agent supprime la machine virtuelle et exécute la suivante.

Remarque
Utilisez cette méthode uniquement lorsque vous validez des sauvegardes de machines virtuelles VMware en exécutant ces sauvegardes sous forme de machines virtuelles sur un hôte ESXi, ainsi que des sauvegardes de machines virtuelles Hyper-V en les exécutant sous forme de machines virtuelles sur un hôte Hyper-V.

Validation de l'instantané

Grâce à cette méthode de validation, l'agent exécute une machine virtuelle depuis la sauvegarde et effectue des instantanés pendant le démarrage de la machine virtuelle. Un module d'intelligence artificielle vérifie les instantanés et, si l'un deux représente un écran de connexion, il marque la sauvegarde comme étant validée.

L'instantané est associé au point de reprise et vous pouvez télécharger ce point de reprise dans la console Cyber Protect dans l'année qui suit la validation. Pour plus informations sur la vérification de l'instantané, reportez-vous à "Vérification du statut de validation d'une sauvegarde" (p. 216).

Si les notifications sont activées pour votre compte utilisateur, vous recevrez un e-mail concernant le statut de validation de la sauvegarde à laquelle l'instantané est associé. Pour plus d'informations sur les notifications, reportez-vous à Modification des paramètres de notification pour un utilisateur.

La validation d'instantané est prise en charge par l'agent des versions 15.0.30971 (sortie en novembre 2022) et ultérieures.

Remarque
La validation d'instantané est plus efficace avec les sauvegardes de systèmes Windows et Linux avec écran de connexion basé sur l'interface utilisateur graphique. Cette méthode n'est pas optimisée pour les systèmes LINUX avec écran de connexion à la console.

Modification du délai d'expiration de la validation du pouls et des captures d'écran d'une machine virtuelle

Lorsque vous validez une sauvegarde en l'exécutant en tant que machine virtuelle, vous pouvez configurer le délai d'expiration entre le démarrage de la machine virtuelle, et l'envoi de la demande de pouls ou la création d'une capture d'écran.

La période par défaut est la suivante :

- Une minute : pour les sauvegardes stockées dans un dossier local ou un partage réseau
- Cinq minutes : pour les sauvegardes stockées dans le cloud

Vous pouvez changer ce paramétrage en modifiant le fichier de configuration de l'agent pour VMware ou pour Hyper-V.

Pour modifier le délai d'expiration

1. Ouvrez le fichier de configuration pour le modifier. Vous pouvez trouver le fichier dans les emplacements suivants :
   - Pour l'agent pour VMware ou pour Hyper-V s'exécutant sous Windows : `C:\Program Files\BackupClient\BackupAndRecovery\settings.config`
   - Pour l'agent pour VMware (appliance virtuelle) : `/bin/mms_settings.config`

Pour plus d'informations sur l'accès au fichier de configuration sur une appliance virtuelle, voir "Connexions SSH à une appliance virtuelle" (p. 180).

2. Accédez à `<validation>`, puis modifiez les valeurs des sauvegardes locales et dans le cloud en fonction des besoins :

```
<validation>
<run_vm>
<initial_timeout_minutes>
<local_backups>1</local_backups>
<cloud_backups>5</cloud_backups>
</initial_timeout_minutes>
</run_vm>
</validation>
```

3. Enregistrez le fichier de configuration.
4. Redémarrez l'agent.
   - [Pour l'agent pour VMware ou pour Hyper-V s'exécutant sous Windows] Exécutez les commandes suivantes à l'invite de commandes :

     ```
     net stop mms
     ```

     ```
     net start mms
     ```

   - [Pour l'agent pour VMware (appliance virtuelle)] Redémarrez la machine virtuelle avec l'agent.

Configuration du nombre de nouvelles tentatives en cas d'erreur

Pour maximiser le nombre de validations réussies, vous pouvez configurer de nouvelles tentatives automatiques pour les validations qui aboutissent à une erreur.

Pour configurer des nouvelles tentatives automatiques

1. Lors de la création d'un plan de validation, cliquez sur l'icône en forme d'engrenage.
2. Dans le panneau **Options**, sélectionnez **Gestion erreurs**.
3. Dans **Réessayer si une erreur se produit**, cliquez sur **Oui**.
4. Dans **Nombre de tentatives**, configurez le nombre maximal de nouvelles tentatives en cas d'erreur.

   L'opération de validation est alors réexécutée jusqu'à ce qu'elle aboutisse sans erreur ou que le nombre maximal de nouvelles tentatives soit atteint.
5. Dans **Intervalle entre les tentatives**, configurez le délai entre deux nouvelles tentatives consécutives.
6. Cliquez sur **Valider**.

Vérification du statut de validation d'une sauvegarde

Vous pouvez vérifier le statut de validation d'une sauvegarde dans l'onglet **Terminaux** ou **Stockage de sauvegarde**.

Vous pouvez également voir le statut de chaque méthode de validation et télécharger la capture d'écran créée à l'aide de la méthode de validation de capture d'écran.

Pour plus d'informations sur le fonctionnement des statuts, reportez-vous à "Statut de validation" (p. 209).

Pour vérifier le statut de validation d'une sauvegarde

Terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez la ressource dont vous souhaitez vérifier le statut de validation de la sauvegarde, puis cliquez sur **Reprise**.
3. [Si plusieurs emplacements de sauvegarde sont disponibles] Sélectionnez l'emplacement de sauvegarde.
4. Sélectionnez la sauvegarde dont vous souhaitez vérifier le statut.

Stockage de sauvegarde

1. Sur la console Cyber Protect, accédez à **Stockage de sauvegarde**.
2. Sélectionnez l'emplacement de stockage de votre ensemble de sauvegardes.
3. Sélectionnez l'ensemble de sauvegardes, puis cliquez sur **Afficher les sauvegardes**.
4. Sélectionnez la sauvegarde dont vous souhaitez vérifier le statut de validation.

Nettoyage

Le nettoyage est une opération qui supprime les sauvegardes obsolètes conformément aux règles de conservation. Cette opération ne s'applique qu'aux agents et aux ressources, et non aux sauvegardes cloud à cloud (qui ne peuvent être supprimées que manuellement).

Remarque
Cette fonctionnalité est disponible pour les tenants clients pour lesquels le quota **Advanced Backup - Serveurs** ou **Advanced Backup - NAS** est activé dans le cadre du pack Advanced Backup.

Emplacements pris en charge

Les plans de nettoyage prennent en charge tous les emplacements de sauvegarde, sauf les dossiers NFS et Secure Zone.

Pour créer un plan de nettoyage

1. Dans la Cyber Protectconsole, cliquez sur **Gestion** > **Nettoyage**.
2. Cliquez sur **Création d'un plan**.
3. Dans **Agent**, sélectionnez l'agent qui effectuera le nettoyage.
   Vous pouvez sélectionner n'importe quel agent ayant accès à l'emplacement de sauvegarde.
4. Dans **Éléments à nettoyer**, sélectionnez les archives ou les emplacements de sauvegarde à nettoyer.
   Pour naviguer entre les archives et les emplacements, utilisez le commutateur **Emplacements** / **Sauvegardes** dans le coin supérieur droit.
   Si vous sélectionnez plusieurs archives chiffrées, leur mot de passe de cryptage doit être identique. Pour les archives qui utilisent des mots de passe de cryptage différents, créez des plans distincts.
5. Dans **Planification**, configurez la planification de nettoyage.
6. Dans **Règles de rétention**, indiquez les règles de rétention.
   Les options suivantes sont disponibles :
   - **Par nombre de sauvegardes**
   - **Par âge des sauvegardes** (paramètres distincts pour les sauvegardes mensuelles, hebdomadaires, quotidiennes et horaires)
   - **Par volume total de sauvegardes**
7. [Si vous avez sélectionné des archives cryptées dans les **Éléments à répliquer**] Activez le commutateur **Mot de passe de sauvegarde**, puis fournissez le mot de passe de chiffrement.
8. [Facultatif] Pour modifier les options du plan, cliquez sur l'icône engrenage, puis configurez les options selon vos besoins.
9. Cliquez sur **Créer**.

Conversion en une machine virtuelle

La conversion en une machine virtuelle n'est disponible que pour les sauvegardes de lecteur. Si une sauvegarde inclut un volume système et contient toutes les informations nécessaires au démarrage du système d'exploitation, la machine virtuelle résultante peut démarrer par elle-même. Sinon, vous pouvez ajouter ses disques virtuels sur une autre machine virtuelle.

Remarque
Les machines virtuelles répliquées via la fonctionnalité native de réplication de machines virtuelles de Scale Computing ne peuvent pas être sauvegardées.

Vous pouvez créer un plan séparé pour la conversion vers une machine virtuelle et exécuter ce plan manuellement ou selon un calendrier.

Pour en savoir plus sur les prérequis et les limitations, reportez-vous à "Ce que vous devez savoir à propos de la conversion" (p. 219).

Remarque
Cette fonctionnalité est disponible pour les tenants clients pour lesquels le quota **Advanced Backup - Serveurs** ou **Advanced Backup - NAS** est activé dans le cadre du pack Advanced Backup.

Pour créer un plan de conversion en une machine virtuelle

1. Cliquez sur **Gestion** > **Conversion en MV**.
2. Cliquez sur **Création d'un plan**.
   Le logiciel affiche un nouveau modèle de plan.
3. [Facultatif] Pour modifier le nom du plan, cliquez sur le nom par défaut.
4. Dans **Convertir en**, sélectionnez le type de machine virtuelle cible. **Vous pouvez sélectionner l'une des options suivantes** :
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **HC3 de Scale Computing**
   - **VMware Workstation**
   - **Fichiers VHDX**

   Remarque
   Pour économiser de l'espace, chaque conversion en fichiers VHDX ou VMware Workstation écrase les fichiers VHDX/VMDK situés dans l'emplacement cible et qui ont été créés lors de la conversion précédente.
5. Effectuez l'une des actions suivantes :
   - [Pour VMware ESXi, Hyper-V et Scale Computing HC3] Cliquez sur **Hôte**, sélectionnez l'hôte cible et spécifiez le nouveau modèle de nom de machine.
   - [Pour d'autres types de machines virtuelles] Dans **Chemin d'accès**, spécifiez où enregistrer les fichiers de la machine virtuelle et le modèle de nom de machine.

   Par défaut, le nom est **[Nom de la Machine]_converted**.
6. Cliquez sur **Agent**, puis sélectionnez l'agent qui exécutera la conversion.
7. Cliquez sur **Éléments à convertir**, puis sélectionnez les sauvegardes que ce plan devra convertir en machines virtuelles.
   Vous pouvez passer de la sélection de sauvegardes à la sélection d'emplacements entiers, et vice-versa, à l'aide de l'option **Emplacements**/**Sauvegardes** dans l'angle supérieur droit.
   Si les sauvegardes sélectionnées sont chiffrées, elles doivent toutes utiliser le même mot de passe de chiffrement. Pour les sauvegardes qui utilisent différents mots de passe de chiffrement, créez des plans séparés.

8. [Uniquement pour VMware ESXi et Hyper-V] Cliquez sur **Magasin de données** pour ESXi ou **Chemin d'accès** pour Hyper-V, puis sélectionnez le magasin de données (stockage) pour la machine virtuelle.
9. [Uniquement pour VMware ESXi et Hyper-V] Sélectionnez le mode de provisionnement du disque. Le paramètre par défaut est **Dynamique** pour VMware ESXi et **En expansion dynamique** pour Hyper-V.
10. [Facultatif] [Pour VMware ESXi, Hyper-V et Scale Computing HC3] Cliquez sur **Paramètres de MV** pour modifier la taille de mémoire, le nombre de processeurs ou les connexions réseau de la machine virtuelle.
11. [Facultatif] Cliquez sur **Planification**, puis modifiez la planification.
12. Si les sauvegardes sélectionnées dans **Éléments à convertir** sont chiffrées, activez l'option **Mot de passe de la sauvegarde**, puis indiquez le mot de passe de chiffrement. Sinon, ignorez cette étape.
13. [Facultatif] Pour modifier les options du plan, cliquez sur l'icône en forme d'engrenage.
14. Cliquez sur **Créer**.

Ce que vous devez savoir à propos de la conversion

Types de machine virtuelle pris en charge

Il est possible d'effectuer la conversion d'une sauvegarde sur une machine virtuelle via le même agent que celui qui a créé la sauvegarde, ou via un autre agent.

Pour effectuer une conversion vers VMware ESXi, Hyper-V ou Scale Computing HC3, vous avez besoin respectivement d'un hôte ESXi, Hyper-V ou HC3 de Scale Computing et d'un agent de protection (agent pour VMware, agent pour Hyper-V ou agent pour Scale Computing HC3) qui gère cet hôte.

La conversion vers des fichiers VHDX présuppose que les fichiers seront connectés en tant que disques virtuels à une machine virtuelle Hyper-V.

Le tableau suivant résume les types de machines virtuelles que vous pouvez créer avec l'opération **Convertir en MV**. Les lignes dans le tableau montrent le type des machines virtuelles converties. Les colonnes montrent les agents qui effectuent la conversion.

Type de MV	Agent pour VMware	Agent pour Hyper-V	Agent pour Windows	Agent pour Linux	Agent pour Mac	Agent pour Scale Computing HC3	Agent pour oVirt (KVM)	Agent pour Virtuozzo Hybrid Infrastructure	Agent pour Virtuozzo
VMware	+	–	–	–	–	–	–	–	–

ESXi									
Microsoft Hyper-V	–	+	–	–	–	–	–	–	–
VMware Workstation	+	+	+	+	–	–	–	–	–
Fichiers VHDX	+	+	+	+	–	–	–	–	–
HC3 de Scale Computing	–	–	–	–	–	+	–	–	–

Limites

- Les sauvegardes stockées sur NFS ne peuvent pas être converties.
- Les sauvegardes stockées dans Secure Zone ne peuvent être converties que par l'agent exécuté sur le même ordinateur.
- Les sauvegardes qui contiennent des volumes logiques Linux (LVM) ne peuvent être converties que si elles ont été créées par l'agent pour VMware, l'agent pour Hyper-V ou l'agent pour Scale Computing HC3, et sont dirigées vers le même hyperviseur. La conversion entre superviseurs n'est pas prise en charge.
- Quand les sauvegardes d'une machine Windows sont converties vers des fichiers VMware Workstation ou VHDX, la machine virtuelle résultante hérite du type de processeur de la machine qui exécute la conversion. En conséquence, les pilotes de processeur correspondants sont installés sur le système d'exploitation invité. S'il est démarré sur un hôte ayant un type de processeur différent, le système invité affiche une erreur de pilote. Mettez à jour ce lecteur manuellement.

Conversion régulière en machine virtuelle ou exécution d'une machine virtuelle depuis une sauvegarde

Les deux opérations vous permettent d'avoir une machine virtuelle qui peut démarrer en quelques secondes si la machine d'origine échoue.

Une conversion régulière en machine virtuelle consomme des ressources de CPU et de mémoire. Les fichiers de la machine virtuelle occupent constamment de l'espace sur le magasin de données (stockage). Cela n'est pas pratique si un hôte de production est utilisé pour la conversion. Cependant, les performances de la machine virtuelle sont limitées uniquement par les ressources de l'hôte.

L'exécution d'une machine virtuelle depuis une sauvegarde consomme des ressources uniquement quand la machine virtuelle est en cours d'exécution. Seule la conservation des modifications des disques virtuels nécessite de l'espace dans le magasin de données (stockage). Cependant, la machine virtuelle peut être plus lente, car l'hôte n'accède pas directement aux disques virtuels, mais communique avec l'agent qui lit les données de la sauvegarde. De plus, la machine virtuelle est temporaire.

Fonctionnement de la conversion régulière vers une machine virtuelle

La façon dont la conversion régulière fonctionne dépend de l'endroit que vous choisissez pour créer la machine virtuelle.

- **Si vous choisissez d'enregistrer la machine virtuelle comme un ensemble de fichiers :** chaque conversion recrée la machine virtuelle à partir de zéro.
- **Si vous choisissez de créer la machine virtuelle sur un serveur de virtualisation** : lors de la conversion d'une sauvegarde incrémentielle ou différentielle, le logiciel met à jour la machine virtuelle existante de manière incrémentielle au lieu de la recréer. Cette conversion est normalement plus rapide. Elle réduit le trafic réseau et l'utilisation des ressources du CPU de l'hôte qui exécute la conversion. Si la mise à jour de la machine virtuelle n'est pas possible, le logiciel la crée de nouveau à partir de rien.

Voici une description détaillée de ces deux cas.

Si vous choisissez d'enregistrer la machine virtuelle comme un ensemble de fichiers

Suite à la première conversion, une nouvelle machine virtuelle sera créée. Toutes les conversions suivantes vont créer cette machine à nouveau. Premièrement, l'ancienne machine est temporairement renommée. Puis, une nouvelle machine virtuelle est créée avec le nom précédent de l'ancienne machine. Si cette opération réussi, l'ancienne machine est supprimée. Si cette opération échoue, la nouvelle machine est supprimée et l'ancienne machine reprend son nom précédent. De cette façon, la conversion finit toujours avec une seule machine. Toutefois, de l'espace de stockage supplémentaire est requis pendant la conversion pour stocker l'ancienne machine.

Si vous choisissez de créer la machine virtuelle sur un serveur de virtualisation

La première conversion crée une nouvelle machine virtuelle. Toute conversion ultérieure fonctionne comme suit :

- Si une *sauvegarde complète* a été réalisée depuis la dernière conversion, la machine virtuelle est créée de nouveau à partir de zéro, comme décrit plus haut dans cette section.
- Sinon, la machine virtuelle existante est mise à jour pour refléter les changements depuis la dernière conversion. Si mise à jour n'est pas possible (par exemple, si vous avez supprimé les instantanés intermédiaires, voir ci-dessous), la machine virtuelle est créée de zéro à partir de rien.

Instantanés intermédiaires

Pour être en mesure de mettre à jour la machine virtuelle convertie de façon sécurisée, le logiciel stocke un instantané intermédiaire d'hyperviseur de celle-ci. Cet instantané est appelé **Réplica...** et doit être conservé.

L'instantané **Réplica...** correspond au résultat de la dernière conversion. Vous pouvez utiliser cet instantané si vous voulez ramener la machine à cet état ; par exemple, si vous avez travaillé avec la machine et que vous voulez supprimer les modifications apportées.

Pour les machines virtuelles Scale Computing HC3 converties, un **Instantané utilitaire** est créé. Seul le service Cyber Protection l'utilise.

Plans et modules de protection

Pour protéger vos données, vous devez créer des plans de protection, puis les appliquer à vos ressources.

Un plan de protection se compose de différents modules de protection. Activez les modules dont vous avez besoin et configurez leurs paramètres afin de créer des plans de protection correspondant à vos besoins.

Les modules suivants sont disponibles :

- Sauvegarde. Sauvegarde vos sources de données dans un stockage local ou dans le Cloud.
- "Implémentation de la reprise d'activité après sinistre" (p. 772). Lance des copies exactes de vos ordinateurs dans le cloud et bascule la ressource des ordinateurs d'origine corrompus vers les serveurs de restauration dans le cloud.
- Protection antivirus et antimalware. Vérifie les ressources à l'aide d'une solution antimalware intégrée.
- Fonctionnalité EDR (Protection évolutive des points de terminaison). Détecte toute activité suspecte sur la ressource, y compris les attaques qui n'ont pas été identifiées, et génère des incidents qui vous aident à comprendre comment une attaque s'est produite et comment éviter qu'elle se reproduise.
- Filtrage des URL. Protège vos ordinateurs des menaces provenant d'Internet en bloquant l'accès aux URL et aux contenus téléchargeables malveillants.
- Antivirus Windows Defender. Gère les paramètres de l'antivirus Windows Defender afin de protéger votre environnement.
- Microsoft Security Essentials. Gère les paramètres de Microsoft Security Essentials afin de protéger votre environnement.
- Évaluation des vulnérabilités. Recherche la présence de vulnérabilités dans les solutions Windows, Linux, macOS, Microsoft tierces et macOS tierces installées sur vos ordinateurs, et vous prévient le cas échéant.

- Gestion des correctifs. Installe des correctifs et des mises à jour pour les solutions Windows, Linux, macOS, Microsoft tierces et macOS tierces sur vos ordinateurs afin de résoudre les vulnérabilités détectées.
- Carte de protection des données. Découvre les données afin de surveiller l'état de protection des fichiers importants.
- Contrôle des terminaux. Spécifie les terminaux que les utilisateurs sont autorisés ou ne sont pas autorisés à utiliser sur leurs ordinateurs.
- Advanced Data Loss Prevention. Empêche la fuite les données sensibles depuis les périphériques (imprimantes ou stockage amovible) ou par les transferts réseau internes et externes, selon la règle du flux de données.

Création d'un plan de protection

Vous pouvez créer un plan de protection de l'une des manières suivantes :

- Dans l'onglet **Terminaux**. Sélectionnez une ou plusieurs ressources à protéger, puis créez un plan de protection pour ces charges.
- Dans l'onglet **Gestion** > **Plans de protection**. Créez un plan de protection, puis sélectionnez une ou plusieurs ressources auxquelles l'appliquer.

Lorsque vous créez un plan de protection, seuls les modules applicables à votre type de ressource sont affichés.

Vous pouvez appliquer un plan de protection à plusieurs ressources. Vous pouvez également appliquer plusieurs plans de protection à la même ressource. Pour en savoir plus sur les conflits possibles, voir "Résolution des conflits de plan" (p. 229).

Pour créer un plan de protection

Terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez les ressources que vous souhaitez protéger, puis cliquez sur **Protection**.
3. [Si des plans sont déjà appliqués] Cliquez sur **Ajouter un plan**.
4. Cliquez sur **Création d'un plan** > **Protection**.
   Le tableau de bord du plan de protection s'ouvre.
5. [Facultatif] Pour renommer le plan de protection, cliquez sur l'icône en forme de crayon, puis saisissez le nouveau nom.
6. [Facultatif] Pour activer ou désactiver un module du plan, utilisez l'interrupteur à côté du nom du module.
7. [Facultatif] Pour configurer un module, cliquez dessus pour l'agrandir, puis modifiez les paramètres selon vos besoins.
8. Lorsque vous avez terminé, cliquez sur **Créer**.

Remarque
Pour créer un plan de protection avec chiffrement, spécifiez un mot de passe de chiffrement. Pour plus d'informations, voir "Chiffrement" (p. 462).

Gestion > Plans de protection

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Cliquez sur **Création d'un plan**.
   Le modèle de plan de protection s'ouvre.
3. [Facultatif] Pour renommer le plan de protection, cliquez sur l'icône en forme de crayon, puis saisissez le nouveau nom.
4. [Facultatif] Pour activer ou désactiver un module du plan, utilisez l'interrupteur à côté du nom du module.
5. [Facultatif] Pour configurer un module, cliquez dessus pour l'agrandir, puis modifiez les paramètres selon vos besoins.
6. [Facultatif] Pour sélectionner les ressources auxquelles appliquer le plan, cliquez sur **Ajouter des terminaux**.

   Remarque
   Vous pouvez créer un plan sans l'appliquer à une ressource. Vous pouvez ajouter des ressources ultérieurement en modifiant le plan. Pour plus d'informations sur l'ajout d'une ressource à un plan, voir "Application d'un plan de protection à une ressource" (p. 225).

7. Lorsque vous avez terminé, cliquez sur **Créer**.

   Remarque
   Pour créer un plan de protection avec chiffrement, spécifiez un mot de passe de chiffrement. Pour plus d'informations, voir "Chiffrement" (p. 462).

Pour exécuter un module à la demande (**Sauvegarde**, **Protection contre les virus et les malwares**, **Évaluation des vulnérabilités**, **Gestion des correctifs** ou **Carte de la protection des données**), cliquez sur **Exécuter maintenant**.

Regardez la vidéo pratique Création du premier plan de protection.

Pour plus d'informations sur le module de reprise d'activité après sinistre, voir "Créer un plan de protection de reprise d'activité après sinistre" (p. 779).

Pour plus d'informations sur le module de contrôle des terminaux, voir "Utilisation du module de contrôle des terminaux" (p. 379).

Actions avec plans de protection

Après avoir créé un plan de protection, vous pouvez l'utiliser pour exécuter les opérations suivantes :

- Appliquer un plan à une ressource ou à un groupe de terminaux.
- Renommer le plan.
- Modifier un plan.

  Vous pouvez activer et désactiver les modules d'un plan, et modifier ses paramètres.
- Activer ou désactiver un plan.

  Un plan désactivé ne sera pas exécuté sur les ressources auxquelles il est appliqué.

  Cette action est utile pour les administrateurs qui prévoient de protéger ultérieurement la même ressource avec le même plan. Le plan n'est pas révoqué de la ressource et vous pouvez restaurer la protection en réactivant le plan.
- Révoquer un plan d'une ressource.

  Un plan révoqué n'est plus appliqué à la ressource.

  Cette action est utile pour les administrateurs qui n'ont pas besoin de protéger rapidement la même ressource avec le même plan. Pour restaurer la protection d'un plan révoqué, vous devez connaître le nom de ce plan, le sélectionner dans la liste des plans disponibles et le réappliquer à la ressource correspondante.
- Arrêter un plan

  Cette action arrête toutes les opérations de sauvegarde en cours d'exécution sur toutes les ressources auxquelles le plan est appliqué. Les sauvegardes redémarrent en fonction de la planification du plan.

  L'analyse antimalware n'est pas concernée par cette action et se poursuit conformément à la configuration de la planification.
- Cloner un plan.

  Vous pouvez créer une copie exacte d'un plan existant. Le nouveau plan n'est affecté à aucune ressource.
- Exporter et importer un plan.

  Vous pouvez exporter un plan sous forme de fichier JSON que vous pourrez réimporter ultérieurement. Par conséquent, vous n'avez pas besoin de créer un nouveau plan manuellement et de configurer ses paramètres.

  Remarque

  Vous pouvez importer les plans de protection créés dans Cyber Protection 9.0 (publiée en mars 2020) et versions ultérieures. Les plans créés dans des versions précédentes ne sont pas compatibles avec Cyber Protection 9.0 et les versions ultérieures.
- Vérifier les détails d'un plan.
- Vérifiez les activités et les alertes relatives à un plan.
- Supprimer un plan.

Application d'un plan de protection à une ressource

Pour protéger une ressource, vous devez lui appliquer un plan de protection.

Vous pouvez appliquer un plan à partir de l'onglet **Terminaux** et de l'onglet **Gestion** > **Plans de protection**.

Terminaux

1. Sélectionnez une ou plusieurs ressources à protéger.
2. Cliquez sur **Protection**.
3. [Si un autre plan de protection est déjà appliqué aux ressources sélectionnées] Cliquez sur **Ajouter un plan**.
4. La liste des plans de protection disponibles s'affiche.
5. Sélectionnez le plan de protection que vous souhaitez appliquer, puis cliquez sur **Appliquer**.

Gestion > Plans de protection

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Sélectionnez le plan de protection que vous souhaitez appliquer.
3. Cliquez sur **Modifier**.
4. Cliquez sur **Gérer les terminaux**.
5. Dans la fenêtre **Terminaux**, cliquez sur **Ajouter**.
6. Sélectionnez les ressources auxquelles vous souhaitez appliquer le plan, puis cliquez sur **Ajouter**.
7. Dans la fenêtre **Terminaux**, cliquez sur **Terminé**.
8. Dans le tableau de bord du plan de protection, cliquez sur **Enregistrer**.

Pour savoir comment appliquer un plan de protection à un groupe de terminaux, voir "Application d'un plan à un groupe" (p. 377).

Modification d'un plan de protection

Lorsque vous modifiez un plan, vous pouvez activer et désactiver ses modules, et modifier leurs paramètres.

Vous pouvez modifier un plan de protection pour toutes les ressources auxquelles il est appliqué ou uniquement pour les ressources sélectionnées.

Vous pouvez modifier un plan à partir des onglets **Terminaux** et **Gestion** > **Plans de protection**.

Terminaux

1. Sélectionnez une ou plusieurs ressources auxquelles le plan est appliqué.
2. Cliquez sur **Protection**.
3. Sélectionnez le plan de protection que vous souhaitez modifier.
4. Cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan, puis sur **Modifier**.

5. Cliquez sur un module que vous souhaitez modifier, puis configurez ses paramètres en fonction de vos besoins.
6. Cliquez sur **Enregistrer**.
7. [Si vous n'avez pas sélectionné toutes les ressources auxquelles le plan est appliqué] Sélectionnez le champ d'application de la modification :
   - Pour modifier le plan pour toutes les ressources auxquelles il est appliqué, cliquez sur **Appliquer les modifications à ce plan (cela a une incidence sur d'autres terminaux)**.
   - Pour ne modifier le plan que pour les ressources sélectionnées, cliquez sur **Créer un plan de protection pour les terminaux sélectionnés uniquement**.

     En conséquence, le plan existant sera révoqué des ressources sélectionnées. Un nouveau plan de protection avec les paramètres que vous avez configurés sera créé et appliqué à ces ressources.

Gestion > Plans de protection

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Sélectionnez le plan de protection que vous souhaitez modifier.
3. Cliquez sur **Modifier**.
4. Cliquez sur les modules que vous souhaitez modifier, puis configurez leurs paramètres en fonction de vos besoins.
5. Cliquez sur **Enregistrer**.

Remarque
La modification d'un plan à partir de l'onglet **Gestion** > **Plans de protection** a une incidence sur toutes les ressources auxquelles ce plan est appliqué.

Révocation d'un plan de protection

Lorsque vous retirez un plan, vous le supprimez d'une ou de plusieurs ressources. Le plan continue à protéger les autres ressources auxquelles il est appliqué.

Vous pouvez révoquer un plan à partir des onglets **Terminaux** et **Gestion** > **Plans de protection**.

Terminaux

1. Sélectionnez les ressources à partir desquelles vous voulez révoquer le plan.
2. Cliquez sur **Protection**.
3. Sélectionnez le plan de protection que vous souhaitez révoquer.
4. Cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan, puis sur **Révoquer**.

Gestion > Plans de protection

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Sélectionnez le plan de protection que vous souhaitez révoquer.

3. Cliquez sur **Modifier**.
4. Cliquez sur **Gérer les terminaux**.
5. Dans la fenêtre **Terminaux**, sélectionnez les ressources à partir desquelles vous souhaitez révoquer le plan.
6. Cliquez sur **Supprimer**.
7. Dans la fenêtre **Terminaux**, cliquez sur **Terminé**.
8. Dans le modèle de plan de protection, cliquez sur **Enregistrer**.

Activation ou désactivation d'un plan de protection

Un plan activé est actif et s'exécute sur les ressources auxquelles il est appliqué. Un plan désactivé est inactif : il est toujours appliqué aux ressources, mais il ne s'y exécute pas.

Lorsque vous activez ou désactivez un plan de protection depuis l'onglet **Terminaux**, votre action n'a une incidence que sur les ressources sélectionnées.

Lorsque vous activez ou désactivez un plan de protection à partir de l'onglet **Gestion** > **Plans de protection**, votre action a une incidence sur toutes les ressources auxquelles ce plan est appliqué. Par ailleurs, vous pouvez activer ou désactiver plusieurs plans de protection.

Terminaux

1. Sélectionnez la ressource que vous envisagez de désactiver.
2. Cliquez sur **Protection**.
3. Sélectionnez le plan de protection que vous souhaitez désactiver.
4. Cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan, puis sur **Activer** ou sur **Désactiver** respectivement.

Gestion > Plans de protection

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Sélectionnez un ou plusieurs plans de protection que vous souhaitez activer ou désactiver.
3. Cliquez sur **Modifier**.
4. Cliquez sur **Activer** ou **Désactiver** respectivement.

Remarque
Cette action n'a aucune incidence sur les plans de protection qui étaient déjà dans l'état cible. Par exemple, si votre sélection comprend des plans activés et désactivés, et que vous cliquiez sur **Activer**, tous les plans sélectionnés seront activés.

Suppression d'un plan de protection

Lorsque vous supprimez un plan, il est révoqué à partir de toutes les ressources et est supprimé de la console Cyber Protect.

Vous pouvez supprimer un plan à partir des onglets **Terminaux** et **Gestion** > **Plans de protection**.

Terminaux

1. Sélectionnez une ressource à laquelle le plan de protection que vous voulez supprimer est appliqué.
2. Cliquez sur **Protection**.
3. Sélectionnez le plan de protection que vous souhaitez supprimer.
4. Cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan de protection, puis sur **Supprimer**.

Gestion > Plans de protection

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Sélectionnez le plan de protection que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.
4. Confirmez votre choix en cochant la case **Je confirme la suppression du plan**, puis cliquez sur **Supprimer**.

Résolution des conflits de plan

Vous pouvez appliquer plusieurs plans de protection à la même ressource. Par exemple, vous pouvez appliquer un plan de protection dans lequel vous n'avez activé et configuré que le module **Antivirus et antimalware**, ainsi qu'un autre plan de protection dans lequel vous n'avez activé et configuré que le module **Sauvegarde**.

Vous pouvez associer des plans de protection dans lesquels les modules activés sont différents. Vous pouvez également associer plusieurs plans de protection dans lesquels le module **Sauvegarde** est le seul activé. Toutefois, un conflit se produit si un autre module est activé dans plusieurs plans. Pour appliquer le plan, vous devez d'abord résoudre le conflit.

Conflit entre un nouveau plan et un plan existant

Si un nouveau plan entre en conflit avec un plan existant, vous pouvez résoudre le conflit de l'une des manières suivantes :

- Créez un nouveau plan, appliquez-le, puis désactivez le plan existant qui entre en conflit avec le nouveau.
- Créez un nouveau plan, puis désactivez-le.

Conflit entre un plan individuel et un plan de groupe

Si un plan de protection individuel entre en conflit avec un plan de groupe appliqué à un groupe de terminaux, vous pouvez résoudre le conflit de l'une des manières suivantes :

- Supprimez la ressource du groupe de terminaux, puis appliquez au groupe le plan de protection individuel.

- Modifiez le plan de groupe existant ou appliquez au groupe de terminaux un nouveau plan de groupe.

Problème de licence

Un module de plan de protection peut exiger l'affectation d'un quota de service spécifique à la ressource protégée. Si le quota de service affecté n'est pas approprié, vous ne pourrez pas exécuter, mettre à jour ou appliquer le plan de protection dans lequel le module correspondant est activé.

Pour résoudre un problème de licence, effectuez l'une des actions suivantes :

- Désactivez le module non supporté par le quota de service affecté, puis continuez à utiliser le plan de protection.
- Modifiez manuellement le quota de service attribué. Pour savoir comment procéder, voir "Modification du quota de service des ordinateurs" (p. 192).

Plans de protection par défaut

Un plan de protection par défaut est un modèle préconfiguré que vous pouvez appliquer à vos ressources pour assurer une protection rapide. En utilisant un plan de protection par défaut, vous n'avez pas à créer de nouveaux plans de protection de toutes pièces.

Lorsque vous appliquez un plan de protection par défaut pour la première fois, le modèle est copié dans votre tenant et vous pouvez modifier les modèles dans le plan et ses paramètres.

Les plans par défaut suivants sont disponibles :

- Cyber Protect Essentials
  Ce plan fournit une fonctionnalité de protection de base et une sauvegarde de niveau fichier.
- Employés en télétravail
  Ce plan est optimisé pour les utilisateurs qui travaillent à distance. Il propose des tâches plus fréquentes (sauvegarde, protection antimalware et évaluation des vulnérabilités, par exemple), des actions de protection plus strictes, des performances optimisées et des options d'alimentation.
- Employés de bureau (Antivirus tiers)
  Ce plan est optimisé pour les employés de bureau qui préfèrent utiliser un logiciel antivirus tiers. Dans ce plan, le module **Protection antivirus et antimalware** est désactivé.
- Employés de bureau (Antivirus Acronis)
  Ce plan est optimisé pour les employés de bureau qui préfèrent utiliser le logiciel antivirus Acronis.

Comparaison des plans de protection par défaut

Modules et options	Plans de protection par défaut			
	Cyber Protect Essentials	**Employés en télétravail**	**Employés de bureau (Antivirus tiers)**	**Employés de bureau (Antivirus Acronis)**
Sauvegarde	Disponible	Disponible	Disponible	Disponible
Quoi sauvegarder Éléments à sauvegarder	Fichiers/dossiers [Dossier de tous les profils]	Toute la machine	Toute la machine	Toute la machine
Protection continue des données (CDP)	Désactivé	Activé	Désactivé	Désactivé
Où sauvegarder	Stockage dans le Cloud	Stockage dans le Cloud	Stockage dans le Cloud	Stockage dans le Cloud
Planification	Du lundi au vendredi, à 23 h	Du lundi au vendredi, à 00 h En plus, options activées et conditions de démarrage : • Si la machine est arrêtée, exécutez les tâches ratées lors du démarrage de la machine • Sortir du mode veille ou veille prolongée pour démarrer une sauvegarde planifiée • Économiser de la batterie : Ne pas démarrer lors d'une alimentation sur batterie • Ne pas	Du lundi au vendredi, à 23 h	Du lundi au vendredi, à 23 h

Modules et options	Plans de protection par défaut			
	Cyber Protect Essentials	**Employés en télétravail**	**Employés de bureau (Antivirus tiers)**	**Employés de bureau (Antivirus Acronis)**
		démarrer pendant une connexion mesurée		
Modèle de sauvegarde	Toujours incrémentielle	Toujours incrémentielle	Toujours incrémentielle	Toujours incrémentielle
Durée de conservation	Conserver les sauvegardes indéfiniment	Mensuelle : 12 mois Hebdomadaire : 4 semaines Quotidienne : 7 jours	Mensuelle : 12 mois Hebdomadaire : 4 semaines Quotidienne : 7 jours	Mensuelle : 12 mois Hebdomadaire : 4 semaines Quotidienne : 7 jours
Options de sauvegarde	Options par défaut	Options par défaut, plus : • Performance et créneau de sauvegarde (l'ensemble vert) : Priorité de CPU : Faible Vitesse de sortie : 50 %	Options par défaut	Options par défaut
Protection contre les virus et les malwares	Disponible	Disponible	Non disponible	Disponible
Active Protection	Désactivée	Désactivée	–	Désactivée
Protection anti-malware Advanced	Activée	Activée	–	Activée
Protection du dossier réseau	Activée	Activée	–	Activée
Protection côté serveur	Désactivée	Désactivée	–	Désactivée
Autoprotection	Activée	Activée	–	Activée

Modules et options	Plans de protection par défaut			
	Cyber Protect Essentials	**Employés en télétravail**	**Employés de bureau (Antivirus tiers)**	**Employés de bureau (Antivirus Acronis)**
Détection d'un processus de cryptominage	Activée	Activée	–	Activée
Quarantaine	Supprimer les fichiers mis en quarantaine après 30 jours	Supprimer les fichiers mis en quarantaine après 30 jours	–	Supprimer les fichiers mis en quarantaine après 30 jours
Moteur de comportement	Quarantaine	Quarantaine	–	Quarantaine
Prévention des failles	Notifier et stopper le processus	Notifier et stopper le processus	–	Notifier et stopper le processus
Protection en temps réel	Quarantaine	Quarantaine	–	Quarantaine
Planifier l'analyse	Analyse rapide : Quarantaine À 14 h 20, du dimanche au samedi Analyse complète : Désactivée	Analyse rapide : Désactivée Analyse complète : Quarantaine À 13 h 55, du dimanche au samedi En plus, options activées et conditions de démarrage : • Si la machine est arrêtée, exécutez les tâches ratées lors du démarrage de la machine • Sortir du mode veille ou veille prolongée pour démarrer une	–	Analyse rapide : Quarantaine À 14 h 20, du dimanche au samedi Analyse complète : Désactivée

Modules et options	Plans de protection par défaut			
	Cyber Protect Essentials	**Employés en télétravail**	**Employés de bureau (Antivirus tiers)**	**Employés de bureau (Antivirus Acronis)**
		sauvegarde planifiée • Économiser de la batterie : Ne pas démarrer lors d'une alimentation sur batterie		
Exclusions	Aucun	Aucun	–	Aucun
Filtrage d'URL	Disponible	Disponible	Disponible	Disponible
Accès à un site Web malveillant	Toujours demander à l'utilisateur	Bloquer	Toujours demander à l'utilisateur	Toujours demander à l'utilisateur
Catégories à filtrer	Options par défaut	Options par défaut	Options par défaut	Options par défaut
Exclusions	Aucun	Aucun	Aucun	Aucun
Évaluation des vulnérabilités	Disponible	Disponible	Disponible	Disponible
Portée d'évaluation des vulnérabilités	Produits Microsoft, produits Windows tiers	Produits Microsoft, produits Windows tiers	Produits Microsoft, produits Windows tiers	Produits Microsoft, produits Windows tiers
Planification	À 13 h 15, uniquement le lundi	À 14 h 20, uniquement le lundi	À 13 h 15, uniquement le lundi	À 13 h 15, uniquement le lundi
Gestion des correctifs	Disponible	Disponible	Disponible	Disponible
Produits Microsoft	Toutes les mises à jour	Toutes les mises à jour	Toutes les mises à jour	Toutes les mises à jour
Produits Windows tiers	Mises à jour principales uniquement	Mises à jour principales uniquement	Mises à jour principales uniquement	Mises à jour principales uniquement
Planification	À 15 h 10,	À 14 h 20, du lundi	À 15 h 10,	À 15 h 10,

Modules et options	Plans de protection par défaut			
	Cyber Protect Essentials	**Employés en télétravail**	**Employés de bureau (Antivirus tiers)**	**Employés de bureau (Antivirus Acronis)**
	uniquement le lundi	au vendredi	uniquement le lundi	uniquement le lundi
Sauvegarde pré-mise à jour	Désactivée	Activée	Désactivée	Désactivée
Carte de la protection des données	Non disponible	Disponible	Disponible	Disponible
Extensions et règles d'exception	–	Options par défaut et autres extensions suivantes : **Images** • .jpeg • .jpg • .png • .gif • .bmp • .ico • .wbmp • .xcf • .psd • .tiff • .dwg **Audio et vidéo** • .avi, • .mov, • .mpeg, • .mpg, • .mkv • .wav • .aif • .aifc • .aiff • .au • .snd	Options par défaut (66 extensions à détecter)	Options par défaut (66 extensions à détecter)

Modules et options	Plans de protection par défaut			
	Cyber Protect Essentials	Employés en télétravail	Employés de bureau (Antivirus tiers)	Employés de bureau (Antivirus Acronis)
		• .mid • .midi • .mpga • .mp3 • .oga • .flac • .opus • .spx • .ogg • .ogx • .mp4		
Planification	–	À 15 h 35, du lundi au vendredi	À 15 h 40, du lundi au vendredi	À 15 h 40, du lundi au vendredi

Remarque
Le nombre de modules d'un plan de protection par défaut peut varier selon votre licence Cyber Protection.

Application d'un plan de protection par défaut

Les plans de protection par défaut initiaux sont des modèles dont vous ne pouvez pas modifier les paramètres. Lorsque vous appliquez un plan par défaut pour la première fois, le modèle est copié dans votre tenant sous forme de plan de protection préconfiguré et il est activé sur les ressources sélectionnées.

Le plan de protection apparaît dans l'onglet **Gestion** > **Plans de protection** et vous pouvez le modifier.

Pour appliquer un plan de protection par défaut pour la première fois

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez les ressources que vous souhaitez protéger.
3. Cliquez sur **Protection**.
4. Sélectionnez l'un des plans par défaut, puis cliquez sur **Appliquer**.

Modification d'un plan de protection par défaut

Vous pouvez modifier un plan de protection par défaut après l'avoir appliqué pour la première fois.

Pour modifier un plan de protection par défaut appliqué

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Sélectionnez le plan que vous souhaitez modifier, puis cliquez sur **Modifier**.
3. Modifiez les modules inclus dans ce plan, ou leurs options, puis cliquez sur **Enregistrer**.

Important
Certaines des options ne peuvent pas être modifiées.

Plans de protection individuels pour l'hébergement des intégrations du panneau de configuration

Lorsque vous activez l'hébergement des intégrations du panneau de configuration sur les serveurs d'hébergement Web qui utilisent DirectAdmin, cPanel ou Plesk, le service Cyber Protection crée automatiquement un plan de protection individuel sous le compte utilisateur pour chaque ressource. Ce plan de protection est associé à la ressource spécifique qui a lancé la création du plan de protection et il ne peut être ni révoqué ni affecté à d'autres ressources.

Pour ne plus utiliser un plan de protection individuel, vous pouvez le supprimer depuis la console Cyber Protect. Vous pouvez identifier les plans de protection individuels à l'aide du signe qui figure après leur nom.

Si vous souhaitez qu'un plan de protection protège plusieurs serveurs d'hébergement Web utilisant les intégrations du panneau de configuration, vous pouvez créer un plan de protection standard dans la console Cyber Protect et lui affecter ces ressources. Toutefois, les modifications apportées à un plan de protection partagé par plusieurs panneaux de configuration d'hébergement Web ne peuvent être effectuées que dans la console Cyber Protect, pas depuis les intégrations.

Score #CyberFit pour les machines

Le Score #CyberFit vous fournit un mécanisme d'évaluation et de notation de la sécurité qui évalue l'état de la sécurité de votre machine. Il identifie les failles de sécurité de l'environnement informatique et les vecteurs d'attaques ouvertes vers les terminaux, et recommande des actions d'amélioration sous la forme d'un rapport. Cette fonctionnalité est disponible dans toutes les éditions de Cyber Protect.

La fonctionnalité Score #CyberFit est prise en charge sur :

- Windows 7 (première version) et versions ultérieures
- Windows Server 2008 R2 et versions ultérieures

Fonctionnement

L'agent de protection installé sur une machine procède à une évaluation de la sécurité et calcule le Score #CyberFit de la machine. Le Score #CyberFit d'une machine est recalculé régulièrement de façon automatique.

Mécanisme de notation #CyberFit

Le Score #CyberFit d'une machine est calculé sur la base des indicateurs suivants :

- Protection contre les malwares 0-275
- Protection des sauvegardes 0-175
- Pare-feu 0-175
- Réseau privé virtuel (VPN) 0-75
- Chiffrement du disque intégral 0-125
- Sécurité du réseau 0-25

Le Score #CyberFit maximum d'une machine est de 850.

Indicateur	Qu'est-ce qui est évalué ?	Recommandations aux utilisateurs	Score
Anti-malware	L'agent vérifie si un logiciel anti-malware est installé ou non sur une machine.	Résultats : • Votre protection contre les malwares est activée (+275 points) • Vous n'avez pas de protection contre les malwares ; votre système pourrait courir un risque (0 point) Recommandations fournies par le Score #CyberFit : Vous devriez avoir une solution anti-malware installée et activée sur votre machine, afin qu'elle reste protégée contre les risques en matière de sécurité. Nous vous invitons à consulter des sites tels que AV-Test ou AV-Comparatives pour obtenir une liste des solutions anti-malware recommandées.	275 : un logiciel anti-malware est installé sur une machine 0 : aucun logiciel anti-malware n'est installé sur une machine
Sauvegarde	L'agent vérifie si une solution de sauvegarde est installée sur un ordinateur.	Résultats : • Vous avez une solution de sauvegarde qui protège vos données (+175 points) • Aucune solution de sauvegarde n'a été trouvée ; vos données pourraient courir un risque (0 point) Recommandations fournies par le Score #CyberFit : Nous vous recommandons de sauvegarder vos données régulièrement afin d'éviter la perte de données ou les attaques par ransomware. Vous trouverez ci-dessous des solutions de sauvegarde à envisager :	175 : une solution de sauvegarde est installée sur une machine 0 : aucune solution de sauvegarde n'est installée sur une machine

		• Acronis Cyber Protect/Cyber Backup/True Image • Sauvegarde de serveur Windows (Windows Server 2008 R2 et versions ultérieures)	
Pare-feu	L'agent vérifie si un pare-feu est disponible et activé dans votre environnement. L'agent effectue les actions suivantes : 1. Vérifie le pare-feu Windows et la protection du réseau pour savoir si un pare-feu public est activé. 2. Vérifie le pare-feu Windows et la protection du réseau pour savoir si un pare-feu privé est activé. 3. Vérifie la solution/l'agent de pare-feu tiers pour savoir si des pare-feu publics ou privés sont désactivés.	Résultats : • Vous avez un pare-feu activé pour les réseaux publics et privés, ou une solution de pare-feu tierce a été trouvée (+175 points) • Vous avez un pare-feu activé uniquement pour les réseaux publics (+100 points) • Vous avez un pare-feu activé uniquement pour les réseaux privés (+75 points) • Vous n'avez pas de pare-feu activé ; vos connexions réseau ne sont pas sécurisées (0 point) Recommandations fournies par le Score #CyberFit : Nous vous recommandons d'activer un pare-feu pour vos réseaux publics et privés afin d'améliorer votre protection contre les attaques malveillantes envers votre système. Vous trouverez ci-dessous des guides détaillés concernant la configuration de votre pare-feu Windows, en fonction de vos besoins de sécurité et de l'architecture de votre réseau : Guides pour les utilisateurs finaux / employés : Comment configurer le Pare-feu Windows Defender sur votre PC Comment configurer le Pare-feu Windows sur votre PC Guides pour les administrateurs et ingénieurs système : Comment déployer le Pare-feu Windows Defender avec la sécurité avancée Comment créer des règles avancées dans le Pare-feu Windows	100 : un pare-feu public Windows est activé 75 : un pare-feu privé Windows est activé 175 : des pare-feu publics et privés Windows sont activés OU une solution de pare-feu tierce est activée 0 : aucun pare-feu Windows ni solution de pare-feu tierce n'est activé
Réseau privé virtuel (VPN)	L'agent vérifie si une solution VPN est installée sur une machine et si le VPN est activé et en cours d'exécution.	Résultats : • Vous avez une solution VPN, et pouvez recevoir et envoyer des données en toute sécurité sur les réseaux publics et partagés (+75 points) • Aucune solution VPN n'a été trouvée ; votre connexion aux réseaux publics et partagés n'est pas sécurisée (0 point)	75 : un VPN est activé et en cours d'exécution 0 : aucun VPN n'est activé

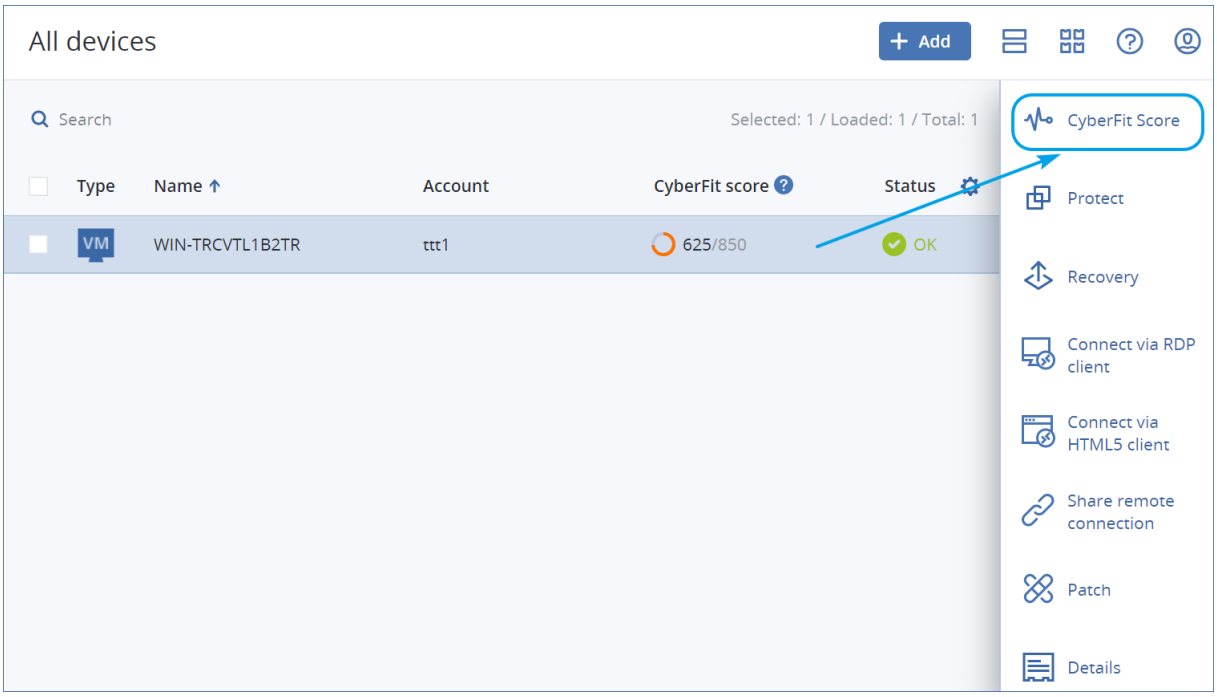
		Recommandations fournies par le Score #CyberFit : Nous vous recommandons d'utiliser un VPN pour accéder à votre réseau d'entreprise et à vos données confidentielles. Il est essentiel d'utiliser un VPN pour que vos communications restent sécurisées et privées, en particulier si vous utilisez la connexion Internet gratuite d'un café, d'une bibliothèque, d'un aéroport ou autre. Vous trouverez ci-dessous des solutions de VPN à envisager : • VPN Acronis Business • OpenVPN • Cisco AnyConnect • NordVPN • TunnelBear • ExpressVPN • PureVPN • CyberGhost VPN • Perimeter 81 • VyprVPN • IPVanish VPN • Hotspot Shield VPN • Fortigate VPN • ZYXEL VPN • SonicWall GVPN • LANCOM VPN	
Chiffrement de disque	L'agent vérifie si le chiffrement du disque est activé sur une machine. L'agent vérifie si Windows BitLocker est activé.	Résultats : • Votre chiffrement complet de disque est activé ; votre machine est protégée contre l'altération physique (+125 points) • Seuls certains disques durs sont chiffrés ; votre machine pourrait courir un risque d'altération physique (+75 points) • Aucun chiffrement de disque n'a été trouvé ; votre machine court un risque d'altération physique (0 point) Recommandations fournies par le Score #CyberFit : Nous vous recommandons d'activer Windows BitLocker afin d'améliorer la protection de vos données et fichiers. Guide : Comment activer un terminal de chiffrement dans Windows	125 : tous les disques sont chiffrés 75 : au moins un de vos disques est chiffré, mais il existe également des disques non chiffrés 0 : aucun disque n'est chiffré

Sécurité du réseau (trafic NTLM sortant vers des serveurs distants)	L'agent vérifie si le trafic NTLM sortant d'une machine est restreint vers des serveurs distants.	Résultats : • Le trafic NTLM sortant vers des serveurs distants est refusé ; vos identifiants sont protégés (+25 points) • Le trafic NTLM sortant vers des serveurs distants n'est pas refusé ; vos identifiants pourraient être exposés (0 point) Recommandations fournies par le Score #CyberFit : Pour une meilleure protection, nous vous recommandons de refuser tout le trafic NTLM sortant vers des serveurs distants. Vous pouvez trouver des informations sur la façon dont modifier les paramètres NTLM et ajouter des exceptions en cliquant sur le lien ci-dessous. Guide : Restreindre le trafic NTLM sortant vers des serveurs distants	25 : le trafic NTLM sortant est défini sur ToutRefuser 0 : le trafic NTLM sortant est défini sur une autre valeur

Sur la base des points cumulés attribués à chaque indicateur, le Score #CyberFit total d'une machine peut correspondre à l'une des notations suivantes, qui reflète le niveau de protection du terminal :

- 0 - 579 : Mauvais
- 580 - 669 : Passable
- 670 - 739 : Bon
- 740 - 799 : Très bon
- 800 - 850 : Excellent

Vous pouvez consulter le Score #CyberFit de vos machines dans la console Cyber Protect : accédez à **Terminaux** > **Tous les terminaux**. Dans la liste des terminaux, vous pouvez voir la colonne **Score #CyberFit**. Vous pouvez également exécuter l'analyse du Score #CyberFit d'une machine pour vérifier sa posture en matière de sécurité.

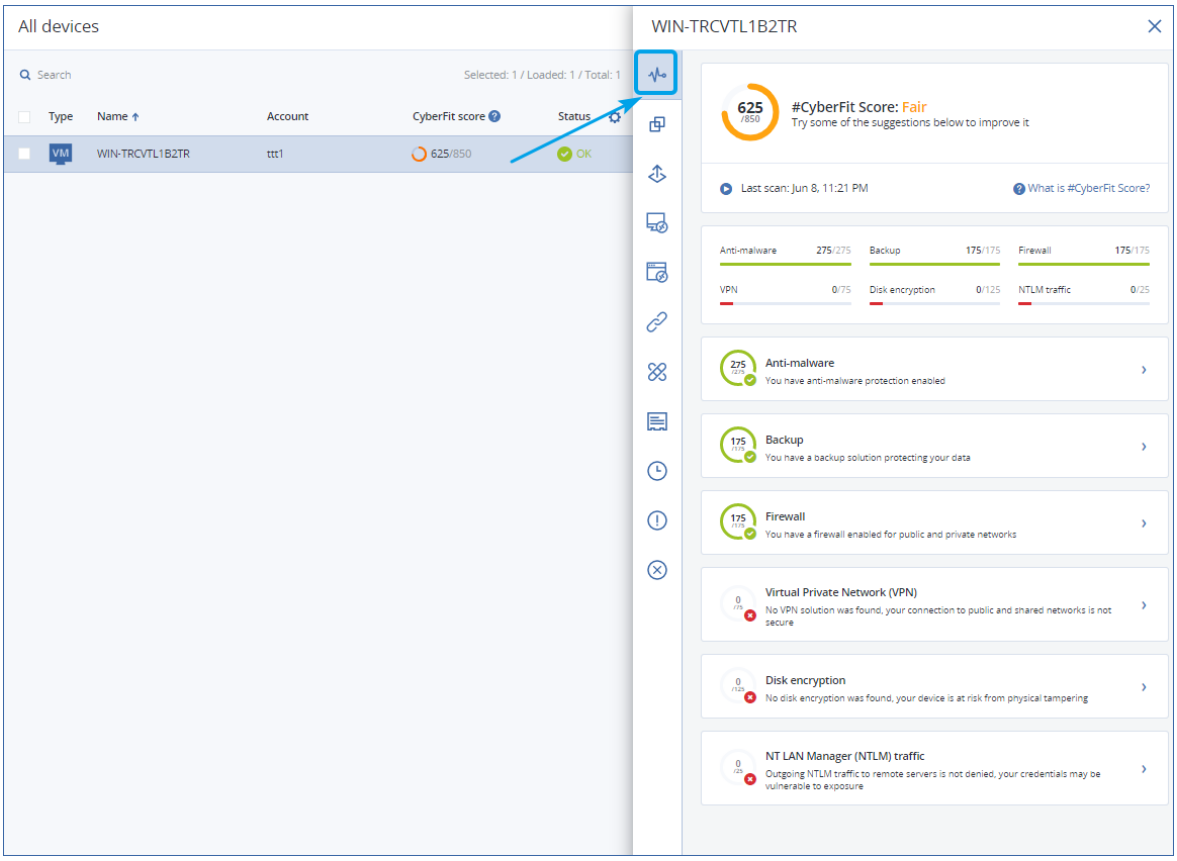


Vous pouvez également obtenir des informations concernant le Score #CyberFit sur les pages de widget et de rapport correspondantes.

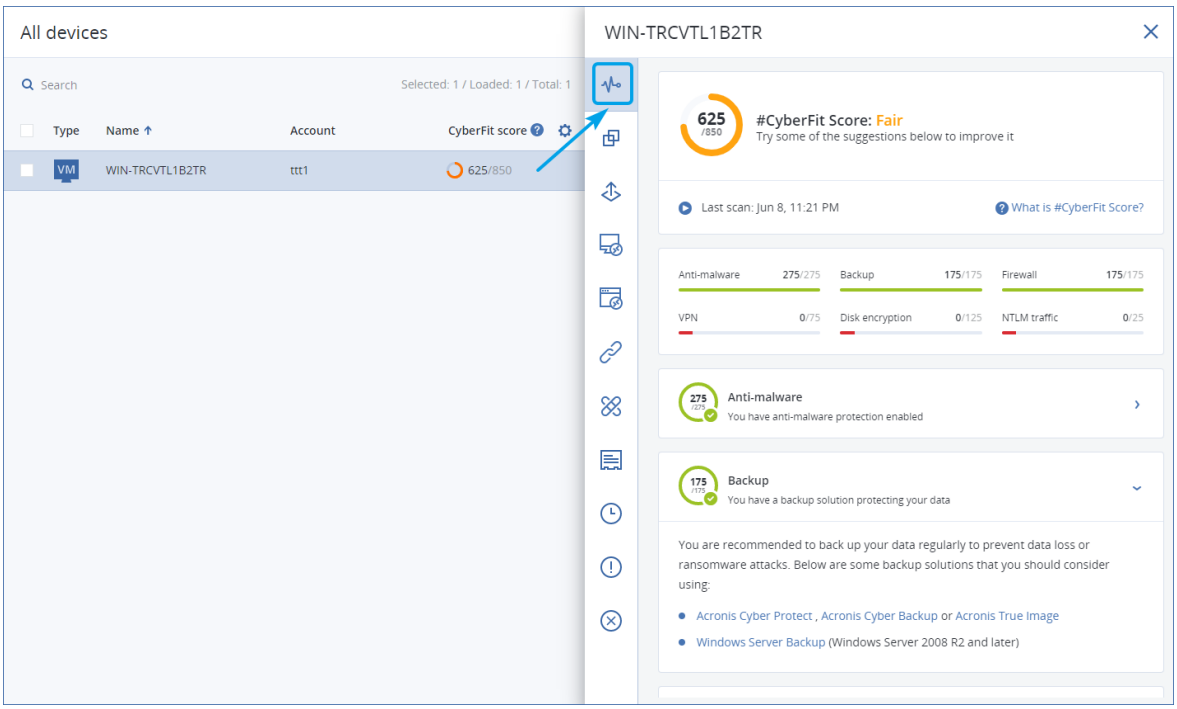
Lancer une analyse du Score #CyberFit

Pour lancer une analyse du Score #CyberFit

1. Dans la console Cyber Protect, accédez à **Terminaux**.
2. Sélectionnez la machine, puis cliquez sur **Score #CyberFit**.
3. Si la machine n'a jamais été analysée, cliquez sur **Exécuter une première analyse**.
4. Une fois l'analyse terminée, vous verrez le Score #CyberFit total de la machine, ainsi que les scores de chacun des six indicateurs évalués : Anti-malware, Sauvegarde, Pare-feu, Réseau privé virtuel (VPN), Chiffrement de disque et Trafic sortant NT LAN Manager (NTLM).



5. Pour vérifier comment améliorer le score de chaque indicateur pour lequel les configurations de sécurité pourraient être améliorées, développez la section correspondante et lisez les recommandations.



6. Après mis les recommandations en place, vous pouvez toujours recalculer le Score #CyberFit de la machine en cliquant sur le bouton flèche juste en dessous du Score #CyberFit total.

Création de cyber-scripts

Avec la création de cyberscripts, vous pouvez automatiser des opérations de routine sur les ordinateurs Windows et macOS de votre environnement : installation de logiciels, modification de configuration, démarrage ou arrêt de services, et création de comptes. Vous pouvez ainsi réduire le risque d'erreur et le temps passé sur de telles opérations lorsque vous les effectuez manuellement.

La création de cyberscripts est disponible pour les administrateurs et les utilisateurs au niveau du client, ainsi que pour les administrateurs partenaires (fournisseurs de services). Pour plus d'informations sur les différents niveaux d'administration, voir "Prise en charge de la mutualisation" (p. 341).

Les scripts que vous pouvez utiliser doivent être approuvés au préalable. Seuls les administrateurs ayant le rôle de **cyberadministrateur** peuvent approuver et tester de nouveaux scripts. Pour plus d'informations sur la modification du statut des scripts, voir "Modification de l'état du script" (p. 255).

En fonction de votre rôle, vous pouvez effectuer des opérations différentes sur les scripts et les plans de script. Pour plus d'informations sur les rôles, voir "Rôles d'utilisateur et droits de création de cyber-scripts" (p. 245).

Prérequis

- La fonctionnalité de création de cyberscripts nécessite le pack Advanced Management.
- Pour utiliser toutes les fonctions de création de cyber-scripts, comme la modification ou l'exécution de scripts, la création de plans de création de scripts, etc., vous devez activer l'authentification à deux facteurs pour votre compte.

Limites

- Les langages de script suivants sont pris en charge :
  - PowerShell
  - Bash
- Les opérations de création de scripts ne peuvent être exécutées que sur les ordinateurs cibles sur lesquels un agent de protection est installé.

Plates-formes prises en charge

Cyber Scripting est disponible pour les ressources Windows et macOS.

Le tableau suivant résume les versions prises en charge.

Système d'exploitation	Version
Windows	Windows 7 SP1 et versions ultérieures - toutes les éditions
	Windows 8/8.1 – toutes les éditions (x86, x64), sauf les éditions Windows RT
	Windows 10 - éditions Home, Pro, Education, Enterprise, IoT Enterprise
	Windows 11
	Windows Server 2008 R2 SP1 et versions ultérieures - éditions Standard, Enterprise, Datacenter, Foundation et Web
	Windows Server 2012/2012 R2 – toutes les éditions
	Windows Server 2016
	Windows Server 2019
	Windows Server 2022
	Windows Storage Server (2008 R2, 2012, 2012 R2, 2016)
macOS	macOS Mojave 10.14
	macOS Catalina 10.15
	macOS Big Sur 11
	macOS Monterey 12

Rôles d'utilisateur et droits de création de cyber-scripts

Les actions disponibles avec les scripts et les plans de création de scripts dépendent de l'état du script et de votre rôle d'utilisateur.

Les administrateurs peuvent gérer les objets dans leur propre tenant et dans ses tenants enfants. Ils ne peuvent pas voir les objets disponibles dans un niveau d'administration plus élevé (le cas échéant), ni y accéder.

Les administrateurs de niveau inférieur n'ont qu'un accès en lecture seule aux plans de création de scripts appliqués à leurs ressources par un administrateur de niveau supérieur.

Les rôles suivants octroient des droits en matière de création de cyber-scripts :

- **Administrateur d'entreprise**
  Ce rôle octroie des droits d'administrateur complets dans tous les services. Concernant la création de cyber-scripts, il octroie les mêmes droits que le rôle Cyberadministrateur.
- **Cyberadministrateur**
  Ce rôle octroie des autorisations complètes, y compris l'approbation des scripts qui peuvent être utilisés dans le tenant, et la capacité à exécuter des scripts avec l'état **Test**.

- **Administrateur**
  Ce rôle octroie des autorisations partielles, avec la capacité d'exécuter des scripts approuvés, ainsi que de créer et d'exécuter des plans de création de scripts qui utilisent des scripts approuvés.
- **Administrateur en lecture seule**
  Ce rôle octroie des autorisations limitées, avec la capacité de visualiser les scripts et les plans de protection utilisés dans le tenant.
- **Utilisateur**
  Ce rôle octroie des autorisations partielles, avec la capacité d'exécuter des scripts approuvés, ainsi que de créer et d'exécuter des plans de création de scripts qui utilisent des scripts approuvés, mais uniquement sur le propre ordinateur de l'utilisateur.

Le tableau suivant résume toutes les actions disponibles, en fonction de l'état du script et du rôle de l'utilisateur.

Rôle	Objet	État du script		
		Brouillon	**Test**	**Approuvé**
Cyberadministrateur **Administrateur d'entreprise**	Plan de création de script	Modifier (supprimer un brouillon de script d'un plan) Supprimer Retirer Désactiver Arrêter	Créer Modifier Appliquer Activer Exécuter Supprimer Retirer Désactiver Arrêter	Créer Modifier Appliquer Activer Exécuter Supprimer Retirer Désactiver Arrêter
	Script	Créer Modifier Modifier l'état Cloner Supprimer Annuler l'exécution	Créer Modifier Modifier l'état Exécuter Cloner Supprimer Annuler l'exécution	Créer Modifier Modifier l'état Exécuter Cloner Supprimer Annuler l'exécution
Administrateur	Plan de création de	Affichage	Affichage	Créer

Utilisateur (pour ses propres ressources)	script	Retirer Désactiver Arrêter	Annuler l'exécution	Modifier Appliquer Activer Exécuter Supprimer Retirer Désactiver Arrêter
	Script	Créer Modifier Cloner Supprimer Annuler l'exécution	Affichage Cloner Annuler l'exécution	Exécuter Cloner Annuler l'exécution
Administrateur en lecture seule	Plan de création de script	Affichage	Affichage	Affichage
	Script	Affichage	Affichage	Affichage

Scripts

Un script est un ensemble d'instructions interprétées lors de l'exécution et exécutées sur une machine cible. Les scripts offrent une solution pratique pour l'automatisation de tâches répétitives ou complexes.

Avec la création de cyberscripts, vous pouvez exécuter un script prédéfini ou créer un script personnalisé. Tous les scripts à votre disposition se trouvent dans **Gestion** > **Référentiel de scripts**. Les scripts prédéfinis se trouvent dans la section **Bibliothèque**. Les scripts que vous avez créés ou clonés sur votre tenant se trouvent dans la section **Mes scripts**.

Vous pouvez utiliser un script en l'incluant dans un plan de création de scripts ou en lançant une opération **Exécution rapide du script**.

Remarque
Vous ne pouvez utiliser que des scripts approuvés, créés ou clonés dans votre tenant. Si un script a été supprimé du référentiel de scripts ou est en état de **brouillon**, il ne s'exécutera pas. Vous pouvez vérifier les détails d'une opération de script ou l'annuler dans **Surveillance** > **Activités**.

Le tableau suivant fournit plus d'informations sur les actions possibles avec un script en fonction de son statut.

Statut	Actions possibles
Brouillon	Les nouveaux scripts que vous créez et ceux que vous clonez dans votre référentiel ont le statut de **brouillon**. Vous n'êtes pas autorisé à exécuter ces scripts ni à les inclure dans des plans de script.
Test	Les administrateurs ayant le rôle de **cyberadministrateur** peuvent exécuter ces scripts et les inclure dans les plans de script.
Approuvé	Vous pouvez exécuter ces scripts et les inclure dans des plans de script.

Seuls les administrateurs ayant le rôle de **cyberadministrateur** peuvent modifier le statut d'un script ou supprimer un script approuvé. Pour plus d'informations, voir "Modification de l'état du script" (p. 255).

Création d'un script

Vous pouvez créer un script en écrivant le code manuellement.

Créer un script

1. Dans la console Cyber Protect, accédez à **Gestion** > **Référentiel de scripts**.
2. Dans **Mes scripts**, cliquez sur **Créer un script à l'aide de l'intelligence artificielle**.
3. Dans le volet principal, écrivez le corps du script.

   Important
   Lorsque vous créez un script, incluez des vérifications de code de sortie pour chaque opération. Dans le cas contraire, l'échec d'une opération pourrait être ignoré et l'état d'activité de création de script dans **Surveillance** > **Activités** pourrait indiquer **Succès** alors que cela n'est pas le cas.

4. Spécifiez les paramètres de script.

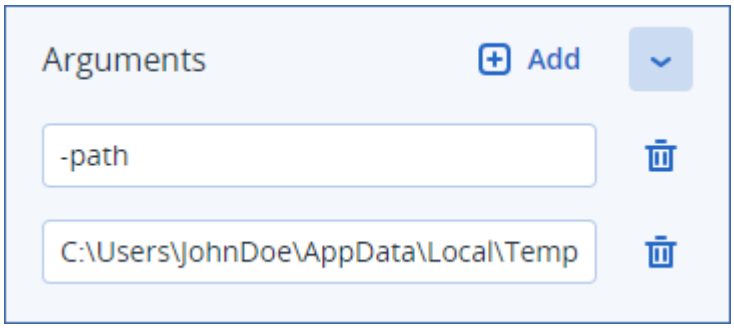
Paramètre	Description
Nom du script	Nom du script. Le champ est rempli automatiquement, mais vous pouvez en modifier la valeur.
Description	Description du script. Ce paramètre est facultatif. [Pour les scripts générés par l'intelligence artificielle] Le champ sera rempli automatiquement lors de la génération du script. Vous pouvez modifier la description fournie par l'intelligence artificielle.
Langue	Langage du script. Les valeurs disponibles sont les suivantes : • **PowerShell**. Il s'agit de la valeur par défaut. • **Bash** [Pour les scripts générés par l'intelligence artificielle] Ce paramètre est configuré

Paramètre	Description
	avant la génération du script.
Système d'exploitation	Système d'exploitation installé sur la ressource cible sur laquelle le script sera exécuté. Les valeurs disponibles sont les suivantes : • **Windows**. Il s'agit de la valeur par défaut. • **macOS** [Pour les scripts générés par l'intelligence artificielle] Ce paramètre est configuré avant la génération du script.
Statut	État du script. • **Brouillon**. Il s'agit de la valeur par défaut. Les nouveaux scripts que vous créez et ceux que vous clonez dans votre référentiel sont à l'état de **Brouillon**. Vous n'êtes pas autorisé à exécuter des scripts **Brouillons** ni à les inclure dans des plans de script. • **Test**. Seuls les administrateurs ayant le rôle de **cyberadministrateur** peuvent changer le statut d'un script en **Test**, exécuter des scripts avec ce statut **Test** et des plans de script avec ces scripts. • **Approuvé**. Vous pouvez exécuter des scripts **approuvés** et les inclure dans des plans de script. Seuls les administrateurs ayant le rôle de **cyberadministrateur** peuvent modifier le statut d'un script ou supprimer un script approuvé. Pour plus d'informations, voir "Modification de l'état du script" (p. 255).
Balises	Les mots-clés ne sont pas sensibles à la casse et peuvent compter jusqu'à 32 caractères. Vous ne pouvez utiliser ni parenthèses, ni crochets, ni virgules, ni espaces. Ce paramètre est facultatif. [Pour les scripts générés par l'intelligence artificielle] La balise **générée par l'intelligence artificielle** est ajoutée automatiquement lors de la génération du script. Vous pouvez la supprimer manuellement ou en ajouter d'autres.

5. [Uniquement pour les scripts qui nécessitent des identifiants] Spécifiez les identifiants.
   Vous pouvez utiliser un identifiant unique (par exemple, un jeton) ou une paire d'identifiants (par exemple, un nom d'utilisateur et un mot de passe).
6. [Uniquement pour les scripts qui nécessitent des arguments] Spécifiez les arguments et leurs valeurs, comme suit :
   a. Cliquez sur **Ajouter**.
   b. Dans le champ **Ajouter des arguments**, indiquez l'argument.
   c. Cliquez sur **Ajouter**.
   d. Dans le deuxième champ qui apparaît, indiquez la valeur de l'argument.

Remarque
Vous ne pouvez spécifier que les arguments que vous avez déjà définis dans le corps du script.

Par exemple :



e. Répétez les étapes ci-dessus si vous avez besoin d'ajouter plusieurs arguments.

7. Cliquez sur **Enregistrer**.

Le script est enregistré dans votre référentiel avec le statut **Brouillon**.

Vous ne pouvez utiliser le script que lorsqu'un administrateur ayant le rôle de **cyberadministrateur** a changé son statut en **Approuvé**. Pour plus d'informations, voir "Modification de l'état du script" (p. 255).

Pour utiliser un script dans un autre tenant que vous gérez, vous devez cloner ce script dans ce tenant. Pour plus d'informations, voir "Clonage d'un script" (p. 253).

Création d'un script à l'aide de l'intelligence artificielle

Remarque
Cette fonctionnalité nécessite le pack Advanced Management.

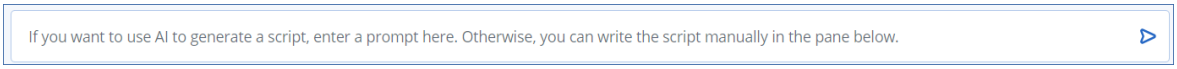
Vous pouvez utiliser l'intelligence artificielle pour transformer les invites en scripts puissants, ce qui vous permet d'économiser du temps et des efforts. Vous pouvez utiliser cette fonctionnalité des manières suivantes :

- Saisissez une invite pour demander à l'intelligence artificielle de créer un script de toutes pièces.
- Saisissez une invite pour demander à l'intelligence artificielle d'examiner et de compléter un code que vous avez saisi dans le corps du script. Vous pouvez utiliser cette fonction lorsque vous avez des difficultés avec des codes plus complexes.

Cette fonctionnalité utilise le modèle GPT-4 d'OpenAI. Vous pouvez l'utiliser pour créer pour votre organisation jusqu'à 100 scripts par mois calendaire, gratuitement.

Pour créer un script en utilisant l'intelligence artificielle

1. Dans la console Cyber Protect, accédez à **Gestion** > **Référentiel de scripts**.
2. Dans **Mes scripts**, cliquez sur **Créer un script à l'aide de l'intelligence artificielle**.
3. Dans l'invite, entrez une description de l'opération que le script doit effectuer. Veillez à ce que la description que vous saisissez soit aussi claire et détaillée que possible.

   Par exemple :

   ```
   I need a script that deletes Temporary files for all users (including user profiles +
   Windows Temps) and disable Windows Update Service to allow the script to run
   ```

4. Dans l'invite, cliquez sur le bouton fléché.
5. Dans la fenêtre de confirmation, sélectionnez la langue et le système d'exploitation, puis cliquez sur **Générer**.

   Le script généré par l'intelligence artificielle s'affiche dans le volet principal. Le nom et la description du script sont automatiquement générés par l'intelligence artificielle afin qu'ils correspondent au script. La balise **Généré par l'intelligence artificielle** est automatiquement attribuée au script.
6. Examinez le script généré par l'intelligence artificielle et, si nécessaire, modifiez-le manuellement.
7. Si nécessaire, modifiez les paramètres du script.

Paramètre	Description
Nom du script	Nom du script. Le champ est rempli automatiquement, mais vous pouvez en modifier la valeur.
Description	Description du script. Ce paramètre est facultatif. [Pour les scripts générés par l'intelligence artificielle] Le champ sera rempli automatiquement lors de la génération du script. Vous pouvez modifier la description fournie par l'intelligence artificielle.
Langue	Langage du script. Les valeurs disponibles sont les suivantes : • **PowerShell**. Il s'agit de la valeur par défaut. • **Bash** [Pour les scripts générés par l'intelligence artificielle] Ce paramètre est configuré

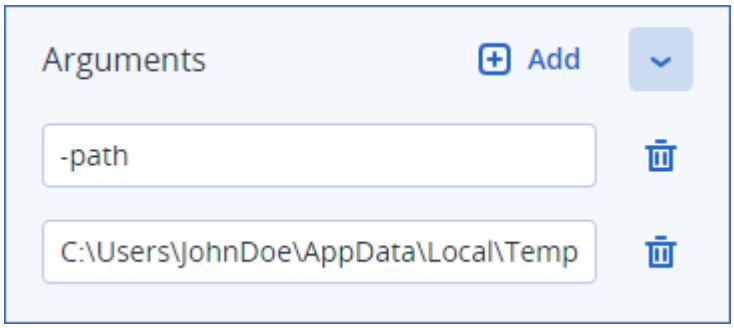
Paramètre	Description
	avant la génération du script.
Système d'exploitation	Système d'exploitation installé sur la ressource cible sur laquelle le script sera exécuté. Les valeurs disponibles sont les suivantes : • **Windows**. Il s'agit de la valeur par défaut. • **macOS** [Pour les scripts générés par l'intelligence artificielle] Ce paramètre est configuré avant la génération du script.
Statut	État du script. • **Brouillon**. Il s'agit de la valeur par défaut. Les nouveaux scripts que vous créez et ceux que vous clonez dans votre référentiel sont à l'état de **Brouillon**. Vous n'êtes pas autorisé à exécuter des scripts **Brouillons** ni à les inclure dans des plans de script. • **Test**. Seuls les administrateurs ayant le rôle de **cyberadministrateur** peuvent changer le statut d'un script en **Test**, exécuter des scripts avec ce statut **Test** et des plans de script avec ces scripts. • **Approuvé**. Vous pouvez exécuter des scripts **approuvés** et les inclure dans des plans de script. Seuls les administrateurs ayant le rôle de **cyberadministrateur** peuvent modifier le statut d'un script ou supprimer un script approuvé. Pour plus d'informations, voir "Modification de l'état du script" (p. 255).
Balises	Les mots-clés ne sont pas sensibles à la casse et peuvent compter jusqu'à 32 caractères. Vous ne pouvez utiliser ni parenthèses, ni crochets, ni virgules, ni espaces. Ce paramètre est facultatif. [Pour les scripts générés par l'intelligence artificielle] La balise **générée par l'intelligence artificielle** est ajoutée automatiquement lors de la génération du script. Vous pouvez la supprimer manuellement ou en ajouter d'autres.

8. [Facultatif] [Uniquement pour les scripts qui nécessitent des identifiants] Spécifiez les identifiants.

   Vous pouvez utiliser un identifiant unique (par exemple, un jeton) ou une paire d'identifiants (par exemple, un nom d'utilisateur et un mot de passe).
9. [Uniquement pour les scripts qui nécessitent des arguments] Spécifiez les arguments et leurs valeurs, comme suit :
   a. Cliquez sur **Ajouter**.
   b. Dans le champ **Ajouter des arguments**, indiquez l'argument.
   c. Cliquez sur **Ajouter**.
   d. Dans le deuxième champ qui apparaît, indiquez la valeur de l'argument.

Remarque
Vous ne pouvez spécifier que les arguments que vous avez déjà définis dans le corps du script.

Par exemple :



e. Répétez les étapes ci-dessus si vous avez besoin d'ajouter plusieurs arguments.

10. Cliquez sur **Enregistrer**.

    Le script est enregistré dans votre référentiel avec le statut **Brouillon**.

    Vous ne pouvez utiliser le script que lorsqu'un administrateur ayant le rôle de **cyberadministrateur** a changé son statut en **Approuvé**. Pour plus d'informations, voir "Modification de l'état du script" (p. 255).

    Pour utiliser un script dans un autre tenant que vous gérez, vous devez cloner ce script dans ce tenant. Pour plus d'informations, voir "Clonage d'un script" (p. 253).

Clonage d'un script

Le clonage d'un script est nécessaire dans les cas suivants :

- Avant d'utiliser un script de la **bibliothèque**. Dans ce cas, vous devez d'abord cloner le script dans la section **Mes scripts**.
- Quand vous souhaitez cloner des scripts que vous avez créé dans un tenant parent dans ses tenants ou unités enfant.

Cloner un script

1. Dans **Référentiel de scripts**, trouvez le script que vous souhaitez cloner.
2. Effectuez l'une des actions suivantes :

- [Si vous clonez un script depuis **Mes scripts**] Cliquez sur les points de suspension (...) situés à côté du nom du script, puis cliquez sur **Cloner**.
- [Si vous clonez un script depuis **Bibliothèque**] Cliquez sur **Cloner** à côté du nom du script que vous avez sélectionné.

3. Dans la fenêtre contextuelle **Cloner le script**, sélectionnez l'un des états de script suivants dans la liste déroulante **État** :
   - **Brouillon** (par défaut) : ce statut ne vous permet pas d'exécuter le script immédiatement.
   - **Test** : ce statut vous permet d'exécuter le script.
   - **Approuvé** : ce statut vous permet d'exécuter le script.
4. [Si vous gérez plusieurs tenants ou unités] Sélectionnez l'emplacement où vous souhaitez cloner le script.
   Dans la boîte de dialogue **Cloner le script**, vous voyez uniquement les tenants que vous pouvez gérer et sur lesquels le pack Advanced Management est appliqué.

Le script est alors cloné dans la section **Mes scripts** du tenant ou de l'unité que vous avez sélectionné. Si vous gérez un seul tenant ne comportant aucune unité, le script est automatiquement copié dans votre section **Mes scripts**.

Important
Les identifiants qu'un script utilise ne sont pas copiés lorsque vous clonez un script vers un tenant autre que le tenant d'origine.

Modification ou suppression d'un script

Remarque
En fonction de votre rôle, vous pouvez effectuer des opérations différentes sur les scripts et les plans de script. Pour plus d'informations sur les rôles, voir "Rôles d'utilisateur et droits de création de cyber-scripts" (p. 245).

Modifier un script

1. Dans **Référentiel de scripts**, accédez à **Mes scripts**, puis trouvez le script que vous souhaitez modifier.
2. Cliquez sur les points de suspension (...) situés à côté du nom du script, puis cliquez sur **Modifier**.
3. Modifiez le script, puis cliquez sur **Enregistrer**.
4. [Si vous modifiez un script utilisé par un plan de création de scripts] Confirmez votre choix en cliquant sur **Enregistrer le script**.

   Remarque
   La dernière version du script sera utilisée lors de la prochaine exécution du plan de création de scripts.

Versions du script

Une nouvelle version du script est créée si vous modifiez l'un des attributs de script suivants :

- corps du script
- nom du script
- description
- langage de script
- informations d'identification
- arguments

Si vous modifiez d'autres attributs, vos modifications seront ajoutées à la version du script actuelle. Pour en savoir plus sur les versions et sur la manière de les comparer, reportez-vous à "Comparaison de versions de script" (p. 256).

Remarque
L'état du script est mis à jour uniquement lorsque vous modifiez la valeur du champ **État**. Seuls les administrateurs disposant du rôle Cyberadministrateur peuvent modifier l'état d'un script.

Supprimer un script

1. Dans **Référentiel de scripts**, accédez à **Mes scripts**, puis trouvez le script que vous souhaitez supprimer.
2. Cliquez sur les points de suspension (...) situés à côté du nom du script, puis cliquez sur **Supprimer**.
3. Cliquez sur **Supprimer**.
4. [Si vous souhaitez modifier un script utilisé par un plan de création de scripts] Confirmez votre choix en cliquant sur **Enregistrer le script**.

   Remarque
   Les plans de création de scripts qui utilisent le script supprimé ne s'exécuteront plus.

Modification de l'état du script

Un nouveau script créé et se trouvant dans l'état **Brouillon** ne peut pas être utilisé tant que son statut n'est pas passé à **Approuvé**. Selon le cas d'utilisation, un script peut rester dans l'état **Test** pendant un certain temps avant d'être approuvé.

Remarque
En fonction de votre rôle, vous pouvez effectuer des opérations différentes sur les scripts et les plans de script. Pour plus d'informations sur les rôles, voir "Rôles d'utilisateur et droits de création de cyber-scripts" (p. 245).

Prérequis

- Votre utilisateur est un administrateur auquel a été attribué le rôle de **cyberadministrateur**.
- Un script avec l'état correspondant est disponible.

Modifier l'état du script

1. Dans le **référentiel de scripts**, accédez à **Mes scripts**.
2. Cliquez sur les points de suspension (...) situés à côté du nom du script, puis cliquez sur **Modifier**.
3. Dans la liste déroulante **Statut**, sélectionnez le statut.
4. Cliquez sur **Enregistrer**.
5. [Si vous modifiez le statut d'un script approuvé] Pour confirmer la modification, cliquez sur **Enregistrer le script**.

> **Remarque**
> Si l'état du script a été modifié et défini sur **Brouillon**, les plans de création de scripts qui l'utilisent ne s'exécuteront plus.
>
> Seuls les administrateurs ayant le rôle de **cyberadministrateur** peuvent exécuter des scripts dans l'état de **test** et des plans de script avec de tels scripts.

Comparaison de versions de script

Vous pouvez comparer deux versions d'un script et rétablir une version précédente de ce dernier. Vous pouvez également vérifier qui a créé une version spécifique et quand cela a été fait.

Comparer des versions de script

1. Dans **Référentiel de scripts**, accédez à **Mes scripts**, puis trouvez le script dont vous souhaitez comparer les versions.
2. Cliquez sur les points de suspension (...) situés à côté du nom du script, puis cliquez sur **Historique des versions**.
3. Sélectionnez deux versions à comparer, puis cliquez sur **Comparer les versions**.
   Toute modification apportée au corps de texte du script, à ses arguments ou aux identifiants est mise en évidence.

Pour rétablir une version précédente

1. Dans la fenêtre **Comparer les versions de script**, cliquez sur **Rétablir à cette version**.
2. Dans la fenêtre contextuelle **Revenir à une version antérieure**, sélectionnez l'état du script dans la liste déroulante **État**.

La version sélectionnée est restaurée et enregistrée en tant que version la plus récente dans l'historique des versions.

Pour restaurer un script, vous pouvez également sélectionner une version dans la fenêtre **Historique des versions**, puis cliquer sur le bouton **Restaurer**.

Important
Vous ne pouvez exécuter que des scripts dont le statut est **Test** ou **Approuvé**. Pour plus d'informations, voir "Modification de l'état du script" (p. 255).

Télécharger le résultat d'une opération de création de scripts

Vous pouvez télécharger le résultat d'une opération de création de scripts sous forme de fichier .zip. Elle contient deux fichiers texte : `stdout` et `stderr`. Dans `stdout`, vous pouvez afficher les résultats d'une opération de création de scripts réussie. Le fichier `stderr` contient des informations sur les erreurs qui se sont produites lors de l'opération de création de scripts.

Télécharger le fichier de résultat

1. Dans la console Cyber Protect, accédez à **Surveillance** > **Activités**.
2. Cliquez sur l'activité de création de cyber-scripts dont vous souhaitez télécharger le résultat.
3. À l'écran **Détails de l'activité**, cliquez sur **Télécharger le résultat**.

Référentiel de scripts

Le référentiel de scripts se trouve dans l'onglet **Gestion**. Dans le référentiel, vous pouvez rechercher des scripts à l'aide de leur nom ou de leur description. Vous pouvez aussi utiliser les filtres, ou trier les scripts en fonction de leur nom ou de leur état.

Pour gérer un script, cliquez sur les points de suspension (...) situés à côté de son nom, puis sélectionnez l'action souhaitée. Vous pouvez aussi cliquer sur le script, puis vous servir des boutons présents sur l'écran qui apparaît.

Le référentiel de scripts doit contenir les sections suivantes :

- **Mes scripts**
  Vous y trouverez les scripts que vous pouvez utiliser directement dans votre environnement. Il s'agit des scripts que vous avez créés à partir de zéro et des scripts que vous avez clonés ici.
  Vous pouvez filtrer les scripts de cette section en fonction des critères suivants :
  - Mots-clés
  - Statut
  - Langue
  - Système d'exploitation
  - Propriétaire du script
- **Bibliothèque**

La bibliothèque contient des scripts prédéfinis que vous pouvez utiliser dans votre environnement après les avoir clonés dans la section **Mes scripts**. Vous pouvez uniquement inspecter et cloner ces scripts.

Vous pouvez filtrer les scripts de cette section en fonction des critères suivants :

- Mots-clés
- Langue
- Système d'exploitation

Pour plus d'informations, voir Scripts approuvés par le fournisseur (70595).

Plans de création de scripts

Un plan de création de scripts vous permet d'exécuter un script sur plusieurs ressources, de planifier l'exécution d'un script et de configurer des paramètres supplémentaires.

Les plans de création de scripts que vous avez créés et ceux appliqués à vos ressources sont disponibles dans **Gestion** > **Plans de création de scripts**. Ici, vous pouvez consulter le propriétaire ou l'état du plan, ainsi que son emplacement d'exécution.

Une barre sur laquelle vous pouvez cliquer affiche les états à code couleur suivants pour les plans de création de scripts :

- En cours d'exécution (bleu)
- Vérification de la compatibilité (gris foncé)
- Désactivé (gris clair)
- OK (verte)
- Alerte critique (rouge)
- Erreur (orange)
- Avertissement (jaune)

En cliquant sur la barre d'état, vous pouvez afficher l'état d'un plan et sur combien de ressources il s'applique. Il est également possible de cliquer sur chaque état.

Dans l'onglet **Plans de création de scripts**, vous pouvez gérer les plans en effectuant les actions suivantes :

- Exécuter
- Arrêter
- Modifier
- Renommer
- Désactiver
- Activer
- Cloner

- Exporter. La configuration du plan sera exportée au format JSON vers la machine locale.
- Supprimer

La visibilité d'un plan de création de scripts et des actions disponibles avec lui dépend du propriétaire du plan et de votre rôle d'utilisateur. Par exemple, les administrateurs d'entreprise ne peuvent voir que les plans de création de scripts appartenant au partenaire et appliqués à leurs ressources. Ils ne peuvent effectuer aucune action sur ces plans.

Pour plus d'informations sur les personnes autorisées à créer et à gérer des plans de création de scripts, reportez-vous à "Rôles d'utilisateur et droits de création de cyber-scripts" (p. 245).

Gérer un plan de création de scripts

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de création de scripts**.
2. Trouvez le plan que vous souhaitez gérer, puis cliquez sur les points de suspension (...) correspondants.
3. Sélectionnez l'action souhaitée, puis suivez les instructions à l'écran.

Création d'un plan de création de scripts

Vous pouvez créer un plan de création de scripts de l'une des manières suivantes :

- Dans l'onglet **Terminaux**
  Sélectionnez des ressources, puis créez un plan de création de scripts pour elles.
- Dans l'onglet **Gestion** > **Plans de création de scripts**
  Créez un plan de création de scripts, puis sélectionnez les ressources auxquelles l'appliquer.

Créer un plan de création de scripts dans l'onglet Terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Sélectionnez les ressources ou les groupes de terminaux auxquels vous souhaitez appliquer un plan de création de scripts, puis cliquez respectivement sur **Protection** ou **Protéger un groupe**.
3. [Si des plans sont déjà appliqués] Cliquez sur **Ajouter un plan**.
4. Cliquez sur **Création d'un plan** > **Plan de création de scripts**.
   Un modèle pour le plan de création de scripts s'ouvre.
5. [Facultatif] Pour modifier le nom du plan de création de scripts, cliquez sur l'icône en forme de crayon.
6. Cliquez sur **Choisir le script**, sélectionnez le script que vous souhaitez utiliser, puis cliquez sur **Terminé**.

   Remarque
   Vous ne pouvez utiliser que vos scripts approuvés dans **Référentiel de scripts** >**Mes scripts**. Seul un administrateur ayant le rôle de **cyberadministrateur** peut utiliser des scripts à l'état de **Test**. Pour plus d'informations sur les rôles, voir "Rôles d'utilisateur et droits de création de cyber-scripts" (p. 245).

7. Configurez la planification et les conditions de démarrage pour le plan de création de scripts.
8. Choisissez le compte dans le cadre duquel le script s'exécutera sur la ressource cible. Les options suivantes sont disponibles :
   - Compte système (sous macOS, il s'agit du compte racine)
   - Compte actuellement connecté
9. Spécifiez la durée pendant laquelle le script peut s'exécuter sur la ressource cible.
   Si l'exécution du script ne peut se terminer dans le délai défini, l'opération de création de cyber-scripts échouera.
   Les valeurs minimale et maximale que vous pouvez spécifier sont respectivement une et 1 440 minutes.
10. [Uniquement pour les scripts PowerShell] Configurez la règle d'exécution PowerShell.
    Pour en savoir plus sur cette règle, reportez-vous à la documentation Microsoft.
11. Cliquez sur **Créer**.

Créer un plan de création de scripts dans l'onglet Plans de création de scripts

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de création de scripts**.
2. Cliquez sur **Création d'un plan**.
   Un modèle pour le plan de création de scripts s'ouvre.
3. [Facultatif] Pour sélectionner les ressources ou les groupes de terminaux auxquels appliquer le nouveau plan, cliquez sur **Ajouter des ressources**.
   a. Cliquez sur **Machines avec des agents** pour développer la liste, puis sélectionnez les ressources ou les groupes de terminaux de votre choix.
   b. Cliquez sur **Ajouter**.

   Pour en savoir plus sur la création de groupes de terminaux au niveau partenaire, reportez-vous à "Onglet Terminaux" (p. 336).

   Remarque
   Vous pouvez aussi sélectionner des ressources ou des groupes de terminaux après avoir créé le plan.

4. [Facultatif] Pour modifier le nom du plan de création de scripts, cliquez sur l'icône en forme de crayon.
5. Cliquez sur **Choisir le script**, sélectionnez le script que vous souhaitez utiliser, puis cliquez sur **Terminé**.

   Remarque
   Vous ne pouvez utiliser que vos scripts approuvés dans **Référentiel de scripts** >**Mes scripts**. Seul un administrateur ayant le rôle de **cyberadministrateur** peut utiliser des scripts à l'état de **Test**. Pour plus d'informations sur les rôles, voir "Rôles d'utilisateur et droits de création de cyber-scripts" (p. 245).

6. Configurez la planification et les conditions de démarrage pour le plan de création de scripts.
7. Choisissez le compte dans le cadre duquel le script s'exécutera sur la ressource cible. Les options suivantes sont disponibles :
   - Compte système (sous macOS, il s'agit du compte racine)
   - Compte actuellement connecté
8. Spécifiez la durée pendant laquelle le script peut s'exécuter sur la ressource cible.
   Si l'exécution du script ne peut se terminer dans le délai défini, l'opération de création de cyber-scripts échouera.
   Les valeurs minimale et maximale que vous pouvez spécifier sont respectivement une et 1 440 minutes.
9. [Uniquement pour les scripts PowerShell] Configurez la règle d'exécution PowerShell.
   Pour en savoir plus sur cette règle, reportez-vous à la documentation Microsoft.
10. Cliquez sur **Créer**.

Planification et conditions de démarrage

Planification

Vous pouvez configurer un plan de création de scripts pour qu'il soit exécuté une seule fois ou de façon répétée, et pour qu'il démarre en fonction d'une planification ou qu'il soit déclenché par un certain événement.

Les options suivantes sont disponibles :

- Ex. une fois
  Pour cette option, vous devez configurer la date et l'heure d'exécution du plan.
- Planifier selon l'horaire
  Avec cette option, vous pouvez configurer des plans de création de scripts qui s'exécutent toutes les heures, tous les jours ou tous les mois.
  Pour que la planification ne soit effective que temporairement, cochez la case **Exécuter sur une plage de dates**, puis configurez la période pendant laquelle le plan planifié sera exécuté.
- Lorsque l'utilisateur se connecte au système
  Vous pouvez choisir si un utilisateur spécifique ou n'importe quel utilisateur qui se connecte déclenche le plan de création de scripts.
- Lorsqu'un utilisateur se déconnecte du système
  Vous pouvez choisir si un utilisateur spécifique ou n'importe quel utilisateur qui se déconnecte déclenche le plan de création de scripts.
- Au démarrage du système
- Lorsque le système est arrêté

Remarque
Cette option de planification ne fonctionne qu'avec les scripts qui s'exécutent dans le compte système.

- Lorsque le système est en ligne

Conditions de démarrage

Les conditions de démarrage ajoutent plus de flexibilité à vos plans planifiés. Si vous configurez plusieurs conditions, toutes devront être remplies simultanément pour que le plan puisse démarrer.

Les conditions de démarrage ne sont pas effectives si vous exécutez le plan manuellement à l'aide de l'option **Exécuter maintenant**.

Condition	Description
Exécuter uniquement si la ressource est en ligne	Le script s'exécutera lorsque la ressource cible sera connectée à Internet.
L'utilisateur est inactif	Cette condition est remplie lorsqu'un écran de veille s'exécute sur l'ordinateur ou si l'ordinateur est verrouillé.
Utilisateur déconnecté	Avec cette condition, vous pouvez reporter un plan de création de scripts planifié jusqu'à ce que l'utilisateur de la ressource cible se déconnecte.
Compris dans un intervalle de temps	Avec cette condition, un plan de création de scripts ne peut démarrer que dans un intervalle de temps spécifié. Par exemple, vous pouvez utiliser cette condition pour limiter la condition **L'utilisateur est déconnecté**.
Économiser de la batterie	Avec cette condition, vous pouvez vous assurer que le plan de création de scripts ne sera pas interrompu en raison d'une batterie faible. Les options suivantes sont disponibles : • Ne pas démarrer lors d'une alimentation sur batterie Le plan démarrera uniquement si l'ordinateur est connecté à une source d'alimentation. • Démarrer pendant l'alimentation sur batterie si le niveau de batterie est supérieur à Le plan démarrera si l'ordinateur est connecté à une source d'alimentation ou si le niveau de batterie est supérieur à la valeur spécifiée.
Ne pas démarrer pendant une connexion mesurée	Cette condition empêche le démarrage du plan si la ressource cible accède à Internet via une connexion mesurée.
Ne pas démarrer pendant une connexion aux réseaux Wi-Fi	Cette condition empêche le démarrage du plan si la ressource cible est connectée à l'un des réseaux sans fil spécifiés. Pour utiliser cette condition, vous devez spécifier le SSID du réseau interdit.

Condition	Description
suivants	La restriction s'applique à tous les réseaux qui contiennent le nom spécifié comme chaîne dans leur nom, quelle que soit la casse. Par exemple, si vous spécifiez `téléphone` comme nom de réseau, le plan ne démarrera pas lorsque le terminal sera connecté à l'un des réseaux suivants : `Téléphone de John`, `téléphone_wifi` ou `mon_wifi_TÉLÉPHONE`.
Vérifier l'adresse IP du terminal	Cette condition empêche le démarrage du plan si l'une des adresses IP de la ressource cible se trouve au sein ou en dehors de la plage d'adresses IP spécifiée. Les options suivantes sont disponibles : • Démarrer si en dehors de la plage d'adresses IP • Démarrer si dans la plage d'adresses IP Prend en charge uniquement les adresses IPv4.
Si les conditions de démarrage ne sont pas remplies, exécutez quand même la tâche	Cette option vous permet de définir l'intervalle de temps après lequel le plan sera exécuté, quelles que soient les autres conditions. Le plan démarrera dès que les autres conditions seront remplies ou dès que la période spécifiée sera écoulée. Cette option n'est pas disponible si vous avez configuré le plan de création de scripts pour qu'il ne s'exécute qu'une seule fois.

Gestion des ressources cibles pour un plan

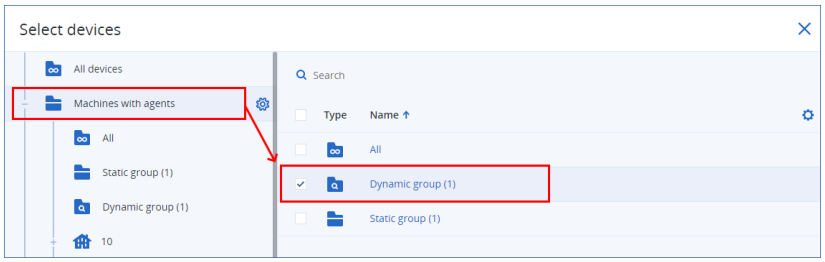
Vous pouvez sélectionner les ressources ou les groupes de terminaux auxquels vous souhaitez appliquer un plan de création de scripts au moment de la création du plan, ou ultérieurement.

Les administrateurs partenaires peuvent appliquer le même plan à des ressources de différents clients, et peuvent créer des groupes de terminaux qui peuvent contenir des ressources de différents clients. Pour apprendre à créer un groupe de terminaux statique ou dynamique au niveau partenaire, reportez-vous à "Onglet Terminaux" (p. 336).

Ajouter des ressources initiales à un plan

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de création de scripts**.
2. Cliquez sur le nom du plan pour lequel vous souhaitez spécifier des ressources cibles.
3. Cliquez sur **Ajouter des ressources**.
4. Sélectionnez les ressources ou les groupes de terminaux souhaités, puis cliquez sur **Ajouter**.

Remarque
Pour sélectionner un groupe de terminaux, cliquez sur son niveau parent, puis, dans le volet principal, cochez la case à côté de son nom.

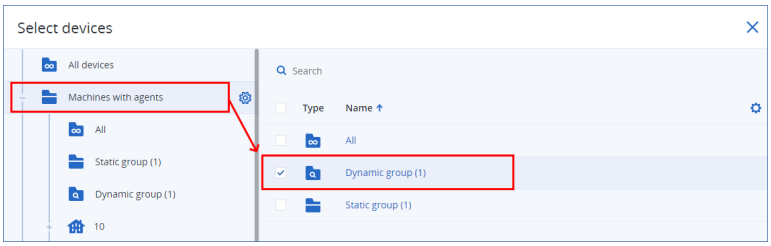


5. Pour enregistrer le plan modifié, cliquez sur **Enregistrer**.

Gérer les ressources existantes pour un plan

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de création de scripts**.
2. Cliquez sur le nom du plan dont vous souhaitez modifier les ressources cibles.
3. Cliquez sur **Gérer les ressources**.
   L'écran **Terminaux** répertorie les ressources auxquelles le plan de création de scripts est actuellement appliqué. Si vous gérez plusieurs tenants, les ressources sont classées par tenant.
   - Pour ajouter de nouvelles ressources ou de nouveaux groupes de terminaux, cliquez sur **Ajouter**.
     a. Sélectionnez les ressources ou les groupes de terminaux souhaités. Vous pouvez ajouter des ressources à partir de tous les tenants que vous gérez.

     Remarque
     Pour sélectionner un groupe de terminaux, cliquez sur son niveau parent, puis, dans le volet principal, cochez la case à côté de son nom.

     b. Cliquez sur **Ajouter**.
   - Pour supprimer des ressources ou des groupes de terminaux, sélectionnez-les, puis cliquez sur **Supprimer**.
4. Cliquez sur **Valider**.
5. Pour enregistrer le plan modifié, cliquez sur **Enregistrer**.

Plans dans les différents niveaux d'administration

Le tableau suivant résume les plans que les administrateurs de différents niveaux peuvent voir et gérer.

Administrateur	Niveau d'administration	Plans	Droits
Administrateur partenaire	Niveau partenaire	Propres plans	Accès complet
		Plans clients (y compris les plans dans les unités)	Accès complet
		Plans d'unité	Accès complet
	Niveau client (pour les clients gérés par le fournisseur de services)	Plans partenaires appliqués aux ressources de ce client	Lecture seule
		Plans clients (y compris les plans dans les unités)	Accès complet
		Plans d'unité	Accès complet
	Niveau unité (pour les clients gérés par le fournisseur de services)	Plans partenaires appliqués aux ressources de cette unité	Lecture seule
		Plans clients appliqués aux ressources de cette unité	Lecture seule
		Plans d'unité	Accès complet
Administrateur d'entreprise	Niveau client	Plans partenaires appliqués aux ressources de ce client ou de cette unité	Lecture seule
		Plans clients (y compris les plans dans les unités)	Accès complet
		Plans d'unité	Accès complet
	Niveau unité	Plans partenaires appliqués aux ressources de cette unité	Lecture seule
		Plans clients appliqués aux ressources de cette unité	Lecture seule
		Plans d'unité	Accès complet

Administrateur	Niveau d'administration	Plans	Droits
Administrateur de l'unité	Niveau unité	Plans partenaires appliqués aux ressources de cette unité	Lecture seule
		Plans clients appliqués aux ressources de cette unité	Lecture seule
		Plans d'unité	Accès complet

Important
Le propriétaire d'un plan est le tenant dans lequel le plan a été créé. Ainsi, si un administrateur partenaire a créé un plan au niveau du tenant client, le tenant client est le propriétaire de ce plan.

Problèmes de compatibilité avec les plans de script

Dans certains cas, l'application d'un plan de script sur une ressource peut provoquer des problèmes de compatibilité. Vous pouvez observer les problèmes de compatibilité suivants :

- Système d'exploitation incompatible : ce problème survient lorsque le système d'exploitation de la ressource n'est pas pris en charge.
- Agent non pris en charge : ce problème survient lorsque la version de l'agent de protection sur la ressource est obsolète et ne prend pas en charge la fonctionnalité Création de cyber-scripts.
- Quota insuffisant : ce problème survient lorsque le quota de service dans le tenant est insuffisant pour l'affectation aux ressources sélectionnées.

Si le plan de script est appliqué à 150 ressources sélectionnées au maximum, vous serez invité à résoudre les conflits existants avant d'enregistrer le plan. Pour résoudre un conflit, supprimez sa cause racine ou les ressources concernées du plan. Pour plus d'informations, voir "Résolution des problèmes de compatibilité avec les plans de script" (p. 266). Si vous enregistrez le plan sans résoudre les conflits, le plan sera désactivé automatiquement pour les ressources non prises en charge, et des alertes s'afficheront.

Si le plan de création de scripts est appliqué à plus de 150 ressources ou à des groupes de terminaux, il sera enregistré sans résolution préalable des conflits, puis sa compatibilité sera vérifiée. Le plan sera automatiquement désactivé pour les ressources incompatibles, et des alertes apparaîtront.

Résolution des problèmes de compatibilité avec les plans de script

Selon la cause des problèmes de compatibilité, vous pouvez effectuer différentes actions afin de résoudre ces problèmes dans le cadre du processus de création d'un nouveau plan de script.

Remarque
Lors de la résolution d'un problème de compatibilité par suppression de ressources d'un plan, vous ne pouvez pas supprimer les ressources faisant partie d'un groupe de terminaux.

Pour résoudre les problèmes de compatibilité

1. Cliquez sur **Examiner les problèmes**.
2. [Pour résoudre les problèmes de compatibilité avec des systèmes d'exploitation incompatibles]
   a. Dans l'onglet **Système d'exploitation incompatible**, sélectionnez les ressources que vous souhaitez supprimer.
   b. Cliquez sur **Supprimer les ressources du plan**.
   c. Cliquez sur **Supprimer**, puis sur **Fermer**.
3. [Pour résoudre les problèmes de compatibilité avec des agents non pris en charge par suppression de ressources du plan]
   a. Dans l'onglet **Agents non pris en charge**, sélectionnez les ressources que vous souhaitez supprimer.
   b. Cliquez sur **Supprimer les ressources du plan**.
   c. Cliquez sur **Supprimer**, puis sur **Fermer**.
4. [Pour résoudre les problèmes de compatibilité avec des agents non pris en charge grâce à la mise à jour de la version de l'agent] Cliquez sur **Accéder à la liste des agents**.

   Remarque
   Cette option est disponible uniquement pour les administrateurs clients.

5. [Pour résoudre les problèmes de compatibilité liés à un quota insuffisant par suppression de ressources du plan]
   a. Dans l'onglet **Quota insuffisant**, sélectionnez les ressources que vous souhaitez supprimer.
   b. Cliquez sur **Supprimer les ressources du plan**.
   c. Cliquez sur **Supprimer**, puis sur **Fermer**.
6. [Pour résoudre les problèmes de compatibilité liés à un quota insuffisant par augmentation du quota du tenant]

   Remarque
   Cette option est disponible uniquement pour les administrateurs partenaires.

   a. Dans l'onglet **Quota insuffisant**, cliquez sur **Accéder au portail de gestion**.
   b. Augmentez le quota de service du client.

Exécution rapide du script

Vous pouvez exécuter un script immédiatement, sans l'inclure dans un plan de script. Vous ne pouvez pas utiliser cette opération sur plus de 150 ressources, sur des ressources hors ligne ou dans des groupes de terminaux.

La ressource cible doit se voir affecter un quota de service qui prend en charge la fonctionnalité Exécution rapide du script, et le pack Advanced Management doit être activé pour son tenant. Un quota de service approprié sera automatiquement affecté s'il est disponible dans le tenant.

Remarque
Vous ne pouvez utiliser que vos scripts approuvés dans **Référentiel de scripts** >**Mes scripts**. Seul un administrateur ayant le rôle de **cyberadministrateur** peut utiliser des scripts à l'état de **Test**. Pour plus d'informations sur les rôles, voir "Rôles d'utilisateur et droits de création de cyber-scripts" (p. 245).

Vous pouvez lancer une exécution rapide de l'une des manières suivantes :

- Depuis l'onglet **Terminaux**
  Sélectionnez une ou plusieurs ressources, puis sélectionnez les scripts à exécuter sur cette ou ces dernières.
- Depuis l'onglet **Gestion** > **Référentiel de création de scripts**
  Sélectionnez un script, puis sélectionnez une ou plusieurs ressources cibles.

Exécuter un script depuis l'onglet Terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez la ressource sur laquelle vous souhaitez exécuter le script, puis cliquez sur **Protection**.
3. Cliquez sur **Exécution rapide du script**.
4. Cliquez sur **Choisir le script**, sélectionnez le script que vous souhaitez utiliser, puis cliquez sur **Terminé**.
5. Choisissez le compte dans le cadre duquel le script s'exécutera sur la ressource cible. Les options suivantes sont disponibles :
   - Compte système (sous macOS, il s'agit du compte racine)
   - Compte actuellement connecté
6. Spécifiez la durée pendant laquelle le script peut s'exécuter sur la ressource cible.
   Si l'exécution du script ne peut se terminer dans le délai défini, l'opération de cyber-script échouera.
   Vous pouvez utiliser des valeurs comprises entre 1 et 1 440 minutes.
7. [Uniquement pour les scripts PowerShell] Configurez la règle d'exécution PowerShell.
   Pour plus d'informations sur cette politique, voir la documentation de Microsoft.
8. Cliquez sur **Exécuter maintenant**.

Exécuter un script depuis l'onglet Référentiel de création de scripts

1. Dans la console Cyber Protect, accédez à **Gestion** > **Référentiel de création de scripts**.
2. Sélectionnez le script que vous souhaitez exécuter, puis cliquez sur **Exécution rapide du script**.

3. Cliquez sur **Ajouter des ressources** pour sélectionner les ressources cibles, puis cliquez sur **Ajouter**.
4. Cliquez sur **Choisir le script**, sélectionnez le script que vous souhaitez utiliser, puis cliquez sur **Terminé**.
5. Choisissez le compte dans le cadre duquel le script s'exécutera sur la ressource cible. Les options suivantes sont disponibles :
   - Compte système (sous macOS, il s'agit du compte racine)
   - Compte actuellement connecté
6. Spécifiez la durée pendant laquelle le script peut s'exécuter sur la ressource cible.
   Si l'exécution du script ne peut se terminer dans le délai défini, l'opération de cyber-script échouera.
   Vous pouvez utiliser des valeurs comprises entre 1 et 1 440 minutes.
7. [Uniquement pour les scripts PowerShell] Configurez la règle d'exécution PowerShell.
   Pour plus d'informations sur cette politique, voir la documentation de Microsoft.
8. Cliquez sur **Exécuter maintenant**.

Protection des applications de collaboration et de communication

Zoom, Cisco Webex Meetings, Citrix Workspace et Microsoft Teams sont désormais largement utilisés pour les communications et conférences Web et vidéo. Le service Cyber Protection vous permet de protéger vos outils de collaboration.

La configuration de la protection pour Zoom, Cisco Webex Meetings, Citrix Workspace et Microsoft Teams est similaire. Dans l'exemple ci-dessous, nous évoquerons la configuration de Zoom.

Pour configurer la protection pour Zoom

1. Installez l'agent de protection sur la machine sur laquelle l'application de collaboration est installée.
2. Connectez-vous à la console Cyber Protect et appliquez un plan de protection dans lequel l'un des modules suivants est activé :
   - **Protection contre les virus et les malwares** (avec les paramètres **Autoprotection** et **Active Protection** activés) – si vous possédez l'une des éditions Cyber Protect.
   - **Active Protection** (avec le paramètre **Autoprotection** activé) – si vous possédez l'une des éditions Cyber Backup.
3. [Facultatif] Pour l'installation automatique des mises à jour, configurez le module de **Gestion des correctifs** du plan de protection.

Par conséquent, votre application Zoom bénéficiera d'une protection qui inclut les activités suivantes :

- Installation automatique des mises à jour client de Zoom
- Protection des processus de Zoom contre les injections de code
- Protection contre des opérations suspectes par des processus de Zoom
- Protection des fichiers « hôtes » contre l'ajout de domaines liés à Zoom

Présentation de votre niveau de protection actuel

Surveillance

L'onglet **Surveillance** fournit des informations importantes concernant votre niveau de protection actuelle, et comprend les tableaux de bord suivants :

- **Vue d'ensemble**
- **Activités**
- **Alertes**
- **Flux de menaces** (pour plus d'informations, voir "Flux de menaces" (p. 316))

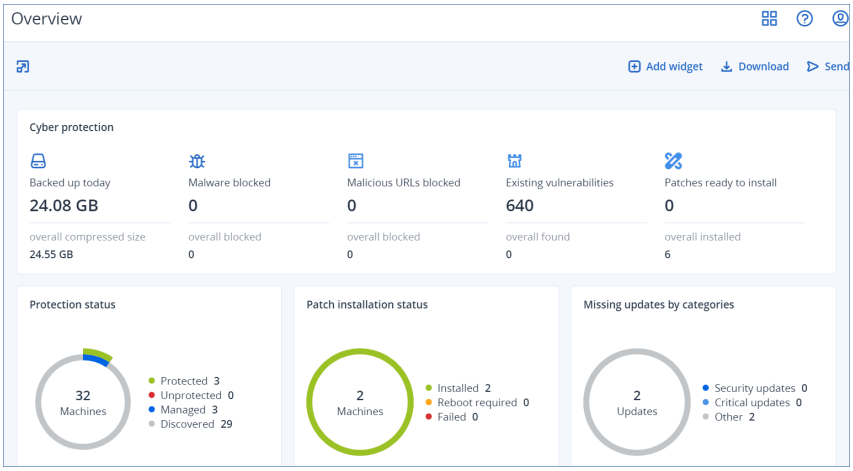
Tableau de bord Vue d'ensemble

Le tableau de bord **Vue d'ensemble** fournit un certain nombre de widgets personnalisables qui apporteront une vue d'ensemble des opérations liées au service Cyber Protection. Des widgets pour d'autres services seront disponibles dans les versions à venir.

Les widgets sont mis à jour toutes les cinq minutes. Les widgets disposent d'éléments sur lesquels cliquer qui permettent de faire des recherches sur les problèmes et de les résoudre. Vous pouvez télécharger l'état actuel du tableau de bord ou bien l'envoyer par courrier électronique au format .pdf et/ou .xlsx.

Vous pouvez faire un choix parmi de nombreux widgets se présentant sous la forme de tableaux, de diagrammes circulaires, de graphiques à barres, de listes et de cartes proportionnelles. Vous pouvez ajouter plusieurs widgets du même type en choisissant différents filtres.

Dans **Surveillance** > **Vue d'ensemble**, les boutons **Télécharger** et **Envoyer** ne sont pas disponibles dans les éditions Standard du service Cyber Protection.



Pour réorganiser les widgets sur le tableau de bord

Glissez-déplacez les widgets en cliquant sur leur nom.

Pour modifier un widget

Cliquez sur l'icône en forme de crayon à côté du nom du widget. Modifier un widget vous permet de le renommer, de modifier l'intervalle de temps, de définir des filtres et de grouper des lignes.

Pour ajouter un widget

Cliquez sur **Ajouter widget**, puis effectuez l'une des actions suivantes :

- Cliquez sur le widget que vous désirez ajouter. Le widget sera ajouté avec les paramètres par défaut.
- Pour modifier le widget avant de l'ajouter, cliquez sur Personnaliser lorsque le widget est sélectionné. Lorsque vous avez terminé de modifier le widget, cliquez sur **Terminé**.

Pour supprimer un widget

Cliquez sur le signe X à côté du nom du widget.

Le tableau de bord Activités

Le tableau de bord **Activités** offre une vue d'ensemble des activités actuelles et passées. Par défaut, la période de rétention est de 90 jours.

Pour personnaliser la vue du tableau de bord **Activités**, cliquez sur l'icône en forme d'engrenage, puis sélectionnez les colonnes que vous souhaitez afficher.

Pour consulter la progression des activités en temps réel, sélectionnez la case **Actualiser automatiquement**. Notez toutefois que l'actualisation fréquente de nombreuses activités a pour effet de dégrader les performances du serveur de gestion.

Vous pouvez effectuer une recherche parmi les activités répertoriées selon les critères suivants :

- **Nom du terminal**
  Il s'agit de l'ordinateur sur lequel l'activité est exécutée.
- **Démarrée par**
  Il s'agit du compte qui a démarré l'activité.

Vous pouvez également filtrer les activités selon les propriétés suivantes :

- **Statut**
  Par exemple, « a réussi », « a échoué », « en cours », « annulée ».
- **Type**
  Par exemple, application de plan, suppression de sauvegardes, installation de mises à jour logicielles.
- **Heure**
  Par exemple, les activités les plus récentes, les activités des dernières 24 heures ou les activités pendant une période spécifique au sein de la période de rétention par défaut.

Pour en savoir plus à propos d'une activité, sélectionnez l'activité dans la liste, puis, dans le volet **Détails de l'activité**, cliquez sur **Toutes les propriétés**. Pour plus d'informations sur les propriétés disponibles, reportez-vous aux références d'API Activité et Tâche sur le portail Developer Network.

Le tableau de bord des alertes

Le tableau de bord des **alertes** affiche toutes vos alertes actuelles. Les alertes répertoriées sont des alertes critiques ou des erreurs, généralement associées à des tâches telles qu'une sauvegarde ayant échoué pour une raison quelconque.

Pour filtrer les alertes dans le tableau de bord

1. Dans la liste déroulante **Affichage**, sélectionnez l'un des critères suivants :
   - **Gravité de l'alerte**
   - **Catégorie d'alerte**
   - **Type d'alerte**
   - **Type de surveillance**
   - **Plage de dates : de ... à ...**
   - **Ressource**
   - **Plan**
   - **Client**
2. Si vous avez sélectionné **Catégorie d'alerte**, sélectionnez, dans la liste déroulante **Catégorie**, la catégorie d'alertes que vous souhaitez visualiser.
3. Si vous souhaitez visualiser toutes les alertes sans les filtrer, cliquez sur **Tous les types d'alerte**.

Vous pouvez effectuer les opérations suivantes dans chaque alerte :

- Accéder au terminal concerné par l'alerte en cliquant sur le lien **Terminaux**.
- Consultez la section **Dépannage** de l'alerte et suivez les indications.
- Accédez à la documentation et à l'article de base de connaissances pertinents en cliquant sur **Rechercher une solution**. La fonctionnalité **Rechercher une solution** préremplit votre demande avec les détails de l'alerte afin de vous faciliter la tâche.

Pour trier les alertes dans le tableau de bord

Dans le tableau des alertes, cliquez sur le bouton fléché figurant à côté de l'un des noms de colonne suivants :

- **Gravité de l'alerte**
- **Type d'alerte**
- **Créé**
- **Catégorie d'alerte**

- **Ressource**
- **Plan**

Si le service Advanced Automation est activé pour votre compte, vous pouvez également créer un ticket auprès du service d'assistance directement à partir de l'alerte.

Pour créer un ticket auprès du service d'assistance

1. Dans l'alerte concernée, cliquez sur **Créer un nouveau ticket**.
   Lorsque vous travaillez en mode d'affichage tableau, vous pouvez également sélectionner une alerte puis sélectionner **Créer un nouveau ticket** dans le volet de droite.
2. Définissez ce qui suit :
   - Dans la section d'en-tête, sélectionnez la case **Facturable** si vous souhaitez que le temps passé sur le ticket soit facturé au client. Cochez également la case **Envoyer un e-mail au client** si vous souhaitez envoyer des mises à jour concernant le ticket au client.
   - Dans la section **Informations générales**, donnez un titre au ticket. Ce champ est prérempli avec un résumé de l'alerte, vous pourrez cependant le modifier.
   - Dans la section **Informations sur le client**, les champs sont préremplis avec les informations concernant l'alerte.
   - Dans la section **Élément ou service de configuration**, les champs sont préremplis avec le terminal associé à l'alerte. Vous pouvez réaffecter un terminal, selon vos besoins.
   - Dans la section **Agent de support**, les champs sont préremplis avec l'agent de support, la catégorie et le groupe de support par défaut. Vous pouvez réaffecter un autre agent, selon vos besoins.
   - Dans la section **Mise à jour du ticket**, les champs sont préremplis avec la description et les détails de l'alerte. Le champ **Statut** est défini sur **Nouveau** par défaut, et peut être modifié.
   - Dans les sections **Pièces jointes**, **Éléments facturables** et **Remarques internes**, ajoutez les éléments pertinents selon vos besoins.
3. Cliquez sur **Valider**. Une fois le ticket créé, un lien vers ce ticket est ajouté à l'alerte.
   Si une alerte est fermée, le ticket associé est également automatiquement fermé.

   Remarque
   Vous ne pouvez créer qu'un seul ticket par alerte.

Types d'alerte

Les alertes seront générées pour les types d'alertes suivants :

- Alertes de sauvegarde
- Alertes de reprise d'activité après sinistre
- Alertes de protection antimalware
- Alertes de licence
- Alertes de filtrage d'URL

- Alertes EDR
- Alertes de contrôle des terminaux
- Alertes système

Alertes de sauvegarde

Alerte	Description	Comment résoudre l'alerte
Échec sauvegarde	Une alerte est générée en cas d'échec (avec erreur pouvant être résolue) d'exécution de la sauvegarde ou d'interruption en raison d'un arrêt du système.	Consultez le journal de l'opération de sauvegarde qui a échoué : cliquez sur la ressource pour la sélectionner, puis sur **Activités** et recherchez l'avertissement dans le journal. Le message doit indiquer la cause racine du problème dont vous informe le logiciel.
Sauvegarde réussie avec avertissements	Une alerte est générée lorsque la sauvegarde s'est déroulée avec des avertissements.	Vérifiez les journaux de conversion en machine virtuelle, de réplication ou des plans de validation. Des problèmes pendant ces opérations génèrent une alerte Échec de l'activité ou Activité terminée avec un avertissement.
La sauvegarde est annulée	Une alerte est générée à chaque annulation manuelle d'une sauvegarde par l'utilisateur.	Vous pouvez démarrer la sauvegarde manuellement en cliquant sur Exécuter maintenant ou patienter jusqu'à l'heure de sa prochaine planification.
Sauvegarde annulée en raison d'un créneau de sauvegarde fermé	Une alerte est générée lorsque l'activité de sauvegarde a été manquée, car elle était plus longue que le créneau indiqué dans les options de sauvegarde.	Reconfigurez la planification ou modifiez les options du plan de sauvegarde dans **Performance et créneau de sauvegarde**. Développez la section concernant votre produit pour accéder aux instructions.
Sauvegarde en attente	Cette alerte est générée en cas de conflit de planification et lorsque deux tâches de sauvegarde sont démarrées en même temps. Dans ce cas, la seconde tâche est mise en file d'attente jusqu'à la fin ou l'arrêt de la première.	Veillez à ce que vos sauvegardes s'exécutent dans les créneaux attendus et conformément à leur planification, et évitez autant que possible les conflits de planification.
La sauvegarde ne répond pas	Une alerte est générée lorsque la sauvegarde en	Le problème provient peut-être d'un blocage. Suivez cet article pour récupérer les

Alerte	Description	Comment résoudre l'alerte
	cours d'exécution n'indique aucune progression depuis un certain temps, ce qui peut signifier qu'elle est figée.	informations de dépannage nécessaires.
La sauvegarde n'a pas démarré	Une alerte est générée lorsque la sauvegarde planifiée n'a pas démarré pour une raison inconnue.	Vérifiez que vous utilisez bien la dernière version de votre produit Acronis Backup. • Si l'ordinateur avec agent était disponible à l'heure de démarrage de la sauvegarde : 1. Modifiez l'heure de démarrage de la sauvegarde. 2. Si l'alerte réapparaît, recréez la tâche de sauvegarde. 3. Si la tâche de sauvegarde que vous venez de créer déclenche également une alerte, contactez le support Acronis pour obtenir de l'aide. • Si l'agent était hors ligne : 1. Ne mettez pas l'ordinateur hors tension pendant la sauvegarde. 2. Si l'ordinateur n'était pas hors tension, vérifiez qu'Acronis Managed Machine Service est en cours d'exécution : Démarrer -> Rechercher -> services.msc -> localisez Acronis Managed Machine Service. Si vous avez besoin d'aide, contactez le support Acronis.
L'état de la sauvegarde est inconnu	Une alerte est générée si l'agent de sauvegarde était hors ligne au moment d'une sauvegarde planifiée. L'état des sauvegardes de ressources sera inconnu jusqu'à ce que l'agent de sauvegarde soit en ligne.	1. Vérifiez si l'agent est censé être hors ligne (s'il s'agit, par exemple, d'un notebook qui se trouve à l'extérieur du réseau du serveur de gestion). 2. Si l'agent n'est pas censé être hors ligne, vérifiez qu'Acronis Managed Machine Service est en cours d'exécution : Démarrer -> Rechercher -> services.msc -> localisez Acronis Managed Machine Service et vérifiez son statut. Démarrez le service s'il est arrêté.
La sauvegarde est	Une alerte est générée si	

Alerte	Description	Comment résoudre l'alerte
manquante	aucune sauvegarde n'a abouti depuis plus de [Jours depuis la dernière sauvegarde] jours.	
La sauvegarde est corrompue	Une alerte est générée lorsque l'activité de validation s'est déroulée avec succès et indique que la sauvegarde est corrompue.	Suivez les étapes de l'article Problèmes de dépannage des sauvegardes corrompues. Si vous avez besoin d'aide pour identifier la cause racine de la corruption de l'archive, contactez le support Acronis.
Échec de la protection continue des données	Une alerte est générée si la protection continue de la sauvegarde a échoué.	Vérifiez les limitations suivantes : 1. La protection continue des données n'est prise en charge que pour le système de fichiers NTFS et pour les systèmes d'exploitation suivants : • Ordinateur de bureau : Windows 7 et versions ultérieures • Serveur : Windows Server 2008 R2 et versions ultérieures 2. La protection continue des données ne prend pas en charge **Acronis Secure Zone** en tant que destination. 3. Les dossiers NFS montés sous Windows ne sont pas pris en charge. 4. La réplication en continue n'est pas prise en charge : si le plan de protection comprend deux emplacements, les tranches de protection continue des données ne sont créées que dans la première destination. Les modifications sont ensuite répliquées sur la seconde destination lors de la sauvegarde suivante. 5. Si des modifications d'un dossier local protégé sont appliquées depuis une source réseau (par exemple, lorsque les utilisateurs ont accès au dossier depuis le réseau), la protection continue des données ne les détecte pas. 6. Si un fichier est utilisé, par exemple si un fichier Excel est modifié, la protection continue des données ne détecte pas les modifications. Pour que les modifications soient détectées par la protection continue

Alerte	Description	Comment résoudre l'alerte
		des données, enregistrez-les et fermez le fichier.
La configuration des hôtes Hyper-V n'est pas valide	Une alerte est générée lorsque plusieurs agents pour Hyper-V, qui sont installés sur des hôtes Hyper-V, possèdent le même nom d'hôte, car cela n'est pas pris en charge au niveau du même compte.	Vous devez enregistrer ces agents pour Hyper-V sous différentes unités enfants de ce compte pour éviter les conflits.
Échec de la validation	Une alerte est générée lorsque la validation de votre sauvegarde ne peut pas aboutir.	Consultez le journal de l'opération qui a échoué : cliquez sur l'ordinateur pour le sélectionner, puis sur **Activités** et recherchez l'avertissement dans le journal. Le message doit indiquer la cause racine du problème dont vous informe le logiciel.
Échec de la migration des sauvegardes dans le stockage Cloud vers le nouveau format	Une alerte est générée en cas d'échec de la migration vers le nouveau format des sauvegardes dans le stockage dans le cloud.	La migration des archives Acronis Cyber Backup Advanced est décrite ici. La migration des archives Acronis Cyber Backup est décrite ici. Avant de contacter le support Acronis, collectez les rapports suivants à l'aide de l'outil migrate_archives : **migrate_archives.exe --account=<compte Acronis> --password=<mot de passe> --subaccounts=Tous > report1.txt** **migrate_archives.exe --cmd=finishUpgrade --account=<compte Acronis> --password=<mot de passe> > report2.txt**
Le mot de passe de chiffrement est manquant	Une alerte est générée lorsque la clé de chiffrement de base de données est incorrecte, corrompue ou manquante.	Il est impossible de restaurer les sauvegardes chiffrées si vous perdez ou oubliez le mot de passe. Vous devez définir le mot de passe de chiffrement localement sur le terminal protégé. Vous ne pouvez pas définir le mot de passe de chiffrement dans le plan de protection. Pour plus d'informations, voir Définition du mot de passe de chiffrement.
Le transfert est en attente	Une alerte est générée si la vérification planifiée détecte que l'envoi des	

Alerte	Description	Comment résoudre l'alerte
	données physiques à l'archive dans le cloud de ce plan de sauvegarde n'est pas transféré au stockage.	
La reprise de la sauvegarde a échoué	Une alerte est générée si l'opération de récupération échoue lorsque vous essayez de restaurer des fichiers ou des sauvegardes système.	Déterminez la date exacte de l'échec de la sauvegarde et essayez d'effectuer une reprise avec la dernière sauvegarde aboutie.

Alertes de reprise d'activité après sinistre

Alerte	Description	Comment résoudre l'alerte
Quota de stockage dépassé	Une alerte est générée lorsque le quota conditionnel du stockage de reprise d'activité après sinistre est dépassé	Augmentez le quota ou supprimez des archives du stockage dans le cloud.
Le quota est atteint	Une alerte est générée dans les cas suivants : • Le quota conditionnel des serveurs cloud est dépassé. • Le quota conditionnel du point de calcul est dépassé. • Le quota conditionnel des adresses IP publiques est dépassé.	
Le quota de stockage est dépassé	Une alerte est générée lorsque le quota inconditionnel du stockage de reprise d'activité après sinistre est dépassé. Ce stockage est utilisé par les serveurs primaires et de restauration. Si le quota est atteint, il n'est pas possible de créer des serveurs primaires et de restauration, ou d'ajouter/étendre des disques à des serveurs primaires existants. Si le quota est dépassé, il n'est pas possible	

Alerte	Description	Comment résoudre l'alerte
	d'initier un basculement ni de simplement démarrer un serveur arrêté. Les serveurs en cours d'exécution continuent à fonctionner.	
Le quota est dépassé	Une alerte est générée dans les cas suivants : • Le quota inconditionnel des serveurs cloud est dépassé. • Le quota inconditionnel du point de calcul est dépassé. • Le quota inconditionnel des adresses IP publiques est dépassé.	Envisagez de faire l'acquisition de quotas de terminaux supplémentaires ou désactivez les tâches de sauvegarde des terminaux que vous n'avez plus besoin de protéger.
Erreur de basculement	Une alerte est générée en cas de problème système après la soumission du basculement.	1. Cliquez sur **Modifier** sur le serveur de restauration. Pour plus d'informations, voir Création d'un serveur de restauration. 2. Réduisez le processeur/la mémoire RAM du serveur de restauration. 3. Réessayez d'effectuer le basculement.
Erreur de basculement test	Une alerte est générée en cas de problème système après la soumission du test.	1. Cliquez sur **Modifier** sur le serveur de restauration. Pour plus d'informations, voir Création d'un serveur de restauration. 2. Réduisez le processeur/la mémoire RAM du serveur de restauration. 3. Réessayez d'effectuer le basculement. **Remarque** Veillez à ce que l'adresse IP que vous spécifiez dans Adresse IP en réseau de production soit la même que celle configurée dans le serveur DHCP.
Erreur de restauration automatique	Une alerte est générée en cas de problème système après le démarrage du basculement.	Vous voyez l'emplacement erroné dans la liste des stockages des sauvegardes : un numéro est indiqué à la place du nom (en général, le nom de l'emplacement correspond à celui de

Alerte	Description	Comment résoudre l'alerte
		l'un des utilisateurs finaux existants) et vous n'êtes pas à l'origine de la création de cet emplacement. Supprimez l'emplacement erroné : 1. Dans la console Cyber Protect, accédez à Stockage des sauvegardes. 2. Recherchez l'emplacement et cliquez sur l'icône représentant une croix (x) pour la supprimer. 3. Confirmez votre choix en cliquant sur Supprimer. 4. Retentez le basculement.
La restauration automatique est annulée	Une alerte est générée lorsque le basculement est annulé par l'utilisateur.	Fermez manuellement l'alerte dans la console.
Erreur de connexion VPN	Une alerte est générée lorsque la connexion VPN échoue pour des raisons indépendantes des actions de l'utilisateur. Le rapport de statut de l'appliance VPN est obsolète.	Si vous avez rencontré un problème lors du déploiement ou de la connexion d'une appliance VPN Acronis, veuillez contacter le support Acronis. Veuillez indiquer dans votre e-mail les informations suivantes : • Captures d'écran des messages d'erreur (le cas échéant) • Capture d'écran de l'interface de ligne de commande de l'appliance VPN Acronis • Votre centre de données Acronis Backup Cloud et le nom de votre groupe.
(VPN inaccessible) La passerelle de connectivité est inaccessible	Une alerte est générée lorsque le service RAS ne peut pas atteindre la passerelle de connectivité. Le rapport de statut de la passerelle de connectivité est obsolète.	Si vous avez rencontré un problème lors du déploiement ou de la connexion d'une appliance VPN Acronis, veuillez contacter le support Acronis. Veuillez indiquer dans votre e-mail les informations suivantes : • Captures d'écran des messages d'erreur (le cas échéant) • Capture d'écran de l'interface de ligne de commande de l'appliance

Alerte	Description	Comment résoudre l'alerte
		VPN Acronis • Votre centre de données Acronis Backup Cloud et le nom de votre groupe
Réaffectation nécessaire de l'adresse IP RAS	Une alerte est générée si l'appliance VPN détecte des modifications réseau.	Réaffectez l'adresse IP. Pour plus d'informations, voir Réaffectation d'adresses IP.
Échec de la passerelle de connectivité	Une alerte est générée en cas d'échec de déploiement du serveur VPN dans le cloud.	Utilisez l'outil Connection Verification Tool et recherchez d'éventuelles erreurs dans son résultat. Autorisez le logiciel Acronis à traverser le contrôle des applications de votre pare-feu et de votre logiciel antimalware.
Échec de création du serveur primaire	Une alerte est générée lorsque le serveur primaire n'a pas été créé en raison d'une erreur.	
Échec de création du serveur de restauration	Une alerte est générée lorsque le serveur de restauration n'a pas été créé en raison d'une erreur.	Vérifiez que le serveur de restauration correspond à la configuration logicielle requise.
Supprimer le serveur primaire	Une alerte est générée lors de la suppression d'un serveur primaire.	
Échec de reprise du serveur	Une alerte est générée lorsque le serveur primaire ou de restauration ne parvient pas à effectuer la reprise.	Recherchez les informations détaillées. Si le message d'erreur est générique ou peu clair (par exemple, Erreur interne), accédez à **Reprise d'activité après sinistre → Serveurs**, puis cliquez sur l'ordinateur concerné et sur **Activités**. Maintenez la touche Ctrl enfoncée et cliquez sur une activité à l'aide du bouton gauche. Des points de suspension (...) apparaissent maintenant à côté de chaque activité. Cliquez sur l'option **Informations sur l'activité de cette tâche** pour la sélectionner.
Échec sauvegarde	Une alerte est générée lorsque	1. Vérifiez la connexion de

Alerte	Description	Comment résoudre l'alerte
	la sauvegarde du serveur cloud (primaire ou serveur dans l'état de basculement de production) a échoué.	l'emplacement de sauvegarde. 2. Vérifiez le périphérique de stockage des sauvegardes (sauvegardes locales).
La limite réseau est dépassée	Une alerte est générée lorsque le nombre maximal (5) de réseaux dans le cloud est atteint.	
Échec de runbook	Une alerte est générée en cas d'échec d'exécution du runbook.	Cela n'a pas d'incidence sur la fonctionnalité du produit et peut sans risque être ignoré. Pour plus d'informations, voir Création d'un runbook.
Avertissement de runbook	Une alerte est générée si l'exécution du runbook se termine avec des avertissements.	Cela n'a pas d'incidence sur la fonctionnalité du produit et peut sans risque être ignoré. Pour plus d'informations, voir Création d'un runbook.
Intervention de l'utilisateur du runbook requise	Une alerte est générée lorsque le runbook attend l'intervention de l'utilisateur.	Cela n'a pas d'incidence sur la fonctionnalité du produit et peut sans risque être ignoré. Pour plus d'informations, voir Création d'un runbook.
Trafic Internet bloqué	Une alerte est générée lorsque le trafic Internet a été bloqué par l'administrateur.	
Trafic Internet débloqué	Une alerte est générée lorsque le trafic Internet a été débloqué par l'administrateur.	
Chevauchement de réseaux locaux	Une alerte est générée lors de la détection de réseaux locaux identiques ou se chevauchant.	
Quota de serveur insuffisant dans le paramètre de licence	Une alerte est générée lorsque le quota des serveurs cloud n'est pas suffisant.	• Vérifiez que le tenant et l'utilisateur disposent d'un quota de serveurs ou de serveurs d'hébergement Web pour un serveur physique. • Vérifiez que le tenant et l'utilisateur disposent d'un quota de serveurs d'hébergement Web ou de machines virtuelles pour un serveur virtuel. Un

Alerte	Description	Comment résoudre l'alerte
		serveur virtuel ne peut pas utiliser le quota des serveurs.
Offre insuffisante dans le paramètre de licence	Une alerte est générée lorsque l'élément de stockage de reprise d'activité après sinistre est désactivé.	Pour plus d'informations, voir Quotas de reprise d'activité après sinistre.
Erreur de paramètre de licence	Une alerte est générée lorsque la mise à niveau de reprise d'activité après sinistre a rencontré une erreur.	
Points de calcul insuffisants dans le paramètre de licence	Une alerte est générée si aucun point de calcul n'est disponible.	Dans le portail de gestion, vérifiez le quota inconditionnel des points suivants et augmentez-le.
Offres de serveurs insuffisantes dans le paramètre de licence	Une alerte est générée lorsque l'offre de serveurs cloud est désactivée.	
La stratégie n'est pas parvenue à créer le serveur de restauration	Une alerte est générée sue une erreur s'est produite pendant la configuration de l'infrastructure de reprise d'activité .après sinistre.	Créez le serveur de restauration manuellement, sans la propriété d'accès à Internet. Pour plus d'informations, voir Création d'un serveur de restauration
Basculement test automatisé du processeur de sauvegarde replanifié	Une alerte est générée lorsque l'exécution du basculement test automatisé a été replanifiée.	
Basculement test automatisé du processeur de sauvegarde expiré	Une alerte est générée lorsque le basculement test automatisé a expiré. **Remarque** Chaque basculement test automatisé consomme des points de calcul facturables.	
Échec global du basculement test automatisé du processeur de sauvegarde	Une alerte est générée en cas d'échec du dernier basculement test automatisé et programmé du serveur de restauration.	1. Démarrez un basculement test du serveur de restauration manuellement. Pour plus d'informations, voir Réalisation d'un basculement test. 2. Patientez jusqu'à la date de planification du prochain

Alerte	Description	Comment résoudre l'alerte
		basculement test automatique
Erreur de transfert de données lors de la restauration automatique	Une alerte est générée en cas d'échec du transfert de données lors de la restauration automatique.	
Échec de restauration automatique	Une alerte est générée en cas d'erreur dans la restauration automatique.	Vous voyez l'emplacement erroné dans la liste des stockages des sauvegardes : un numéro est indiqué à la place du nom (en général, le nom de l'emplacement correspond à celui de l'un des utilisateurs finaux existants) et vous n'êtes pas à l'origine de la création de cet emplacement. Supprimez l'emplacement erroné : 1. Dans Cyber Protection, accédez au stockage des sauvegardes. 2. Recherchez l'emplacement et cliquez sur l'icône représentant une croix (x) pour la supprimer. 3. Confirmez votre choix en cliquant sur **Supprimer**. Retentez le basculement.
Échec de confirmation de la restauration automatique	Une alerte est générée en cas d'échec de confirmation de la restauration automatique.	
L'ordinateur de restauration automatique est prêt pour le basculement	Une alerte est générée lorsque l'ordinateur est prêt pour le basculement.	
Basculement de la restauration automatique terminé	Une alerte est générée lorsque le basculement s'est terminé avec succès.	Fermez manuellement l'alerte dans la console.
Agent cible de la restauration automatique hors ligne	Une alerte est générée lorsque l'agent est hors ligne.	

Alertes de protection antimalware

Alerte	Description	Comment résoudre l'alerte
Une activité suspecte de connexion à distance est	Une alerte est générée lorsqu'un ransomware est	Fermez manuellement l'alerte dans la console.

Alerte	Description	Comment résoudre l'alerte
détectée	détecté sur une connexion à distance.	
Une activité suspecte est détectée	Une alerte est générée lorsqu'un ransomware est détecté dans la ressource.	Fermez manuellement l'alerte dans la console. pour désactiver l'alerte. Selon l'option indiquée dans le plan Active Protection, le processus malveillant est arrêté et les modifications apportées par ce processus sont annulées. Si aucune action n'a encore été exécutée, vous devrez résoudre le problème manuellement. Pour plus d'informations sur le processus à l'origine du chiffrement des fichiers et sur les fichiers concernés, consultez les informations détaillées de l'alerte. Si vous considérez que le processus à l'origine du chiffrement des fichiers est sanctionné par erreur (alerte de type faux positif), ajoutez-le aux processus de confiance : 1. Ouvrez le plan Active Protection. 2. Cliquez sur **Modifier** pour modifier les paramètres. 3. Dans **Processus de confiance**, spécifiez les processus de confiance à ne jamais considérer comme des ransomware. Spécifiez le chemin d'accès complet au processus exécutable, en commençant par la lettre du lecteur. Par exemple : C:\Windows\Temp\er76s7sdkh.exe.
Une activité de cryptomining est détectée	Une alerte est générée lorsque des cryptomineurs interdits sont détectés dans la ressource	Fermez manuellement l'alerte dans la console.
Défense MBR : Une activité suspecte est détectée et suspendue	Une alerte est générée lorsqu'un ransomware est détecté dans la ressource (spécifiquement, la partition	Fermez manuellement l'alerte dans la console.

Alerte	Description	Comment résoudre l'alerte
	MBR/GPT est modifiée par le ransomware).	
Un chemin d'accès réseau non valide est spécifié	Une alerte est générée lorsque le chemin de la reprise que fournit l'administrateur n'est pas un chemin d'accès à un dossier local.	Spécifiez le chemin d'accès locale pour la protection des dossiers réseau (chemin de reprise). Fermez manuellement l'alerte dans la console
Le processus critique est ajouté avec le statut « dangereux » au plan Active Protection	Une alerte est générée lorsqu'un processus critique est ajouté en tant que processus bloqué dans la liste des exclusions de la protection.	Fermez manuellement l'alerte dans la console.
Échec de l'application d'une règle Active Protection	Une alerte est générée en cas d'échec d'application de la stratégie Active Protection.	Consultez le message d'erreur si vous souhaitez connaître les raisons pour lesquelles la stratégie Active Protection ne peut pas être appliquée.
Secure Zone : Une opération non autorisée est détectée et bloquée	Une alerte est générée lorsqu'un ransomware est détecté dans la ressource (la partition ASZ est modifiée par le ransomware).	Fermez manuellement l'alerte dans la console.
Le service Active Protection ne fonctionne pas	Une alerte est générée en cas de plantage/de non-exécution du service Active Protection.	Consultez le message d'erreur si vous souhaitez connaître les raisons pour lesquelles le service Active Protection ne s'exécute pas.
Le service Active Protection n'est pas disponible	Une alerte est générée lorsque le service Active Protection n'est pas disponible, car un pilote est absent ou incompatible.	Consultez les journaux d'événements Windows et recherchez-y les plantages du service Acronis Active Protection (acronis_protection_service.exe).
Conflit avec une autre solution de sécurité	Une alerte est générée si Active Protection n'est pas disponible pour l'ordinateur {{resourceName}}, car un conflit avec une autre solution de sécurité a été détecté. Pour activer Active Protection, désactivez ou désinstallez l'autre solution de sécurité.	**Solution 1** : Si vous souhaitez utiliser la protection en temps réel Acronis, désinstallez l'antivirus tiers de l'ordinateur. **Solution 2** : Si vous souhaitez utiliser l'antivirus tiers, désactivez la protection en temps réel d'Acronis, le filtrage des adresses URL et l'antivirus

Alerte	Description	Comment résoudre l'alerte
		Windows Defender dans le plan de protection.
Échec de l'action de quarantaine	Une alerte est générée lorsque l'antimalware ne parvient pas à mettre en quarantaine un malware qu'il a détecté.	Consultez le message d'erreur si vous souhaitez connaître les raisons pour lesquelles la mise en quarantaine a échoué.
Un processus malveillant est détecté	Une alerte est générée lorsque le moteur de comportement détecte un malware (type processus). Le malware détecté est mis en quarantaine.	Fermez manuellement l'alerte dans la console.
Un processus malveillant est détecté, mais il n'est pas mis en quarantaine	Une alerte est générée lorsque le moteur de comportement détecte un malware (type processus). Le malware détecté n'est pas mis en quarantaine.	Fermez manuellement l'alerte dans la console.
Un malware est détecté et bloqué (ODS)	Une alerte est générée lorsqu'une analyse planifiée détecte un malware. Le malware détecté est mis en quarantaine.	Fermez manuellement l'alerte dans la console.
Un malware est détecté et bloqué (RTP)	Une alerte est générée lorsque la protection en temps réel détecte un malware. Le malware détecté est mis en quarantaine.	Fermez manuellement l'alerte dans la console.
Un malware a été détecté dans une sauvegarde	Une alerte est générée lorsque l'analyse de la sauvegarde détecte un malware.	Fermez manuellement l'alerte dans la console.
Conflit détecté entre la protection anti-malware en temps réel et un produit de sécurité	Une alerte est générée lorsque l'antimalware ne parvient pas à s'inscrire auprès du Centre de sécurité Windows.	Désactivez ou désinstallez le produit de sécurité tiers, ou désactivez la protection antimalware en temps réel dans le plan de protection.
Échec de l'exécution du module	Une alerte est générée en cas d'échec de l'exécution du	Consultez le message d'erreur si vous souhaitez connaître les raisons pour

Alerte	Description	Comment résoudre l'alerte
Microsoft Security Essentials	module Microsoft Security Essentials.	lesquelles l'exécution de Microsoft Security Essentials a échoué.
La protection en temps réel n'est pas disponible car un logiciel antivirus tiers est installé	Une alerte est générée lorsque la protection en temps réel ne s'active pas, car celle d'un antivirus tiers est encore activée.	Désactivez ou désinstallez le produit de sécurité tiers, ou désactivez la protection antimalware en temps réel dans le plan de protection.
La protection en temps réel n'est pas disponible en raison d'un pilote absent ou incompatible	Une alerte est générée lorsque la protection en temps réel n'est pas disponible en raison d'un pilote absent ou incompatible.	Consultez le message d'erreur si vous souhaitez connaître les raisons pour lesquelles Acronis ne parvient pas à installer le pilote sur la ressource.
Le service Cyber Protection (ou Active Protection) ne répond pas	Une alerte est générée lorsque le service Cyber Protection répond à une commande ping de vérification d'intégrité envoyée depuis la console.	Fermez manuellement l'alerte dans la console.
Échec de la mise à jour des définitions de sécurité	Une alerte est générée en cas d'échec de mise à jour de la définition de sécurité.	Consultez le message d'erreur si vous souhaitez connaître les raisons pour lesquelles la mise à jour des définitions de sécurité a échoué.
La protection de l'intégrité est activée	Une alerte est générée lorsque les paramètres Microsoft Defender ne peuvent pas être modifiés car la protection de l'intégrité est activée.	Désactivez les paramètres de protection de l'intégrité sur la ressource Windows.
Échec de l'exécution du module Windows Defender	Une alerte est générée en cas d'échec de l'exécution du module Windows Defender.	Consultez le message d'erreur si vous souhaitez connaître les raisons pour lesquelles l'exécution du module Windows Defender a échoué.
Windows Defender est bloqué par un logiciel antivirus tiers	Une alerte est générée si Windows Defender est bloqué en raison de la présence d'un antivirus tiers installé sur l'ordinateur.	Désactivez ou désinstallez le produit de sécurité tiers.
Conflit de stratégie de groupe	Une alerte est générée lorsque les paramètres Microsoft Defender ne	Désactivez les paramètres de stratégie de groupe sur la ressource Windows.

Alerte	Description	Comment résoudre l'alerte
	peuvent pas être modifiés, car ils sont contrôlés par une stratégie de groupe.	
Microsoft Security Essentials a entrepris une action pour protéger cette machine des malware	Une alerte est générée lorsque Microsoft Security Essentials a supprimé/mis en quarantaine un malware.	Fermez manuellement l'alerte dans la console.
Microsoft Security Essentials a détecté un malware	Une alerte est générée lorsque Microsoft Security Essentials a détecté un malware et d'autres logiciels potentiellement indésirables.	Fermez manuellement l'alerte dans la console.

Alertes de licence

Alerte	Description	Comment résoudre l'alerte
Quota de stockage presque atteint	Une alerte est générée lorsque l'utilisation chute en dessous de 80 % (après un nettoyage ou une mise à niveau de quota).	Envisagez d'acheter un stockage supplémentaire ou libérez de l'espace dans votre stockage dans le cloud.
Quota de stockage dépassé	Une alerte est générée lorsque le quota de stockage est utilisé à 100 %.	Achetez plus d'espace de stockage. Pour plus d'informations, consultez la procédure permettant d'acheter plus de stockage dans le cloud.
Quota de la ressource atteint	Une alerte est générée lorsque l'utilisation de l'offre est supérieure à 0, qu'elle est supérieure au quota, mais inférieure ou égale au quota + surconsommation.	
Quota de la ressource dépassé	Une alerte est générée lorsque l'utilisation de l'offre est supérieure au quota + surconsommation.	
La ressource n'a aucun quota pour appliquer un plan de sauvegarde (aucun quota de service)	Une alerte est générée dans les cas suivants : • Le quota a été supprimé manuellement : **Terminal** > **Détails** >	

Alerte	Description	Comment résoudre l'alerte
	Quota de service, puis cliquez sur **Modifier** et sélectionnez l'option **Aucun quota**. • L'élément sur la console de gestion est désactivé. • La valeur quota+surconsommation de l'élément sur la console de gestion est inférieure à l'utilisation en cours.	
Impossible de protéger une ressource avec un quota affecté	Une alerte est générée lorsque l'offre est insuffisante et que vous avez besoin des éléments suivants : • Un groupe dynamique. • Un plan de sauvegarde affecté à ce groupe. • Vous avez ajouté une ressource appartenant à ce groupe dynamique, mais dont certaines propriétés empêchent l'application de ce même plan de sauvegarde.	
Licence d'abonnement expirée	Une alerte est générée lorsque la recherche quotidienne d'alertes d'expiration de licence/maintenance, après interrogation du serveur de licences, a reçu une réponse indiquant que la licence est arrivée à expiration.	Après l'expiration d'un abonnement, toutes les fonctionnalités du produit, à l'exception de la reprise, sont bloquées jusqu'au renouvellement de l'abonnement. Les données sauvegardées restent accessibles pour la reprise. Faites l'achat d'une nouvelle licence.

Alerte	Description	Comment résoudre l'alerte
		Remarque Si vous avez fait l'achat récemment d'un nouvel abonnement, mais continuez à recevoir un message indiquant que l'abonnement est arrivé à expiration, vous devez importer le nouvel abonnement depuis le compte Acronis : dans la console de gestion, accédez à Paramètres -> Licences, puis cliquez sur Sync, en haut à droite. Les abonnements seront synchronisés.
La licence par abonnement arrivera bientôt à expiration	Une alerte est générée lorsque la recherche quotidienne d'alertes d'expiration de licence/maintenance, après interrogation du serveur de licences, a reçu une réponse indiquant que la licence arrivera à expiration dans moins de 30 jours.	Pensez à faire l'achat d'un nouvel abonnement.

Alertes de filtrage d'URL

Alerte	Description	Comment résoudre l'alerte
Une URL malveillante a été bloquée	Une alerte est générée lorsqu'une adresse URL malveillante est bloquée par le filtrage d'URL.	Vérifiez les paramètres du filtrage d'URL. Le filtrage d'URL bloque des pages conformément aux paramètres Filtrage d'URL.
Un avertissement d'URL malveillante a été ignoré	Une alerte est générée lorsque vous avez choisi de poursuivre la navigation sur une adresse URL malveillante bloquée par le filtrage d'URL.	Vérifiez les paramètres du filtrage d'URL.
Conflit détecté entre le filtrage d'URL et un produit de sécurité	Une alerte est générée lorsque le filtrage des adresses URL ne peut pas être activé en raison d'un conflit avec une autre solution de sécurité.	Vérifiez les paramètres du filtrage d'URL.
L'URL du site Web est bloquée	Une alerte est générée	Vérifiez les paramètres du filtrage

Alerte	Description	Comment résoudre l'alerte
	lorsqu'une adresse URL remplit tous les critères spécifiés dans la catégorie des adresses bloquées pour le filtrage d'URL.	d'URL.

Alertes EDR

Alerte	Description	Comment résoudre l'alerte
Incident détecté	Une alerte est générée lorsqu'un incident est créé ou que le statut d'un incident existant est mis à jour.	Cette alerte vous informe d'un nouvel incident ou de la mise à jour d'un ancien incident. Vous pouvez visualiser l'alerte et la fermer. Vous pouvez choisir d'ouvrir l'incident à des fins d'investigation si nécessaire.
Indicateur de compromission détecté	Une alerte est générée lorsque le service EDR de recherche de menaces a détecté un nouvel indicateur de compromission.	Cette alerte vous informe qu'un indicateur de compression a été détecté sur une ou plusieurs ressources. Lorsque cette alerte s'affiche, vous pouvez cliquer sur son lien afin de visualiser les détails concernant l'indicateur de compromission.
Échec de l'isolation de la ressource du réseau	Une alerte est générée lorsque l'utilisateur déclenche l'action permettant d'isoler l'ordinateur du réseau, mais que cette action échoue.	Prenez les mesures nécessaires.
Échec de reconnexion de la ressource au réseau	Une alerte est générée lorsque l'utilisateur déclenche l'action permettant de reconnecter l'ordinateur au réseau, mais que cette action échoue.	Prenez les mesures nécessaires.
Les paramètres du Pare-feu Windows Defender ont été modifiés	Une alerte est générée lorsque les paramètres du pare-feu ont été modifié sur l'ordinateur isolé.	Cette alerte vous informe que les informations détaillées du pare-feu ont été modifiées sur l'ordinateur isolé. Elle n'est fournie qu'à titre d'information et vous pouvez la fermer après en avoir pris connaissance.

Alertes de contrôle des terminaux

Alerte	Description	Comment résoudre l'alerte
Le contrôle des terminaux et la prévention de la perte de données s'exécuteront avec des fonctionnalités limitées (processeur incompatible détecté)	Une alerte est générée lorsque l'agent DeviceLock a démarré sur une machine physique avec processeur prenant en charge la technologie CET.	Désactivez l'option sur les ordinateurs concernés afin d'éviter les alertes.
La fonctionnalité de contrôle de terminaux n'est pas encore prise en charge sur macOS Ventura	Une alerte est générée lorsque l'agent DeviceLock a démarré sur une machine physique macOS Ventura et que le plan de protection avec contrôle des terminaux est appliqué à l'agent. S'applique uniquement aux versions présentant un problème de panique du noyau lié au pilote DeviceLock.	
Transfert autorisé des données sensibles	Une alerte est générée lorsque le transfert de contenu de sensibilité est autorisé.	
Transfert justifié de données sensibles	Une alerte est générée lorsque le transfert de contenu de sensibilité est justifié.	
Transfert de données sensibles refusé	Une alerte est générée lorsque le transfert de contenu de sensibilité est bloqué.	
Examinez les résultats du mode d'observation de la prévention de perte de données	Une alerte est générée lorsque les résultats de l'observation doivent être examinés : • La licence du pack Advanced DLP n'est pas appliquée. • Un mois s'est écoulé depuis l'activation du mode Observation dans un plan de protection appliqué à une ressource au moins. • Un mois s'est écoulé depuis la dernière génération d'une alerte semblable et la détection	

Alerte	Description	Comment résoudre l'alerte
	d'une utilisation de DLP en mode Observation.	
L'identificateur de sécurité a été modifié pour l'utilisateur	Une alerte est générée dans le cas où un SID est mis à jour pour un nom d'utilisateur connu. Cela peut se produire lorsque le système d'exploitation est réinstallé sur un PC hors du domaine.	
L'accès au périphérique est bloqué	Une alerte est générée lorsque certaines actions (lecture/écriture) sont bloquées sur les terminaux pris en charge.	
Impossible de se connecter à une ressource SSL distante.	Une alerte est générée lorsque l'accès à une ressource SSL distante est bloqué en raison d'une prévention d'échange supplémentaire utilisée au niveau de la ressource.	Ajoutez la ressource à la liste d'autorisations pour les hôtes distants.

Alertes système

Alerte	Description	Comment résoudre l'alerte
L'agent est obsolète	Une alerte est générée lorsque la version de l'agent est obsolète.	Accédez à la liste des agents et démarrez la mise à jour de l'agent.
Échec de la mise à jour automatique	Une alerte est générée lorsque la mise à jour automatique de l'agent a échoué.	Essayez d'effectuer une mise à jour manuelle.
Vous devez redémarrer le terminal après avoir installé un nouvel agent	Une alerte est générée lorsqu'un redémarrage est nécessaire après une installation effectuée à distance avec succès.	Redémarrez la ressource.
Échec de l'activité	Une alerte est générée lorsqu'une activité a échoué.	Redémarrez tous les services Acronis sur l'ordinateur.
Activité réussie avec avertissements	Une alerte est générée lorsqu'une activité a abouti, mais que des avertissements ont été générés.	
L'activité ne répond pas	Une alerte est générée lorsqu'une activité en cours ne répond pas.	

Alerte	Description	Comment résoudre l'alerte
Échec du plan de déploiement	Une alerte est générée en cas d'échec de déploiement du plan de protection.	
Échec de la conversion du nom d'utilisateur en SID	Une alerte est générée en cas d'échec de la conversion SID de la planification.	

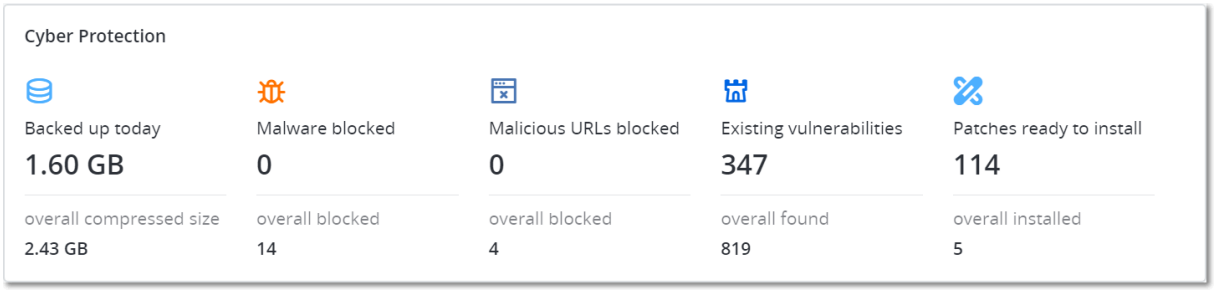
Widgets d'alerte

Dans les widgets d'alertes, vous pouvez consulter les détails suivants des alertes relatives à votre ressource :

Champs	Description
Widget 5 dernières alertes	Liste des cinq dernières alertes.
Résumé de l'historique des alertes	Widget graphique affichant les alertes par gravité, type et période.
Résumé des alertes actives	Widget graphique affichant les alertes activez par gravité et type, ainsi que la somme des alertes actives.
Historique des alertes	Affichage tableau de l'historique des alertes.
Détails des alertes actives	Affichage tableau des alertes actives.

Cyber Protection

Ce widget affiche les informations globales concernant la taille des sauvegardes, des malware bloqués, des URL bloquées, des vulnérabilités trouvées et des correctifs installés.



La ligne supérieure affiche les statistiques actuelles :

- **Sauvegardé aujourd'hui :** la somme des tailles de point de récupération pour les dernières 24 heures.

- **Malwares bloqués :** le nombre d'alertes relatives à des malwares bloqués, actives actuellement.
- **URL bloquées** : le nombre d'alertes relatives à des URL bloquées, actives actuellement
- **Vulnérabilités existantes :** le nombre actuel de vulnérabilités existantes.
- **Correctifs prêts à être installés :** le nombre actuel de correctifs disponibles et prêts à être installés.

La ligne inférieure affiche les statistiques globales :

- La taille compressée de toutes les sauvegardes
- Le nombre accumulé de malware bloqués sur l'ensemble des machines
- Le nombre accumulé d'URL bloquées sur l'ensemble des machines
- Le nombre cumulé des vulnérabilités découvertes sur l'ensemble des machines
- Le nombre cumulé de mises à jour/correctifs installés sur l'ensemble des machines

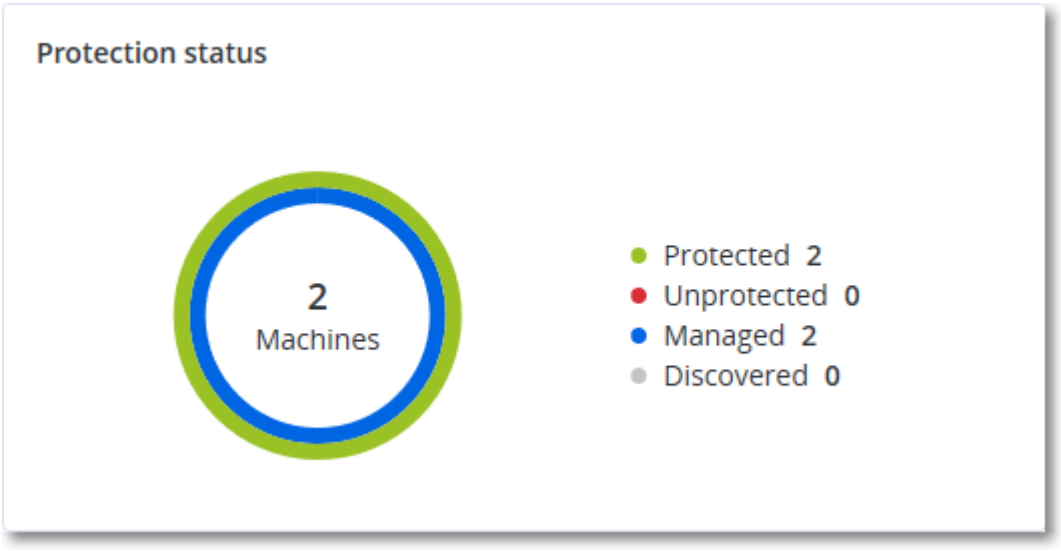
État de protection

Ce widget affiche l'état de protection actuel de toutes les machines.

Une machine peut présenter l'un des états suivants :

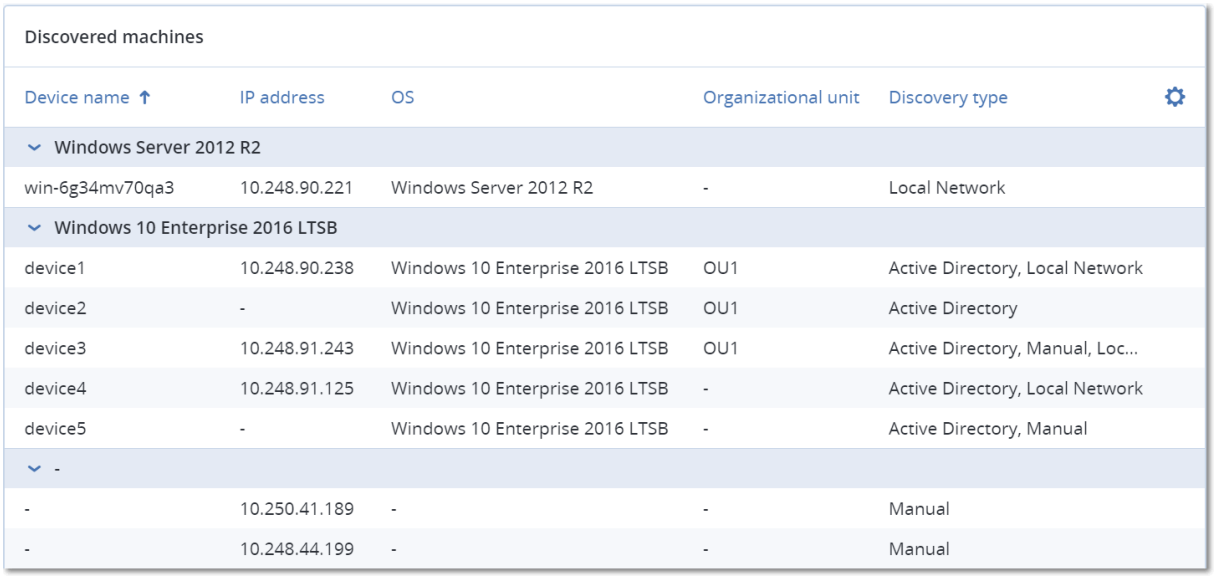
- **Protégé** : machines sur lesquelles le plan de protection est appliqué.
- **Non protégé** : machines sur lesquelles le plan de protection n'est pas appliqué. Elles comprennent à la fois les machines découvertes et les machines gérées auxquelles aucun plan de protection n'est appliqué.
- **Géré** : machines sur lesquelles l'agent de protection est installé.
- **Découvert** : les machines sur lesquelles l'agent de protection n'est pas installé.

Si vous cliquez sur l'état de la machine, vous serez redirigé vers la liste des machines qui présentent le même état pour en savoir plus.



Machines découvertes

Ce widget affiche la liste des machines découvertes pendant la période spécifiée.



Discovered machines

Device name ↑	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Manual, Loc...
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Local Network
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Manual
-				
-	10.250.41.189	-	-	Manual
-	10.248.44.199	-	-	Manual

Widgets de protection évolutive des points de terminaison

La fonction EDR comprend sept widgets qui sont tous accessibles depuis le tableau de bord **Vue d'ensemble**. Trois d'entre eux sont également affichés par défaut dans la fonctionnalité EDR (voir "Examen des incidents" (p. 950)).

Voici les sept widgets disponibles :

- Distribution des principaux incidents par ressource
- Statut de la menace (affiché dans EDR)
- Historique de gravité de l'incident (affiché dans EDR)
- Temps moyen de réparation des incidents de sécurité
- Résolution des incidents de sécurité
- Détection par tactique (affiché dans EDR)
- Statut réseau des ressources

Distribution des principaux incidents par ressource

Ce widget affiche les cinq premières ressources qui comportent le plus d'incidents (cliquez sur **Afficher tout** pour rediriger l'utilisateur vers la liste des incidents ; elle est filtrée en fonction des paramètres du widget).

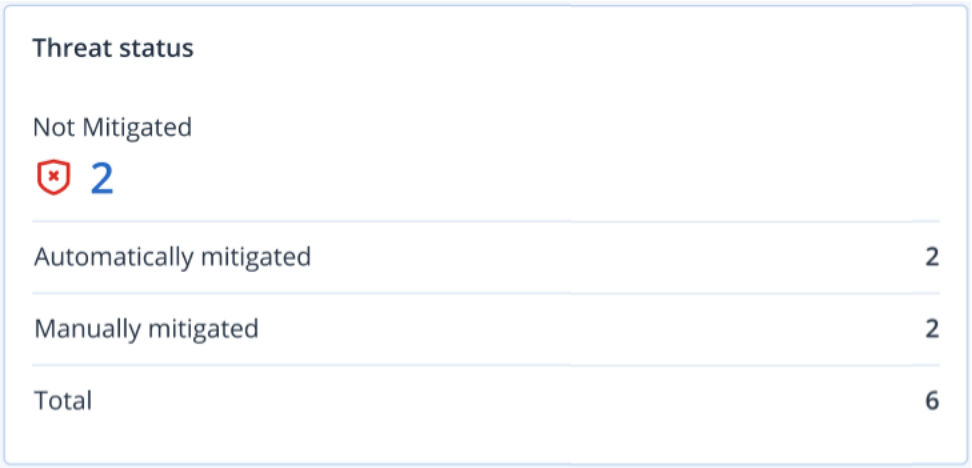
Survolez une ligne de ressource pour afficher le détail de l'état des enquêtes en cours menées sur les incidents ; les états d'enquête sont les suivants : **Non démarrée**, **Enquête en cours**, **Clôturée** et

Faux positif. Cliquez ensuite sur la ressource que vous souhaitez analyser plus en détail ; la liste des incidents est actualisée en fonction des paramètres du widget.

Statut de la menace

Ce widget affiche le statut de menace actuel pour toutes les ressources en mettant en évidence le nombre actuel d'incidents qui ne sont pas résolus et doivent faire l'objet d'enquêtes. Le widget indique également le nombre d'incidents résolus (manuellement et/ou automatiquement par le système).

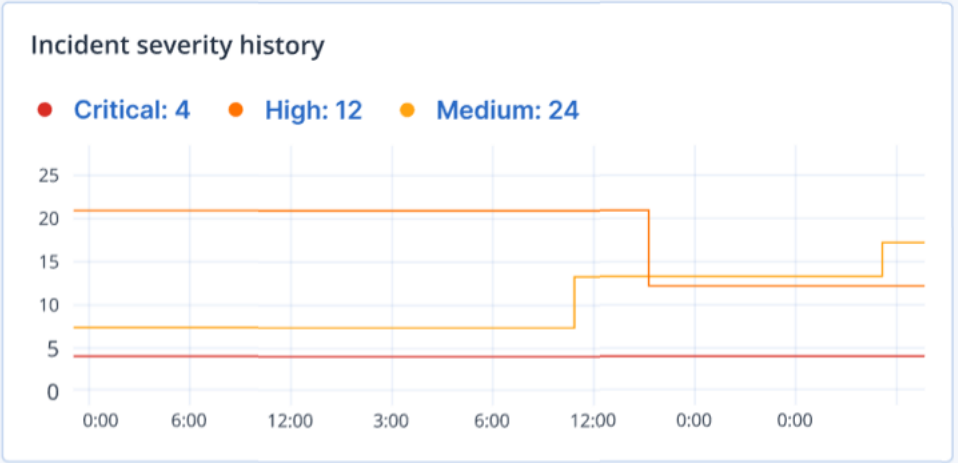
Cliquez sur le numéro **Non atténué** pour affiche la liste des incidents non résolus uniquement.



Historique de gravité de l'incident

Ce widget affiche l'évolution des attaques classées par gravité et peut indiquer des campagnes d'attaques. Lorsque des pics sont visibles, cela indique que l'organisation subit une attaque.

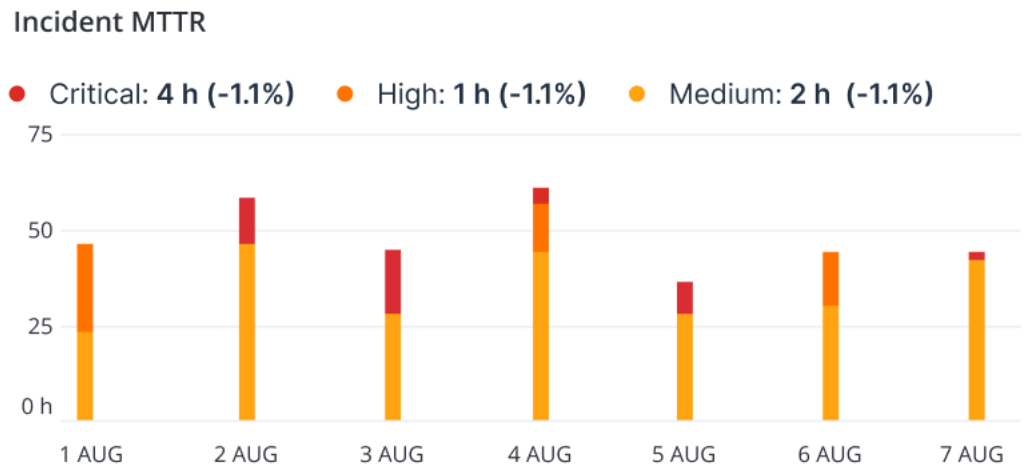
Survolez le graphique pour afficher le détail de l'historique d'un incident à un point spécifique au cours des 24 dernières heures (période par défaut). Cliquez sur le niveau de gravité (**Critique**, **Élevé** ou **Moyen**) si vous souhaitez afficher la liste des incidents associés. Vous êtes alors redirigé vers la liste préfiltrée des incidents correspondant au niveau de gravité sélectionné.



Temps moyen de réparation des incidents de sécurité

Ce widget affiche le temps de résolution moyen des incidents de sécurité. Il indique la vitesse à laquelle les incidents font l'objet d'enquêtes et sont résolus.

Cliquez sur une colonne pour afficher le détail des incidents en fonction de la gravité (**Critique**, **Élevé** et **Moyen**), ainsi qu'une indication de la durée qui a été nécessaire à la résolution des différents niveaux de gravité. La valeur % figurant entre parenthèses indique l'augmentation ou la diminution par rapport à la période précédente.

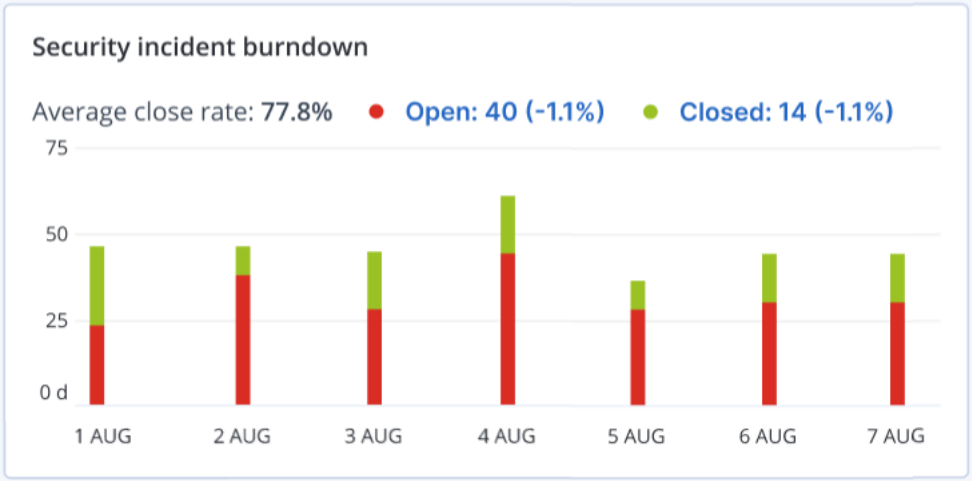


Résolution des incidents de sécurité

Ce widget indique l'efficacité de la clôture des incidents ; le nombre d'incidents ouverts est mesuré en fonction du nombre d'incidents clôturés pendant une période définie.

Survolez une colonne pour afficher le détail des incidents clôturés et ouverts pour le jour sélectionné. Si vous cliquez sur Ouvrir, la liste des incidents apparaît et n'affiche que les incidents ouverts (état **Enquête en cours** ou **Non démarré**). Si vous cliquez sur Clôturé, la liste des incidents qui s'affiche ne répertorie que les incidents qui ne sont plus ouverts (état **Clôturé** ou **Faux positif**).

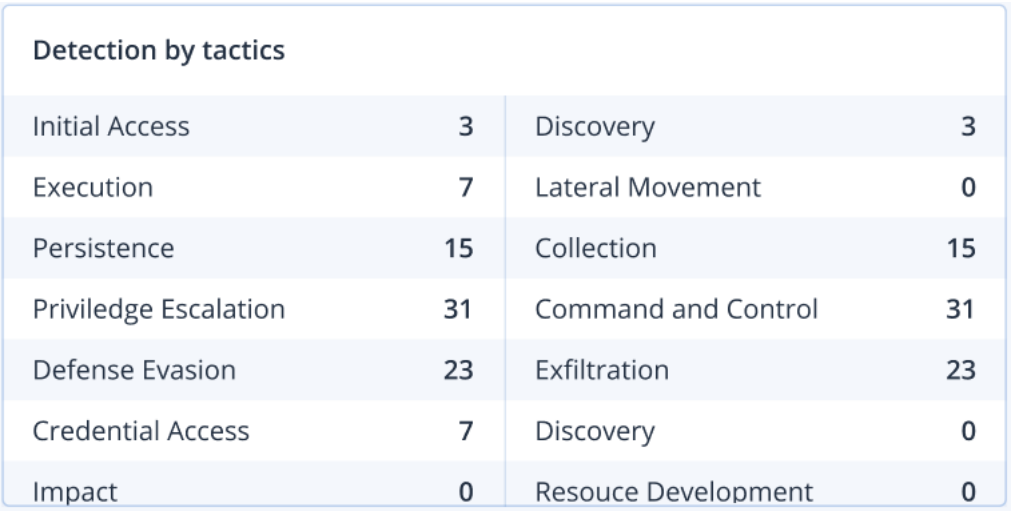
La valeur % figurant entre parenthèses indique l'augmentation ou la diminution par rapport à la période précédente.



Détection par tactique

Ce widget affiche le nombre de techniques d'attaque spécifiques détectées dans les incidents au cours de la période sélectionnée.

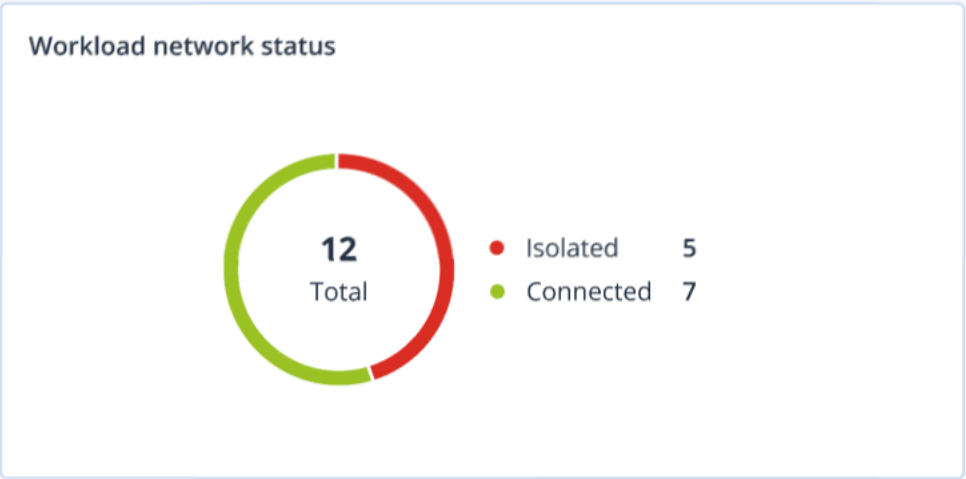
Les valeurs affichées en vert et en rouge indiquent respectivement une augmentation ou une diminution au cours de la période précédente. Dans l'exemple ci-dessous, les attaques d'élévation de privilèges et de commande et contrôle ont augmenté au cours de la période précédente. Cela peut indiquer que votre gestion des identifiants doit être analysée et que les mesures de sécurité doivent être améliorées.



Statut réseau des ressources

Ce widget affiche le statut réseau actuel de vos ressources ; il indique le nombre de ressources isolées et le nombre de ressources connectées.

Cliquez sur Isolé (dans le menu **Ressources** sur la console Cyber Protect) pour afficher uniquement la liste des ressources isolées avec agents. Cliquez sur Connecté pour afficher la liste des ressources avec agents connectées.



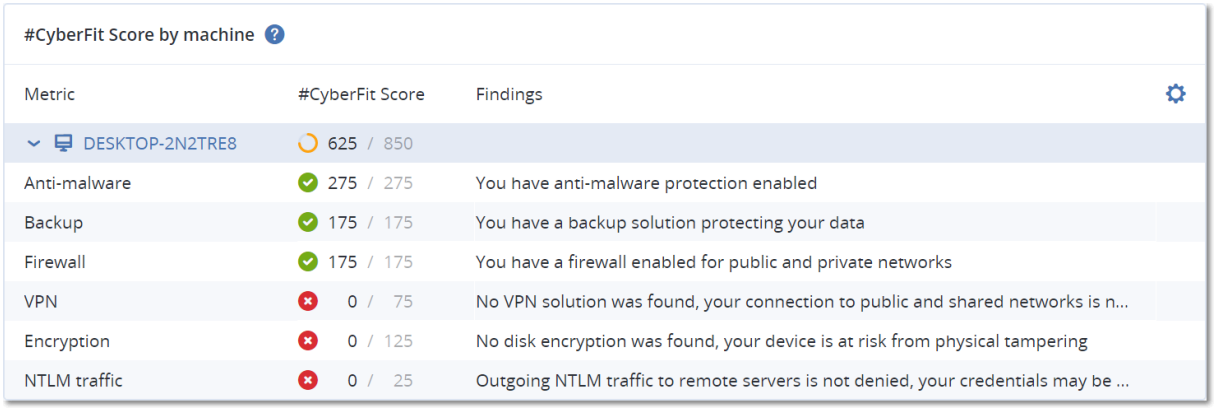
Score #CyberFit par machine

Ce widget affiche, pour chaque machine, le Score #CyberFit total, une combinaison de ses scores ainsi que les résultats pour chaque indicateur évalué :

- Anti-malware
- Sauvegarde
- Pare-feu
- VPN
- Chiffrement
- Trafic NTLM

Afin d'améliorer le score de chaque indicateur, vous pouvez afficher les recommandations disponibles dans le rapport.

Pour en savoir plus sur le Score #CyberFit, reportez-vous à « Score #CyberFit pour les machines ».



Surveillance de l'intégrité du disque

La surveillance de l'intégrité du disque fournit des informations sur l'intégrité actuelle du disque, ainsi que des prévisions concernant cette dernière. Vous pouvez ainsi prévenir les pertes de données liées à une panne du disque. Les disques durs, tout comme les SSD, sont pris en charge.

Limites

- La prévision de l'intégrité du disque est prise en charge uniquement pour les ordinateurs Windows.
- Seuls les disques des machines physiques sont surveillés. Les disques des machines virtuelles ne peuvent pas être surveillés et ne s'affichent pas dans les widgets d'intégrité du disque.
- Les configurations RAID ne sont pas prises en charge. Les widgets d'intégrité du disque n'incluent aucune information sur les ordinateurs avec implémentation RAID.
- Les disques SSD NVMe ne sont pas supportés.

L'intégrité du disque est représentée par l'un des états suivants :

- **OK :**
  l'intégrité du disque est comprise entre 70 et 100 %.
- **Avertissement :**
  l'intégrité du disque est comprise entre 30 et 70 %.
- **Critique :**
  l'intégrité du disque est comprise entre 0 et 30 %.
- **Calcul des données du disque :**
  l'intégrité actuelle et la prévision de l'intégrité du disque sont en cours de calcul.

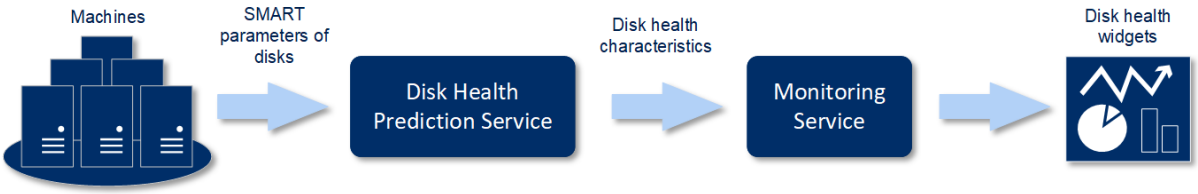
Fonctionnement

Le service Prévision de l'intégrité du disque se sert d'un modèle de prévision basé sur l'intelligence artificielle.

1. L'agent de protection collecte les paramètres SMART des disques et transmet ces données au service Prévision de l'intégrité du disque :
   - SMART 5 : nombre de secteurs réalloués.
   - SMART 9 : nombre d'heures de fonctionnement.
   - SMART 187 : nombre d'erreurs signalées qui n'ont pas été corrigées.
   - SMART 188 : expiration de commandes.
   - SMART 197 : nombre actuel de secteurs en attente.
   - SMART 198 : nombre de secteurs hors ligne impossible à corriger.
   - SMART 200 : taux d'erreurs d'écriture.

2. Le service Prévision de l'intégrité du disque traite les paramètres SMART reçus, effectue des prévisions, puis fournit les caractéristiques d'intégrité du disque suivantes :
   - État de santé actuel du disque : OK, Avertissement, Critique.
   - Prévision de l'état de santé du disque : négatif, stable, positif.
   - Probabilité de prévision de l'état de santé du disque en pourcentage.

   La période de prévision est d'un mois.
3. Le service de surveillance reçoit ces caractéristiques, puis affiche les informations pertinentes dans les widgets d'intégrité du disque dans la console Cyber Protect.



Widgets de l'état de santé du disque

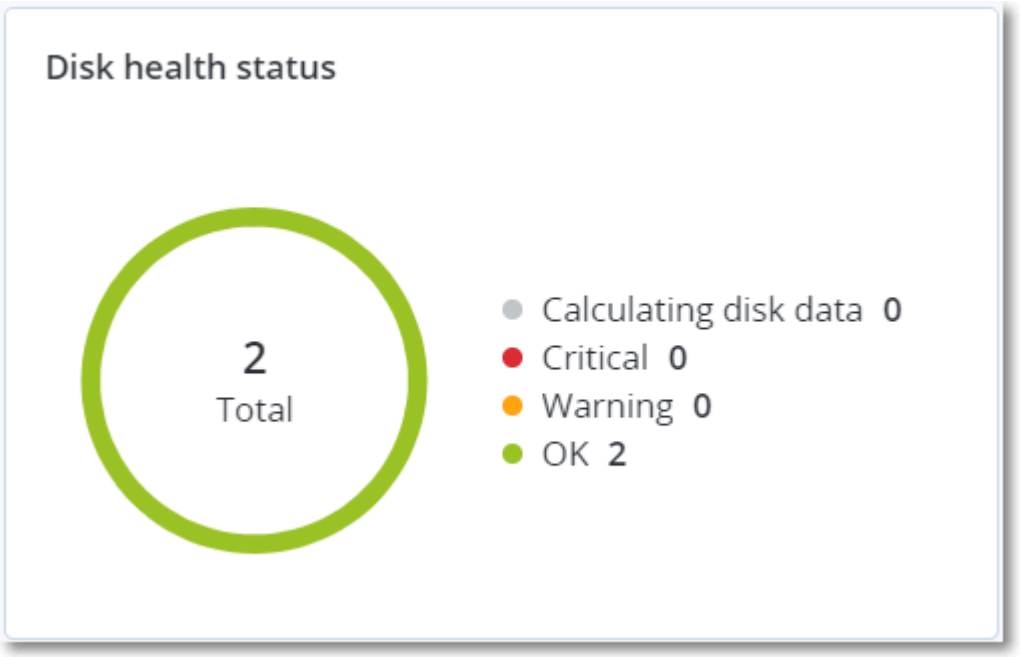
Les résultats de la surveillance de l'intégrité du disque sont présentés dans les widgets suivants, disponibles dans la console Cyber Protect.

- **Vue d'ensemble de l'intégrité du disque** est un widget en forme de carte proportionnelle, qui possède deux niveaux de détails que vous pouvez explorer :
  - Niveau ordinateur
    Affiche des informations résumées concernant l'intégrité du disque en fonction des ordinateurs client que vous avez sélectionnés. Seul l'état de disque le plus critique est affiché. Les autres états s'affichent dans une info-bulle lorsque vous passez le pointeur sur un bloc en particulier. La taille du bloc d'un ordinateur dépend de la taille totale de l'ensemble de ses disques. La couleur du bloc d'une machine dépend de l'état de disque le plus critique identifié.

- Niveau disque
  Affiche l'intégrité actuelle de tous les disques pour l'ordinateur sélectionné. Chaque bloc de disque affiche les prévisions d'intégrité du disque suivantes, ainsi que leur probabilité en pourcentage :
  - Sera altéré
  - Restera stable

- Sera amélioré

- **Intégrité du disque** est un widget de graphique circulaire qui affiche le nombre de disques pour chaque état.



Alertes relatives à l'état de santé du disque

La vérification de l'intégrité du disque est exécutée toutes les 30 minutes, alors que l'alerte correspondante n'est générée qu'une fois par jour. Lorsque l'intégrité du disque passe de **Avertissement** à **Critique**, une alerte est toujours générée.

Nom de l'alerte	La gravité	Intégrité du disque	Description
Une défaillance du disque dur est possible	Avertissement	(30 – 70)	Il est possible que le disque <nom du disque> sur cet ordinateur échoue à l'avenir. Exécutez une sauvegarde d'image complète du disque dès que possible, remplacez ce dernier, puis restaurez l'image sur le nouveau disque.
La défaillance du disque dur est imminente	Critique	(0 – 30)	Le disque <nom du disque> sur cet ordinateur est dans un état critique et risque fortement d'échouer très bientôt. Nous ne vous recommandons pas d'effectuer une sauvegarde d'image de ce disque à ce stade, car la contrainte supplémentaire risque de causer la défaillance du disque. Sauvegardez les fichiers les plus importants sur le disque dès maintenant et remplacez-le.

Carte de la protection des données

Remarque
Cette fonctionnalité est disponible avec le pack Advanced Backup.

La fonctionnalité Carte de la protection des données vous permet de découvrir toutes les données qui ont une importance à vos yeux, et d'obtenir des informations détaillées concernant le nombre, la taille, l'emplacement et l'état de protection de tous les fichiers importants, le tout sous forme de carte proportionnelle dont vous pouvez faire varier l'échelle.

La taille de chaque bloc dépend du nombre total ou de la taille totale des fichiers importants qui appartiennent à un client ou à une machine.

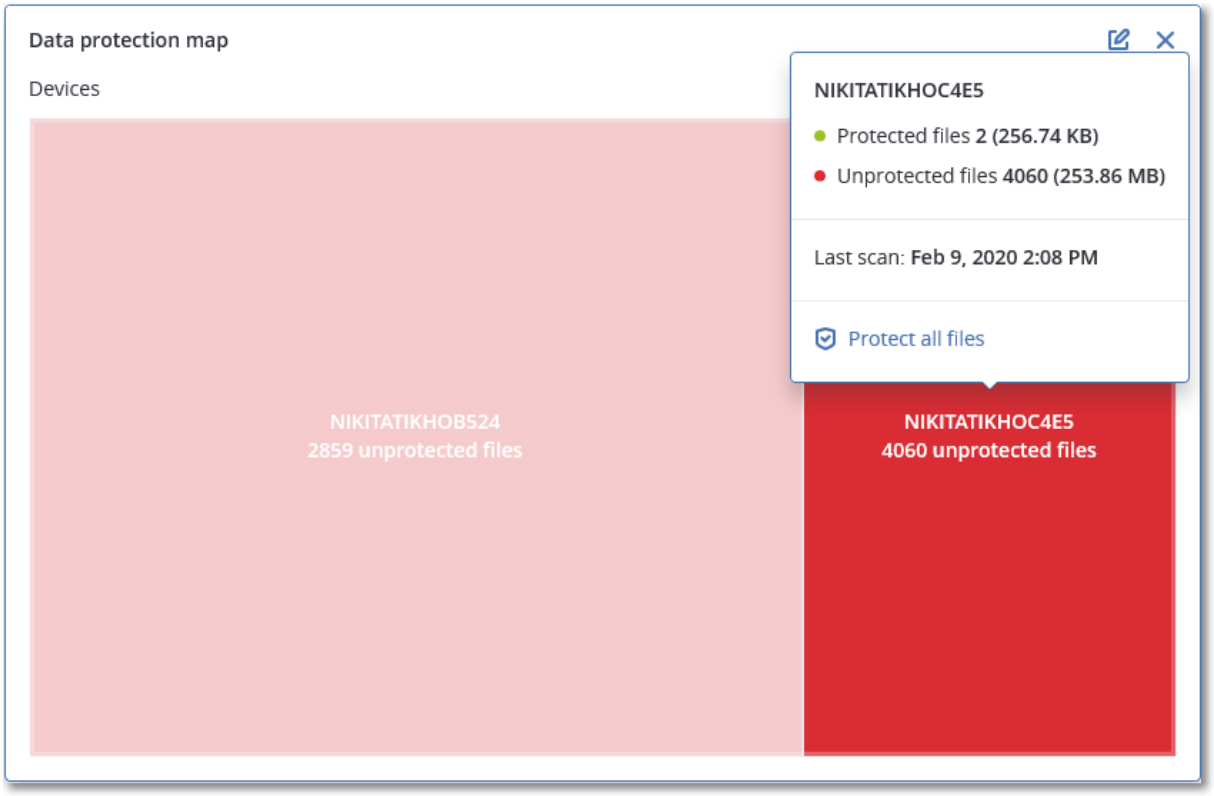
Les fichiers peuvent présenter l'un des états de protection suivants :

- **Critique** : de 51 à 100 % des fichiers non protégés et présentant l'extension que vous avez spécifiée ne sont pas sauvegardés et ne le seront pas non plus avec les paramètres de sauvegarde existants pour la machine ou l'emplacement sélectionné.
- **Basse** : de 21 à 50 % des fichiers non protégés et présentant l'extension que vous avez spécifiée ne sont pas sauvegardés et ne le seront pas non plus avec les paramètres de sauvegarde existants pour la machine ou l'emplacement sélectionné.

- **Moyen** : de 1 à 20 % des fichiers non protégés et présentant l'extension que vous avez spécifiée ne sont pas sauvegardés et ne le seront pas non plus avec les paramètres de sauvegarde existants pour la machine ou l'emplacement sélectionné.
- **Élevé** : tous les fichiers présentant l'extension que vous avez spécifiée sont protégés (sauvegardés) pour la machine ou l'emplacement sélectionné.

Les résultats de l'examen de la protection des données sont disponibles sur le tableau de bord de surveillance dans le widget Carte de la protection des données, un widget sous forme de carte proportionnelle, qui permet d'afficher des informations au niveau de l'ordinateur :

- Niveau machine : affiche des informations concernant l'état de protection de fichiers importants en fonction des machines du client sélectionné.



Pour protéger des fichiers qui ne sont pas protégés, passez le pointeur de la souris sur le bloc, puis cliquez sur **Protéger tous les fichiers**. Dans la boîte de dialogue, vous trouverez des informations concernant le nombre de fichiers non protégés, ainsi que leur emplacement. Pour les protéger, cliquez sur **Protéger tous les fichiers**.

Vous pouvez aussi télécharger un rapport détaillé au format CSV.

Widgets d'évaluation des vulnérabilités

Machines vulnérables

Ce widget affiche les ordinateurs vulnérables en les classant en fonction de la gravité de leur vulnérabilité.

La vulnérabilité découverte peut présenter l'un des niveaux de gravité suivants, d'après le système d'évaluation des vulnérabilités (CVSS) v3.0 :

- Sécurisé : aucune vulnérabilité n'a été trouvée
- Critique : 9,0 – 10,0 CVSS
- Élevé : 7,0 – 8,9 CVSS
- Moyen : 4,0 – 6,9 CVSS
- Faible : 0,1 – 3,9 CVSS
- Aucun : 0,0 CVSS

Vulnérabilités existantes

Ce widget affiche les vulnérabilités existant actuellement sur les machines. Dans le widget **Vulnérabilités existantes**, il existe deux colonnes affichant la date et l'heure de la dernière modification :

- **Première détection** : date et heure à laquelle une vulnérabilité a initialement été détectée sur une machine.
- **Dernière détection** : date et heure à laquelle une vulnérabilité a été détectée sur une machine pour la dernière fois.

Existing vulnerabilities

Machine name	Vendor	Product	Vulnerability name/ID	Severity	Last detected	First detected
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM

More

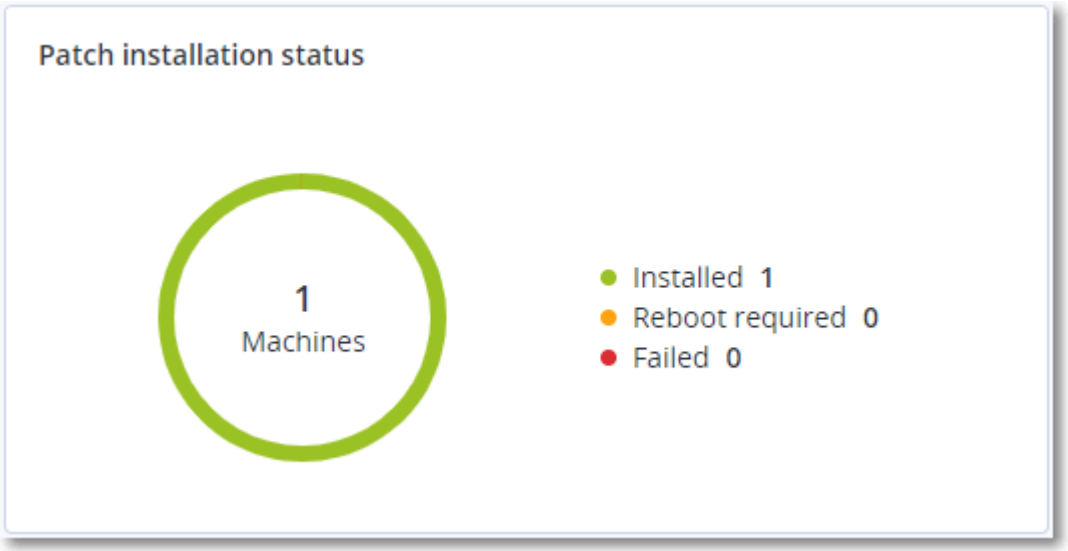
Widgets d'installation des correctifs

Il existe quatre widgets en lien avec la fonctionnalité de gestion des correctifs.

Statut d'installation des correctifs

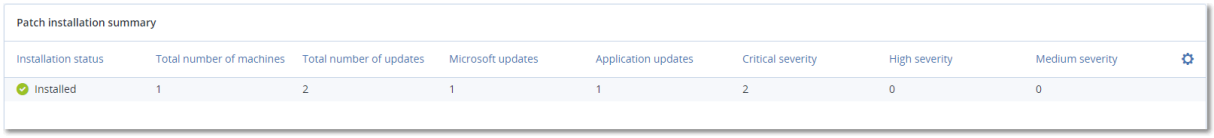
Ce widget affiche le nombre de machines, en les regroupant par statut d'installation des correctifs.

- **Installé :** tous les correctifs disponibles sont installés sur une machine.
- **Redémarrage nécessaire :** après l'installation des correctifs, un redémarrage est requis pour une machine.
- **Échec :** l'installation des correctifs sur une machine a échoué.



Résumé d'installation des correctifs

Ce widget affiche le résumé des correctifs sur les machines, en les regroupant par statut d'installation des correctifs.



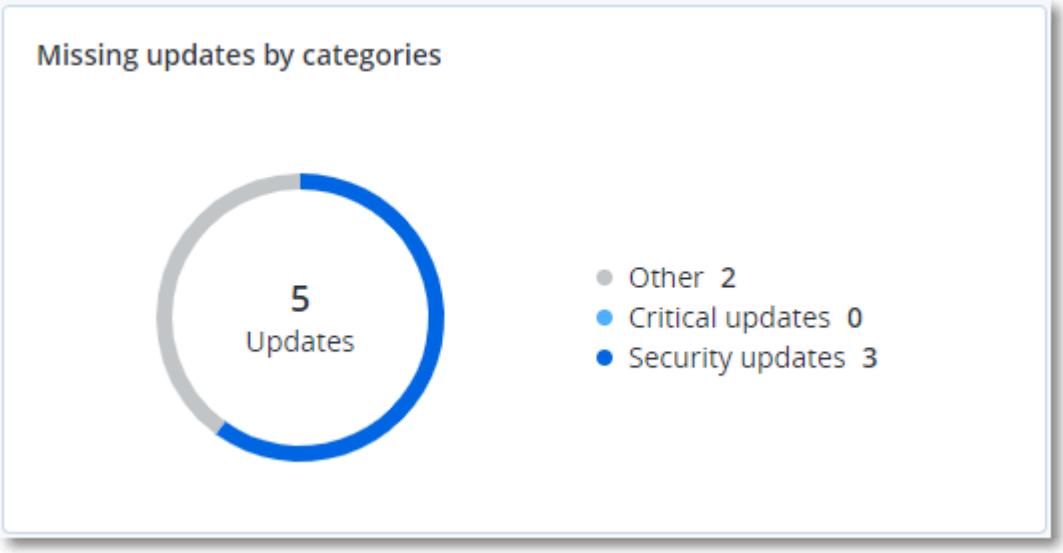
Historique d'installation des correctifs

Ce widget affiche des informations détaillées au sujet des correctifs sur les machines.

Mises à jour manquantes, par catégorie

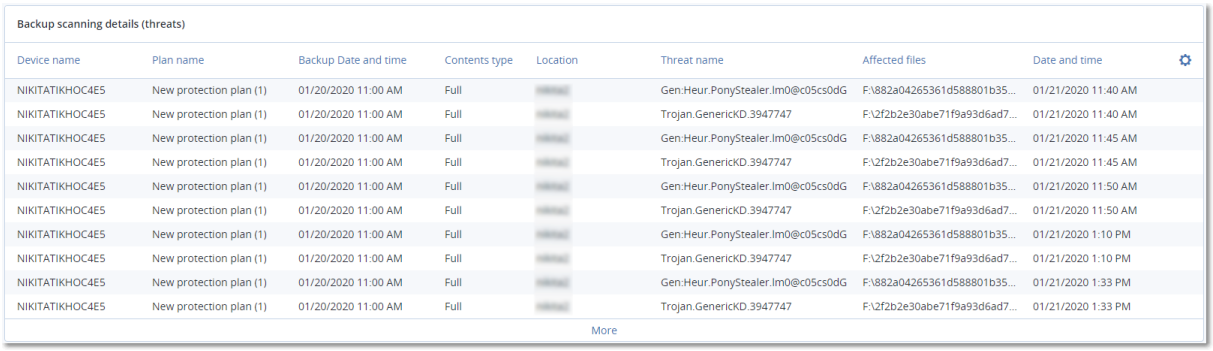
Ce widget affiche le nombre de mises à jour manquantes, en les classant par catégorie Les catégories suivantes sont répertoriées :

- Mises à jour de sécurité
- Mises à jour critiques
- Autre



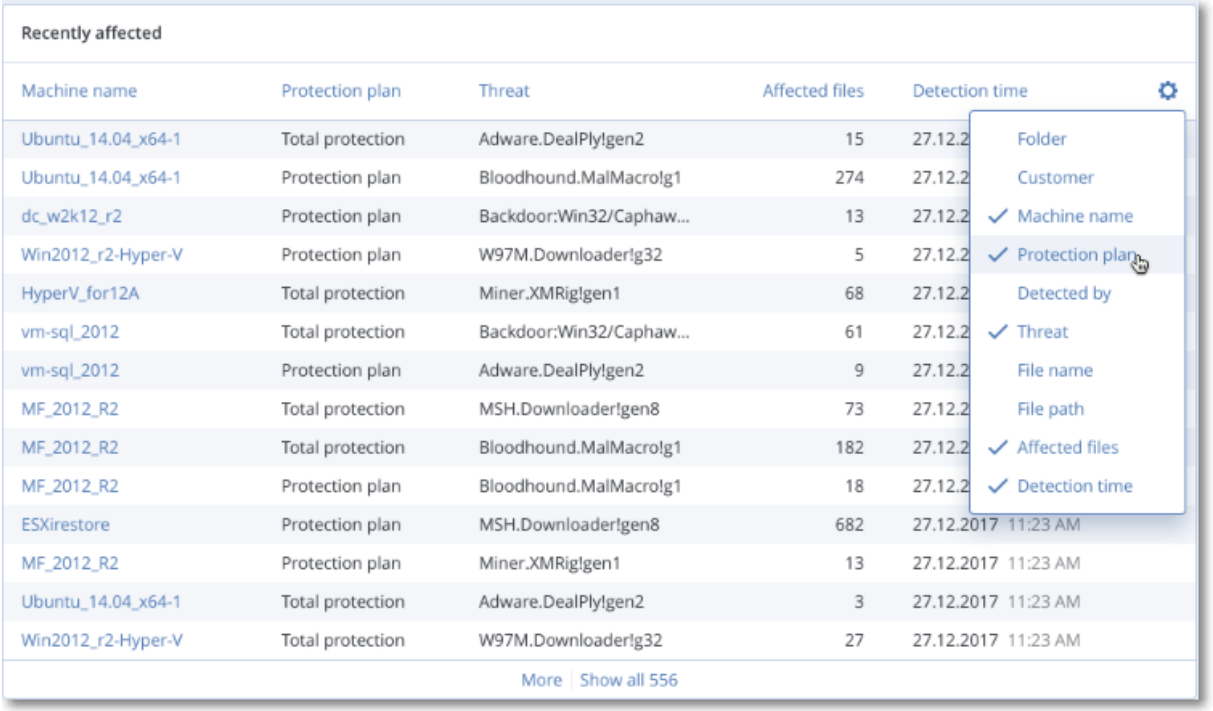
Détails de l'analyse de la sauvegarde

Ce widget affiche des informations détaillées au sujet des menaces détectées dans les sauvegardes.



Affectés récemment

Ce widget montre des informations détaillées au sujet des ressources touchées par des menaces telles que des virus, des malwares et des ransomwares. Vous y trouverez des informations concernant les menaces détectées, l'heure de détection et le nombre de fichiers touchés.



Téléchargement de données pour les ressources récemment affectées

Vous pouvez télécharger les données pour les ressources récemment affectées, générer un fichier CSV et l'envoyer aux destinataires que vous spécifiez.

Pour télécharger les données pour les ressources récemment affectées

1. Dans le widget **Affectés récemment**, cliquez sur **Télécharger les données**.
2. Dans le champ **Période**, saisissez le nombre de jours pendant lequel vous souhaitez télécharger des données. Le nombre maximum de jours que vous pouvez entrer est 200.

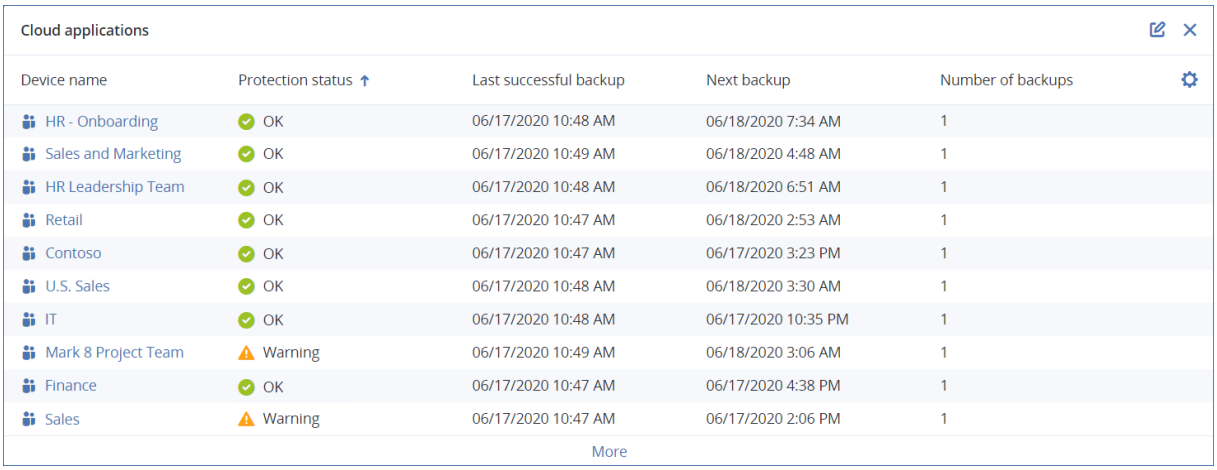
3. Dans le champ **Destinataires**, saisissez l'adresse e-mail de toutes les personnes qui recevront un e-mail avec un lien pour télécharger le fichier CSV.
4. Cliquez sur **Télécharger**.

   Le système commence à générer le fichier CSV avec les données pour les ressources qui ont été affectées au cours de la période que vous avez spécifiée. Quand le fichier CSV est prêt, le système envoie un e-mail aux destinataires. Chaque destinataire peut ensuite télécharger le fichier CSV.

Applications dans le Cloud

Ce widget affiche des informations détaillées concernant les ressources de Cloud à Cloud :

- Utilisateurs Microsoft 365 (boîte aux lettres, OneDrive)
- Groupes Microsoft 365 (boîte aux lettres, site de groupe)
- Dossiers publics Microsoft 365
- Collections de sites Microsoft 365
- Microsoft 365 Teams
- Utilisateurs Google Workspace (Gmail, Google Drive)
- Drive partagés Google Workspace



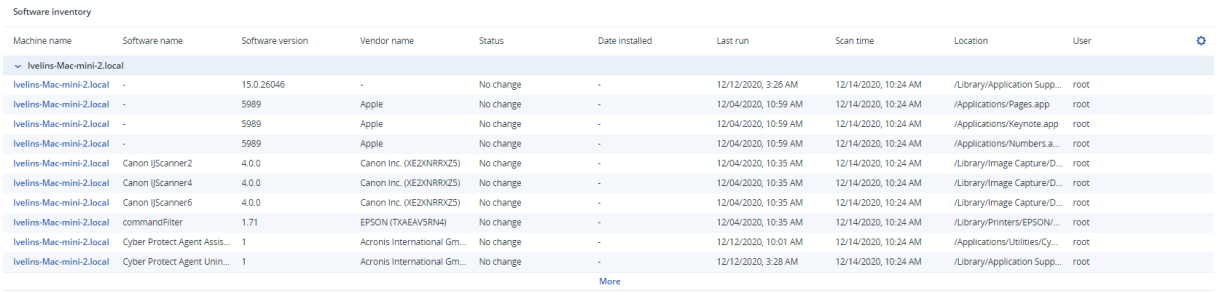
Vous trouverez des ressources de Cloud à Cloud supplémentaires dans les widgets suivants :

- Activités
- Liste des activités
- 5 dernières alertes
- Historique des alertes
- Résumé des alertes actives
- Résumé de l'historique des alertes

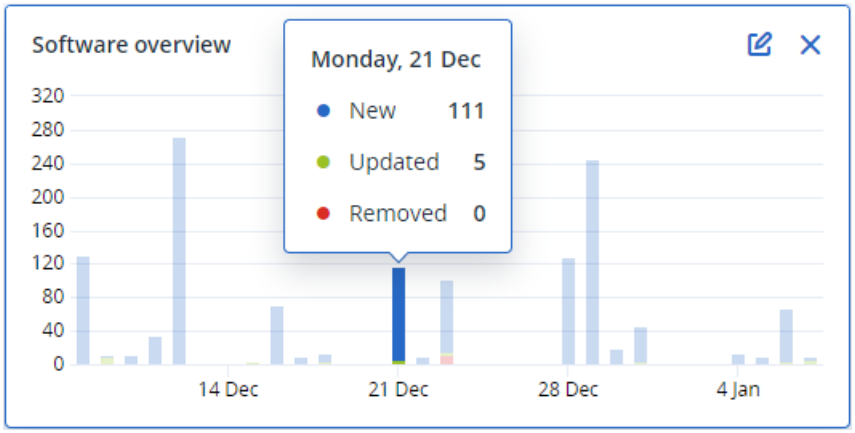
- Détails de l'alerte active
- Résumé des emplacements

Widget d'inventaire du logiciel

Le widget de tableau **Inventaire du logiciel** contient des informations détaillées concernant tout le logiciel installé sur les terminaux physiques Windows et macOS de votre organisation.



Le widget **Aperçu du logiciel** contient le nombre de nouvelles applications ou d'applications mises à jour et supprimées sur les terminaux physiques Windows et macOS de votre organisation sur une période donnée (7 jours, 30 jours ou le mois en cours).



Lorsque vous passez le pointeur sur une barre en particulier, une infobulle contenant les informations suivantes s'affiche :

Nouvelles – le nombre d'applications nouvellement installées.

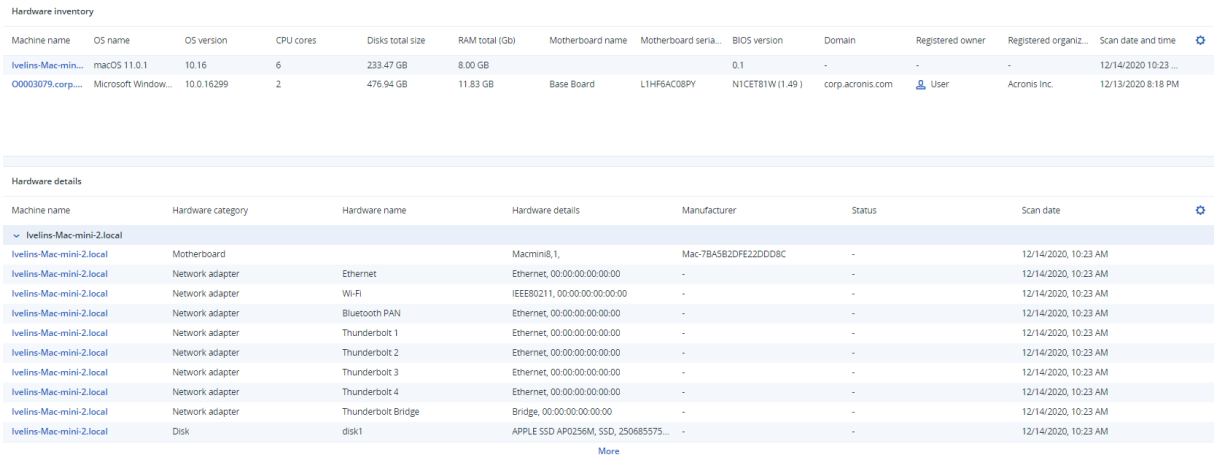
Mises à jour – le nombre d'applications mises à jour.

Supprimées – le nombre d'applications supprimées.

Lorsque vous cliquez sur la partie de la barre correspondant à un certain statut, vous êtes redirigé vers la page **Gestion de logiciel** -> **Inventaire du logiciel**. Les informations de cette page sont filtrées en fonction de la date et du statut correspondants.

Widgets d'inventaire du matériel

Les widgets de tableau **Inventaire du matériel** et **Détails du matériel** contiennent des informations concernant tout le matériel installé sur les terminaux physiques et virtuels Windows et macOS de votre organisation.



Hardware inventory

Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner	Registered organiz...	Scan date and time
Ivelins-Mac-min...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-	-	12/14/2020 10:23 ...
O0003079.corp....	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.acronis.com	User	Acronis Inc.	12/13/2020 8:18 PM

Hardware details

Machine name	Hardware category	Hardware name	Hardware details	Manufacturer	Status	Scan date
Ivelins-Mac-mini-2.local						
Ivelins-Mac-mini-2.local	Motherboard		Macmini8,1,	Mac-7BA5B2DFE22DDD8C	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Ethernet	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Wi-Fi	IEEE80211, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Bluetooth PAN	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 1	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 2	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 3	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 4	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt Bridge	Bridge, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Disk	disk1	APPLE SSD AP0256M, SSD, 250685575...	-	-	12/14/2020, 10:23 AM

More

Le widget de tableau **Modifications apportées au matériel** contient des informations concernant le matériel ajouté, supprimé et modifié sur les terminaux physiques et virtuels Windows et macOS de votre organisation sur une période donnée (7 jours, 30 jours ou le mois en cours).

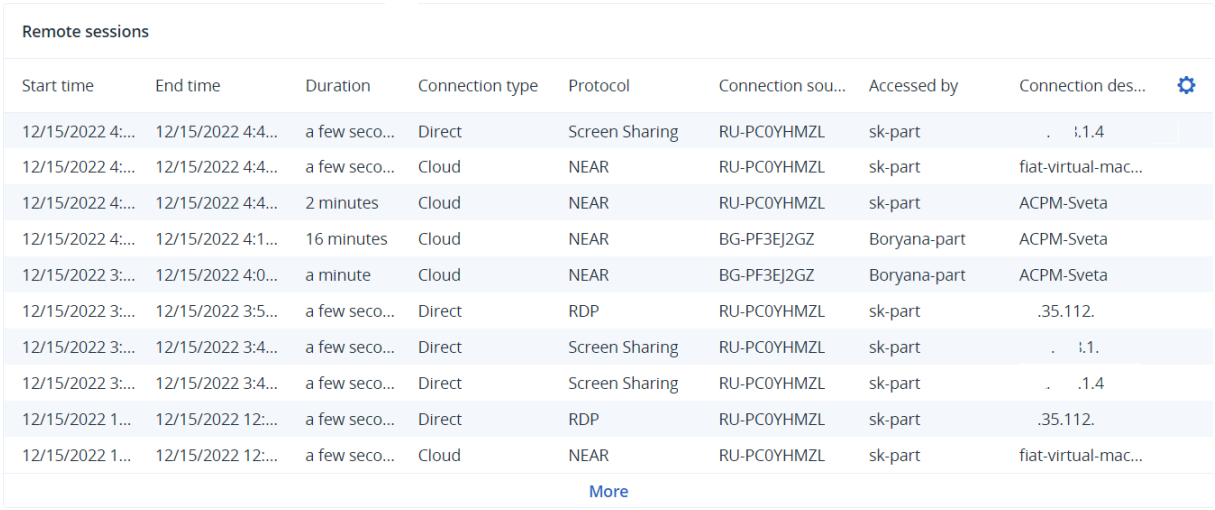
Hardware changes

Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF					
DESKTOP-0FF9TTF	Network adapter	Changed	Oracle Corporation, Ethernet 802.3,...	Oracle Corporation, Ethernet 802.3, ...	01/11/2021 9:28 AM
DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor Corp., Ether...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Torronto 5C1, PF0PJB10	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), WDC WD10JP...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 802.3, 00:0...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ethernet 802.3, ...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00 GB	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows Provider V9...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM

More

Widget Sessions distantes

Ce widget affiche les informations détaillées concernant les sessions Bureau à distance et transfert de fichiers.



Remote sessions

Start time	End time	Duration	Connection type	Protocol	Connection sou...	Accessed by	Connection des...
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...
12/15/2022 4:...	12/15/2022 4:4...	2 minutes	Cloud	NEAR	RU-PC0YHMZL	sk-part	ACPM-Sveta
12/15/2022 4:...	12/15/2022 4:1...	16 minutes	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 4:0...	a minute	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 3:5...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 1...	12/15/2022 12:...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 1...	12/15/2022 12:...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...

More

Protection intelligente

Flux de menaces

Le centre opérationnel de cyber protection Acronis (CPOC) génère des alertes de sécurité qui sont envoyées uniquement aux régions géographiques concernées. Ces alertes de sécurité fournissent des informations sur les malwares, les vulnérabilités, les catastrophes naturelles, la santé publique, et d'autres types d'événements mondiaux qui peuvent avoir un impact sur la protection des données. Le flux de menaces vous informe des menaces potentielles et vous permet de les éviter.

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

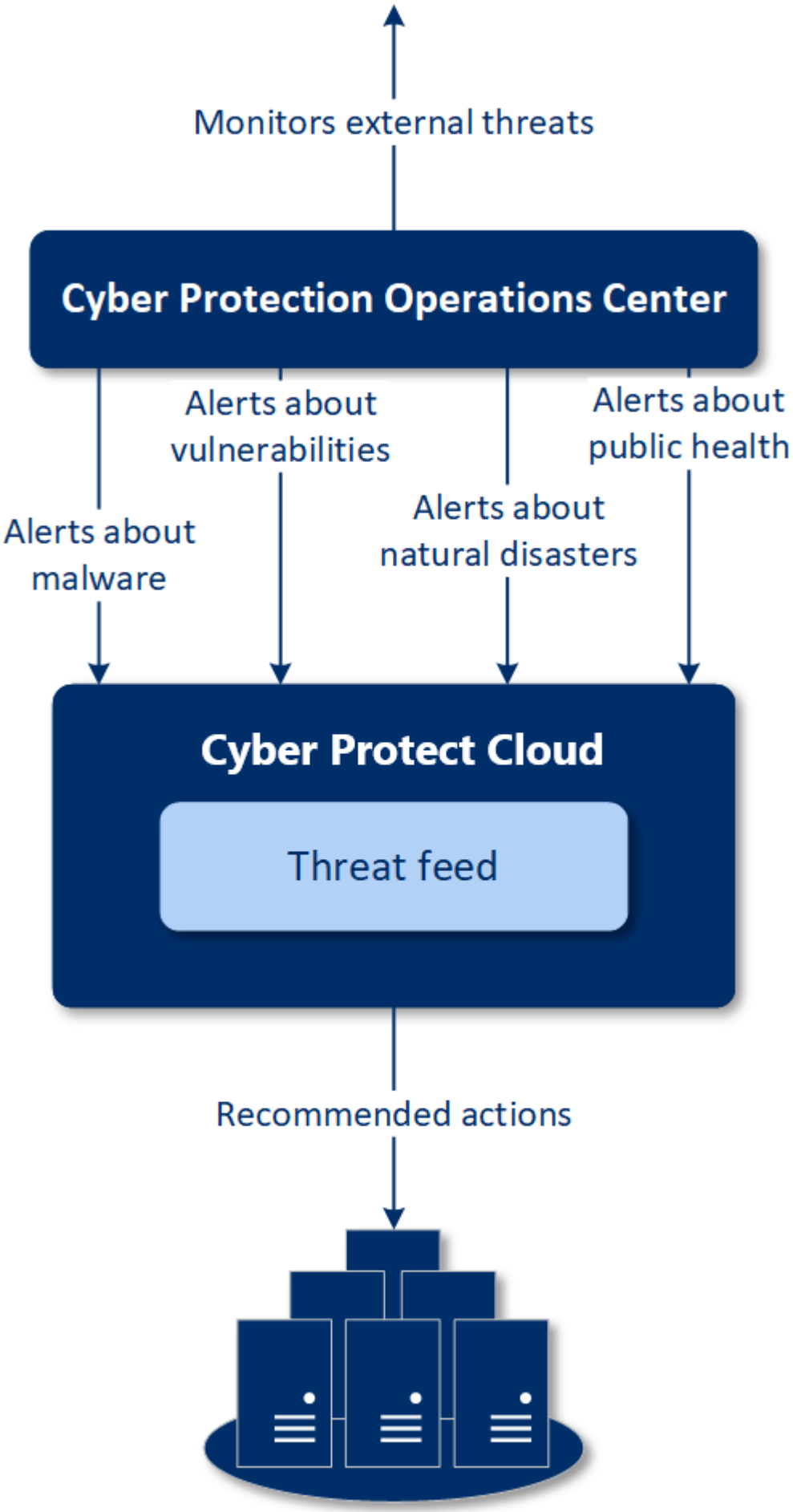
Certaines alertes de sécurité peuvent être résolues en suivant un ensemble d'actions spécifiques fournies par les experts de la sécurité. D'autres alertes de sécurité vous informent simplement de menaces à venir, mais ne vous recommandent pas d'actions de réparation.

Remarque
Des alertes de malware sont générées uniquement pour les ordinateurs sur lesquelles l'agent de protection antimalware est installé.

Fonctionnement

Le centre opérationnel de cyber protection Acronis surveille les menaces externes et génère des alertes concernant les menaces liées aux malwares, aux vulnérabilités, aux catastrophes naturelles et à la santé publique. Vous pourrez consulter toutes ces alertes dans la console Cyber Protect, dans la section **Flux de menaces**. Selon le type d'alerte, vous pouvez exécuter les actions de réparation recommandées respectives.

La procédure principale de ce flux de menaces est illustrée dans le diagramme ci-dessous.

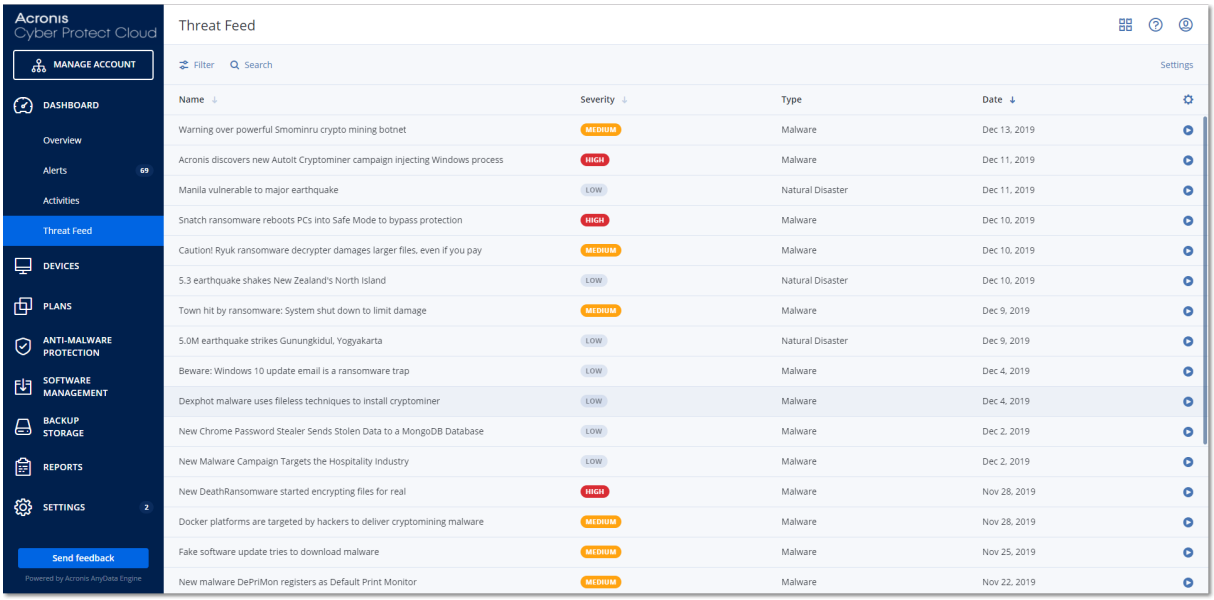


Pour exécuter les actions recommandées suite aux alertes envoyées par le centre opérationnel de cyber protection Acronis, procédez comme suit :

1. Dans la console Cyber Protect, accédez à **Surveillance** > **Flux de menaces** pour vérifier s'il existe des alertes de sécurité.
2. Sélectionnez une alerte dans la liste, puis consultez les détails fournis.
3. Cliquez sur **Démarrer** pour lancer l'assistant.
4. Sélectionnez les actions que vous souhaitez effectuer, ainsi que les machines auxquelles ces actions doivent être appliquées. Les actions suivantes peuvent être suggérées :
   - **Évaluation des vulnérabilités :** pour analyser les machines à la recherche de vulnérabilités.
   - **Gestion des correctifs :** pour installer des correctifs sur les machines sélectionnées.
   - **Protection contre les malwares :** pour exécuter une analyse complète des machines sélectionnées.

     Remarque
     Cette action est disponible uniquement pour les machines sur lesquelles l'agent de protection contre les malwares est installé.

   - **Sauvegarde de machines protégées ou non protégées :** pour sauvegarder des ressources protégées/non protégées.
     Si aucune sauvegarde n'existe déjà pour la ressource (dans tous les emplacements accessibles, cloud et locaux) ou si les sauvegardes existantes sont chiffrées, le système crée une sauvegarde complète avec le format de nom suivant :
     `%workload_name%-Remediation`
     Par défaut, la destination de la sauvegarde est le stockage Cyber Protect Cloud, mais vous pouvez configurer un autre emplacement avant de commencer l'opération.
     Si une sauvegarde non chiffrée existe déjà, le système crée une sauvegarde incrémentielle dans l'archive existante.
5. Cliquez sur **Démarrer**.
6. Sur la page **Activités**, vérifiez que l'activité a bien été effectuée.



Suppression de toutes les alertes

Le nettoyage automatique du flux des menaces est effectué après les périodes suivantes :

- Catastrophes naturelles : 1 semaine
- Vulnérabilités : 1 mois
- Malwares : 1 mois
- Santé publique : 1 semaine

Carte de la protection des données

La fonctionnalité Carte de la protection des données vous permet d'effectuer les tâches suivantes :

- Obtenir des informations détaillées concernant les données stockées (classification, emplacements, statut de protection et informations supplémentaires) sur vos machines.
- Détecter si les données sont protégées ou non. Les données sont considérées comme protégées si elles sont protégées par une sauvegarde (un plan de protection avec module de sauvegarde activé).
- Effectuer des actions relatives à la protection des données.

Fonctionnement

1. En premier lieu, vous créez un plan de protection avec le module Carte de la protection des données activé.
2. Ensuite, une fois le plan exécuté et vos données découvertes et analysées, vous obtiendrez une représentation visuelle de la protection des données dans le widget Carte de la protection des données.
3. Vous pouvez également accéder à **Terminaux** > **Carte de la protection des données** et y trouver des informations concernant les fichiers non protégés par terminal.

4. Vous pouvez prendre des mesures pour protéger les fichiers non protégés détectés sur les terminaux.

Gestion des fichiers non protégés détectés

Pour protéger les fichiers importants qui ont été détectés comme non protégés, procédez comme suit :

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Carte de la protection des données**.
   Dans la liste des terminaux, vous trouverez des informations générales concernant le nombre de fichiers non protégés, la taille de ces fichiers par terminal, ainsi que la date de dernière découverte.
   Pour protéger les fichiers sur une machine particulière, cliquez sur l'icône en forme de points de suspension, puis sur **Protéger tous les fichiers**. Vous serez redirigé vers la liste de plans dans laquelle vous pouvez créer un plan de protection avec le module de sauvegarde activé.
   Pour supprimer de la liste le terminal particulier qui possède des fichiers non protégés, cliquez sur **Masquer jusqu'à la prochaine découverte de données**.
2. Pour afficher des informations plus détaillées sur les fichiers non protégés sur un terminal en particulier, cliquez sur le nom du terminal.
   Vous verrez le nombre de fichiers non protégés par extension de fichier et par emplacement. Dans le champ de recherche, définissez les extensions de fichier pour lesquelles vous souhaitez obtenir des informations relatives aux fichiers non protégés.
3. Pour protéger les fichiers non protégés, cliquez sur **Protéger tous les fichiers**. Vous serez redirigé vers la liste de plans dans laquelle vous pouvez créer un plan de protection avec le module de sauvegarde activé.

Pour obtenir des informations relatives aux fichiers non protégés sous la forme d'un rapport, cliquez sur **Télécharger le rapport détaillé au format CSV**.

Paramètres de la carte de protection des données

Pour apprendre à créer un plan de protection avec le module de carte de protection des données, reportez-vous à la section « Création d'un plan de protection ».

Vous pouvez définir les paramètres suivants pour le module de carte de protection des données.

Planification

Vous pouvez définir différents paramètres afin de créer le planning selon laquelle la tâche relative à la carte de protection des données sera effectuée.

Champs	Description
Planifiez l'exécution de la tâche à l'aide des événements	Ce paramètre définit le moment où la tâche sera exécutée. Les valeurs suivantes sont disponibles : • **Planifier selon l'horaire** : il s'agit du paramètre par défaut. La tâche

Champs	Description
suivants	sera exécutée selon l'horaire spécifié. • **Lorsque l'utilisateur se connecte au système** : par défaut, la connexion de n'importe quel utilisateur lancera la tâche. Vous pouvez modifier ce paramètre pour que seul un compte utilisateur spécifique déclenche la tâche. • **Lorsqu'un utilisateur se déconnecte du système** : par défaut, la déconnexion de n'importe quel utilisateur lancera la tâche. Vous pouvez modifier ce paramètre pour que seul un compte utilisateur spécifique déclenche la tâche. **Remarque** La tâche ne sera pas lancée lors d'un arrêt du système. Dans la configuration de planification, un arrêt est différent d'une déconnexion. • **Au démarrage du système** : la tâche sera exécutée au démarrage du système d'exploitation. • **À l'arrêt du système** : la tâche sera exécutée à l'arrêt du système d'exploitation.
Type de planification	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Mensuelle :** sélectionnez les mois et les semaines ou jours du mois pendant lesquels la tâche sera exécutée. • **Quotidienne** : il s'agit du paramètre par défaut. Sélectionnez les jours de la semaine au cours desquels la tâche sera exécutée. • **Horaire :** sélectionnez les jours de la semaine, le nombre de répétitions et l'intervalle d'exécution de la tâche.
Débuter à	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants** Sélectionnez l'heure exacte à laquelle la tâche sera exécutée.
Exécuter sur une plage de date	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Configurez une plage pendant laquelle la planification configurée sera effective.
Précisez un compte	Ce champ apparaît si vous avez sélectionné l'option **Lorsque l'utilisateur se connecte au système** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**.

Champs	Description
utilisateur dont la connexion au système d'exploitation lancera une tâche	Les valeurs suivantes sont disponibles : • **Tout utilisateur** : utilisez cette option si vous souhaitez que la connexion de n'importe quel utilisateur déclenche la tâche. • **L'utilisateur suivant** : utilisez cette option si vous souhaitez que la connexion d'un compte utilisateur spécifique déclenche la tâche.
Précisez un compte utilisateur dont la déconnexion du système d'exploitation lancera une tâche	Ce champ apparaît si vous avez sélectionné l'option **Lorsqu'un utilisateur se déconnecte du système** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Tout utilisateur** : utilisez cette option si vous souhaitez que la déconnexion de n'importe quel utilisateur déclenche la tâche. • **L'utilisateur suivant** : utilisez cette option si vous souhaitez que la déconnexion d'un compte utilisateur spécifique déclenche la tâche.
Conditions de démarrage	Définit toutes les conditions qui doivent être remplies simultanément pour que la tâche soit exécutée. Les conditions de démarrage des analyses antimalware sont semblables aux conditions de démarrage du module **Sauvegarde** qui sont décrites dans la section Conditions de démarrage. Vous pouvez définir les conditions de démarrage suivantes : • **Répartir les heures de démarrage de tâche dans une fenêtre de temps :** cette option vous permet de définir le délai pour la tâche afin d'éviter les goulots d'étranglement au niveau du réseau. Vous pouvez indiquer le délai en heures ou minutes. Par exemple, si l'heure de démarrage par défaut est 10 h et que le délai est 60 minutes, la tâche démarrera entre 10 h et 11 h. • **Si la machine est arrêtée, exécutez les tâches ratées lors du démarrage de la machine** • **Empêcher l'activation du mode veille ou veille prolongée lors de l'exécution de la tâche** : cette option fonctionne uniquement pour les machines sous Windows. • **Si les conditions de démarrage ne sont pas remplies, exécutez quand même la tâche au bout de :** spécifiez la période après laquelle la tâche sera lancée, quelles que soient les autres conditions de démarrage. **Remarque** Les conditions de démarrage ne sont pas prises en charge sous Linux.

Extensions et règles d'exception

Dans l'onglet **Extensions**, vous pouvez définir la liste des extensions de fichier qui seront considérées comme importantes lors de la découverte de données, et dont le statut de protection sera vérifié. Pour définir des extensions, utilisez le format suivant :

```
.html, .7z, .docx, .zip, .pptx, .xml
```

Dans l'onglet **Règles d'exception**, vous pouvez définir les fichiers et dossiers dont le statut de protection ne doit pas être vérifié lors de la découverte de données.

- **Fichiers et dossiers cachés :** si cette option est sélectionnée, les fichiers et dossiers cachés seront ignorés lors de l'examen des données.
- **Fichiers et dossiers système :** si cette option est sélectionnée, les fichiers et dossiers système seront ignorés lors de l'examen des données.

Onglet Activités

L'onglet **Activités** offre une vue d'ensemble des activités des 90 derniers jours.

Pour filtrer les activités dans le tableau de bord

1. Dans le champ **Nom du terminal**, spécifiez l'ordinateur sur lequel l'activité est exécutée.
2. Dans la liste déroulante **Statut**, sélectionnez le statut. Par exemple, « a réussi », « a échoué », « en cours », « annulée ».
3. Dans la liste déroulante **Actions à distance**, sélectionnez l'action. Par exemple, application de plan, suppression de sauvegardes, installation de mises à jour logicielles.
4. Dans le champ **Plus récent**, définissez la période d'activités. Par exemple, les activités les plus récentes, les activités des dernières 24 heures ou les activités pendant une période spécifique au cours des 90 derniers jours.
5. Si vous accédez à l'onglet **Activités** en tant qu'administrateur partenaire, vous pouvez filtrer les activités pour un client spécifique que vous gérez.

Pour personnaliser la vue de l'onglet **Activités**, cliquez sur l'icône en forme d'engrenage, puis sélectionnez les colonnes que vous souhaitez afficher. Pour consulter la progression des activités en temps réel, sélectionnez la case **Actualiser automatiquement**.

Pour annuler une activité en cours d'exécution, cliquez sur son nom, puis, dans l'écran **Détails**, cliquez sur **Annuler**.

Vous pouvez effectuer une recherche parmi les activités répertoriées selon les critères suivants :

- Nom du terminal
  Il s'agit de l'ordinateur sur lequel l'activité est exécutée.
- Démarrée par
  Il s'agit du compte qui a démarré l'activité.

Les activités Bureau à distance peuvent être filtrées à l'aide des propriétés suivantes :

- Création du plan
- Application du plan
- Révocation du plan
- Suppression du plan
- Connexion à distance
  - Connexion Bureau à distance dans le cloud via RDP
  - Connexion Bureau à distance dans le cloud via NEAR
  - Connexion Bureau à distance dans le cloud via le partage d'écran Apple
  - Connexion Bureau à distance via le client Web
  - Connexion Bureau à distance via Assistance rapide
  - Connexion Bureau à distance directe via RDP
  - Connexion Bureau à distance directe via le partage d'écran Apple
  - Transfert de fichiers
  - Transfert de fichiers via Assistance rapide
- Action à distance
  - Arrêt d'une ressource
  - Redémarrage d'une ressource
  - Déconnexion d'un utilisateur distant sur la ressource
  - Vidage de la corbeille d'un utilisateur sur la ressource
  - Mise en veille d'une ressource

Cyber Protect Monitor

Cyber Protect Monitor affiche des informations sur l'état de protection de l'ordinateur sur lequel l'agent pour Windows ou pour Mac est installé, et permet aux utilisateurs de configurer le chiffrement de la sauvegarde et les paramètres du serveur proxy.

Lorsque l'agent pour File Sync & Share est installé sur l'ordinateur, Cyber Protect Monitor permet d'accéder au service File Sync & Share. La fonctionnalité File Sync & Share est accessible après une phase d'intégration obligatoire au cours de laquelle les utilisateurs se connectent à leur propre compte File Sync & Share et sélectionnent un dossier de synchronisation personnel. Pour plus d'informations sur l'agent pour File Sync & Share, voir le guide de l'utilisateurCloud Cyber Files .

Important
Cyber Protect Monitor est accessible aux utilisateurs qui ne disposent peut-être pas de droits d'administration pour Cyber Protection ou le service File Sync & Share.

Le tableau ci-dessous résume les opérations disponibles pour les utilisateurs ne disposant pas de droits d'administration.

Agents installés	Les utilisateurs peuvent	Les utilisateurs ne peuvent pas
Agent pour Windows ou agent pour Mac	• Appliquer le plan de protection par défaut à leurs ordinateurs • Vérifier l'état de protection de leur ordinateur • Recevoir des notifications de protection active • Interrompre temporairement la sauvegarde de leur ordinateur • Configurer les paramètres du serveur proxy • Modifier les paramètres de chiffrement de la sauvegarde **Avertissement !** La modification des paramètres de chiffrement dans Cyber Protect Monitor écrase les paramètres du plan de protection et affecte toutes les sauvegardes de l'ordinateur. Cette opération peut entraîner l'échec de certains plans de protection. Pour plus d'informations, voir "Chiffrement" (p. 462). Il est impossible de restaurer les sauvegardes chiffrées si vous perdez ou oubliez le mot de passe.	• Appliquer des plans de protection personnalisés • Gérer les plans de protection déjà appliqués
Agent pour Windows et agent pour Sync and Share Agent pour Mac et agent pour Sync and Share	• Synchroniser le contenu de leur dossier de synchronisation local et de leur compte File Sync & Share • Interrompre les opérations de synchronisation • Modifier le dossier de synchronisation • Vérifier les types de fichiers qui ne peuvent pas être synchronisés	• Modifier les types de fichiers qui ne peuvent pas être synchronisés

Configuration des paramètres de serveur proxy dans Cyber Protect Monitor

Vous pouvez configurer les paramètres de serveur proxy dans Cyber Protect Monitor. La configuration aura une incidence sur tous les agents installés sur l'ordinateur.

Pour configurer les paramètres du serveur proxy

1. Ouvrez Cyber Protect Monitor, puis cliquez sur l'icône en forme d'engrenage dans le coin supérieur droit.
2. Cliquez sur **Paramètres**, puis cliquez sur **Proxy**.
3. Activez le commutateur **Utiliser un serveur proxy**, puis saisissez l'adresse et le port du serveur proxy.
4. [Si l'accès au serveur proxy est protégé par un mot de passe] Activez le commutateur **Mot de passe requis**, puis saisissez le nom d'utilisateur et le mot de passe nécessaires pour accéder au serveur proxy.
5. Cliquez sur **Enregistrer**.
   Les paramètres du serveur proxy sont enregistrés dans le fichier `http-proxy.yaml`.

Rapports

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Un rapport au sujet des opérations peut inclure n'importe quel ensemble de widgets du tableau de bord. Tous les widgets présentent le résumé pour l'ensemble de l'entreprise.

En fonction du type de widget, le rapport inclut les données pour une période ou pour le moment de la navigation ou de la génération de rapport. Consultez "Données rapportées en fonction du type de widget" (p. 329).

Tous les widgets historiques présentent les données pour le même intervalle de temps. Vous pouvez modifier cela dans les paramètres de rapport.

Vous pouvez utiliser des rapports par défaut ou créer un rapport personnalisé.

Vous pouvez télécharger un rapport ou l'envoyer par e-mail au format Excel (XLSX) ou PDF.

L'ensemble de rapports par défaut dépend de l'édition du service Cyber Protection que vous possédez. Les rapports par défaut sont répertoriés ci-dessous :

Nom du rapport	Description
Score #CyberFit par machine	Affiche le score #CyberFit basé sur l'évaluation des indicateurs et des configurations de sécurité pour chaque machine, ainsi que des recommandations d'amélioration.
Alertes	Affiche les alertes survenues pendant une période donnée.
Détails de l'analyse de la sauvegarde	Affiche des informations détaillées au sujet des menaces détectées dans les sauvegardes.
Activités quotidiennes	Affiche des informations résumées au sujet des activités réalisées lors d'une période donnée.
Carte de la	Affiche des informations détaillées concernant le nombre, la taille, l'emplacement et

protection des données	l'état de protection de tous les fichiers importants présents sur des machines.
Menaces détectées	Affiche les détails des machines affectées en les classant par nombre de menaces bloquées, ainsi que le nombre de machines saines et vulnérables.
Machines découvertes	Affiche toutes les machines trouvées dans le réseau de l'organisation.
Prévision de l'état de santé du disque	Affiche des prévisions concernant le moment où votre disque dur/SSD tombera en panne, ainsi que l'état actuel des disques.
Vulnérabilités existantes	Affiche les vulnérabilités existantes pour le système d'exploitation et les applications dans votre organisation. Le rapport affiche également les détails des machines affectées dans votre réseau pour chaque produit répertorié.
Inventaire du logiciel	Affiche des informations concernant le logiciel installé sur les terminaux de votre entreprise.
Inventaire matériel	Affiche des informations concernant le matériel disponible sur les terminaux de votre entreprise.
Résumé de la gestion des correctifs	Affiche le nombre de correctifs manquants, installés et applicables. Vous pouvez explorer les rapports pour obtenir des informations sur les correctifs manquants/installés, ainsi que sur tous les systèmes
Résumé	Affiche des informations résumées au sujet des terminaux protégés pendant une période donnée.
Activités hebdomadaires	Affiche des informations résumées au sujet des activités réalisées lors d'une période donnée.
Sessions distantes	Affiche les informations concernant les sessions Bureau à distance et transfert de fichiers.

Actions relatives aux rapports

Pour afficher un rapport, cliquez sur son nom.

Pour ajouter un nouveau rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Au bas de la liste des rapports disponibles, cliquez sur **Ajouter un rapport**.
3. [Pour ajouter un rapport prédéfini] Cliquez sur le nom du rapport prédéfini.
4. [Pour ajouter un rapport personnalisé] Cliquez sur **Personnalisé**, puis ajoutez des widgets au rapport.
5. [Facultatif] Glissez-déplacez les widgets pour les réorganiser.

Pour modifier un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport que vous souhaitez modifier.
   Vous pouvez effectuer les opérations suivantes :
   - Renommer le rapport.
   - Modifier l'intervalle de temps de tous les widgets du rapport.
   - Spécifier les destinataires du rapport, ainsi que le moment où le rapport leur sera envoyé. Les formats disponibles sont PDF et XLSX.

Pour supprimer un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport que vous souhaitez supprimer.
3. Cliquez sur l'icône représentant des points de suspension (...), puis cliquez sur **Supprimer**.
4. Confirmez votre choix en cliquant sur **Supprimer**.

Pour planifier un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport que vous souhaitez planifier, puis cliquez sur **Paramètres**.
3. Activez le commutateur **Planifié**.
   - Spécifiez l'adresse e-mail des destinataires.
   - Sélectionnez le format du rapport.

     Remarque
     Vous pouvez exporter jusqu'à 1 000 éléments dans un fichier PDF et jusqu'à 10 000 éléments dans un fichier XLSX. Les horodatages des fichiers PDF et XLSX utilisent l'heure locale de votre ordinateur.

   - Sélectionnez la langue du rapport.
   - Configurez la planification.
4. Cliquez sur **Enregistrer**.

Pour télécharger un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport, puis cliquez sur **Télécharger**.
3. Sélectionnez le format du rapport.

Pour envoyer un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport, puis cliquez sur **Envoyer**.

3. Spécifiez l'adresse e-mail des destinataires.
4. Sélectionnez le format du rapport.
5. Cliquez sur **Envoyer**.

Pour exporter la structure des rapports

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport.
3. Cliquez sur l'icône représentant des points de suspension (...), puis cliquez sur **Exporter**.

En conséquence, la structure du rapport est enregistrée sur votre ordinateur en tant que fichier JSON.

Pour vider les données du rapport

En utilisant cette option, vous pouvez exporter toutes les données d'une période personnalisée, sans la filtrer, vers un fichier CSV et envoyer ce fichier par e-mail vers un destinataire.

Remarque
Vous pouvez exporter jusqu'à 150 000 éléments dans un fichier CSV. Les horodatages dans le fichier CSV utilisent le temps universel coordonné (UTC).

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport dont vous souhaitez vider les données.
3. Cliquez sur l'icône représentant des points de suspension (...), puis cliquez sur **Vider les données**.
4. Spécifiez l'adresse e-mail des destinataires.
5. Dans la zone **Plage de temps**, spécifiez la période personnalisée pour laquelle vous souhaitez vider les données.

   Remarque
   La préparation des fichiers CSV pour de plus longues périodes prend plus de temps.

6. Cliquez sur **Envoyer**.

Données rapportées en fonction du type de widget

Les widgets du tableau de bord peuvent être classés selon deux catégories, selon le type de données qu'ils présentent :

- Les widgets qui affichent les données actuelles au moment de la navigation ou de la génération du rapport.
- Les widgets qui affichent les données historiques.

Lorsque vous configurez une plage de dates dans les paramètres de rapport afin d'effectuer un vidage mémoire des données d'une certaine période, la plage de dates sélectionnée s'applique uniquement aux widgets qui affichent des données historiques. Elle n'est pas applicable aux widgets qui affichent les données actuelles au moment de la navigation ou de la génération du rapport.

Le tableau suivant énumère les widgets et leurs plages de données.

Nom du widget	Données affichées dans le widget et les rapports
Score #CyberFit par machine	Actuelles
5 dernières alertes	Actuelles
Détails des alertes actives	Actuelles
Résumé des alertes actives	Actuelles
Activités	Historiques
Liste des activités	Historiques
Historique des alertes	Historiques
Statistiques des tactiques d'attaque	Historiques
Détails de l'analyse de la sauvegarde (menaces)	Historiques
État de la sauvegarde	Historiques, dans les colonnes **Total des exécutions** et **Nombre d'exécutions réussies** Actuelles, dans toutes les autres colonnes
URL bloquées	Actuelles
Applications dans le Cloud	Actuelles
Cyberprotection	Actuelles
Carte de la protection des données	Historiques
Terminaux	Actuelles
Machines découvertes	Actuelles
Vue d'ensemble de l'état de santé du disque	Actuelles
Intégrité de disque par terminaux physiques	Actuelles
Vulnérabilités existantes	Historiques
Modifications apportées au matériel	Historiques

Détails du matériel	Actuelles
Inventaire matériel	Actuelles
Résumé de l'historique des alertes	Historiques
Historique de gravité de l'incident	Historiques
Résumé des emplacements	Actuelles
Mises à jour manquantes, par catégorie	Actuelles
Non protégé	Actuelles
Historique d'installation des correctifs	Historiques
Statut d'installation des correctifs	Historiques
Résumé d'installation des correctifs	Historiques
État de protection	Actuelles
Affectés récemment	Historiques
Sessions distantes	Historiques
Résolution des incidents de sécurité	Historiques
Temps moyen de réparation des incidents de sécurité	Historiques
Inventaire du logiciel	Actuelles
Aperçu du logiciel	Historiques
Statut de la menace	Actuelles
Machines vulnérables	Actuelles
Statut réseau des ressources	Actuelles

Gestion des ressources dans la console de Cyber Protect

Cette section décrit le mode de gestion de vos ressources dans la console de Cyber Protect.

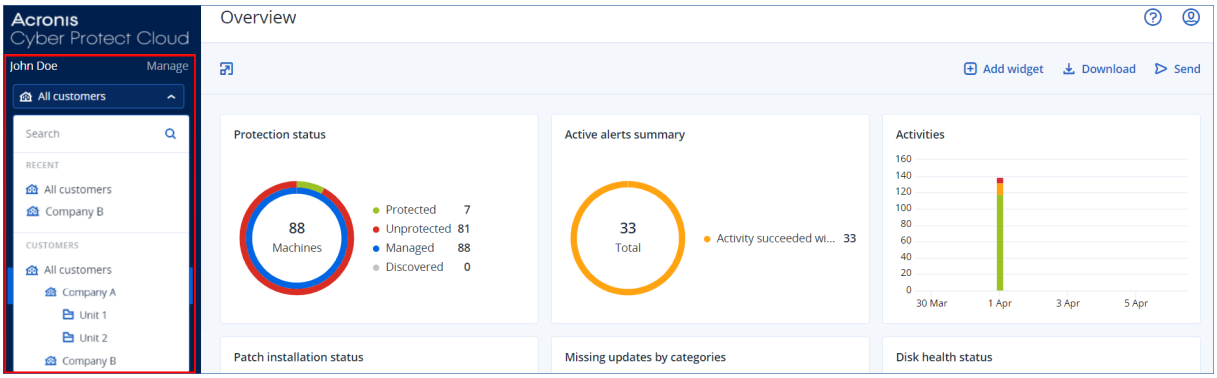
La console Cyber Protect

Dans la console Cyber Protect, vous pouvez gérer les ressources et les plans, modifier les paramètres de protection, configurer des rapports ou examiner votre stockage des sauvegardes.

La console Cyber Protect vous donne accès à des services ou fonctionnalités supplémentaires, comme File Sync & Share ou la protection contre les virus et les malwares, la gestion des correctifs, le contrôle des terminaux et l'évaluation des vulnérabilités. Le type et le nombre de ces services varient selon votre licence Cyber Protection.

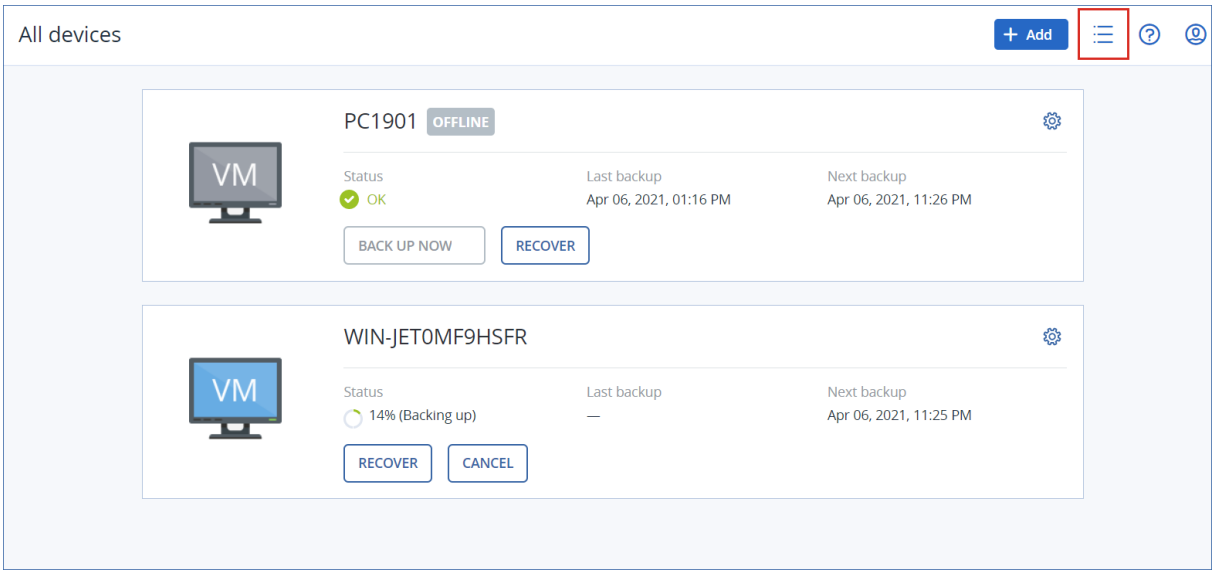
Pour afficher le tableau de bord qui vous fournit les informations les plus importantes concernant votre protection, accédez à **Surveillance** > **Vue d'ensemble**.

Selon vos autorisations d'accès, vous pouvez gérer la protection d'un ou plusieurs tenants clients ou unités dans un tenant. Pour changer le niveau de hiérarchie, utilisez la liste déroulante de votre menu de navigation. Seuls les niveaux auxquels vous avez accès s'affichent. Pour accéder au Portail de gestion, cliquez sur **Gérer**.

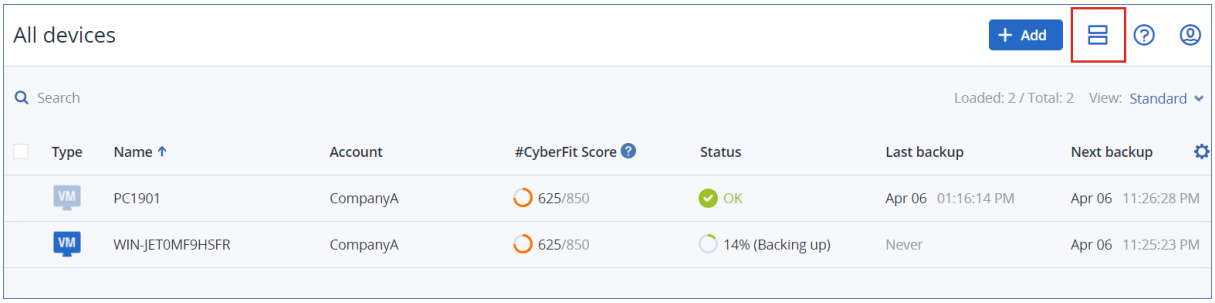


La section **Terminaux** est disponible en mode d'affichage simple et en mode d'affichage tableau. Pour passer de l'un à l'autre, cliquez sur l'icône correspondante dans l'angle supérieur droit.

Le mode d'affichage simple affiche uniquement quelques ressources.



Le mode d'affichage tableau est activé automatiquement lorsque le nombre de ressources devient plus important.



Les deux modes d'affichage donnent accès aux mêmes fonctionnalités et aux mêmes opérations. Ce document explique comment accéder aux différentes opérations depuis le mode d'affichage tableau.

Lorsqu'une ressource passe en ligne ou hors ligne, un certain temps est nécessaire avant que son état soit modifié dans la console Cyber Protect. L'état de la ressource est vérifié toutes les minutes. Si l'agent installé sur l'ordinateur correspondant n'est pas en train de transférer des données, et que cinq vérifications consécutives ne donnent aucun résultat, la ressource apparaît hors ligne. La ressource apparaît à nouveau en ligne lorsqu'elle répond à une vérification d'état ou commence à transférer des données.

Nouveautés de la console Cyber Protect

Lorsque les nouvelles fonctionnalités de Cyber Protect Cloud sont disponibles, vous voyez une fenêtre pop-up indiquant une brève description de ces fonctionnalités lors de la connexion à la console Cyber Protect.

Vous pouvez également consulter la description des nouvelles fonctionnalités en cliquant sur le lien **Nouveautés** en bas à gauche de la fenêtre principale de la console Cyber Protect.

En l'absence de nouvelles fonctionnalités, le lien **Nouveautés** n'est pas affiché.

Utilisation de la console Cyber Protect en tant qu'administrateur partenaire

En tant qu'administrateur partenaire, vous pouvez utiliser la console Cyber Protect au niveau du tenant partenaire (**Tous les clients**) ou au niveau du tenant client.

Niveau tenant partenaire (**Tous les clients**)

Au niveau du tenant partenaire (**Tous les clients**), vous pouvez effectuer les actions suivantes :

- Gérer les plans de script pour les ressources de tous vos clients gérés.
  Vous pouvez appliquer le même plan de script aux ressources de différents clients et créer des groupes de terminaux avec des ressources de différents clients. Pour savoir comment créer un groupe de terminaux statique ou dynamique au niveau du partenaire, voir "Création d'un groupe statique de terminaux au niveau du partenaire" (p. 337) et "Création d'un groupe dynamique de terminaux au niveau du partenaire" (p. 337). Pour plus d'informations sur les scripts et les plans de script, voir "Création de cyber-scripts" (p. 244).
- Créez des plans de surveillance pour les ressources de tous vos tenants clients gérés.
- Créez des plans de gestion à distance pour les ressources de tous vos tenants clients gérés.
- Visualisez et gérez les incidents EDR (liés à la détection et à la réponse des points d'accès) pour tous les clients dans une même interface de gestion des incidents, plutôt que d'accéder aux différents écrans d'incidents de chaque client.
- Effectuez la découverte automatique des ordinateurs de tous vos tenants clients gérés.

Niveau tenant client

À ce niveau, vous avez les mêmes droits que l'administrateur d'entreprise pour le compte duquel vous agissez.

Sélection d'un niveau de tenant

Vous pouvez sélectionner le niveau du tenant sur lequel travailler dans la console Cyber Protect.

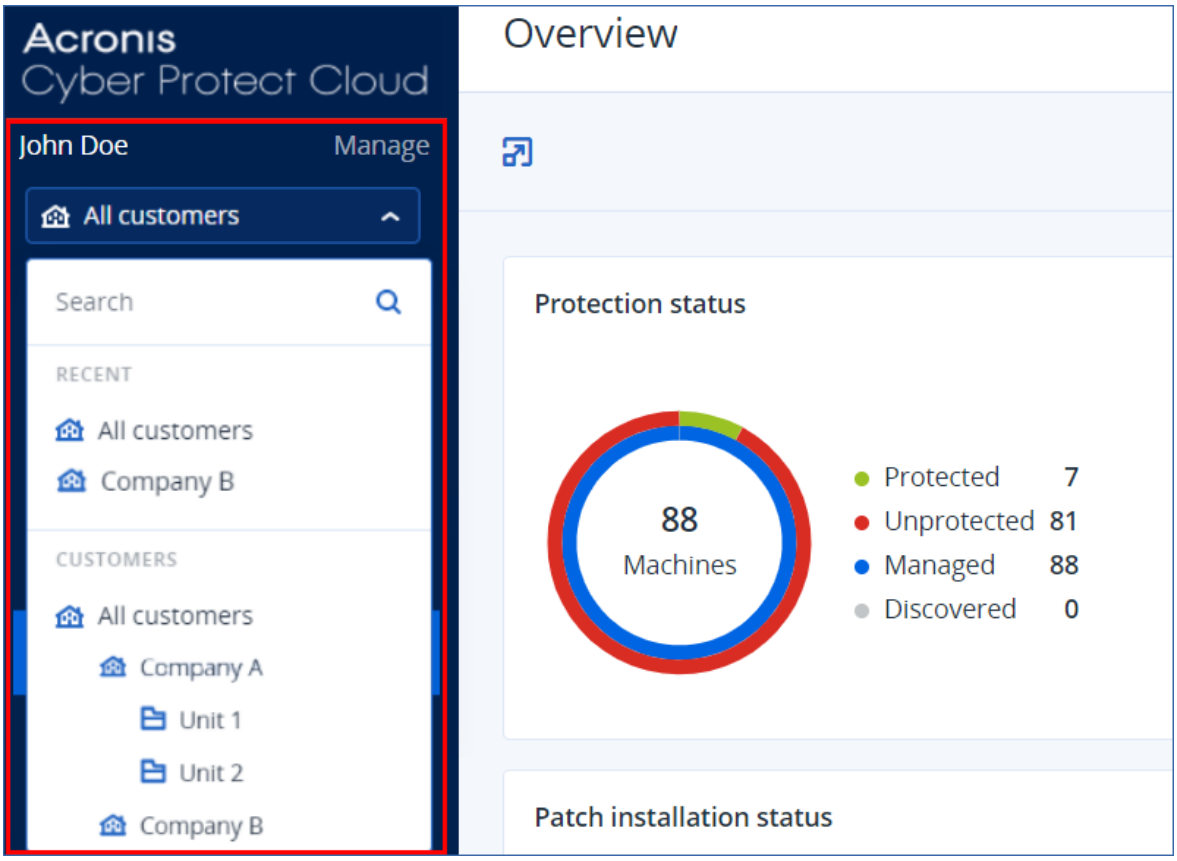
Prérequis

- Vous avez des droits d'accès à la console Cyber Protect et au portail de gestion.
- Vous pouvez gérer plusieurs tenants ou unités.

Pour sélectionner un niveau de tenant dans la console Cyber Protect

1. Dans le menu de navigation à gauche, cliquez sur la flèche à côté du nom du tenant client.
2. Sélectionnez l'une des options suivantes :
   - Pour travailler au niveau partenaire, sélectionnez **Tous les clients**.

- Pour travailler au niveau client ou unité, sélectionnez le nom de ce client ou de cette unité.



Niveau du tenant partenaire dans la console Cyber Protect

Lorsque vous utilisez la console Cyber Protect au niveau du tenant partenaire (**Tous les clients**), une vue personnalisée est disponible.

Les onglets **Alertes** et **Activités** fournissent des filtres supplémentaires liés aux partenaires, alors que les onglets **Terminaux** et **Gestion** offrent uniquement l'accès aux fonctionnalités ou objets accessibles aux administrateurs partenaires.

Onglet Alertes

Dans cet onglet, vous pouvez voir les alertes de tous les clients que vous gérez. Vous pouvez également les rechercher et les filtrer selon les critères suivants :

- Terminal
- Client
- Plan

Vous pouvez sélectionner plusieurs éléments pour chacun de ces critères.

Onglet Activités

Dans cet onglet, vous pouvez voir les activités de tous les tenants que vous gérez ou les activités dans un tenant client spécifique.

Vous pouvez filtrer les activités par client, état, heure et type.

Les types d'activités suivants sont automatiquement présélectionnés à ce niveau :

- Application du plan
- Création du plan de protection
- Plan de protection
- Révocation du plan
- Création de script

Onglet Terminaux

Dans l'onglet **Machines avec des agents**, vous pouvez afficher toutes les ressources de vos tenants client gérés, et vous pouvez sélectionner des ressources d'un ou plusieurs tenants. Vous pouvez également créer des groupes de terminaux contenant des ressources de différents tenants.

Important
Lorsque vous travaillez au niveau partenaire (**Tous les clients**), vous ne pouvez effectuer qu'un nombre limité d'opérations sur les terminaux. Par exemple, vous ne pouvez effectuer aucune des opérations suivantes :

- Voir et gérer les plans de protection existants sur les terminaux des clients.
- Créer de nouveaux plans de protection.
- Restaurer les sauvegardes.
- Utiliser Disaster Recovery.
- Accédez aux fonctions de Cyber Protection Desktop.

Pour effectuer l'une de ces opérations, vous devez travailler au niveau du client.

Onglet Gestion de logiciel

Si l'analyse de l'inventaire des logiciels est activée pour les ressources des clients, vous pouvez voir les résultats de l'analyse des logiciels.

Visualisation des ressources de clients spécifiques

En tant qu'administrateur partenaire, vous pouvez visualiser les ressources appartenant aux tenants clients que vous gérez.

Pour visualiser les ressources d'un client spécifique

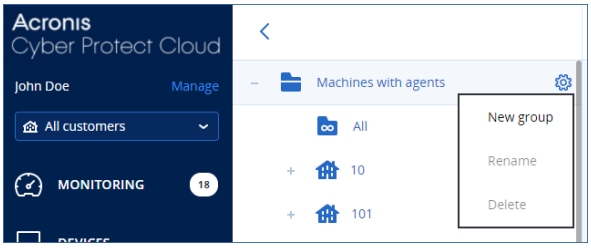
1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Dans l'arborescence, cliquez sur **Machines avec des agents** pour développer la liste.
3. Cliquez sur le nom du client dont vous souhaitez consulter et gérer les ressources.

Création d'un groupe statique de terminaux au niveau du partenaire

Vous pouvez créer des groupes de terminaux statiques au niveau du partenaire (**Tous les terminaux**).

Créer un groupe de terminaux statique au niveau partenaire

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Cliquez sur l'icône en forme d'engrenage située à côté de **Machines avec des agents**, puis cliquez sur **Nouveau groupe**.



3. Spécifiez le nom du groupe.
4. [Facultatif] Ajoutez une description.
5. Cliquez sur **OK**.

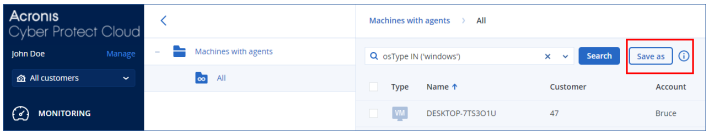
Création d'un groupe dynamique de terminaux au niveau du partenaire

Vous pouvez créer des groupes de terminaux dynamiques au niveau du partenaire (**Tous les terminaux**).

Créer un groupe de terminaux dynamique au niveau partenaire

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Dans l'arborescence, cliquez sur **Machines avec des agents** pour développer la liste.
3. Cliquez sur **Tous**.
4. Dans le champ de recherche, spécifiez les critères selon lesquels vous souhaitez créer un groupe de terminaux dynamique, puis cliquez sur **Rechercher**.

   Pour en savoir plus sur les critères de recherche disponibles, voir "Rechercher des attributs pour les ressources autres que cloud à cloud" (p. 361) et "Rechercher des attributs pour les ressources de cloud à cloud" (p. 360).
5. Cliquez sur **Enregistrer sous**, puis spécifiez le nom du groupe.



6. [Facultatif] Ajoutez une description.
7. Cliquez sur **OK**.

Découverte automatique des ordinateurs au niveau du tenant partenaire

Vous pouvez effectuer une découverte automatique des ordinateurs au niveau du tenant partenaire (**Tous les clients**).

Prérequis

Au moins un ordinateur avec agent de protection est installé dans le réseau local ou dans le domaine Active Directory de votre client.

Important
Seuls les agents installés sur des ordinateurs Windows peuvent être des agents de découverte. S'il n'existe aucun agent de découverte dans l'environnement de vos clients, vous ne pourrez pas utiliser l'option **Terminaux multiples** dans le panneau **Ajouter des terminaux**.

La découverte automatique n'est pas prise en charge pour l'ajout de contrôleurs de domaine en raison des autorisations supplémentaires requises pour le fonctionnement du service de l'agent.

L'installation à distance des agents n'est prise en charge uniquement pour les ordinateurs exécutant Windows (Windows XP n'est pas pris en charge). Pour l'installation à distance sur un ordinateur exécutant Windows Server 2012 R2, la mise à jour Windows KB2999226 doit être installée.

Pour effectuer la découverte automatique des ordinateurs au niveau du tenant partenaire

1. Dans la console Cyber Protect, sélectionnez **Tous les clients**.
2. Accédez à **Terminaux** > **Tous les terminaux**.
3. Cliquez sur **Ajouter**.
4. Dans **Terminaux multiples**, cliquez sur **Windows uniquement**. L'assistant de découverte s'ouvre.
5. Sélectionnez un tenant client, puis l'agent de découverte qui effectuera la recherche des ordinateurs.
6. Sélectionnez la méthode de découverte :
   - **Rechercher dans Active Directory**. Assurez-vous que la machine sur laquelle l'agent de découverte est installé est membre du domaine Active Directory.
   - **Analyser le réseau local**. Si l'agent de découverte sélectionné ne trouve aucune machine, sélectionnez un autre agent de découverte.
   - **Spécifier manuellement ou importer à partir d'un fichier**. Définissez manuellement les machines à ajouter, ou importez-les à partir d'un fichier texte.
7. [Si la méthode de découverte sur Active Directory est sélectionnée] Sélectionnez comment rechercher des machines :

- **Dans une liste d'unités organisationnelles**. Sélectionnez le groupe de machines à ajouter.
- **Par demande de dialecte LDAP**. Servez-vous d'une demande de Dialecte LDAP pour sélectionner les ordinateurs. La **Base de recherche** définit l'endroit de la recherche et le **Filtre** permet de spécifier les critères de sélection des ordinateurs.

8. En fonction de la méthode de découverte que vous avez sélectionnée, effectuez l'une des actions suivantes :

Méthode de découverte	Action
Recherche dans Active Directory	Dans la liste des ordinateurs découverts, sélectionnez les ordinateurs que vous souhaitez ajouter.
Analyse du réseau local	Dans la liste des ordinateurs découverts, sélectionnez les ordinateurs que vous souhaitez ajouter.

Spécifier manuellement ou importer à partir d'un fichier	Indiquez les adresses IP ou les noms d'hôte des ordinateurs, ou importez la liste des ordinateurs à partir d'un fichier texte. Le fichier doit contenir les adresses IP/noms d'hôtes, un élément par ligne. Voici un exemple de fichier :
	`156.85.34.10`
	`156.85.53.32`
	`156.85.53.12`
	`EN-L00000100`
	`EN-L00000101`
	Après l'ajout manuel ou l'importation de machines à partir d'un fichier, l'agent essaie d'effectuer un ping des machines ajoutées et de définir leur disponibilité.

9. Sélectionnez les actions à effectuer après la découverte :

Option	Description
Installer des agents et enregistrer des ordinateurs	Vous pouvez sélectionner les composants à installer sur les ordinateurs en cliquant sur **Sélectionner les composants**. Pour plus de détails, voir "Sélection des composants à installer" (p. 138).
Compte de connexion pour le service de l'agent	Ce paramètre est disponible dans l'écran **Sélectionner des composants**. Ce paramètre définit le compte sous lequel les services seront exécutés. Vous pouvez sélectionner l'une des options suivantes : • **Utiliser des comptes d'utilisateur du service** (par défaut pour l'agent de service) Les comptes d'utilisateur du service sont des comptes système Windows utilisés pour exécuter des services. Ce paramètre présente l'avantage suivant : les politiques de sécurité du domaine n'affectent pas les droits d'utilisateur de ces comptes. Par défaut, l'agent est exécuté sous le compte **Système Local**. • **Créer un nouveau compte** Le nom de compte pour l'agent sera Agent User.

Option	Description
	• **Utiliser le compte suivant** Si vous installez l'agent sur un contrôleur de domaine, le système vous invite à spécifier des comptes existants (ou le même compte) pour l'agent. Pour des raisons de sécurité, le système ne crée pas automatiquement de nouveaux comptes sur un contrôleur de domaine. Si vous avez choisi l'option **Créer un nouveau compte** ou **Utiliser le compte suivant**, assurez-vous que les politiques de sécurité du domaine n'affectent pas les droits des comptes associés. Si un compte est privé des droits d'utilisateur attribués lors de l'installation, le composant peut fonctionner de manière incorrecte ou ne pas fonctionner du tout.
Enregistrer les ordinateurs avec les agents installés	Utilisez cette option si l'agent est déjà installé sur les ordinateurs et qu'il vous suffit de les enregistrer sur Cyber Protection. Si aucun agent n'est trouvé sur les ordinateurs, ces derniers sont ajoutés en tant qu'ordinateurs **Non gérés**.
Ajouter en tant qu'ordinateurs non gérés	Si vous sélectionnez cette option, l'agent ne sera pas installé sur les ordinateurs. Vous pourrez les visualiser dans la console, et installer ou enregistrer l'agent ultérieurement.
Redémarrer l'ordinateur, si nécessaire	Cette option apparaît lorsque l'option **Installer les agents et enregistrer les ordinateurs** est sélectionnée. Si vous sélectionnez cette option, l'ordinateur est redémarré autant de fois que nécessaire pour terminer l'installation. Le redémarrage de la machine peut être nécessaire dans l'un des cas suivants : • L'installation des prérequis est terminée et un redémarrage est nécessaire pour que l'installation puisse se poursuivre. • L'installation est terminée, mais un redémarrage est nécessaire, car certains fichiers sont bloqués pendant l'installation. • L'installation est terminée, mais un redémarrage est nécessaire pour les autres logiciels précédemment installés.
Ne pas redémarrer si l'utilisateur s'est connecté	Cette option apparaît lorsque l'option **Redémarrer l'ordinateur si nécessaire** est sélectionné. Si vous sélectionnez cette option, l'ordinateur ne sera pas redémarré automatiquement si l'utilisateur est connecté au système. Par exemple, si un utilisateur travaille pendant que l'installation nécessite un redémarrage, le système n'est pas redémarré. Si les prérequis ont été installés, mais que l'ordinateur n'a pas été redémarré parce qu'un utilisateur était connecté, vous devez redémarrer l'ordinateur et recommencer l'installation pour la terminer. Si l'agent a été installé, mais que l'ordinateur n'a pas été redémarré, vous devez redémarrer l'ordinateur.
Utilisateur pour	[Si votre organisation comporte des unités] Sélectionnez le compte utilisateur de

Option	Description
lequel enregistrer les ordinateurs	l'unité ou des unités subordonnées sous lesquelles vous voulez enregistrer les ordinateurs. [Lors de la découverte automatique au niveau tenant partenaire] Dans la liste des tenants clients que vous gérez, développez l'arborescence, puis sélectionnez le compte utilisateur sous lequel vous souhaitez enregistrer les ordinateurs. [Lors de la découverte automatique en tant qu'administrateur du client] Si vous avez sélectionné **Installer les agents et enregistrer les ordinateurs** ou **Enregistrer les ordinateurs avec les agents installés**, vous avez également la possibilité d'appliquer le plan de protection aux ordinateurs. Si vous disposez de plusieurs plans de protection, vous pouvez sélectionner celui que vous souhaitez utiliser.

10. Fournissez les identifiants de l'utilisateur qui dispose de droits d'administrateur pour toutes les machines.

    Important
    L'installation à distance des agents sans aucune préparation ne fonctionne que si vous spécifiez les identifiants du compte administrateur intégré (le premier compte créé lors de l'installation du système d'exploitation). Si vous souhaitez définir des identifiants d'administrateur personnalisés, vous devez effectuer d'autres opérations préparatoires, comme décrit dans "Prérequis" (p. 338).

11. Le système vérifie la connectivité à toutes les machines. En cas d'échec de connexion à certaines des machines, vous pouvez modifier leurs identifiants.

Une fois la découverte des ordinateurs lancée, vous pouvez voir la tâche correspondante dans **Surveillance** > **Activités** > **Découverte des ordinateurs**.

Prise en charge de la mutualisation

Le service Cyber Protection prend en charge la mutualisation, ce qui implique une administration aux niveaux suivants :

- [Pour les fournisseurs de service] Niveau tenant partenaire (**Tous les clients**)
  Ce niveau est uniquement disponible pour les administrateurs partenaires qui gèrent des tenants clients.
- Niveau tenant client
  Ce niveau est géré par les administrateurs d'entreprise.
  Les administrateurs partenaires peuvent également travailler dans ce niveau dans les tenants clients qu'ils gèrent. À ce niveau, les administrateurs partenaires ont les mêmes droits que les administrateurs client pour le compte desquels ils agissent.
- Niveau unité
  Ce niveau est géré par les administrateurs d'unité et par les administrateurs d'entreprise à partir du tenant client parent.

Les administrateurs partenaires qui gèrent le tenant client parent peuvent également accéder au niveau unité. À ce niveau, ils ont les mêmes droits que les administrateurs client pour le compte desquels ils agissent.

Les administrateurs peuvent gérer les objets dans leur propre tenant et dans ses tenants enfants. Ils ne peuvent pas voir les objets disponibles dans un niveau d'administration plus élevé (le cas échéant), ni y accéder.

Par exemple, les administrateurs d'entreprise peuvent gérer les plans de protection à la fois au niveau tenant client et au niveau unité. Les administrateurs d'unité peuvent gérer leurs propres plans de protection au niveau unité. Ils ne peuvent pas gérer de plans de protection au niveau tenant client et ne peuvent pas gérer les plans de protection créés par l'administrateur client au niveau unité.

Les administrateurs partenaires peuvent également créer et appliquer des plans de création de scripts dans les tenants clients qu'ils gèrent. Les administrateurs d'entreprise dans ces tenants n'ont qu'un accès en lecture seule aux plans de création de scripts appliqués à leurs ressources par un administrateur partenaire. Toutefois, les administrateurs client peuvent créer et appliquer leurs propres plans de création de scripts ou de protection.

Ressources

Une ressource correspond à tout type de ressource protégée ; il peut s'agir, par exemple, d'une machine physique, d'une machine virtuelle, d'une boîte aux lettres ou d'une instance de base de données. Dans la console Cyber Protect, la ressource est affichée comme étant un objet auquel vous pouvez appliquer un plan (de protection, de sauvegarde ou de création de script).

Certaines ressources nécessitent l'installation d'un agent de protection ou le déploiement d'une appliance virtuelle. Vous pouvez installer les agents à l'aide de l'interface graphique ou de l'interface de ligne de commande (installation sans assistance). Vous pouvez utiliser l'installation sans assistance pour automatiser la procédure d'installation. Pour plus d'informations sur l'installation des agents de protection, voir "Installation et déploiement d'agents Cyber Protection" (p. 61).

Une appliance virtuelle est une machine virtuelle prête à l'emploi qui contient un agent de protection. Elle vous permet de sauvegarder d'autres machines virtuelles du même environnement sans y installer d'agent de protection (sauvegarde sans agent). Les appliances virtuelles sont disponibles dans des formats propres à l'hyperviseur, tels que .ovf, .ova ou .qcow. Pour plus d'informations sur les plates-formes de virtualisation qui prennent en charge la sauvegarde sans agent, voir "Plates-formes de virtualisation prises en charge" (p. 32).

Important
Les agents doivent être en ligne au moins une fois tous les 30 jours. Sinon, leurs plans sont révoqués et les ressources ne sont plus protégées.

Le tableau ci-dessous récapitule les types de ressources et leurs agents respectifs.

Type de ressource	Agent	Exemples (liste non exhaustive)
Machines physiques	Un agent de protection est installé sur chaque machine protégée.	Station de travail Ordinateur portable Serveur
Machines virtuelles	Selon la plate-forme de virtualisation, les méthodes de sauvegarde suivantes peuvent être disponibles : • Sauvegarde avec agent : un agent de protection est installé sur chaque machine protégée. • Sauvegarde sans agent : un agent de protection est installé uniquement sur l'hôte de l'hyperviseur, sur une machine virtuelle dédiée, ou est déployé sous forme d'appliance virtuelle. Cet agent sauvegarde toutes les machines virtuelles de l'environnement.	Machine virtuelle VMware Machine virtuelle Hyper-V Machine virtuelle basée sur un noyau (KVM) et gérée par oVirt
Ressources Microsoft 365 Business Ressources Google Workspace	Ces ressources sont sauvegardées par un agent cloud ne nécessitant aucune installation. Pour utiliser l'agent cloud, vous devez ajouter votre organisation Microsoft 365 ou Google Workspace à la console Cyber Protect. En outre, un agent local pour Office 365 est disponible. Il nécessite une installation et ne peut être utilisé que pour sauvegarder les boîtes aux lettres Exchange Online. Pour plus d'informations sur les différences entre l'agent local et l'agent dans le cloud, voir "Protection des données Microsoft 365" (p. 628). .	Boîte aux lettres Microsoft 365 Microsoft 365 OneDrive Microsoft Teams Site SharePoint Boîte aux lettres Google Google Drive
Applications	Les données d'applications spécifiques sont sauvegardées par des agents dédiés tels que l'agent pour SQL, l'agent pour Exchange, l'agent pour MySQL/MariaDB ou l'agent pour Active Directory.	Bases de données SQL Server Bases de données MySQL/MariaDB Base de données Oracle Active Directory
Terminaux mobiles	Une application mobile est installée sur les terminaux protégés.	Terminaux Android ou iOS
Sites Web	Les sites Web sont sauvegardés par un agent cloud ne	Sites Web

Type de ressource	Agent	Exemples (liste non exhaustive)
	nécessitant aucune installation.	accessibles via les protocoles SFTP ou SSH

Pour plus d'informations sur l'agent nécessaire et sur son emplacement d'installation, voir "De quel agent ai-je besoin ?" (p. 64)

Ajout de ressources à la console Cyber Protect

Pour démarrer la protection de vos ressources, commencez par ajouter ces ressources à la console Cyber Protect.

Remarque
Les types de ressources que vous pouvez ajouter dépendent des quotas de service de votre compte. Si un type de ressource spécifique est manquant, il est grisé dans le panneau **Ajouter des terminaux**.

Un administrateur partenaire peut activer les quotas de service requis dans le portail de gestion. Pour plus d'informations, veuillez consulter l'article "Informations pour les administrateurs partenaires" (p. 348).

Pour ajouter une ressource

1. Connectez-vous à la console Cyber Protect.
2. Accédez à **Terminaux** > **Tous les terminaux**, puis cliquez sur **Ajouter**.
   Le panneau **Ajouter des terminaux** s'ouvre à droite.
3. Sélectionnez le canal de publication.
4. Cliquez sur le type de ressource que vous souhaitez ajouter, puis suivez les instructions pour la ressource que vous avez sélectionnée.

Le tableau suivant récapitule les types de ressources et les actions requises.

Ressources à ajouter	Action requise	Procédure à suivre
Plusieurs ordinateurs Windows	Exécutez une découverte automatique dans votre environnement. Pour exécuter la découverte automatique, vous avez besoin d'au moins un ordinateur sur lequel est installé un agent de protection dans votre réseau local ou votre domaine Active Directory. Cet agent est utilisé	"Effectuer une découverte automatique et découverte manuelle" (p. 133)

Ressources à ajouter	Action requise	Procédure à suivre
	comme agent de découverte.	
Postes de travail Windows Serveurs Windows	Installez l'agent pour Windows.	"Installation des agents de protection sous Windows" (p. 80) ou "Installation ou désinstallation sans assistance sous Windows" (p. 91)
Postes de travail macOS	Installez l'agent pour macOS.	"Installation des agents de protection sous macOS" (p. 85) ou "Installation et désinstallation sans assistance sous macOS" (p. 115)
Serveurs Linux	Installez l'agent pour Linux.	"Installation des agents de protection sous Linux" (p. 82) ou "Installation ou désinstallation sans assistance sous Linux" (p. 109)
Terminaux mobiles (iOS, Android)	Installez l'application mobile.	"Protection des terminaux mobiles" (p. 620)
Ressources de cloud à cloud		
Microsoft 365 Business	Ajoutez votre organisation Microsoft 365 à la console Cyber Protect et utilisez l'agent cloud pour protéger les boîtes aux lettres Exchange Online, les fichiers OneDrive, Microsoft Teams, ainsi que les sites SharePoint. Vous pouvez également installer l'agent local pour Office 365. Il ne fournit que la sauvegarde des boîte aux lettres Exchange Online. Pour plus d'informations sur les différences entre l'agent local et l'agent cloud, voir "Protection des données Microsoft 365" (p. 628).	"Protection des données Microsoft 365" (p. 628)

Ressources à ajouter	Action requise	Procédure à suivre
Google Workspace	Ajoutez votre organisation Google Workspace à la console Cyber Protect et utilisez l'agent cloud pour protéger les boîtes aux lettres Gmail et les fichiers Google Drive.	"Protection des données Google Workspace" (p. 674)
Machines virtuelles		
VMware ESXi	Déployez l'agent pour VMware (appliance virtuelle) dans votre environnement.	"Déploiement de l'agent pour VMware (appliance virtuelle)" (p. 141)
	Installez l'agent pour VMware (Windows).	"Installation des agents de protection sous Windows" (p. 80) ou "Installation ou désinstallation sans assistance sous Windows" (p. 91)
Virtuozzo Hybrid Infrastructure	Déployez l'agent pour Virtuozzo Hybrid Infrastructure (appliance virtuelle) dans votre environnement.	"Déploiement de l'agent pour Virtuozzo Hybrid Infrastructure (appliance virtuelle)" (p. 151)
Hyper-V	Installez l'agent pour Hyper-V.	"Installation des agents de protection sous Windows" (p. 80) ou "Installation ou désinstallation sans assistance sous Windows" (p. 91)
Virtuozzo	Installez l'agent pour Virtuozzo.	"Installation des agents de protection sous Linux" (p. 82) ou "Installation ou désinstallation sans assistance sous Linux" (p. 109)
KVM	Installez l'agent pour Windows.	"Installation des agents de protection sous Windows" (p. 80) ou "Installation ou désinstallation sans assistance sous Windows" (p. 91)

Ressources à ajouter	Action requise	Procédure à suivre
	Installez l'agent pour Linux.	"Installation des agents de protection sous Linux" (p. 82) ou "Installation ou désinstallation sans assistance sous Linux" (p. 109)
Red Hat Virtualization (oVirt)	Déployez l'agent pour oVirt (appliance virtuelle) dans votre environnement.	"Déploiement de l'agent pour oVirt (appliance virtuelle)" (p. 159)
Citrix XenServer	Installez l'agent pour Windows.	"Installation des agents de protection sous Windows" (p. 80) ou "Installation ou désinstallation sans assistance sous Windows" (p. 91)
	Installez l'agent pour Linux.	"Installation des agents de protection sous Linux" (p. 82) ou "Installation ou désinstallation sans assistance sous Linux" (p. 109)
Nutanix AHV	Installez l'agent pour Windows.	"Installation des agents de protection sous Windows" (p. 80) ou "Installation ou désinstallation sans assistance sous Windows" (p. 91)
	Installez l'agent pour Linux.	"Installation des agents de protection sous Linux" (p. 82) ou "Installation ou désinstallation sans assistance sous Linux" (p. 109)
VM Oracle	Installez l'agent pour Windows.	"Installation des agents de protection sous Windows" (p. 80) ou "Installation ou désinstallation

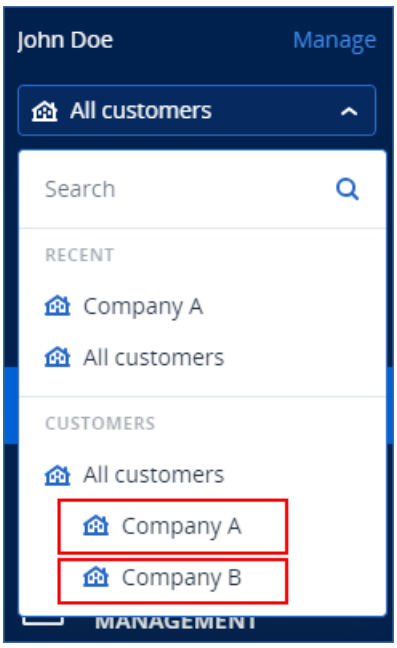
Ressources à ajouter	Action requise	Procédure à suivre
		sans assistance sous Windows" (p. 91)
	Installez l'agent pour Linux.	"Installation des agents de protection sous Linux" (p. 82) ou "Installation ou désinstallation sans assistance sous Linux" (p. 109)
HC3 de Scale Computing	Déployez l'agent pour Scale Computing HC3 (appliance virtuelle) dans votre environnement.	"Déploiement de l'agent pour Scale Computing HC3 (appliance virtuelle)" (p. 146)
Stockage en réseau		
Synology	Déployez l'agent pour Synology (appliance virtuelle) dans votre environnement.	"Déploiement de l'agent pour Synology" (p. 166)
Applications		
Microsoft SQL Server	Installez l'agent pour SQL.	"Installation des agents de protection sous Windows" (p. 80) ou "Installation ou désinstallation sans assistance sous Windows" (p. 91)
Microsoft Exchange Server	Installez l'agent pour Exchange.	
Microsoft Active Directory	Installez l'agent pour Active Directory.	
Base de données Oracle	Installez l'agent pour Oracle.	"Sauvegarde d'Oracle Database" (p. 703)
Site Web	Configurez la connexion au site Web.	"Protection des sites Web et hébergement des serveurs" (p. 710)

Pour plus d'informations sur les agents de protection disponibles et sur leur emplacement d'installation, reportez-vous à "De quel agent ai-je besoin ?" (p. 64)

Informations pour les administrateurs partenaires

- Un type de ressource peut manquer dans le panneau **Ajouter des terminaux** si un quota de service requis n'est pas activé dans le portail de gestion. Pour plus d'informations sur les quotas de service requis en fonction des ressources, consultez la section Activation ou désactivation d'éléments dans le Guide de l'administrateur partenaire.

- En tant qu'administrateur partenaire, vous ne pouvez pas ajouter de ressources au niveau **Tous les clients**. Pour ajouter une ressource, sélectionnez un tenant client.



Suppression de ressources de la console Cyber Protect

Vous pouvez supprimer de la console Cyber Protect les ressources que vous n'avez plus besoin de protéger. La procédure dépend du type de ressource.

Vous pouvez également désinstaller l'agent sur la ressource protégée. Lorsque vous désinstallez un agent, la ressource protégée est supprimée automatiquement de la console Cyber Protect.

Important
Lorsque vous supprimez une ressource de la console Cyber Protect, tous les plans appliqués à cette ressource sont révoqués. La suppression d'une ressource ne supprime aucun plan ni sauvegarde, et ne désinstalle pas l'agent de protection.

Le tableau suivant récapitule les types de ressources et les actions requises.

Ressources à supprimer	Actions requises	Procédure à suivre
Machines physiques et virtuelles		
Machines physiques ou virtuelles sur lesquelles un agent de protection est installé	1. Supprimez la ressource de la console Cyber Protect. 2. [Facultatif] Désinstallez l'agent de protection.	"Pour supprimer une ressource de la console Cyber Protect" (p. 351) (Ressource avec agent de protection)

Ressources à supprimer	Actions requises	Procédure à suivre
Machines virtuelles sauvegardées au niveau de l'hyperviseur (sauvegarde sans agent)	1. Dans la console Cyber Protect, supprimez l'ordinateur sur lequel l'agent de protection est installé. Toutes les machines virtuelles sauvegardées par cet agent sont supprimées automatiquement de la console. 2. [Facultatif] Désinstallez l'agent de protection.	"Pour supprimer une ressource de la console Cyber Protect" (p. 351) (Ressource sans agent de protection)
Ressources de cloud à cloud		
Ressources Microsoft 365 Business Ressources Google Workspace	Supprimez l'organisation Microsoft 365 ou Google Workspace de la console Cyber Protect. Toutes les ressources de cette organisation sont supprimées automatiquement de la console.	"Pour supprimer une ressource de la console Cyber Protect" (p. 351) (Ressource cloud à cloud)
Terminaux mobiles		
Terminaux Android Terminaux iOS	1. Supprimez le terminal mobile de la console Cyber Protect. 2. [Facultatif] Sur le terminal mobile, désinstallez l'application.	"Pour supprimer une ressource de la console Cyber Protect" (p. 351) (Terminal mobile)
Stockage en réseau		
Synology	1. Supprimez la ressource de la console Cyber	"Pour supprimer une ressource de la console Cyber Protect" (p. 351)

Ressources à supprimer	Actions requises	Procédure à suivre
	Protect. 2. [Facultatif] Désinstallez l'agent de protection.	(Ressource avec agent de protection)
Applications		
Microsoft SQL Server Microsoft Exchange Server Microsoft Active Directory Base de données Oracle	1. Dans la console Cyber Protect, supprimez l'ordinateur sur lequel l'agent de protection est installé. Les objets sauvegardés par cet agent sont supprimés automatiquement de la console. 2. [Facultatif] Désinstallez l'agent de protection.	"Pour supprimer une ressource de la console Cyber Protect" (p. 351) (Ressource sans agent de protection)
Sites Web	Supprimez le site Web de la console Cyber Protect.	"Pour supprimer une ressource de la console Cyber Protect" (p. 351) (Site Web)

Pour supprimer une ressource de la console Cyber Protect

Ressource avec agent de protection

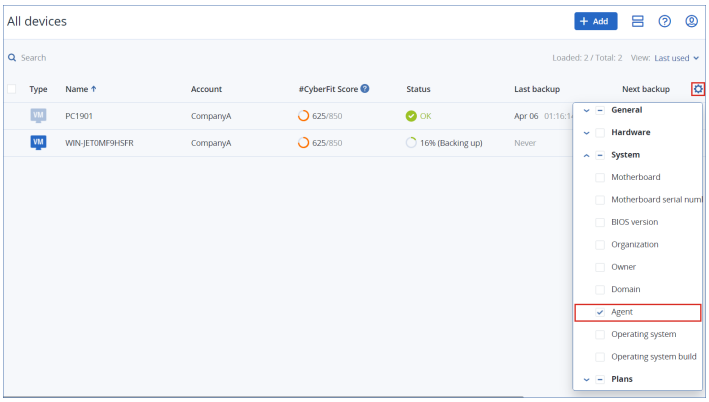
Vous pouvez supprimer ce type de ressource directement.

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cochez la case à côté de la ou des ressources à supprimer.
3. Dans le panneau **Actions**, cliquez sur **Supprimer**.
4. Confirmez votre choix en cliquant sur **Supprimer**.
5. [Facultatif] Désinstallez l'agent en suivant les indications de "Désinstallation d'agents" (p. 188).

Ressource sans agent de protection

Pour supprimer ce type de ressource, vous devez supprimer l'ordinateur sur lequel l'agent de protection est installé.

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Dans l'angle supérieur droit, cliquez sur l'icône en forme d'engrenage, puis cochez la case **Agent**.



La colonne **Agent** apparaît.

3. Dans la colonne **Agent**, cochez le nom de l'ordinateur sur lequel l'agent de protection est installé.
4. Dans la console Cyber Protect, cochez la case située à côté de l'ordinateur sur lequel l'agent de protection est installé.
5. Dans le panneau **Actions**, cliquez sur **Supprimer**.
6. Confirmez votre choix en cliquant sur **Supprimer**.
7. [Facultatif] Désinstallez l'agent en suivant les indications de "Désinstallation d'agents" (p. 188).

Ressource cloud à cloud

Pour supprimer les ressources sauvegardées par l'agent cloud, supprimez l'organisation Microsoft 365 ou Google Workspace de la console Cyber Protect.

1. Dans la console Cyber Protect, sélectionnez **Terminaux** > **Microsoft 365** ou **Terminaux** > **Google Workspace**.
2. Cliquez sur le nom de votre organisation Microsoft 365 ou Google Workspace.
3. Dans le panneau **Actions**, cliquez sur **Supprimer le groupe**.
4. Cliquez sur **Supprimer** pour confirmer votre action.

Terminal mobile

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cochez la case à côté de la ressource à supprimer.
3. Dans le panneau **Actions**, cliquez sur **Supprimer**.
4. Confirmez votre choix en cliquant sur **Supprimer**.
5. [Facultatif] Sur le terminal mobile, désinstallez l'application.

Site Web

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cochez la case à côté de la ressource à supprimer.

3. Dans le panneau **Actions**, cliquez sur **Supprimer**.
4. Confirmez votre choix en cliquant sur **Supprimer**.

Groupes du terminal

Grâce aux groupes de terminaux, vous pouvez protéger plusieurs ressources semblables avec un plan de groupe. Le plan est appliqué au groupe dans son intégralité et ne peut pas être révoqué d'un membre du groupe.

Une ressource peut être membre de plusieurs groupes. Une ressource incluse dans un groupe de terminaux peut toujours être protégée par différents plans.

Vous ne pouvez ajouter à un groupe de terminaux que des ressources du même type. Par exemple, sous **Hyper-V**, vous ne pouvez créer que des groupes de machines virtuelles Hyper-V. Sous **Machines avec des agents**, vous ne pouvez créer que des groupes de machines avec des agents installés.

Vous ne pouvez pas créer de groupes de terminaux dans un groupe de type **Tout** tel que le groupe root (superutilisateur) **Tous les terminaux** ou dans des groupes intégrés tels que **Machines avec des agents** > **Tout**, **Microsoft 365** > votre organisation > **Utilisateurs** > **Tous les utilisateurs**.

Groupes par défaut et groupes personnalisés

Groupes par défaut

Une fois qu'une ressource est enregistrée dans la console Cyber Protect, elle apparaît dans l'un des groupes root (superutilisateur) par défaut dans l'onglet **Terminaux**, par exemple, **Machines avec des agents**, **Microsoft 365** ou **Hyper-V**.

Toutes les ressources autres que de cloud à cloud enregistrées sont également répertoriées dans le groupe root (superutilisateur) **Tous les terminaux**. Un groupe root (superutilisateur) par défaut distinct portant le nom du tenant contient toutes les ressources autres que de cloud à cloud et toutes les unités de ce tenant.

Vous ne pouvez pas supprimer ou modifier les groupes root (superutilisateur), ni leur appliquer des plans.

Certains des groupes root (superutilisateur) contiennent un ou plusieurs niveaux de sous-groupes par défaut, par exemple, **Machines avec des agents** > **Tous**, **Microsoft 365** > votre organisation > **Équipes** > **Toutes les équipes**, **Google Workspace** > votre organisation > **Lecteurs partagés** > **Tous les disques partagés**.

Vous ne pouvez ni modifier ni supprimer les sous-groupes par défaut.

Groupes personnalisés

La protection de toutes les ressources d'un groupe par défaut n'est peut-être pas très pratique, car certaines ressources nécessitent une planification de protection ou des paramètres de protection

différents.

Dans certains des groupes root (superutilisateur), par exemple dans **Machines avec des agents**, **Microsoft 365** ou **Google Workspace**, vous pouvez créer des sous-groupes personnalisés. Ces sous-groupes peuvent être statiques ou dynamiques.

Vous pouvez modifier, renommer ou supprimer n'importe quel groupe personnalisé.

Groupes statiques et dynamiques

Vous pouvez créer le type de groupes personnalisés suivant :

- Statique
- Dynamique

Groupes statiques

Les groupes statiques contiennent des ressources ajoutées manuellement.

Le contenu d'un groupe statique change uniquement lorsque vous ajoutez ou supprimez une ressource explicitement.

Exemple : Vous créez un groupe statique pour le service comptable de votre entreprise, puis ajoutez les ordinateurs des comptables à ce groupe manuellement. Lorsque vous appliquez un plan de groupe, les ordinateurs de ce groupe sont protégés. Si un nouveau comptable est embauché, vous devrez ajouter son ordinateur au groupe statique manuellement.

Groupes dynamiques

Les groupes dynamiques contiennent des ressources qui correspondent à des critères spécifiques. Vous définissez ces critères par avance en créant une requête de recherche qui comprend des attributs (par exemple, `osType`), leurs valeurs (par exemple, `Windows`) et des opérateurs de recherche (par exemple, `IN`).

Par conséquent, vous pouvez créer un groupe dynamique pour tous les ordinateurs dont le système d'exploitation est Windows ou un groupe dynamique contenant tous les utilisateurs de votre organisation Microsoft 365 dont les adresses e-mail commencent par `john`.

Toutes les ressources disposant des attributs et valeurs nécessaires sont ajoutées automatiquement au groupe, et toute ressource perdant un attribut ou une valeur nécessaire est supprimée automatiquement du groupe.

Exemple 1 : Les noms d'hôte des ordinateurs appartenant au service comptable comportent le mot « comptabilité ». Vous recherchez les ordinateurs dont les noms contiennent le mot « comptabilité », puis enregistrez les résultats de la recherche en tant que groupe dynamique. Vous appliquez ensuite un plan de protection au groupe. Si un nouveau comptable est embauché, le nom de son ordinateur contiendra le mot « comptabilité » et cet ordinateur sera ajouté automatiquement au groupe dynamique dès que vous l'enregistrez dans la console Cyber Protect.

Exemple 2 : Le service comptable forme une unité d'organisation (UO) Active Directory séparée. Vous indiquez l'UO de comptabilité comme étant un attribut nécessaire, puis enregistrez les résultats de la recherche en tant que groupe dynamique. Vous appliquez ensuite un plan de protection au groupe. Si un nouveau comptable est embauché, son ordinateur est ajouté au groupe dynamique dès qu'il est ajouté à l'UO Active Directory, puis il est enregistré dans la console Cyber Protect (quel que soit l'ordre d'arrivée).

Groupes de cloud à cloud et groupes autres que de cloud à cloud

Les groupes de cloud à cloud contiennent des ressources Microsoft 365 ou Google Workspace qui sont sauvegardées par un agent cloud.

Les groupes autres que de cloud à cloud contiennent tous les autres types de ressources.

Plans pris en charge pour les groupes de terminaux

Le tableau suivant récapitule les plans que vous pouvez appliquer à un groupe de terminaux.

Groupe	Plans disponibles	Emplacement du plan
Ressources de cloud à cloud (ressources Microsoft 365 et Google Workspace)	Plan de sauvegarde	**Gestion** > **Sauvegarde d'applications dans le Cloud**
Ressources autres que de cloud à cloud	Plan de protection	**Gestion** > **Plans de protection**
	Plan de gestion à distance	**Gestion** > **Plans de gestion à distance**
	Plan de création de script	**Gestion** > **Plans de création de scripts**

Les ressources cloud telles que les utilisateurs Microsoft 365 ou Google Workspace, les partages OneDrive et Google Drive, Microsoft Teams ou les groupes Azure AD sont synchronisées dans la console Cyber Protect immédiatement après que vous ajoutez une organisation Microsoft 365 ou Google Workspace à la console. Toutes les autres modifications apportées à une organisation sont synchronisées une fois par jour.

Si vous devez synchroniser une modification immédiatement, accédez depuis la console Cyber Protect à **Terminaux** > **Microsoft 365** ou **Terminaux** > **Google Workspace** respectivement, sélectionnez l'organisation nécessaire, puis cliquez sur **Actualiser**.

Création d'un groupe statique

Vous pouvez créer un groupe statique vide et lui ajouter des ressources.

Vous pouvez également sélectionner des ressources et créer un nouveau groupe statique à partir de votre sélection.

Vous ne pouvez pas créer de groupes de terminaux dans un groupe de type **Tout** tel que le groupe root (superutilisateur) **Tous les terminaux** ou dans des groupes intégrés tels que **Machines avec des agents** > **Tout**, **Microsoft 365** > votre organisation > **Utilisateurs** > **Tous les utilisateurs**.

Pour créer un groupe statique

Dans la fenêtre principale

1. Cliquez sur **Terminaux**, puis sélectionnez le groupe root (superutilisateur) contenant les ressources pour lesquelles vous souhaitez créer un groupe statique.
2. [Facultatif] Pour créer un groupe imbriqué, accédez à un groupe statique existant.

   Remarque
   La création de groupes statiques imbriqués n'est pas disponible pour les ressources de cloud à cloud.

3. Cliquez sur **+ Nouveau groupe statique** en dessous de l'arborescence de groupe ou sur **Nouveau groupe statique** dans le volet **Actions**.
4. Indiquez le nom du nouveau groupe.
5. [Facultatif] Ajoutez un commentaire pour le groupe.
6. Cliquez sur **OK**.

Dans l'arborescence du groupe

1. Cliquez sur **Terminaux**, puis sélectionnez le groupe root (superutilisateur) contenant les ressources pour lesquelles vous souhaitez créer un groupe statique.
2. Cliquez sur l'icône en forme d'engrenage en regard du nom du groupe dans lequel vous souhaitez créer un nouveau groupe statique.

   Remarque
   La création de groupes statiques imbriqués n'est pas disponible pour les ressources de cloud à cloud.

3. Cliquez sur **Nouveau groupe statique**.
4. Indiquez le nom du nouveau groupe.
5. [Facultatif] Ajoutez un commentaire pour le groupe.
6. Cliquez sur **OK**.

À partir de la sélection

1. Cliquez sur **Terminaux**, puis sélectionnez le groupe root (superutilisateur) contenant les ressources pour lesquelles vous souhaitez créer un groupe statique.

Remarque
Vous ne pouvez pas créer de groupes de terminaux dans un groupe de type **Tout** tel que le groupe root (superutilisateur) **Tous les terminaux** ou dans des groupes intégrés tels que **Machines avec des agents** > **Tout**, **Microsoft 365** > votre organisation > **Utilisateurs** > **Tous les utilisateurs**.

2. Cochez les cases en regard des ressources pour lesquelles vous souhaitez créer un nouveau groupe, puis cliquez sur **Ajouter au groupe**.
3. Dans l'arborescence de dossiers, sélectionnez le niveau parent du nouveau groupe, puis cliquez sur **Nouveau groupe statique**.

Remarque
La création de groupes statiques imbriqués n'est pas disponible pour les ressources de cloud à cloud.

4. Indiquez le nom du nouveau groupe.
5. [Facultatif] Ajoutez un commentaire pour le groupe.
6. Cliquez sur **OK**.
   Le nouveau groupe apparaît dans l'arborescence de dossiers.
7. Cliquez sur **Valider**.

Ajout de ressources à un groupe statique

Vous pouvez sélectionner le groupe cible en premier, puis lui ajouter des ressources.

Vous pouvez également sélectionner les ressources en premier, puis les ajouter à un groupe.

Pour ajouter des ressources à un groupe statique

Sélection du groupe cible en premier

1. Cliquez sur **Terminaux**, puis accédez au groupe cible.
2. Sélectionnez le groupe cible, puis cliquez sur **Ajouter des terminaux**.
3. Dans l'arborescence de dossiers, sélectionnez le groupe contenant les ressources requises.
4. Cochez les cases en regard des ressources que vous souhaitez ajouter, puis cliquez sur **Ajouter**.

Sélection des ressources en premier

1. Cliquez sur **Terminaux**, puis sélectionnez le groupe root (superutilisateur) contenant les ressources requises.
2. Cochez les cases en regard des ressources que vous souhaitez ajouter, puis cliquez sur **Ajouter au groupe**.
3. Dans l'arborescence de dossiers, sélectionnez le groupe cible, puis cliquez sur **Terminé**.

Création d'un groupe dynamique

Vous créez un groupe dynamique en recherchant des ressources ayant des attributs spécifiques dont vous définissez les valeurs dans une requête de recherche. Enregistrez ensuite les résultats de la recherche en tant que groupe dynamique.

Les attributs pris en charge pour la recherche et la création de groupes dynamiques diffèrent pour les ressources de cloud à cloud et les ressources non-cloud à cloud. Pour plus d'informations sur les attributs pris en charge, voir "Rechercher des attributs pour les ressources autres que cloud à cloud" (p. 361) et "Rechercher des attributs pour les ressources de cloud à cloud" (p. 360).

Les groupes dynamiques sont créés dans leurs groupes root (superutilisateur) respectifs. Les groupes dynamiques imbriqués ne sont pas pris en charge.

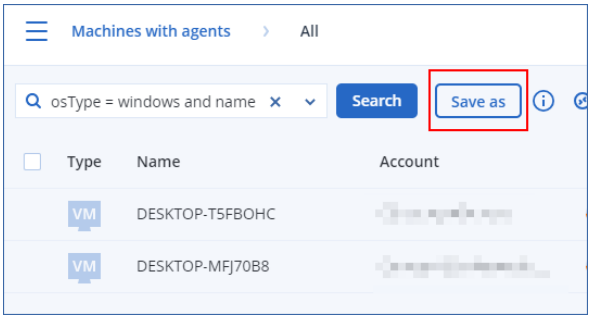
Vous ne pouvez pas créer de groupes de terminaux dans un groupe de type **Tout** tel que le groupe root (superutilisateur) **Tous les terminaux** ou dans des groupes intégrés tels que **Machines avec des agents** > **Tout**, **Microsoft 365** > votre organisation > **Utilisateurs** > **Tous les utilisateurs**.

Pour créer un groupe dynamique

Ressources autres que de cloud à cloud

1. Cliquez sur **Terminaux**, puis sélectionnez le groupe contenant les ressources pour lesquelles vous souhaitez créer un groupe dynamique.
2. Recherchez les ressources à l'aide des attributs et des opérateurs de recherche pris en charge.

   Vous pouvez utiliser plusieurs attributs et opérateurs dans une même requête. Pour plus d'informations sur les attributs pris en charge, voir "Rechercher des attributs pour les ressources autres que cloud à cloud" (p. 361).
3. Cliquez sur **Enregistrer sous** en regard du champ de recherche.



Remarque

Le bouton **Enregistrer sous** n'est pas disponible si vous n'êtes pas autorisé à créer un groupe dynamique à un niveau spécifique, par exemple dans le groupe racine **Terminaux** > **Tous les terminaux**.

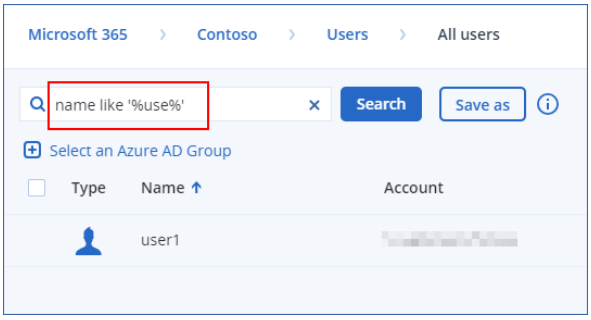
Sélectionnez un autre niveau (par exemple, **Terminaux** > **Terminaux avec agents** > **Tous**), puis répétez les étapes ci-dessus. Avec cette recherche, vous pouvez créer un groupe dynamique dans **Terminaux avec agents**, et non dans **Terminaux avec agents** > **Tous**.

4. Indiquez le nom du nouveau groupe.
5. [Facultatif] Dans le champ **Commentaire**, ajoutez une description pour le nouveau groupe.
6. Cliquez sur **OK**.

Ressources de cloud à cloud

1. Cliquez sur **Terminaux**, puis sélectionnez **Microsoft 365** ou **Google Workspace**.
2. Sélectionnez le groupe qui contient les ressources pour lesquelles vous souhaitez créer un nouveau groupe dynamique. Par exemple, **Utilisateurs** > **Tous les utilisateurs**.
3. Recherchez les ressources à l'aide des attributs et des opérateurs de recherche pris en charge, ou en sélectionnant des utilisateurs de Microsoft 365 dans un groupe Active Directory spécifique.

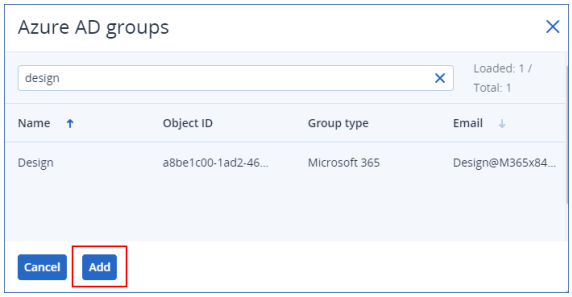
   Vous pouvez utiliser plusieurs attributs et opérateurs dans une même requête. Pour plus d'informations sur les attributs pris en charge, voir "Rechercher des attributs pour les ressources de cloud à cloud" (p. 360).



4. [Uniquement pour **Microsoft 365** > **Utilisateurs**] Pour sélectionner des utilisateurs dans un groupe Active Directory spécifique, procédez comme suit :
   a. Accédez à **Utilisateurs** > **Tous les utilisateurs**.
   b. Cliquez sur **Sélectionnez un groupe Azure AD**.

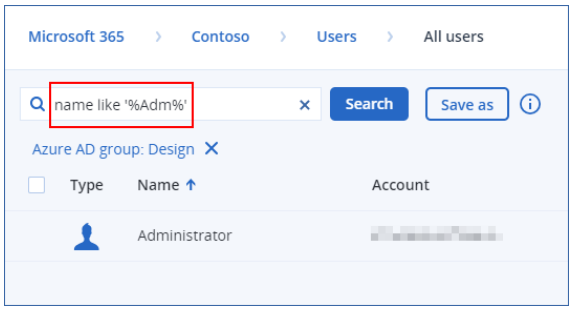
      La liste des groupes Active Directory de votre organisation s'affiche.

      Vous pouvez rechercher dans cette liste un groupe spécifique, ou trier les groupes par nom ou par adresse e-mail.
   c. Sélectionnez le groupe Active Directory souhaité, puis cliquez sur **Ajouter**.



   d. [Facultatif] Pour inclure ou exclure des utilisateurs spécifiques du groupe Active Directory sélectionné, créez une requête de recherche à l'aide des attributs et opérateurs de recherche pris en charge.

Vous pouvez utiliser plusieurs attributs et opérateurs dans une même requête. Pour plus d'informations sur les attributs pris en charge, voir "Rechercher des attributs pour les ressources de cloud à cloud" (p. 360).



5. Cliquez sur **Enregistrer sous** en regard du champ de recherche.

Remarque
Le bouton **Enregistrer sous** n'est pas disponible si vous n'êtes pas autorisé à créer un groupe dynamique à un niveau spécifique. Par exemple, dans **Microsoft 365** > votre organisation > **Utilisateurs**.
Sélectionnez un autre niveau (par exemple, **Microsoft 365** > votre organisation > **Utilisateurs** > **Tous**), puis répétez les étapes ci-dessus. Avec cette recherche, vous pouvez créer un groupe dynamique dans **Microsoft 365** > votre organisation > **Utilisateurs** >, et non dans **Utilisateurs** > **Tous**.

6. Indiquez le nom du nouveau groupe.
7. [Facultatif] Dans le champ **Commentaire**, ajoutez une description pour le nouveau groupe.
8. Cliquez sur **OK**.

Rechercher des attributs pour les ressources de cloud à cloud

Le tableau suivant récapitule les attributs que vous pouvez utiliser dans vos requêtes de recherche pour les ressources Microsoft 365 et Google Workspace.

Pour voir les attributs que vous pouvez utiliser dans les requêtes de recherche d'autres types de ressources, reportez-vous à "Rechercher des attributs pour les ressources autres que cloud à cloud" (p. 361).

Attribut	Signification	Utilisable dans	Exemples de requête de recherche	Pris en charge pour la création de groupe
`name`	Nom affiché d'une ressource Microsoft 365 ou Google Workspace	Toutes les ressources de cloud à cloud	`name = 'My Name'` `name LIKE '*nam*'`	Oui

Attribut	Signification	Utilisable dans	Exemples de requête de recherche	Pris en charge pour la création de groupe

`email`	Adresse e-mail d'un utilisateur ou d'un groupe Microsoft 365, ou d'un utilisateur Google Workspace	Microsoft 365 > Groupes
		Microsoft 365 > Utilisateurs
		Google Workspace > Utilisateurs
			`email = 'my_group_email@mycompany.com'`
			`email LIKE '*@company*'`
			`email NOT LIKE '*enterprise.com'`
				Oui

`siteName`	Nom d'un site associé à un groupe Microsoft 365	Microsoft 365 > Groupes	`siteName = 'my_site'` `siteName LIKE '*company.com*support*'`	Oui
`url`	Adresse Web d'un groupe Microsoft 365 ou d'un site SharePoint	Microsoft 365 > Groupes Microsoft 365 > Collections de sites	`url = 'https://www.mycompany.com/'` `url LIKE '*www.mycompany.com*'`	Oui

Rechercher des attributs pour les ressources autres que cloud à cloud

Le tableau suivant récapitule les attributs que vous pouvez utiliser dans vos requêtes de recherche pour les ressources autres que cloud à cloud.

Pour voir les attributs que vous pouvez utiliser dans les requêtes de recherche de ressources de cloud à cloud, reportez-vous à "Rechercher des attributs pour les ressources de cloud à cloud" (p. 360).

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
Général			
`name`	Nom de la ressource, par exemple : • Nom d'hôte pour les machines physiques • Nom des machines virtuelles • Nom de la base de	`name = 'en-00'`	Oui

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	données • Adresse électronique pour les boîtes aux lettres		
`id`	Identifiant du terminal. Pour afficher l'identifiant du terminal, sous **Terminaux**, sélectionnez le terminal, puis cliquez sur **Détails** > **Toutes les propriétés**. L'identifiant apparaît dans le champ `id`.	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Oui
`resourceType`	Type de ressource. Valeurs possibles : • `'machine'` • `'exchange'` • `'mssql_server'` • `'mssql_instance'` • `'mssql_database'` • `'mssql_database_folder'` • `'msexchange_database'` • `'msexchange_storage_group'` • `'msexchange_mailbox.msexchange'` • `'msexchange_mailbox.office365'` • `'mssql_aag_group'` • `'mssql_aag_database'` • `'virtual_machine.vmww'` • `'virtual_machine.vmwesx'` • `'virtual_host.vmwesx'` • `'virtual_cluster.vmwesx'` • `'virtual_`	`resourceType = 'machine'` `resourceType in ('mssql_aag_database', 'mssql_database')`	Oui

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	appliance.vmwesx' • 'virtual_ application.vmwesx' • 'virtual_resource_ pool.vmwesx' • 'virtual_center.vmwesx' • 'datastore.vmwesx' • 'datastore_ cluster.vmwesx' • 'virtual_ network.vmwesx' • 'virtual_data_ center.vmwesx' • 'virtual_machine.vmww' • 'virtual_ cluster.mshyperv' • 'virtual_ machine.mshyperv' • 'virtual_host.mshyperv' • 'virtual_ network.mshyperv' • 'virtual_ folder.mshyperv' • 'virtual_data_ center.mshyperv' • 'datastore.mshyperv' • 'virtual_machine.msvs' • 'virtual_ machine.parallelsw' • 'virtual_ host.parallelsw' • 'virtual_ cluster.parallelsw' • 'virtual_machine.rhev' • 'virtual_machine.kvm' • 'virtual_machine.xen' • 'bootable_media'		

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
`chassis`	Type de châssis. Valeurs possibles : • `laptop` • `desktop` • `server` • `other` • `unknown`	`chassis = 'laptop'` `chassis IN ('laptop', 'desktop')`	Oui
`ip`	Adresse IP (uniquement pour les machines physiques).	`ip RANGE ('10.250.176.1','10.250.176.50')`	Oui
`comment`	Commentaire pour un terminal. Il peut être spécifié automatiquement ou manuellement. Valeur par défaut : • Pour les machines physiques sous Windows, la description de l'ordinateur dans Windows est automatiquement copiée en tant que commentaire. Cette valeur est synchronisée toutes les 15 minutes. • Vide pour d'autres terminaux. **Remarque** La synchronisation automatique est désactivée si du texte est ajouté manuellement dans le champ de commentaire. Pour réactiver la synchronisation, effacez ce texte.	`comment = 'important machine'` `comment = ''` (toutes les machines sans commentaire)	Oui

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe

	Pour actualiser les commentaires automatiquement synchronisés pour vos ressources, redémarrez le service de machine gérée dans **Services Windows** ou exécutez les commandes suivantes dans l'invite de commandes :
	`net stop mms`
	`net start mms`
	Pour afficher un commentaire concernant un terminal, sous **Terminaux**, sélectionnez le terminal, cliquez sur **Détails**, puis localisez la section **Commentaire**.
	Pour ajouter ou modifier un commentaire manuellement, cliquez sur **Ajouter** ou **Modifier**.
	Pour les terminaux sur lesquels un agent de protection est installé, il existe deux champs de commentaire distincts :
	• Commentaire sur l'agent
	◦ Pour les machines physiques sous Windows, la description de l'ordinateur dans Windows est automatiquement		

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	copiée en tant que commentaire. Cette valeur est synchronisée toutes les 15 minutes. ◦ Vide pour d'autres terminaux. **Remarque** La synchronisation automatique est désactivée si du texte est ajouté manuellement dans le champ de commentaire. Pour réactiver la synchronisation, effacez ce texte. • Commentaires sur le terminal ◦ Si le commentaire sur l'agent est automatiquement spécifié, il est copié en tant que commentaire sur le terminal. Les commentaires sur l'agent ajoutés manuellement ne sont pas copiés en tant que commentaires sur le terminal. ◦ Les commentaires sur le terminal ne sont pas copiés en tant que commentaires sur l'agent. Concernant un terminal,		

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	l'un de ces champs de commentaire peut être rempli, ou les deux, ou encore les deux peuvent être laissés vierges. Si les deux commentaires sont spécifiés, le commentaire sur le terminal sera prioritaire. Pour afficher un commentaire sur un agent, sous **Paramètres** > **Agents**, sélectionnez un terminal avec l'agent, cliquez sur **Détails**, puis localisez la section **Commentaire**. Pour afficher un commentaire concernant un terminal, sous **Terminaux**, sélectionnez le terminal, cliquez sur **Détails**, puis localisez la section **Commentaire**. Pour ajouter ou modifier un commentaire manuellement, cliquez sur **Ajouter** ou **Modifier**.		
`isOnline`	Disponibilité de la ressource. Valeurs possibles : • `true` • `false`	`isOnline = true`	Non
`hasAsz`	Disponibilité de la zone sécurisée. Valeurs possibles : • `true`	`hasAsz = true`	Oui

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	• `false`		

`tzOffset`	Décalage UTC, en minutes.	`tzOffset = 120`
		`tzOffset > 120`
		`tzOffset < 120`
			Oui

CPU, mémoire, disques			
`cpuArch`	Architecture du processeur. Valeurs possibles : • `'x64'` • `'x86'`	`cpuArch = 'x64'`	Oui
`cpuName`	Nom du processeur.	`cpuName LIKE '%XEON%'`	Oui
`memorySize`	Taille de la mémoire RAM en mégaoctets.	`memorySize < 1024`	Oui
`diskSize`	Taille du disque dur en gigaoctets ou en mégaoctets (uniquement pour les machines physiques).	`diskSize < 300GB` `diskSize >= 3000000MB`	Non
Système d'exploitation			
`osName`	Nom du système d'exploitation.	`osName LIKE '%Windows XP%'`	Oui
`osType`	Type de système d'exploitation. Valeurs possibles : • `'windows'` • `'linux'` • `'macosx'`	`osType = 'windows'` `osType IN ('linux', 'macosx')`	Oui
`osArch`	Architecture du système d'exploitation. Valeurs possibles : • `'x64'`	`cpuArch = 'x86'`	Oui

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	• `'x86'`		
`osProductType`	Type de produit du système d'exploitation. Valeurs possibles : • `'dc'` Représente le contrôleur de domaine. **Remarque** Lorsque le rôle de contrôleur de domaine est affecté à un serveur Windows, la valeur `osProductType` passe de `server` à `dc`. Ces ordinateurs ne seront pas inclus dans les résultats de recherche pour `osProductType='server'`. • `'server'` • `'workstation'`	`osProductType = 'server'`	Oui
`osSp`	Service Pack du système d'exploitation.	`osSp = 1`	Oui
`osVersionMajor`	Version majeure du système d'exploitation.	`osVersionMajor = 1`	Oui
`osVersionMinor`	Version mineure du système d'exploitation.	`osVersionMinor > 1`	Oui
Agent			
`agentVersion`	Version de l'agent de protection installé.	`agentVersion LIKE '12.0.*'`	Oui
`hostId`	Identifiant interne de l'agent de protection. Pour afficher l'identifiant de	`hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Oui

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	l'agent de protection, sous **Terminaux**, sélectionnez le terminal, puis cliquez **Détails** > **Toutes les propriétés**. Vérifiez la valeur `id` de la propriété `agent`.		
`virtualType`	Type de machine virtuelle. Valeurs possibles : • `'vmwesx'` Machines virtuelles VMware. • `'mshyperv'` Machines virtuelles Hyper-V. • `'pcs'` Machines virtuelles Virtuozzo. • `'hci'` Machines virtuelles Virtuozzo Hybrid Infrastructure. • `'scale'` Machines virtuelles Scale Computing HC3. • `'ovirt'` Machines virtuelles oVirt.	`virtualType = 'vmwesx'`	Oui
`insideVm`	Machine virtuelle avec un agent. Valeurs possibles : • `true` • `false`	`insideVm = true`	Oui
Emplacement			
`tenant`	Nom du tenant auquel appartient le terminal.	`tenant = 'Unit 1'`	Oui

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
`tenantId`	Identificateur du tenant auquel appartient le terminal. Pour afficher l'identifiant du tenant, sous **Terminaux**, sélectionnez le terminal, puis cliquez **Détails** > **Toutes les propriétés**. L'identifiant apparaît dans le champ `ownerId`.	`tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'`	Oui
`ou`	Terminaux appartenant à l'unité organisationnelle Active Directory spécifiée.	`ou IN ('RnD', 'Computers')`	Oui
Statut			
`state`	État du terminal. Valeurs possibles : • `'idle'` • `'interactionRequired'` • `'canceling'` • `'backup'` • `'recover'` • `'install'` • `'reboot'` • `'failback'` • `'testReplica'` • `'run_from_image'` • `'finalize'` • `'failover'` • `'replicate'` • `'createAsz'` • `'deleteAsz'` • `'resizeAsz'`	`state = 'backup'`	Non
status	État de protection. Valeurs possibles : • ok	`status = 'ok'` `status IN ('error', 'warning')`	Non

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	• `warning` • `error` • `critical` • `protected` • `notProtected`		
`protectedByPlan`	Terminaux protégés par un plan de protection avec un identifiant donné. Pour voir l'identifiant du plan, sélectionnez un plan dans **Gestion** > **Plans de protection**, cliquez sur la barre dans la colonne **État**, puis cliquez sur le nom de l'état. Une nouvelle recherche avec l'identifiant du plan sera créée.	`protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Non
`okByPlan`	Terminaux protégés par un plan de protection avec un identifiant donné et un état **OK**.	`okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Non
`errorByPlan`	Terminaux protégés par un plan de protection avec un identifiant donné et un état **Erreur**.	`errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Non
`warningByPlan`	Terminaux protégés par un plan de protection avec un identifiant donné et un état **Avertissement**.	`warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Non
`runningByPlan`	Terminaux protégés par un plan de protection avec un identifiant donné et un état **En cours d'exécution**.	`runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Non
`interactionByPlan`	Terminaux protégés par un plan de protection avec un identifiant donné et un état	`interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Non

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	Intervention requise.		

`lastBackupTime`*	Date et heure de la dernière sauvegarde réussie.
	Le format est « `AAAA-MM-JJ HH:MM` ».
		`lastBackupTime > '2023-03-11'`
		`lastBackupTime <= '2023-03-11 00:15'`
		`lastBackupTime is null`
			Non

`lastBackupTryTime`*	Heure de la dernière tentative de sauvegarde. Le format est « `AAAA-MM-JJ HH:MM` ».	`lastBackupTryTime >= '2023-03-11'`	Non
`nextBackupTime`*	Heure de la prochaine sauvegarde. Le format est « `AAAA-MM-JJ HH:MM` ».	`nextBackupTime >= '2023-08-11'`	Non

`lastVAScanTime`*	Date et heure de la dernière évaluation des vulnérabilités réussie.
	Le format est « `AAAA-MM-JJ HH:MM` ».
		`lastVAScanTime > '2023-03-11'`
		`lastVAScanTime <= '2023-03-11 00:15'`
		`lastVAScanTime is null`
			Oui

`lastVAScanTryTime`*	Heure de la dernière tentative d'évaluation des vulnérabilités. Le format est « `AAAA-MM-JJ HH:MM` ».	`lastVAScanTimeTryTime >= '2022-03-11'`	Oui
`nextVAScanTime`*	Heure de la prochaine évaluation des vulnérabilités. Le format est « `AAAA-MM-JJ HH:MM` ».	`nextVAScanTime <= '2023-08-11'`	Oui
`network_status`	Statut d'isolation réseau d'EDR (Détection et réponse des terminaux). Valeurs possibles :	`network_status= 'connected'`	Oui

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	• `connected` • `isolated`		

Remarque
Si vous n'indiquez pas la valeur heure et minutes, la date et l'heure de début seront considérées comme étant AAAA-MM-JJ 00:00, et la date et l'heure de fin seront considérées comme étant AAAA-MM-JJ 23:59:59. Par exemple, `dernièreHeuredeSauvegarde = 2023-01-20`, signifie que les résultats de recherche incluront toutes les sauvegardes de l'intervalle `dernièreHeuredeSauvegarde >= 2023-01-20 00:00` et `dernièreHeuredeSauvegarde <= 2023-01-20 23:59:59`.

Opérateurs de recherche

Le tableau suivant récapitule les opérateurs que vous pouvez utiliser dans vos requêtes de recherche.

Vous pouvez utiliser plusieurs opérateurs dans une même requête.

Opérateur	Pris en charge pour	Signification	Exemples
`AND`	Toutes les ressources	Opérateur de conjonction logique	`name like 'en-00' AND tenant = 'Unit 1'`
`OR`	Toutes les ressources	Opérateur de disjonction logique	`state = 'backup' OR state = 'interactionRequired'`
`NOT`	Toutes les ressources	Opérateur de négation logique	`NOT(osProductType = 'workstation')`
`IN (<value1>,... <valueN>)`	Toutes les ressources	Cet opérateur vérifie si une expression correspond à une valeur d'une liste.	`osType IN ('windows', 'linux')`
`NOT IN`	Toutes les ressources	Cet opérateur est l'opposé de l'opérateur `IN`.	`NOT osType IN ('windows', 'linux')`
`LIKE 'wildcard pattern'`	Toutes les ressources	Cet opérateur vérifie si une expression	`name LIKE 'en-00'` `name LIKE '*en-00'`

Opérateur	Pris en charge pour	Signification	Exemples

		correspond au modèle de caractères génériques.
		
		Vous pouvez utiliser les opérateurs de caractères génériques suivants :
		
		• * ou % L'astérisque et le symbole du pourcentage représentent zéro, un ou plusieurs caractères.
		• _ Le tiret bas représente un seul caractère.
			`name LIKE '*en-00*'`
			
			`name LIKE 'en-00_'`

`NOT LIKE 'wildcard pattern'`	Toutes les ressources	Cet opérateur est l'opposé de l'opérateur `LIKE`.
		
		Vous pouvez utiliser les opérateurs de caractères génériques suivants :
		
		• * ou % L'astérisque et le symbole du pourcentage représentent zéro, un ou plusieurs caractères.
		• _ Le tiret bas représente un seul caractère.
			`NOT name LIKE 'en-00'`
			
			`NOT name LIKE '*en-00'`
			
			`NOT name LIKE '*en-00*'`
			
			`NOT name LIKE 'en-00_'`

`RANGE (<starting_value>, <ending_value>)`	Toutes les ressources	Cet opérateur vérifie si une expression est comprise dans une plage (inclusive) de valeurs.
		
		Les requêtes avec chaînes alphanumériques
			`ip RANGE('10.250.176.1','10.250.176.50')`
			
			`name RANGE('a','d')`
			
			Avec cette requête, vous pouvez filtrer tous les noms commençant par A, B et C, tels qu'`Alice`, `Bob`, `Claire`. En revanche, seule la lettre D répond aux exigences. Par conséquent, les noms comportant plus de lettres tels que `Diana` ou `Don` ne seront pas

Opérateur	Pris en charge pour	Signification	Exemples
		utilisent l'ordre de tri ASCII, mais ne font pas la différence entre les majuscules et les minuscules.	inclus. Pour obtenir le même résultat, vous pouvez également utiliser la requête suivante : `name >= 'a' AND name <= 'd'`
= ou ==	Toutes les ressources	Opérateur *Égal à*	`osProductType = 'server'`
!= ou <>	Toutes les ressources	Opérateur *Différent de*	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`
<	Ressources autres que de cloud à cloud	Opérateur *Inférieur à*	`memorySize < 1024`
>	Ressources autres que de cloud à cloud	Opérateur *Supérieur à*.	`diskSize > 300GB`
<=	Ressources autres que de cloud à cloud	Opérateur *Inférieur ou égal à*	`lastBackupTime <= '2022-03-11 00:15'`
>=	Ressources autres que de cloud à cloud	Opérateur *Supérieur ou égal à*	`nextBackupTime >= '2022-08-11'`

Modification d'un groupe dynamique

Vous modifiez un groupe dynamique en changeant la requête de recherche qui définit le contenu du groupe.

Dans les groupes dynamiques basés sur Active Directory, vous pouvez également modifier le groupe Active Directory.

Pour modifier un groupe dynamique

En modifiant la requête de recherche

1. Cliquez sur **Terminaux**, accédez au groupe dynamique que vous souhaitez modifier, puis sélectionnez-le.

2. Cliquez sur l'icône en forme d'engrenage située à côté du nom du groupe, puis sur **Modifier**. Vous pouvez également cliquer sur **Modifier** dans le volet **Actions**.
3. Modifiez la requête de recherche en changeant les attributs de recherche, leurs valeurs ou les opérateurs de recherche, puis cliquez sur **Rechercher**.
4. Cliquez sur **Enregistrer** en regard du champ de recherche.

En modifiant le groupe Active Directory

Remarque
Cette procédure s'applique aux groupes dynamiques basés sur Active Directory. Les groupes dynamiques basés sur Active Directory ne sont disponibles que dans **Microsoft 365** > **Utilisateurs**.

1. Cliquez sur **Terminaux**, accédez à **Terminaux** > **Microsoft 365** > votre organisation > **Utilisateurs**.
2. Sélectionnez le groupe dynamique que vous souhaitez modifier.
3. Cliquez sur l'icône en forme d'engrenage située à côté du nom du groupe, puis sur **Modifier**. Vous pouvez également cliquer sur **Modifier** dans le volet **Actions**.
4. Modifiez le contenu du groupe en effectuant l'une des opérations suivantes :
   - Modifiez le groupe Active Directory déjà sélectionné en cliquant sur son nom, puis en sélectionnant un nouveau groupe Active Directory dans la liste qui s'affiche.
   - Modifiez la requête de recherche, puis cliquez sur **Rechercher**.
     La requête de recherche est limitée au groupe Active Directory sélectionné.
5. Cliquez sur **Enregistrer** en regard du champ de recherche.

Vous pouvez également enregistrer vos modifications sans remplacer le groupe actuel. Pour enregistrer la configuration modifiée en tant que nouveau groupe, cliquez sur le bouton fléché en regard du champ de recherche, puis cliquez sur **Enregistrer sous**.

Suppression d'un groupe

Lorsque vous supprimez un groupe de terminaux, tous les plans appliqués à ce groupe sont révoqués. Les ressources du groupe ne sont plus protégées si aucun autre plan ne leur est appliqué.

Pour supprimer un groupe de terminaux

1. Cliquez sur **Terminaux**, puis accédez au groupe que vous souhaitez supprimer.
2. Cliquez sur l'icône en forme d'engrenage située à côté du nom du groupe, puis sur **Supprimer**.
3. Confirmez votre choix en cliquant sur **Supprimer**.

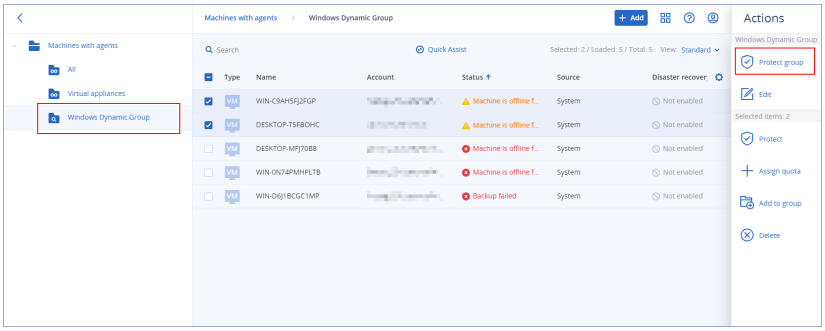
Application d'un plan à un groupe

Vous pouvez appliquer un plan à un groupe en sélectionnant d'abord le groupe, puis en lui attribuant un plan.

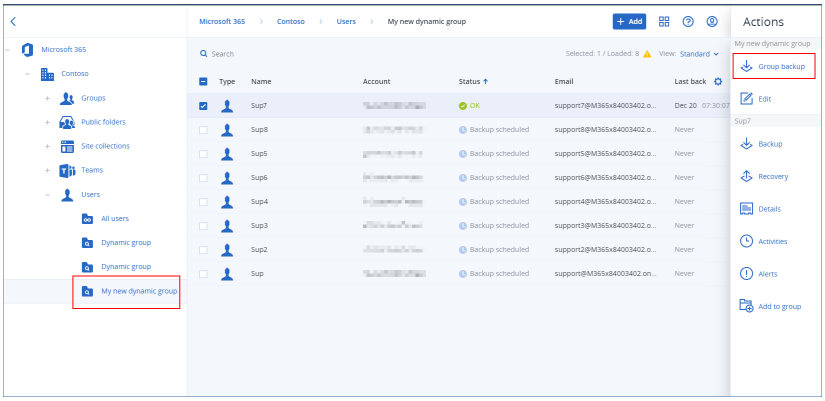
Vous pouvez également ouvrir un plan pour le modifier, puis lui ajouter un groupe.

Pour appliquer un plan à un groupe

1. Cliquez sur **Terminaux**, puis accédez au groupe auquel vous souhaitez appliquer un plan.
2. [Pour les ressources autres que de cloud à cloud] Cliquez sur **Protéger un groupe**.



   La liste des plans pouvant être appliqués s'affiche.
3. [Pour les ressources de cloud à cloud] Cliquez sur **Sauvegarde de groupe**.



   La liste des plans de sauvegarde pouvant être appliqués s'affiche.
4. [Pour appliquer un plan existant] Sélectionnez le plan, puis cliquez sur **Appliquer**.
5. [Pour créer un nouveau plan] Cliquez sur **Création d'un plan**, sélectionnez le type de plan, puis créez le nouveau plan.

   Pour plus d'informations sur les types de plans disponibles et sur leur création, reportez-vous à "Plans pris en charge pour les groupes de terminaux" (p. 355).

Remarque
Les plans de sauvegarde appliqués aux groupes de terminaux cloud à cloud sont planifiés automatiquement pour s'exécuter une fois par jour. Vous ne pouvez pas exécuter ces plans à la demande en cliquant sur **Exécuter maintenant**.

Révocation d'un plan à partir d'un groupe

Vous pouvez révoquer un plan à partir d'un groupe en sélectionnant d'abord le groupe, puis en en révoquant le plan.

Vous pouvez également ouvrir le plan pour le modifier, puis en supprimer le groupe.

Pour révoquer un plan à partir d'un groupe

1. Cliquez sur **Terminaux**, puis accédez au groupe depuis lequel vous souhaitez révoquer un plan.
2. [Pour les ressources autres que de cloud à cloud] Cliquez sur **Protéger un groupe**.
   La liste des plans appliqués au groupe s'affiche.
3. [Pour les ressources de cloud à cloud] Cliquez sur **Sauvegarde de groupe**.
   La liste des plans de sauvegarde appliqués au groupe s'affiche.
4. Sélectionnez le plan que vous souhaitez révoquer.
5. [Pour les ressources autres que de cloud à cloud] Cliquez sur l'icône représentant des points de suspension (...), puis cliquez sur **Révoquer**.
6. [Pour les ressources de cloud à cloud] Cliquez sur l'icône représentant un engrenage, puis cliquez sur **Révoquer**.

Utilisation du module de contrôle des terminaux

Dans le cadre des plans de protection du service Cyber Protection, le module de contrôle des terminaux[1] tire parti d'un sous-ensemble fonctionnel de l'agent de prévention des pertes de données[2] sur chaque ordinateur protégé afin de détecter et de prévenir la consultation et la transmission non autorisées de données via les canaux de l'ordinateur local. Il offre un contrôle précis d'un large éventail de voies de fuites de données, y compris l'échange de données à l'aide de supports amovibles, d'imprimantes, de terminaux virtuels et redirigés, et du presse-papiers Windows.

Ce module est disponible pour les éditions Cyber Protect Essentials, Cyber Protect Standard et Cyber Protect Advanced, sous licence en fonction de la ressource.

---

[1]Dans le cadre d'un plan de protection, le module de contrôle des terminaux tire parti d'un sous-ensemble fonctionnel de l'agent de prévention des pertes de données sur chaque ordinateur protégé afin de détecter et de prévenir la consultation et la transmission non autorisées de données via les canaux de l'ordinateur local. Cela comprend l'accès de l'utilisateur aux ports et périphériques, l'impression de documents, les opérations de copier-coller, le formatage des supports et les opérations d'éjection, ainsi que les synchronisations aux terminaux mobiles connectés localement. Le module de contrôle des terminaux offre un contrôle granulaire et contextuel sur les types de terminaux et de ports auxquels les utilisateurs peuvent accéder sur l'ordinateur protégé, ainsi que les actions que ces utilisateurs peuvent réaliser sur ces terminaux.

[2]Un composant client du système de prévention des pertes de données qui protège son ordinateur hôte contre l'utilisation, la transmission et le stockage non autorisés de données confidentielles, protégées ou sensibles en appliquant une combinaison de techniques d'analyse de contexte et de contenu et en mettant en œuvre des politiques de prévention des pertes de données gérées de manière centralisée. Cyber Protection propose un agent de prévention des pertes de données complet. Toutefois, la fonctionnalité de l'agent sur un ordinateur protégé est limitée à l'ensemble de fonctionnalités de prévention des pertes de données disponibles sous licence dans Cyber Protection, et dépend du plan de protection appliqué à cet ordinateur.

Remarque
Sur les ordinateurs Windows, les fonctionnalités de contrôle des terminaux nécessitent l'installation de l'agent de prévention des pertes de données. Celui-ci sera installé automatiquement pour les ressources protégées si le module **Contrôle des terminaux** est activé dans leurs plans de protection.

Le module de contrôle des terminaux s'appuie sur les fonctions de prévention des pertes de données[1] de l'agent afin d'imposer un contrôle contextuel de l'accès aux données et des opérations de transfert sur l'ordinateur protégé. Cela comprend l'accès de l'utilisateur aux ports et périphériques, l'impression de documents, les opérations de copier-coller, le formatage des supports et les opérations d'éjection, ainsi que les synchronisations aux terminaux mobiles connectés localement. L'agent de prévention des pertes de données comprend un framework pour tous les composants centraux de gestion et d'administration du module de contrôle des terminaux, et doit donc être installé sur chaque ordinateur à protéger avec le module de contrôle des terminaux. L'agent autorise, restreint ou refuse les actions des utilisateurs en fonction des paramètres de contrôle des terminaux qu'il reçoit de la part du plan de protection appliqué à l'ordinateur protégé.

Le module de contrôle des terminaux contrôle l'accès à différents périphériques, qu'ils soient utilisés directement sur des ordinateurs protégés ou redirigés dans des environnements de virtualisation hébergés sur des ordinateurs protégés. Il reconnaît les terminaux redirigés dans Microsoft Remote Desktop Server, Citrix XenDesktop/XenApp/XenServer et VMware Horizon. Il peut également contrôler les opérations de copies de données entre le presse-papiers du système d'exploitation invité exécuté sur VMware Workstation/Player, Oracle VM VirtualBox ou Windows Virtual PC, et le presse-papiers du système d'exploitation hôte exécuté sur l'ordinateur protégé.

Le module de contrôle des terminaux peut protéger les ordinateurs exécutant les systèmes d'exploitation suivants :

Contrôle des terminaux

- Microsoft Windows 7 Service Pack 1 et versions ultérieures
- Microsoft Windows Server 2008 R2 et versions ultérieures
- macOS 10.15 (Catalina)
- macOS 11.2.3 (Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)

[1]Un système de technologies intégrées et de mesures organisationnelles destinées à détecter et à prévenir la divulgation/consultation accidentelle ou intentionnelle de données confidentielles, protégées ou sensibles par des entités non autorisées, au sein ou en dehors de l'organisation, ou le transfert de telles données vers des environnements non dignes de confiance.

Remarque
Agent for Data Loss Prevention pour macOS ne prend en charge que les processeurs x64. Les processeurs Apple Silicon ARM ne sont pas supportés.

Prévention des pertes de données

- Microsoft Windows 7 Service Pack 1 et versions ultérieures
- Microsoft Windows Server 2008 R2 et versions ultérieures

Remarque
Agent for Data Loss Prevention peut être installé sur des systèmes macOS non pris en charge, car il fait partie intégrante d'Agent for Mac. Dans ce cas, la console Cyber Protect indiquera que Agent for Data Loss Prevention est installé sur l'ordinateur, mais les fonctionnalités de contrôle des terminaux et de prévention des pertes de données ne fonctionneront pas. La fonctionnalité de contrôle des terminaux ne fonctionnera que sur les systèmes macOS supporté par Agent for Data Loss Prevention.

Limitation de l'utilisation de l'agent de prévention des pertes de données avec Hyper-V

N'installez pas l'agent de prévention des pertes de données sur des hôtes Hyper-V dans des clusters Hyper-V, car cela est susceptible d'entraîner des problèmes d'écran bleu de la mort (BSOD), principalement dans les clusters Hyper-V avec des volumes partagés de cluster (CSV).

Si vous utilisez l'une des versions suivantes de l'agent pour Hyper-V, vous devez supprimer manuellement l'agent de prévention des pertes de données :

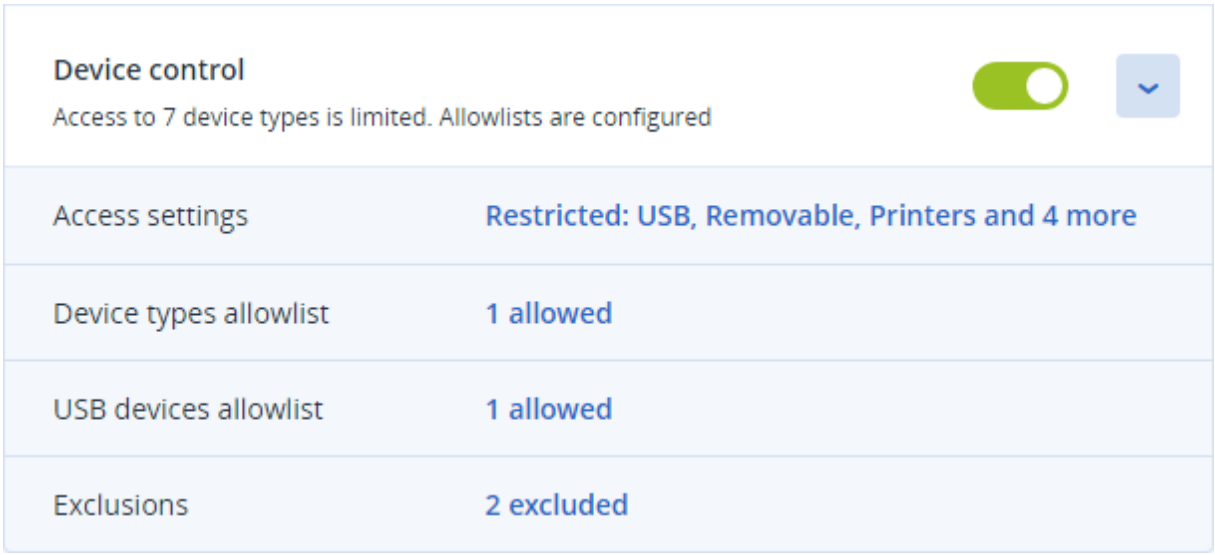
- 15.0.26473 (C21.02)
- 15.0.26570 (C21.02 HF1)
- 15.0.26653 (C21.03)
- 15.0.26692 (C21.03 HF1)
- 15.0.26822 (C21.04)

Pour supprimer l'agent de prévention des pertes de données, sur l'hôte Hyper-V, exécutez manuellement le programme d'installation et désélectionnez la case Agent pour empêcher les pertes de données, ou exécutez la commande suivante :

```
<installer_name> --remove-components=agentForDlp -quiet
```

Vous pouvez activer et configurer le module de contrôle des terminaux dans la section **Contrôle des terminaux** de votre plan de protection dans la console Cyber Protect. Pour obtenir des instructions, consultez les étapes pour activer ou désactiver le contrôle des terminaux.

La section **Contrôle des terminaux** affiche un résumé de la configuration du module :



- Paramètres d'accès : affiche un résumé des types de terminaux et des ports avec accès restreint (refusé ou en lecture seule), le cas échéant. Sinon, indique que tous les types de terminaux sont autorisés. Cliquez sur ce résumé pour consulter ou modifier les paramètres d'accès (consultez les étapes pour consulter ou modifier les paramètres d'accès).
- Liste d'autorisation des types de terminaux : affiche le nombre de sous-classes de terminaux autorisées en étant exclues du contrôle d'accès des terminaux, le cas échéant. Sinon, indique que la liste d'autorisation est vide. Cliquez sur ce résumé pour consulter ou modifier la sélection de sous-classes de terminaux autorisées (consultez les étapes pour exclure des sous-classes de terminaux du contrôle d'accès).
- Liste d'autorisation des terminaux USB : affiche le nombre de modèles/terminaux USB autorisés en étant exclus du contrôle d'accès des terminaux, le cas échéant. Sinon, indique que la liste d'autorisation est vide. Cliquez sur ce résumé pour consulter ou modifier la liste de modèles/terminaux USB (consultez les étapes pour exclure des terminaux USB individuels du contrôle d'accès).
- Exclusions : affiche le nombre d'exclusions de contrôle d'accès qui ont été définies pour le presse-papiers Windows, les captures d'écran, les imprimantes et les terminaux mobiles.

Utilisation du contrôle des terminaux

Cette section donne des instructions pas à pas pour effectuer des tâches de base lors de l'utilisation du module de contrôle des terminaux.

Activer ou désactiver le contrôle des terminaux

Vous pouvez activer le contrôle des terminaux lors de la création d'un plan de protection. Vous pouvez modifier un plan de protection existant afin d'activer ou de désactiver le contrôle des terminaux.

Pour activer ou désactiver le contrôle des terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Effectuez l'une des actions suivantes pour ouvrir le panneau du plan de protection :
   - Si vous souhaitez créer un plan de protection, sélectionnez un ordinateur à protéger, cliquez sur **Protection**, puis sur **Création d'un plan**.
   - Si vous souhaitez modifier un plan de protection existant, sélectionnez une machine protégée, cliquez sur **Protection**, sur les points de suspension (...) à côté du nom du plan de protection, puis sur **Modifier**.
3. Dans le panneau du plan de protection, accédez à la zone **Contrôle des terminaux**, et activez ou désactivez **Contrôle des terminaux**.
4. Effectuez l'une des actions suivantes pour appliquer vos modifications :
   - Si vous créez un plan de protection, cliquez sur **Créer**.
   - Si vous modifiez un plan de protection, cliquez sur **Enregistrer**.

Vous pouvez également accéder au panneau du plan de protection depuis l'onglet Gestion. Toutefois, cette fonctionnalité n'est pas disponible dans toutes les éditions du service Cyber Protection.

Activer l'utilisation du module de contrôle de terminaux sur macOS

Les paramètres de contrôle de terminaux d'un plan de protection ne deviennent effectifs qu'une fois le lecteur de contrôle de terminaux chargé sur la ressource protégée. Cette section décrit comment charger le lecteur de contrôle de terminaux pour permettre l'utilisation du module de contrôle de terminaux sur macOS. Cette opération ne doit être effectuée qu'une seule fois, mais requiert les privilèges administrateur sur l'ordinateur de terminal.

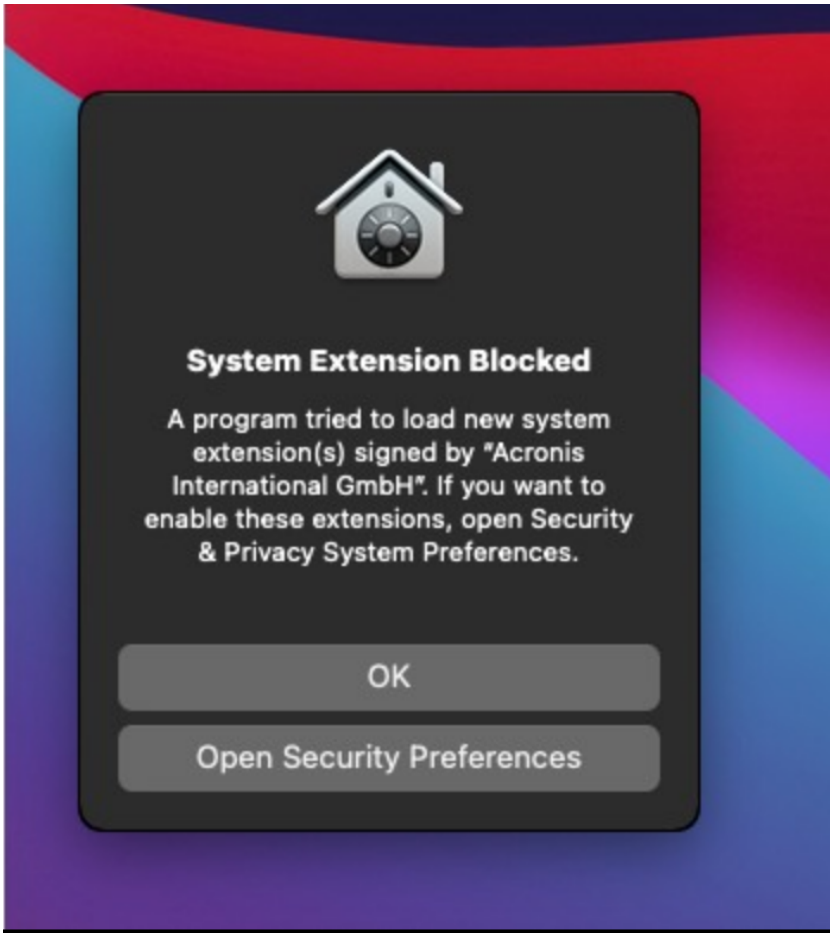
Versions de macOS prises en charge :

- macOS 10.15 (Catalina) et versions ultérieures
- macOS 11.2.3 (Big Sur) et versions ultérieures
- macOS 12.2 (Monterey) et versions ultérieures
- macOS 13.2 (Ventura) et versions ultérieures

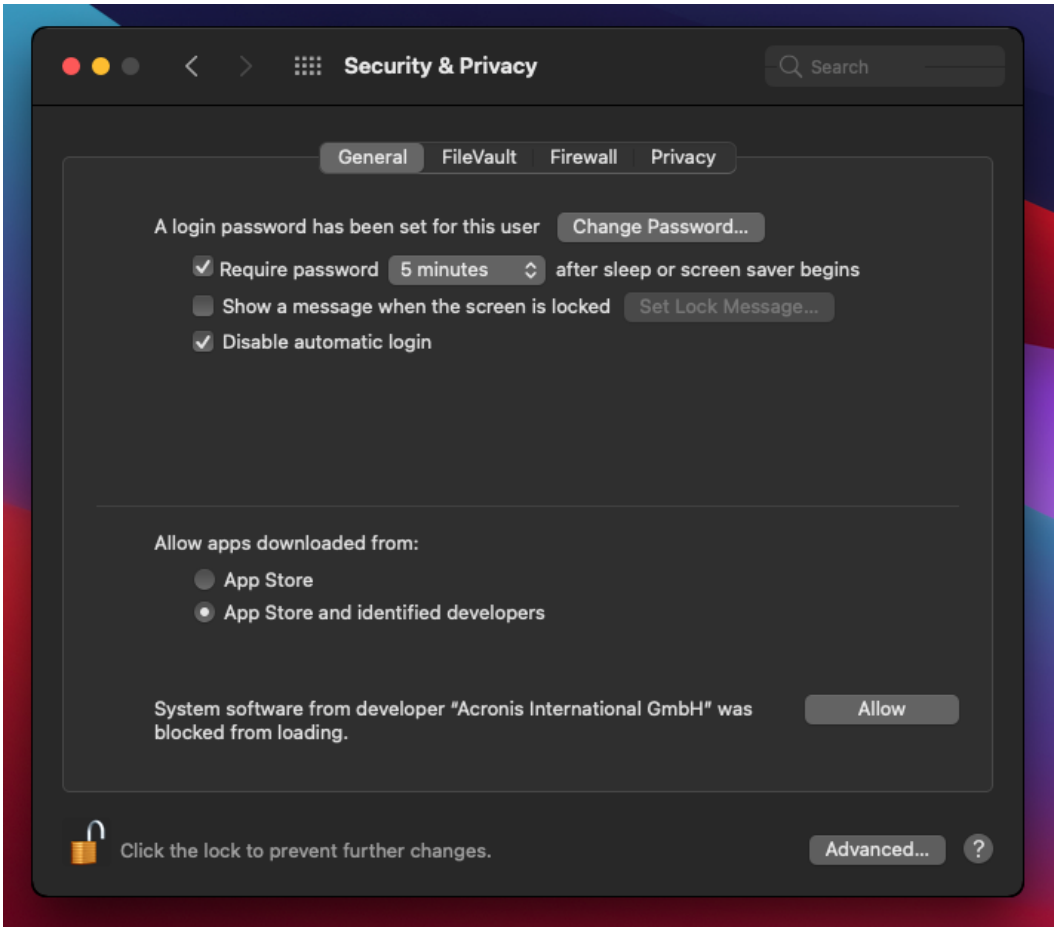
Pour activer l'utilisation du module de contrôle de terminaux sur macOS

1. Installez l'agent pour Mac sur l'ordinateur que vous voulez protéger.
2. Dans le plan de protection, activez les paramètres de contrôle de terminaux.
3. Appliquez le plan de protection.

4. L'avertissement « Extension système bloquée » apparaît sur la ressource protégée. Cliquez sur **Ouvrir les préférences de sécurité**.



5. Dans le volet **Sécurité et confidentialité** qui s'affiche, sélectionnez **App Store et développeurs identifiés**, puis cliquez sur **Autoriser**.



6. Dans la boîte de dialogue qui apparaît, cliquez sur **Redémarrer** pour redémarrer la ressource et activer les paramètres de contrôle de terminaux.

Remarque
Si les paramètres sont désactivés par la suite, vous n'aurez pas à répéter ces étapes pour les réactiver.

Consulter ou modifier les paramètres d'accès

Dans le panneau du plan de protection, vous pouvez gérer les paramètres d'accès pour le module de contrôle des terminaux. Vous pouvez ainsi autoriser ou refuser l'accès à certains types de terminaux, ainsi qu'activer ou désactiver les notifications et les alertes.

Pour consulter ou modifier les paramètres d'accès

1. Ouvrez le panneau du plan de protection pour un plan de protection et activez le contrôle des terminaux dans ce plan (consultez les étapes pour activer ou désactiver le contrôle des terminaux).
2. Cliquez sur l'icône de flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur le lien à côté de **Paramètres d'accès**.

3. Sur la page de gestion des paramètres d'accès qui apparaît, consultez ou modifiez les paramètres d'accès comme vous le souhaitez.

Remarque
Les paramètres d'accès configurés dans le contrôle du terminal peuvent être remplacés lors de l'utilisation du contrôle du terminal et d'Advanced DLP pour protéger une ressource. Voir "Activation d'Advanced Data Loss Prevention dans les plans de protection" (p. 924).

Activer ou désactiver les notifications du système d'exploitation et les alertes de service

Lorsque vous gérez les paramètres d'accès, vous pouvez activer ou désactiver les notifications du système d'exploitation et les alertes de service, informant l'utilisateur des tentatives d'exécution d'actions non autorisées.

Pour activer ou désactiver les notifications du système d'exploitation

1. Suivez les étapes pour consulter ou modifier les paramètres d'accès.
2. Sur la page de gestion des paramètres d'accès, sélectionnez ou désélectionnez la case **Affichez des notifications du système d'exploitation aux utilisateurs finaux s'ils essaient d'utiliser un type de terminal ou de port bloqué**.

Pour activer ou désactiver les alertes de service

1. Suivez les étapes pour consulter ou modifier les paramètres d'accès.
2. Sur la page de gestion des paramètres d'accès, sélectionnez ou désélectionnez la case **Afficher une alerte** pour le ou les types de terminaux souhaités.

La case **Afficher une alerte** est disponible uniquement pour les types de terminaux avec accès restreint (Lecture seule ou Accès refusé), à l'exception des captures d'écran.

Exclure des sous-classes de terminaux du contrôle d'accès

Dans le panneau du plan de protection, vous pouvez choisir les sous-classes de terminaux à exclure du contrôle d'accès. Par conséquent, l'accès à ces terminaux est autorisé, quels que soient les paramètres d'accès du contrôle des terminaux.

Pour exclure des sous-classes de terminaux du contrôle d'accès

1. Ouvrez le panneau du plan de protection pour un plan de protection et activez le contrôle des terminaux dans ce plan (consultez les étapes pour activer ou désactiver le contrôle des terminaux).
2. Cliquez sur l'icône de flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur le lien à côté de **Liste d'autorisation des types de terminaux**.
3. Sur la page de gestion de la liste d'autorisation qui apparaît, consultez ou modifiez la sélection de sous-classes de terminaux à exclure du contrôle d'accès.

Exclure des terminaux USB particuliers du contrôle d'accès

Dans le panneau du plan de protection, vous pouvez spécifier des terminaux ou des modèles de terminaux USB à exclure du contrôle d'accès des terminaux. Par conséquent, l'accès à ces terminaux est autorisé, quels que soient les paramètres d'accès du contrôle des terminaux.

Pour exclure un terminal USB du contrôle d'accès

1. Ouvrez le panneau du plan de protection pour un plan de protection et activez le contrôle des terminaux dans ce plan (consultez les étapes pour activer ou désactiver le contrôle des terminaux).
2. Cliquez sur l'icône de flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur le lien à côté de **Liste d'autorisation des terminaux USB**.
3. Sur la page de gestion de la liste d'autorisation qui apparaît, cliquez sur **Ajouter depuis la base de données**.
4. Sur la page de sélection des terminaux USB qui apparaît, sélectionnez le ou les terminaux souhaités parmi ceux enregistrés dans la base de données des terminaux USB.
5. Cliquez sur le bouton **Ajouter à la liste d'autorisation**.

Pour arrêter d'exclure un terminal USB du contrôle d'accès

1. Ouvrez le panneau du plan de protection pour un plan de protection et activez le contrôle des terminaux dans ce plan (consultez les étapes pour activer ou désactiver le contrôle des terminaux).
2. Cliquez sur l'icône de flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur le lien à côté de **Liste d'autorisation des terminaux USB**.
3. Sur la page de gestion de la liste d'autorisation qui apparaît, cliquez sur l'icône de suppression à la fin de l'élément de liste représentant le terminal souhaité.

Ajouter ou supprimer le terminal USB de la base de données

Pour exclure un terminal USB en particulier du contrôle d'accès, vous devez l'ajouter à la base de données des terminaux USB. Vous pouvez ensuite ajouter des terminaux à la liste d'autorisation en les sélectionnant depuis cette base de données.

Les procédures suivantes s'appliquent aux plans de protection pour lesquels la fonctionnalité de contrôle des terminaux est activée.

Pour ajouter des terminaux USB à la base de données

1. Ouvrir le plan de protection d'un terminal pour le modifier :

   Cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan de protection, puis sélectionnez **Modifier**.

Remarque
Le contrôle des terminaux doit être activé dans le plan, afin que vous puissiez accéder aux paramètres de contrôle des terminaux.

2. Cliquez sur l'icône de flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur le lien à côté de **Liste d'autorisation des terminaux USB**.
3. Sur la page de **liste d'autorisation des terminaux USB** qui apparaît, cliquez sur **Ajouter depuis la base de données**.
4. Sur la page de gestion de la base de données des terminaux USB qui apparaît, cliquez sur **Ajouter à la base de données**.
5. Dans la boîte de dialogue **Ajouter un terminal USB** qui apparaît, cliquez sur l'ordinateur auquel le terminal USB est connecté.
   Seuls les ordinateurs en ligne s'affichent dans la liste des ordinateurs.
   La liste des terminaux USB s'affiche uniquement pour les ordinateurs sur lesquels l'agent Prévention des pertes de données est installé.
   Les terminaux USB sont répertoriés sous la forme d'une arborescence. Le premier niveau de l'arborescence représente un modèle de terminal. Le deuxième niveau représente un terminal spécifique de ce modèle.
   Une icône bleue à côté de la description du terminal indique que le terminal est actuellement connecté à l'ordinateur. Si le terminal n'est pas connecté à l'ordinateur, l'icône est grisée.
6. Cochez les cases correspondant aux terminaux USB que vous voulez ajouter à la base de données, puis cliquez sur **Ajouter à la base de données**.
   Les terminaux USB sélectionnés sont ajoutés à la base de données.
7. Fermez ou enregistrez le plan de protection.

Pour ajouter des terminaux USB à la base de données depuis le panneau de détails de l'ordinateur

Remarque
Cette procédure s'applique uniquement aux terminaux qui sont en ligne et sur lesquels l'agent Prévention des pertes de données est installé. Vous ne pouvez pas consulter la liste des terminaux USB d'un ordinateur hors ligne ou sur lequel l'agent Prévention des pertes de données n'est pas installé.

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez un ordinateur auquel le terminal USB souhaité a déjà été connecté et, dans le menu de droite, cliquez sur **Inventaire**.
   Le panneau de détails de l'ordinateur s'ouvre.
3. Dans le panneau de détails de l'ordinateur, cliquez sur l'onglet **Terminaux USB**.
   La liste des terminaux USB connus sur l'ordinateur sélectionné s'affiche.

Les terminaux USB sont répertoriés sous la forme d'une arborescence. Le premier niveau de l'arborescence représente un modèle de terminal. Le deuxième niveau représente un terminal spécifique de ce modèle.

Une icône bleue à côté de la description du terminal indique que le terminal est actuellement connecté à l'ordinateur. Si le terminal n'est pas connecté à l'ordinateur, l'icône est grisée.

4. Cochez les cases correspondant aux terminaux USB que vous voulez ajouter à la base de données, puis cliquez sur **Ajouter à la base de données**.

Pour ajouter des terminaux USB à la base de données depuis des alertes de service

1. Dans la console Cyber Protect, accédez à **Surveillance** > **Alertes**.
2. Trouvez une alerte de contrôle de terminal qui vous informe de l'accès refusé au terminal USB.
3. Dans la vue d'alerte simple, cliquez sur **Autoriser ce terminal USB**.
   Cela exclut le terminal USB du contrôle d'accès et l'ajoute à la base de données pour référence ultérieure.

Pour ajouter des terminaux USB en important une liste de terminaux dans la base de données

Vous pouvez importer un fichier JSON contenant une liste de terminaux USB à ajouter à la base de données. Consultez "Importer une liste de terminaux USB dans la base de données" (p. 401).

Pour supprimer des terminaux USB de la base de données

1. Ouvrir le plan de protection d'un terminal pour le modifier :
   Cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan de protection, puis sélectionnez **Modifier**.

   Remarque
   Le contrôle des terminaux doit être activé dans le plan, afin que vous puissiez accéder aux paramètres de contrôle des terminaux.

2. Cliquez sur la flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur la ligne **Liste d'autorisation des terminaux USB**.
3. Sur la page de gestion de la liste d'autorisation qui apparaît, cliquez sur **Ajouter depuis la base de données**.
4. Sur la page de sélection de terminaux USB depuis la base de données, cliquez sur les points de suspension (...) situés à la fin de l'élément de liste représentant le terminal, cliquez sur **Supprimer**, puis confirmez la suppression.
   Les terminaux USB sont supprimés de la base de données.
5. Fermez ou enregistrez le plan de protection.

Afficher les alertes de contrôle des terminaux

Le module de contrôle des terminaux peut être configuré pour émettre des alertes qui vous informent des tentatives refusées d'utilisation de certains types de terminaux par l'utilisateur (voir

Activer ou désactiver les notifications du système d'exploitation et les alertes de service). Procédez comme suit pour afficher ces alertes.

Pour afficher les alertes de contrôle des terminaux

1. Dans la console Cyber Protect, accédez à **Surveillance** > **Alertes**.
2. Recherchez des alertes ayant le statut suivant : « L'accès au périphérique est bloqué ».

Consultez Alertes de contrôle des terminaux pour en savoir plus.

Paramètres d'accès

Sur la page des **paramètres d'accès**, vous pouvez autoriser ou refuser l'accès à certains types de terminaux, ainsi qu'activer ou désactiver les notifications du système d'exploitation et les alertes de contrôle des terminaux.

Remarque
Les paramètres d'accès configurés dans le contrôle du terminal peuvent être remplacés lors de l'utilisation du contrôle du terminal et d'Advanced DLP pour protéger une ressource. Voir "Activation d'Advanced Data Loss Prevention dans les plans de protection" (p. 924).

Les paramètres d'accès vous permettent de limiter l'accès des utilisateurs aux ports et types de terminaux suivants :

- **Amovible** (contrôle d'accès par type de terminal) : terminaux possédant une interface permettant de se connecter à un ordinateur (USB, FireWire, PCMCIA, IDE, SATA, SCSI, etc.) et reconnus par le système d'exploitation comme étant des périphériques de stockage amovibles (par exemple, clés USB, lecteurs de carte, lecteurs magnéto-optiques, etc.). Le contrôle des terminaux classifie tous les disques durs connectés via USB, FireWire et PCMCIA en tant que terminaux amovibles. Il classifie également certains disques durs (généralement SATA et SCSI) en tant que terminaux amovibles s'ils prennent en charge la fonction de branchement à chaud et que le système d'exploitation en cours d'exécution n'est pas installé sur eux.

  Vous pouvez autoriser l'accès complet ou l'accès en lecture seule aux terminaux amovibles, ou en refuser l'accès pour contrôler les opérations de copie de données vers et depuis tout terminal amovible sur un ordinateur protégé. Les droits d'accès n'affectent pas les terminaux chiffrés avec BitLocker ou FileVault (uniquement avec le système de fichiers HFS+).

  Ce type de terminaux est pris en charge à la fois sur Windows et macOS.
- **Amovible chiffré** (contrôle d'accès par type de terminal) : terminaux amovibles chiffrés avec le chiffrement de lecteur BitLocker (sur Windows) ou FileVault (sur macOS).

  Sur macOS, seuls les lecteurs amovibles chiffrés lecteur utilisant le système de fichiers HFS+ (également nommé HFS Plus ou Mac OS Extended, ou encore HFS Extended) sont pris en charge. Les lecteurs amovibles chiffrés utilisant le système de fichiers APFS sont traités comme des lecteurs amovibles.

  Vous pouvez autoriser l'accès complet ou l'accès en lecture seule aux terminaux amovibles chiffrés, ou en refuser l'accès pour contrôler les opérations de copie de données vers et depuis

tout terminal amovible chiffré sur un ordinateur protégé. Les droits d'accès affectent uniquement les terminaux chiffrés avec BitLocker ou FileVault (uniquement avec le système de fichiers HFS+).

Ce type de terminaux est pris en charge à la fois sur Windows et macOS.

- **Imprimantes** (contrôle d'accès par type de terminal) : imprimantes physiques avec une interface de connexion à un ordinateur, quelle qu'elle soit (USB, LPT, Bluetooth, etc.), ainsi que toutes les imprimantes auxquelles un ordinateur sur le réseau peut accéder.

  Vous pouvez autoriser ou refuser l'accès aux imprimantes afin de contrôler l'impression de documents sur n'importe quelle imprimante sur un ordinateur protégé.

  Remarque
  Lorsque vous définissez le paramètre d'accès aux imprimantes sur **Refuser**, les applications et processus qui accèdent aux imprimantes doivent être redémarrés pour appliquer les paramètres d'accès nouvellement configurés. Pour vous assurer que les paramètres d'accès sont correctement appliqués, redémarrez les ressources protégées.

  Ce type de terminaux est pris en charge sur Windows uniquement.
- **Presse-papiers** (contrôle d'accès par type de terminal) : presse-papiers Windows.

  Vous pouvez autoriser l'accès ou refuser l'accès au presse-papiers pour contrôler les opérations de copier-coller via le presse-papiers Windows sur un ordinateur protégé.

  Remarque
  Lorsque vous définissez le paramètre d'accès au presse-papiers sur **Refuser**, les applications et processus qui accèdent au presse-papiers doivent être redémarrés pour appliquer les paramètres d'accès nouvellement configurés. Pour vous assurer que les paramètres d'accès sont correctement appliqués, redémarrez les ressources protégées.

  Ce type de terminaux est pris en charge sur Windows uniquement.
- **Capture d'écran** (contrôle d'accès par type de terminal) : permet la capture d'écran de l'écran complet, de la fenêtre active ou d'une partie sélectionnée de l'écran.

  Vous pouvez autoriser ou refuser l'accès aux captures d'écran afin de contrôler la capture d'écran sur un ordinateur protégé.

  Remarque
  Lorsque vous définissez le paramètre d'accès aux captures d'écran sur **Refuser**, les applications et processus qui accèdent à la capture d'écran doivent être redémarrés pour appliquer les paramètres d'accès nouvellement configurés. Pour vous assurer que les paramètres d'accès sont correctement appliqués, redémarrez les ressources protégées.

  Ce type de terminaux est pris en charge sur Windows uniquement.
- **Terminaux mobiles** (contrôle d'accès par type de terminal) : terminaux (ex. : smartphones Android, etc.) qui communiquent avec un ordinateur via le protocole MTP (Media Transfer Protocol), avec n'importe quelle interface utilisée pour se connecter à un ordinateur (USB, IP, Bluetooth).

Vous pouvez autoriser l'accès complet ou l'accès en lecture seule aux terminaux mobiles, ou en refuser l'accès pour contrôler les opérations de copie de données vers et depuis tout terminal mobile sur un ordinateur protégé.

Remarque
Lorsque vous définissez le paramètre d'accès aux terminaux mobiles sur **Lecture seule** ou **Refuser**, les applications et processus qui accèdent aux terminaux mobiles doivent être redémarrés pour appliquer les paramètres d'accès nouvellement configurés. Pour vous assurer que les paramètres d'accès sont correctement appliqués, redémarrez les ressources protégées.

Ce type de terminaux est pris en charge sur Windows uniquement.

- **Bluetooth** (contrôle d'accès par type de terminal) : terminaux Bluetooth internes ou externes disposant d'une interface de connexion à un ordinateur, quelle qu'elle soit (USB, PCMCIA, etc.). Ce paramètre contrôle l'utilisation des terminaux de ce type, plutôt que l'échange de données à l'aide de tels terminaux.

  Vous pouvez autoriser ou refuser l'accès au Bluetooth afin de contrôler le Bluetooth sur un ordinateur protégé.

  Remarque
  Sur macOS, les droits d'accès pour le Bluetooth n'affectent pas les terminaux Bluetooth HID. L'accès de ces terminaux est toujours autorisé pour éviter que les terminaux HID sans fil (souris et claviers) ne soient désactivés sur le matériel iMac et Mac Pro.

  Ce type de terminaux est pris en charge à la fois sur Windows et macOS.
- **Lecteurs optiques** (contrôle d'accès par type de terminal) : lecteurs CD/DVD/BD internes ou externes (y compris graveurs) disposant d'une interface de connexion à un ordinateur, quelle qu'elle soit (IDE, SATA, USB, FireWire, PCMCIA, etc.).

  Vous pouvez autoriser l'accès complet ou l'accès en lecture seule aux lecteurs optiques, ou en refuser l'accès pour contrôler les opérations de copie de données vers et depuis tout lecteur optique sur un ordinateur protégé.

  Ce type de terminaux est pris en charge à la fois sur Windows et macOS.
- **Disquettes** (contrôle d'accès par type de terminal) : lecteurs de disquettes internes ou externes disposant d'une interface de connexion à un ordinateur, quelle qu'elle soit (IDE, USB, PCMCIA, etc.). Certains modèles de lecteurs de disquettes sont reconnus par le système d'exploitation comme des lecteurs amovibles. Dans ce cas, le module de contrôle des terminaux identifie également ces lecteurs comme étant des terminaux amovibles.

  Vous pouvez autoriser l'accès complet ou l'accès en lecture seule aux lecteurs de disquettes, ou en refuser l'accès pour contrôler les opérations de copie de données vers et depuis tout lecteur de disquettes sur un ordinateur protégé.

  Ce type de terminaux est pris en charge sur Windows uniquement.
- **USB** (contrôle d'accès par interface de terminal) : tout terminal connecté à un port USB, à l'exception des concentrateurs.

Vous pouvez autoriser l'accès complet ou l'accès en lecture seule aux ports USB, ou en refuser l'accès pour contrôler les opérations de copie de données vers et depuis tout port USB sur un ordinateur protégé.

Ce type de terminaux est pris en charge à la fois sur Windows et macOS.

- **FireWire** (contrôle d'accès par interface de terminal) : tout terminal connecté à un port FireWire (IEEE 1394), à l'exception des concentrateurs.

  Vous pouvez autoriser l'accès complet ou l'accès en lecture seule aux ports FireWire, ou en refuser l'accès pour contrôler les opérations de copie de données vers et depuis tout port FireWire sur un ordinateur protégé.

  Ce type de terminaux est pris en charge à la fois sur Windows et macOS.
- **Terminaux redirigés** (contrôle d'accès par interface de terminal) : lecteurs mappés (disques durs, lecteurs amovibles et lecteurs optiques), terminaux USB et presse-papiers redirigés vers des sessions d'application virtuelle ou de bureau virtuel.

  Le module de contrôle des terminaux reconnaît les terminaux redirigés via les protocoles à distance Microsoft RDP, Citrix ICA, VMware PCoIP et HTML5/WebSockets dans les environnements de virtualisation Microsoft RDS, Citrix XenDesktop, Citrix XenApp, Citrix XenServer et VMware Horizon hébergés sur des ordinateurs Windows protégés. Il peut également contrôler les opérations de copies de données entre le presse-papiers Windows du système d'exploitation invité exécuté sur VMware Workstation, VMware Player, Oracle VM VirtualBox ou Windows Virtual PC, et le presse-papiers du système d'exploitation hôte exécuté sur l'ordinateur Windows protégé.

  Ce type de terminaux est pris en charge sur Windows uniquement.

  Vous pouvez configurer l'accès aux terminaux redirigés comme suit :

  - **Lecteurs mappés** : autorisez l'accès complet ou l'accès en lecture seule, ou refusez l'accès afin de contrôler les opérations de copie de données vers et depuis tout disque dur, lecteur amovible ou lecteur optique redirigé vers la session hébergée sur un ordinateur protégé.
  - **Presse-papiers entrant** : autorisez ou refusez l'accès pour contrôler les opérations de copie de données via le presse-papiers vers la session hébergée sur un ordinateur protégé.

    Remarque
    Lorsque vous définissez le paramètre d'accès au presse-papiers entrant sur **Refuser**, les applications et processus qui accèdent au presse-papiers doivent être redémarrés pour appliquer les paramètres d'accès nouvellement configurés. Pour vous assurer que les paramètres d'accès sont correctement appliqués, redémarrez les ressources protégées.

  - **Presse-papiers sortant** : autorisez ou refusez l'accès pour contrôler les opérations de copie de données via le presse-papiers depuis la session hébergée sur un ordinateur protégé.

    Remarque
    Lorsque vous définissez le paramètre d'accès au presse-papiers sortant sur **Refuser**, les applications et processus qui accèdent au presse-papiers doivent être redémarrés pour appliquer les paramètres d'accès nouvellement configurés. Pour vous assurer que les paramètres d'accès sont correctement appliqués, redémarrez les ressources protégées.

- **Ports USB** : autorisez ou refusez l'accès pour contrôler les opérations de copie des données vers et depuis les terminaux connectés à n'importe quel port USB redirigé vers la session hébergée sur un ordinateur protégé.

Les paramètres de contrôle des terminaux affectent tous les utilisateurs de la même manière. Par exemple, si vous refusez l'accès à des terminaux amovibles, vous empêchez tout utilisateur de copier des données depuis et à partir de ces terminaux sur un ordinateur protégé. Il est possible d'autoriser l'accès à des terminaux USB particuliers en les excluant du contrôle d'accès (voir Liste d'autorisation des types de terminaux et Liste d'autorisation des terminaux USB).

Lorsque l'accès à un terminal est contrôlé à la fois par son type et par son interface, le refus de l'accès au niveau interface a priorité. Par exemple, si l'accès aux ports USB est refusé (interface de terminal), l'accès aux terminaux mobiles connectés à un port USB est refusé, que l'accès aux terminaux mobiles soit autorisé ou non (type de terminal). Pour autoriser l'accès à un tel terminal, vous devez autoriser à la fois son interface et son type.

Remarque
Si le plan de protection utilisé sur macOS inclut des paramètres pour les types de terminaux qui sont uniquement pris en charge par Windows, alors ces paramètres sont ignorés pour macOS.

Important
Lorsqu'un terminal amovible, un terminal amovible chiffré, une imprimante ou un terminal Bluetooth est connecté à un port USB, l'autorisation de l'accès à ce terminal outrepasse le refus d'accès défini au niveau de l'interface USB. Si vous autorisez un tel type de terminal, l'accès à ce terminal est autorisé, que l'accès au port USB soit refusé ou non.

Notifications du système d'exploitation et alertes de service

Vous pouvez configurer le contrôle des terminaux afin qu'il affiche des notifications du système d'exploitation aux utilisateurs finaux s'ils essaient d'utiliser un type de terminal ou de port bloqué sur des ordinateurs protégés. Lorsque la case **Affichez des notifications du système d'exploitation aux utilisateurs finaux s'ils essaient d'utiliser un type de terminal ou de port bloqué** est cochée dans les paramètres d'accès, l'agent affiche un message contextuel dans la zone de notifications de l'ordinateur protégé si l'un des événements suivants se produit :

- Tentative refusée d'utilisation d'un terminal sur un port USB ou FireWire. Cette notification apparaît chaque fois qu'un utilisateur branche un terminal USB ou FireWire refusé au niveau de l'interface (par exemple, lors du refus d'un accès au port USB) ou au niveau du type (par exemple, lors du refus de l'utilisation de terminaux amovibles).La notification informe l'utilisateur qu'il n'est pas autorisé à accéder au terminal/lecteur spécifié.
- Une tentative refusée de copie d'un objet de données (comme un fichier) depuis un certain terminal. Cette notification apparaît lors du refus d'un accès en lecture aux terminaux suivants : lecteurs de disquettes, lecteurs optiques, terminaux amovibles, terminaux amovibles chiffrés, terminaux mobiles, lecteurs mappés redirigés, et données entrantes de presse-papiers redirigées. La notification informe l'utilisateur qu'il n'est pas autorisé à récupérer l'objet de

données spécifié depuis le terminal spécifié.

La notification de lecture refusée s'affiche également lors du refus d'un accès en lecture/écriture au Bluetooth, à un port FireWire, à un port USB ou à un port USB redirigé.

- Une tentative refusée de copie d'un objet de données (comme un fichier) vers un certain terminal. Cette notification apparaît lors du refus d'un accès en écriture aux terminaux suivants : lecteur de disquettes, lecteurs optiques, terminaux amovibles, terminaux amovibles chiffrés, terminaux mobiles, presse-papiers local, captures d'écran, imprimantes, lecteurs mappés redirigés, et données sortantes de presse-papiers redirigées. La notification informe l'utilisateur qu'il n'est pas autorisé à envoyer l'objet de données spécifié vers le terminal spécifié.

Les tentatives de l'utilisateur d'accéder à des types de terminaux bloqués sur des ordinateurs protégés peut entraîner des alertes qui sont consignées dans la console Cyber Protect. Il est possible d'activer des alertes pour chaque type de terminal (à l'exception des captures d'écran) ou de port séparément en cochant la case **Afficher une alerte** dans les paramètres d'accès. Par exemple, si l'accès aux terminaux amovibles est restreint à un accès en lecture seule et que la case **Afficher une alerte** est cochée pour ce type de terminal, une alerte est consignée chaque fois qu'un utilisateur essaie de copier des données vers un terminal amovible sur un ordinateur protégé. Consultez Alertes de contrôle des terminaux pour en savoir plus.

Voir aussi les étapes pour activer ou désactiver les notifications du système d'exploitation et les alertes de service.

Liste d'autorisation des types de terminaux

Sur la page **Liste d'autorisation des types de terminaux**, vous pouvez choisir les sous-classes de terminaux à exclure du contrôle d'accès des terminaux. Par conséquent, l'accès à ces terminaux est autorisé, quels que soient les paramètres d'accès dans le module de contrôle des terminaux.

Le module de contrôle des terminaux offre la possibilité d'autoriser l'accès à des terminaux de certaines sous-classes au sein d'un type de terminal refusé. Cette option vous permet de refuser tous les terminaux d'un certain type, à l'exception de certaines sous-classes de terminaux de ce type. Cela peut être utile lorsque, par exemple, vous devez refuser l'accès à tous les ports USB, tout en autorisant l'utilisation d'un clavier et d'une souris USB.

Lors de la configuration du module de contrôle des terminaux, vous pouvez spécifier les sous-classes de terminaux à exclure du contrôle d'accès des terminaux. Lorsqu'un terminal appartient à une sous-classe exclue, l'accès à ce terminal est autorisé, que ce type de terminal ou de port soit refusé ou non. De manière sélective, vous pouvez exclure les sous-classes de terminaux suivantes du contrôle d'accès des terminaux :

- **USB HID (souris, clavier, etc.)** : lorsque cette option est sélectionnée, permet l'accès aux terminaux d'interface (souris, clavier, etc.) connectés à un port USB, même si l'accès aux ports USB est refusé. Par défaut, cette option est sélectionnée pour que le refus d'accès au port USB ne désactive pas le clavier ni la souris.
  Pris en charge à la fois sur Windows et macOS.

- **Cartes réseau USB et FireWire** : lorsque cette option est sélectionnée, permet l'accès aux cartes réseau connectées à un port USB ou FireWire (IEEE 1394), même si l'accès aux ports USB et/ou FireWire est refusé.
  Pris en charge à la fois sur Windows et macOS.
- **Scanners et périphériques d'images fixes USB** : lorsque cette option est sélectionnée, permet l'accès aux scanners et aux périphériques d'images fixes connectés à un port USB, même si l'accès aux ports USB est refusé.
  Pris en charge uniquement sur Windows.
- **Périphériques audio USB** : lorsque cette option est sélectionnée, permet l'accès aux périphériques audio, comme les casques et les microphones, connectés à un port USB, même si l'accès aux ports USB est refusé.
  Pris en charge uniquement sur Windows.
- **Appareils photo USB** : lorsque cette option est sélectionnée, permet l'accès aux webcams connectées à un port USB, même si l'accès aux ports USB est refusé.
  Pris en charge uniquement sur Windows.
- **Bluetooth HID (souris, clavier, etc.)** : lorsque cette option est sélectionnée, permet l'accès aux terminaux d'interface (souris, clavier, etc.) connectés via Bluetooth, même si l'accès au Bluetooth est refusé.
  Pris en charge uniquement sur Windows.
- **Fonction copier-coller du presse-papiers dans l'application** : lorsque cette option est sélectionnée, permet le copier-coller de données via le presse-papiers au sein de la même application, même si l'accès au presse-papiers est refusé.
  Pris en charge uniquement sur Windows.

Remarque
Les paramètres pour les sous-classes de terminaux non pris en charge sont ignorés si ces paramètres sont configurés dans le plan de protection appliqué.

Lorsque vous devez placer des terminaux sur la liste d'autorisation, considérez ce qui suit :

- Avec la liste d'autorisation de types de terminaux, vous ne pouvez autoriser qu'une sous-classe entière de terminal. Vous ne pouvez pas autoriser un modèle de terminal spécifique, tout en refusant tous les autres de la même sous-classe. Par exemple, en excluant les caméras USB du contrôle d'accès des terminaux, vous autorisez toutes les caméras USB, quels que soient leur modèle et leur fabricant. Pour découvrir comment autoriser des terminaux/modèles spécifiques, consultez Liste d'autorisation des périphériques USB.
- Les types de terminaux peuvent uniquement être sélectionnés à partir d'une liste fermée de sous-classes de terminaux. Si le terminal à autoriser appartient à une autre sous-classe, il ne peut pas être autorisé à l'aide de la liste d'autorisation des types de terminaux. Par exemple, une sous-classe « Lecteur de cartes USB » ne peut pas être ajoutée à la liste d'autorisation. Pour autoriser un lecteur de cartes USB lorsque l'accès aux ports USB est refusé, suivez les instructions dans la Liste d'autorisation des périphériques USB.

- La liste d'autorisation des types de terminaux fonctionne uniquement pour les terminaux qui utilisent des pilotes Windows standard. Le module de contrôle des terminaux ne reconnaîtra peut-être pas la sous-classe de certains terminaux USB disposant de pilotes propriétaires. Vous ne pouvez donc pas autoriser l'accès à de tels terminaux USB à l'aide de la liste d'autorisation des types de terminaux. Dans ce cas, vous pourriez autoriser l'accès par terminal/modèle (consultez Liste d'autorisation des périphériques USB).

Liste d'autorisation des périphériques USB

La liste d'autorisation est conçue pour autoriser l'utilisation de certains terminaux USB, quels que soient les autres paramètres de contrôle des terminaux. Vous pouvez ajouter des terminaux ou des modèles de terminaux donnés à la liste d'autorisation afin de désactiver le contrôle d'accès pour ces terminaux. Par exemple, si vous ajoutez un terminal mobile avec un ID unique à la liste d'autorisation, vous autorisez l'utilisation de ce terminal particulier, même si n'importe quel autre terminal USB est refusé.

Sur la page **Liste d'autorisation des terminaux USB**, vous pouvez spécifier des terminaux ou des modèles de terminaux USB à exclure du contrôle d'accès des terminaux. Par conséquent, l'accès à ces terminaux est autorisé, quels que soient les paramètres d'accès dans le module de contrôle des terminaux.

Il existe deux façons d'identifier les terminaux dans la liste d'autorisation :

- Modèle de terminal : identifie collectivement tous les terminaux d'un certain modèle. Chaque modèle de terminal est identifié par identifiant de fournisseur (VID) et identifiant de produit (PID), par exemple USB\VID_0FCE&PID_E19E.

  Cette combinaison VID/PID n'identifie pas un terminal spécifique, mais un modèle de terminal complet. En ajoutant un modèle de terminal à la liste d'autorisation, vous autorisez l'accès à n'importe quel terminal de ce modèle. De cette manière, vous pouvez par exemple autoriser l'utilisation d'un modèle particulier d'imprimante USB.
- Terminal unique : identifie un certain terminal. Chaque modèle de terminal est identifié par identifiant de fournisseur (VID), identifiant de produit (PID) et numéro de série, par exemple USB\VID_0FCE&PID_E19E\D55E7FCA.

  Tous les terminaux USB ne possèdent pas de numéro de série. Vous pouvez ajouter un terminal à la liste d'autorisation en tant que terminal unique à condition qu'un numéro de série ait été attribué à ce terminal lors de la production. Par exemple, une clé USB qui dispose d'un numéro de série unique.

Pour ajouter un terminal à la liste d'autorisation, vous devez d'abord l'ajouter à la base de données des terminaux USB. Vous pouvez ensuite ajouter des terminaux à la liste d'autorisation en les sélectionnant depuis cette base de données.

La liste d'autorisation est gérée sur une page de configuration séparée appelée **Liste d'autorisation des terminaux USB**. Chaque élément de la liste représente un terminal ou un modèle de terminal et dispose des champs suivants :

- **Description** : le système d'exploitation attribue une certaine description lors de la connexion du terminal USB. Vous pouvez modifier la description du terminal dans la base de données des terminaux USB (voir la page de gestion de la base de données USB).
- **Type de terminal :** affiche « Unique » si l'élément de liste est un terminal unique, ou « Modèle » s'il s'agit d'un modèle de terminal.
- **Lecture seule :** lorsque cette option est sélectionnée, n'autorise que la réception de données depuis le terminal. Si le terminal ne prend pas en charge l'accès en lecture, l'accès au terminal est bloqué. Désélectionnez cette case pour autoriser l'accès complet au terminal.
- **Réinitialiser** : lorsque l'option est sélectionnée, force le terminal à simuler une déconnexion/connexion lorsqu'un nouvel utilisateur se connecte. Certains terminaux USB nécessitent une réinitialisation pour fonctionner. Par conséquent, nous vous recommandons de cocher cette case pour ces terminaux (souris, clavier, etc.). Nous vous recommandons également de désélectionner cette case pour les périphériques de stockage de données (clés USB, lecteurs optiques, disques durs externes, etc.).
  Le module de contrôle des terminaux ne sera peut-être pas en mesure de réinitialiser certains terminaux USB disposant de pilotes propriétaires. Si vous ne parvenez pas à accéder à un tel périphérique, vous devez retirer le périphérique USB du port USB, puis le réinsérer.

Remarque
Le champ **Réinitialiser** est masqué par défaut. Pour l'afficher dans le tableau, cliquez sur l'icône en forme d'engrenage en haut à droite du tableau, puis cochez la case **Réinitialiser**.

Remarque
Les champs **En lecture seule** et **Réinitialiser** ne sont pas pris en charge sur macOS. Si ces champs sont configurés dans le plan de protection appliqué, ils seront ignorés.

Vous pouvez ajouter ou supprimer des terminaux/modèles de la liste d'autorisation comme suit :

- Cliquez sur **Ajouter depuis la base de données** au-dessus de la liste, puis sélectionnez le ou les terminaux souhaités parmi ceux enregistrés dans la base de données des terminaux USB. Le terminal sélectionné est ajouté à la liste, où vous pouvez configurer ses paramètres et confirmer les modifications.
- Cliquez sur **Autoriser ce terminal USB** dans une alerte informant que l'accès au terminal USB est refusé (consultez Alertes de contrôle des terminaux). Le terminal est alors ajouté à la liste d'autorisation et à la base de données des terminaux USB.
- Cliquez sur l'icône de suppression à la fin d'un élément de liste. Le terminal/modèle en question est supprimé de la liste d'autorisation.

Base de données des périphériques USB

Le module de contrôle des terminaux tient à jour une base de données des terminaux USB depuis laquelle vous pouvez ajouter des terminaux à la liste d'exclusions (voir Liste d'autorisation des terminaux USB). Un terminal USB peut être enregistré dans la base de données de l'une des manières suivantes :

- Ajoutez un terminal à la page qui apparaît lors de l'ajout d'un terminal à la liste d'exclusion (voir Page de gestion de la base de données des terminaux USB).
- Ajoutez un terminal depuis l'onglet Terminaux USB du volet Inventaire d'un ordinateur dans la console Cyber Protect (voir Liste des terminaux USB sur un ordinateur).
- Autorisez un terminal à partir d'une alerte refusant l'accès à ce dernier (voir Alertes de contrôle des terminaux).

Voir aussi les étapes pour ajouter ou supprimer des terminaux USB de la base de données.

Page de gestion de la base de données des terminaux USB

Lors de la configuration de la liste d'autorisation pour les terminaux USB, vous avez la possibilité d'ajouter un terminal depuis la base de données. Si vous choisissez cette option, une page de gestion apparaît avec une liste de terminaux. Sur cette page, vous pouvez voir la liste de tous les terminaux enregistrés dans la base de données. Vous pouvez sélectionner les terminaux à ajouter à la liste d'autorisation et effectuer les opérations suivantes :

Enregistrer un terminal dans la base de données

1. Cliquez sur **Ajouter à la base de données** en haut de la page.
2. Dans la boîte de dialogue **Ajouter un terminal USB** qui apparaît, cliquez sur l'ordinateur auquel le terminal USB est connecté.
   Seuls les ordinateurs en ligne s'affichent dans la liste des ordinateurs.
   La liste des terminaux USB s'affiche uniquement pour les ordinateurs sur lesquels l'agent Prévention des pertes de données est installé.
   Les terminaux USB sont répertoriés sous la forme d'une arborescence. Le premier niveau de l'arborescence représente un modèle de terminal. Le deuxième niveau représente un terminal spécifique de ce modèle.
   Une icône bleue à côté de la description du terminal indique que le terminal est actuellement connecté à l'ordinateur. Si le terminal n'est pas connecté à l'ordinateur, l'icône est grisée.
3. Cochez la case correspondant au terminal USB que vous voulez enregistrer, puis cliquez sur **Ajouter à la base de données**.

Modifier la description d'un terminal

1. Sur la page **Base de données des terminaux USB**, cliquez sur les points de suspension (...) situés à la fin de l'élément de liste représentant le terminal, puis cliquez sur **Modifier**.
2. Modifiez la description dans la boîte de dialogue qui apparaît.

Supprimer un terminal de la base de données

1. Cliquez sur les points de suspension (...) situés à la fin de l'élément de liste représentant le terminal.
2. Cliquez sur **Supprimer**, puis confirmez la suppression.

Pour chaque terminal, la liste sur la page fournit les informations suivantes :

- **Description** : un identifiant lisible du terminal. Vous pouvez modifier la description comme vous le souhaitez.
- **Type de terminal :** affiche « Unique » si l'élément de liste est un terminal unique, ou « Modèle » s'il s'agit d'un modèle de terminal. Un terminal unique doit disposer d'un numéro de série, ainsi que d'un identifiant de fournisseur (VID) et d'un identifiant de produit, alors qu'un modèle de terminal est identifié par une combinaison de VID et PID.
- **Identifiant du fournisseur**, **ID de produit**, **Numéro de série** : ensemble, ces valeurs constituent l'identifiant du périphérique, sous la forme USB\VID_<identifiant de fournisseur>&PID_<identifiant de produit>\<numéro de série>.
- **Compte** : indique le tenant à qui appartient ce terminal. Il s'agit du tenant qui contient le compte utilisateur qui a été utilisé pour enregistrer le terminal dans la base de données.

  Remarque
  Cette colonne est masquée par défaut. Pour l'afficher dans le tableau, cliquez sur l'icône en forme d'engrenage en haut à droite du tableau, puis sélectionnez **Compte**.

La colonne la plus à gauche permet de sélectionner les terminaux à ajouter à la liste d'autorisation : Cochez la case correspondant à chaque terminal à ajouter, puis cliquez sur le bouton **Ajouter à la liste d'autorisation**. Pour sélectionner ou désélectionner toutes les cases, cliquez sur la case à cocher située dans l'en-tête de colonne.

Vous pouvez effectuer une recherche dans la liste des terminaux ou y appliquer des filtres :

- Cliquez sur **Rechercher** en haut de la page, puis entrez une chaîne à rechercher. La liste affiche les terminaux dont la description correspond à la chaîne que vous avez saisie.
- Cliquez sur **Filtrer**, puis configurez et appliquez un filtre dans la boîte de dialogue qui apparaît. La liste est limitée aux terminaux correspondant au type, à l'identifiant de fournisseur, à l'identifiant de produit et au compte que vous avez sélectionnés lors de la configuration du filtre. Pour annuler le filtre et afficher tous les terminaux, cliquez sur **Réinitialiser au défaut**.

Exporter la liste des terminaux USB présents dans la base de données

Vous pouvez exporter la liste des terminaux USB ajoutés à la base de données.

1. Ouvrez le plan de protection d'un terminal pour le modifier.
2. Cliquez sur l'icône de flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur la ligne **Liste d'autorisation des périphériques USB**.
3. Sur la page de liste d'autorisation des terminaux USB, cliquez sur **Ajouter depuis la base de données**.
4. Sur la page de gestion de la base de données des terminaux USB qui apparaît, cliquez sur **Exporter**.
   La boîte de dialogue Parcourir par défaut s'ouvre.
5. Sélectionnez l'emplacement dans lequel vous souhaitez sauvegarder le fichier, entrez un nouveau nom si besoin, puis cliquez sur **Enregistrer**.

La liste des terminaux USB est exportée sous la forme d'un fichier JSON.

Vous pouvez modifier le fichier JSON obtenu afin d'y ajouter ou d'y retirer des terminaux, ou modifier en masse les descriptions des terminaux.

Importer une liste de terminaux USB dans la base de données

Au lieu d'ajouter des terminaux USB depuis l'interface utilisateur de la console Cyber Protect, vous pouvez importer une liste de terminaux USB. La liste est un fichier au format JSON.

Remarque
Vous pouvez importer des fichiers JSON à une base de données qui ne contient pas les terminaux décrits dans le fichier. Pour importer un fichier modifié vers la base de données depuis laquelle il a été exporté, vous devez d'abord effacer la base de données, car vous ne pouvez pas importer d'entrées dupliquées. Si vous exportez la liste des terminaux USB, la modifiez et essayez de l'importer dans la même base de données sans effacer cette dernière, l'importation échouera.

1. Ouvrez le plan de protection d'un terminal pour le modifier.
2. Cliquez sur l'icône de flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur la ligne **Liste d'autorisation des périphériques USB**.
3. Sur la page de liste d'autorisation des terminaux USB, cliquez sur **Ajouter depuis la base de données**.
4. Sur la page de gestion de la base de données des terminaux USB qui apparaît, cliquez sur **Importer**.
   La boîte de dialogue Importer des terminaux USB depuis un fichier s'ouvre.
5. Utilisez le glisser-déplacer (ou la navigation) pour le fichier que vous souhaitez importer.

La console Cyber Protect vérifie si la liste contient des entrées dupliquées qui existent déjà dans la base de données et les ignore. Les terminaux USB qui ne figurent pas dans la base de données sont ajoutés à la fin de celle-ci.

Liste des terminaux USB sur un ordinateur

Le volet Inventaire d'un ordinateur dans la console Cyber Protect inclut l'onglet **Terminaux USB**. Si l'ordinateur est en ligne et que l'agent Prévention des pertes de données est installé dessus, l'onglet **Terminaux USB** affiche une liste de tous les terminaux USB qui ont déjà été connectés à cet ordinateur.

Les terminaux USB sont répertoriés sous la forme d'une arborescence. Le premier niveau de l'arborescence représente un modèle de terminal. Le deuxième niveau représente un terminal spécifique de ce modèle.

Pour chaque terminal, la liste fournit les informations suivantes :

- **Description** : le système d'exploitation attribue une description lors de la connexion du terminal USB. Cette description peut servir d'identifiant visible pour le terminal.

Une icône bleue à côté de la description du terminal indique que le terminal est actuellement connecté à l'ordinateur. Si le terminal n'est pas connecté à l'ordinateur, l'icône est grisée.

- **Identifiant du périphérique** : l'identifiant que le système d'exploitation a attribué au terminal. L'identifiant possède le format suivant : USB\VID_<identifiant de fournisseur>&PID_<identifiant de produit>\<numéro de série>, où <numéro de série> est facultatif. Exemples : USB\VID_0FCE&PID_ADDE\D55E7FCA (terminal avec numéro de série) ; USB\VID_0FCE&PID_ADDE (terminal sans numéro de série).

Pour ajouter des terminaux à la base de données des terminaux USB, cochez la case des terminaux souhaités, puis cliquez sur le bouton **Ajouter à la base de données**.

Exclusion de processus du contrôle d'accès

L'accès au presse-papiers Windows, aux captures d'écran, aux imprimantes et aux terminaux mobiles est contrôlé par le biais de hooks injectés dans des processus. Si des processus ne disposent pas d'un hook, l'accès à ces terminaux n'est pas contrôlé.

Remarque
L'exclusion de processus du contrôle d'accès n'est pas prise en charge sur macOS. Si une liste de processus exclus est configurée dans le plan de protection appliqué, elle sera ignorée.

Sur la page **Exclusions**, vous pouvez spécifier une liste de processus qui ne disposeront pas d'un hook. Cela signifie que les contrôles d'accès au presse-papiers (local et redirigé), aux captures d'écran, à une imprimante et aux terminaux mobiles ne seront pas appliqués à ces processus.

Par exemple, vous avez appliqué un plan de protection qui refuse l'accès aux imprimantes, puis vous lancez l'application Microsoft Word. Une tentative d'impression depuis cette application sera bloquée. Toutefois, si vous ajoutez le processus Microsoft Word à la liste d'exclusions, l'application ne disposera pas d'un hook. En conséquence, l'impression depuis Microsoft Word ne sera pas bloquée, contrairement à l'impression depuis d'autres applications.

Pour ajouter des processus aux exclusions

1. Ouvrir le plan de protection d'un terminal pour le modifier :
   Cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan de protection, puis sélectionnez **Modifier**.

   Remarque
   Le contrôle des terminaux doit être activé dans le plan, afin que vous puissiez accéder aux paramètres de contrôle des terminaux.

2. Cliquez sur la flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur la ligne **Exclusions**.
3. Sur la page **Exclusions**, à la ligne **Processus et dossiers**, cliquez sur **+Ajouter**.
4. Ajoutez les processus que vous souhaitez exclure du contrôle d'accès.
   Par exemple, `C:\Dossier\sous-dossier\processus.exe`.

Vous pouvez utiliser les caractères génériques suivants :

- * remplace n'importe quel nombre de caractères.
- ? remplace un caractère.

Par exemple :

```
C:\Dossier\*
*\Dossier\Sous-dossier?\*
*\processus.exe
```

5. Cliquez sur la coche, puis sur **Terminé**.
6. Dans le plan de protection, cliquez sur **Enregistrer**.
7. Redémarrez les processus que vous avez exclus pour vous assurer que les hooks ont bien été supprimés.

Les processus exclus auront accès au presse-papiers, aux captures d'écran, aux imprimantes et aux terminaux mobiles, quels que soient les paramètres d'accès pour ces terminaux.

Pour supprimer un processus de la liste d'exclusions

Ouvrir le plan de protection d'un terminal pour le modifier :

Cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan de protection, puis sélectionnez **Modifier**.

Remarque
Le contrôle des terminaux doit être activé dans le plan, afin que vous puissiez accéder aux paramètres de contrôle des terminaux.

1. Cliquez sur la flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur la ligne **Exclusions**.
2. Sur la page **Exclusions**, cliquez sur l'icône de corbeille à côté du processus que vous souhaitez supprimer de la liste d'exclusions.
3. Cliquez sur **Valider**.
4. Dans le plan de protection, cliquez sur **Enregistrer**.
5. Redémarrez le processus pour vous assurer que les hooks ont été correctement injectés.

Les paramètres d'accès issus du plan de protection seront appliqués aux processus que vous avez supprimés de la liste d'exclusions.

Pour modifier un processus dans la liste d'exclusions

1. Ouvrir le plan de protection d'un terminal pour le modifier :
   Cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan de protection, puis sélectionnez **Modifier**.

Remarque
Le contrôle des terminaux doit être activé dans le plan, afin que vous puissiez accéder aux paramètres de contrôle des terminaux.

2. Cliquez sur la flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur la ligne **Exclusions**.
3. Sur la page **Exclusions**, cliquez sur l'icône **Modifier** à côté du processus que vous souhaitez modifier.
4. Appliquez les modifications souhaitées, puis cliquez sur la coche pour les confirmer.
5. Cliquez sur **Valider**.
6. Dans le plan de protection, cliquez sur **Enregistrer**.
7. Redémarrez les processus affectés afin de vous assurer que vos modifications ont été correctement appliquées.

Alertes de contrôle des terminaux

Le module de contrôle des terminaux tient un journal d'événements qui suit les utilisateurs qui tentent d'accéder à des types de terminaux, des ports ou des interfaces contrôlés. Certains événements peuvent entraîner des alertes qui sont consignées dans la console Cyber Protect. Par exemple, le module de contrôle des terminaux peut être configuré pour empêcher l'utilisation de terminaux amovibles, avec une alerte consignée chaque fois qu'un utilisateur tente de copier des données depuis ou vers un tel terminal.

Lors de la configuration du module de contrôles des terminaux, vous pouvez activer des alertes pour la plupart des éléments répertoriés sous le Type (à l'exception des captures d'écran) ou les Ports des terminaux. Si les alertes sont activées, une alerte est générée chaque fois qu'un utilisateur tente d'effectuer une opération qui n'est pas autorisée. Par exemple, si l'accès aux terminaux amovibles est restreint à un accès en lecture seule et que l'option **Afficher une alerte** est sélectionnée pour ce type de terminal, une alerte est générée chaque fois qu'un utilisateur essaie de copier des données vers un terminal amovible sur un ordinateur protégé.

Pour afficher les alertes dans la console Cyber Protect, accédez à **Surveillance** > **Alertes**. Au sein de chaque alerte du module de contrôle des terminaux, la console fournit les informations suivantes sur l'événement respectif :

- **Type** : avertissement.
- **État** : affiche « L'accès au périphérique est bloqué ».
- **Message** : affiche « L'accès à '<type de terminal ou port>' sur '<nom de l'ordinateur>' est bloqué ». Par exemple, « L'accès à 'Amovible' sur 'pc-comptable' est bloqué ».
- **Date et heure** : date et heure auxquelles l'événement s'est produit.
- **Terminal** : nom de l'ordinateur sur lequel l'événement s'est produit.
- **Nom du plan** : nom du plan de protection à l'origine de l'événement.

- **Source** : terminal ou port impliqué dans l'événement. Par exemple, si la tentative d'accès d'un utilisateur à un terminal amovible a été refusée, ce champ indique Terminal amovible.
- **Action** : opération à l'origine de l'événement. Par exemple, si la tentative de copie de données sur un terminal d'un utilisateur a été refusée, ce champ indique Lecture. Pour plus d'informations, voir Valeurs du champ Action.
- **Nom** : nom de l'objet cible de l'événement, par exemple, fichier que l'utilisateur a essayé de copier ou terminal que l'utilisateur a essayé d'utiliser. Ne s'affiche pas si l'objet cible n'a pas pu être identifié.
- **Informations** : informations supplémentaires à propos du terminal cible de l'événement, comme l'identifiant de périphérique pour les périphériques USB. Ne s'affiche pas si aucune information supplémentaire sur le terminal cible n'est disponible.
- **Utilisateur** : nom de l'utilisateur à l'origine de l'événement.
- **Processus** : chemin d'accès complet au fichier exécutable de l'application à l'origine de l'événement. Dans certains cas, le nom du processus peut s'afficher à la place du chemin d'accès. Ne s'affiche pas si aucune information de processus n'est disponible.

Si une alerte s'applique à un terminal USB (y compris les terminaux amovibles et les terminaux amovibles chiffrés), l'administrateur peut, directement depuis l'alerte, ajouter le terminal à la liste d'autorisation, ce qui empêche le module de contrôle des terminaux de restreindre l'accès à ce terminal en particulier. Cliquer sur **Autoriser ce périphérique USB** l'ajoute à la liste d'autorisation des terminaux USB dans la configuration du module de contrôle des terminaux et l'ajoute également à la base de données des terminaux USB pour référence ultérieure.

Voir aussi les étapes pour afficher les alertes de contrôle des terminaux.

Valeurs du champ Action

Le champ **Action** d'alerte peut contenir les valeurs suivantes :

- **Lecture** : obtenir des données du terminal ou du port.
- **Écriture** : envoyer des données au terminal ou au port.
- **Formater** : accès direct (formatage, vérification du disque, etc.) au terminal. Dans le cas d'un port, l'opération s'applique au terminal connecté à ce port.
- **Éjecter** : supprimer le terminal du système ou éjecter le support du terminal. Dans le cas d'un port, l'opération s'applique au terminal connecté à ce port.
- **Imprimer** : envoyer un document à l'imprimante.
- **Copier le son** : copier-coller des données audio via le presse-papiers local.
- **Copier le fichier** : copier-coller un fichier via le presse-papiers local.
- **Copier l'image** : copier-coller une image via le presse-papiers local.
- **Copier le texte** : copier-coller du texte via le presse-papiers local.
- **Copier le contenu non identifié** : copier-coller d'autres données via le presse-papiers local.

- **Copier les données RTF (image)** : copier-coller une image via le presse-papiers local, au format texte enrichi (RTF).
- **Copier les données RTF (fichier)** : copier-coller un fichier via le presse-papiers local, au format texte enrichi (RTF).
- **Copier les données RTF (texte, image)** : copier-coller du texte accompagné d'une image via le presse-papiers local, au format texte enrichi (RTF).
- **Copier les données RTF (texte, fichier)** : copier-coller du texte accompagné d'un fichier via le presse-papiers local, au format texte enrichi (RTF).
- **Copier les données RTF (image, fichier)** : copier-coller une image accompagnée d'un fichier via le presse-papiers local, au format texte enrichi (RTF).
- **Copier les données RTF (texte, image, fichier)** : copier-coller du texte accompagné d'une image et d'un fichier via le presse-papiers local, au format texte enrichi (RTF).
- **Supprimer** : supprimer des données d'un terminal (par exemple, un terminal amovible, un terminal mobile, etc.).
- **Accès du terminal** : accéder à certains terminaux ou ports (par exemple, un terminal Bluetooth, un port USB, etc.).
- **Son entrant** : copier-coller des données audio, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé.
- **Fichier entrant** : copier-coller un fichier, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé.
- **Image entrante** : copier-coller une image, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé.
- **Texte entrant** : copier-coller du texte, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé.
- **Contenu non identifié entrant** : copier-coller d'autres données, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé.
- **Données RTF entrantes (image)** : copier-coller une image, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Données RTF entrantes (fichier)** : copier-coller un fichier, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé, au format texte enrichi (RTF)
- **Données RTF entrantes (texte, image)** : copier-coller du texte accompagné d'une image, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Données RTF entrantes (texte, fichier)** : copier-coller du texte accompagné d'un fichier, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Données RTF entrantes (image, fichier)** : copier-coller une image accompagnée d'un fichier, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé, au format texte enrichi (RTF).

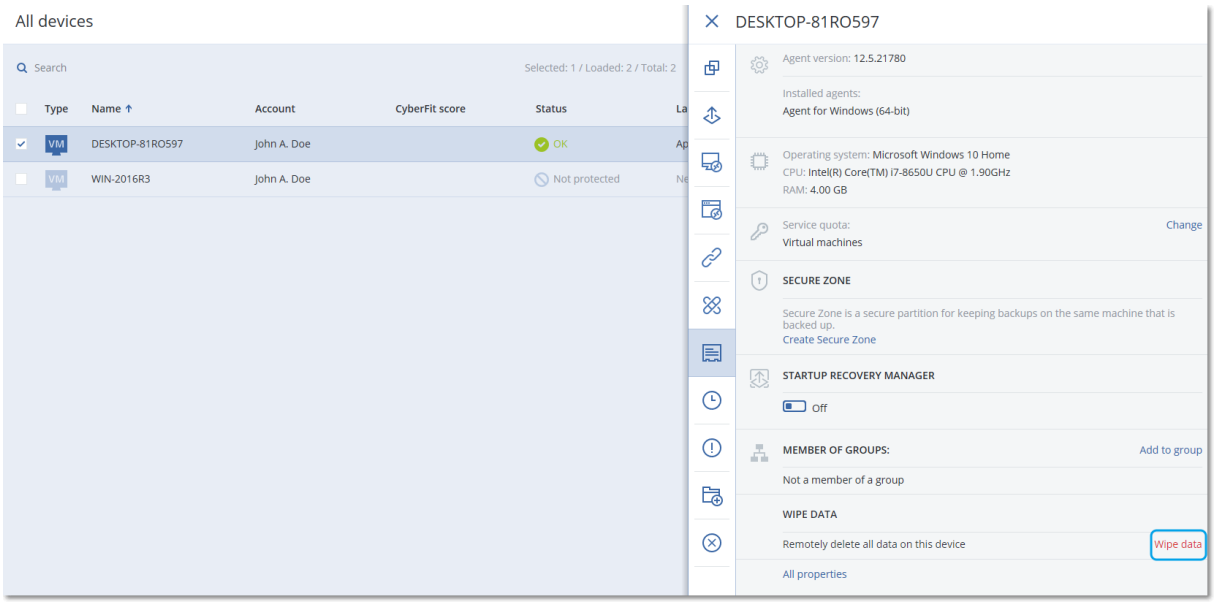
- **Données RTF entrantes (texte, image, fichier)** : copier-coller du texte, accompagné d'une image et d'un fichier, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Insérer** : Connecter un terminal USB ou un terminal FireWire.
- **Son sortant** : copier-coller des données audio, de la session hébergée vers l'ordinateur client, via le presse-papiers redirigé.
- **Fichier sortant** : copier-coller un fichier, de la session hébergée vers l''ordinateur client, via le presse-papiers redirigé.
- **Image sortante** : copier-coller une image, de la session hébergée vers l'ordinateur client, via le presse-papiers redirigé.
- **Texte sortant** : copier-coller du texte, de la session hébergée vers l'ordinateur client, via le presse-papiers redirigé.
- **Contenu non identifié sortant** : copier-coller d'autres données, de la session hébergée vers l'ordinateur client, via le presse-papiers redirigé.
- **Données RTF sortantes (image)** : copier-coller une image, de la session hébergée vers l'ordinateur entier client, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Données RTF sortantes (fichier)** : copier-coller un fichier, de la session hébergée vers l'ordinateur client, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Données RTF sortantes (texte, image)** : copier-coller du texte accompagné d'une image, de la session hébergée vers l'ordinateur client, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Données RTF sortantes (texte, fichier)** : copier-coller du texte accompagné d'un fichier, de la session hébergée vers l'ordinateur client, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Données RTF sortantes (image, fichier)** : copier-coller une image accompagnée d'un fichier, de la session hébergée vers l'ordinateur client, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Données RTF sortantes (texte, image, fichier)** : copier-coller du texte, accompagné d'une image et d'un fichier, de la session hébergée vers l'ordinateur client, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Renommer** : renommer les fichiers sur un terminal (par exemple, sur des périphériques amovibles, terminaux mobiles ou autres).

Effacement des données d'une ressource gérée

Remarque
L'effacement à distance est disponible dans le pack Advanced Security.

L'effacement à distance permet à un administrateur du service Cyber Protection et au propriétaire d'une machine de supprimer des données sur une machine gérée, si elle est égarée ou volée par exemple. Tout accès non autorisé à des informations sensibles sera donc évité.

L'effacement à distance est uniquement disponible pour les ordinateurs exécutant Windows 10 et versions ultérieures. Afin de recevoir la commande d'effacement, la machine doit être allumée et connectée à Internet.



Pour effacer les données d'une machine

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez la machine dont vous souhaitez effacer les données.

   Remarque
   Vous ne pouvez effacer les données que d'une machine à la fois.

3. Cliquez sur **Détails**, puis sur **Effacer les données**.
   Si la machine que vous avez sélectionnée est hors ligne l'option **Effacer les données** est inaccessible.
4. Confirmez votre choix.
5. Saisissez les identifiants de l'administrateur local de la machine, puis cliquez sur **Effacer les données**.

   Remarque
   Vous pouvez consulter les détails du processus d'effacement et la personne l'ayant initié dans **Surveillance** > **Activités**.

Affichage des ressources gérées par les intégrations RMM

Remarque
Cette fonctionnalité n'est disponible que si le service Advanced Automation est activé.

Lorsque vous intégrez une plate-forme RMM dans le cadre du service Advanced Automation, vous pouvez afficher et surveiller les informations à partir des terminaux gérés par cette plate-forme. Ces informations sont disponibles dans la console Cyber Protect en accédant à **Terminaux**.

Pour afficher les ressources gérées par les intégrations RMM

1. Accédez à **Terminaux > Tous les terminaux**.
2. (Facultatif) Triez la colonne **Intégration RMM** pour localiser l'intégration souhaitée.
3. Sélectionnez la ressource pertinente.
4. Dans le panneau **Actions**, sélectionnez **Détails**.
5. Le panneau affiche l'une des trois options en fonction de la ressource configurée :
   - Si les services Acronis sont définis pour la ressource sans intégration RMM : Si la ressource est configurée pour ne fonctionner qu'avec les services Acronis, aucune information sur l'intégration RMM ne s'affiche.
   - Si les services Acronis et une intégration RMM sont configurés pour la ressource : Les services Acronis et les détails concernant l'intégration RMM figurent dans deux onglets : **Vue d'ensemble** et **Intégration RMM**. Cliquez sur **Intégration RMM** pour afficher les détails de l'intégration, y compris le nom, le type (fourni par la plate-forme RMM), la description et l'emplacement de la ressource. Par ailleurs, tous les modules complémentaires d'agent RMM installés et activés sont également affichés.
   - Si la ressource est configurée avec une intégration RMM uniquement : Les détails de l'intégration RMM sont affichés, y compris le nom, le type (fourni par la plate-forme RMM), la description et l'emplacement de la ressource. Par ailleurs, tous les modules complémentaires d'agent RMM installés et activés sont également affichés.

   Notez que, lorsque la ressource est configurée avec l'intégration RMM (seule ou avec les services Acronis), vous pouvez effectuer les opérations suivantes :
   - Établissement d'une connexion à distance (disponible pour les intégrations Datto RMM, N-able N-central et N-able RMM)
   - Examen des modules complémentaires installés sur le terminal RMM tiers (disponible uniquement pour N-able RMM)
   - Accès direct aux informations détaillées sur le terminal RMM tiers (disponible pour Datto RMM, N-able N-central, NinjaOne)

Ressources CyberApp

Les ressources CyberApp sont créées par des éditeurs de logiciels indépendants et apparaissent dans la console Cyber Protect une fois que vous avez activé une intégration CyberApp. Les conditions suivantes doivent être satisfaites :

- Le point d'extension **Ressources et actions** doit être activé dans l'application CyberApp.
- Un **type de ressource** au moins doit être défini dans l'application CyberApp.
- Le service de connecteur hébergé par l'éditeur de logiciels indépendant doit s'assurer que les ressources CyberApp sont ajoutées et mises à jour dans la plate-forme Acronis.

Pour plus d'informations sur le portail dédié aux fournisseurs et sur la création d'applications CyberApp, consultez le Guide de l'utilisateur du portail dédié aux fournisseurs.

Ressources agrégées

Une ressource physique peut avoir un agent Cyber Protect, et un ou plusieurs agents CyberApp installés simultanément. Dans ce cas, la même ressource aura plusieurs représentations dans l'écran **Tous les terminaux**. Un enregistrement distinct s'affiche pour la ressource Acronis et pour chaque ressource CyberApp. Si la fusion automatique des ressources est activée et configurée dans le portail dédié aux fournisseurs ou dans la console Cyber Protect, le système compare les adresses d'hôte et les adresses MAC des ressources Acronis et CyberApp, et fusionne toutes les représentations en une même ressource agrégée. Vous pouvez fusionner et annuler la fusion des ressources manuellement, dans la console Cyber Protect.

Utilisation de ressources CyberApp

Outre les actions standard intégrées dans la console Cyber Protect, vous pouvez effectuer les opérations qui deviennent disponibles une fois que les ressources CyberApp apparaissent dans la console telles que la fusion manuelle de ressources dans une ressource agrégée. Par ailleurs, vous pouvez également réaliser les opérations personnalisées configurées dans l'application CyberApp.

Fusionner

Prérequis

- Les ressources de différentes sources sont disponibles pour le tenant.

Vous pouvez fusionner manuellement une ressource Acronis avec une ou plusieurs ressources CyberApp dans une seule ressource agrégée.

Pour fusionner manuellement des ressources dans une ressource agrégée

1. Dans l'écran **Tous les terminaux**, cliquez sur les ressources que vous souhaitez fusionner.

   Remarque
   L'action de fusion s'affiche si vous sélectionnez des ressources de sources distinctes, par exemple une ressource Acronis et une ressource CyberApp.

2. Cliquez sur **Fusionner des ressources**.

Exécuter des actions personnalisées

Prérequis

- Une intégration CyberApp pour laquelle l'option **Actions sur les ressources** définie est activée pour le tenant.

Les actions personnalisées sont des actions configurées dans l'application CyberApp qui deviennent disponibles pour la ressource CyberApp correspondante lorsque vous activez l'intégration CyberApp pour le tenant.

Pour exécuter des actions personnalisées

1. Dans l'écran **Tous les terminaux**, cliquez sur la ressource.
2. Cliquez sur **Actions d'application intégrées**.
3. Cliquez sur l'action.

Utilisation de ressources agrégées

Outre les actions standard intégrées dans la console Cyber Protect, vous pouvez effectuer les opérations suivantes avec des ressources agrégées : affichage des détails et annulation de la fusion de ressources sources. Par ailleurs, vous pouvez également réaliser les opérations personnalisées configurées dans les applications CyberApp.

Afficher les détails

Prérequis

- Une ressource agrégée au moins est disponible pour le tenant.

Pour afficher les détails d'une ressource agrégée

1. Dans l'écran **Tous les terminaux**, cliquez sur la ressource agrégée.
2. Cliquez sur **Détails**.
   Les informations concernant la ressource agrégée sont disponibles dans différents onglets. Chaque onglet affiche les informations détaillées de chaque représentation de ressource.

Annuler la fusion

Prérequis

- Une ressource agrégée au moins est disponible pour le tenant.

Lorsque vous annulez la fusion d'une ressource agrégée, elle ne s'affiche plus dans la liste des terminaux. Vous voyez en revanche une entrée distincte pour chaque ressource source qui a été fusionnée dans la ressource agrégée.

Pour annuler la fusion d'une ressource agrégée

1. Dans l'écran **Tous les terminaux**, cliquez sur la ressource agrégée dont vous souhaitez annuler la fusion.
2. Cliquez sur **Annuler la fusion de ressources sources**.
3. Dans la fenêtre de confirmation, cliquez sur **Annuler la fusion**.

Exécuter des actions personnalisées

Prérequis

- Au moins une intégration CyberApp pour laquelle l'option **Actions sur les ressources** définie est activée pour le tenant.

Les actions personnalisées sont des actions configurées dans les applications CyberApp qui deviennent disponibles pour la ressource CyberApp correspondante lorsque vous activez l'intégration CyberApp pour le tenant.

Pour exécuter des actions personnalisées

1. Dans l'écran **Tous les terminaux**, cliquez sur la ressource.
2. Cliquez sur **Actions d'application intégrées**.
3. Selon les actions personnalisées disponibles, effectuez l'une des opérations suivantes.
   - Si la ressource agrégée comprend une ressource CyberApp, cliquez sur l'action.
   - Si la ressource agrégée comprend plusieurs ressources CyberApp, cliquez sur le nom de l'application CyberApp, puis sur l'action.

Association de ressources à des utilisateurs spécifiques

Remarque
Cette fonctionnalité n'est disponible que si le service Advanced Automation est activé.

En associant une ressource à un utilisateur spécifique, vous pouvez l'associer automatiquement à de nouveaux tickets du service d'assistance créé par l'utilisateur ou qui lui sont affectés.

Pour associer une ressource à un utilisateur

1. Accédez à **Terminaux > Tous les terminaux**, puis sélectionnez la ressource pertinente.
2. Dans le panneau **Actions**, sélectionnez **Associer à un utilisateur**.
3. Sélectionnez l'utilisateur souhaité.
   Vous pouvez également modifier l'utilisateur sélectionné pour les ressources associées existantes si nécessaire.
4. Cliquez sur **Valider**. L'utilisateur sélectionné s'affiche désormais dans la colonne **Utilisateur lié**.

Pour dissocier une ressource d'un utilisateur

1. Accédez à **Terminaux > Tous les terminaux**, puis sélectionnez la ressource pertinente.
2. Dans le panneau **Actions**, sélectionnez **Associer à un utilisateur**.
3. Cliquez sur **Dissocier l'utilisateur**.
4. Cliquez sur **Valider**.

Rechercher le dernier utilisateur connecté

Pour que les administrateurs puissent gérer les terminaux, ils doivent identifier l'utilisateur actuel et les utilisateurs précédents connectés à un terminal. Ces informations sont affichées dans le tableau de bord ou dans les détails des ressources.

Vous pouvez activer or désactiver l'affichage des informations concernant la dernière connexion dans les plans de gestion à distance.

Dans le tableau de bord :

1. Cliquez sur **Terminaux**. La fenêtre **Tous les terminaux** s'affiche.
2. La colonne **Dernière connexion** indique pour chaque terminal le nom du dernier utilisateur connecté.
3. La colonne **Heure de la dernière connexion** indique pour chaque terminal l'heure de la dernière connexion de l'utilisateur.

Dans les détails du terminal :

1. Cliquez sur **Terminaux**. La fenêtre **Tous les terminaux** s'affiche.
2. Cliquez sur le terminal dont vous souhaitez vérifier les détails.
3. Cliquez sur l'icône **Détails**. La section **Derniers utilisateurs connectés** indique le nom de l'utilisateur, ainsi que les date et heure des dernières connexions depuis le terminal sélectionné.

Remarque
La section **Derniers utilisateurs connectés** affiche jusqu'à 5 utilisateurs qui se sont connectés au terminal.

Pour afficher ou masquer les colonnes Dernière connexion et Heure de la dernière connexion dans le tableau de bord

1. Cliquez sur **Terminaux**. La fenêtre **Tous les terminaux** s'affiche.
2. Cliquez sur l'icône en forme d'engrenage en haut à droite et effectuez l'une des opérations suivantes dans la section **Général** :
   - Activez les colonnes **Dernière connexion** et **Heure de la dernière connexion** si vous souhaitez les afficher dans le tableau de bord.
   - Désactivez les colonnes **Dernière connexion** et **Heure de la dernière connexion** si vous souhaitez les masquer dans le tableau de bord.

Gestion de la sauvegarde et de la reprise des ressources et fichiers

Le module de sauvegarde permet la sauvegarde et la restauration de machines physiques et virtuelles, de fichiers et de bases de données vers un système de stockage local ou dans le Cloud.

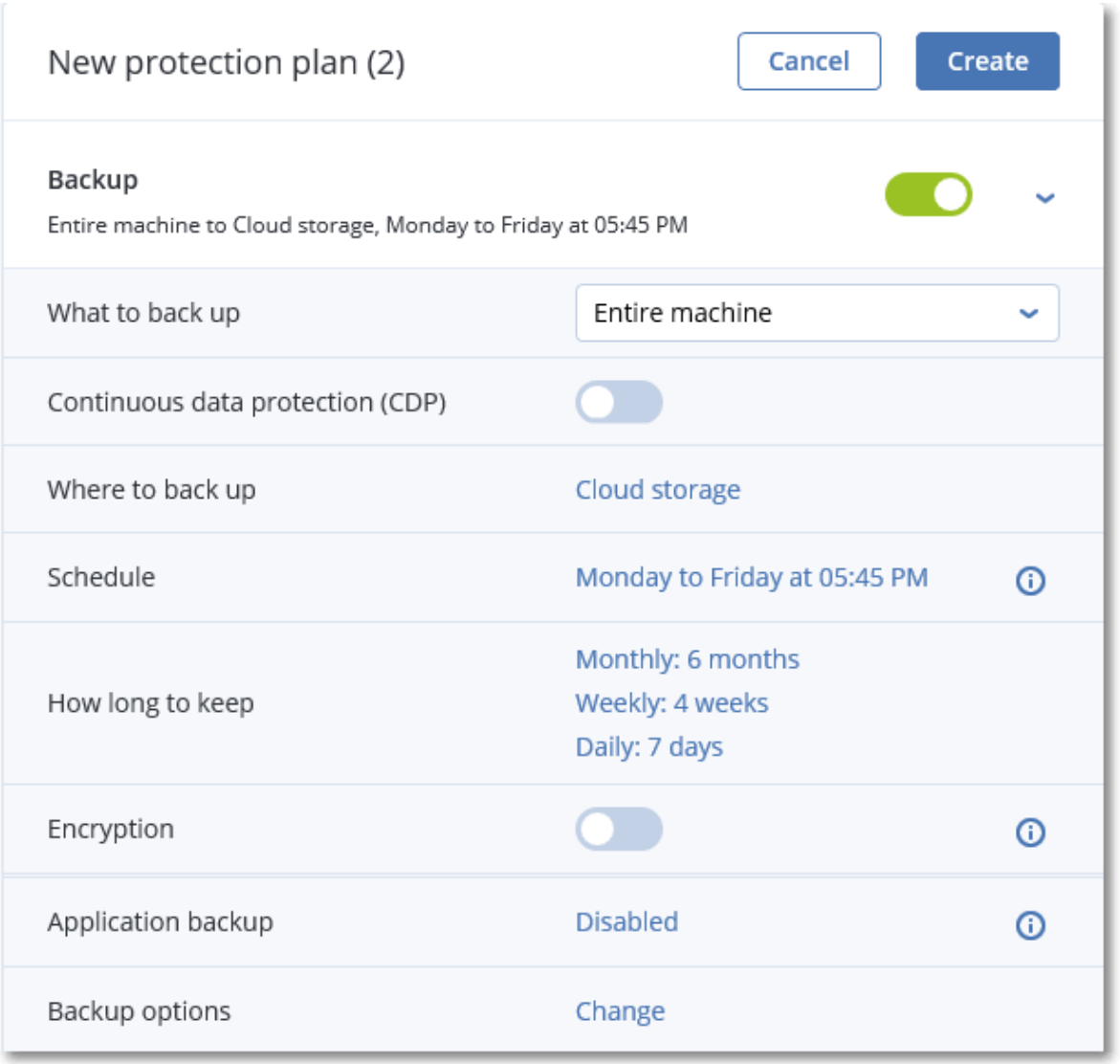
Sauvegarde

Un plan de protection avec module de sauvegarde activé est un ensemble de règles qui définissent la manière dont les données en question seront protégées sur une machine spécifique.

Un plan de protection peut être appliqué à plusieurs machines, soit au moment de sa création, soit plus tard.

Créer votre premier plan de protection avec module de sauvegarde activé

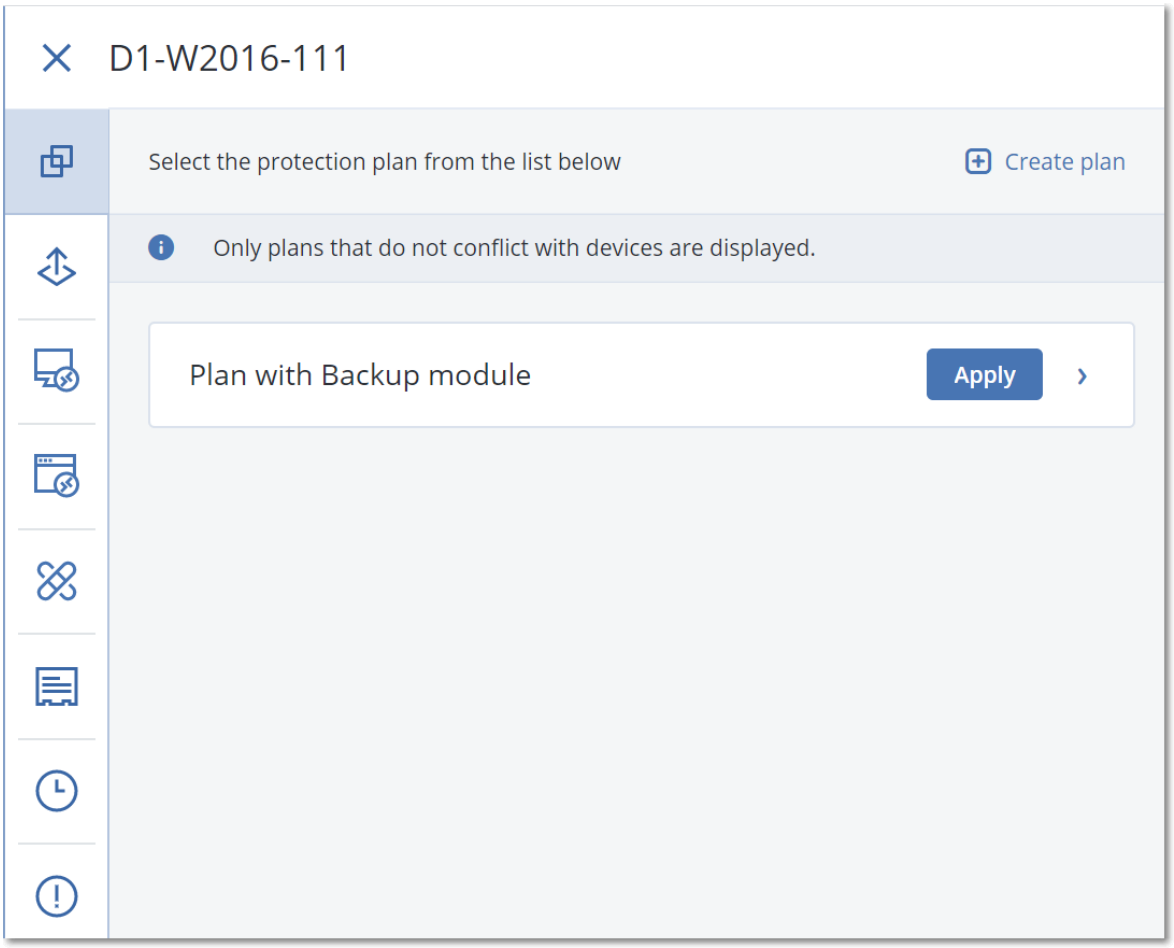
1. Sélectionnez les machines que vous voulez sauvegarder.
2. Cliquez sur **Protection**.
   Les plans de protection appliqués à l'ordinateur s'affichent. Si aucun plan n'est encore appliqué à la machine, vous verrez le plan de protection par défaut qui peut être appliqué. Vous pouvez modifier les paramètres le cas échéant et appliquer ce plan ou en créer un nouveau.
3. Pour créer un plan, cliquez sur **Création d'un plan**. Activez le module **Sauvegarde** et dévoilez les paramètres.



4. [Facultatif] Pour modifier le nom du plan de protection, cliquez sur le nom par défaut.
5. [Facultatif] Pour modifier les paramètres du module de sauvegarde, cliquez sur la section correspondante du volet du plan de protection.
6. [Facultatif] Pour modifier les options de sauvegarde, cliquez sur **Modifier** à côté d'**Options de sauvegarde**.
7. Cliquez sur **Créer**.

Appliquer un plan de protection existant

1. Sélectionnez les machines que vous voulez sauvegarder.
2. Cliquez sur **Protection**. Si un plan de protection courant est déjà appliqué aux machines sélectionnées, cliquez sur **Ajouter un plan**.
   Le logiciel affiche les plans de protection existants.



3. Sélectionnez un plan de protection à appliquer.
4. Cliquez sur **Appliquer**.

Aide-mémoire pour plan de protection

Le tableau suivant résume les paramètres de plan de protection disponibles. Aidez-vous du tableau pour créer le plan de protection qui correspond au mieux à vos besoins.

QUOI SAUVEGARDER	ÉLÉMENTS A SAUVEGARDER Méthodes de sélection	OÙ SAUVEGARDER	PLANIFICATION Modèles de sauvegarde	DURÉE DE CONSERVATION
Disques/volumes (machines physiques[1])	Sélection directe Règles de stratégie	Cloud Dossier local Dossier réseau	Toujours incrémentielle (fichier unique) Toujours	Par âge des sauvegardes (règle unique/par lot de sauvegarde)

[1]Une machine sauvegardée par un agent installé sur le système d'exploitation.

	Filtres de fichiers	NFS* Secure Zone**	complète Complète hebdomadaire, incrémentielle journalière Complète mensuelle, différentielle hebdomadaire, incrémentielle journalière (GFS) Personnalisée (C-D-I)	Par nombre de sauvegardes Par volume total de sauvegardes*** Conserver indéfiniment
Disques/volumes (machines virtuelles[1])	Règles de stratégie Filtres de fichiers	Cloud Dossier local Dossier réseau NFS*		
Fichiers (machines physiques uniquement[2])	Sélection directe Règles de stratégie Filtres de fichiers	Cloud Dossier local Dossier réseau NFS* Secure Zone**		
Configuration ESXi	Sélection directe	Dossier local Dossier réseau NFS*		
Sites Web (fichiers et bases de données MySQL)	Sélection directe	Cloud	—	

[1]Une machine virtuelle sauvegardée au niveau de l'hyperviseur par un agent externe tel que l'agent pour VMware ou l'agent pour Hyper-V. Une machine virtuelle avec un agent interne est traitée comme une machine physique au niveau de la sauvegarde.
[2]Une machine sauvegardée par un agent installé sur le système d'exploitation.

Etat du système		Sélection directe	Cloud Dossier local Dossier réseau	Toujours complète Complète hebdomadaire, incrémentielle journalière Toujours incrémentielle (fichier unique) Personnalisée (C-I)	
Bases de données SQL					
Bases de données Exchange					
Microsoft 365	Boîtes aux lettres (agent local pour Microsoft 365)	Sélection directe	Cloud Dossier local Dossier réseau		
	Boîtes aux lettres (agent Cloud pour Microsoft 365)	Sélection directe	Cloud	Toujours incrémentielle (fichier unique) - Uniquement pour les bases de données SQL Jusqu'à 6 sauvegardes par jour	
	Dossiers publics				
	Teams				
	Fichiers OneDrive	Sélection directe Règles de stratégie			
	Données SharePoint Online				
Google Workspace	Boîtes aux lettres Gmail	Sélection directe	Cloud	Jusqu'à 6 sauvegardes par jour	
	Fichiers Google Drive	Sélection directe Règles de stratégie			
	Fichiers de Drive partagés				

* La sauvegarde vers des partages NFS n'est pas disponible sous Windows.

** Il est impossible de créer Secure Zone sur un Mac.

*** La règle de rétention **Par volume total de sauvegardes** n'est pas disponible avec le modèle de sauvegarde **Toujours incrémentielle (fichier unique)** ni lors de la sauvegarde dans le stockage dans le Cloud.

Sélection des données à sauvegarder

Sélection d'un ordinateur complet

La sauvegarde d'une machine dans son intégralité correspond à une sauvegarde de tous ses disques non amovibles. Pour plus d'informations sur la sauvegarde de disque, reportez-vous à "Sélection de disques ou de volumes" (p. 419).

Limites

- Les sauvegardes de disque ne sont pas prises en charge pour les volumes APFS chiffrés qui sont verrouillés. Ce type de volumes est ignoré lors des sauvegardes complètes de machine.
- Par défaut, le dossier racine OneDrive est exclu des opérations de sauvegarde. Si vous choisissez de sauvegarder des fichiers et dossiers OneDrive spécifiques, ils seront sauvegardés. Les fichiers qui ne sont pas disponibles sur le terminal auront un contenu non valide dans l'ensemble de sauvegarde.

Sélection de disques ou de volumes

Une sauvegarde de niveau disque contient une copie d'un disque ou d'un volume sous forme compacte. Vous pouvez restaurer des disques, volumes, dossiers et fichiers depuis une sauvegarde de disque.

Vous pouvez sélectionner les disques ou les volumes à sauvegarder pour chaque ressource figurant dans le plan de protection (sélection directe) ou configurer des règles de stratégie pour plusieurs ressources. Par ailleurs, vous pouvez exclure certains fichiers d'une sauvegarde ou n'inclure que des fichiers spécifiques en configurant des filtres de fichier. Pour plus d'informations, voir "Filtres de fichiers (Inclusions/Exclusions)" (p. 481).

Pour sélectionner des disques ou des volumes

Sélection directe

La sélection directe n'est disponible que pour les machines physiques.

1. Dans **Quoi sauvegarder**, sélectionnez **Disques/volumes**.
2. Cliquez sur **Éléments à sauvegarder**.
3. Dans **Sélectionner les éléments à sauvegarder**, sélectionnez **Directement**.
4. Pour chacune des ressources comprises dans le plan de protection, cochez les cases à côté des disques ou des volumes à sauvegarder.
5. Cliquez sur **Valider**.

Par règles de stratégie

1. Dans **Quoi sauvegarder**, sélectionnez **Disques/volumes**.
2. Cliquez sur **Éléments à sauvegarder**.
3. Dans **Sélectionner les éléments à sauvegarder**, choisissez **Utilisation des règles de stratégie**.
4. Sélectionnez n'importe quelle règle prédéfinie, créez les vôtres ou combinez les deux.
   Pour plus d'informations sur les règles de stratégie disponibles, voir "Règles de stratégie pour les disques et les volumes" (p. 421).
   Les règles de stratégie seront appliquées à l'ensemble des ressources incluses dans le plan de protection.

Si aucune des règles spécifiées ne peut être appliquée à une ressource, la sauvegarde de cette ressource échoue.

5. Cliquez sur **Valider**.

Limites

- Les sauvegardes de disque ne sont pas prises en charge pour les volumes APFS chiffrés qui sont verrouillés. Ce type de volumes est ignoré lors des sauvegardes complètes de machine.
- Par défaut, le dossier racine OneDrive est exclu des opérations de sauvegarde. Si vous choisissez de sauvegarder des fichiers et dossiers OneDrive spécifiques, ils seront sauvegardés. Les fichiers qui ne sont pas disponibles sur le terminal auront un contenu non valide dans l'ensemble de sauvegarde.
- Vous pouvez sauvegarder des disques connectés via le protocole iSCSI sur une machine physique. Toutefois, des limites s'appliquent si vous utilisez l'agent pour VMware ou l'agent pour Hyper-V pour sauvegarder les disques connectés à iSCSI. Pour plus d'informations, voir "Limites" (p. 34).

Que stocke une sauvegarde de disque ou de volume ?

Une sauvegarde de disque ou de volume stocke le **système de fichiers** d'un disque ou d'un volume en entier et inclut toutes les informations nécessaires pour le démarrage du système d'exploitation. Il est possible de restaurer des disques ou volumes entiers à partir de telles sauvegardes de même que des fichiers ou dossiers individuels.

Avec l'option **secteur-par-secteur (mode nu)**activée, une sauvegarde de disque stocke tous les secteurs du disque. L'option secteur-par-secteur peut être utilisée pour la sauvegarde de disques avec systèmes de fichiers non-reconnus ou non-supportés ainsi que d'autres formats de données propriétaires.

Windows

Une sauvegarde de volume stocke tous les fichiers et dossiers du volume sélectionné indépendemment de leurs attributs (y compris fichiers cachés et système), secteur de démarrage, tableau d'allocation de fichiers (FAT) s'il existe, fichier racine et la piste zéro du disque dur avec le secteur de démarrage principal (MBR).

Une sauvegarde de disque stocke tous les volumes du disque sélectionné (incluant les volumes cachés tels que les partitions de maintenance du fabricant) et la piste zéro avec la zone d'amorce maître.

Les éléments suivants ne sont *pas* inclus dans une sauvegarde de disque ou de volume (de même que dans une sauvegarde de niveau fichier) :

- Le fichier d'échange (pagefile.sys) et le fichier qui maintient le contenu de la RAM quand la machine se met en veille (hiberfil.sys). Après la restauration, les fichiers seront re-créés dans leur emplacement approprié avec une taille zéro.

- Si la sauvegarde est effectuée sous le système d'exploitation (par opposition au support de démarrage ou à la sauvegarde de machines virtuelles au niveau hyperviseur) :
  - Stockage Windows shadow. Le chemin vers cet emplacement de stockage est déterminé par la valeur de registre **VSS Default Provider** qui peut être trouvée dans la clé de registre **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup**. Ceci signifie que dans les systèmes d'exploitation démarrant avec Windows Vista, les points de restauration Windows ne sont pas sauvegardés.
  - Si l'option de sauvegarde **service de cliché instantané des volumes (VSS)** est activée, les fichiers et les dossiers qui ont été indiqués dans la clé de la base de registre **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** .

Linux

Une sauvegarde de volume stocke tous les fichiers et répertoires du volume sélectionné indépendemment de leurs attributs, du secteur de démarrage, et le système de fichiers super bloc.

Une sauvegarde de disque stocke tous les volumes des disques ainsi que la piste zéro avec la zone d'amorce maître.

Mac

Un disque ou une sauvegarde de volume stocke tous les fichiers et répertoires du disque ou volume sélectionné, plus une description de la disposition du volume.

Les éléments suivants sont exclus :

- Métadonnées de système, telles que le journal du système de fichiers et l'index Spotlight
- La poubelle
- Chronométrez les sauvegardes de la machine

Physiquement, les disques et volumes d'un Mac sont sauvegardés au niveau du fichier. La restauration à froid à partir des sauvegardes de disque et de volume est possible, mais le mode de sauvegarde secteur par secteur n'est pas disponible.

Règles de stratégie pour les disques et les volumes

Lorsque vous sélectionnez des disques ou des volumes à sauvegarder, vous pouvez utiliser les stratégies de règle suivantes en fonction du système d'exploitation de la ressource protégée.

Windows

- `[All Volumes]` sélectionne tous les volumes sur l'ordinateur.
- Lettre de lecteur (par exemple, `C:\`) sélectionne le volume correspondant à la lettre de lecteur indiquée.
- `[Fixed Volumes (physical machines)]` sélectionne tous les volumes d'une machine physique, à l'exception des supports amovibles. Les volumes fixes incluent les volumes sur les périphériques SCSI, ATAPI, ATA, SSA, SAS et SATA, et sur les matrices RAID.

- `[BOOT+SYSTEM]` sélectionne les volumes système et les volumes de démarrage. Il s'agit de la combinaison minimale à partir de laquelle vous pouvez restaurer un système d'exploitation.
- `[Disk 1]` sélectionne le premier disque de la machine, en prenant en compte l'ensemble de ses volumes. Pour sélectionner un autre disque, saisissez son numéro correspondant.

Linux

- `[All Volumes]` sélectionne tous les volumes montés sur l'ordinateur.
- `/dev/hda1` sélectionne le premier volume du premier disque dur IDE.
- `/dev/sda1` sélectionne le premier volume du premier disque dur SCSI.
- `/dev/md1` sélectionne le premier logiciel de disque dur RAID.
- Pour sélectionnez d'autres volumes de base, spécifiez `/dev/xdyN`, où :
  - « x » correspond au type de disque
  - « y » correspond au numéro de disque (a pour le premier disque, b pour le second, etc.)
  - « N » étant le nombre de volumes.
- Pour sélectionner un volume logique, indiquez son chemin tel qu'il apparaît après l'exécution de la commande `ls /dev/mapper` sous le compte racine.

  Par exemple :

  ```
  [root@localhost ~]# ls /dev/mapper/
  control vg_1-lv1 vg_1-lv2
  ```

  Cette sortie montre deux volumes logiques, `lv1` et `lv2`, qui appartiennent au groupe de volumes `vg_1`. Pour sauvegarder ces volumes, spécifiez :

  `/dev/mapper/vg_1-lv1`

  `/dev/mapper/vg-l-lv2`

macOS

- `[All Volumes]` sélectionne tous les volumes montés sur l'ordinateur.
- `[Disk 1]` sélectionne le premier disque de la machine, en prenant en compte l'ensemble de ses volumes. Pour sélectionner un autre disque, spécifiez le numéro correspondant.

Sélection de fichiers ou de dossiers

Utilisez la sauvegarde de fichier pour ne protéger que des données spécifiques, par exemple les fichiers de votre projet en cours. Les sauvegardes de fichier sont moins volumineuses que les sauvegardes de disque et permettent d'économiser l'espace de stockage.

Important
Vous ne pouvez pas restaurer un système d'exploitation à partir d'une sauvegarde de fichier.

Vous pouvez sélectionner les fichiers et les dossiers à sauvegarder pour chaque ressource figurant dans le plan de protection (sélection directe) ou configurer des règles de stratégie pour plusieurs

ressources. Par ailleurs, vous pouvez exclure certains fichiers d'une sauvegarde ou n'inclure que des fichiers spécifiques en configurant les filtres. Pour plus d'informations, voir "Filtres de fichiers (Inclusions/Exclusions)" (p. 481).

Pour sélectionner des fichiers ou des dossiers

Sélection directe

1. Dans **Quoi sauvegarder**, sélectionnez **Fichiers/dossiers**.
2. Dans **Éléments à sauvegarder**, cliquez sur **Spécifier**.
3. Dans **Sélectionner les éléments à sauvegarder**, sélectionnez **Directement**.
4. Spécifiez les fichiers ou dossiers à sauvegarder pour chaque ressource dans le plan de protection.
   a. Cliquez sur **Sélectionner les fichiers et dossiers**.
   b. Cliquez sur **Dossier local** ou sur **Dossier réseau**.
      Les dossiers réseau doivent être accessibles depuis l'ordinateur sélectionné.
      Lorsque vous sélectionnez la source **Dossier réseau**, vous pouvez sauvegarder les données de stockages NAS tels que les terminaux NetApp. Les terminaux NAS de tous les fournisseurs sont pris en charge.
   c. Dans l'arborescence des dossiers, accédez aux fichiers ou dossiers nécessaires.
      Vous pouvez également spécifier leur chemin d'accès, puis cliquer sur le bouton fléché.
   d. [Pour les dossiers partagés] Lorsque vous y êtes invité, spécifiez les identifiants d'accès au dossier partagé.
      La sauvegarde des dossiers avec accès anonyme n'est pas prise en charge.
   e. Sélectionnez les fichiers et dossiers nécessaires.
   f. Cliquez sur **Valider**.

Par règles de stratégie

1. Dans **Quoi sauvegarder**, sélectionnez **Fichiers/dossiers**.
2. Dans **Éléments à sauvegarder**, cliquez sur **Spécifier**.
3. Dans **Sélectionner les éléments à sauvegarder**, choisissez **Utilisation des règles de stratégie**.
4. Sélectionnez n'importe quelle règle prédéfinie, créez les vôtres ou combinez les deux.
   Pour plus d'informations sur les règles de stratégie disponibles, voir "Règles de stratégie pour les fichiers et les dossiers" (p. 424).
   Les règles de stratégie seront appliquées à l'ensemble des ressources incluses dans le plan de protection.
   Si aucune des règles spécifiées ne peut être appliquée à une ressource, la sauvegarde de cette ressource échoue.
5. Cliquez sur **Valider**.

Limites

- Vous pouvez sélectionner des fichiers et des dossiers lorsque vous sauvegardez des machines physiques ou virtuelles sur lesquelles un agent est installé (sauvegarde avec agent). La sauvegarde de fichier n'est pas disponible pour les machines virtuelles que vous sauvegardez en mode sans agent. Pour plus d'informations sur les différences entre ces types de sauvegarde, voir "Sauvegarde avec et sans agent" (p. 67).
- Par défaut, le dossier racine OneDrive est exclu des opérations de sauvegarde. Si vous choisissez de sauvegarder des fichiers et dossiers OneDrive spécifiques, ils seront sauvegardés. Les fichiers qui ne sont pas disponibles sur le terminal auront un contenu non valide dans l'ensemble de sauvegarde.
- Vous pouvez sauvegarder des fichiers et des dossiers stockés sur des disques connectés via le protocole iSCSI à une machine physique. Certaines limites s'appliquent si vous utilisez l'agent pour VMware ou l'agent pour Hyper-V pour sauvegarder les données sur des disques connectés à iSCSI.

Règles de stratégie pour les fichiers et les dossiers

Lorsque vous sélectionnez des fichiers ou des dossiers à sauvegarder, vous pouvez utiliser les stratégies de règle suivantes en fonction du système d'exploitation de la ressource protégée.

Windows

- Chemin complet vers un fichier ou un dossier. Par exemple, `D:\Work\Text.doc` ou `C:\Windows`.
- Règles prédéfinies :
  - `[All Files]` sélectionne tous les fichiers sur tous les volumes de la machine.
  - `[All Profiles Folder]` sélectionne le dossier dans lequel se trouvent tous les profils utilisateur. Par exemple, `C:\Users` ou `C:\Documents and Settings`.
- Variables d'environnement :
  - `%ALLUSERSPROFILE%` sélectionne le dossier où se trouvent les données communes à tous les profils des utilisateurs. Par exemple, `C:\ProgramData` ou `C:\Documents and Settings\All Users`.
  - `%PROGRAMFILES%` sélectionne le dossier `Program Files`. Par exemple, `C:\Program Files`.
  - `%WINDIR%` sélectionne le dossier `Windows`. Par exemple, `C:\Windows`.

  Vous pouvez utiliser d'autres variables d'environnement ou une combinaison de variables d'environnement et de texte. Par exemple, pour sélectionner le dossier Java dans le dossier Program Files, spécifiez : `%PROGRAMFILES%\Java`.

Linux

- Chemin complet vers un fichier ou un répertoire.

  Par exemple, pour sauvegarder `file.txt` sur le volume `/dev/hda3` monté sur `/home/usr/docs`, spécifiez `/dev/hda3/file.txt` ou `/home/usr/docs/file.txt`.
- Règles prédéfinies :

- `[All Profiles Folder]` sélectionne `/home`. Par défaut, tous les profils utilisateur sont stockés dans ce dossier.
- `/home` sélectionne le répertoire personnel des utilisateurs courants.
- `/root` sélectionne le répertoire personnel de l'utilisateur racine.
- `/usr` sélectionne le répertoire de tous les programmes liés aux utilisateurs.
- `/etc` sélectionne le répertoire des fichiers de configuration du système.

macOS

- Chemin complet vers un fichier ou un répertoire.
  Par exemple :
  - Pour sauvegarder `fichier.txt` sur le bureau d'un utilisateur, spécifiez `/Utilisateurs/<nom utilisateur>/Bureau/fichier.txt`.
  - Pour sauvegarder les dossiers `Bureau`, `Documents` ou `Téléchargements` d'un utilisateur, spécifiez `/Utilisateurs/<nom utilisateur>/Bureau`, `/Utilisateurs/<nom utilisateur>/Documents` ou `/Utilisateurs/<nom utilisateur>/Téléchargements`.
  - Pour sauvegarder le dossier de base de tous les utilisateurs qui possèdent un compte sur cet ordinateur, spécifiez `/Utilisateurs`.
  - Pour sauvegarder le dossier dans lequel les applications sont installées, spécifiez `/Applications`.
- Règles prédéfinies
  - `[All Profiles Folder]` sélectionne `/Utilisateurs`. Par défaut, tous les profils utilisateur sont stockés dans ce dossier.

Sélection de l'état du système

Remarque
La sauvegarde de l'état du système est disponible pour les ordinateurs exécutant Windows 7 et versions ultérieures sur lesquels l'agent pour Windows est installé. La sauvegarde de l'état du système n'est pas disponible pour les pour les machines virtuelles qui sont sauvegardées au niveau de l'hyperviseur (sauvegarde sans agent).

Pour sauvegarder l'état du système, dans **Quoi sauvegarder**, sélectionnez **Etat du système**.

Une sauvegarde de l'état du système se compose des fichiers suivants :

- Configuration du planificateur de tâches
- VSS Metadata Store
- Informations de configuration du compteur de performances
- Service MSSearch
- Service de transfert intelligent en arrière-plan (BITS)
- Le registre

- Windows Management Instrumentation (WMI)
- Bases de données d'enregistrement des services de composants

Sélection de la configuration ESXi

La sauvegarde d'une configuration d'hôte ESXi vous permet de restaurer un hôte ESXi de manière complète. La restauration est exécutée sous un support de démarrage.

Les machines virtuelles s'exécutant sur l'hôte ne sont pas incluses dans la sauvegarde. Elles peuvent être sauvegardées et restaurées séparément.

La sauvegarde d'une configuration d'hôte ESXi inclut :

- Le chargeur de démarrage et les partitions de banque de démarrage de l'hôte
- L'état de l'hôte (informations relatives à la configuration de la mise en réseau et du stockage virtuels, aux clés SSL, aux paramètres réseau du serveur, et à l'utilisateur local)
- Les extensions et correctifs installés ou préconfigurés sur l'hôte
- Les fichiers journaux

Prérequis

- SSH doit être activé dans le **Profil de sécurité** de la configuration de l'hôte ESXi.
- Vous devez connaître le mot de passe du compte « racine » sur l'hôte ESXi.

Limites

- La sauvegarde de la configuration ESXi n'est pas prise en charge pour les hôtes exécutant VMware ESXi 7.0 et les versions ultérieures.
- Une configuration ESXi ne peut pas être sauvegardée sur le stockage dans le Cloud.

Pour sélectionner une configuration ESXi

1. Cliquez sur **Terminaux** > **Tous les terminaux**, puis sélectionnez les hôtes ESXi que vous voulez sauvegarder.
2. Cliquez sur **Protection**.
3. Dans **Quoi sauvegarder**, sélectionnez **Configuration ESXi**.
4. Dans **Mot de passe « racine » ESXi**, spécifiez un mot de passe pour le compte « racine » pour chacun des hôtes sélectionnés ou appliquez le même mot de passe pour tous les hôtes.

Protection continue des données (CDP)

La Protection continue des données (CDP) fait partie du pack Advanced Backup. Elle sauvegarde les données critiques dès leur modification. De cette manière, aucune modification ne sera perdue en cas de panne du système entre deux sauvegardes planifiées. Vous pouvez configurer la protection continue des données pour les données suivantes :

- Fichiers ou dossiers dans des emplacements spécifiques
- Fichiers modifiés par des applications spécifiques

La protection continue des données n'est prise en charge que pour le système de fichiers NTFS et pour les systèmes d'exploitation suivants :

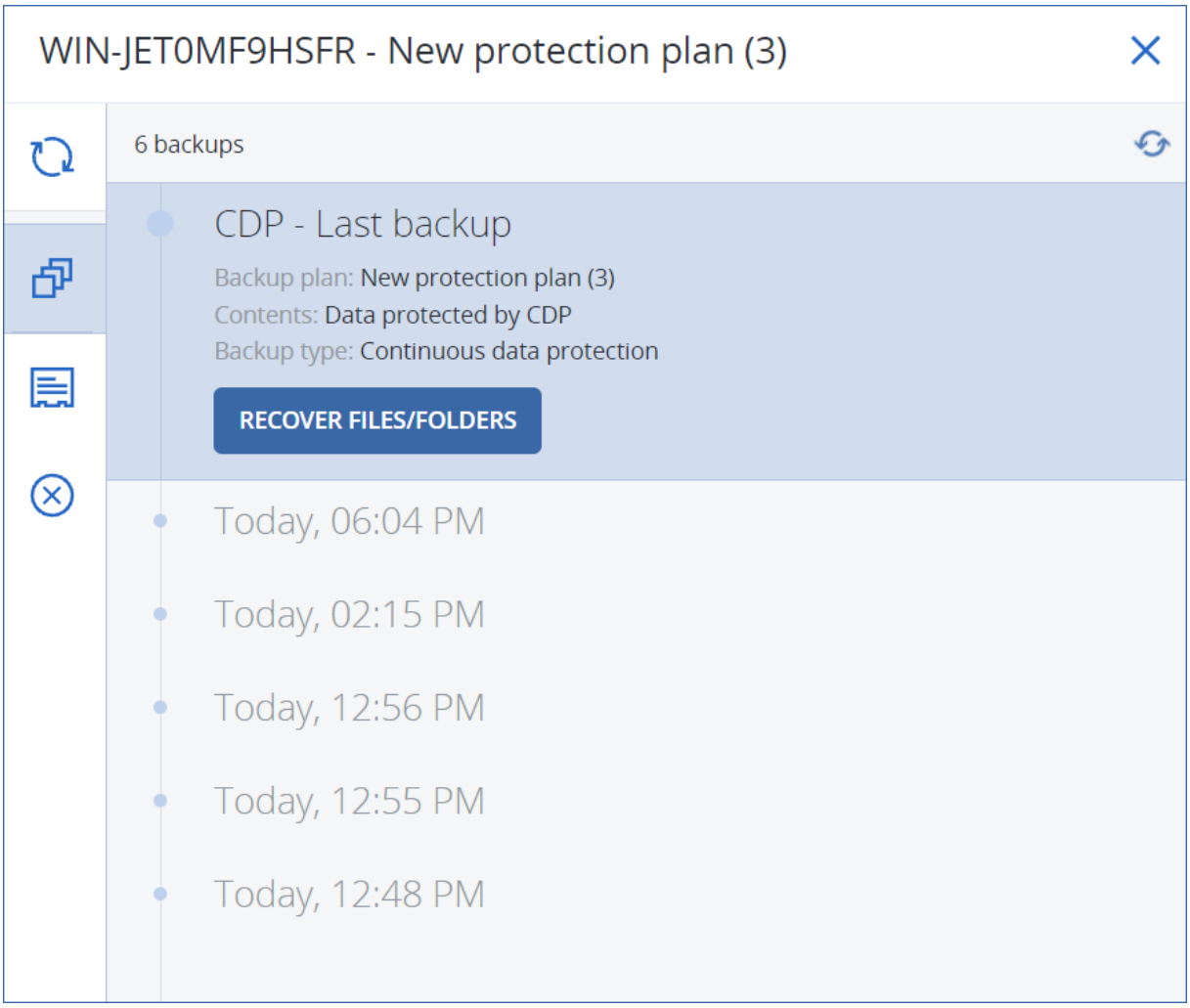
- Ordinateur de bureau : Windows 7 et versions ultérieures
- Serveur : Windows Server 2008 R2 et versions ultérieures

Seuls les dossiers locaux sont pris en charge. Les dossiers réseau ne peuvent pas être sélectionnés pour la protection continue des données.

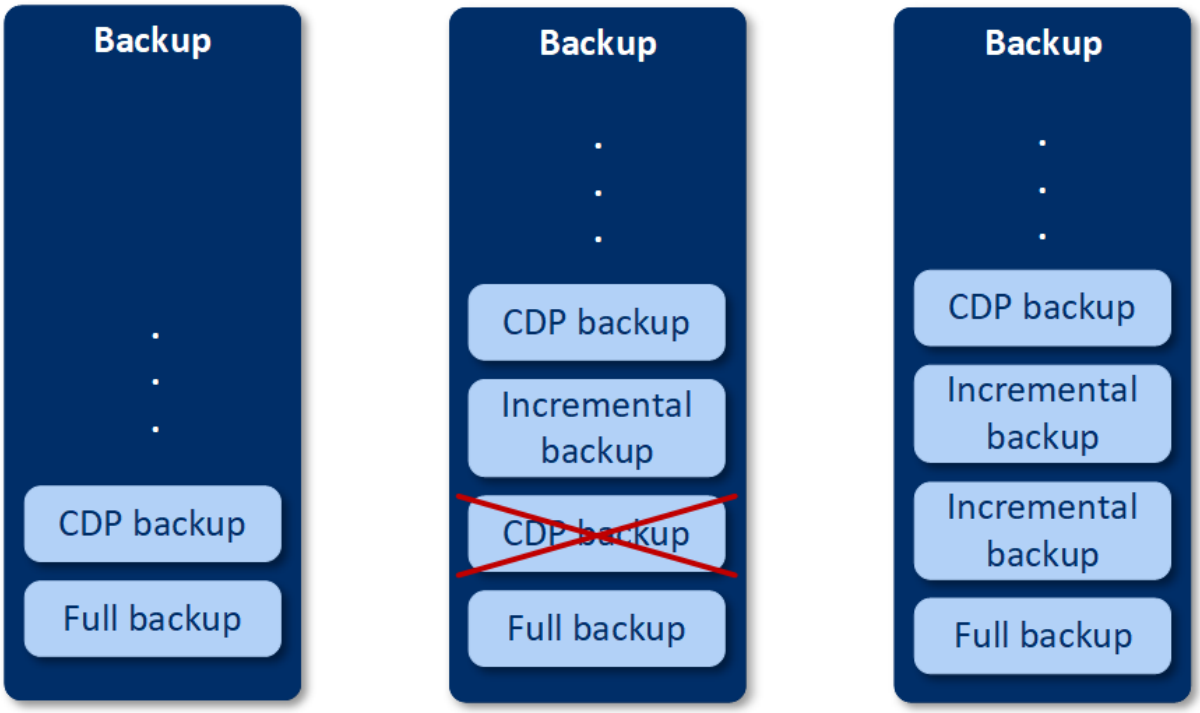
La protection continue des données n'est pas compatible avec l'option **Sauvegarde d'applications**.

Fonctionnement

Les modifications apportées aux fichiers et aux dossiers suivis par la protection continue des données sont immédiatement sauvegardées dans une sauvegarde CDP spéciale. Seule une sauvegarde CDP est présente dans un jeu de sauvegarde, et il s'agit toujours de la sauvegarde la plus récente.



Lorsqu'une sauvegarde normale planifiée démarre, la protection continue des données est mise en attente, car les dernières données sont incluses dans la sauvegarde planifiée. Lorsque la sauvegarde planifiée se termine, la protection continue des données reprend, l'ancienne sauvegarde CDP est supprimée, et une nouvelle sauvegarde CDP est créée. Par conséquent, la sauvegarde CDP reste toujours la sauvegarde la plus récente du jeu de sauvegarde et ne stocke que le dernier état des fichiers ou des dossiers suivis.



Si votre ordinateur plante lors d'une sauvegarde normale, la protection continue des données reprend automatiquement au redémarrage de l'ordinateur et crée une sauvegarde CDP au-dessus de la dernière sauvegarde planifiée réussie.

La protection continue des données exige qu'au moins une sauvegarde normale soit créée avant la sauvegarde CDP. Pour cette raison, lorsque vous exécutez un plan de protection avec protection continue des données pour la première fois, une sauvegarde complète est créée, et une sauvegarde CDP est immédiatement ajoutée au-dessus de celle-ci. Si vous activez l'option de **protection continue des données** pour un plan de protection existant, la sauvegarde CDP est ajoutée au jeu de sauvegarde existant.

Remarque
La protection continue des données est activée par défaut pour les plans de protection que vous créez depuis l'onglet **Terminaux** si la fonctionnalité Advanced Backup est activée à votre place et que vous n'utilisez pas les autres fonctionnalités Advanced Backup des ordinateurs sélectionnés. Si vous possédez déjà un plan avec la protection continue des données d'un ordinateur sélectionné, la protection continue des données n'est pas activée par défaut pour cet ordinateur dans les nouveaux plans créés.
La protection continue des données n'est pas activée par défaut pour les plans créés pour les groupes de terminaux.

Sources de données prises en charge

Vous pouvez configurer la protection continue des données pour les sources de données suivantes :

- Toute la machine
- Disques/volumes
- Fichiers/dossiers

Après avoir sélectionné la source de données dans la section **Que sauvegarder** du plan de protection, sélectionnez les fichiers, les dossiers ou les applications auxquels appliquer la protection continue des données dans la section **Éléments à protéger continuellement**. Pour en savoir plus sur la configuration de la protection continue des données, reportez-vous à "Configuration d'une sauvegarde CDP" (p. 429).

Destinations prises en charge

Vous pouvez configurer la protection continue des données pour les destinations suivantes :

- Dossier local
- Dossier réseau
- Stockage dans le Cloud
- Acronis Cyber Infrastructure
- Emplacement défini par un script

Remarque
Seuls les emplacements répertoriés ci-dessus peuvent être définis par un script.

Configuration d'une sauvegarde CDP

Vous pouvez configurer la protection continue des données (CDP) dans le module **Sauvegarde** d'un plan de protection. Pour en savoir plus sur la création d'un plan de protection, reportez-vous à "Création d'un plan de protection" (p. 223).

Pour configurer les paramètres de protection continue des données

1. Dans le module **Sauvegarde** d'un plan de protection, activez le commutateur **Protection continue des données (CDP)**.

   Ce commutateur est disponible uniquement pour les sources de données suivantes :

   - Toute la machine
   - Disque/volumes
   - Fichiers/dossiers

2. Dans **Éléments à protéger continuellement**, configurez la protection continue des données pour **Applications** et/ou **Fichiers/dossiers**.

   - Cliquez sur **Applications** afin de configurer la sauvegarde de protection continue des données pour les fichiers modifiés par des applications spécifiques.

     Vous pouvez sélectionner des applications à partir de catégories prédéfinies ou ajouter d'autres applications en définissant le chemin d'accès à leur fichier exécutable, par exemple :

     - `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`
     - `*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE`

   - Cliquez sur **Fichiers/dossiers** afin de configurer la sauvegarde de protection continue des données pour les fichiers dans des emplacements spécifiques.

     Vous pouvez définir ces emplacements à l'aide de règles de sélection ou en sélectionnant directement des fichiers et des dossiers.

     - [Pour tous les ordinateurs] Pour créer une règle de sélection, servez-vous de la zone de texte.

       Vous pouvez spécifier des chemins d'accès complets aux fichiers ou des chemins d'accès avec des caractères génériques (* et ?). L'astérisque remplace zéro caractère ou plus. Le point d'interrogation remplace un seul caractère.

       Important

       Pour créer une sauvegarde CDP pour un dossier, vous devez spécifier son contenu à l'aide du caractère générique « astérisque » :

       Chemin d'accès correct : `D:\Data\*`

       Chemin d'accès incorrect : `D:\Data\`

     - [Pour les ordinateurs en ligne] Pour sélectionner des fichiers et des dossiers directement :
       - Dans **Machine à parcourir**, sélectionnez l'ordinateur sur lequel les fichiers ou dossiers se trouvent.
       - Cliquez sur **Sélectionner les fichiers et dossiers** pour parcourir l'ordinateur sélectionné.

         Votre sélection directe crée une règle de sélection. Si vous appliquez le plan de protection à plusieurs ordinateurs et qu'une règle de sélection n'est pas valide pour l'un d'entre eux, elle sera ignorée sur l'ordinateur en question.

3. Dans le volet du plan de protection, cliquez sur **Créer**.

Les données que vous spécifiez seront sauvegardées de manière continue entre les sauvegardes planifiées.

Sélection d'une destination

Cliquez sur **Où sauvegarder**, puis sélectionnez l'une des options suivantes :

- **Stockage dans le Cloud**

  Les sauvegardes seront stockées dans le centre de données du Cloud.
- **Dossiers locaux**

  Si une seule machine est sélectionnée, naviguez jusqu'au dossier souhaité ou indiquez son chemin sur cette même machine.

  Si plusieurs machines sont sélectionnées, saisissez le chemin du dossier. Les sauvegardes seront stockées dans ce dossier, sur chacune des machines sélectionnées ou sur la machine où l'agent pour machines virtuelles est installé. Si le dossier n'existe pas, il sera créé.
- **Dossier réseau**

  Il s'agit d'un dossier partagé via SMB/CIFS/DFS.

  Naviguez vers le dossier partagé souhaité ou indiquez son chemin au format suivant :
  - Pour les partages SMB/CIFS : `\\<nom d'hôte>\<chemin>\` ou `smb://<nom d'hôte>/<chemin>/`
  - Pour les partages DFS : `\\<nom de domaine DNS complet>\<racine DFS>\<chemin>`

    Par exemple, `\\exemple.entreprise.com\partage\fichiers`

  Cliquez ensuite sur la flèche. Si vous y êtes invité, spécifiez le nom d'utilisateur et le mot de passe requis pour accéder au dossier partagé. Vous pouvez modifier ces identifiants à tout moment en cliquant sur l'icône en forme de clé à côté du nom de dossier.

  La sauvegarde dans un dossier avec accès anonyme n'est pas prise en charge.
- **Cloud public**

  Cette option est disponible dans le pack Advanced Backup.

  Elle vous permet de configurer une sauvegarde directe vers un stockage compatible avec le cloud public sans avoir à déployer d'autres composants (Microsoft Azure ou d'autres machines virtuelles telles que les passerelles). Sélectionnez le cloud public souhaité pour vous y connecter.

  Pour plus d'informations, voir "Sauvegarde de ressources dans des clouds publics" (p. 565).
- **Dossier NFS** (disponible uniquement sur les machines sous Linux ou macOS)

  Vérifiez que le package nfs-utils est installé sur le serveur Linux sur lequel l'agent pour Linux est installé.

  Naviguez vers le dossier NFS souhaité ou indiquez son chemin au format suivant :

  `nfs://<nom d'hôte>/<dossier exporté>:/<sous-dossier>`

  Cliquez ensuite sur la flèche.

  Remarque

  Il est impossible de sauvegarder un dossier NFS protégé par mot de passe.
- **Secure Zone** (disponible uniquement s'il est présent sur chacune des machines sélectionnées)

Secure Zone est une partition sécurisée sur un disque de la machine sauvegardée. Cette partition doit être créée manuellement, avant de configurer une sauvegarde. Pour en savoir plus sur la manière de créer Secure Zone, ses avantages et ses limites, consultez "À propos de Secure Zone" (p. 433).

Option de stockage avancée

Remarque
Cette fonctionnalité est disponible uniquement dans l'édition avancée du service Cyber Protection.

Défini par un script (disponible sur les machines fonctionnant sous Windows)

Vous pouvez stocker les sauvegardes de chaque machine dans un dossier défini par un script. Le logiciel prend en charge les scripts écrits en JScript, VBScript ou Python 3.5. Lors du déploiement du plan de protection, le logiciel exécute le script sur chaque machine. La sortie de script pour chaque ordinateur doit être un chemin de dossier local ou réseau. Si un dossier n'existe pas, il sera créé (limite : les scripts écris dans Python ne peuvent pas créer des dossiers sur des partages réseau). Dans l'onglet **Stockage de sauvegarde**, chaque dossier est affiché comme un emplacement de sauvegarde distinct.

Dans **Type de script**, sélectionnez le type de script (**JScript**, **VBScript** ou **Python**), puis importez, ou copiez et collez le script. Pour les dossiers réseau, spécifiez les informations d'identification avec les autorisations de lecture/écriture.

Exemples :

- Le script JScript suivant fournit l'emplacement de sauvegarde pour un ordinateur au format `\\bkpsrv\<nom de l'ordinateur>` :

  ```
  WScript.Echo("\\\\bkpsrv\\" + WScript.CreateObject("WScript.Network").ComputerName);
  ```

  De ce fait, les sauvegardes de chaque ordinateur sont sauvegardées dans un dossier du même nom sur le serveur **bkpsrv**.
- Le script JScript suivant fournit l'emplacement de sauvegarde dans un dossier de l'ordinateur sur lequel le script s'exécute :

  ```
  WScript.Echo("C:\\Backup");
  ```

  De ce fait, les sauvegardes de cet ordinateur seront enregistrées dans le dossier `C:\Backup` sur le même ordinateur.

  Remarque
  Dans ces scripts, le chemin d'accès de l'emplacement est sensible à la casse. Ainsi, `C:\Backup` et `C:\backup` s'affichent en tant qu'emplacements différents dans la console Cyber Protect. Utilisez également la majuscule pour la lettre du lecteur.

À propos de Secure Zone

Secure Zone est une partition sécurisée sur un disque de la machine sauvegardée. Cette partition peut stocker des sauvegardes de disques ou de fichiers sur cette machine.

Si une panne du disque devait se produire, les sauvegardes situées dans Secure Zone pourraient être perdues. C'est pourquoi Secure Zone ne devrait pas être le seul emplacement où une sauvegarde est stockée. Dans un environnement d'entreprise, Secure Zone peut être considérée comme un emplacement intermédiaire utilisé pour la sauvegarde quand un emplacement ordinaire est momentanément indisponible ou connecté sur un canal lent ou occupé.

Pourquoi utiliser Secure Zone ?

Secure Zone :

- Permet la restauration d'un disque sur le même disque où la sauvegarde du disque est située.
- Offre une méthode rentable et pratique pour la protection de données contre les dysfonctionnements logiciels, les virus et les erreurs humaines.
- Élimine le besoin d'un support séparé ou d'une connexion réseau pour sauvegarder ou restaurer les données. Ceci est particulièrement utile pour les utilisateurs itinérants.
- Peut servir en tant que destination primaire lors de l'utilisation de la réplication des sauvegardes.

Limites

- Secure Zone ne peut pas être organisée sur un Mac.
- Secure Zone est une partition sur un disque de base. Cette partition ne peut pas être organisée sur un disque dynamique ou créé en tant que volume logique (géré par LVM).
- Secure Zone est formatée avec le système de fichiers FAT32. FAT32 ayant une limite de taille par fichier de 4 Go, les sauvegardes plus volumineuses sont fractionnées lorsqu'elles sont enregistrées sur Secure Zone. Cela n'affecte pas la procédure ni la vitesse de restauration.

Comment la création de Secure Zone transforme le disque

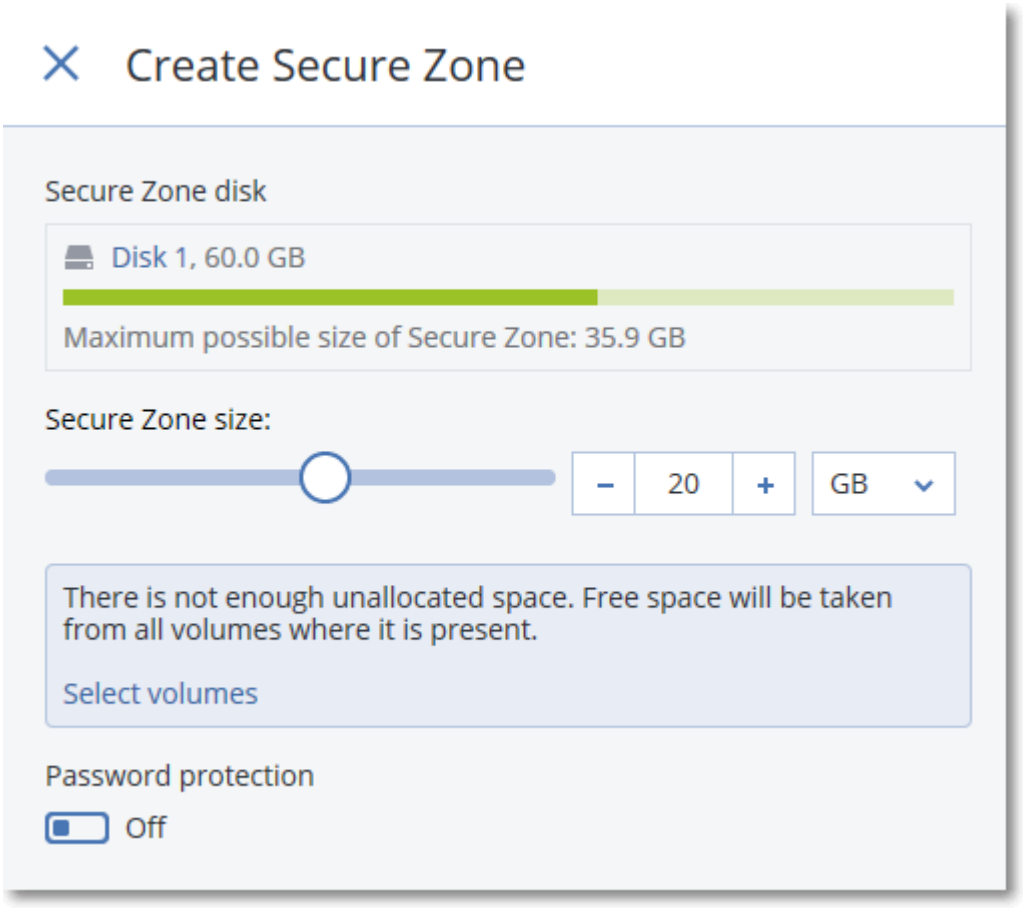
- Secure Zone est toujours créée à la fin d'un disque dur.
- S'il n'y a pas ou pas assez d'espace non alloué à la fin du disque, mais s'il y a de la place entre les volumes, les volume sont déplacés pour ajouter plus d'espace non-alloué vers la fin du disque.
- Lorsque tout l'espace non alloué est collecté mais que ce n'est toujours pas assez, le logiciel prend de l'espace libre dans les volumes que vous sélectionnez, proportionnellement à la taille des volumes.
- Cependant, il doit toujours y avoir de l'espace libre sur un volume, de façon à ce que le système d'exploitation et les opérations puissent fonctionner ; par exemple, pour la création de fichiers temporaires. Le logiciel ne réduira pas un volume où l'espace libre occupe ou occupera moins de 25 % de la taille totale du volume. Le logiciel continuera la réduction proportionnelle des volumes seulement quand tous les volumes sur le disque auront 25 % d'espace libre ou moins.

Comme il apparaît clairement ci-dessus, spécifier la taille de Secure Zone la plus grande possible n'est pas conseillé. Vous finirez avec aucun espace libre restant sur les volumes ce qui pourrait causer des problèmes sur le système d'exploitation ou les applications, tels qu'un fonctionnement instable, voire un échec du démarrage.

Important
Le déplacement ou le redimensionnement d'un volume à partir duquel le système a été démarré nécessite un redémarrage.

Comment créer Secure Zone

1. Sélectionnez la machine sur laquelle vous voulez créer Secure Zone.
2. Cliquez sur **Détails** > **Créer Secure Zone**.
3. Sous **disque Secure Zone**, cliquez sur **Sélectionner**, puis choisissez un disque dur (s'il en existe plusieurs) sur lequel vous voulez créer la zone.
   Le logiciel calcule la taille maximale possible de Secure Zone.
4. Entrez la taille de Secure Zone ou utilisez le curseur pour sélectionner n'importe quelle taille entre les tailles minimales et maximales.
   La taille minimale est d'environ 50 Mo, en fonction de la géométrie du disque dur. La taille maximale est égale à l'espace non alloué du disque plus l'espace libre total sur tous les volumes du disque.
5. Lorsque l'espace non alloué n'est pas suffisant pour la taille spécifiée, le logiciel prend de l'espace libre dans les volumes existants. Par défaut, tous les volumes sont sélectionnés. Si vous souhaitez exclure certains volumes, cliquez sur **Sélectionner volumes**. Sinon, ignorez cette étape.



6. [Facultatif] Activez la **Protection par mot de passe** et définissez un mot de passe.
   Ce mot de passe sera nécessaire pour accéder aux sauvegardes situées dans Secure Zone. La sauvegarde sur Secure Zone ne nécessite pas de mot de passe, sauf si elle est effectuée via un support de démarrage.
7. Cliquez sur **Créer**.
   Le logiciel affiche la structure de partition attendue. Cliquez sur **OK**.
8. Patientez pendant que le logiciel crée Secure Zone.

Vous pouvez à présent choisir Secure Zone sous **Où sauvegarder** lors de la création d'un plan de protection.

Comment supprimer Secure Zone

1. Sélectionnez une machine avec Secure Zone.
2. Cliquez sur **Détails**.
3. Cliquez sur l'icône en forme d'engrenage située à côté de **Secure Zone**, puis cliquez sur **Supprimer**.
4. [Facultatif] Sélectionnez les volumes auxquels ajouter l'espace libéré par la zone. Par défaut, tous les volumes sont sélectionnés.
   L'espace est réparti équitablement sur chaque volume sélectionné. Si vous ne sélectionnez aucun volume, l'espace libéré devient non alloué.

Le redimensionnement d'un volume à partir duquel le système a été démarré nécessite un redémarrage.

5. Cliquez sur **Supprimer**.

Secure Zone est alors supprimée avec toutes les sauvegardes qu'elle contient.

Planification de sauvegarde

Vous pouvez configurer une sauvegarde pour qu'elle s'exécute automatiquement à une heure spécifique, à des intervalles spécifiques ou lors d'un événement spécifique.

Les sauvegardes planifiées pour les ressources autres que de cloud à cloud s'exécutent en fonction des paramètres de fuseau horaire de la ressource sur laquelle l'agent de protection est installé. Par exemple, si vous appliquez le même plan de protection à des ressources dont les paramètres de fuseau horaire sont différents, les sauvegardes démarrent en fonction du fuseau horaire local de chaque ressource.

La planification d'une sauvegarde comprend les actions suivantes :

- Sélection d'un modèle de sauvegarde
- Configuration de l'heure ou sélection de l'événement déclenchant la sauvegarde
- Configuration du paramètre facultatif et des conditions de démarrage

Modèles de sauvegarde

Le modèle de sauvegarde fait partie de la planification du plan de protection ; il définit le type de sauvegarde (complète, différentielle ou incrémentielle) créé, ainsi que le moment de son exécution. Vous pouvez sélectionner l'un des modèles de sauvegarde prédéfinis ou créer un modèle personnalisé.

Les modèles et types de sauvegarde disponibles dépendent de l'emplacement et de la source de la sauvegarde. Par exemple, une sauvegarde différentielle n'est pas disponible lorsque vous sauvegardez les données SQL ou Exchange, ou l'état du système. Le modèle **Toujours incrémentielle (fichier unique)** n'est pas pris en charge pour les lecteurs de bandes.

Modèle de sauvegarde	Description	Éléments configurables
Toujours incrémentielle (fichier unique)	La première sauvegarde est complète ; elle peut donc prendre un certain temps. Les sauvegardes suivantes seront incrémentielles et considérablement plus rapides.	• Type de planification : mensuelle, hebdomadaire, quotidienne, horaire

Modèle de sauvegarde	Description	Éléments configurables
	Les sauvegardes utilisent le format de sauvegarde sous forme d'un fichier unique[1]*. Par défaut, les sauvegardes s'effectuent de manière quotidienne, du lundi au vendredi. Nous vous recommandons d'utiliser ce modèle lorsque vous stockez vos sauvegardes dans le stockage dans le cloud, car les sauvegardes incrémentielles sont rapides et nécessitent un trafic réseau moindre.	• Déclencheur de sauvegarde : heure ou événement • Heure de démarrage • Conditions de démarrage • Options supplémentaires
Toujours complète	Toutes les sauvegardes de l'ensemble de sauvegarde sont complètes. Par défaut, les sauvegardes s'effectuent de manière quotidienne, du lundi au vendredi.	• Type de planification : mensuelle, hebdomadaire, quotidienne, horaire • Déclencheur de sauvegarde : heure ou événement • Heure de démarrage • Conditions de démarrage • Options supplémentaires
Complète hebdomadaire, incrémentielle journalière	Une sauvegarde complète est créée une fois par semaine et les autres sauvegardes sont incrémentielles. La première sauvegarde est complète et les autres sauvegardes planifiées pendant la semaine sont incrémentielles ; ce cycle se répète ensuite. Pour sélectionner le jour de création de la sauvegarde complète hebdomadaire, cliquez dans le plan de protection sur l'icône représentant un engrenage, puis accédez à **Options de sauvegarde** > **Sauvegarde hebdomadaire**. Par défaut, les sauvegardes s'effectuent de	• Déclencheur de sauvegarde : heure ou événement • Heure de démarrage • Conditions de démarrage • Options supplémentaires

[1]Format de sauvegarde, pour lequel les sauvegardes complètes et incrémentielles suivantes sont enregistrées sous forme d'un fichier .tibx unique. Ce format accélère la vitesse de la méthode de sauvegarde incrémentielle, tout en évitant ses principaux inconvénients et la suppression complexe de sauvegardes ayant expiré. Le logiciel définit les blocs de sauvegarde utilisés par des sauvegardes ayant expiré comme étant « libres » et y inscrit les nouvelles sauvegardes. Ce procédé permet un nettoyage extrêmement rapide et une consommation minimale des ressources. Le format de sauvegarde sous forme de fichier unique n'est pas disponible lorsque la sauvegarde est effectuée sur des emplacements qui ne prennent pas en charge les lectures et écritures en accès aléatoire.

Modèle de sauvegarde	Description	Éléments configurables
	manière quotidienne, du lundi au vendredi.	
Complète mensuelle, différentielle hebdomadaire, incrémentielle journalière (GFS)	Par défaut, les sauvegardes incrémentielles s'effectuent de manière quotidienne, du lundi au vendredi. Les sauvegardes différentielles sont effectuées tous les samedis. Les sauvegardes complètes sont effectuées le premier jour de chaque mois. **Remarque** Ceci est un schéma personnalisé prédéfini. Dans le plan de protection, il est affiché comme étant **Personnalisé**.	• Modifier la planification existante par type de sauvegarde : ◦ Type de planification : mensuelle, hebdomadaire, quotidienne, horaire ◦ Déclencheur de sauvegarde : heure ou événement ◦ Heure de démarrage ◦ Conditions de démarrage ◦ Options supplémentaires • Ajouter de nouvelles planifications par type de sauvegarde
Personnalisé	Vous devez sélectionner les types de sauvegarde (complète, différentielle et incrémentielle), puis configurer une planification distincte pour chacune d'entre elles*.	• Modifier la planification existante par type de sauvegarde : ◦ Type de planification : mensuelle, hebdomadaire, quotidienne, horaire ◦ Déclencheur de sauvegarde : heure ou événement ◦ Heure de démarrage ◦ Conditions de démarrage ◦ Options supplémentaires

Modèle de sauvegarde	Description	Éléments configurables
		• Ajouter de nouvelles planifications par type de sauvegarde

* Après avoir créé un plan de protection, vous ne pouvez plus passer du modèle **Toujours incrémentielle (fichier unique)** à l'un des autres modèles de sauvegarde, et inversement. Le modèle **Toujours incrémentielle (fichier unique)** est un modèle de fichier unique et les autres modèles sont des modèles de fichiers multiples. Si vous souhaitez passer d'un format à un autre, créez un plan de protection.

Types de sauvegarde

Les types de sauvegarde suivants sont disponibles :

- Complète : une sauvegarde complète contient toutes les données source. Cette sauvegarde se suffit à elle-même. Pour restaurer les données, vous n'avez pas besoin d'accéder à d'autres sauvegardes.

  Remarque
  La première sauvegarde créée par un plan de protection est toujours une sauvegarde complète.

- Incrémentielle : une sauvegarde incrémentielle stocke les modifications apportées à des données depuis la dernière sauvegarde, qu'elle soit complète, différentielle ou incrémentielle. Pour restaurer les données, vous aurez besoin de toute la chaîne de sauvegardes, jusqu'à la sauvegarde complète initiale, dont dépend la sauvegarde incrémentielle.
- Différentielle : une sauvegarde différentielle stocke les modifications apportées aux données depuis la dernière sauvegarde complète. Pour restaurer les données, vous aurez besoin de la sauvegarde différentielle et de la sauvegarde complète correspondante dont dépend cette sauvegarde différentielle.

Exécution d'une sauvegarde à partir d'une planification

Pour exécuter une sauvegarde automatiquement, à une heure spécifique ou lors d'un événement spécifique, activez une planification dans le plan de protection.

Pour activer une planification

1. Dans le plan de protection, développez le module **Sauvegarde**.
2. Cliquez sur **Planification**.
3. Activez le commutateur de planification.
4. Sélectionnez le modèle de sauvegarde.
5. Configurez la planification en fonction de vos besoins, puis cliquez sur **Terminé**.

Pour plus d'informations sur les options de planification disponibles, voir "Planifier selon l'horaire" (p. 440) et "Planifier par événement" (p. 442).

6. [Facultatif] Configurez les conditions de démarrage ou d'autres options de planification.
7. Enregistrez le plan de protection.

En conséquence, une opération de sauvegarde démarre toutes les heures lorsque les conditions de planification sont satisfaites.

Pour désactiver une planification

1. Dans le plan de protection, développez le module **Sauvegarde**.
2. Cliquez sur **Planification**.
3. Désactivez le commutateur de planification.
4. Enregistrez le plan de protection.

Par conséquent, la sauvegarde ne s'exécute que si vous la démarrez manuellement.

Remarque
Si la planification est désactivée, les règles de rétention ne sont pas appliquées automatiquement. Pour les appliquer, exécutez la sauvegarde manuellement.

Planifier selon l'horaire

Le tableau suivant récapitule les options de planification basées sur l'heure. La disponibilité de ces options dépend du modèle de sauvegarde. Pour plus d'informations, voir "Modèles de sauvegarde" (p. 436).

Option	Description	Exemples
Mens.	Sélectionnez les mois, les jours du mois ou de la semaine, puis l'heure de début de la sauvegarde.	Exécuter une sauvegarde le 1er janvier et le 3 février à 00 h 00. Exécuter une sauvegarde le premier jour de chaque mois à 10 h 00. Exécuter une sauvegarde le 1er mars, le 5 mars, le 1er avril et le 5 avril à 09 h 00. Exécuter une sauvegarde les deuxième et troisième vendredis de chaque mois à 11 h 00. Exécuter une sauvegarde le dernier mercredi du mois à 22 h 30.
Hebdo.	Sélectionnez les jours de la semaine, puis l'heure de début de la sauvegarde.	Exécuter une sauvegarde du lundi au vendredi à 10 h 00. Exécuter une sauvegarde le lundi à 23 h

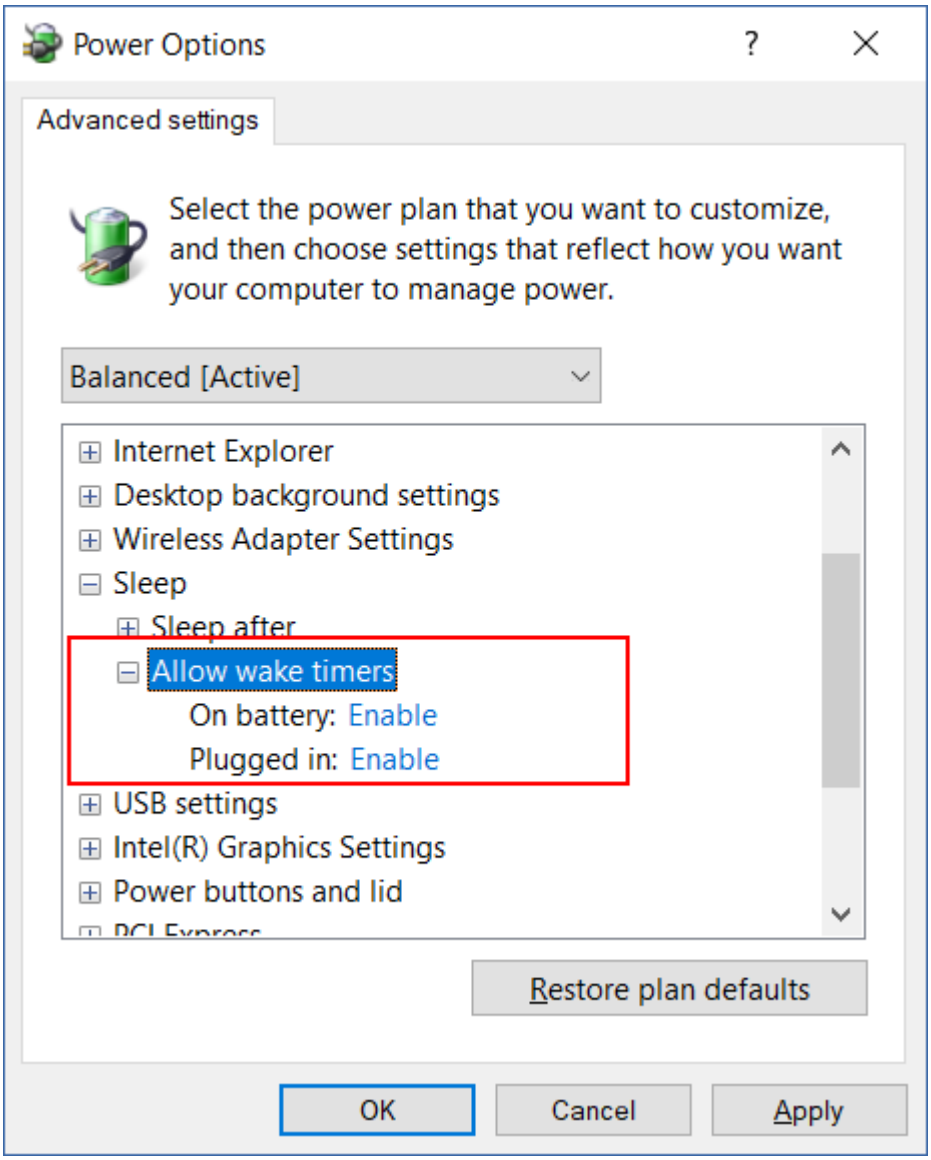
Option	Description	Exemples
		00. Exécuter une sauvegarde le mardi et le samedi à 08 h 00.
Journ.	Sélectionnez les jours (Tous les jours ou Les jours de la semaine), puis l'heure de début de la sauvegarde.	Exécuter une sauvegarde tous les jours à 11 h 45. Exécuter une sauvegarde du lundi au vendredi à 21 h 30.
Par heure	Sélectionnez les jours de la semaine, puis un intervalle de temps entre deux sauvegardes consécutives, ainsi que la plage de temps au cours de laquelle les sauvegardes s'exécutent. Lorsque vous configurez l'intervalle en minutes, vous pouvez sélectionner un intervalle suggéré entre 10 et 60 minutes, ou indiquer un intervalle personnalisé, par exemple, 45 ou 75 minutes.	Exécuter une sauvegarde toutes les heures entre 08 h 00 et 18 h 00, du lundi au vendredi. Exécuter une sauvegarde toutes les 3 heures entre 01 h 00 et 18 h 00, le samedi et le dimanche.

Options supplémentaires

Lorsque vous planifiez une sauvegarde en fonction de l'heure, les options de planification supplémentaires suivantes sont disponibles.

Pour y accéder, cliquez dans le volet **Planification** sur **Afficher plus**.

- **Si la machine est arrêtée, exécutez les tâches ratées lors du démarrage de la machine**
  Paramètre par défaut : Désactivé.
- **Empêcher l'activation du mode veille ou veille prolongée pendant la sauvegarde**
  Cette option ne s'applique qu'aux ordinateurs exécutant Windows.
  Paramètre par défaut : Activé.
- **Sortir du mode veille ou veille prolongée pour démarrer une sauvegarde planifiée**
  Cette option ne s'applique qu'aux ordinateurs exécutant Windows, dans les plans d'alimentation pour lesquels l'option **Autoriser les minuteurs de sortie de veille** est activée.



Cette option n'utilise pas la fonctionnalité Wake-on-LAN et ne s'applique pas aux ordinateurs éteints.

Paramètre par défaut : Désactivé.

Planifier par événement

Pour configurer une sauvegarde qui s'exécute lors d'un événement spécifique, sélectionnez l'une des options suivantes.

Option	Description	Exemples
Lors du temps écoulé depuis la dernière sauvegarde	Une sauvegarde démarre après une période spécifiée qui suit la dernière sauvegarde réussie.	Exécutez une sauvegarde un jour après la dernière sauvegarde réussie. Exécutez une sauvegarde quatre heures après la dernière sauvegarde réussie.

Option	Description	Exemples
	Remarque Cette option dépend du résultat de la sauvegarde précédente. En cas d'échec d'une sauvegarde, la sauvegarde suivante ne démarre pas automatiquement. Dans ce cas, vous devez exécuter la sauvegarde manuellement et veillez à ce qu'elle se termine avec succès pour réinitialiser la planification.	
Lorsqu'un utilisateur se connecte au système	Une sauvegarde démarre lorsqu'un utilisateur se connecte à l'ordinateur. Vous pouvez configurer cette option pour toutes les connexions ou pour la connexion d'un utilisateur spécifique. **Remarque** Une connexion à l'aide d'un profil utilisateur temporaire ne démarre pas de sauvegarde.	Exécuter une sauvegarde lorsque l'utilisateur Jean Dupont se connecte.
Lorsqu'un utilisateur se déconnecte du système	Une sauvegarde démarre lorsqu'un utilisateur se déconnecte de l'ordinateur. Vous pouvez configurer cette option pour toutes les déconnexions ou pour la déconnexion d'un utilisateur spécifique. **Remarque** Une déconnexion d'un profil utilisateur temporaire ne démarre pas de sauvegarde. L'arrêt d'un ordinateur ne démarre pas de sauvegarde.	Exécuter une sauvegarde à la déconnexion de chaque utilisateur.
Au démarrage du système	Une sauvegarde s'exécute lorsque la machine protégée démarre.	Exécuter une sauvegarde lorsqu'un utilisateur démarre l'ordinateur.
À l'arrêt du système	Une sauvegarde s'exécute lorsque la machine protégée s'arrête.	Exécuter une sauvegarde lorsqu'un utilisateur arrête l'ordinateur.
Lors d'un événement du Journal des événements Windows	Une sauvegarde s'exécute lors d'un événement Windows que vous spécifiez.	Exécuter une sauvegarde lorsque l'événement 7 de type erreur, avec la source disque est enregistré dans le journal système Windows.

La disponibilité de ces options dépend de la source de la sauvegarde et du système d'exploitation des ressources protégées. Le tableau ci-dessous répertorie les options disponibles pour Windows, Linux et macOS.

L'événement	Source de sauvegarde (Quoi sauvegarder)					
	Toute la machine, Disques/volumes ou Fichiers/dossiers (machines physiques)	**Toute la machine ou Disques/volumes (machines virtuelles)**	**Configuration ESXi**	**Boîtes aux lettres Microsoft 365**	**Bases de données et boîtes aux lettres Exchange**	**Bases de données SQL**
Lors du temps écoulé depuis la dernière sauvegarde	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Lorsqu'un utilisateur se connecte au système	Windows	Sans Objet	Sans Objet	Sans Objet	Sans Objet	Sans Objet
Lorsqu'un utilisateur se déconnecte du système	Windows	Sans Objet	Sans Objet	Sans Objet	Sans Objet	Sans Objet
Au démarrage du système	Windows, Linux, macOS	Sans Objet	Sans Objet	Sans Objet	Sans Objet	Sans Objet
À l'arrêt du système	Windows	Sans Objet	Sans Objet	Sans Objet	Sans Objet	Sans Objet
Lors d'un événement du Journal des événements Windows	Windows	Sans Objet	Sans Objet	Windows	Windows	Windows

Lors d’un événement du Journal des événements Windows

Vous pouvez exécuter une sauvegarde automatiquement lorsqu'un événement spécifique est enregistré dans un Journal des événements Windows tel que le journal des applications, le journal de sécurité ou le journal système.

Remarque
Vous pouvez parcourir les événements et afficher leurs propriétés dans **Gestion de l'ordinateur** > **Observateur d'événements** sous Windows. Pour ouvrir le journal de sécurité, vous devez disposer des droits d'administrateur.

Paramètres d'événement

Le tableau suivant récapitule les paramètres que vous devez indiquer lors de la configuration de l'option **Lors d'un événement du Journal des événements Windows**.

Paramètre	Description
Nom du journal	Nom du journal. Sélectionnez le nom d'un journal standard (Application, Sécurité ou Système) ou saisissez un autre nom. Par exemple, Sessions Microsoft Office.
Source d'événement	L'événement source indique le programme ou le composant système qui a causé l'événement. Par exemple, disk. Toute source d'événement contenant la chaîne de texte spécifiée déclenchera la sauvegarde planifiée. Cette option n'est pas sensible à la casse. Par exemple, si vous spécifiez `service`, les sources d'événement Gestionnaire de contrôle du service et Time-Service déclencheront toutes les deux une sauvegarde.
Type d'événement	Type de l'événement : Erreur, Avertissement, Information, Succès de l'audit ou Échec de l'audit.
Identifiant d'événement	L'ID d'événement identifie une sorte particulière d'événement dans une source d'événement. Par exemple, un événement Erreur avec la source d'événement disque et l'identifiant d'événement 7 se produit lorsque Windows découvre un bloc défectueux sur un disque, alors qu'un événement Erreur avec la source d'événement disque et l'identifiant d'événement 15 se produit quand un disque n'est pas prêt pour l'accès.

Exemple : Sauvegarde d'urgence en cas de blocs défaillants sur le disque dur

Un ou plusieurs blocs défectueux sur un disque dur indiquent une défaillance imminente. C'est la raison pour laquelle vous souhaiterez peut-être créer une sauvegarde en cas de détection d'un bloc défaillant.

Lorsque Windows détecte un bloc défaillant sur le disque, un événement d'erreur avec la source d'événement disque de et le numéro d'événement 7 est enregistré dans le journal système. Dans le plan de protection, configurez la planification suivante :

- Planification : Lors d'un événement du Journal des événements Windows
- Nom de journal : Système
- Source d'événement : disque
- Type d'événement : Erreur
- ID d'événement : 7

Important
Pour que la sauvegarde s'effectue malgré ces blocs défaillants, accédez à **Options de sauvegarde** > **Gestion erreurs**, puis cochez la case **Ignorer les secteurs défectueux**.

Conditions de démarrage

Pour qu'une sauvegarde s'exécute uniquement si des conditions spécifiques sont remplies, configurez une ou plusieurs conditions de démarrage. Si vous configurez plusieurs conditions, toutes devront être remplies simultanément pour que la sauvegarde puisse démarrer. Vous pouvez spécifier une période après laquelle les sauvegardes s'exécuteront, que les conditions soient remplies ou non. Pour plus d'informations sur cette option de sauvegarde, voir "Conditions de démarrage de tâche" (p. 513).

Les conditions de démarrage ne s'appliquent pas lorsque vous démarrez une sauvegarde manuellement.

Le tableau ci-dessous affiche les conditions de démarrage disponibles pour diverses données sous les systèmes d'exploitation Windows, Linux et macOS.

Condition de démarrage	Source de sauvegarde (Quoi sauvegarder)					
	Toute la machine, Disques/volumes ou Fichiers/dossiers (machines physiques)	**Toute la machine ou Disques/volumes (machines virtuelles)**	**Configuration ESXi**	**Boîtes aux lettres Microsoft 365**	**Bases de données et boîtes aux lettres Exchange**	**Bases de données SQL**
L'utilisateur est inactif	Windows	Sans Objet	Sans Objet	Sans Objet	Sans Objet	Sans Objet
L'hôte de l'emplacement de la sauvegarde est disponible	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Utilisateurs déconnectés	Windows	Sans Objet	Sans Objet	Sans	Sans	Sans

Condition de démarrage	Source de sauvegarde (Quoi sauvegarder)					
	Toute la machine, Disques/volumes ou Fichiers/dossiers (machines physiques)	Toute la machine ou Disques/volumes (machines virtuelles)	Configuration ESXi	Boîtes aux lettres Microsoft 365	Bases de données et boîtes aux lettres Exchange	Bases de données SQL
				Objet	Objet	Objet
Tient dans l'intervalle de temps	Windows, Linux, macOS	Windows, Linux	Sans Objet	Sans Objet	Sans Objet	Sans Objet
Économiser de la batterie	Windows	Sans Objet	Sans Objet	Sans Objet	Sans Objet	Sans Objet
Ne pas démarrer pendant une connexion mesurée	Windows	Sans Objet	Sans Objet	Sans Objet	Sans Objet	Sans Objet
Ne pas démarrer pendant une connexion aux réseaux Wi-Fi suivants	Windows	Sans Objet	Sans Objet	Sans Objet	Sans Objet	Sans Objet
Vérifier l'adresse IP du terminal	Windows	Sans Objet	Sans Objet	Sans Objet	Sans Objet	Sans Objet

L'utilisateur est inactif

« L'utilisateur est inactif » signifie qu'un écran de veille s'exécute sur la machine ou que la machine est verrouillée.

Exemple

Exécutez une sauvegarde tous les jours à 21 h 00, de préférence lorsque l'utilisateur est inactif. Si l'utilisateur est toujours actif à 23 h 00, exécutez quand même la sauvegarde.

- Planification : **Quotidiennement**, **Exécuter tous les jours**. Démarrage à : **21 h 00**.
- Condition : **L'utilisateur est inactif**.

- Conditions de démarrage de la sauvegarde : **Patienter jusqu'à ce que les conditions soient remplies**, **Lancer quand même la tâche après 2** heures.

En conséquence :

- Si l'utilisateur devient inactif avant 21 h 00, la sauvegarde débute à 21 h 00.
- Si l'utilisateur devient inactif entre 21 h 00 et 23 h 00, la sauvegarde démarre immédiatement.
- Si l'utilisateur est encore actif à 23 h 00, la sauvegarde débute à 23 h 00.

L'hôte de l'emplacement de la sauvegarde est disponible

« L'hôte de l'emplacement de la sauvegarde est disponible » signifie que l'ordinateur hébergeant l'emplacement de la sauvegarde est disponible sur le réseau.

Cette condition s'applique aux dossiers réseau, au stockage dans le cloud et aux emplacements gérés par un nœud de stockage.

Cette condition ne couvre pas la disponibilité de l'emplacement en soi, seulement la disponibilité de l'hôte. Par exemple, si l'hôte est disponible, mais que le dossier du réseau sur cet hôte n'est pas partagé ou que les accréditations pour ce dossier ne sont plus valides, la condition est toujours considérée comme étant remplie.

Exemple

Vous exécutez des sauvegardes dans un dossier réseau tous les jours ouvrés à 21 h 00. Si l'ordinateur qui héberge le dossier n'est pas disponible à ce moment-là (à cause, par exemple, d'un travail de maintenance), ignorez la sauvegarde et attendez le démarrage planifié du jour ouvré suivant.

- Planification : **Quotidienne**, **Exécuter de lundi à vendredi**. Démarrage à : **21 h 00**.
- Condition : **L'hôte de l'emplacement de la sauvegarde est disponible**.
- Conditions de démarrage de la sauvegarde : **Ignorer la sauvegarde planifiée**.

En conséquence :

- Si l'hôte est disponible à 21 h 00, la sauvegarde débute immédiatement.
- Si l'hôte n'est pas disponible à 21 h 00, la sauvegarde débute le jour ouvré suivant (si l'hôte est disponible à 21 h 00 ce jour-là).
- Si l'hôte n'est jamais disponible lors des jours ouvrés à 21 h 00, la sauvegarde ne démarre jamais.

Utilisateurs déconnectés

Utilisez cette condition de démarrage pour reporter une sauvegarde jusqu'à ce que tous les utilisateurs se déconnectent d'un ordinateur Windows.

Exemple

Vous exécutez une sauvegarde tous les vendredis à 20 h 00, de préférence lorsque tous les utilisateurs sont déconnectés. Si l'un des utilisateurs est toujours connecté à 23 h 00, lancer quand même la sauvegarde.

- Planification : **Hebdomadaire**, le vendredi. Démarrage à : **20 h 00**.
- Condition : **Utilisateurs déconnectés**.
- Conditions de démarrage de la sauvegarde : **Patienter jusqu'à ce que les conditions soient remplies**, **Lancer quand même la sauvegarde après 3** heures.

En conséquence :

- Si tous les utilisateurs sont déconnectés à 20 h 00, la sauvegarde débute à 20 h 00.
- Si le dernier utilisateur se déconnecte entre 20 h 00 et 23 h 00, la sauvegarde démarre immédiatement.
- Si des utilisateurs sont encore connectés à 23 h 00, la sauvegarde débute à 23 h 00.

Tient dans l'intervalle de temps

Utilisez cette condition de démarrage pour limiter le début d'une sauvegarde à un intervalle spécifié.

Exemple

Une société sauvegarde des données utilisateur et des serveurs dans différents emplacements d'un même stockage réseau.

Le jour ouvré débute à 08 h 00 et se termine à 17 h 00. Les données utilisateur doivent être sauvegardées dès que les utilisateurs se déconnectent, mais pas avant 16 h 30.

Les serveurs de la société sont sauvegardés tous les jours à 23 h 00. Les données utilisateur doivent être sauvegardées de préférence avant 23 h 00 afin de libérer la bande passante du réseau pour les sauvegardes des serveurs.

La sauvegarde des données utilisateur ne prend pas plus d'une heure ; par conséquent, l'heure de début de la dernière sauvegarde est 22 h 00. Si un utilisateur est toujours connecté dans l'intervalle de temps spécifié, ou se déconnecte à un autre moment, la sauvegarde des données utilisateur doit être ignorée.

- Événement : **Lorsqu'un utilisateur se déconnecte du système**. Spécifiez le compte utilisateur : **Tout utilisateur**.
- Condition : **Tient dans l'intervalle de temps** de **16 h 30** à **22 h 00**.
- Conditions de démarrage de la sauvegarde : **Ignorer la sauvegarde planifiée**.

En conséquence :

- Si l'utilisateur se déconnecte entre 16 h 30 et 22 h 00, la sauvegarde démarre immédiatement.
- Si l'utilisateur se déconnecte à un autre moment, la sauvegarde est ignorée.

Économiser de la batterie

Utilisez cette condition de démarrage pour empêcher une sauvegarde si un ordinateur (portable ou tablette, par exemple) n'est pas connecté à une source d'alimentation. En fonction de la valeur de l'option Conditions de démarrage de la sauvegarde, la sauvegarde ignorée démarrera ou ne démarrera pas après la connexion de l'ordinateur à une source d'alimentation.

Les options suivantes sont disponibles :

- **Ne pas démarrer lors d'une alimentation sur batterie**
  Une sauvegarde démarrera uniquement si l'ordinateur est connecté à une source d'alimentation.
- **Démarrer pendant l'alimentation sur batterie si le niveau de batterie est supérieur à**
  Une sauvegarde démarrera si l'ordinateur est connecté à une source d'alimentation ou si le niveau de batterie est supérieur à la valeur spécifiée.

Exemple

Vous sauvegardez vos données tous les jours ouvrés à 21 h 00. Si votre ordinateur n'est pas connecté à une source d'alimentation, il est préférable d'ignorer la sauvegarde pour économiser de la batterie et d'attendre que vous le connectiez à une source d'alimentation.

- Planification : **Quotidienne**, **Exécuter de lundi à vendredi**. Démarrage à : **21 h 00**.
- Condition : **Économiser de la batterie**, **Ne pas démarrer lors d'une alimentation sur batterie**.
- Conditions de démarrage de la sauvegarde : **Attendre que les conditions soient satisfaites**.

En conséquence :

- Si l'ordinateur est connecté à une source d'alimentation à 21 h 00, la sauvegarde démarre immédiatement.
- Si l'ordinateur s'exécute sur batterie à 21 h 00, la sauvegarde démarre lorsque vous le connectez à une source d'alimentation.

Ne pas démarrer pendant une connexion mesurée

Utilisez cette condition de démarrage pour empêcher une sauvegarde (y compris une sauvegarde sur un disque local) si l'ordinateur est connecté à Internet via une connexion mesurée dans Windows. Pour plus d'informations sur les connexions mesurées dans Windows, consultez l'article https://support.microsoft.com/en-us/help/17452/windows-metered-internet-connections-faq.

La condition de démarrage supplémentaire **Ne pas démarrer pendant une connexion aux réseaux Wi-Fi suivants** est activée automatiquement lorsque vous activez la condition **Ne pas démarrer pendant une connexion mesurée**. Il s'agit d'une mesure supplémentaire qui empêche

les sauvegardes via une connexion mobile. Les noms de réseaux suivants sont spécifiés par défaut : android, téléphone, mobile et modem.

Pour supprimer ces noms de la liste, cliquez sur le symbole X. Pour ajouter un nouveau nom, saisissez-le dans le champ vide.

Exemple

Vous sauvegardez vos données tous les jours ouvrés à 21 h 00. Si l'ordinateur est connecté à Internet via une connexion mesurée, il est préférable d'ignorer la sauvegarde pour économiser du trafic réseau et d'attendre le démarrage planifié le jour ouvré suivant.

- Planification : **Quotidienne**, **Exécuter de lundi à vendredi**. Démarrage à : **21 h 00**.
- Condition : **Ne pas démarrer pendant une connexion mesurée**.
- Conditions de démarrage de la sauvegarde : **Ignorer la sauvegarde planifiée**.

En conséquence :

- À 21 h 00, si l'ordinateur n'est pas connecté à Internet par l'intermédiaire d'une connexion mesurée, la sauvegarde démarre immédiatement.
- À 21 h 00, si l'ordinateur est connecté à Internet par l'intermédiaire d'une connexion mesurée, la sauvegarde démarre le jour ouvré suivant.
- Si l'ordinateur est toujours connecté à Internet par l'intermédiaire d'une connexion mesurée les jours ouvrés à 21 h 00, la sauvegarde ne démarre jamais.

Ne pas démarrer pendant une connexion aux réseaux Wi-Fi suivants

Utilisez cette condition de démarrage pour empêcher une sauvegarde (y compris une sauvegarde sur un disque local) si l'ordinateur est connecté à l'un des réseaux sans fil spécifiés (par exemple, si vous souhaitez limiter les sauvegardes via une connexion mobile).

Vous pouvez spécifier les noms des réseaux Wi-Fi, également connus sous le nom de Service Set Identifiers (SSID). La restriction s'applique à tous les réseaux qui contiennent le nom spécifié comme sous-chaîne dans leur nom, quelle que soit la casse. Par exemple, si vous spécifiez `phone` comme nom de réseau, la sauvegarde ne démarrera pas lorsque le ordinateur sera connecté à l'un des réseaux suivants : `John's iPhone`, `phone_wifi` ou `my_PHONE_wifi`.

La condition de démarrage **Ne pas démarrer pendant une connexion aux réseaux Wi-Fi suivants** est activée automatiquement lorsque vous activez la condition **Ne pas démarrer pendant une connexion mesurée**. Les noms de réseaux suivants sont spécifiés par défaut : android, `téléphone`, `mobile` et modem.

Pour supprimer ces noms de la liste, cliquez sur le symbole X. Pour ajouter un nouveau nom, saisissez-le dans le champ vide.

Exemple

Vous sauvegardez vos données tous les jours ouvrés à 21 h 00. Si l'ordinateur est connecté à Internet via une connexion mobile, il est préférable d'ignorer la sauvegarde et d'attendre le démarrage programmé le jour ouvré suivant.

- Planification : **Quotidienne**, **Exécuter de lundi à vendredi**. Démarrage à : **21 h 00**.
- Condition : **Ne pas démarrer pendant une connexion aux réseaux Wi-Fi suivants**, **Nom du réseau** : `<SSID du réseau>`.
- Conditions de démarrage de la sauvegarde : **Ignorer la sauvegarde planifiée**.

En conséquence :

- Si l'ordinateur n'est pas connecté au réseau spécifié à 21 h 00, la sauvegarde démarre immédiatement.
- Si l'ordinateur est connecté au réseau spécifié à 21 h 00, la sauvegarde démarre le jour ouvré suivant.
- Si l'ordinateur est toujours connecté au réseau spécifié les jours ouvrés à 21 h 00, la sauvegarde ne démarre jamais.

Vérifier l'adresse IP du terminal

Utilisez cette condition de démarrage pour empêcher une sauvegarde (y compris une sauvegarde sur un disque local) si l'une des adresses IP de l'ordinateur est située dans ou en dehors de la plage d'adresses IP spécifiée. Par exemple, vous pouvez éviter les frais élevés de transit de données lors de la sauvegarde d'ordinateurs d'utilisateurs à l'étranger, ou empêcher les sauvegardes sur connexion VPN (Virtual Private Network).

Les options suivantes sont disponibles :

- **Démarrer si en dehors de la plage d'adresses IP**
- **Démarrer si dans la plage d'adresses IP**

Quelle que soit l'option, vous pouvez spécifier plusieurs plages. Prend en charge uniquement les adresses IPv4.

Exemple

Vous sauvegardez vos données tous les jours ouvrés à 21 h 00. Si le terminal est connecté au réseau de l'entreprise via un tunnel VPN, il est préférable d'ignorer la sauvegarde.

- Planification : **Quotidienne**, **Exécuter de lundi à vendredi**. Démarrage à **21 h 00**.
- Condition : **Vérifier l'adresse IP du terminal**, **Démarrer si en dehors de la plage d'adresses IP**, **De** : `<début de la plage d'adresses IP VPN>`, **À** : `<fin de la plage d'adresses IP VPN>`.
- Conditions de démarrage de la sauvegarde : **Attendre que les conditions soient satisfaites**.

En conséquence :

- Si l'adresse IP de l'ordinateur se situe en dehors de la plage spécifiée à 21 h 00, la sauvegarde démarre immédiatement.
- Si l'adresse IP de l'ordinateur se situe dans la plage spécifiée à 21 h 00, la sauvegarde démarre lorsque l'ordinateur obtient une adresse IP non-VPN.
- Si l'adresse IP de l'ordinateur se situe toujours dans la plage spécifiée à 21 h 00, la sauvegarde ne démarre jamais.

Options de planification supplémentaires

Vous pouvez configurer les sauvegardes pour qu'elles s'exécutent uniquement si des conditions spécifiques sont remplies, uniquement pendant une période spécifiée ou avec un retard par rapport à la planification.

Pour configurer des conditions de démarrage

1. Dans le plan de protection, développez le module **Sauvegarde**.
2. Cliquez sur **Planification**.
3. Dans le volet **Planification**, cliquez sur click **Afficher plus**.
4. Cochez les cases situées à côté des conditions de démarrage que vous souhaitez inclure, puis cliquez sur **Terminé**.
   Pour plus d'informations sur les conditions de démarrage disponibles et sur leur configuration, voir "Conditions de démarrage" (p. 446).
5. Enregistrez le plan de protection.

Pour configurer un intervalle de temps

1. Dans le plan de protection, développez le module **Sauvegarde**.
2. Cliquez sur **Planification**.
3. Cochez la case **Exécuter le plan dans une plage de dates**.
4. Spécifiez la période en fonction de vos besoins, puis cliquez sur **Terminé**.
5. Enregistrez le plan de protection.

Par conséquent, les sauvegardes s'exécuteront uniquement pendant la période spécifiée.

Pour configurer un délai

Afin d'éviter toute charge excessive sur le réseau lorsque vous sauvegardez plusieurs ressources dans un emplacement réseau, un petit délai aléatoire est configuré comme option de sauvegarde. Vous pouvez le désactiver ou modifier son paramètre.

1. Dans le plan de protection, développez le module **Sauvegarde**.
2. Cliquez sur **Options de sauvegarde**, puis sélectionnez **Planification**.
   La valeur de délai de chaque ressource est sélectionnée de façon aléatoire entre zéro et la valeur maximale que vous spécifiez. Par défaut, la valeur maximale est de 30 minutes.
   Pour plus d'informations sur cette option de sauvegarde, voir "Planification" (p. 511)

La valeur du délai pour chaque ressource est calculée lorsque vous appliquez le plan de protection à cette ressource, et reste la même tant que vous n'avez pas modifié la valeur de délai maximal.

3. Spécifiez la période en fonction de vos besoins, puis cliquez sur **Terminé**.
4. Enregistrez le plan de protection.

Exécution manuelle d'une sauvegarde

Vous pouvez exécuter manuellement des sauvegardes planifiées et non planifiées.

Pour exécuter une sauvegarde manuellement

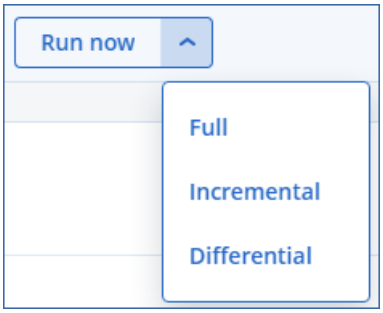
1. Dans la console Cyber Protect, accédez à **Terminaux**.
2. Sélectionnez la ressource pour laquelle vous souhaitez exécuter une sauvegarde, puis cliquez sur **Protéger**.
3. Sélectionnez le plan de protection dont vous souhaitez créer la sauvegarde.

   Si aucun plan de protection n'est appliqué à la ressource, appliquez un plan existant ou créez-en un nouveau.

   Pour plus d'informations sur la création d'un plan de protection, voir "Création d'un plan de protection" (p. 223).
4. [Pour créer le type de sauvegarde par défaut] Dans le plan de protection, cliquez sur l'icône **Exécuter maintenant**.

   Vous pouvez également, dans le plan de protection, développer le module **Sauvegarde**, puis cliquer sur le bouton **Exécuter maintenant**.
5. [Pour créer un type de sauvegarde spécifique] Dans le plan de protection, développez le module **Sauvegarde**, cliquez sur la flèche située à côté du bouton **Exécuter maintenant**, puis sélectionnez le type de sauvegarde.

Remarque
La sélection du type n'est pas disponible pour les modèles de sauvegarde qui utilisent une seule méthode de sauvegarde, par exemple, **Toujours incrémentielle (fichier unique)** ou **Toujours complète**.

Par conséquent, l'opération de sauvegarde démarre. Vous pouvez vérifier sa progression et ses résultats dans l'onglet **Terminaux**, colonne **État**.

Règles de rétention

Pour supprimer automatiquement les anciennes sauvegardes, configurez les règles de rétention de sauvegarde dans le plan de protection.

Vous pouvez baser les règles de rétention sur l'une des propriétés de sauvegarde suivantes :

- Numéro
- Âge
- Taille

Les règles de rétention disponibles et leurs options dépendent du schéma de sauvegarde. Les règles s'appliquent également aux agents, aux ressources et aux sauvegardes de cloud à cloud. Pour plus d'informations, voir "Règles de rétention en fonction du modèle de sauvegarde" (p. 456).

Vous pouvez désactiver le nettoyage automatique des anciennes sauvegardes en sélectionnant l'option **Conserver les sauvegardes indéfiniment** lors de la configuration des règles de rétention. L'utilisation du stockage risque d'augmenter et vous devrez supprimer manuellement les anciennes sauvegardes inutiles.

Conseils importants

- Les règles de rétention font partie du plan de protection. Si vous révoquez ou supprimez un plan, ses règles de rétention ne sont plus appliquées. Pour plus d'informations sur la suppression des sauvegardes dont vous n'avez plus besoin, voir "Suppression de sauvegardes" (p. 558).
- Si, conformément au modèle et au format de sauvegarde, chaque sauvegarde est stockée dans un fichier distinct, vous ne pouvez pas supprimer une sauvegarde dont dépendent d'autres sauvegardes incrémentielles ou différentielles. Cette sauvegarde sera supprimée conformément aux règles de rétention appliquées aux sauvegardes dépendantes. Cette configuration peut entraîner une augmentation de l'utilisation de l'espace de stockage, car la suppression de certaines sauvegardes est reportée. En outre, l'âge, le nombre ou la taille des sauvegardes peuvent dépasser les valeurs que vous avez spécifiées. Pour plus d'informations sur la modification de ce comportement, voir "Consolidation de sauvegarde" (p. 470).
- Par défaut, la dernière sauvegarde créée par un plan de protection n'est jamais supprimée. Toutefois, si vous configurez une règle de rétention pour nettoyer les sauvegardes avant de lancer une nouvelle opération de sauvegarde et que vous définissez le nombre de sauvegardes à

conserver sur zéro, la dernière sauvegarde est également supprimée.

Avertissement !
Si vous appliquez cette règle de rétention à un ensemble de sauvegardes ne comportant qu'une seule sauvegarde et que l'opération de sauvegarde échoue, vous ne pourrez pas restaurer vos données, car la sauvegarde existante sera supprimée avant la création d'une nouvelle.

Règles de rétention en fonction du modèle de sauvegarde

Les règles de rétention disponibles et leurs paramètres dépendent du modèle de sauvegarde que vous utilisez dans le plan de protection. Pour plus d'informations sur les modèles de sauvegarde, voir "Modèles de sauvegarde" (p. 436).

Le tableau suivant récapitule les règles de rétention disponibles et leurs paramètres.

Modèle de sauvegarde	Planification	Règles de rétention et paramètres disponibles
Toujours incrémentielle (fichier unique)	Mens. Hebdo. Journ. Par heure Sauvegardes déclenchées par un événement	Par nombre de sauvegardes Par âge des sauvegardes (paramètres distincts pour les sauvegardes mensuelles, hebdomadaires, quotidiennes et horaires) Conserver les sauvegardes indéfiniment
Toujours complète	Mens. Hebdo. Journ. Par heure Sauvegardes déclenchées par un événement	Par nombre de sauvegardes Par âge des sauvegardes (paramètres distincts pour les sauvegardes mensuelles, hebdomadaires, quotidiennes et horaires) Par volume total de sauvegardes Conserver les sauvegardes indéfiniment
Complète hebdomadaire, incrémentielle journalière	Journ. Sauvegardes déclenchées par un événement	Par nombre de sauvegardes Par âge des sauvegardes (paramètres distincts pour les sauvegardes hebdomadaires et quotidiennes) Par volume total de sauvegardes Conserver les sauvegardes indéfiniment
Complète mensuelle, Différentielle hebdomadaire, Incrémentielle	Mens. Hebdo. Journ.	Par nombre de sauvegardes Par âge des sauvegardes (paramètres distincts pour les sauvegardes complètes, différentielles et incrémentielles)

Modèle de sauvegarde	Planification	Règles de rétention et paramètres disponibles
quotidienne	Par heure Sauvegardes déclenchées par un événement	Par volume total de sauvegardes Conserver les sauvegardes indéfiniment
Personnalisé	Mens. Hebdo. Journ. Par heure Sauvegardes déclenchées par un événement	Par nombre de sauvegardes Par âge des sauvegardes (paramètres distincts pour les sauvegardes complètes, différentielles et incrémentielles) Par volume total de sauvegardes Conserver les sauvegardes indéfiniment

Pourquoi y a-t-il des sauvegardes mensuelles avec un modèle horaire ?

Selon le modèle de sauvegarde, vous pouvez configurer l'option **Par âge des sauvegardes** pour l'une des sauvegardes suivantes :

- Sauvegardes mensuelles, hebdomadaires, quotidiennes et horaires.

  Ces paramètres sont disponibles avec tous les modèles de sauvegarde non personnalisés et sont basés sur le temps. Toutes ces sauvegardes (mensuelles, hebdomadaires, quotidiennes et horaires) sont disponibles, même si vous configurez vos sauvegardes pour qu'elles s'exécutent toutes les heures. Voir l'exemple ci-dessous.

Sauvegarde	Description
Mens.	Une sauvegarde mensuelle correspond à la première sauvegarde de chaque mois.
Hebdo.	Une sauvegarde hebdomadaire correspond à la première sauvegarde du jour de la semaine que vous spécifiez dans l'option Sauvegarde hebdomadaire. Ce jour est considéré comme étant le début de la semaine dans les règles de rétention. Si une sauvegarde hebdomadaire est également la première sauvegarde du mois, elle est considérée comme étant mensuelle. Dans ce cas, une sauvegarde hebdomadaire est créée lors du jour sélectionné de la semaine suivante.
Journ.	Une sauvegarde quotidienne correspond à la première sauvegarde du jour, sauf si elle répond à la définition d'une sauvegarde mensuelle ou hebdomadaire. Dans ce cas, une sauvegarde quotidienne est créée le jour suivant.
Par heure	Une sauvegarde horaire correspond à la première sauvegarde de

Sauvegarde	Description
	l'heure, sauf si elle répond à la définition d'une sauvegarde mensuelle, hebdomadaire ou quotidienne. Dans ce cas, une sauvegarde horaire est créée à l'heure suivante.

- Sauvegardes complètes, différentielles et incrémentielles.

  Ces paramètres sont disponibles pour le modèle de sauvegarde **Personnalisé** et sont basés sur la méthode de sauvegarde. Le modèle **Complète mensuelle, Différentielle hebdomadaire, Incrémentielle quotidienne** est un modèle personnalisé préconfiguré.

Exemple

Vous utilisez le modèle de sauvegarde **Toujours incrémentielle (fichier unique)** avec le paramètre par défaut des sauvegardes horaires :

- Planifier selon l'horaire.
- Les sauvegardes s'exécutent toutes les heures : Du lundi au vendredi, toutes les heures, de 08 h 00 à 18 h 00.
- L'option **Sauvegarde hebdomadaire** est définie sur Lundi.

Dans la section **Durée de conservation** du plan de protection, vous pouvez appliquer des règles de rétention à des sauvegardes mensuelles, hebdomadaires, quotidiennes et horaires.

Le tableau suivant récapitule les types de sauvegarde créés pendant une période de 8 jours.

Date	Jour de la semaine	Description
1er juillet	Lundi	La première sauvegarde de chaque mois est mensuelle, si bien que la première sauvegarde du jour est mensuelle. Les autres sauvegardes planifiées pendant la journée sont horaires. Cette semaine, la première sauvegarde est considérée comme étant mensuelle. C'est la raison pour laquelle il n'y a pas de sauvegarde hebdomadaire. La première sauvegarde de la semaine suivante sera une sauvegarde hebdomadaire.
2 juillet	Mardi	La première sauvegarde est quotidienne ; les autres sauvegardes planifiées pendant la journée sont horaires.
3 juillet	Mercredi	La première sauvegarde est quotidienne ; les autres sauvegardes planifiées pendant la journée sont horaires.
4 juillet	Jeudi	La première sauvegarde est quotidienne ; les autres sauvegardes planifiées pendant la journée sont horaires.
5 juillet	Vendredi	La première sauvegarde est quotidienne ; les autres sauvegardes planifiées pendant la journée sont horaires.

Date	Jour de la semaine	Description
6 juillet	Samedi	La première sauvegarde est quotidienne ; les autres sauvegardes planifiées pendant la journée sont horaires.
7 juillet	Dimanche	La première sauvegarde est quotidienne ; les autres sauvegardes planifiées pendant la journée sont horaires.
8 juillet	Lundi	La première sauvegarde est hebdomadaire ; les autres sauvegardes planifiées pendant la journée sont horaires.

Configuration des règles de rétention

Les règles de rétention font partie du plan de protection, et leur disponibilité et leurs options dépendent du modèle de sauvegarde. Pour plus d'informations, voir "Règles de rétention en fonction du modèle de sauvegarde" (p. 456).

Pour configurer les règles de rétention

1. Dans le plan de protection, développez le module **Sauvegarde**.
2. Cliquez sur **Quantité à conserver**.
3. Sélectionnez l'une des options suivantes :
   - **Par nombre de sauvegardes**
   - **Par âge des sauvegardes**

     Des paramètres distincts pour les sauvegardes mensuelles, hebdomadaires, quotidiennes et horaires sont disponibles. La valeur maximale de tous les types est 9999.

     Vous pouvez également utiliser un seul paramètre pour toutes les sauvegardes.
   - **Par volume total de sauvegardes**

     Ce paramètre n'est pas disponible avec le modèle de sauvegarde **Toujours incrémentielle (fichier unique)**.
   - **Conserver les sauvegardes indéfiniment**
4. [Si vous n'avez pas sélectionné **Conserver les sauvegardes indéfiniment**] Configurez les valeurs de l'option sélectionnée.
5. [Si vous n'avez pas sélectionné **Conserver les sauvegardes indéfiniment**] Sélectionnez le moment où les règles de rétention sont appliquées :
   - Après la sauvegarde
   - Avant la sauvegarde

     Cette option n'est pas disponible lors de la sauvegarde de clusters Microsoft SQL Server ou Microsoft Exchange Server.
6. Cliquez sur **Valider**.
7. Enregistrez le plan de protection.

Réplication

Avec la réplication, chaque nouvelle sauvegarde est automatiquement copiée dans un emplacement de réplication. Les sauvegardes de l'emplacement de réplication ne dépendent pas des sauvegardes de l'emplacement source, et vice versa.

Seule la dernière sauvegarde de l'emplacement source est répliquée. Toutefois, si des sauvegardes antérieures ne sont pas répliquées (par exemple, en raison d'un problème de connexion réseau), l'opération de réplication inclura toutes les sauvegardes créées après la dernière réplication réussie.

Si une opération de réplication est interrompue, les données traitées seront utilisées par l'opération de réplication suivante.

Remarque
Cette rubrique décrit la réplication dans le cadre d'un plan de protection. Vous pouvez également créer un plan de réplication des sauvegardes distinct. Pour plus d'informations, voir "Réplication de sauvegarde" (p. 205).

Exemples d'utilisation

- Garantir une restauration fiable

  Stockez vos sauvegardes à la fois sur site (pour une restauration immédiate) et hors site (pour garantir que les sauvegardes restent en sécurité même en cas de défaillance du stockage ou de catastrophe naturelle affectant le site principal).
- Utiliser le stockage cloud pour protéger les données en cas de catastrophe naturelle

  Répliquer les sauvegardes vers le stockage sur le Cloud en transférant uniquement les modifications de données.
- Conserver seulement les points de restauration les plus récents

  Configurez des règles de rétention pour supprimer les anciennes sauvegardes d'un stockage rapide, afin d'économiser sur les coûts de stockage.

Emplacements pris en charge

Emplacement	En tant qu'emplacement de la source	En tant qu'emplacement de réplication
Dossier local	+	+
Dossier réseau	+	+
Stockage dans le Cloud	-	+
Secure Zone	+	–
Cloud public	+	+

Pour activer la réplication

1. Dans un plan de protection, développez le module **Sauvegarde**, puis cliquez sur **Ajouter un emplacement**.

   Remarque
   L'option **Ajouter un emplacement** n'est pas disponible lorsque vous sélectionnez le stockage dans le cloud dans **Où sauvegarder**.

2. Dans la liste des emplacements disponibles, sélectionnez l'emplacement de réplication.
   L'emplacement apparaît dans le plan de protection en tant que **2e emplacement**, **3e emplacement**, **4e emplacement** ou **5e emplacement**, en fonction du nombre d'emplacements ajoutés pour la réplication.
3. [Facultatif] Cliquez sur l'icône d'engrenage pour configurer les options de l'emplacement de réplication.
   - **Performance et fenêtre de sauvegarde** – définir la fenêtre de sauvegarde pour l'emplacement sélectionné, comme décrit dans "Performance et créneau de sauvegarde" (p. 500). Ces paramètres définissent les performances de réplication.
   - **Supprimer l'emplacement** : supprime l'emplacement de réplication actuellement sélectionné.
   - [Uniquement pour le stockage dans le cloud] **Envoi de données physiques** – enregistrer la sauvegarde initiale sur un périphérique de stockage amovible et l'expédier pour qu'elle soit transférée vers le stockage dans le cloud, au lieu de la répliquer via Internet.
     Cette option convient aux emplacements où la connexion réseau est lente ou lorsque vous souhaitez économiser de la bande passante lors de transferts de fichiers volumineux sur le réseau. L'activation de l'option ne nécessite pas de quotas de service avancés pour Cyber Protect, mais vous aurez besoin d'un quota de service d'envoi de données physiques pour créer un ordre d'expédition et en assurer le suivi. Voir "Envoi de données physiques" (p. 504).

     Remarque
     Cette option est prise en charge avec l'agent de protection à partir de la version C21.06.

4. [Facultatif] Dans la ligne **Combien conserver** sous l'emplacement de réplication, configurez les règles de rétention pour cet emplacement, comme décrit dans "Règles de rétention" (p. 455).
5. [Facultatif] Répétez les étapes 1 à 4 pour ajouter d'autres emplacements de réplication.
   Vous pouvez configurer jusqu'à quatre emplacements de réplication (**2e emplacement**, **3e emplacement**, **4e emplacement** et **5e emplacement**). Si vous sélectionnez le **stockage dans le cloud**, vous ne pouvez pas ajouter d'autres emplacements de réplication.

Important
Si vous activez la sauvegarde et la réplication dans le même plan de protection, assurez-vous que la réplication se termine avant la prochaine sauvegarde planifiée. Si la réplication est toujours en cours, la sauvegarde planifiée ne démarrera pas. Par exemple, une sauvegarde planifiée exécutée une fois toutes les 24 heures ne démarrera pas si l'exécution de la réplication dure 26 heures.

Pour éviter cette dépendance, utilisez un plan séparé pour la réplication de sauvegarde. Pour plus d'informations sur ce plan spécifique, voir "Réplication de sauvegarde" (p. 205).

Chiffrement

L'algorithme cryptographique AES (Advanced Encryption Standard) fonctionne en mode GCM (Galois/Counter Mode) et utilise une clé de 256 bits générée de manière aléatoire. La clé de chiffrement est ensuite chiffrée avec l'algorithme AES-256 ; le hachage SHA-2 (256 bits) du mot de passe est utilisé comme clé. Le mot de passe proprement dit n'est stocké ni sur le disque ni dans les sauvegardes, et le hachage du mot de passe est utilisé pour la vérification.

Avec cette sécurité à deux niveaux, les données de sauvegarde sont protégées de tout accès non autorisé. Par ailleurs, il n'est pas possible de restaurer un mot de passe perdu.

Remarque
L'utilisation de l'algorithme AES-256 avec un mot de passe fort offre un chiffrement de cryptographie post-quantique qui protège des attaques cryptanalytiques reposant sur l'informatique quantique.

Nous vous recommandons de chiffrer toutes les sauvegardes stockées dans le stockage sur le Cloud, en particulier si votre société est soumise à la conformité réglementaire.

Vous pouvez configurer le chiffrement comme suit :

- Dans le plan de protection
- En tant que propriété de l'ordinateur, à l'aide de Cyber Protect Monitor ou de l'interface de ligne de commande

Configuration du chiffrement dans le plan de protection

Dans un plan de protection, le chiffrement est activé par défaut. L'algorithme AES-256 est utilisé.

Avec un mot de passe fort, l'algorithme AES-256 fournit un chiffrement de cryptographie post-quantique.

Pour les comptes en mode Conformité, vous ne pouvez pas configurer le chiffrement dans le plan de protection. Pour plus d'informations sur la configuration du chiffrement sur le terminal protégé, voir "Configuration du chiffrement en tant que propriété de l'ordinateur" (p. 463).

Pour configurer le chiffrement

1. Dans un plan de protection, développez le module **Sauvegarde**.
2. Dans **Chiffrement**, cliquez sur **Spécifier le mot de passe**.
3. Indiquez et confirmez le mot de passe de chiffrement.
4. Cliquez sur **OK**.

Avertissement !
Il est impossible de restaurer les sauvegardes chiffrées si vous perdez ou oubliez le mot de passe.

Vous ne pouvez pas modifier les paramètres de chiffrement après avoir appliqué le plan de protection. Pour utiliser d'autres paramètres de chiffrement, créez un nouveau plan.

Configuration du chiffrement en tant que propriété de l'ordinateur

Vous pouvez configurer le chiffrement de sauvegarde en tant que propriété de l'ordinateur. Dans ce cas, le chiffrement n'est pas configuré dans le plan de protection, mais sur la ressource protégée. Le chiffrement en tant que propriété de l'ordinateur utilise l'algorithme AES avec une clé de 256 bits (AES-256).

Remarque
L'utilisation de l'algorithme AES-256 avec un mot de passe fort offre un chiffrement de cryptographie post-quantique qui protège des attaques cryptanalytiques reposant sur l'informatique quantique.

La configuration du chiffrement en tant que propriété de l'ordinateur affecte les plans de protection de la manière suivante :

- **Plans de protection déjà appliqués à la machine.** Si les paramètres de chiffrement d'un plan de protection sont différents, les sauvegardes échouent.
- **Plans de protection appliqués à l'ordinateur ultérieurement.** Les paramètres de chiffrement sauvegardés sur l'ordinateur remplacent les paramètres de chiffrement dans le plan de protection. Toute sauvegarde est chiffrée, même si le chiffrement est désactivé dans les paramètres du module de sauvegarde.

Pour les comptes en mode Conformité, seul le chiffrement en tant que propriété de la machine est disponible.

Si vous avez plusieurs agents pour VMware connecté au même vCenter Server, et que vous configurez le chiffrement comme une propriété de l'ordinateur, vous devez utiliser le même mot de passe de chiffrement sur tous les ordinateurs avec l'agent pour VMware, en raison de l'équilibrage de la charge entre les agents.

Vous pouvez configurer le chiffrement en tant que propriété de l'ordinateur de la manière suivante :

- Sur la ligne de commande
- Dans Cyber Protect Monitor (disponible pour Windows et macOS)

Pour configurer le chiffrement

Sur la ligne de commande

1. Connectez-vous en tant qu'administrateur (dans Windows) ou utilisateur root (dans Linux).
2. Dans la ligne de commande, exécutez la commande suivante :
   - Pour Windows :

     ```
     <installation_path>\PyShell\bin\acropsh.exe -m manage_creds --set-password
     <encryption_password>
     ```

     Par défaut, le chemin d'installation est `%ProgramFiles%\BackupClient`.
   - Pour Linux :

     ```
     /usr/sbin/acropsh -m manage_creds --set-password <encryption_password>
     ```

   - Pour une appliance virtuelle :

     ```
      /./sbin/acropsh -m manage_creds --set-password <encryption_password>
     ```

Avertissement !
Il est impossible de restaurer les sauvegardes chiffrées si vous perdez ou oubliez le mot de passe.

Dans Cyber Protect Monitor

1. Connectez-vous en tant qu'administrateur.
2. Cliquez sur l'icône Cyber Protect Monitor dans la zone de notification (dans Windows) ou la barre de menus (dans macOS).
3. Cliquez sur l'icône en forme d'engrenage, puis cliquez sur **Paramètres** > **Chiffrement**.
4. Sélectionnez **Définir un mot de passe pour cet ordinateur**, puis spécifiez et confirmez le mot de passe de chiffrement.
5. Cliquez sur **Enregistrer**.

Avertissement !
Il est impossible de restaurer les sauvegardes chiffrées si vous perdez ou oubliez le mot de passe.

Pour réinitialiser les paramètres de chiffrement

1. Connectez-vous en tant qu'administrateur (dans Windows) ou utilisateur root (dans Linux).
2. Dans la ligne de commande, exécutez la commande suivante :
   - Pour Windows :

     ```
     <installation_path>\PyShell\bin\acropsh.exe -m manage_creds --reset
     ```

     Par défaut, le chemin d'installation est `%ProgramFiles%\BackupClient`.
   - Pour Linux :

```
/usr/sbin/acropsh -m manage_creds --reset
```

- Pour une appliance virtuelle :

```
/./sbin/acropsh -m manage_creds --reset
```

Important
Si vous réinitialisez le chiffrement en tant que propriété de l'ordinateur ou changez le mot de passe de chiffrement après la création d'une sauvegarde par un plan de protection, l'opération de sauvegarde suivante échoue. Pour continuer à sauvegarder la ressource, créez un nouveau plan de protection.

Notarisation

Remarque
Cette fonctionnalité est disponible avec le pack Advanced Backup.

La notarisation vous permet de prouver qu'un fichier est authentique et inchangé depuis sa sauvegarde. Nous vous recommandons d'activer la notarisation lors de la sauvegarde de vos fichiers juridiques ou tout autre fichier requérant une authentification.

La notarisation est disponible uniquement pour les sauvegardes au niveau du fichier. Les fichiers avec une signature numérique sont ignorés, car ils n'ont pas besoin d'être notariés.

La notarisation *n'est pas* disponible :

- Si le format de sauvegarde est défini sur **Version 11**
- Si la destination de sauvegarde est Secure Zone

Comment utiliser la notarisation

Pour activer la notarisation de tous les fichiers sélectionnés pour la sauvegarde (à l'exception des fichiers avec une signature numérique), activez le commutateur **Notarisation** lors de la création d'un plan de protection.

Lors de la configuration de la restauration, les fichiers notariés seront marqués d'une icône spéciale. Vous pourrez ainsi vérifier l'authenticité du fichier.

Fonctionnement

Lors d'une sauvegarde, l'agent calcule les code de hachage des fichiers sauvegardés, crée un arbre de hachage (basé sur la structure du dossier), enregistre l'arbre dans la sauvegarde, puis envoie la racine de l'arbre de hachage au service Notary. Le service Notary enregistre la racine de l'arbre de hachage dans la base de données blockchain Ethereum pour s'assurer que cette valeur ne change pas.

Lors de la vérification de l'authenticité d'un fichier, l'agent calcule le hachage du fichier, puis le compare avec le hachage stocké dans l'arbre de hachage sauvegardé. Si ces hachages ne correspondent pas, le fichier n’est pas authentique. Sinon, l'authenticité du fichier est garantie par l'arbre de hachage.

Pour vérifier que l'arbre de hachage n'a pas été compromis, l'agent envoie la racine de l'arbre de hachage au service Notary. Le service Notary la compare avec celle stockée dans la base de données blockchain. Si les hachages correspondent, le fichier sélectionné est authentique. Sinon, le logiciel affiche un message indiquant que le fichier n’est pas authentique.

Options de sauvegarde par défaut

Les valeurs par défaut des options de sauvegarde existent aux niveaux de la société, de l'unité et de l'utilisateur. Lorsqu'une unité ou un compte utilisateur sont créés au sein d'une société ou d'une unité, ils héritent des valeurs par défaut pour la société ou l'unité.

Les administrateurs de la société, les administrateurs de l'unité et tous les utilisateurs ne disposant pas de droits d'administrateur peuvent modifier une valeur d'option par défaut en utilisant la valeur prédéfinie. La nouvelle valeur sera utilisée par défaut pour tous les plans de protection que vous créerez à leur niveau respectif après la prise d'effet de la modification.

Lors de la création d'un plan de protection, un utilisateur peut remplacer une valeur par défaut par une valeur personnalisée qui sera spécifique à ce plan.

Pour changer une valeur d'option par défaut

1. Effectuez l'une des actions suivantes :
   - Pour modifier la valeur par défaut pour la société, connectez-vous à la console Cyber Protect en tant qu'administrateur de la société.
   - Pour modifier la valeur par défaut d'une unité, connectez-vous à la console Cyber Protect en tant qu'administrateur de l'unité.
   - Pour modifier la valeur par défaut pour vous-même, connectez-vous à la console Cyber Protect à l'aide d'un compte qui ne dispose pas des droits d'administrateur.
2. Cliquez sur **Paramètres** > **Paramètres système**.
3. Développez la section **Options de sauvegarde par défaut**.
4. Sélectionnez l'option, puis effectuez les modifications nécessaires.
5. Cliquez sur **Enregistrer**.

Options de sauvegarde

Pour modifier les options de sauvegarde d'un plan de protection, accédez au module **Sauvegarde**, puis cliquez dans le champ **Options de sauvegarde** sur **Modifier**.

Disponibilité des options de sauvegarde

L'ensemble des options de sauvegarde disponibles dépendent des éléments suivants :

- l'environnement dans lequel l'agent fonctionne (Windows, Linux, macOS) ;
- le type de données en cours de sauvegarde (disques, fichiers, machines virtuelles, données d'application) ;
- la destination de la sauvegarde (dossier réseau, local ou stockage sur le Cloud).

Le tableau suivant résume la disponibilité des options de sauvegarde.

	Sauvegarde au niveau disque			**Sauvegarde au niveau fichier**			**Machines virtuelles**			**SQL et Exchange**
	Windows	**Linux**	**macOS**	**Windows**	**Linux**	**macOS**	**ESXi**	**Hyper-V**	**Virtuozzo**	**Windows**
Alertes	+	+	+	+	+	+	+	+	+	+
Consolidation de sauvegarde	+	+	+	+	+	+	+	+	+	-
Nom de fichier de la sauvegarde	+	+	+	+	+	+	+	+	+	+
Format de la sauvegarde	+	+	+	+	+	+	+	+	+	+
Validation de la sauvegarde	+	+	+	+	+	+	+	+	+	+
Suivi des blocs modifiés (CBT)	+	-	-	-	-	-	+	+	-	-
Mode de sauvegarde de cluster	-	-	-	-	-	-	-	-	-	+
Niveau de compression	+	+	+	+	+	+	+	+	+	+
Gestion erreurs										
Réessayer si une erreur se produit	+	+	+	+	+	+	+	+	+	+
Ne pas afficher les messages et dialogues pendant le traitement (mode silencieux)	+	+	+	+	+	+	+	+	+	+
Ignorer les secteurs défectueux	+	-	+	+	-	+	+	+	+	-

Réessayer si une erreur se produit lors de la création d'instantané de MV	-	-	-	-	-	-	+	+	+	-
Sauvegarde incrémentielle/différentielle rapide	+	+	+	-	-	-	-	-	-	-
Instantané de sauvegarde de niveau fichier	-	-	-	+	+	+	-	-	-	-
Filtres de fichiers	+	+	+	+	+	+	+	+	+	-
Données d'investigation	+	-	-	-	-	-	-	-	-	-
Troncation de journal	-	-	-	-	-	-	+	+	-	SQL uniquement
Prise d'instantanés LVM	-	+	-	-	-	-	-	-	-	-
Points de montage	-	-	-	+	-	-	-	-	-	-
Snapshot Multi-volume	+	+	-	+	+	-	-	-	-	-
Reprise en un seul clic	+	+	-	-	-	-	-	-	-	-
Performance et créneau de sauvegarde	+	+	+	+	+	+	+	+	+	+
Envoi de données physiques	+	+	+	+	+	+	+	+	+	-
Commandes Pré/Post	+	+	+	+	+	+	+	+	+	+
Commandes de capture de données Pré/Post	+	+	+	+	+	+	-	-	-	+
Planification										
Répartir les heures de démarrage dans une fenêtre de	+	+	+	+	+	+	+	+	+	+

temps										
Limiter le nombre de sauvegardes simultanées	-	-	-	-	-	-	+	+	+	-
Sauvegarde secteur par secteur	+	+	-	-	-	-	+	+	+	-
Fractionnement	+	+	+	+	+	+	+	+	+	+
Traitement de l'échec de tâche	+	+	+	+	+	+	+	+	+	+
Conditions de démarrage de tâche	+	+	-	+	+	-	+	+	+	+
Service de cliché instantané des volumes	+	-	-	+	-	-	-	+	-	+
Service de cliché instantané des volumes (VSS) pour les machines virtuelles	-	-	-	-	-	-	+	+	-	-
Sauvegarde hebdomadaire	+	+	+	+	+	+	+	+	+	+
Journal des événements Windows	+	-	-	+	-	-	+	+	-	+

Alertes

Aucune sauvegarde réussie sur plusieurs jours d'affilée

Le préréglage est le suivant : **Désactivé**.

Cette option permet de déterminer s'il faut ou non générer une alerte lorsque le plan de protection n'a créé aucune sauvegarde pendant une période définie. Outre les échecs de sauvegarde, le logiciel fait le compte des sauvegardes qui n'ont pas été exécutées à l'heure prévue (sauvegardes manquées).

Les alertes sont générées sur une base « par machine » et sont affichées sous l'onglet **Alertes**.

Vous pouvez spécifier le nombre de jours consécutifs sans sauvegarde après lesquels l'alerte est générée.

Consolidation de sauvegarde

Cette option définit s'il faut consolider les sauvegardes durant le nettoyage ou supprimer les chaînes de sauvegarde entières.

Le préréglage est le suivant : **Désactivé**.

La consolidation est un processus qui associe deux sauvegardes subséquentes ou plus dans une même sauvegarde.

Si cette option est activée, une sauvegarde qui devrait être supprimée pendant le nettoyage est consolidée avec la sauvegarde dépendante suivante (incrémentielle ou différentielle).

Dans le cas contraire, la sauvegarde est conservée jusqu'à ce que toutes les autres sauvegardes dépendantes puissent également être supprimées. Cela permet d'éviter la consolidation qui pourrait nécessiter un temps considérable, mais il nécessite de l'espace supplémentaire pour le stockage des sauvegardes dont la suppression est différée. L'âge ou le nombre de sauvegardes peut dépasser les valeurs spécifiées dans les règles de rétention.

Important
Sachez que la consolidation n'est qu'une méthode de suppression et non une alternative à la suppression. La sauvegarde obtenue ne contiendra pas les données qui étaient présentes dans la sauvegarde supprimée et absentes de la sauvegarde incrémentielle ou différentielle conservée.

Elle *n'est pas* effective si l'une des conditions suivantes est remplie :

- La destination de la sauvegarde est le stockage sur le Cloud.
- Le modèle de sauvegarde est défini sur **Toujours incrémentielle (fichier unique)**.
- Le format de sauvegarde est défini sur **Version 12**.

Les sauvegardes stockées sur le Cloud, ainsi que les sauvegardes sous forme d'un fichier unique (formats Version 11 et 12), sont toujours consolidées, car leur structure interne permet une consolidation rapide et facile.

Toutefois, si le format Version 12 est utilisé et que plusieurs chaînes de sauvegarde sont présentes (chaque chaîne étant stockée dans un fichier .tibx séparé), la consolidation ne fonctionne qu'avec la dernière chaîne. Toute autre chaîne est supprimée en bloc, à l'exception de la première, qui est réduite à la taille minimum pour conserver les méta-informations (environ 12 Ko). Ces méta-informations sont requises pour assurer la cohérence des données lors d'opérations de lecture et écriture simultanées. Les sauvegardes incluses dans ces chaînes disparaissent de l'interface graphique dès que la règle de rétention est appliquée, même si elles existent physiquement tant que la chaîne entière n'est pas supprimée.

Dans tous les autres cas, les sauvegardes dont la suppression est différée sont marquées de l'icône d'une corbeille () dans l'interface utilisateur graphique. Si vous supprimez une telle sauvegarde en cliquant sur le signe X, la consolidation sera exécutée.

Nom de fichier de sauvegarde

Cette option définit le nom des fichiers de sauvegarde créés par le plan de protection ou par le plan de sauvegarde des applications dans le cloud.

Pour les fichiers de sauvegarde créés par des plans de protection, vous pouvez voir ces noms dans un gestionnaire de fichiers lorsque vous parcourez l'emplacement de sauvegarde.

Qu'est-ce qu'un fichier de sauvegarde ?

Chaque plan de protection crée un ou plusieurs fichiers à l'emplacement de sauvegarde, selon le modèle et le format de sauvegarde utilisés. Le tableau suivant répertorie les fichiers qui peuvent être créés par machine ou par boîte aux lettres.

	Toujours incrémentielle (fichier unique)	**Autres modèles de sauvegarde**
Format de sauvegarde **Version 11**	Un fichier TIB et un fichier de métadonnées XML	Plusieurs fichiers TIB et un fichier de métadonnées XML
Format de sauvegarde **Version 12**	Un fichier TIBX par chaîne de sauvegarde (une sauvegarde complète ou différentielle et toutes les sauvegardes incrémentielles qui en dépendent). Si la taille d'un fichier stocké dans un dossier local ou réseau (SMB) dépasse 200 Go, le fichier est divisé par défaut en fichiers de 200 Go.	

Tous les fichiers ont le même nom, avec ou sans ajout d'une estampille ou d'un numéro séquentiel. Vous pouvez définir ce nom (appelé nom de fichier de sauvegarde) lors de la création ou de la modification d'un plan de protection ou d'plan de sauvegarde d'applications dans le cloud.

Remarque
La date et l'heure sont ajoutées au nom de fichier de la sauvegarde uniquement dans la version 11 du format de sauvegarde.

Si vous changez le nom d'un fichier de sauvegarde dans un plan de protection ou un plan de sauvegarde d'applications dans le cloud, la sauvegarde suivante sera une sauvegarde complète.

Si vous spécifiez le nom de fichier d'une sauvegarde existante du même ordinateur, une sauvegarde complète, incrémentielle ou différentielle est créée en fonction de la planification du plan.

Remarque
Si vous déplacez des fichiers de sauvegarde (.tibx) depuis leur stockage d'origine, ne les renommez pas. Les fichiers renommés apparaîtront comme étant endommagés et vous ne pouvez pas en restaurer les données.

Il est possible de définir des noms de fichier de sauvegarde pour des emplacements qui ne peuvent pas être parcourus par un gestionnaire de fichiers (tel que le stockage dans le cloud). Dans ce cas, vous voyez les noms personnalisés dans l'onglet **Stockage de sauvegarde**.

Où puis-je voir les noms des fichiers de sauvegarde ?

Pour les plans de protection, sélectionnez dans l'onglet **Stockage de sauvegarde** l'emplacement, puis l'archive de sauvegardes.

- Le nom de fichier de sauvegarde par défaut s'affiche dans le volet **Détails**.
- Si vous définissez un nom de fichier de sauvegarde non par défaut, il s'affichera directement dans l'onglet **Stockage de sauvegarde**, dans la colonne **Nom**.

Pour les plans de sauvegarde d'applications dans le cloud, sélectionnez dans l'onglet **Stockage de sauvegarde** l'emplacement et l'archive de sauvegardes, puis cliquez sur l'icône en forme d'engrenage.

Limites des noms de fichier de sauvegarde

- Un nom de fichier de sauvegarde ne peut pas se terminer par un numéro.
  La lettre A est ajoutée à la fin du nom de fichier de sauvegarde par défaut afin d'éviter qu'il se termine par un numéro. Si vous créez un nom personnalisé, assurez-vous toujours qu'il ne se termine pas par un numéro. Si vous utilisez des variables, le nom ne doit pas se terminer par une variable, car cette dernière peut finir par un numéro.
- Un nom de fichier de sauvegarde ne peut pas contenir les symboles suivants : **()&?*$<>":\|/#**, renvoi à la ligne (**\n**) et tabulations (**\t**).

Remarque
Choisissez des noms de fichier de sauvegarde conviviaux. De cette manière, vous pourrez distinguer facilement les sauvegardes en parcourant l'emplacement de sauvegarde avec un gestionnaire de fichiers.

Nom de fichier de sauvegarde par défaut

Le nom du fichier de sauvegarde par défaut pour les sauvegardes de machines physiques et virtuelles intégrales, disques/volumes, fichiers/dossiers, base de données Microsoft SQL Server, bases de données Microsoft Exchange Server et configuration ESXi est `[Machine Name]-[Plan ID]-[Unique ID]A`.

Le nom par défaut des sauvegardes de boîte aux lettres Exchange et de sauvegardes de boîte aux lettres Microsoft 365 créées par un Agent local pour Microsoft 365 est `[Mailbox ID]_mailbox_[Plan ID]A`.

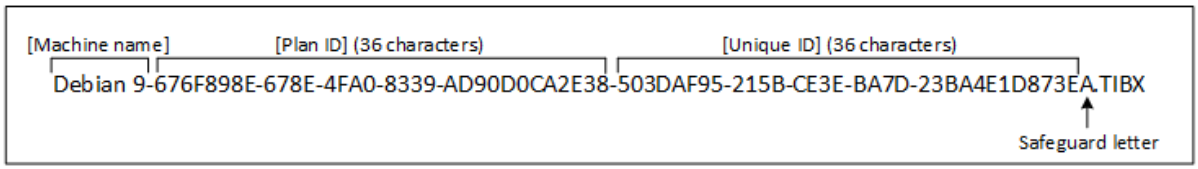
Le nom par défaut des sauvegardes Microsoft Azure est préfixé avec `[Mailbox ID]_`. Ce préfixe ne peut pas être retiré.

Le nom par défaut pour les sauvegardes d'application Cloud créées par les agents dans le Cloud est `[Resource Name]_[Resource Type]_[Resource Id]_[Plan Id]A`.

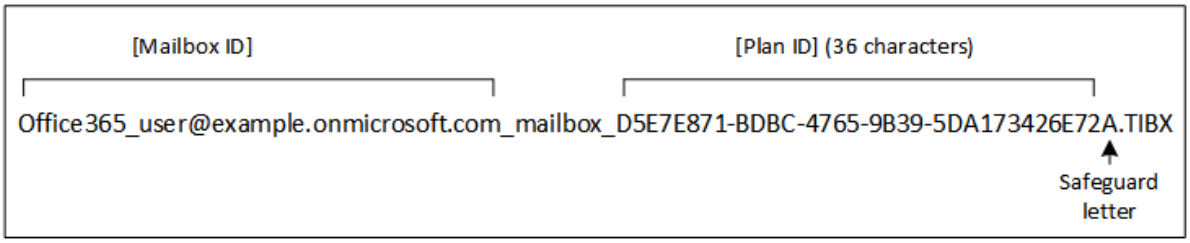
Le nom par défaut est constitué des variables suivantes :

- `[Machine Name]` Cette variable est remplacée par le nom de l'ordinateur (celui qui est affiché dans la console Cyber Protect).
- `[Plan ID]`, `[Plan Id]` Ces variables sont remplacées par l'identifiant unique du plan de protection. Cette valeur ne change pas si le plan est renommé.
- `[Unique ID]` Cette variable est remplacée par l'identificateur unique de la machine sélectionnée. Cette valeur ne change pas si la machine est renommée.
- `[Mailbox ID]` Cette variable est remplacée par le nom principal de l'utilisateur (UPN) de la boîte aux lettres.
- `[Resource Name]` Cette variable est remplacée par le nom de la source de données Cloud, comme le nom principal de l'utilisateur (UPN), l'URL du site SharePoint ou le nom du Drive partagé.
- `[Resource Type]` Cette variable est remplacée par le type de source des données Cloud, comme `mailbox`, `O365Mailbox`, `O365PublicFolder`, `OneDrive`, `SharePoint`, `GDrive`.
- `[Resource ID]` Cette variable est remplacée par l'identificateur unique de la source de données Cloud. Cette valeur ne change pas si la source de données Cloud est renommée.
- « `A` » est une lettre de protection ajoutée à la fin du nom de fichier de sauvegarde afin d'éviter qu'il se termine par un numéro.

Le diagramme ci-dessous affiche le nom de fichier de sauvegarde par défaut.



Le diagramme ci-dessous affiche le nom de fichier de sauvegarde par défaut pour les sauvegardes de boîte aux lettres Microsoft 365 réalisées par un agent local.



Noms sans variables

Si vous remplacez le nom du fichier de sauvegarde par `MyBackup`, les fichiers de sauvegarde ressembleront aux exemples suivants. Dans les deux exemples, on suppose des sauvegardes incrémentielles quotidiennes planifiées à 14h40 à partir du 13 septembre 2016.

Pour le format version 12 avec le modèle de sauvegarde **« Toujours incrémentielle (fichier unique) »** :

```
MyBackup.tibx
```

Pour le format version 12 avec un autre modèle de sauvegarde :

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

Utilisation de variables

Outre les variables utilisées par défaut, vous pouvez utiliser les variables suivantes :

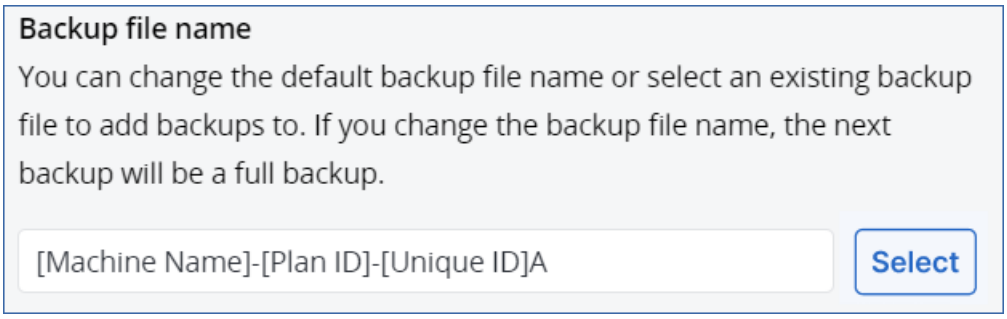
- La variable `[Plan name]`, qui est remplacée par le nom du plan de protection.
- La variable `[Virtualization Server Type]`, qui est remplacée par « vmwesx » si les machines virtuelles sont sauvegardées par l'agent pour VMware ou par « mshyperv » si les machines virtuelles sont sauvegardées par l'agent pour Hyper-V.

Si plusieurs machines ou boîtes aux lettres sont sélectionnées pour la sauvegarde, le nom du fichier de sauvegarde doit contenir la variable `[Machine Name]`, `[Unique ID]`, `[Mailbox ID]`, `[Resource Name]`, la variable `[Resource Id]`.

Création de sauvegardes dans une archive de sauvegarde existante

Vous pouvez configurer les sauvegardes d'une ressource pour qu'elles soient ajoutées à une archive de sauvegardes existante.

Cette option peut être utile, par exemple, lorsqu'un plan de protection est appliqué à un seul ordinateur, et que vous devez supprimer cet ordinateur de la console Cyber Protect ou désinstaller l'agent avec ses paramètres de configuration. Après avoir rajouté l'ordinateur ou réinstallé l'agent, vous pouvez forcer le plan de protection à poursuivre la sauvegarde vers l'archive d'origine.



Pour configurer les sauvegardes d'une ressource à ajouter à une archive de sauvegardes existante

Ressources autres que de cloud à cloud

1. Dans l'écran **Tous les terminaux**, cliquez sur la ressource, puis sur **Protéger**.
2. Dans les paramètres du plan de protection, développez le module **Sauvegarde**.
3. Cliquez sur **Options de sauvegarde**, puis sur **Modifier**.
4. Dans l'onglet **Nom de fichier de la sauvegarde**, cliquez sur **Sélectionner**.

Le bouton **Sélectionner** affiche les sauvegardes à l'emplacement sélectionné dans la section **Où sauvegarder** du plan de protection.

Remarque
Le bouton **Sélectionner** n'est disponible que pour les plans de protection créés pour une seule ressource à laquelle ils sont appliqués.

5. Sélectionnez une archive, puis cliquez sur **Terminé**.
6. Cliquez sur **Terminé**, puis sur **Appliquer**.

Ressources de cloud à cloud

1. Dans l'onglet **Gestion** > **Sauvegarde des applications cloud**, sélectionnez le plan.
2. Cliquez sur **Modifier**, puis sur l'icône en forme d'engrenage située à côté du nom du plan.
3. Dans l'onglet **Nom de la sauvegarde**, cliquez sur **Sélectionner**.

Remarque
Le bouton **Sélectionner** n'est disponible que pour les plans de sauvegarde créés (et appliqués) pour une seule ressource.

4. Sélectionnez une archive de sauvegardes, puis cliquez sur **Terminé**.
5. Cliquez sur **Terminé**, puis sur **Enregistrer les modifications**.

Format de sauvegarde

L'option **Format de sauvegarde** définit le format des sauvegardes créées par le plan de protection. Cette option est disponible uniquement pour les plans de protection qui utilisent déjà le format de sauvegarde version 11. Si tel est le cas, vous pouvez modifier le format de sauvegarde en version 12. Après le passage du format de sauvegarde en version 12, l'option deviendra indisponible.

- **Version 11**
  Le format hérité conservé pour une compatibilité descendante.

  Remarque
  Vous ne pouvez pas sauvegarder de groupes de disponibilité de la base de données (DAG) à l'aide du format de sauvegarde version 11. La sauvegarde de groupes DAG est prise en charge uniquement au format version 12.

- **Version 12**
  Le format de sauvegarde qui a été introduit dans Acronis Backup 12 pour une sauvegarde et une restauration plus rapides. Chaque chaîne de sauvegarde (une sauvegarde complète ou différentielle et toutes les sauvegardes incrémentielles qui en dépendent) est enregistrée dans un fichier TIBX unique.

Format et fichiers de sauvegarde

Pour les emplacements de sauvegarde qui peuvent être parcourus avec un gestionnaire de fichiers (comme les dossiers locaux et réseau), le format de sauvegarde détermine le nombre de fichiers et leur extension. Le tableau suivant répertorie les fichiers qui peuvent être créés par machine ou par boîte aux lettres.

	Toujours incrémentielle (fichier unique)	**Autres modèles de sauvegarde**
Format de sauvegarde **Version 11**	Un fichier TIB et un fichier de métadonnées XML	Plusieurs fichiers TIB et un fichier de métadonnées XML
Format de sauvegarde **Version 12**	Un fichier TIBX par chaîne de sauvegarde (une sauvegarde complète ou différentielle et toutes les sauvegardes incrémentielles qui en dépendent). Si la taille d'un fichier stocké dans un dossier local ou réseau (SMB) dépasse 200 Go, le fichier est divisé par défaut en fichiers de 200 Go.	

Modification du format de sauvegarde en version 12 (TIBX)

Si vous faites passer le format de sauvegarde de la version 11 (format TIB) à la version 12 (format TIBX) :

- La sauvegarde suivante sera complète.
- Dans les emplacements de sauvegarde qui peuvent être parcourus avec un gestionnaire de fichiers (comme les dossiers locaux et réseau), un nouveau fichier TIBX sera créé. Le nouveau fichier aura le même nom que l'original, avec le suffixe **_v12A**.
- Les règles de rétention et de réplication seront appliquées uniquement aux nouvelles sauvegardes.
- Les anciennes sauvegardes ne seront pas supprimées et resteront disponibles dans l'onglet **Stockage de sauvegarde**. Vous pouvez les supprimer manuellement.
- Les anciennes sauvegardes dans le Cloud ne consommeront pas le quota de **Stockage dans le Cloud**.
- Les anciennes sauvegardes locales consommeront le quota de **sauvegarde locale** jusqu'à ce que vous les supprimiez manuellement.

Déduplication dans l'archive

Le format de sauvegarde TIBX de la version 12 est compatible avec la déduplication dans l'archive, qui offre les avantages suivants :

- Taille des sauvegardes considérablement réduite, avec déduplication intégrée au niveau du bloc pour n'importe quel type de données
- Une gestion efficace des liens directs garantit l'absence de doublons de stockage.
- Segmentation basée sur le hachage

Remarque
La déduplication dans l'archive est activée par défaut pour toutes les sauvegardes au format TIBX. Il n'est pas nécessaire que vous l'activiez dans les options de sauvegarde, et vous ne pouvez pas la désactiver.

Compatibilité des formats de sauvegarde dans différentes versions de solution

Pour plus d'informations sur la compatibilité des formats de sauvegarde, reportez-vous à Compatibilité des archives de sauvegarde dans différentes versions de solution (1689).

Validation de la sauvegarde

La validation est une opération qui vérifie la possibilité de restauration de données à partir d'une sauvegarde. Lorsque cette option est activée, chaque sauvegarde créée par le plan de protection est validée immédiatement après sa création à l'aide de la méthode de vérification de somme de contrôle. Cette opération est effectuée par l'agent de protection.

Le préréglage est le suivant : **Désactivé**.

Pour en savoir plus sur la validation par vérification de somme de contrôle, reportez-vous à "Vérification de la somme de contrôle" (p. 212).

Remarque
Selon les paramètres choisis par votre fournisseur de services, il se peut que la validation ne soit pas disponible lors d'une sauvegarde sur le stockage dans le Cloud. La validation est également indisponible pour les emplacements de sauvegarde dans le cloud public.

Suivi des blocs modifiés (CBT)

Cette option est effective pour les sauvegardes suivantes :

- Sauvegardes de disque de machines virtuelles
- Sauvegardes de disque de machines physiques fonctionnant sous Windows
- Sauvegardes de bases de données Microsoft SQL Server
- Sauvegardes de bases de données Microsoft Exchange Server

Le préréglage est le suivant : **Activé**.

Cette option détermine l'utilisation du suivi des blocs modifiés (CBT) lors de l'exécution d'une sauvegarde incrémentielle ou différentielle.

La technologie CBT accélère le processus de sauvegarde. Les modifications apportées au disque ou à la base de données sont continuellement suivies au niveau des blocs. Lorsqu'une sauvegarde commence, les modifications peuvent être immédiatement enregistrées sur la sauvegarde.

Mode de sauvegarde de cluster

Remarque
Cette fonctionnalité est disponible avec le pack Advanced Backup.

Ces options sont effectives pour les sauvegardes de niveau base de données de Microsoft SQL Server et de Microsoft Exchange Server.

Ces options ne sont effectives que si le cluster lui-même (groupes de disponibilité AlwaysOn (AAG) de Microsoft SQL Server ou groupe de disponibilité de la base de données (DAG) de Microsoft Exchange Server) est sélectionné pour la sauvegarde plutôt que les nœuds ou bases de données qu'il contient. Si vous sélectionnez des éléments individuels au sein du cluster, la sauvegarde ne prendra pas en charge le cluster et seules les copies sélectionnées des éléments seront sauvegardées.

Microsoft SQL Server

Cette option détermine le mode de sauvegarde des groupes de disponibilité AlwaysOn (AAG) de Microsoft SQL Server. Pour que cette option prenne effet, l'agent pour SQL doit être installé sur tous les nœuds AAG. Pour plus d'informations sur la sauvegarde des groupes de disponibilité AlwaysOn, consultez la section « Protection des groupes de disponibilité AlwaysOn (AAG) ».

Le préréglage est le suivant : **Réplica secondaire si possible.**

Vous pouvez choisir l'une des options suivantes:

- **Réplica secondaire si possible**
  Si tous les réplicas secondaires sont hors ligne, le réplica principal est sauvegardé. La sauvegarde du réplica principal peut ralentir les performances de SQL Server, mais les données seront sauvegardées dans leur état le plus récent.
- **Réplica secondaire**
  Si tous les réplicas secondaires sont hors ligne, la sauvegarde échouera. La sauvegarde des réplicas secondaires n'affecte pas les performances de SQL Server et vous permet d'agrandir le créneau de sauvegarde. Toutefois, les réplicas passifs peuvent contenir des informations qui ne sont pas à jour parce qu'ils sont souvent configurés pour être mis à jour de façon asynchrone (décalée).
- **Réplica principal**
  Si le réplica principal est hors ligne, la sauvegarde échouera. La sauvegarde du réplica principal peut ralentir les performances de SQL Server, mais les données seront sauvegardées dans leur état le plus récent.

Quelle que soit la valeur de cette option, afin d'assurer la cohérence de la base de données, le logiciel ignore les bases de données qui ne sont *pas* dans l'état **SYNCHRONISÉ** ou **SYNCHRONISATION** au démarrage de la sauvegarde. Si toutes les bases de données sont ignorées, la sauvegarde échoue.

Microsoft Exchange Server

Cette option détermine le mode de sauvegarde des groupe de disponibilité de la base de données (DAG) Exchange Server. Afin que cette option prenne effet, l'agent pour Exchange doit être installé sur tous les nœuds DAG. Pour plus d'informations sur la sauvegarde des groupes de disponibilité de la base de données, consultez la section « Protection des groupes de disponibilité de la base de données (DAG) ».

Le préréglage est le suivant : **Copie passive si possible**

Vous pouvez choisir l'une des options suivantes:

- **Copie passive si possible**
  Si toutes les copies passives sont hors ligne, la copie active est sauvegardée. La sauvegarde de la copie active peut ralentir les performances d'Exchange Server, mais les données seront sauvegardées dans leur état le plus récent.
- **Copie passive**
  Si toutes les copies passives sont hors ligne, la sauvegarde échouera. La sauvegarde des copies passives n'affecte pas les performances du serveur Exchange et vous permet d'agrandir le créneau de sauvegarde. Toutefois, les copies passives peuvent contenir des informations qui ne sont pas à jour parce que ces copies sont souvent configurées pour être mises à jour de façon asynchrone (décalées).
- **Copie active**
  Si la copie active est hors ligne, la sauvegarde échouera. La sauvegarde de la copie active peut ralentir les performances d'Exchange Server, mais les données seront sauvegardées dans leur état le plus récent.

Quelle que soit la valeur de cette option, afin d'assurer la cohérence de la base de données, le logiciel ignore les bases de données qui ne sont *pas* dans l'état **SAIN** ou **ACTIF** au démarrage de la sauvegarde. Si toutes les bases de données sont ignorées, la sauvegarde échoue.

Niveau de compression

Remarque
Cette option n'est pas disponible pour les sauvegardes cloud à cloud. La compression pour ces sauvegardes est activée par défaut avec un niveau fixe correspondant au niveau **Normale** ci-dessous.

L'option définit le niveau de compression appliqué aux données sauvegardées. Les niveaux disponibles sont les suivants : **Aucune**, **Normale**, **Élevée**, **Maximale**.

Le préréglage est le suivant : **Normale**.

Un niveau de compression supérieur signifie que le processus de sauvegarde prend plus de temps, mais que la sauvegarde en résultant occupe moins d'espace. Pour le moment, le fonctionnement des niveaux **Élevée** et **Maximale** est identique.

Le niveau de compression des données optimal dépend du type de données en cours de sauvegarde. Par exemple, même une compression maximale ne réduira pas de manière significative la taille de la sauvegarde si cette dernière contient essentiellement des fichiers comprimés tels que des fichiers .jpg, .pdf ou .mp3. Cependant, des formats tels que .doc ou .xls seront bien comprimés.

Gestion erreurs

Ces options vous permettent de spécifier comment traiter des erreurs qui peuvent se produire pendant la restauration.

Réessayer si une erreur se produit

Le préréglage est le suivant : **Activé. Nombre de tentatives : 10. Intervalle entre les tentatives : 30 secondes.**

Lorsqu'une erreur récupérable se produit, le programme essaie à nouveau d'effectuer l'opération qui a échoué. Vous pouvez définir l'intervalle de temps ainsi que le nombre de tentatives. Les tentatives s'arrêteront dès que l'opération réussira ou que le nombre de tentatives sera atteint, le premier de ces deux cas prévalant.

Par exemple, si la destination de sauvegarde sur le réseau devient inaccessible ou inatteignable lors d'une sauvegarde en cours d'exécution, le logiciel essaiera d'atteindre la destination toutes les 30 secondes, mais pas plus de 30 fois. Les tentatives s'arrêteront dès que la connexion sera rétablie ou que le nombre de tentatives sera atteint, le premier de ces deux cas prévalant.

Toutefois, si la destination de sauvegarde n'est pas disponible lors du démarrage de la sauvegarde, seules 10 tentatives seront effectuées.

Ne pas afficher les messages et dialogues pendant le traitement (mode silencieux)

Le préréglage est le suivant : **Activé**.

Avec le mode silencieux activé, le programme gérera automatiquement les situations qui nécessitent l'intervention de l'utilisateur (sauf pour le traitement des secteurs défectueux, qui est défini comme une option séparée). Si une opération ne peut pas se poursuivre sans l'intervention de l'utilisateur, elle échouera. Les détails de l'opération, y compris les erreurs, le cas échéant, apparaissent dans le journal des opérations.

Ignorer les secteurs défectueux

Le préréglage est le suivant : **Désactivé**.

Lorsque cette option est désactivée, chaque fois que le programme rencontre un secteur défectueux, l'activité de sauvegarde présente l'état **Intervention nécessaire**. Afin de pouvoir sauvegarder les informations valides d'un disque se détériorant rapidement, activez la fonction ignorer les secteurs défectueux. Le programme continuera de sauvegarder les autres données et

vous pourrez monter la sauvegarde de disque en résultant et extraire les fichiers valides vers un autre disque.

Remarque
La fonctionnalité permettant d'ignorer les secteurs défectueux n'est pas prise en charge sous Linux. Vous pouvez sauvegarder les systèmes Linux avec des secteurs défectueux en mode hors ligne à l'aide de l'outil de création de supports de démarrage dans la version sur site de Cyber Protect. L'utilisation de l'outil de création de supports de démarrage sur site nécessite une licence distincte. Contactez le support pour obtenir de l'aide.

Réessayer si une erreur se produit lors de la création d'instantané de MV

Le préréglage est le suivant : **Activé. Nombre de tentatives : 3. Intervalle entre les tentatives : 5 minutes.**

Lorsque la prise d'un instantané de machine virtuelle échoue, le programme essaie à nouveau d'effectuer l'opération qui a échoué. Vous pouvez définir l'intervalle de temps ainsi que le nombre de tentatives. Les tentatives s'arrêteront dès que l'opération réussira OU que le nombre de tentatives sera atteint, le premier de ces deux cas prévalant.

Sauvegarde incrémentielle/différentielle rapide

Cette option est effective pour une sauvegarde incrémentielle et différentielle de niveau disque.

Cette option n'est pas efficace (toujours désactivée) pour les volumes formatés avec les systèmes de fichiers JFS, ReiserFS3, ReiserFS4, ReFS ou XFS.

Le préréglage est le suivant : **Activé**.

Une sauvegarde incrémentielle ou différentielle capture uniquement des modifications de données. Pour accélérer le processus de sauvegarde, le programme détermine si un fichier a été modifié ou non grâce à la taille du fichier et à la date / l'heure à laquelle le fichier a été modifié pour la dernière fois. Si cette fonctionnalité est désactivée, le programme comparera les contenus entiers des fichiers à ceux stockés dans la sauvegarde.

Filtres de fichiers (Inclusions/Exclusions)

Utilisez les filtres de fichiers pour inclure certains fichiers et dossiers dans une sauvegarde, ou en exclure d'une sauvegarde.

Sauf indication contraire, les filtres de fichiers sont disponibles pour les sauvegardes d'un ordinateur complet, de disque et de niveau fichier.

Les filtres de fichiers ne sont pas disponibles avec les systèmes de fichiers XFS, JFS, exFAT et ReiserFS4. Pour plus d'informations, voir "Systèmes de fichiers pris en charge" (p. 55).

Les filtres de fichiers ne s'appliquent pas aux disques dynamiques (volumes LVM ou LDM) de machines virtuelles sauvegardées en mode sans agent, par Agent pour VMware, Agent pour Hyper-V ou Agent pour Scale Computing, par exemple.

Pour activer les filtres de fichiers

1. Dans un plan de protection, développez le module **Sauvegarde**.
2. Dans **Options de sauvegarde**, cliquez sur **Modifier**.
3. Sélectionnez **Filtres de fichiers (Inclusions/Exclusions)**.
4. Choisissez les options parmi celles décrites ci-dessous.

Filtres d'inclusion et d'exclusion

Il existe deux filtres : le filtre d'inclusion et le filtre d'exclusion.

- **Incluez uniquement les fichiers correspondant aux critères suivants**

  Si vous indiquez `C:\Fichier.exe` dans le filtre d'inclusion, ce fichier sera le seul à être sauvegardé, même si vous sélectionnez la sauvegarde Toute la machine.

  Remarque
  Ce filtre n'est pas pris en charge pour les sauvegardes de niveau fichier lorsque le format de sauvegarde est **Version 11** et que la destination de sauvegarde n'est pas le stockage dans le cloud.

- **Excluez les fichiers correspondant aux critères suivants**

  Si vous indiquez `C:\Fichier.exe` dans le filtre d'exclusion, ce fichier sera ignoré lors de la sauvegarde, même si vous sélectionnez la sauvegarde Toute la machine.

Vous pouvez utiliser les deux filtres en même temps. Le filtre d'exclusion est prioritaire sur le filtre d'inclusion, c'est-à-dire que si vous indiquez `C:\File.exe` dans les deux champs, ce fichier sera ignoré lors de la sauvegarde.

Critères de filtre

Vous pouvez utiliser comme critères de filtre des noms de fichiers et de dossiers, des chemins complets vers des fichiers et des dossiers, ainsi que des masques avec des symboles de caractères génériques.

Les critères de filtre ne sont pas sensibles à la casse. Par exemple, lorsque vous spécifiez `C:\Temp`, cela revient à sélectionner `C:\TEMP` et `C:\temp`.

- Nom

  Spécifiez le nom du fichier ou du dossier, comme `Document.txt`. Tous les fichiers et dossiers portant ce nom seront sélectionnés.
- Chemin complet

  Spécifiez le chemin d'accès complet au fichier ou dossier, en commençant par la lettre du lecteur (lors de la sauvegarde de Windows) ou le répertoire racine (lors de la sauvegarde de Linux ou macOS). Sous Windows, Linux et macOS, vous pouvez utiliser des barres obliques (par exemple, `C:/Temp/Fichier.tmp`). Sous Windows, vous pouvez également utiliser les barres obliques inverses traditionnelles (par exemple, `C:\Temp\fichier.tmp`).

Important
Si le système d'exploitation de l'ordinateur sauvegardé n'est pas détecté correctement pendant la sauvegarde de disque, les filtres de chemin complet vers les fichiers ne fonctionneront pas. Pour un filtre d'exclusion, un avertissement s'affichera. En présence d'un filtre d'inclusion, la sauvegarde échouera.

Par exemple, un chemin d'accès complet à un fichier peut être `C:\Temp\Fichier.tmp`. Un filtre de chemin d'accès complet, qui inclut la lettre du lecteur ou le répertoire racine (par exemple `C:\Temp\Fichier.tmp` ou `C:\Temp\*`) entraînera un avertissement ou une erreur.

Un filtre qui n'inclut pas la lettre du lecteur ni le répertoire racine (par exemple `Temp\*` ou `Temp\File.tmp`) ou un filtre qui commence par un astérisque (par exemple, `*C:\`) n'entraînera pas d'avertissement ni d'erreur. Toutefois, si le système d'exploitation de l'ordinateur sauvegardé n'est pas détecté correctement, ces filtres ne fonctionneront pas.

- Masque

  Vous pouvez utiliser les caractères génériques suivants pour les noms et les chemins complets : astérisque (*), double astérisque (**) et point d'interrogation (?).

  L'astérisque (*) représente zéro ou plusieurs caractères. Par exemple, le critère de filtre **Doc*.txt** englobe les fichiers tels que `Doc.txt` et `Document.txt`.

  Le double astérisque (**) représente zéro ou plusieurs caractères, y compris le caractère barre oblique. Par exemple, le critère ****/Docs/**.txt** correspond à tous les fichiers .txt dans tous les sous-dossiers de tous les dossiers `Docs`. Vous ne pouvez utiliser le caractère générique de double astérisque (**) que pour les sauvegardes au format Version 12.

  Le point d'interrogation (?) représente un seul caractère. Par exemple, **Doc?.txt** englobe les fichiers tels que `Doc1.txt` et `Docs.txt`, mais pas les fichiers `Doc.txt` ou `Doc11.txt`.

Instantané de sauvegarde de niveau fichier

Cette option est effective uniquement pour une sauvegarde de niveau fichier.

Cette option définit s'il faut sauvegarder des fichiers un par un ou en prenant une image statique instantanée des données.

Remarque
Les fichiers situés sur des réseaux partagés sont toujours sauvegardés un à la fois.

Le préréglage est le suivant :

- Si des machines sous Linux uniquement sont sélectionnées pour la sauvegarde : **Ne pas créer d'instantané.**
- Sinon : **Créer un instantané si cela est possible.**

Vous pouvez sélectionner l'une des options suivantes :

- **Créer un instantané si cela est possible**

  Sauvegarder directement les fichiers s'il n'est pas possible de prendre une image statique.
- **Toujours créer un instantané**

  Utiliser une image statique permet la sauvegarde de tous les fichiers, y compris les fichiers ouverts en accès exclusif. Les fichiers seront sauvegardés au même point dans le temps. Choisissez ce paramètre uniquement si ces facteurs sont critiques, c'est à dire que sauvegarder des fichiers sans image statique ne sert à rien. Si une image statique ne peut pas être prise, la sauvegarde échoue.
- **Ne pas créer d'instantané**

  Toujours sauvegarder les fichiers directement. Essayer de sauvegarder des fichiers qui sont ouverts en accès exclusif entraînera une erreur de lecture. Les fichiers dans la sauvegarde peuvent ne pas être constants dans le temps.

Données d'investigation

Les virus, malware et ransomware peuvent réaliser des activités malveillantes comme des vols ou des modifications de données. De telles activités doivent être examinées, mais cela est possible uniquement si vous en conservez une preuve numérique. Cependant, ces preuves numériques, par ex. des fichiers ou des traces d'activité, peuvent être supprimées ou l'ordinateur sur lequel l'activité malveillante s'est produite peut devenir indisponible.

Les sauvegardes avec des données d'investigation permettent aux enquêteurs d'analyser les zones de disque qui ne sont généralement pas incluses dans une sauvegarde de disque habituelle. L'option de sauvegarde avec **Données d'investigation** vous permet de recueillir les preuves pouvant être utilisées dans les enquêtes d'investigation : captures d'écran d'espace de disque libre, vidages mémoire et captures d'écran de processus en cours d'exécution.

Les sauvegardes avec données d'investigation sont automatiquement notarisées.

Actuellement, l'option de sauvegarde avec **Données d'investigation** est disponible uniquement pour les sauvegardes complètes d'ordinateurs Windows exécutant les versions de système d'exploitation suivantes :

- Windows 8.1, Windows 10
- Windows Server 2012 R2 – Windows Server 2019

Les sauvegardes avec des données d'investigation ne sont pas disponibles pour les ordinateurs suivants :

- Ordinateurs connectées à votre réseau via VPN et qui n'ont pas d'accès direct à Internet
- Ordinateurs avec des disques chiffrés par BitLocker

Remarque
Une fois un plan de protection appliqué à un ordinateur avec un module de **sauvegarde**, les paramètres des données d'investigation ne peuvent pas être modifiés. Pour utiliser des paramètres de données d'investigation différents, créez un nouveau plan de protection.

Vous pouvez stocker les sauvegardes avec données d'investigations sous les emplacements suivants :

- Stockage dans le Cloud
- Dossier local

  Remarque
  Le stockage sur un dossier local n'est pris en charge que sur les disques durs externes connectés via USB.
  Le stockage sur les disques dynamiques locaux n'est pas pris en charge pour les sauvegardes avec données d'investigation.

- Dossier réseau

Processus de sauvegarde d'investigation

Le système effectue les opérations suivantes lors d'un processus de sauvegarde d'investigation :

1. Collecte le vidage mémoire brut et la liste des processus en cours d'exécution.
2. Redémarre automatiquement une machine dans le support de démarrage.
3. Crée la sauvegarde qui inclut aussi bien l'espace occupé que l'espace non alloué.
4. Notarise les disques sauvegardés.
5. Redémarre dans le système d'exploitation en ligne et poursuit l'exécution du plan (par exemple, réplication, rétention, validation et autre).

Pour configurer un recueil de données d'investigation

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**. Le plan de protection peut également être créé depuis l'onglet **Gestion**.
2. Sélectionnez le terminal et cliquez sur **Protection**.
3. Dans le plan de protection, activez le module **Sauvegarde**.
4. Dans **Quoi sauvegarder**, sélectionnez **Toute la machine**.
5. Dans **Options de sauvegarde**, cliquez sur **Modifier**.
6. Trouvez l'option **Données d'investigation**.
7. Activez **Collecter des données d'investigation**. Le système recueillera automatiquement un vidage de mémoire et créera un instantané des processus en cours d'exécution.

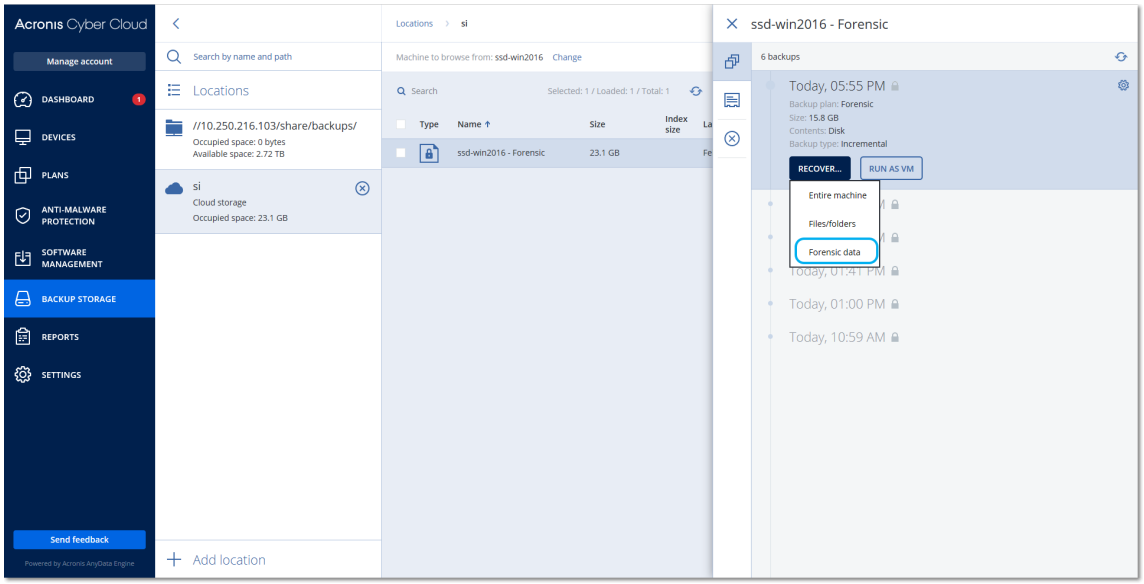
Remarque
Il se peut que le vidage mémoire complet contienne des données sensibles telles que des mots de passe.

8. Précisez l'emplacement.
9. Cliquez sur **Exécuter maintenant** pour exécuter immédiatement une sauvegarde avec données d'investigation, ou attendez que la sauvegarde ait été créée selon la planification.
10. Accédez à **Surveillance** > **Activités**, puis vérifiez que la sauvegarde avec données d'investigation a bien été créée.

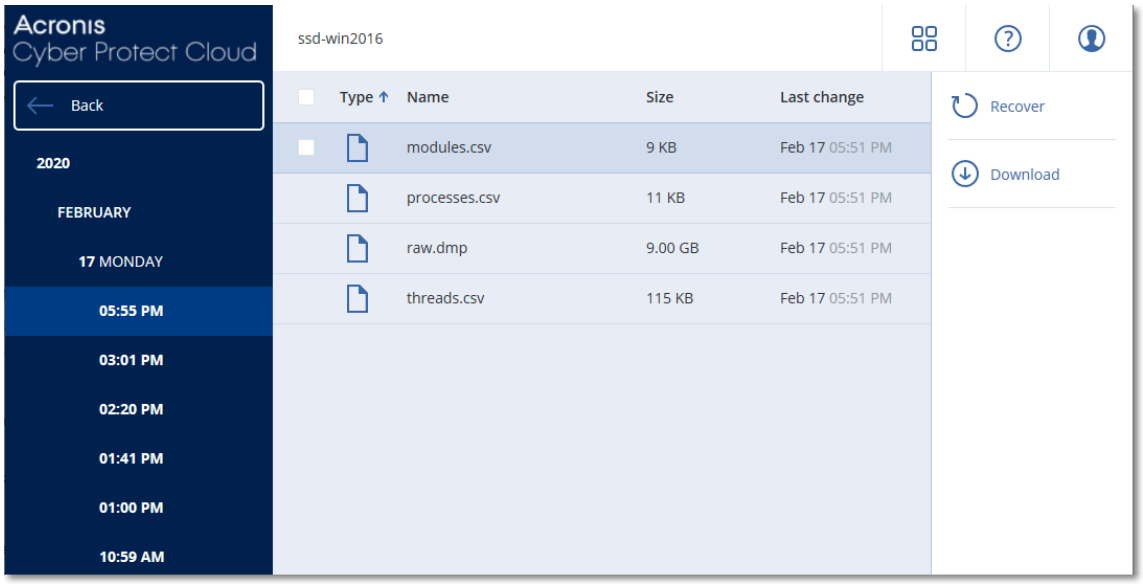
Par conséquent, les sauvegardes incluront les données d'investigation que vous pourrez récupérer et analyser. Les sauvegardes avec données d'investigation sont identifiées et peuvent être filtrées parmi d'autres sauvegardes dans **Stockage de sauvegarde** > **Emplacements** à l'aide de l'option **Uniquement avec les données d'investigation**.

Comment récupérer des données d'investigation à partir d'une sauvegarde ?

1. Dans la console Cyber Protect, accédez à **Stockage de sauvegarde** et sélectionnez l'emplacement avec les sauvegardes contenant des données d'investigation.
2. Sélectionnez la sauvegarde avec données d'investigation et cliquez sur **Afficher les sauvegardes**.
3. Cliquez sur **Restaurer** pour la sauvegarde avec données d'investigation.
   - Pour obtenir uniquement les données d'investigation, cliquez sur **Données d'investigation**.



Le système affichera un dossier avec données d'investigation. Sélectionnez un fichier de vidage mémoire ou tout autre fichier d'investigation, puis cliquez sur **Télécharger**.



- Pour restaurer une sauvegarde d'investigation, cliquez sur **Toute la machine**. Le système restaurera la sauvegarde sans mode de démarrage. Il sera donc possible de vérifier que le disque n'a pas été modifié.

Vous pouvez utiliser le vidage mémoire fourni avec plusieurs logiciels d'investigation tiers ; utilisez par exemple Volatility Framework sur https://www.volatilityfoundation.org/ pour une analyse plus complète de la mémoire.

Notarisation des sauvegardes avec les données d'investigation

Pour garantir qu'une sauvegarde avec données d'investigation est exactement l'image qui a été prise et qu'elle n'a pas été compromise, le module de sauvegarde fournit la notarisation des sauvegardes avec données d'investigation.

Fonctionnement

La notarisation vous permet de prouver qu'un disque contenant des données d'investigation est authentique et inchangé depuis sa sauvegarde.

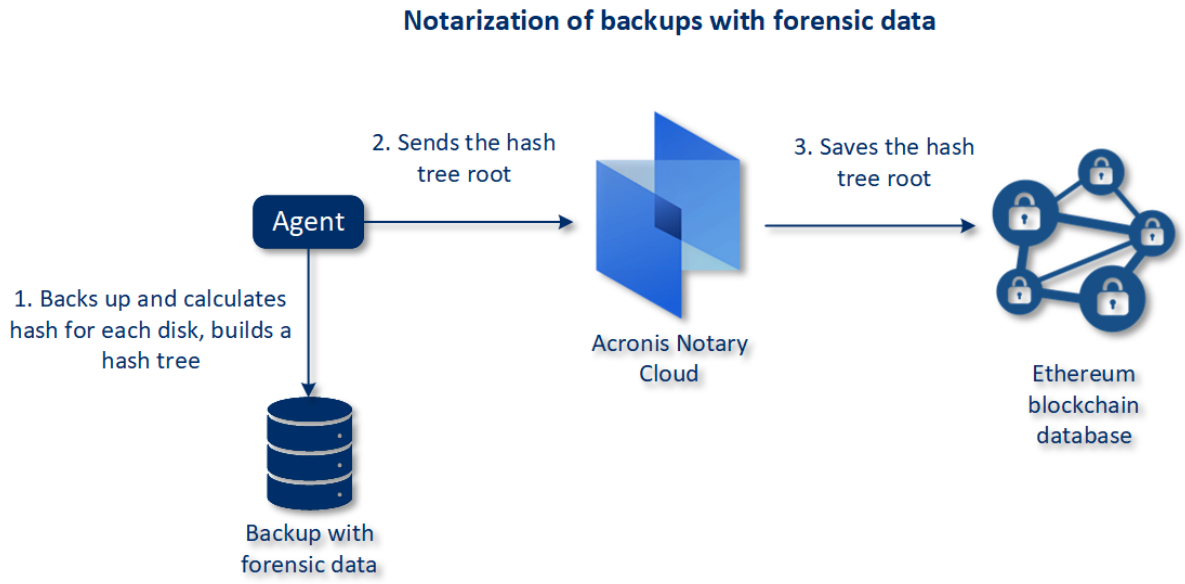
Lors d'une sauvegarde, l'agent calcule les codes de hachage des disques sauvegardés, crée un arbre de hachage, enregistre l'arbre dans la sauvegarde, puis envoie la racine de l'arbre de hachage au service Notary. Le service Notary enregistre la racine de l'arbre de hachage dans la base de données blockchain Ethereum pour s'assurer que cette valeur ne change pas.

Lors de la vérification de l'authenticité d'un disque contenant des données d'investigation, l'agent calcule le hachage du disque, puis le compare avec le hachage stocké dans l'arbre de hachage sauvegardé. Si ces hachages ne correspondent pas, le disque n'est pas authentique. Sinon, l'authenticité du disque est garantie par l'arbre de hachage.

Pour vérifier que l'arbre de hachage n'a pas été compromis, l'agent envoie la racine de l'arbre de hachage au service Notary. Le service Notary la compare avec celle stockée dans la base de données

blockchain. Si les hachages correspondent, le disque sélectionné est authentique. Sinon, le logiciel affiche un message indiquant que le disque n'est pas authentique.

Le schéma ci-dessous montre brièvement le processus de notarisation pour les sauvegardes avec données d'investigation.



Pour vérifier manuellement la sauvegarde de disque notarisée, vous pouvez en obtenir le certificat et suivre la procédure de vérification affichée avec le certificat, en utilisant l'outil tibxread.

Obtenir le certificat pour les sauvegardes avec données d'investigation

Pour obtenir le certificat pour une sauvegarde avec données d'investigation, procédez comme suit :

1. Accédez à **Stockage de sauvegarde** et sélectionnez la sauvegarde avec données d'investigation.
2. Restaurez la machine entière.
3. Le système ouvre la vue **Mappage de disque**.
4. Cliquez sur l'icône **Obtenir certificat** pour le disque.
5. Le système génèrera le certificat et ouvrira une nouvelle fenêtre dans votre navigateur, avec le certificat. Sous le certificat s'afficheront les instructions concernant la vérification manuelle de la sauvegarde de disque notarisée.

L'outil « tibxread » pour obtenir les données sauvegardées

Cyber Protection fournit l'outil, intitulé `tibxread`, pour la vérification manuelle de l'intégrité du disque sauvegardé. L'outil vous laisse toujours obtenir les données d'une sauvegarde et calcule le hachage du disque indiqué. L'outil est installé automatiquement avec les composants suivants : Agent pour Windows, agent pour Linux et agent pour Mac.

Le chemin d'installation : le même dossier que celui que détient l'agent (par exemple, `C:\Program Files\BackupClient\BackupAndRecovery`).

Les emplacements pris en charge sont les suivants :

- Le disque local
- Le dossier réseau (CIFS/SMB) auquel vous pouvez accéder sans identifiants.

  En cas de dossier réseau protégé par mot de passe, vous pouvez monter le dossier réseau sur le dossier local à l'aide des outils OS, puis le dossier local comme source pour cet outil.
- Le stockage sur le Cloud

  Vous devez fournir l'URL, le port et le certificat. Vous pouvez obtenir l'URL et le port à partir de la clé de registre Windows ou des fichiers de configuration sur les machines Linux/Mac.

  Pour Windows :

  ```
  HKEY_LOCAL_
  MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Defa
  ult\<tenant_login>\FesUri
  ```

  Pour Linux :

  ```
  /etc/Acronis/BackupAndRecovery.config
  ```

  Pour macOS :

  ```
  /Library/Application Support/Acronis/Registry/BackupAndRecovery.config
  ```

  Vous pouvez trouver le certificat dans les emplacements suivants :

  Pour Windows :

  ```
  %allusersprofile%\Acronis\BackupAndRecovery\OnlineBackup\Default
  ```

  Pour Linux :

  ```
  /var/lib/Acronis/BackupAndRecovery/OnlineBackup/Default
  ```

  Pour macOS :

  ```
  /Library/Application Support/Acronis/BackupAndRecovery/OnlineBackup/Default
  ```

L'outil contient les commandes suivantes :

- `list backups`
- `list content`
- `get content`
- `calculate hash`

list backups

Répertorie les points de récupérations dans une sauvegarde.

SYNOPSIS :

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

Options

```
--loc=URI
--arc=BACKUP_NAME
--raw
--utc
--log=PATH
```

Modèle de sortie :

```
GUID   Date   Horodatage date
----   ------ --------------
<guid> <date> <timestamp>
```

<guid> – un GUID de sauvegarde.

<date> – une date de création de la sauvegarde. Le format est « JJ.MM.AAAA HH24:MM:SS ». En fuseau horaire local par défaut (peut être modifié à l'aide de l'option --utc).

Exemple de sortie :

```
GUID   Date   Horodatage date
----   ------ --------------
516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865
516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925
```

list content

Répertorie le contenu dans un point de restauration.

SYNOPSIS :

```
tibxread list content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID
--raw --log=PATH
```

Options

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--raw
--log=PATH
```

Modèle de sortie :

```
Disque     Taille   Statut de notarisation
-------- ------ --------------------
<number> <size> <notarization_status>
```

<numéro> – identificateur du disque.

<taille> – taille in octets.

<statut_de_notarisation> – les statuts suivants sont possibles : Sans notarisation, Notarisé, Prochaine sauvegarde.

Exemple de sortie :

```
Disque     Taille   Statu de notarisation
-------- ------ --------------
1        123123465798 notarisé
2        123123465798 notarisé
```

obtenir le contenu

Écrit le contenu du disque indiqué dans le point de récupération sur la sortie standard (stdout).

SYNOPSIS :

```
tibxread get content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID -
-disk=DISK_NUMBER --raw --log=PATH --progress
```

Options

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
--progress
```

calculer le hachage

Calcule le hachage du disque indiqué dans le point de reprise à l'aide de l'algorithme SHA-2 (256 bits) et l'écrit sur le stdout.

SYNOPSIS :

```
tibxread calculate hash --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_
ID --disk=DISK_NUMBER --raw --log=PATH --progress
```

Options

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
```

Description des options

Option	Description
--arc=BACKUP_NAME	Le nom du fichier de sauvegarde que vous pouvez obtenir depuis les propriétés de sauvegarde de la console Cyber Protect. Le fichier de sauvegarde doit être indiqué par l'extension .tibx.
--backup=RECOVERY_POINT_ID	L'identificateur du point de restauration
--disk=DISK_NUMBER	Numéro de disque (le même que celui écrit sur la sortie de la commande « Obtenir le contenu »)

--loc=URI	Une URI d'emplacement de sauvegarde. Les formats possibles de l'option « --loc » sont :
	• Nom du chemin local (Windows)
	`c:/upload/backups`
	• Nom du chemin local (Linux)
	`/var/tmp`
	• SMB/CIFS
	`\\server\folder`
	• Stockage dans le Cloud
	`--loc=<IP_address>:443 --cert=<path_to_certificate> [--storage_path=/1]`
	`<IP_address>` – vous le trouverez dans la clé de registre dans Windows : HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<tenant_login>\FesUri
	`<path_to_certificate>` – un chemin vers le fichier du certificat, pour accéder à Cyber Protect Cloud. Par exemple, sous Windows, ce certificat est situé dans `C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<username>.crt` où <username> – est le nom de compte nécessaire pour accéder à Cyber Protect Cloud.

--log=PATH	Permet d'écrire les journaux via le chemin indiqué (chemin local uniquement, le format est le même que pour le paramètre `--loc=URI`). Le niveau de journalisation est DÉBOGAGE.
--	Un mot de passe de chiffrement pour votre sauvegarde. Si la sauvegarde n'est pas

password=PASSWORD	chiffrée, laissez cette valeur vierge.

--raw	Masque l'en-tête (deux premières lignes) dans la sortie de commande. Ceci est utilisé lorsque la sortie de commande doit être analysée.
	Exemple de sortie sans « `--raw` » :
	`GUID Date Horodatage date`
	`---- ------ --------------`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`
	Sortie avec « `--raw` » :
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`

--utc	Affiche les dates en UTC

--progress	Affiche la progression de l'opération.
	Par exemple :
	`1 %`
	`2 %`
	`3 %`
	`4 %`
	`...`
	`100 %`

Troncation de journal

Cette option est effective pour la sauvegarde des bases de données backup Microsoft SQL Server et la sauvegarde de niveau disque avec la sauvegarde de l'application Microsoft SQL Server activée.

Cette option définit si les journaux de transaction SQL Server sont tronqués après la réussite d'une sauvegarde.

Le préréglage est le suivant : **Activé**.

Lorsque cette option est activée, une base de données peut être restaurée uniquement à un point dans le temps d'une sauvegarde créée par ce logiciel. Désactivez cette option si vous sauvegardez les journaux de transaction en utilisant le moteur de sauvegarde natif de Microsoft SQL Server. Vous pourrez appliquer les journaux de transaction après une restauration et ainsi restaurer une base de données à n'importe quel point dans le temps.

Prise d'instantanés LVM

Cette option est effective uniquement pour les machines physiques.

Cette option est effective pour la sauvegarde de volumes de niveau disque gérée par Linux Logical Volume Manager (LVM). Ces volumes sont également appelés volumes logiques.

Cette option définit comment prendre un instantané d'un volume logique. Le logiciel de sauvegarde peut effectuer cette opération ou la confier à Linux Logical Volume Manager (LVM).

Le préréglage est le suivant : **Par le logiciel de sauvegarde**.

- **Par le logiciel de sauvegarde**. Les données de l'instantané sont principalement conservées dans RAM. La sauvegarde est plus rapide et l'espace non alloué sur le groupe de volumes n'est pas requis. Par conséquent, nous vous recommandons de ne modifier le préréglage que si vous rencontrez des problèmes avec la sauvegarde de volumes logiques.
- **Par LVM**. L'instantané est stocké dans un espace non alloué du groupe de volumes. Si l'espace non alloué est manquant, l'instantané sera pris par le logiciel de sauvegarde.

L'instantané est utilisé uniquement pendant l'opération de sauvegarde et il est supprimé automatiquement lorsque cette opération est terminée. Aucun fichier temporaire n'est conservé.

Points de montage

Cette option est efficace uniquement sous Windows, pour la sauvegarde de niveau fichier d'une source de données qui inclut des volumes montés ou des volumes partagés de cluster.

Cette option est efficace seulement lorsque vous sélectionnez un dossier à sauvegarder qui est supérieur au point de montage dans l'arborescence des dossiers. (Un point de montage est un dossier sur lequel un volume supplémentaire est logiquement attaché.)

- Si un tel dossier (un dossier parent) est sélectionné pour la sauvegarde, et que l'option **Points de montage** est activée, tous les fichiers situés sur le volume monté seront inclus dans la sauvegarde. Si l'option **Points de montage** est désactivée, le point de montage dans la sauvegarde sera vide.

  Pendant la restauration d'un dossier parent, le contenu du point de montage est ou n'est pas restauré, selon que l'option **Points de montage** pour la restauration est activée ou désactivée.
- Si vous sélectionnez directement le point de montage, ou sélectionnez n'importe quel dossier dans le volume monté, les dossiers sélectionnés seront considérés comme des dossiers ordinaires. Ils seront sauvegardés, peu importe l'état de l'option **Points de montage**, et restaurés peu importe l'état de l'option **Points de montage** pour la restauration.

Le préréglage est le suivant : **Désactivé**.

Remarque
Vous pouvez sauvegarder des machines virtuelles Hyper-V résidant sur un volume partagé de cluster en sauvegardant les fichiers nécessaires ou l'ensemble du volume avec une sauvegarde de niveau fichier. Mettez simplement les machines virtuelles hors tension afin de vous assurer qu'elles sont sauvegardées dans un état cohérent.

Exemple

Supposons que le dossier **C:\Data1** est un point de montage pour le volume monté. Le volume contient les dossiers **Folder1** et **Folder2**. Vous créez un plan de protection pour la sauvegarde de niveau fichier de vos données.

Si vous cochez la case pour le volume C et activez l'option **Points de montage**, le dossier **C:\Data1** dans votre sauvegarde contiendra les dossiers **Folder1** et **Folder2**. Lorsque vous restaurez les données sauvegardées, soyez conscient de la bonne utilisation de l'option **Points de montage** pour la restauration.

Si vous cochez la case pour le volume C et désactivez l'option **Points de montage**, le dossier **C:\Data1** dans votre sauvegarde sera vide.

Si vous cochez la case pour les dossiers **Data1**, **Folder1** ou **Folder2**, les dossiers cochés seront inclus dans la sauvegarde comme des dossiers ordinaires, peu importe l'état de l'option **Points de montage**.

Snapshot Multi-volume

Cette option est effective pour les sauvegardes des machines physiques sous Windows ou Linux.

Cette option s'applique à une sauvegarde de niveau disque. Cette option s'applique également à une sauvegarde de niveau fichier lorsque la sauvegarde de niveau fichier est effectuée en réalisant un instantané. (L'option « Image statique de sauvegarde de niveau fichier » détermine si un instantané est pris pendant la sauvegarde de niveau fichier).

Cette option détermine si des instantanés de plusieurs volumes doivent être pris simultanément ou un par un.

Le préréglage est le suivant :

- Si au moins une machine sous Windows est sélectionnée pour la sauvegarde : **Activé**.
- Sinon : **Désactivé**.

Lorsque cette option est activée, des instantanés de tous les volumes en cours de sauvegarde sont créés simultanément. Utilisez cette option pour créer une sauvegarde cohérente dans le temps de données éparpillées sur plusieurs volumes, par exemple pour une base de données Oracle.

Lorsque cette option est désactivée, les instantanés des volumes sont pris l'un après l'autre. Par conséquent, si les données sont éparpillées sur plusieurs volumes, la sauvegarde en résultant peut ne pas être cohérente.

Reprise en un seul clic

Remarque
Cette fonctionnalité est disponible avec le pack Advanced Backup.

Avec la restauration en un clic, vous pouvez restaurer automatiquement une sauvegarde de disque de votre ordinateur Windows ou Linux. Cette sauvegarde peut être une sauvegarde de l'ensemble de l'ordinateur, ou de disques ou volumes spécifiques de cet ordinateur.

La restauration en un seul clic prend en charge les opérations suivantes :

- Restauration automatique à partir de la dernière sauvegarde
- Restauration à partir d'une sauvegarde spécifique (également connue sous le nom de point de restauration) dans l'archive de sauvegardes

La restauration en un seul clic prend en charge les stockages de sauvegarde suivants :

- Secure Zone
- Dossier local
- Dossier réseau
- Stockage dans le Cloud

Important
Suspendez le chiffrement BitLocker jusqu'au prochain redémarrage de votre ordinateur lorsque vous effectuez l'une des opérations suivantes :

- Créer, modifier ou supprimer Secure Zone.
- Activer ou désactiver Startup Recovery Manager.
- [Uniquement si Startup Recovery Manager n'a pas déjà été activé] Exécuter la première sauvegarde après avoir activé la restauration en un seul clic dans le plan de protection. Cette opération active automatiquement Startup Recovery Manager.
- Mettre à jour Startup Recovery Manager, par exemple en mettant à jour la protection.

Si le chiffrement BitLocker n'a pas été suspendu au cours de ces opérations, vous devrez spécifier votre code PIN Bitlocker après avoir redémarré votre ordinateur.

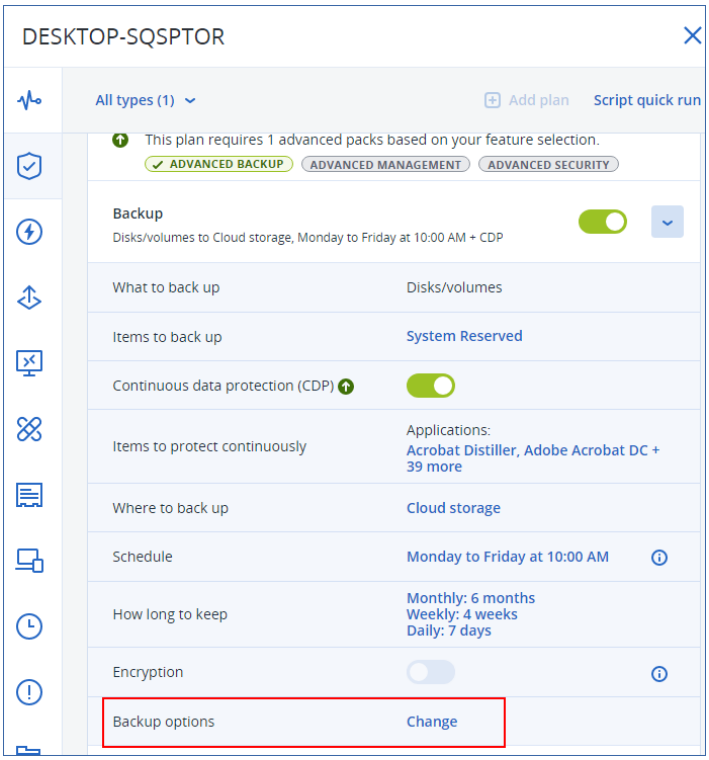
Activation de la restauration en un clic

La restauration en un clic est une option de sauvegarde dans le plan de protection. Pour plus d'informations sur la création d'un plan, voir "Création d'un plan de protection" (p. 223).

Remarque
L'activation de la restauration en un clic active également Startup Recovery Manager sur la machine cible. Si Startup Recovery Manager ne peut pas être activé, l'opération de sauvegarde qui crée des sauvegardes de récupération en un clic échouera. Pour plus d'informations sur Startup Recovery Manager, voir "Startup Recovery Manager" (p. 770).

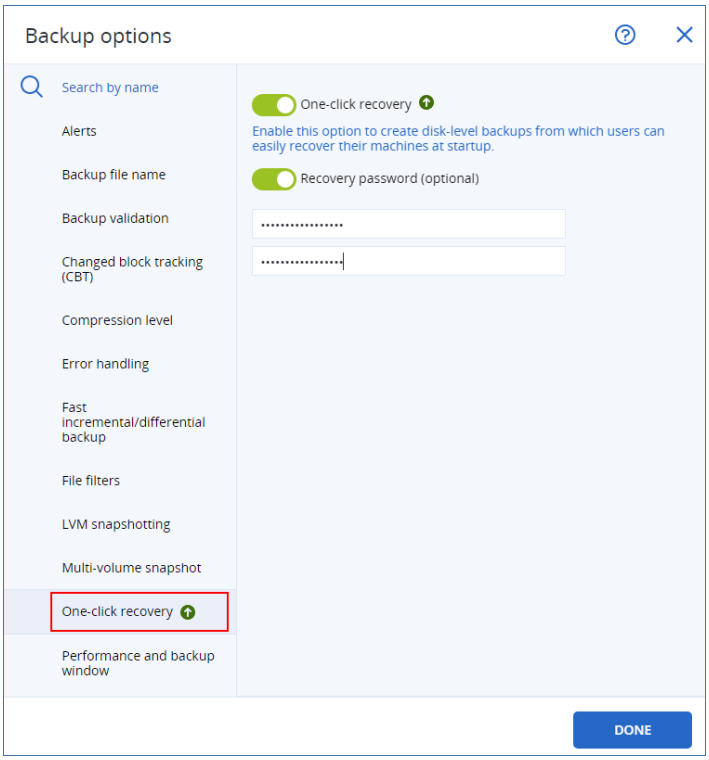
Pour activer la restauration en un clic

1. Dans le plan de protection, développez le module **Sauvegarde**.
2. Dans **Quoi sauvegarder**, sélectionnez **Toute la machine** ou **Disque/volumes**.
3. [Si vous avez sélectionné **Disque/volumes**]. Dans **Éléments à sauvegarder**, spécifiez le disque ou les volumes à sauvegarder.
4. Dans **Options de sauvegarde**, cliquez sur **Modifier**, puis sélectionnez **Reprise en un seul clic**.



5. Activez le commutateur **Reprise en un seul clic**.
6. [Facultatif] Activez le commutateur **Mot de passe de reprise**, puis définissez un mot de passe.

Important
Nous vous recommandons vivement de spécifier un mot de passe de reprise. Assurez-vous que l'utilisateur qui exécute la restauration en un seul clic sur la machine cible connaît ce mot de passe.



7. Cliquez sur **Valider**.
8. Configurez les autres éléments du plan de protection selon vos besoins, puis enregistrez le plan.

En conséquence, après que le plan de protection a été exécuté et a créé une sauvegarde, la restauration en un seul clic devient accessible aux utilisateurs de la machine protégée.

Important
La restauration en un clic devient temporairement indisponible lorsque vous mettez à jour l'agent de protection. Pour la réactiver, exécutez une sauvegarde. Une fois la sauvegarde terminée, vous pourrez à nouveau effectuer une restauration en un clic.

Désactivation de la Restauration en un clic

Vous pouvez désactiver la Restauration en un clic pour une ressource spécifique de la manière suivante :

- Désactivez l'option **Restauration en un clic** dans le plan de protection appliqué à la ressource.
- Révoquez le plan de protection dans lequel l'option **Restauration en un clic** est activée.
- Supprimez le plan de protection dans lequel l'option **Restauration en un clic** est activée.

Restauration d'une machine à l'aide de la restauration en un seul clic

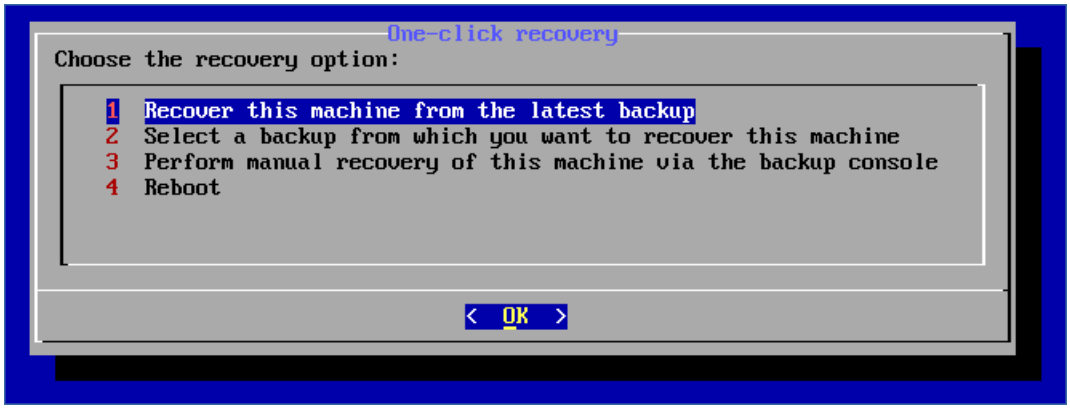
Prérequis

- Un plan de protection avec l'option de sauvegarde **Reprise en un seul clic** activée est appliqué à l'ordinateur.

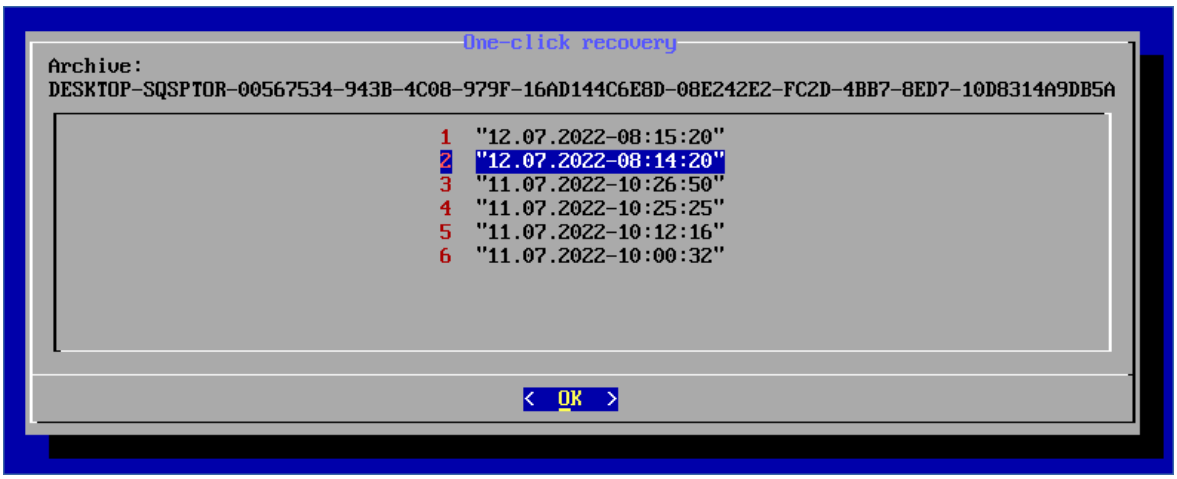
- Il existe au moins une sauvegarde de disque de l'ordinateur.

Pour restaurer une machine

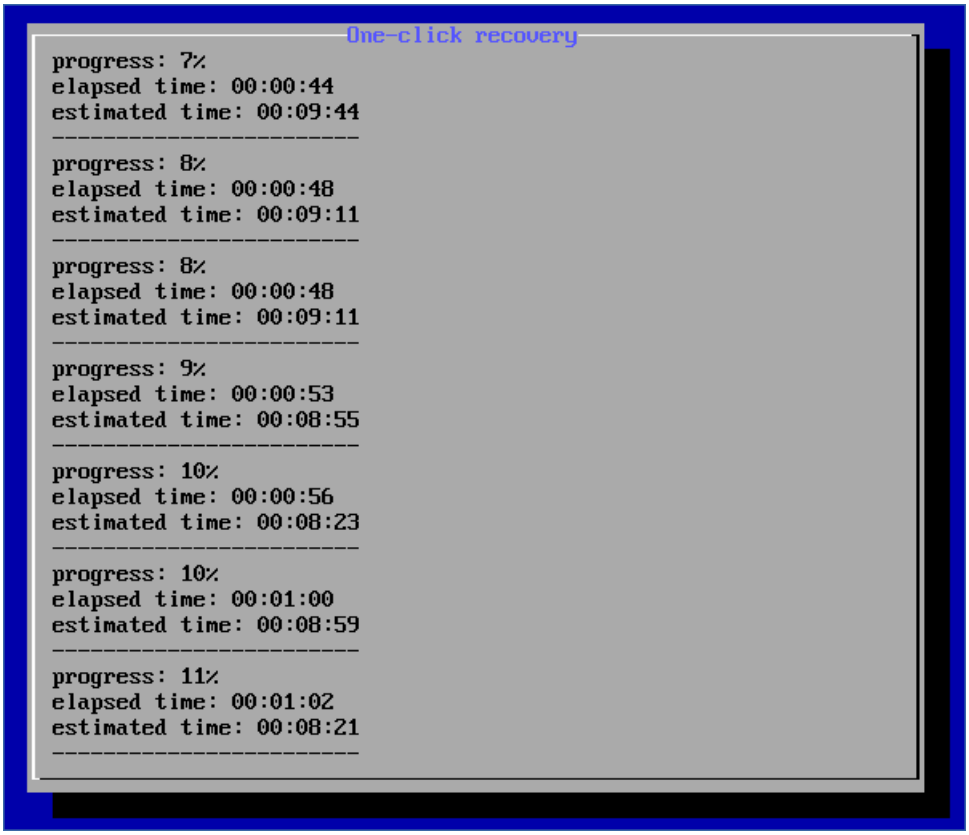
1. Redémarrez la machine que vous voulez restaurer.
2. Lors du redémarrage, appuyez sur F11 pour entrer dans Startup Recovery Manager.
   La fenêtre de support de secours s'ouvre.
3. Sélectionnez **Acronis Cyber Protect**.
4. [Si un mot de passe de récupération a été indiqué dans le plan de protection] Saisissez le mot de passe de récupération, puis, cliquez sur **OK**.
5. Sélectionnez une option de restauration en un seul clic.
   - Pour restaurer automatiquement la dernière sauvegarde en date, sélectionnez la première option, puis cliquez sur **OK**.
   - Pour restaurer une autre sauvegarde dans l'archive de sauvegardes, sélectionnez la deuxième option, puis cliquez sur **OK**.



6. Confirmez votre choix en cliquant sur **Oui**.
   La fenêtre de support de secours s'ouvre, puis disparaît. La procédure de restauration se poursuit sans cette interface.
7. [Si vous avez choisi de restaurer une sauvegarde spécifique] Sélectionnez la sauvegarde que vous souhaitez restaurer, puis cliquez sur **OK**.



Au bout d'un temps, la restauration commence et sa progression s'affiche. Une fois la restauration terminée, votre ordinateur redémarre.



Performance et créneau de sauvegarde

Cette option vous permet de définir l'un de trois niveaux de performances de sauvegarde (faibles, élevées, interdites) pour chaque heure au cours d'une semaine. Ainsi, vous pouvez définir une fenêtre de temps pendant laquelle les sauvegardes seront autorisées à démarrer et s'exécuter. Les performances faibles et élevées sont configurables sur le plan de la priorité du processus et de la vitesse de sortie.

Cette option n'est pas disponible pour les sauvegardes exécutées par les agents Cloud, telles que les sauvegardes de sites Web ou celles de serveurs situés sur le site de reprise du Cloud.

Cette option est effective uniquement pour les processus de sauvegarde et de réplication de sauvegarde. Les commandes post-sauvegarde et d'autres opérations incluses dans un plan de protection (par exemple, la validation) s'exécuteront en dépit de cette option.

Le préréglage est le suivant : **Désactivé**.

Quand cette option est désactivée, les sauvegardes sont autorisées à s'exécuter à tout moment, avec les paramètres suivants (cela n'a pas d'importance si les paramètres ont été modifiés par rapport à la valeur préréglée) :

- Priorité du processeur : **Faible** (dans Windows, cela correspond à **Inférieure à la normale**)
- Vitesse de sortie : **Illimitée**

Lorsque cette option est activée, les sauvegardes planifiées sont autorisées ou bloquées en fonction des paramètres de performances spécifiés pour l'heure courante. Au début d'une heure où les sauvegardes sont bloquées, un processus de sauvegarde est automatiquement arrêté et une alerte est générée. Même si les sauvegardes planifiées sont bloquées, une sauvegarde peut être lancée manuellement. Elle utilisera les paramètres de performances de la dernière heure au cours de laquelle les sauvegardes ont été autorisées.

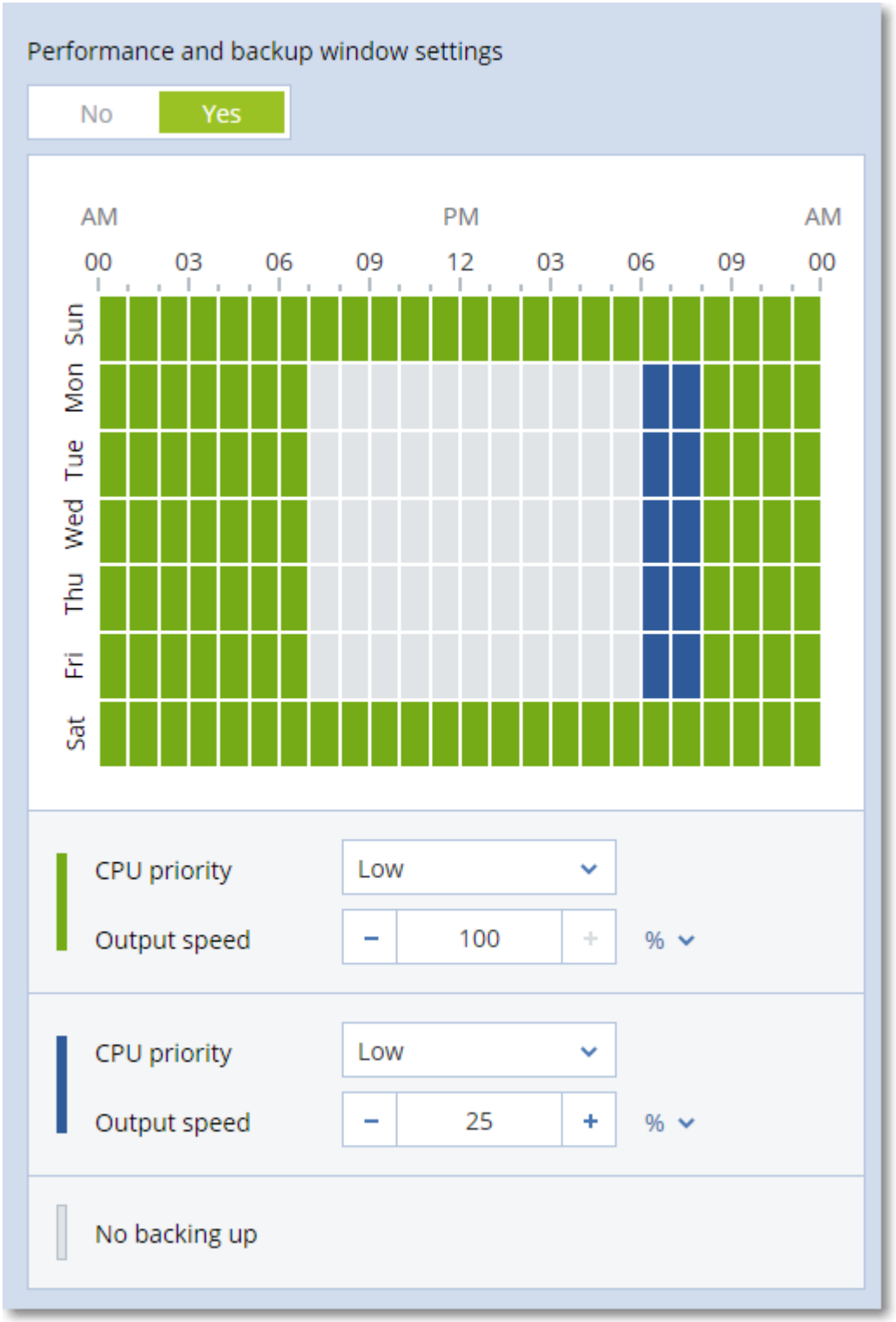
Remarque
Vous pouvez configurer les performances et la fenêtre de sauvegarde pour chaque emplacement de réplication individuellement. Pour accéder aux paramètres de l'emplacement de réplication, cliquez dans le plan de protection sur l'icône en forme d'engrenage située à côté du nom de l'emplacement, puis sur **Performances et fenêtre de sauvegarde**.

Créneau de sauvegarde

Chaque rectangle représente une heure au cours d'un jour de semaine. Cliquez sur un rectangle pour parcourir les états suivants :

- **Vert :** la sauvegarde est autorisée avec les paramètres spécifiés dans la section verte ci-dessous.
- **Bleu :** la sauvegarde est autorisée avec les paramètres spécifiés dans la section bleue ci-dessous. Cet état est indisponible si le format de sauvegarde est défini sur **Version 11**.
- **Gris :** la sauvegarde est bloquée.

Vous pouvez cliquer et faire glisser pour changer simultanément l'état de plusieurs rectangles.



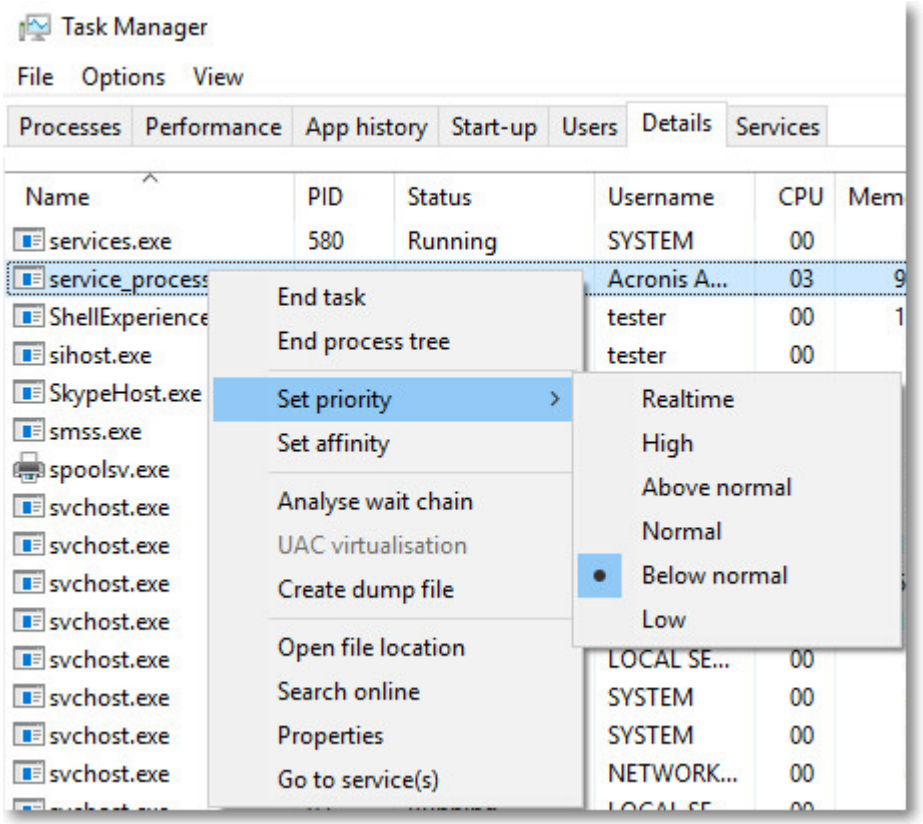
Priorité de CPU

Ce paramètre définit la priorité du processus de sauvegarde dans le système d'exploitation.

Les paramètres disponibles sont les suivants : **Basse**, **Normale**, **Élevé**.

Le degré de priorité des processus exécutés dans un système détermine le niveau d'utilisation du processeur et la quantité de ressources système qui leur sont allouées. Réduire la priorité de sauvegarde libérera davantage de ressources pour les autres applications. Augmenter la priorité de sauvegarde pourrait accélérer le processus de sauvegarde en imposant au système d'exploitation d'allouer plus de ressources, par exemple de processeur, à l'application de sauvegarde. Cependant, l'effet correspondant dépendra de l'utilisation globale du processeur ainsi que d'autres facteurs comme la vitesse d'E/S du disque ou le trafic réseau.

Cette option définit la priorité du processus de sauvegarde (**service_process.exe)** sous Windows et l'agréabilité du processus de sauvegarde (**service_process)** sous Linux et macOS.



Le tableau ci-dessous répertorie le mappage de ce paramètre sous Windows, Linux et macOS.

Priorité Cyber Protection	Priorité Windows	Caractère agréable Linux et macOS
Faible	Inférieure à la normale	10
Normal	Normal	0
Élevée	Élevée	-10

Vitesse de sortie au cours de la sauvegarde

Ce paramètre vous permet de limiter la vitesse d'écriture du disque dur (lors d'une sauvegarde dans un dossier local) ou la vitesse de transfert des données de la sauvegarde via le réseau (lors d'une sauvegarde sur un espace de stockage sur le Cloud ou un partage réseau).

Lorsque cette option est activée, vous pouvez spécifier la vitesse de sortie maximum autorisée :

- En tant que pourcentage de l'estimation de la vitesse d'écriture du disque dur de destination (lors d'une sauvegarde dans un dossier local) ou de l'estimation de la vitesse maximale de la connexion réseau (lors d'une sauvegarde sur un espace de stockage sur le Cloud ou un partage réseau).

  Ce paramètre fonctionne uniquement si l'agent est en cours d'exécution sous Windows.
- En ko/seconde (pour toutes les destinations).

Envoi de données physiques

Cette option est disponible si la destination de la sauvegarde ou de la réplication est le stockage dans le cloud et que le format de sauvegarde est défini sur **Version 12**.

Cette option est effective pour les sauvegardes de lecteur et pour les sauvegardes de fichier créées par l'agent pour Windows, l'agent pour Linux, l'agent pour Mac, l'agent pour VMware, l'agent pour Hyper-V et l'agent pour Virtuozzo.

Utilisez cette option pour envoyer la première sauvegarde complète créée par le plan de protection vers le stockage dans le Cloud ou sur un disque dur à l'aide du service d'envoi de données physiques. Les sauvegardes incrémentielles suivantes seront effectuées via le réseau.

Pour les sauvegardes locales qui sont répliquées vers le Cloud, les sauvegardes incrémentielles se poursuivent et sont enregistrées en local jusqu'à ce que la sauvegarde initiale soit chargée sur le stockage dans le Cloud. Ensuite, toutes les modifications incrémentielles sont répliquées vers le Cloud et la réplication se poursuit conformément à la planification.

Le préréglage est le suivant : **Désactivé.**

À propos du service d’envoi de données physiques

L'interface Web du service d’envoi de données physiques est disponible uniquement pour les administrateurs.

Pour des instructions détaillées concernant l'utilisation du service d’envoi de données physiques et l'outil de création de commandes, consultez le Guide de l'administrateur sur le service d’envoi de données physiques. Pour accéder à ce document dans l'interface Web du service d’envoi de données physiques, cliquez sur l'icône en forme de point d'interrogation.

Présentation du processus d’envoi de données physiques

1. [Pour envoyer des sauvegardes dont l'emplacement de sauvegarde principal est le stockage dans le Cloud]
   a. Créer un nouveau plan de protection avec sauvegarde sur le Cloud.
   b. Sur la ligne **options de sauvegarde**, cliquez sur **Modifier**.
   c. Dans la liste des options disponibles, cliquez sur **Envoi de données physiques**.

   Vous pouvez sauvegarder directement vers un lecteur amovible ou sauvegarder vers un dossier local ou réseau, puis copier/déplacer la (les) sauvegarde(s) vers le lecteur.
2. [Pour envoyer des sauvegardes locales qui sont répliquées vers le Cloud]

   Remarque
   Cette option est prise en charge avec l'agent de protection à partir de la version C21.06.

   a. Créer un nouveau plan de protection avec sauvegarde dans un stockage local ou réseau.
   b. Cliquez sur **Ajouter un emplacement** et sélectionnez **Stockage dans le Cloud**.
   c. Sur la ligne d'emplacement **Stockage dans le Cloud**, cliquez sur la roue d'engrenage et sélectionnez **Envoi de données physiques**.
3. Sous **Utiliser l’envoi de données physiques**, cliquez sur **Oui** puis sur **Terminé**.
   L'option Chiffrement est automatiquement activée dans le plan de protection, car toutes les sauvegardes qui sont envoyées doivent être chiffrées.
4. Sur la ligne **Chiffrement**, cliquez sur **Spécifier un mot de passe** et saisissez un mot de passe pour le chiffrement.
5. Sur la ligne **Envoi de données physiques**, sélectionnez le lecteur amovible sur lequel la sauvegarde initiale sera enregistrées.
6. Cliquez sur **Créer** pour enregistrer le plan de protection.
7. Une fois la première sauvegarde effectuée, utilisez l'interface Web du service d’envoi de données physiques pour télécharger l'outil de création de commandes et créez la commande.
   Pour accéder à cette interface Web, connectez-vous au portail de gestion, cliquez sur **Vue d'ensemble** > **Utilisation**, puis cliquez sur **Gérer le service** ou sur **Envoi de données physiques**.

   Important
   Une fois la sauvegarde complète initiale effectuée, les sauvegardes suivantes doivent être effectuées selon le même plan de protection. Un autre plan de protection, y compris avec des paramètres et une machine identiques, nécessitera un autre cycle d'envoi de données physiques.
8. Emballez les lecteurs et envoyez-les au centre de données.

Important
Assurez-vous de suivre les instructions d'emballage fournies dans le Guide de l'administrateur sur le service d'envoi de données physiques.

9. Suivez le statut de la commande en utilisant l'interface Web du service d'envoi de données physiques. Veuillez noter que les sauvegardes suivantes échoueront jusqu'à ce que la sauvegarde initiale soit téléchargée sur le stockage sur le Cloud.

Commandes Pré/Post

L'option vous permet de définir les commandes à exécuter automatiquement avant et après la procédure de sauvegarde.

Le modèle suivant illustre quand les commandes pre/post sont exécutées.

Commandes avant la sauvegarde	Sauvegarde	Commande après la sauvegarde

Exemples d'utilisation des commandes pre/post :

- Supprimer certains fichiers temporaires du disque avant de démarrer la sauvegarde.
- Configurer un produit antivirus tiers pour qu'il démarre chaque fois avant le début de la sauvegarde.
- Copier sélectivement des sauvegardes vers un autre emplacement. Cette option peut être utile car la réplication configurée dans un plan de protection copie *chaque* sauvegarde vers les emplacements suivants.

L'agent effectue la réplication *après* l'exécution de la commande post-sauvegarde.

Le programme ne prend pas en charge de commandes interactives, c'est-à-dire des commandes qui impliquent une saisie de l'utilisateur (par exemple, « pause »).

Commandes avant la sauvegarde

Pour spécifier une commande / un fichier de traitement par lots à exécuter avant le démarrage du processus de sauvegarde

1. Activez le commutateur **Exécuter une commande avant la sauvegarde**.
2. Dans le champ **Commande...**, saisissez une commande ou naviguez jusqu'à un fichier de traitement par lots. Le programme ne prend pas en charge de commandes interactives, c'est à dire des commandes qui impliquent une saisie de l'utilisateur (par exemple, « pause »).
3. Dans le champ **Répertoire de travail**, indiquez un chemin vers un répertoire où la commande/le fichier de traitement par lots sera exécuté.
4. Dans le champ **Arguments**, indiquez les arguments d'exécution de commande si nécessaire.
5. En fonction du résultat que vous voulez obtenir, sélectionnez les options appropriées comme

décrit dans le tableau ci-dessous.

6. Cliquez sur **Valider**.

Case à cocher	**Sélection**			
Faire échouer la sauvegarde si l'exécution de la commande échoue*	Sélectionné	Effacé	Sélectionné	Effacé
Ne pas sauvegarder tant que l'exécution de la commande n'est pas achevée	Sélectionné	Sélectionné	Effacé	Effacé
Résultat				
	Préréglage Effectuer la sauvegarde uniquement si la commande a été exécutée avec succès. Faire échouer la sauvegarde si l'exécution de la commande échoue.	Effectuer la sauvegarde après l'exécution de la commande a été exécutée, indépendamment de l'échec ou du succès de l'exécution.	Sans Objet	Effectuer la sauvegarde en même temps que l'exécution de la commande et quel que soit le résultat de l'exécution de la commande.

* Une commande est considérée comme ayant échoué si son code de sortie n'est pas égal à zéro.

Remarque
Si un script échoue en raison d'un conflit lié à une version de bibliothèque obligatoire dans Linux, excluez les variables d'environnement `LD_LIBRARY_PATH` et `LD_PRELOAD`, en ajoutant les lignes suivantes à votre script :

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

Commande après la sauvegarde

Pour spécifier une commande / un fichier exécutable à exécuter une fois la sauvegarde terminée

1. Activez le commutateur **Exécuter une commande après la sauvegarde**.
2. Dans le champ **Commande...**, saisissez une commande ou naviguez jusqu'à un fichier de traitement par lots.
3. Dans le champ **Répertoire de travail**, indiquez un chemin vers un répertoire où la commande/le fichier de traitement par lots sera exécuté.
4. Dans le champ **Arguments**, spécifiez les arguments d'exécution de commande si nécessaire.
5. Sélectionnez la case à cocher **Faire échouer la sauvegarde si l'exécution de la commande échoue** si la réussite de l'exécution de la commande est cruciale pour vous. La commande est considérée comme ayant échoué si son code de sortie n'est pas égal à zéro. Si l'exécution de la commande échoue, l'état de la sauvegarde sera défini sur **Erreur**.

   Lorsque la case n'est pas cochée, le résultat d'exécution de commande n'a pas d'incidence sur l'échec ou la réussite de la sauvegarde. Vous pouvez retrouver le résultat de l'exécution de la commande en explorant l'onglet **Activités**.
6. Cliquez sur **Valider**.

Commandes de capture de données Pré/Post

L'option vous permet de définir les commandes à exécuter automatiquement avant et après la capture des données (c'est à dire, la prise de l'instantané des données). La capture des données est exécutée au début de la procédure de sauvegarde.

Le modèle suivant illustre le moment où les commandes avant/après capture de données sont exécutées.

	<---------- **Sauvegarde** ---------->				
Commandes avant la sauvegarde	Commande avant la capture de données	Capture des données	Commande après la capture de données	Écrire des données dans le jeu de sauvegarde	Commande après la sauvegarde

Interaction avec d'autres options de sauvegarde

L'exécution de commandes avant/après capture de données peut être modifiée par d'autres options de sauvegarde.

Si l'option **Instantané Multi-volume** est activée, les commandes avant/après capture de données ne seront exécutées qu'une seule fois, car les instantanés pour tous les volumes sont créés simultanément. Si l'option **Instantané Multi-volume** est désactivée, les commandes avant/après capture de données seront exécutées pour chaque volume sauvegardé, car les instantanés sont créés de manière séquentielle, un instantané après l'autre.

Si l'option **Service de cliché instantané des volumes (VSS)** est activée, les commandes avant/après capture des données et les actions Microsoft VSS seront exécutées comme suit :

Commandes avant capture des données > Suspension de VSS > Capture des données > Reprise de VSS > Commandes après capture des données

À l'aide des commandes de capture des données avant/après, vous pouvez suspendre et redémarre une base de données ou une application qui n'est pas compatible avec VSS. La capture des données prenant quelques secondes, le temps durant lequel la base de données ou l'application seront ralenties sera minimal.

Commande avant la capture de données

Pour spécifier une commande / un fichier de traitement par lots à exécuter avant la capture des données

1. Activez le commutateur **Exécuter une commande avant la capture des données**.
2. Dans le champ **Commande...**, saisissez une commande ou naviguez jusqu'à un fichier de traitement par lots. Le programme ne prend pas en charge de commandes interactives, c'est à dire des commandes qui impliquent une saisie de l'utilisateur (par exemple, « pause »).
3. Dans le champ **Répertoire de travail**, indiquez un chemin vers un répertoire où la commande/le fichier de traitement par lots sera exécuté.
4. Dans le champ **Arguments**, indiquez les arguments d'exécution de commande si nécessaire.
5. En fonction du résultat que vous voulez obtenir, sélectionnez les options appropriées comme décrit dans le tableau ci-dessous.
6. Cliquez sur **Valider**.

Case à cocher	**Sélection**			
Faire échouer la sauvegarde si l'exécution de la commande échoue*	Sélectionné	Effacé	Sélectionné	Effacé
Ne pas exécuter la saisie des données tant que l'exécution de la commande n'est pas achevée	Sélectionné	Sélectionné	Effacé	Effacé
Résultat				
	Préréglage	Effectuer la sauvegarde après	Sans Objet	Effectuer la capture des

	Effectuer la capture des données uniquement si la commande a été exécutée avec succès. Faire échouer la sauvegarde si l'exécution de la commande échoue.	l'exécution de la commande, indépendamment de l'échec ou du succès de l'exécution.		données en même temps que la commande et quel que soit le résultat de l'exécution de la commande.

* Une commande est considérée comme ayant échoué si son code de sortie n'est pas égal à zéro.

Remarque
Si un script échoue en raison d'un conflit lié à une version de bibliothèque obligatoire dans Linux, excluez les variables d'environnement `LD_LIBRARY_PATH` et `LD_PRELOAD`, en ajoutant les lignes suivantes à votre script :

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

Commande après la capture de données

Pour spécifier une commande / un fichier de traitement par lots à exécuter après la capture des données

1. Activez le commutateur **Exécuter une commande après la capture des données**.
2. Dans le champ **Commande...**, saisissez une commande ou naviguez jusqu'à un fichier de traitement par lots. Le programme ne prend pas en charge de commandes interactives, c'est à dire des commandes qui impliquent une saisie de l'utilisateur (par exemple, « pause »).
3. Dans le champ **Répertoire de travail**, indiquez un chemin vers un répertoire où la commande/le fichier de traitement par lots sera exécuté.
4. Dans le champ **Arguments**, indiquez les arguments d'exécution de commande si nécessaire.
5. En fonction du résultat que vous voulez obtenir, sélectionnez les options appropriées comme décrit dans le tableau ci-dessous.
6. Cliquez sur **Valider**.

Case à cocher	Sélection			
Faire échouer la sauvegarde si l'exécution de la commande échoue*	Sélectionné	Effacé	Sélectionné	Effacé
Ne pas	Sélectionné	Sélectionné	Effacé	Effacé

sauvegarder tant que l'exécution de la commande n'est pas achevée				
Résultat				
	Préréglage Continuer la sauvegarde uniquement si la commande a été exécutée avec succès.	Effectuer la sauvegarde après l'exécution de la commande a été exécutée, indépendamment de l'échec ou du succès de l'exécution.	Sans Objet	Continuer la sauvegarde en même temps que l'exécution de la commande et quel que soit le résultat de l'exécution de la commande.

* Une commande est considérée comme ayant échoué si son code de sortie n'est pas égal à zéro.

Planification

Cette option définit si les sauvegardes commencent exactement telles qu'elles sont planifiées ou en différé, et indique le nombre de machines virtuelles sauvegardées simultanément.

Pour plus d'informations sur la configuration du calendrier de sauvegarde, voir "Exécution d'une sauvegarde à partir d'une planification" (p. 439).

Le préréglage est le suivant : **Répartir les heures de démarrage de sauvegarde dans une fenêtre de temps**. **Retard maximum** : **30 minutes**.

Vous pouvez sélectionner l'une des options suivantes :

- **Démarrer toutes les sauvegardes exactement comme planifié**
  Les sauvegardes des machines virtuelles commenceront exactement comme planifié. Les machines seront sauvegardées une par une.
- **Répartir les heures de démarrage dans une fenêtre de temps**
  La sauvegarde des machines physiques commencera en différé selon l'heure planifiée. La valeur de délai pour chaque machine est sélectionnée de façon aléatoire et comprise entre zéro et la valeur maximale que vous spécifiez. Il se peut que vous souhaitiez utiliser ce paramètre lors de sauvegarde de machines multiples sur un emplacement réseau, pour éviter une charge excessive du réseau. La valeur du délai pour chaque machine est déterminée quand le plan de protection est appliqué à la machine, et reste la même tant que vous n'avez pas modifié le plan de protection et changé la valeur de délai maximal.
  Les machines seront sauvegardées une par une.
- **Limiter le nombre de sauvegardes simultanées par**
  Utilisez cette option pour gérer la sauvegarde parallèle de machines virtuelles sauvegardées au niveau de l'hyperviseur (sauvegarde sans agent).

Les plans de protection dans lesquels cette option est sélectionnée peuvent s'exécuter simultanément avec d'autres plans de protection gérés par le même agent. Lorsque vous sélectionnez cette option, vous devez indiquer le nombre de sauvegardes parallèles par plan. Le nombre total d'ordinateurs sauvegardés simultanément par tous les plans est limité à 10 par agent. Pour plus d'informations sur la modification de la limite par défaut, voir "Limite le nombre total de machines virtuelles sauvegardées simultanément." (p. 740).

Les plans de protection dans lesquels cette option n'est pas sélectionnée exécutent les opérations de sauvegarde de manière séquentielle, une machine virtuelle après l'autre.

Sauvegarde secteur par secteur

Cette option est effective uniquement pour une sauvegarde de niveau disque.

Cette option définit si une copie exacte d'un disque ou d'un volume sur un niveau physique doit être créée.

Le préréglage est le suivant : **Désactivé**.

Si cette option est activée, tous les secteurs du disque ou du volume seront sauvegardés, y compris l'espace non alloué et les secteurs qui ne contiennent aucunes données. La sauvegarde obtenue sera de la même taille que le disque en cours de sauvegarde (si l'option Niveau de compression est définie sur **Aucune**). Le logiciel passe automatiquement en mode secteur par secteur lorsque la sauvegarde présente des systèmes de fichiers non reconnus ou non pris en charge.

Remarque
Il sera impossible d'exécuter une restauration des données d'application à partir des sauvegardes créées en mode secteur par secteur.

Fractionnement

Cette option vous permet de sélectionner la méthode de fractionnement des sauvegardes volumineuses en fichiers plus petits

Remarque
Le fractionnement n'est pas disponible dans les plans de protection qui utilisent le stockage dans le cloud en tant qu'emplacement de sauvegarde.

Le préréglage est le suivant :

- Si l'emplacement de sauvegarde est un dossier local ou réseau (SMB), et que le format de sauvegarde est la Version 12 : **Taille fixe – 200 Go**

  Avec ce paramètre, le logiciel de sauvegarde peut fonctionner avec de grosses quantités de données sur le système de fichiers NTFS, sans que la fragmentation de fichiers ne cause d'effets indésirables.
- Sinon : **Automatique**

Les paramètres suivants sont disponibles :

- **Automatique**
  Une sauvegarde sera fractionnée si elle excède la taille de fichier maximum prise en charge par le système de fichiers.
- **Taille fixe**
  Entrez la taille de fichier souhaitée ou sélectionnez-la à partir de la liste déroulante.

Traitement de l'échec de tâche

Cette option détermine le comportement du programme lorsqu'un plan de protection programmé échoue ou que votre ordinateur redémarre pendant l'exécution d'une sauvegarde. Cette option ne fonctionne pas lorsqu'un plan de protection est démarré manuellement.

Si cette option est activée, le programme essaiera de nouveau d'exécuter le plan de protection. Vous pouvez spécifier le nombre de tentatives et l'intervalle de temps entre ces tentatives. Le programme s'arrête dès qu'une tentative aboutit ou que le nombre spécifié de tentatives est atteint, selon le cas de figure qui se produit en premier.

Si cette option est activée et que votre ordinateur redémarre pendant l'exécution d'une sauvegarde, l'opération de sauvegarde n'échoue pas. Quelques minutes après le redémarrage, l'opération de sauvegarde se poursuit automatiquement et crée le fichier de sauvegarde avec les données manquantes. Dans ce cas d'utilisation, l'option **Intervalle entre les tentatives** n'est pas pertinente.

Le préréglage est le suivant : **Activé**.

Remarque
Cette option n'est pas effective pour les sauvegardes riches en données d'investigation numérique.

Conditions de démarrage de tâche

Cette option est effective à la fois dans les systèmes d'exploitation Windows et Linux.

Cette option détermine le comportement du programme lorsqu' une tâche est sur le point de démarrer (l'heure planifiée arrive ou l'événement spécifié dans la planification se produit), mais la condition (ou l'une des nombreuses conditions) n'est pas remplie. Pour plus d'informations sur les conditions, consultez la section "Conditions de démarrage" (p. 446).

Le préréglage est le suivant : **Attendre que les conditions de la planification soient remplies.**

Attendre que les conditions de la planification soient remplies

Avec ce paramètre, le planificateur commence à surveiller les conditions et lance la tâche dès que les conditions sont remplies. Si les conditions ne sont jamais remplies, la tâche ne démarrera jamais.

Pour gérer la situation lorsque les conditions ne sont pas remplies pendant trop longtemps et qu'il devient trop risqué de retarder la tâche, vous pouvez définir l'intervalle de temps à l'issue duquel la tâche sera exécutée, quelle que soit la condition. Cochez la case **Exécuter la tâche de toutes façons après**, puis spécifiez l'intervalle de temps. La tâche démarrera dès que les conditions seront

remplies OU que le délai maximum sera écoulé, en fonction du cas de figure qui se produira en premier.

Sauter l'exécution de la tâche

Il peut être impossible de retarder une tâche, par exemple, lorsque vous devez impérativement exécuter une tâche au moment spécifié. Il est alors pertinent de passer outre la tâche plutôt que d'attendre que les conditions soient remplies, particulièrement si les tâches sont effectuées relativement fréquemment.

Service de cliché instantané des volumes

Cette option ne s'applique qu'aux systèmes d'exploitation Windows.

Elle définit si une sauvegarde peut réussir si un ou plusieurs enregistreurs VSS (service de cliché instantané des volumes) échouent, et indique également si le fournisseur doit informer les applications compatibles VSS que la sauvegarde va démarrer.

L'utilisation du service VSS (service de cliché instantané des volumes) garantit la cohérence de toutes les données utilisées par les applications, en particulier, l'achèvement de toutes les transactions de la base de données au moment de la prise de l'instantané des données par le logiciel de sauvegarde. La cohérence des données garantit, quant à elle, que l'application sera restaurée dans l'état approprié et deviendra opérationnelle immédiatement après la restauration.

L'instantané est utilisé uniquement pendant l'opération de sauvegarde et il est supprimé automatiquement lorsque cette opération est terminée. Aucun fichier temporaire n'est conservé.

Vous pouvez également utiliser les commandes avant et après la capture de données afin de vous assurer que les données sont sauvegardées de façon cohérente. Par exemple, spécifiez des commandes avant la capture de données, qui suspendront la base de données et videront tous les caches pour garantir que toutes les transactions sont terminées, et des commandes après la capture de-données, qui remettront la base de données en service une fois l'instantané pris.

Remarque
Les fichiers et les dossiers qui sont indiqués dans la clé de la base de registre **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** ne sont pas sauvegardés. En particulier, les fichiers de données Outlook hors connexion (.ost) ne sont pas sauvegardés, car ils sont indiqués dans la valeur **OutlookOST** de cette clé.

Ignorer les enregistreurs VSS échoués

Vous pouvez sélectionner l'une des options suivantes :

- **Ignorer les enregistreurs VSS échoués**
  Grâce à cette option, les sauvegardes sont réussies, même en cas d'échec d'un ou de plusieurs enregistreurs VSS.

Important
Les sauvegardes reconnaissant les applications échouent toujours si l'enregistreur propre à l'application échoue. Par exemple, si vous effectuez la sauvegarde reconnaissant les applications de données SQL Server et que l'enregistreur **SqlServerWriter** échoue, l'opération de sauvegarde échoue également.

Lorsque cette option est activée, trois tentatives consécutives de création d'instantané VSS sont réalisées.

Pour la première tentative, tous les enregistreurs VSS sont nécessaires. En cas d'échec, cette tentative est relancée. Si la deuxième tentative échoue également, les enregistreurs VSS qui ont échoué sont exclus de l'opération de sauvegarde et une troisième tentative est lancée. Si cette troisième tentative réussit, la sauvegarde s'effectue, avec un avertissement concernant les enregistreurs VSS qui ont échoué. En cas d'échec de la troisième tentative, la sauvegarde échoue.

- **Exiger la réussite du traitement de tous les enregistreurs VSS**
  En cas d'échec de l'un des enregistreurs VSS, l'opération de sauvegarde échoue également.

Sélectionner le fournisseur d'instantanés

Vous pouvez sélectionner l'une des options suivantes :

- **Sélection automatique du fournisseur d'instantanés**
  Sélection automatique parmi les fournisseurs d'instantanés matériels, logiciels et Microsoft Software Shadow Copy.
- **Utilisation du fournisseur de cliché instantané des logiciels Microsoft**
  Nous vous recommandons de choisir cette option lors de la sauvegarde de serveurs d'applications (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint ou Active Directory).

Activer la sauvegarde complète VSS

Si cette option est activée, les journaux de Microsoft Exchange Server et des autres applications compatibles VSS (sauf Microsoft SQL Server) seront tronqués après chaque sauvegarde de disque complète, incrémentielle ou différentielle réussie.

Le préréglage est le suivant : **Désactivé**.

Laissez cette option désactivée dans les cas suivants :

- Si vous utilisez l'agent pour Exchange ou un logiciel tiers pour sauvegarder les données Exchange Server. La raison est que la troncature du journal interférera avec les sauvegardes des journaux des transactions consécutives.
- Si vous utilisez un logiciel tiers pour sauvegarder les données SQL Server. La raison pour cela est que le logiciel tiers prendra la sauvegarde de niveau disque résultante comme sa « propre » sauvegarde complète. En conséquence, la sauvegarde différentielle suivante des données SQL

Server échouera. Les sauvegardes continueront à échouer jusqu'à ce que le logiciel tiers crée sa prochaine « propre » sauvegarde complète.

- Si d'autres applications compatibles VSS sont en cours d'exécution sur la machine et que vous devez conserver leurs journaux pour une raison quelconque.

Important
L'activation de cette option n'entraîne pas la troncature des journaux Microsoft SQL Server. Pour tronquer le journal SQL Server après une sauvegarde, activez l'option de sauvegarde Troncation de journal.

Service de cliché instantané des volumes (VSS) pour les machines virtuelles

Cette option définit si les instantanés suspendus des machines virtuelles sont pris.

Le préréglage est le suivant : **Activé**.

Lorsque cette option est désactivée, un cliché instantané non suspendu est pris. La machine virtuelle sera sauvegardée dans un état cohérent en cas de panne.

Lorsque cette option est activée, les transactions de toutes les applications VSS en cours d'exécution sur la machine virtuelle sont terminées, puis un instantané est pris.

Si un instantané suspendu ne peut être pris après le nombre de tentatives spécifié dans l'option « Gestion des erreurs » et que la sauvegarde d'application est activée, la sauvegarde échoue.

Si un instantané suspendu ne peut pas être pris après le nombre de tentatives spécifié dans l'option « Gestion des erreurs » et que la sauvegarde de l'application est désactivée, une sauvegarde cohérente en cas de plantage est créée. Pour que la sauvegarde échoue au lieu de créer une sauvegarde cohérente de plantage, cochez la case **Échec de la sauvegarde si la prise d'un instantané suspendu n'est pas possible**.

Le tableau suivant résume les paramètres disponibles et leurs résultats.

Paramètres	L'instantané suspendu a été pris avec succès		L'instantané suspendu n'a pas été pris	
	Sauvegarde de l'application activée	Sauvegarde de l'application désactivée	Sauvegarde de l'application activée	Sauvegarde de l'application désactivée
Activation du **service de cliché instantané des volumes (VSS) pour les machines virtuelles**	L'instantané suspendu est pris. La sauvegarde cohérente de l'application est créée.	L'instantané suspendu est pris. La sauvegarde cohérente de l'application est créée.	La sauvegarde échoue.	Un instantané non suspendu est pris. Une sauvegarde cohérente de plantage est créée.

Paramètres	L'instantané suspendu a été pris avec succès		L'instantané suspendu n'a pas été pris	
	Sauvegarde de l'application activée	**Sauvegarde de l'application désactivée**	**Sauvegarde de l'application activée**	**Sauvegarde de l'application désactivée**
Échec de la sauvegarde si la prise d'un instantané suspendu n'est pas possible non sélectionné				
Activation du **service de cliché instantané des volumes (VSS) pour les machines virtuelles** **Échec de la sauvegarde si la prise d'un instantané suspendu n'est pas possible** sélectionné	L'instantané suspendu est pris. La sauvegarde cohérente de l'application est créée.	L'instantané suspendu est pris. La sauvegarde cohérente de l'application est créée.	La sauvegarde échoue.	La sauvegarde échoue.
Service de cliché instantané des volumes (VSS) désactivé **pour les machines virtuelles**	Un instantané non suspendu est pris. Une sauvegarde cohérente de plantage est créée.	Un instantané non suspendu est pris. Une sauvegarde cohérente de plantage est créée.	Un instantané non suspendu est pris. Une sauvegarde cohérente de plantage est créée.	Un instantané non suspendu est pris. Une sauvegarde cohérente de plantage est créée.

L'activation de **service de cliché instantané des volumes (VSS) pour les machines virtuelles** déclenche également les scripts de pré-gel et de post-dégel que vous pouvez avoir sur la machine virtuelle sauvegardée. Pour plus d'informations sur ces scripts, consultez "Exécution automatique de scripts pre-freeze et post-thaw" (p. 733).

Pour prendre un instantané en suspend, le logiciel de sauvegarde exécute un VSS sur une machine virtuelle en utilisant VMware Tools, Hyper-V Integration Services, Virtuozzo Guest Tools, Red Hat Virtualization Guest Tools ou QEMU Guest Tools, respectivement.

Remarque
Pour les machines virtuelles Red Hat Virtualization (oVirt), nous vous recommandons d'installer QEMU Guest Tools plutôt que Red Hat Virtualization Guest Tools. Certaines versions de Red Hat Virtualization Guest Tools ne prennent pas en charge les instantanés cohérents avec les applications.

Cette option n'affecte pas les machines virtuelles Scale Computing HC3. Pour celles-ci, la suspension dépend de l'installation ou non des outils Scale sur la machine virtuelle.

Sauvegarde hebdomadaire

Cette option détermine quelles sauvegardes sont considérées comme « hebdomadaires » dans les règles de rétention et les plans de sauvegarde. Une sauvegarde « hebdomadaire » correspond à la première sauvegarde créée dès qu'une semaine commence.

Le préréglage est le suivant : **Lundi**.

Journal des événements Windows

Cette option est effective uniquement dans les systèmes d'exploitation Windows.

Cette option définit si les agents doivent consigner des événements des opérations de sauvegarde dans journal des événements d'applications Windows (pour voir ce journal, exécutez eventvwr.exe ou sélectionnez **Panneau de configuration** > **Outils administratifs** > **Affichage des événements**). Vous pouvez filtrer les événements à consigner.

Le préréglage est le suivant : **Désactivé**.

Restauration

Restauration de l'aide-mémoire

Le tableau suivant résume les méthodes de restauration disponibles. Utilisez le tableau afin de choisir la méthode de restauration qui correspond le mieux à vos besoins.

Remarque
Vous ne pouvez pas restaurer les sauvegardes dans la console Cyber Protect pour les tenants en mode Conformité. Pour plus d'informations sur la restauration de ces sauvegardes, voir "Restauration de sauvegardes pour les tenants en mode Conformité" (p. 1149).

Quoi restaurer	Méthode de restauration
Machine physique (Windows ou Linux)	Utilisation de la console Cyber Protect Utilisation d'un support de démarrage

Machine physique (Mac)	Utilisation d'un support de démarrage
Machine virtuelle (VMware, Hyper-V, Red Hat Virtualization (oVirt) ou Scale Computing HC3)	Utilisation de la console Cyber Protect Utilisation d'un support de démarrage
Machine virtuelle ou conteneur (Virtuozzo, Virtuozzo Hybrid Server ou Virtuozzo Hybrid Infrastructure)	Utilisation de la console Cyber Protect
Configuration ESXi	Utilisation d'un support de démarrage
Fichiers/Dossiers	Utilisation de la console Cyber Protect Téléchargement de fichiers depuis le Cloud Utilisation d'un support de démarrage Extraction de fichiers à partir de sauvegardes locales
Etat du système	Utilisation de la console Cyber Protect
Bases de données SQL	Utilisation de la console Cyber Protect
Bases de données Exchange	Utilisation de la console Cyber Protect
Boîtes aux lettres Exchange	Utilisation de la console Cyber Protect
Sites Web	Utilisation de la console Cyber Protect
Microsoft 365	
Boîtes aux lettres (agent local pour Microsoft 365)	Utilisation de la console Cyber Protect
Boîtes aux lettres (agent Cloud pour Microsoft 365)	Utilisation de la console Cyber Protect
Dossiers publics	Utilisation de la console Cyber Protect
Fichiers OneDrive	Utilisation de la console Cyber Protect
Données SharePoint Online	Utilisation de la console Cyber Protect
Google Workspace	
Boîtes aux lettres	Utilisation de la console Cyber Protect

Fichiers Google Drive	Utilisation de la console Cyber Protect
Fichiers de Drive partagés	Utilisation de la console Cyber Protect

Restauration interplate-forme

La restauration interplate-forme est disponible pour les sauvegardes d'ordinateurs complets et de disques contenant un système d'exploitation.

Une restauration interplate-forme s'effectue dans les cas suivants :

- Une sauvegarde est créée par un type d'agent, mais elle est restaurée par un type d'agent différent.
- Une sauvegarde avec agent est restaurée au niveau de l'hyperviseur (restauration sans agent), ou une sauvegarde sans agent est restaurée par un agent (restauration avec agent).
- Une sauvegarde est restaurée sur un matériel différent (y compris les appliances virtuelles).

Remarque
Certains périphériques tels que les imprimantes risquent de ne pas être restaurés correctement lorsque vous effectuez une restauration interplate-forme.

Le tableau ci-dessous présente quelques exemples de restauration interplate-forme.

Restauration interplate-forme	
Sauvegarde sans agent	Restauration avec agent
Sauvegarde basée sur un agent	Restauration sans agent
Sauvegarde par l'agent pour Windows	Restauration par l'agent pour VMware
Sauvegarde par l'agent pour VMware	Restauration par l'agent pour Hyper-V
Sauvegarde par l'agent pour Windows qui est installé sur une machine virtuelle VMware ESXi (avec agent)	Restauration par l'agent pour VMware (sans agent) sur le même hôte VMware ESXi
Sauvegarde par l'agent pour Windows	Restauration par l'agent pour Windows qui est installé sur un ordinateur avec matériel différent
Sauvegarde d'une machine physique	Restauration d'une machine virtuelle

Remarque pour les utilisateurs Mac

- Depuis la version 10.11 du système d'exploitation El Capitan, certains fichiers système, dossiers et processus sont marqués comme protégés avec l'ajout de l'attribut de fichier com.apple.rootless. Cette fonctionnalité est appelée Protection de l'intégrité du système (System Integrity Protection, SIP). Les fichiers protégés comprennent les applications préinstallées, ainsi que la plupart des dossiers des répertoires /system, /bin, /sbin et /usr.

Les fichiers et dossiers protégés ne peuvent pas être écrasés lors de la restauration du système d'exploitation. Si vous souhaitez écraser les fichiers protégés, effectuez une restauration à partir d'un support de démarrage.

- Désormais, dans macOS Sierra 10.12, les fichiers rarement utilisés peuvent être déplacés vers iCloud au moyen de la fonctionnalité de stockage dans le Cloud. De petites empreintes de ces fichiers sont conservées sur le système de fichiers. Ces empreintes sont sauvegardées à la place des fichiers d'origine.

  Lorsque vous restaurez une empreinte à l'emplacement d'origine, elle est synchronisée avec iCloud, et le fichier d'origine redevient disponible. Si vous restaurez une empreinte à un emplacement différent, celle-ci n'est pas synchronisée avec iCloud et le fichier d'origine est indisponible.

Restauration sûre

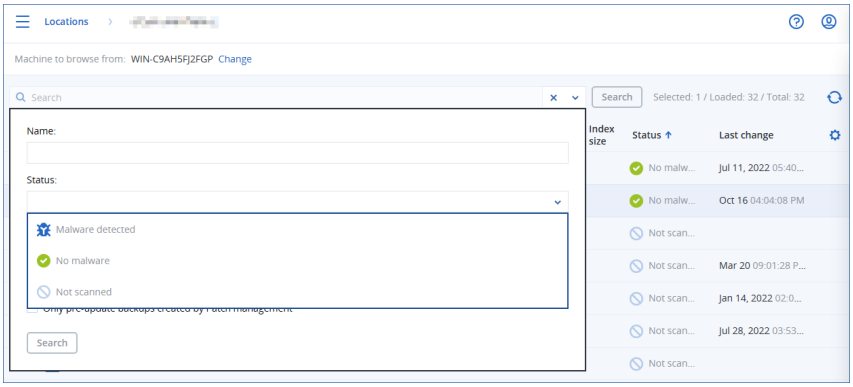
Utilisez une restauration complète avec des sauvegardes de type **Machine complète** ou **Disques/volumes** de ressources Windows afin de ne restaurer que des données exemptes de malware, même si la sauvegarde contient des fichiers infectés.

Pendant une opération de restauration sécurisée, la sauvegarde fait l'objet d'une recherche automatique de malware. L'agent de protection restaure ensuite la sauvegarde sur la ressource cible et supprime les fichiers infectés. En conséquence, la sauvegarde restaurée est exempte de malware.

Par ailleurs, l'un des états suivants est attribué à la sauvegarde :

- Malware détecté
- Aucun malware
- Non analysé

Vous pouvez utiliser l'état pour filtrer les archives de sauvegarde.



Limites

- La restauration sécurisée est prise en charge pour les machines physiques et virtuelles Windows sur lesquelles un agent de protection est installé.

- La restauration sécurisée est prise en charge pour les sauvegardes **Machine complète** ou **Disques/volumes**.
- La recherche de malware ne porte que sur les volumes NTFS. Les volumes non-NTFS sont restaurés sans analyse antimalware.
- La restauration sécurisée n'est pas prise en charge pour les sauvegardes de type protection continue des données de l'archive. Pour restaurer les données de la sauvegarde de type protection continue des données, exécutez une autre opération de restauration de **Fichiers/dossiers**. Pour plus d'instructions sur les sauvegardes de type protection continue des données, consultez "Protection continue des données (CDP)" (p. 426).

Restauration d'une machine

Restauration de machines physiques

Cette section décrit la restauration des machines physiques via l'interface Web.

Utilisez un support de démarrage plutôt que l'interface Web pour restaurer :

- Un ordinateur fonctionnant sous macOS
- Un ordinateur d'un tenant en mode Conformité
- Tout système d'exploitation de manière complète ou sur une machine hors ligne
- La structure des volumes logiques (volumes créés par Logical Volume Manager sous Linux). Le support vous permet de recréer automatiquement la structure des volumes logique.

Remarque
Vous ne pouvez pas restaurer les sauvegarde de disque d'ordinateurs Mac Intel sur des Mac utilisant des puces silicone Apple, et inversement. Vous pouvez restaurer des fichiers et des dossiers.

Restauration avec redémarrage

La restauration d'un système d'exploitation et de volumes chiffrés avec BitLocker nécessite un redémarrage. Vous pouvez choisir de redémarrer automatiquement la machine ou de lui attribuer le statut **Intervention nécessaire**. Le système d'exploitation restauré est automatiquement mis en ligne.

Important
Les volumes chiffrés et sauvegardés sont restaurés comme volumes non chiffrés.

La reprise des volumes chiffrés par BitLocker nécessite la présence sur la même machine d'un volume non chiffré disposant d'au moins 1 Go d'espace disponible. Si aucune de ces conditions n'est remplie, la reprise échoue.

La reprise d'un volume système chiffré ne requiert aucune action supplémentaire. Pour restaurer un volume non-système chiffré, vous devez d'abord le verrouiller, par exemple en ouvrant un fichier

qui y réside. Dans le cas contraire, la reprise se poursuit sans redémarrage et le volume récupéré risque de ne pas être reconnu par Windows.

Remarque
Si la reprise échoue et que votre machine redémarre avec l'erreur `Impossible d'obtenir le fichier de la partition`, essayez de désactiver le démarrage sécurisé. Pour en savoir plus sur la façon de procéder, consultez la section Désactivation du démarrage sécurisé dans la documentation Microsoft.

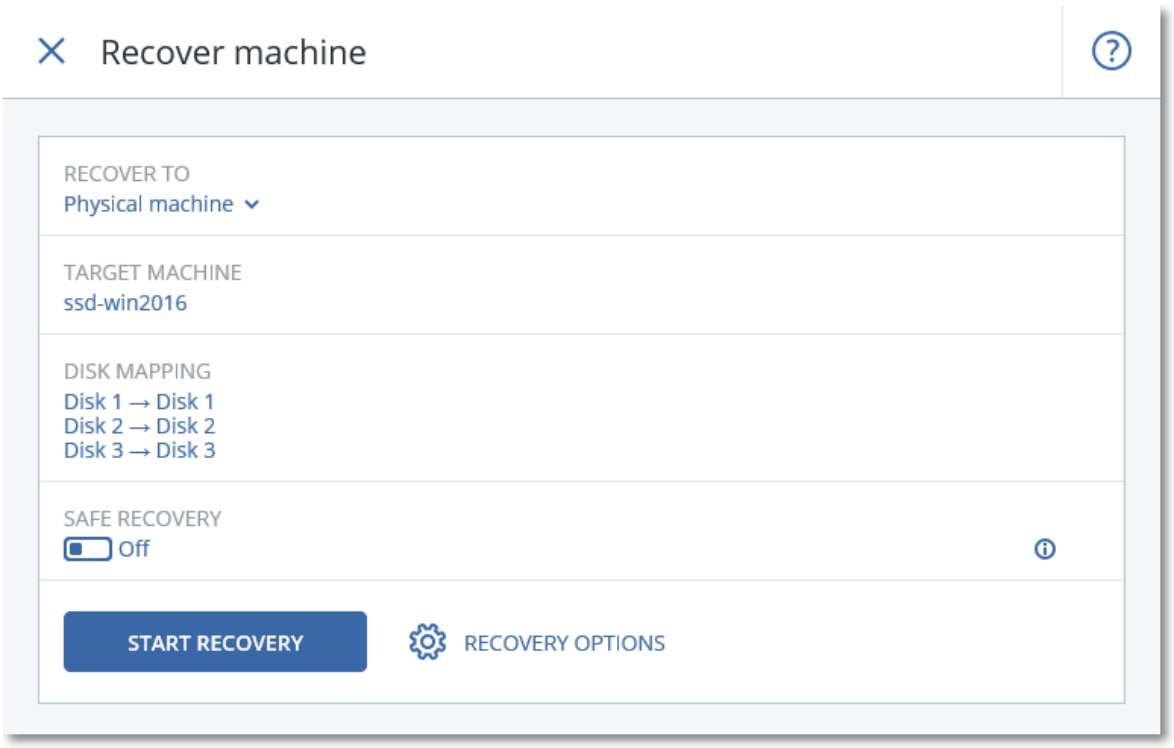
Pour restaurer une machine physique

1. Sélectionnez la machine sauvegardée.
2. Cliquez sur **Restauration**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

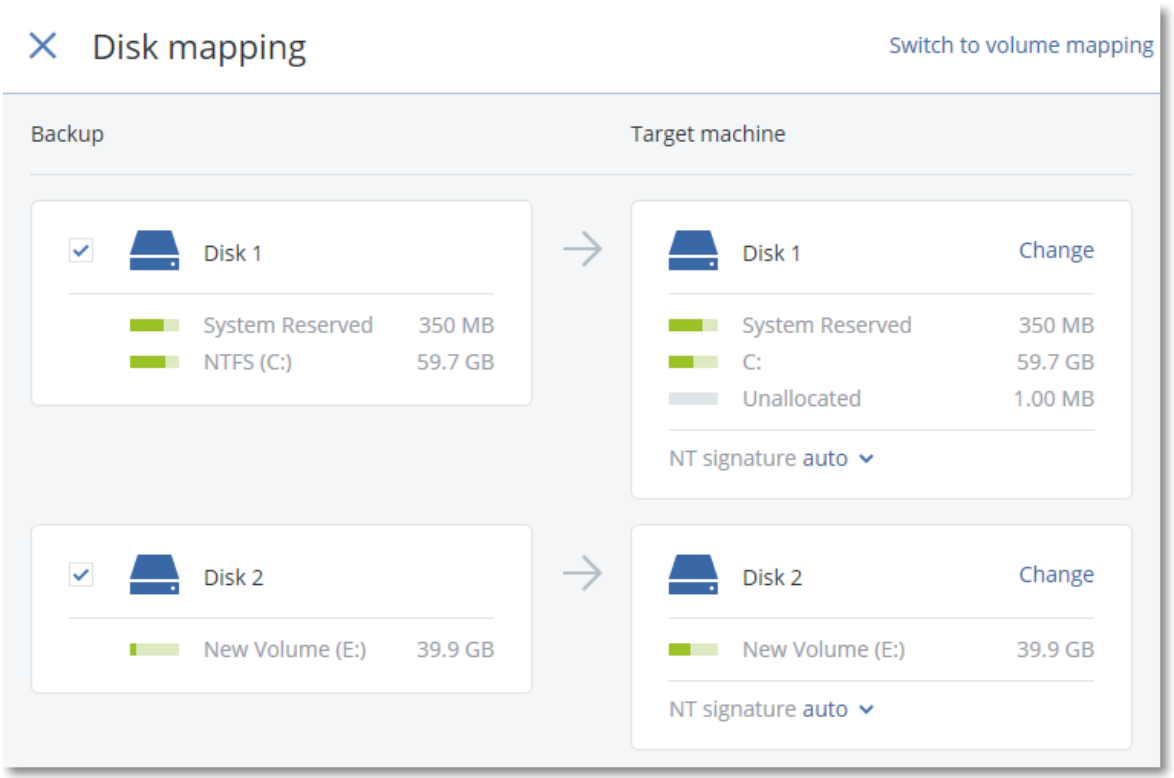
   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Effectuez l'une des actions suivantes :
   - Si la sauvegarde est située sur le Cloud ou à un emplacement de stockage partagé (c.-à-d. que d'autres agents peuvent y accéder), cliquez sur **Sélectionner une machine**, sélectionnez une machine cible qui est en ligne, puis choisissez un point de restauration.
   - Sélectionnez un point de récupération dans l'onglet Stockage de sauvegarde.
   - Restaurez la machine comme décrit dans « Restauration de disques via un support de démarrage ».
4. Cliquez sur **Restaurer** > **Toute la machine**.

   Le logiciel mappe automatiquement les disques depuis la sauvegarde vers les disques de la machine cible.

   Pour effectuer une restauration sur une autre machine physique, cliquez sur **Machine cible**, puis sélectionnez une machine cible en ligne.



5. Si vous n'êtes pas satisfait du résultat du mappage ou si le mappage du disque échoue, cliquez sur **Mappage de volume** pour re-mapper les disques manuellement.
   La section Mappage permet également de choisir les disques ou volumes à restaurer. Vous pouvez passer de la restauration de disques à la restauration de volumes, et vice-versa, à l'aide du lien **Basculer vers...** dans l'angle supérieur droit.



6. [Disponible uniquement pour les ordinateurs Windows sur lesquels un agent de protection est installé] Activez le curseur **Restauration sûre** afin de vous assurer que les données restaurées sont exemptes de malware. Pour plus d'informations sur le fonctionnement de la restauration sécurisée, voir "Restauration sûre" (p. 521).
7. Cliquez sur **Démarrer la récupération**.
8. Confirmez que vous souhaitez écraser les données du disque avec leurs versions sauvegardées. Choisissez si vous souhaitez redémarrer automatiquement la machine.

La progression de la restauration sont affichées dans l'onglet **Activités**.

Machine physique à virtuelle

Vous pouvez restaurer une machine physique vers une machine virtuelle sur l'un des hyperviseurs pris en charge. Il s'agit également d'un mécanisme de migration d'une machine physique vers une machine virtuelle. Pour en savoir plus sur les chemins de migration P2V pris en charge, consultez « Migration de machine ».

Cette section décrit la restauration d'une machine physique en tant que machine virtuelle à l'aide de l'interface Web. Cette opération peut être effectuée si au moins un agent pour l'hyperviseur concerné est installé et enregistré dans le serveur de gestion Acronis. Par exemple, une restauration vers VMware ESXi nécessite au moins un Agent pour VMware, une restauration vers Hyper-V nécessite au moins un Agent pour Hyper-V installé et enregistré dans l'environnement.

La récupération via l'interface Web n'est pas disponible pour les tenants en mode Conformité.

Remarque
Vous ne pouvez pas restaurer des machines virtuelles macOS sur des hôtes Hyper-V, car Hyper-V ne prend pas en charge macOS. Vous pouvez restaurer des machines virtuelles macOS sur un hôte VMware installé sur un matériel Mac.

Vous ne pouvez pas non plus restaurer de sauvegarde de machines physiques macOS en tant que machines virtuelles.

Restauration d'une machine physique en tant que machine virtuelle

1. Sélectionnez la machine sauvegardée.
2. Cliquez sur **Restauration**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Effectuez l'une des actions suivantes :
   - Si la sauvegarde est située sur le Cloud ou à un emplacement de stockage partagé (c.-à-d. que d'autres agents peuvent y accéder), cliquez sur **Sélectionner une machine**, sélectionnez une machine qui est en ligne, puis choisissez un point de restauration.
   - Sélectionnez un point de récupération dans l'onglet Stockage de sauvegarde.

- Restaurez la machine comme décrit dans « Restauration de disques via un support de démarrage ».

4. Cliquez sur **Restaurer** > **Toute la machine**.
5. Dans **Restaurer vers**, sélectionnez **Machine virtuelle**.
6. Cliquez sur **Machine cible**.
   a. Sélectionnez l'hyperviseur.

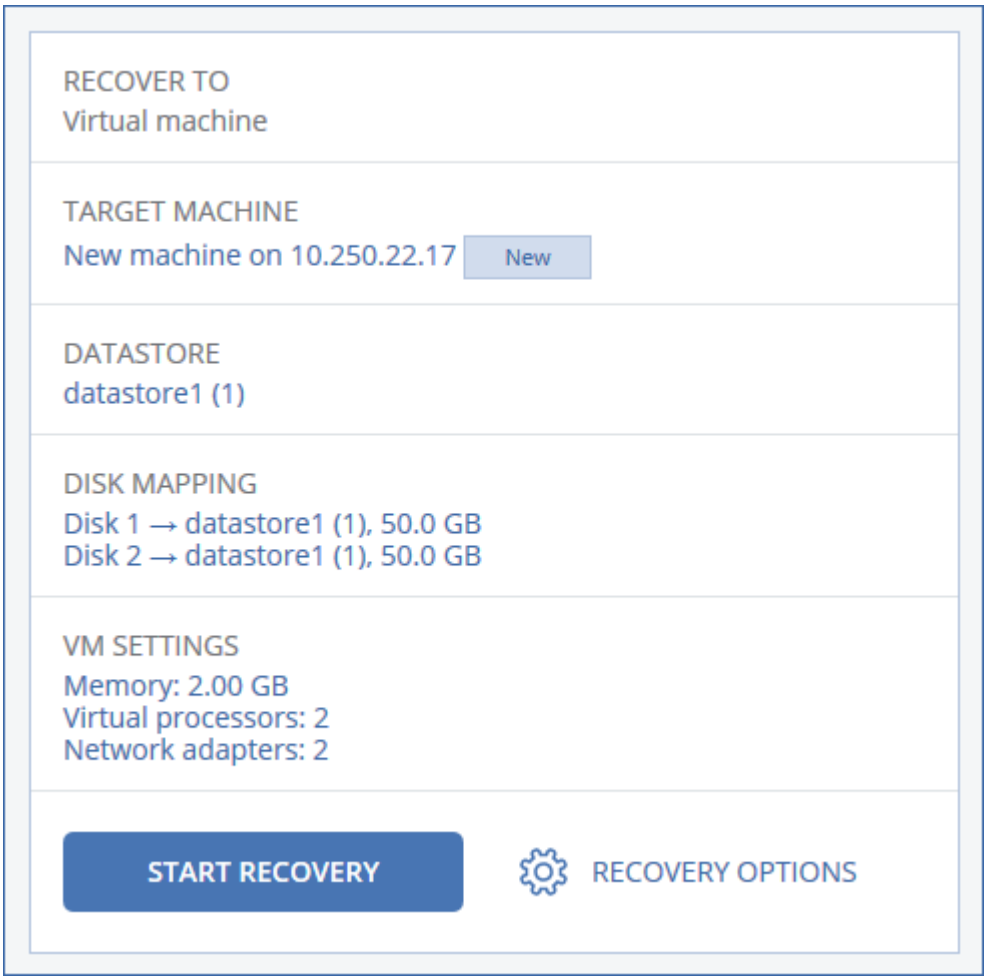
      Remarque
      Au moins un agent pour l'hyperviseur doit être installé et enregistré dans le serveur de gestion Acronis.

   b. Sélectionnez si vous souhaitez restaurer sur une machine nouvelle ou existante. L'option de nouvelle machine est préférable, étant donné qu'elle ne nécessite pas une correspondance exacte entre la configuration de disque de la machine cible et celle de la sauvegarde.
   c. Sélectionnez l'hôte et spécifiez le nouveau nom de machine ou sélectionnez une machine cible existante.
   d. Cliquez sur **OK**.
7. [Pour Virtuozzo Hybrid Infrastructure] Cliquez sur **Paramètres de MV** pour sélectionner **Variété**. Vous avez la possibilité de modifier la taille de la mémoire, le nombre de processeurs et les connexions réseau de la machine virtuelle.

   Remarque
   Il est obligatoire de sélectionner une variété pour Virtuozzo Hybrid Infrastructure.

8. [Facultatif] Configurez les options de récupération supplémentaires :
   - [Non disponible pour Virtuozzo Hybrid Infrastructure] Cliquez sur **Magasin de données** pour ESXi ou **Chemin d'accès** pour Hyper-V, puis sélectionnez le magasin de données (stockage) pour la machine virtuelle.
   - Cliquez sur **Mappage de disque** afin de sélectionner le magasin de données (stockage), l'interface et le mode d'allocation de chaque disque virtuel. La section Mappage permet également de choisir les disques individuels à restaurer.

     Pour Virtuozzo Hybrid Infrastructure, vous pouvez uniquement sélectionner la stratégie de stockage pour les disques de destination. Pour cela, sélectionnez le disque de destination souhaité, puis cliquez sur Modifier. Dans la lame qui s'ouvre, cliquez sur l'icône en forme d'engrenage, sélectionnez la stratégie de stockage, puis cliquez sur Terminé.
   - [Pour VMware ESXi, Hyper-V et Red Hat Virtualization/oVirt] Cliquez sur **Paramètres de MV** pour modifier la taille de mémoire, le nombre de processeurs et les connexions réseau de la machine virtuelle.



9. [Disponible uniquement pour les ordinateurs Windows sur lesquels un agent de protection est installé] Activez le curseur **Restauration sûre** afin de vous assurer que les données restaurées sont exemptes de malware. Pour plus d'informations sur le fonctionnement de la restauration sécurisée, voir "Restauration sûre" (p. 521).
10. Cliquez sur **Démarrer la récupération**.
11. Lors de la restauration sur une machine virtuelle existante, confirmez que vous souhaitez écraser les disques.

La progression de la restauration sont affichées dans l'onglet **Activités**.

Restauration d'une machine virtuelle

Vous pouvez restaurer des machines virtuelles avec leurs sauvegardes.

Remarque
Vous ne pouvez pas restaurer les sauvegardes dans la console Cyber Protect pour les tenants en mode Conformité. Pour plus d'informations sur la restauration de ces sauvegardes, voir "Restauration de sauvegardes pour les tenants en mode Conformité" (p. 1149).

Prérequis

- Lors de la restauration sur cette machine, vous devez arrêter la machine virtuelle. Par défaut, le logiciel stoppe la machine sans invite. Une fois la restauration terminée, vous devrez redémarrer manuellement la machine. Vous pouvez modifier ce comportement par défaut à l'aide de l'option de restauration de gestion de l'alimentation de MV (cliquez sur **Options de récupération** > **Gestion de l'alimentation de MV**).

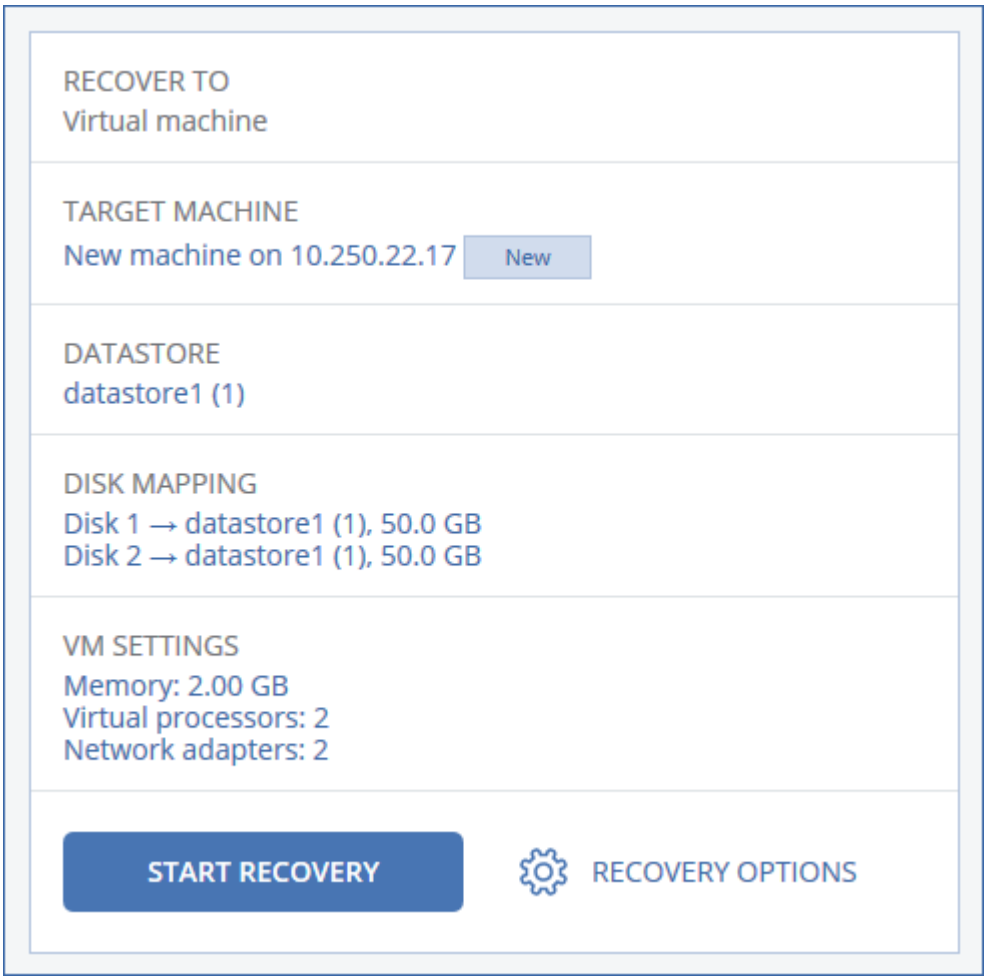
Procédure

1. Effectuez l'une des actions suivantes :
   - Sélectionnez une machine sauvegardée, cliquez sur **Restauration**, puis sélectionnez un point de restauration.
   - Sélectionnez un point de récupération dans l'onglet Stockage de sauvegarde.
2. Cliquez sur **Restaurer** > **Toute la machine**.
3. Si vous souhaitez effectuer la restauration vers une machine physique, sélectionnez **Machine physique** dans **Restaurer vers**. Sinon, ignorez cette étape.
   La restauration vers une machine physique est uniquement possible si la configuration de disque de la machine cible correspondant exactement à celle de la sauvegarde.
   Dans ce cas, poursuivez avec l'étape 4 dans « Machine physique ». Sinon, nous vous recommandons d'effectuer une migration V2P à l'aide d'un support de démarrage.
4. [Facultatif] Par défaut, le logiciel sélectionne automatiquement la machine d'origine comme machine cible. Pour effectuer la restauration vers une autre machine virtuelle, cliquez sur **Machine cible**, puis procédez comme suit :
   a. Sélectionnez l'hyperviseur (**VMware ESXi**, **Hyper-V**, **Virtuozzo Virtuozzo Hybrid Infrastructure**, **Scale Computing HC3** ou **oVirt**).
      Seules les machines virtuelles Virtuozzo peuvent être restaurées sur Virtuozzo. Pour plus d'informations sur la migration V2V, consultez « Migration de machine ».
   b. Sélectionnez si vous souhaitez restaurer sur une machine nouvelle ou existante.
   c. Sélectionnez l'hôte et spécifiez le nouveau nom de machine ou sélectionnez une machine cible existante.
   d. Cliquez sur **OK**.
5. Configurez les options de récupération supplémentaires dont vous avez besoin.
   - [Facultatif] [Non disponible pour Virtuozzo Hybrid Infrastructure et Scale Computing HC3] Pour sélectionner le magasin de données pour la machine virtuelle, cliquez sur **Magasin de données** pour ESXi, **Chemin d'accès** pour Hyper-V et Virtuozzo, ou **Domaine de stockage** pour Red Hat Virtualization (oVirt), puis sélectionnez le magasin de données (stockage) pour la machine virtuelle.
   - [Facultatif] Pour afficher le magasin de données (stockage), l'interface et le mode de provisionnement de chaque disque virtuel, cliquez sur **Mappage de disque**. Vous pouvez modifier ces paramètres, à moins que vous ne restauriez un conteneur Virtuozzo ou une machine virtuelle de Virtuozzo Hybrid Infrastructure.

Pour Virtuozzo Hybrid Infrastructure, vous pouvez uniquement sélectionner la stratégie de stockage pour les disques de destination. Pour cela, sélectionnez le disque de destination souhaité, puis cliquez sur **Modifier**. Dans la lame qui s'ouvre, cliquez sur l'icône en forme d'engrenage, sélectionnez la stratégie de stockage, puis cliquez sur **Terminé**.

La section Mappage permet également de choisir les disques individuels à restaurer.

- [Facultatif] [Disponible pour VMware ESXi, Hyper-V et Virtuozzo] Cliquez sur **Paramètres de MV** pour modifier la taille de mémoire, le nombre de processeurs et les connexions réseau de la machine virtuelle.
- [Pour Virtuozzo Hybrid Infrastructure] Cliquez sur **Variété** pour modifier la taille de mémoire et le nombre de processeurs ou les connexions réseau de la machine virtuelle.



6. [Disponible uniquement pour les ordinateurs Windows sur lesquels un agent de protection est installé] Activez le curseur **Restauration sûre** afin de vous assurer que les données restaurées sont exemptes de malware. Pour plus d'informations sur le fonctionnement de la restauration sécurisée, voir "Restauration sûre" (p. 521).
7. Cliquez sur **Démarrer la récupération**.
8. Lors de la restauration sur une machine virtuelle existante, confirmez que vous souhaitez écraser les disques.

La progression de la restauration sont affichées dans l'onglet **Activités**.

Restauration de disques via un support de démarrage

Pour en savoir plus sur la manière de créer un support de démarrage, consultez la section "Création d'un support de démarrage physique" (p. 748).

Remarque
Vous ne pouvez pas restaurer les sauvegarde de disque d'ordinateurs Mac Intel sur des Mac utilisant des puces silicone Apple, et inversement. Vous pouvez restaurer des fichiers et des dossiers.

Pour restaurer des disques via un support de démarrage

1. Démarrez la machine cible par le biais d'un support de démarrage.
2. [Uniquement lors de la restauration d'un Mac] Si vous restaurez des disques/volumes formatés APFS vers une machine non d'origine ou à froid, recréez la configuration du disque d'origine manuellement :
   a. Cliquez sur **Utilitaire de disque**.
   b. Effacer et formater le disque de destination dans APFS. Pour obtenir des instructions, consultez l'article https://support.apple.com/en-us/HT208496#erasedisk.
   c. Recréez la configuration du disque d'origine. Pour obtenir des instructions, consultez l'article https://support.apple.com/guide/disk-utility/add-erase-or-delete-apfs-volumes-dskua9e6a110/19.0/mac/10.15.
   d. Cliquez sur **Utilitaire de disque** > **Quitter l'utilitaire de disque**.
3. Cliquez sur **Gérer cette machine localement** ou double-cliquez sur **Support de Secours Bootable**, en fonction du type de support que vous utilisez.
4. Si un serveur proxy est activé dans votre réseau, cliquez sur **Outils** > **Serveur proxy**, puis spécifiez l'adresse IP/nom de l'hôte, le port et les informations d'identification du serveur proxy. Sinon, ignorez cette étape.
5. [Facultatif] Lors d'une restauration depuis Windows ou Linux, cliquez sur **Outils** > **Enregistrer le support au sein du service Cyber Protection** , puis spécifiez le jeton d'enregistrement que vous avez obtenu lorsque vous avez téléchargé le support. Si vous faites cela, vous n'aurez pas besoin de saisir d'informations d'identification ni de code d'inscription pour accéder au stockage Cloud, comme décrit à l'étape 8.
6. Sur l'écran d'accueil, cliquez sur **Restaurer**.
7. Cliquez sur **Sélectionner des données**, puis cliquez sur **Parcourir**.
8. Indiquez l'emplacement de la sauvegarde :
   - Pour restaurer des informations depuis le Cloud, sélectionnez **Stockage dans le Cloud**. Saisissez les informations d'identification du compte auquel la machine sauvegardée a été associée.

     Lors d'une restauration Windows ou Linux, vous avez la possibilité de demander un code d'inscription et de l'utiliser à la place de vos informations d'identification. Cliquez sur **Utiliser**

le code d'inscription > **Demander le code**. Le logiciel affiche le lien et le code d'inscription. Vous pouvez les copier et effectuer les étapes d'enregistrement sur une autre machine. Le code d'enregistrement n'est valable qu'une heure.

- Pour effectuer une restauration depuis un dossier local ou réseau, rendez-vous dans **Dossiers locaux** ou **Dossiers réseau**.
- Pour effectuer une restauration à partir d'emplacements de sauvegarde sur un stockage dans le cloud public tel que Microsoft Azure, Amazon S3, Wasabi ou S3 compatible, cliquez d'abord sur **Enregistrer le support dans le service Cyber Protection**, puis configurez la restauration à l'aide de l'interface Web. Pour plus d'informations sur la gestion des supports à distance via l'interface Web, voir "Opérations à distance avec un support de démarrage" (p. 766).

Cliquez sur **OK** pour confirmer votre sélection.

9. Sélectionnez la sauvegarde à partir de laquelle vous voulez restaurer les données. Si vous y êtes invité, saisissez le mot de passe pour la sauvegarde.
10. Dans **Contenu des sauvegardes**, sélectionnez les disques que vous souhaitez restaurer. Cliquez sur **OK** pour confirmer votre sélection.
11. Sous **Où restaurer**, le logiciel mappe automatiquement les disques sélectionnés vers les disques cibles.

    Si le mappage échoue, ou si vous n'êtes pas satisfait du résultat, vous pouvez remapper les disques manuellement.

    Remarque
    Modifier la disposition du disque peut affecter la capacité de démarrage du système d'exploitation. Veuillez utiliser la disposition originale du disque de la machine à moins que vous ne soyez certain de votre succès.

12. [Lors de la restauration de Linux] Si la machine sauvegardée possédait des volumes logiques (LVM) et que vous voulez en reproduire la structure initiale :
    a. Assurez-vous que le nombre de disques sur la machine cible et que leur capacité sont équivalents ou supérieurs à ceux de la machine d'origine, puis cliquez sur **Appliquer RAID/LVM**.
    b. Revoyez la structure des volumes et cliquez ensuite sur **Appliquer RAID/LVM** pour la créer.
13. [Facultatif] Cliquez sur **Options de restauration**, pour spécifier des paramètres supplémentaires.
14. Cliquez sur **OK** pour démarrer la restauration.

En utilisant Universal Restore

Les systèmes d'exploitation les plus récents peuvent être démarrés lorsqu'ils sont restaurés sur un matériel différent, notamment sur les plates-formes VMware ou Hyper-V. Si un système d'exploitation restauré ne démarre pas, utilisez l'outil Universal Restore pour mettre à jour les pilotes et les modules essentiels au démarrage du système d'exploitation.

Universal Restore peut s'appliquer à Windows et Linux.

Pour appliquer Universal Restore

1. Démarrez la machine à partir du support de démarrage.
2. Cliquez sur **Appliquer Universal Restore**.
3. S'il existe plusieurs systèmes d'exploitation sur la machine, choisissez celui sur lequel appliquer Universal Restore.
4. [Pour Windows uniquement] Configurez les paramètres supplémentaires.
5. Cliquez sur **OK**.

Universal Restore sous Windows

Préparation

Préparez les pilotes

Avant d'appliquer Universal Restore à un système d'exploitation Windows, assurez-vous que vous avez les pilotes pour le nouveau contrôleur de disque dur et pour le jeu de puces. Ces pilotes sont cruciaux pour lancer le système d'exploitation. Utilisez le CD ou le DVD fourni par le fabricant du matériel ou téléchargez les pilotes depuis le site Web du fabricant. Les fichiers pilotes doivent avoir l'extension *.inf. Si vous téléchargez les pilotes au format *.exe, *.cab ou *.zip, veuillez les extraire en utilisant une application tierce.

La meilleure pratique consiste à stocker les pilotes pour tout le matériel utilisé dans votre organisation dans un seul dépôt trié par type de terminal ou par configuration matérielle. Vous pouvez conserver une copie du dépôt sur un DVD ou sur un lecteur flash ; choisissez des pilotes et ajoutez-les au support de démarrage ; créez le support de démarrage personnalisé avec les pilotes nécessaires (et les configurations réseau nécessaires) pour chacun de vos serveurs. Vous pouvez aussi simplement spécifier le chemin vers le répertoire chaque fois que Universal Restore est utilisé.

Vérifiez l'accès aux pilotes dans l'environnement de démarrage

Assurez-vous que vous avez accès au terminal contenant les pilotes quand vous travaillez en utilisant un support de démarrage. Utilisez un support basé sur WinPE si le terminal est disponible sous Windows mais que le support basé sur Linux ne le détecte pas.

Paramètres de Universal Restore

Recherche de pilote automatique

Spécifiez où le programme recherchera les pilotes de la couche d'abstraction matérielle (HAL - Hardware Abstraction Layer), du contrôleur de disque dur et de l'adaptateur réseau :

- Si les pilotes se trouvent sur le disque d'un fournisseur ou sur un autre support amovible, activez **Rechercher dans le support amovible**.

- Si les pilotes sont situés dans un dossier en réseau ou sur le support de démarrage, spécifiez le chemin d'accès au dossier en cliquant sur **Ajouter un dossier**.

En outre, Universal Restore recherche dans le dossier Windows de stockage des pilotes par défaut. Son emplacement est indiqué dans la valeur de registre **DevicePath**, laquelle se trouve dans la clé de la base de registre **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion**. Ce dossier de stockage est généralement WINDOWS / inf.

Universal Restore exécute une recherche récursive dans tous les sous-dossiers du dossier spécifié, trouve les pilotes HAL et de contrôleur de disque dur les plus appropriés de tous ceux qui sont disponibles, et les installe sur le système restauré. Universal Restore recherche également le pilote de la carte réseau ; le chemin vers le pilote trouvé est alors transmis par Universal Restore au système d'exploitation. Si le matériel possède plusieurs cartes d'interface réseau, Universal Restore tentera de configurer les pilotes de toutes les cartes.

Pilotes de stockage de masse à installer de toutes façons

Vous avez besoin de ce paramètre si :

- Le matériel a un contrôleur de stockage de masse spécifique tel que RAID (particulièrement NVIDIA RAID) ou un adaptateur fibre channel.
- Vous avez effectué la migration d'un système sur une machine virtuelle qui utilise un contrôleur de disque dur SCSI. Utilisez les pilotes SCSI fournis avec le logiciel de virtualisation ou téléchargez les versions les plus récentes des pilotes à partir du site Web du fabricant du logiciel.
- La recherche de pilotes automatiques n'aide pas a démarrer le système.

Spécifiez les pilotes appropriés en cliquant sur **Ajouter le pilote**. Les pilotes définis ici sont installés, avec un avertissement approprié, même si le programme trouve un meilleur pilote.

Processus Universal Restore

Après avoir spécifié les paramètres requis, cliquez sur **OK**.

Si Universal Restore ne peut pas trouver un pilote compatible dans les emplacements spécifiés, il affiche une invite sur le terminal problématique. Effectuez l'une des actions suivantes :

- Ajoutez le pilote dans n'importe quel emplacement spécifié précédemment et cliquez sur **Réessayer**.
- Si vous ne vous souvenez pas de l'emplacement, cliquez sur **Ignorer** pour continuer le processus. Si le résultat n'est pas satisfaisant, appliquez Universal Restore à nouveau. Lorsque vous configurez l'opération, spécifiez le pilote nécessaire.

Lorsque Windows démarre, la procédure courante pour l'installation de nouveaux matériels sera initialisée. Le pilote de l'adaptateur réseau est installé silencieusement si le pilote a la signature Microsoft Windows. Sinon, Windows demandera de confirmer l'installation du pilote ne possédant pas la signature.

Après cela, vous pouvez configurer la connexion réseau et spécifier les pilotes pour les adaptateurs graphique, USB et autres périphériques.

Universal Restore sous Linux

Universal Restore peut être appliqué aux systèmes opérationnels de version Linux 2.6.8 ou supérieure.

Quand Universal Restore est appliqué à un système d'exploitation Linux, il met à jour un système de fichiers temporaire connu comme le disque RAM initial (initrd). Cela garantit que le système d'exploitation peut démarrer sur le nouveau matériel.

Universal Restore ajoute des modules pour le nouveau matériel (y compris les pilotes de périphériques) pour le disque RAM initial. En règle générale, il trouve les modules nécessaires dans le répertoire **/lib/modules**. Si Universal Restore ne peut pas trouver un module dont il a besoin, il enregistre le nom de fichier du module dans le journal.

Universal Restore peut modifier la configuration du chargeur de démarrage GRUB. Cela peut être nécessaire, par exemple, pour assurer la capacité de démarrage du système lorsque la nouvelle machine possède une structure de volume différente de la machine d'origine.

Universal Restore ne modifie jamais le noyau Linux.

Pour rétablir le disque RAM initial d'origine

Vous pouvez rétablir le disque RAM initial d'origine si nécessaire.

Le disque RAM initial est stocké sur la machine dans un fichier. Avant de mettre à jour le disque RAM initial pour la première fois, Universal Restore en enregistre une copie dans le même répertoire. Le nom de la copie est le nom du fichier, suivi par le suffixe **_acronis_backup.img**. Cette copie ne sera pas écrasée si vous exécutez Universal Restore plusieurs fois (par exemple, après avoir ajouté des pilotes manquants).

Pour rétablir le disque RAM initial d'origine, exécutez l'une des actions suivantes :

- Renommez la copie en conséquence. Par exemple, exécutez une commande semblable à celle-ci :

  ```
  mv initrd-2.6.16.60-0.21-default_acronis_backup.img initrd-2.6.16.60-0.21-default
  ```

- Spécifiez la copie dans la ligne **initrd** de la configuration du chargeur de démarrage GRUB.

Restauration des fichiers

Restauration de fichiers dans la console Cyber Protect

Remarque
Vous ne pouvez pas restaurer les sauvegardes dans la console Cyber Protect pour les tenants en mode Conformité. Pour plus d'informations sur la restauration de ces sauvegardes, voir "Restauration de sauvegardes pour les tenants en mode Conformité" (p. 1149).

1. Sélectionnez la machine sur laquelle les données que vous souhaitez restaurer étaient initialement présentes.
2. Cliquez sur **Restauration**.
3. Sélectionnez le point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

   Si la machine sélectionnée est physique et hors ligne, les points de restauration ne sont pas affichés. Effectuez l'une des actions suivantes :

   - [Recommandé] Si la sauvegarde est située sur le Cloud ou à un emplacement de stockage partagé (c.-à-d. que d'autres agents peuvent y accéder), cliquez sur **Sélectionner une machine**, sélectionnez une machine cible qui est en ligne, puis choisissez un point de récupération.
   - Sélectionnez un point de récupération dans l'onglet Stockage de sauvegarde.
   - Téléchargement de fichiers depuis le Cloud
   - Utilisation d’un support de démarrage
4. Cliquez sur **Restaurer** > **Fichiers/dossiers**.
5. Accédez au dossier requis ou servez-vous de la barre de recherche pour obtenir la liste des fichiers et dossiers requis.

   La recherche ne dépend pas de la langue.

   Vous pouvez utiliser un ou plusieurs caractères génériques (* et ?). Pour plus de détails sur l’utilisation de caractères génériques, voir "Masque" (p. 483).

   Remarque
   La recherche n’est pas disponible pour les sauvegardes de lecteur qui sont stockées dans le Cloud.
6. Sélectionnez les fichiers que vous voulez restaurer.
7. Si vous souhaitez enregistrer les fichiers au format .zip, cliquez sur **Télécharger**, sélectionnez l’emplacement où enregistrer les données et cliquez sur **Enregistrer**. Sinon, ignorez cette étape.

   Le téléchargement n'est pas disponible si votre sélection contient des dossiers ou si la taille totale des fichiers sélectionnés dépasse 100 Mo. Pour récupérer de plus grandes quantités de

données depuis le cloud, suivez la procédure "Téléchargement de fichiers depuis le Cloud" (p. 536).

8. Cliquez sur **Restaurer**.

   Dans **Restaurer vers**, cliquez pour sélectionner la cible de l'opération de récupération ou conservez la cible par défaut. La cible par défaut varie en fonction de la source de la sauvegarde.

   Les cibles suivantes sont disponibles :

   - Machine source (si un agent de protection y est installé).

     Il s'agit de l'ordinateur qui contenait à l'origine les fichiers que vous souhaitez restaurer.
   - Autres ordinateurs sur lesquelles un agent de protection est installé : machines physiques, machines virtuelles et hôtes de virtualisation sur lesquels un agent de protection est installé, ou appliances virtuelles.

     Vous pouvez restaurer des fichiers sur des machines physiques, des machines virtuelles et des hôtes de virtualisation sur lesquels un agent de protection est installé. Vous ne pouvez pas restaurer des fichiers sur des machines virtuelles sur lesquelles aucun agent de protection n'est installé (à l'exception des machines virtuelles Virtuozzo).
   - Conteneurs ou machines virtuelles Virtuozzo.

     Vous pouvez restaurer des fichiers sur des conteneurs et des machines virtuelles Virtuozzo, avec toutefois quelques restrictions. Pour plus d'informations, voir "Limites de la restauration des fichiers dans la console Cyber Protect" (p. 541).
9. Dans **Chemin d'accès**, sélectionnez la destination de la restauration. Vous pouvez sélectionner l'une des options suivantes :
   - [Lors d'une restauration vers l'ordinateur d'origine] Emplacement d'origine.
   - Dossier local ou stockage attaché localement sur la machine cible.

     Remarque
     Les liens symboliques ne sont pas pris en charge.
   - Un dossier réseau accessible depuis la machine cible
10. Cliquez sur **Démarrer la récupération**.
11. Sélectionnez l'une des options d'écrasement de fichier :
    - **Écraser les fichiers existants**
    - **Écraser un fichier existant s'il est plus ancien**
    - **Ne pas écraser les fichiers existants**

La progression de la restauration sont affichées dans l'onglet **Activités**.

Téléchargement de fichiers depuis le Cloud

Dans la console Web de restauration, vous pouvez parcourir le stockage dans le cloud, voir le contenu des sauvegardes et télécharger des fichiers et des dossiers sauvegardés.

Remarque
Vous ne pouvez accéder à la console Web de restauration que si vous êtes administrateur du client Cyber Protection ou utilisateur du tenant du client. Les rôles d'utilisateur de niveau partenaire ne sont pas autorisés.

Limites

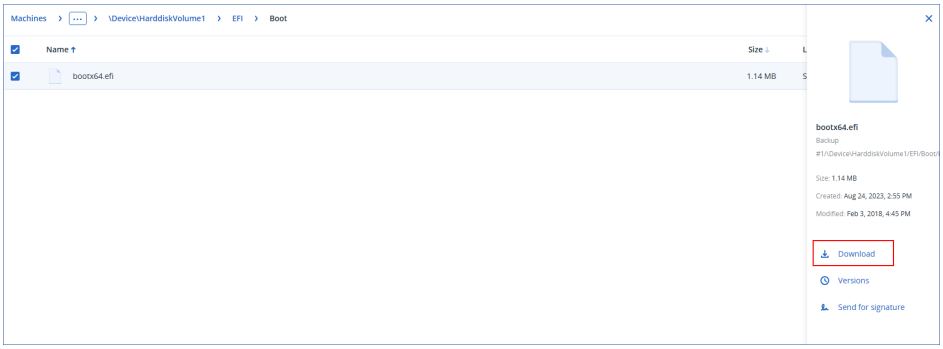
- Vous ne pouvez pas télécharger des disques, des volumes ou des points de restauration complets sauvegardés.
- Lorsque vous parcourez les sauvegardes de niveau disque, les volumes logiques (tels que LVM et LDM) ne sont pas affichés.
- Vous ne pouvez pas parcourir les sauvegardes de l'état du système, des bases de données SQL et des bases de données Exchange.

Pour télécharger des fichiers et des dossiers du stockage dans le cloud

1. Dans la console Cyber Protection, sélectionnez la ressource requise, puis cliquez sur **Restauration**.
2. [Si plusieurs emplacements de sauvegarde sont disponibles] Sélectionnez l'emplacement de sauvegarde, puis cliquez sur **Autres méthodes de restauration**.
3. Cliquez sur **Télécharger les fichiers**.
4. Sous **Ordinateurs**, cliquez sur le nom de la ressource, puis sur l'archive de sauvegarde.
   Une archive de sauvegarde contient une ou plusieurs sauvegardes (points de restauration).
5. Cliquez sur le numéro de sauvegarde (point de restauration) à partir duquel vous souhaitez télécharger des fichiers ou des dossiers, puis accédez aux éléments requis.
6. Cochez les cases situées à côté des éléments à télécharger.

   Remarque
   Si vous sélectionnez plusieurs éléments, ils sont téléchargés sous forme de fichier ZIP.

7. Cliquez sur **Télécharger**.



Vérification de l'authenticité d'un fichier grâce à Notary Service

Si la notarisation a été activée lors de la sauvegarde, vous pouvez vérifier l'authenticité d'un fichier sauvegardé.

Pour vérifier l'authenticité d'un fichier

1. Sélectionnez le fichier tel que décrit dans les étapes 1 à 6 de la section « Restauration de fichiers via l'interface Web », ou les étapes 1 à 5 de la section « Téléchargement de fichiers depuis le Cloud ».
2. Assurez-vous que le fichier sélectionné possède l'icône suivante :  . Cela signifie que le fichier est notarié.
3. Effectuez l'une des actions suivantes :
   - Cliquez sur **Vérifier**.
     Le logiciel vérifie l'authenticité du fichier et affiche le résultat.
   - Cliquez sur **Obtenir certificat**.
     Un certificat confirmant la notarisation du fichier est ouvert dans une fenêtre de navigateur Web. La fenêtre contient également les instructions qui vous permettent de vérifier l'authenticité d'un fichier manuellement.

Signer un fichier avec ASign

Remarque
Cette fonctionnalité est disponible avec le pack Advanced Backup.

ASign est un service permettant à plusieurs personnes de signer électroniquement un fichier sauvegardé. Cette fonctionnalité est accessible uniquement pour les sauvegardes de niveau fichier stockées dans le stockage dans le Cloud.

Une seule version de fichier peut être signée à la fois. Si le fichier a été sauvegardé à plusieurs reprises, vous devez choisir la version à signer, et seule cette version sera signée.

ASign peut par exemple être utilisé pour la signature électronique des fichiers suivants :

- Contrats de location ou baux
- Contrats de vente
- Conventions d'achat de biens
- Contrats de prêt
- Feuilles de permission
- Documents financiers
- Documents d'assurance
- Décharges de responsabilité

- Documents médicaux
- Documents de recherche
- Certificats d'authenticité
- Accords de non-divulgation
- Lettres de proposition
- Accords de confidentialité
- Contrats de prestataires indépendants

Pour signer une version de fichier

1. Sélectionnez le fichier tel que décrit dans les étapes 1 à 6 de la section « Restauration de fichiers via l'interface Web », ou les étapes 1 à 5 de la section « Téléchargement de fichiers depuis le Cloud ».
2. Assurez-vous que la bonne date et la bonne heure sont sélectionnées dans le volet de gauche.
3. Cliquez sur **Signer cette version de fichier**.
4. Indiquez le mot de passe pour le compte de stockage dans le Cloud sous lequel la sauvegarde est stockée. L'identifiant de connexion du compte est affiché dans votre fenêtre d'invite.
   L'interface du service ASign est ouverte dans une fenêtre de navigateur Web.
5. Ajoutez d'autres signataires en indiquant leur adresse e-mail. Il n'est pas possible d'ajouter ou supprimer des signataires après avoir envoyé les invitations, assurez-vous donc que la liste contient chaque personne dont la signature est nécessaire.
6. Cliquez sur **Inviter à signer** pour envoyer l'invitation aux signataires.
   Chaque signataire reçoit un e-mail contenant la demande de signature. Lorsque tous les signataires auxquels vous l'aurez demandé auront signé le fichier, ce dernier sera notarié et signé via le service de notarisation.
   Vous recevrez une notification à la signature de chaque signataire, et lorsque le processus sera entièrement terminé. Vous pouvez accéder à la page Web ASign en cliquant sur **Afficher les détails** dans l'un des e-mails que vous recevez.
7. Une fois le processus terminé, rendez-vous sur la page Web ASign et cliquez sur **Obtenir le document** pour télécharger un document .pdf contenant :
   - La page du certificat de signature avec toutes les signatures récoltées.
   - La page du journal d'audit contenant l'historique des activités : date/heure à laquelle l'invitation a été envoyée aux signataires, date/heure à laquelle chaque signataire a signé le fichier, etc.

Restauration de fichiers via un support de démarrage

Pour en savoir plus sur la manière de créer un support de démarrage, consultez la section « Création d'un support de démarrage ».

Pour restaurer des fichiers via un support de démarrage

1. Démarrez la machine cible à l'aide du support de démarrage.
2. Cliquez sur **Gérer cette machine localement** ou double-cliquez sur **Support de Secours Bootable**, en fonction du type de support que vous utilisez.
3. Si un serveur proxy est activé dans votre réseau, cliquez sur **Outils** > **Serveur proxy**, puis spécifiez l'adresse IP/nom de l'hôte, le port et les informations d'identification du serveur proxy. Sinon, ignorez cette étape.
4. [Facultatif] Lors d'une restauration depuis Windows ou Linux, cliquez sur **Outils** > **Enregistrer le support au sein du service Cyber Protection** , puis spécifiez le jeton d'enregistrement que vous avez obtenu lorsque vous avez téléchargé le support. Si vous faites cela, vous n'aurez pas besoin de saisir d'informations d'identification ni de code d'inscription pour accéder au stockage Cloud, comme décrit à l'étape 7.
5. Sur l'écran d'accueil, cliquez sur **Restaurer**.
6. Cliquez sur **Sélectionner des données**, puis cliquez sur **Parcourir**.
7. Indiquez l'emplacement de la sauvegarde :
   - Pour restaurer des informations depuis le Cloud, sélectionnez **Stockage dans le Cloud**. Saisissez les informations d'identification du compte auquel la machine sauvegardée a été associée.

     Lors d'une restauration Windows ou Linux, vous avez la possibilité de demander un code d'inscription et de l'utiliser à la place de vos informations d'identification. Cliquez sur **Utiliser le code d'inscription** > **Demander le code**. Le logiciel affiche le lien et le code d'inscription. Vous pouvez les copier et effectuer les étapes d'enregistrement sur une autre machine. Le code d'enregistrement n'est valable qu'une heure.
   - Pour effectuer une restauration depuis un dossier local ou réseau, rendez-vous dans **Dossiers locaux** ou **Dossiers réseau**.
   - Pour effectuer une restauration à partir d'emplacements de sauvegarde sur un stockage dans le cloud public tel que Microsoft Azure, Amazon S3, Wasabi ou S3 compatible, cliquez d'abord sur **Enregistrer le support dans le service Cyber Protection**, puis configurez la restauration à l'aide de l'interface Web. Pour plus d'informations sur la gestion des supports à distance via l'interface Web, voir "Opérations à distance avec un support de démarrage" (p. 766).

   Cliquez sur **OK** pour confirmer votre sélection.
8. Sélectionnez la sauvegarde à partir de laquelle vous voulez restaurer les données. Si vous y êtes invité, saisissez le mot de passe pour la sauvegarde.
9. Dans **Contenu des sauvegardes**, sélectionnez **Dossiers/fichiers**.
10. Sélectionnez les données que vous voulez restaurer. Cliquez sur **OK** pour confirmer votre sélection.
11. Dans **Où restaurer**, indiquez un dossier. Vous pouvez également empêcher l'écrasement des versions plus récentes des fichiers ou exclure certains fichiers de la restauration.
12. [Facultatif] Cliquez sur **Options de restauration**, pour spécifier des paramètres

supplémentaires.

13. Cliquez sur **OK** pour démarrer la restauration.

Extraction de fichiers à partir de sauvegardes locales

Vous pouvez explorer les contenus de sauvegardes et extraire les fichiers dont vous avez besoin.

Configuration requise

- Cette fonctionnalité est uniquement disponible sous Windows à l'aide de l'Explorateur de fichiers.
- Le système du fichier sauvegardé doit être l'un des suivants : FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS ou HFS+.

Prérequis

- Un agent de protection doit être installé sur la machine utilisée pour explorer la sauvegarde.
- La sauvegarde doit être stockée dans un dossier local ou sur un partage réseau (SMB/CIFS).

Extraction de fichiers à partir d'une sauvegarde

1. Accédez à l'emplacement de la sauvegarde à l'aide de l'Explorateur de fichiers.
2. Double-cliquez sur le fichier de sauvegarde. Les noms des fichiers reposent sur l'exemple suivant :

   `<nom de machine> - <GUID du plan de protection>`
3. Si la sauvegarde est chiffrée, saisissez le mot de passe de chiffrement. Sinon, ignorez cette étape.

   L'Explorateur de fichiers affiche les points de restauration.
4. Double-cliquez sur le point de restauration.

   L'Explorateur de fichiers affiche les données sauvegardées.
5. Accédez au dossier requis.
6. Copiez les fichiers requis vers n'importe quel dossier du système de fichiers.

Limites de la restauration des fichiers dans la console Cyber Protect

Tenants en mode Conformité

Vous ne pouvez pas restaurer les sauvegardes dans la console Cyber Protect pour les tenants en mode Conformité. Pour plus d'informations sur la restauration de ces sauvegardes, voir "Restauration de sauvegardes pour les tenants en mode Conformité" (p. 1149).

Reprise sur des conteneurs ou machines virtuelles Virtuozzo

- L'agent client QEMU doit être installé sur la machine virtuelle cible.
- [S'applique uniquement lors de la restauration dans des conteneurs] Les points de montage dans les conteneurs ne peuvent pas être utilisés comme cible de reprise. Par exemple, vous ne pouvez pas restaurer des fichiers sur un second disque dur ou sur un partage NFS monté dans un

conteneur.

- Lors de la restauration de fichiers dans une machine virtuelle Windows et si l'option de reprise "Sécurité de niveau fichier" (p. 548) est activée, l'attribut de bit d'archive est défini sur les fichiers restaurés.
- Les fichiers comportant dans leur nom des caractères non-ANSI sont restaurés avec des noms incorrects sur les ordinateurs exécutant Windows Server 2012 ou une version antérieure, et Windows 7 ou une version antérieure.
- Pour restaurer des fichiers sur des machines virtuelles CentOS ou Red Hat Enterprise Linux qui s'exécutent sur un serveur hybride Virtuozzo, vous devez modifier le fichier `qemu-ga` comme suit :
  - Sur la machine virtuelle cible, accédez à `/etc/sysconfig/`, puis ouvrez le fichier `qemu-ga` pour le modifier.
  - Accédez à la ligne suivante, puis supprimez tout ce qui suit le signe égal (=) :

    ```
    BLACKLIST_RPC=
    ```

  - Redémarrez l'agent client QEMU en exécutant la commande suivante :

    ```
    systemctl restart qemu-guest-agent
    ```

Restauration de l'état du système

Remarque
Vous ne pouvez pas restaurer les sauvegardes dans la console Cyber Protect pour les tenants en mode Conformité. Pour plus d'informations sur la restauration de ces sauvegardes, voir "Restauration de sauvegardes pour les tenants en mode Conformité" (p. 1149).

1. Sélectionnez la machine pour laquelle vous voulez restaurer l'état du système.
2. Cliquez sur **Restauration**.
3. Sélectionnez un point de restauration de l'état du système. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.
4. Cliquez sur **Restaurer l'état du système**.
5. Confirmez que vous souhaitez écraser l'état du système avec sa version sauvegardée.

La progression de la restauration sont affichées dans l'onglet **Activités**.

Restauration d'une configuration ESXi

Pour restaurer une configuration ESXi, vous avez besoin d'un support de démarrage basé sur Linux. Pour en savoir plus sur la manière de créer un support de démarrage, consultez la section "Création d'un support de démarrage physique" (p. 748).

Si vous restaurez une configuration ESXi sur un hôte non d'origine et que l'hôte ESXi d'origine est toujours connecté au vCenter Server, déconnectez et supprimez cet hôte du vCenter Server pour éviter des problèmes inattendus au cours de la restauration. Si vous souhaitez conserver l'hôte

d'origine ainsi que l'hôte restauré, vous pouvez de nouveau l'ajouter une fois la restauration terminée.

Les machines virtuelles s'exécutant sur l'hôte ne sont pas incluses dans la sauvegarde de la configuration ESXi. Elles peuvent être sauvegardées et restaurées séparément.

Pour restaurer une configuration ESXi

1. Démarrez la machine cible à l'aide du support de démarrage.
2. Cliquez sur **Gérer cette machine localement**.
3. Sur l'écran d'accueil, cliquez sur **Restaurer**.
4. Cliquez sur **Sélectionner des données**, puis cliquez sur **Parcourir**.
5. Indiquez l'emplacement de la sauvegarde :
   - Accédez au dossier sous **Dossiers locaux** ou **Dossiers réseau**.

   Cliquez sur **OK** pour confirmer votre sélection.
6. Dans **Afficher**, sélectionnez **Configurations ESXi**.
7. Sélectionnez la sauvegarde à partir de laquelle vous voulez restaurer les données. Si vous y êtes invité, saisissez le mot de passe pour la sauvegarde.
8. Cliquez sur **OK**.
9. Dans **Disques à utiliser pour les nouveaux magasins de données**, procédez comme suit :
   - Sous **Restaurer ESXi sur**, sélectionnez le disque de restauration de la configuration de l'hôte. Si vous restaurez la configuration sur l'hôte d'origine, le disque d'origine est sélectionné par défaut.
   - [Facultatif] Sous **Utiliser pour les nouveaux magasins de données**, sélectionnez les disques où les nouveaux magasins de données seront créés. Soyez vigilant car toutes les données sur les disques sélectionnés seront perdues. Si vous souhaitez conserver les machines virtuelles dans les magasins de données existants, ne sélectionnez aucun disque.
10. Si aucun disque pour les nouveaux magasins de données n'est sélectionné, sélectionnez la méthode de création de magasins de données dans **Comment créer de nouveaux magasins de données** : **Créer un magasin de données par disque** ou **Créer un magasin de données sur tous les disques durs sélectionnés**.
11. [Facultatif] Dans **Mappage de réseau**, changez le résultat du mappage automatique des commutateurs virtuels présents dans la sauvegarde pour les adaptateurs réseau physiques.
12. [Facultatif] Cliquez sur **Options de restauration**, pour spécifier des paramètres supplémentaires.
13. Cliquez sur **OK** pour démarrer la restauration.

Options de restauration

Pour modifier les options de restauration, cliquez sur **Options de restauration** lors de la configuration de la restauration.

Disponibilité des options de restauration

L'ensemble des options de restauration disponibles dépendent de :

- L'environnement dans lequel fonctionne l'agent effectuant la restauration (Windows, Linux, macOS ou support de démarrage).
- le type de données en cours de restauration (disques, fichiers, machines virtuelles, données d'application).

Le tableau suivant résume la disponibilité des options de restauration.

	Disques			**Fichiers**				**Machines virtuelles**	**SQL et Exchange**
	Windows	**Linux**	**Support de démarrage**	**Windows**	**Linux**	**macOS**	**Support de démarrage**	**ESXi, Hyper-V et Virtuozzo**	**Windows**
Validation de la sauvegarde	+	+	+	+	+	+	+	+	+
Mode de démarrage	+	-	-	-	-	-	-	+	-
Date et heure des fichiers	-	-	-	+	+	+	+	-	-
Gestion erreurs	+	+	+	+	+	+	+	+	+
Exclusions de fichiers	-	-	-	+	+	+	+	-	-
Sécurité de niveau fichier	-	-	-	+	-	-	-	-	-
Flashback	+	+	+	-	-	-	-	+	-
Restauration de chemin d'accès complet	-	-	-	+	+	+	+	-	-
Points de	-	-	-	+	-	-	-	-	-

montage									
Performance	+	+	-	+	+	+	-	+	+
Commandes Pré/Post	+	+	-	+	+	+	-	+	+
Modification de SID	+	-	-	-	-	-	-	-	-
Gestion de l'alimentation des MV	-	-	-	-	-	-	-	+	-
Journal des événements Windows	+	-	-	+	-	-	-	Hyper-V uniquement	+

Validation de la sauvegarde

Cette option définit si la sauvegarde doit être validée avant la restauration des données afin de garantir qu'elle n'est pas corrompue. Cette opération est effectuée par l'agent de protection.

Le préréglage est le suivant : **Désactivé**.

Pour en savoir plus sur la validation par vérification de somme de contrôle, reportez-vous à "Vérification de la somme de contrôle" (p. 212).

Remarque
Selon les paramètres choisis par votre fournisseur de services, il se peut que la validation ne soit pas disponible lors d'une sauvegarde sur le stockage dans le Cloud.

Mode de démarrage

Cette option est effective lors de la restauration d'une machine physique ou virtuelle depuis une sauvegarde de lecteur contenant un système d'exploitation Windows.

Cette option vous permet de sélectionner le mode de démarrage (BIOS ou UEFI) que Windows utilisera après la restauration. Si le mode de démarrage de la machine d'origine diffère du mode de démarrage sélectionné, le logiciel :

- Initialisera le disque vers lequel vous restaurez le volume système, en fonction du mode de démarrage sélectionné (MBR pour BIOS, GPT pour UEFI).
- Ajustera le système d'exploitation Windows afin qu'il puisse démarrer en utilisant le mode de démarrage sélectionné.

Le préréglage est le suivant : **Comme sur la machine cible.**

Vous pouvez choisir l'une des options suivantes:

- **Comme sur la machine cible**

  L'agent qui s'exécute sur la machine cible détecte le mode de démarrage actuellement utilisé par Windows et procède aux ajustements en fonction du mode de démarrage sélectionné.

  C'est la valeur la plus sûre qui entraîne un système bootable, sauf si les restrictions répertoriées ci-dessous s'appliquent. Étant donné que l'option **Mode de démarrage** est absente sous le support de démarrage, l'agent sur le support se comporte toujours comme si la valeur était choisie.
- **Comme sur la machine sauvegardée**

  L'agent qui s'exécute sur la machine cible lit le mode de démarrage depuis la sauvegarde et procède aux ajustements en fonction de ce mode de démarrage. Ceci vous aide à restaurer un système sur une machine différente, même si cette machine utilise un autre mode de démarrage, puis remplace le disque dans la machine sauvegardée.
- **BIOS**

  L'agent qui s'exécute sur la machine cible procède aux ajustements nécessaires à l'utilisation de BIOS.
- **UEFI**

  L'agent qui s'exécute sur la machine cible procède aux ajustements nécessaires à l'utilisation d'UEFI.

Une fois qu'un paramètre sera modifié, la procédure de mappage de disque sera répétée. Cela peut prendre un certain temps.

Recommandations

Si vous devez transférer Windows entre UEFI et BIOS :

- Restaurez le disque à l'emplacement du volume système. Si vous restaurez uniquement le volume système au-dessus d'un volume existant, l'agent ne pourra pas initialiser correctement le disque de destination.
- N'oubliez pas que le BIOS ne permet pas l'utilisation de plus de 2 To d'espace disque.

Limites

- Le transfert entre UEFI et BIOS est compatible avec :
  - Les systèmes d'exploitation Windows 64 bits à partir de Windows 7
  - Les systèmes d'exploitation Windows Server 64 bits à partir de Windows Server 2008 SP1
- Le transfert entre UEFI et BIOS n'est pas pris en charge si la sauvegarde est stockée sur un lecteur de bandes.

Lorsque le transfert d'un système entre UEFI et BIOS n'est pas pris en charge, l'agent se comporte comme si le paramètre **Comme sur la machine sauvegardée** était choisi. Si la machine cible prend en charge à la fois UEFI et BIOS, vous devez activer manuellement le mode de démarrage correspondant à la machine d'origine. Sinon, le système ne démarrera pas.

Date et heure des fichiers

Cette option est effective uniquement lors de la restauration de fichiers.

Cette option définit si la date et l'heure des fichiers doivent être restaurées depuis la sauvegarde ou assignées selon les valeurs actuelles.

Si cette option est activée, les fichiers présenteront la date et l'heure actuelles.

Le préréglage est le suivant : **Activé**.

Gestion erreurs

Ces options vous permettent de spécifier comment traiter des erreurs qui peuvent se produire pendant la restauration.

Réessayer si une erreur se produit

Le préréglage est le suivant : **Activé. Nombre de tentatives : 30. Intervalle entre les tentatives : 30 secondes.**

Lorsqu'une erreur récupérable se produit, le programme essaie à nouveau d'effectuer l'opération qui a échoué. Vous pouvez définir l'intervalle de temps ainsi que le nombre de tentatives. Les tentatives s'arrêteront dès que l'opération réussira OU que le nombre de tentatives sera atteint, le premier de ces deux cas prévalant.

Ne pas afficher les messages et dialogues pendant le traitement (mode silencieux)

Le préréglage est le suivant : **Désactivé**.

Avec le mode silencieux activé, le programme gérera automatiquement les situations nécessitant une intervention de l'utilisateur dans la mesure du possible. Si une opération ne peut pas se poursuivre sans l'intervention de l'utilisateur, elle échouera. Les détails de l'opération, y compris les erreurs, le cas échéant, apparaissent dans le journal des opérations.

Enregistrer des informations système au cas où un redémarrage échouerait

Cette option est effective pour une restauration de disque ou volume sur une machine physique sous Windows ou Linux.

Le préréglage est le suivant : **Désactivé**.

Quand cette option est activée, vous pouvez indiquer un dossier sur le disque local (y compris des lecteurs flash ou des disques durs connectés à la machine cible) ou sur un partage réseau où seront enregistrés le journal, les informations système et les fichiers de vidage mémoire après plantage. Ce fichier aidera le personnel du support technique à identifier le problème.

Exclusions de fichiers

Cette option est effective uniquement lors de la restauration de fichiers.

Cette option définit les fichiers et dossiers à ignorer pendant le processus de restauration et à exclure ainsi de la liste des éléments restaurés.

Remarque
Les exclusions remplacent la sélection des éléments de données à restaurer. Par exemple, si vous sélectionnez cette option pour restaurer le fichier MonFichier.tmp en excluant tous les fichiers .tmp, le fichier MonFichier.tmp ne sera pas restauré.

Sécurité de niveau fichier

Cette option est effective lors de la restauration de fichiers sur disque et au niveau des fichiers pour des volumes formatés NTFS.

Cette option définit s'il faut restaurer les permissions NTFS pour les fichiers avec les fichiers eux-mêmes.

Le préréglage est le suivant : **Activé**.

Vous pouvez choisir de restaurer les permissions ou de laisser les fichiers hériter des permissions NTFS du dossier vers lequel ils sont restaurés.

Flashback

Cette option est efficace lors de la restauration des disques et volumes sur des machines physiques et virtuelles, excepté pour Mac.

Cette option fonctionne uniquement si la disposition du volume du disque en cours de restauration correspond exactement à celui du disque de destination.

Si l'option est activée, seules les différences entre les données de la sauvegarde et le disque de destination sont restaurées. Cela accélère la restauration des machines physiques et virtuelles. Les données sont comparées au niveau des blocs.

Lors de la restauration d'une machine physique, le préréglage est : **Désactivé**.

Lors de la restauration d'une machine virtuelle, le préréglage est : **Activé**.

Restauration de chemin d'accès complet

Cette option est effective seulement lors de la restauration de données d'une sauvegarde de niveau fichier.

Si cette option est activée, le chemin d'accès complet au fichier est recréé dans l'emplacement cible

Le préréglage est le suivant : **Désactivé**.

Points de montage

Cette option est efficace seulement sous Windows pour restaurer des données d'une sauvegarde de niveau fichier.

Activez cette option pour restaurer des fichiers et dossiers qui ont été stockés sur des volumes montés et qui ont été sauvegardés avec l'option Points de montage activée.

Le préréglage est le suivant : **Désactivé**.

Cette option est efficace seulement lorsque vous sélectionnez un dossier à restaurer qui est supérieur au point de montage dans l'arborescence des dossiers. Si vous sélectionnez des dossiers à restaurer qui sont dans le point de montage ou le point de montage lui-même, les éléments sélectionnés seront restaurés peu importe la valeur de l'option **Points de montage**.

Remarque
Veuillez être conscients que si le volume n'est pas monté au moment de la restauration, les données seront restaurées directement dans le dossier était le point de montage au moment de la sauvegarde.

Performance

Cette option définit la priorité du processus de restauration dans le système d'exploitation.

Les paramètres disponibles sont les suivants : **Basse**, **Normale**, **Élevé**.

Le préréglage est le suivant : **Normale**.

Le degré de priorité des processus exécutés dans un système détermine le niveau d'utilisation du processeur et la quantité de ressources système qui leur sont allouées. Réduire la priorité de restauration libérera davantage de ressources pour les autres applications. Augmenter la priorité de restauration pourrait accélérer le processus de restauration en imposant au système d'exploitation d'allouer plus de ressources à l'application qui effectuera la restauration Cependant, l'effet en résultant dépendra de l'utilisation globale du processeur ainsi que d'autres facteurs comme la vitesse d'E/S du disque ou le trafic réseau.

Commandes Pré/Post

L'option vous permet de définir les commandes à exécuter automatiquement avant et après la restauration des données.

Exemple de possibilités d'utilisation des commandes avant/après :

- Lancez la commande **Checkdisk** afin de détecter et réparer les erreurs de systèmes de fichiers logiques, les erreurs physiques ou les secteurs défectueux à démarrer avant le début de la restauration ou après la fin de la restauration.

Le programme ne prend pas en charge de commandes interactives, c'est à dire des commandes qui impliquent une saisie de l'utilisateur (par exemple, « pause »).

Une commande post-récupération ne sera pas exécutée si la récupération exécute un redémarrage.

Commande avant la restauration

Pour spécifier une commande / un fichier de traitement par lots à exécuter avant le début du processus de restauration

1. Activez le commutateur **Exécuter une commande avant la restauration**.
2. Dans le champ **Commande...**, saisissez une commande ou naviguez jusqu'à un fichier de traitement par lots. Le programme ne prend pas en charge de commandes interactives, c'est à dire des commandes qui impliquent une saisie de l'utilisateur (par exemple, « pause »).
3. Dans le champ **Répertoire de travail**, indiquez un chemin vers un répertoire où la commande/le fichier de traitement par lots sera exécuté.
4. Dans le champ **Arguments**, indiquez les arguments d'exécution de commande si nécessaire.
5. En fonction du résultat que vous voulez obtenir, sélectionnez les options appropriées comme décrit dans le tableau ci-dessous.
6. Cliquez sur **Valider**.

Case à cocher	**Sélection**			
Faire échouer la restauration si l'exécution de la commande échoue*	Sélectionné	Effacé	Sélectionné	Effacé
Ne pas récupérer tant que l'exécution de la commande n'est pas achevée	Sélectionné	Sélectionné	Effacé	Effacé
Résultat				
	Préréglage Effectuer la restauration uniquement si la commande a été exécutée avec succès. Faire échouer la restauration si l'exécution de la commande échoue.	Effectuer la sauvegarde après l'exécution de la commande, indépendamment de l'échec ou du succès de l'exécution.	Sans Objet	Effectuer la restauration en même temps que l'exécution de la commande et quel que soit le résultat de l'exécution de la commande.

* Une commande est considérée comme ayant échoué si son code de sortie n'est pas égal à zéro.

Commande après la restauration

Pour spécifier une commande / un fichier exécutable à exécuter une fois la restauration terminée

1. Activez le commutateur **Exécuter une commande après la restauration**.
2. Dans le champ **Commande...**, saisissez une commande ou naviguez jusqu'à un fichier de traitement par lots.
3. Dans le champ **Répertoire de travail**, indiquez un chemin vers un répertoire où la commande/le fichier de traitement par lots sera exécuté.
4. Dans le champ **Arguments**, spécifiez les arguments d'exécution de commande si nécessaire.
5. Sélectionnez la case à cocher **Faire échouer la restauration si l'exécution de la commande échoue** si la réussite de l'exécution de la commande est cruciale pour vous. La commande est considérée comme ayant échoué si son code de sortie n'est pas égal à zéro. Si l'exécution de la commande échoue, l'état de la restauration sera défini sur **Erreur**.

   Lorsque la case n'est pas cochée, le résultat d'exécution de commande n'a pas d'incidence sur l'échec ou la réussite de la restauration. Vous pouvez retrouver le résultat de l'exécution de la commande en explorant l'onglet **Activités**.
6. Cliquez sur **Valider**.

Remarque
Une commande post-récupération ne sera pas exécutée si la récupération exécute un redémarrage.

Modification de SID

Cette option est effective lors de la restauration de Windows 8.1/Windows Server 2012 R2 ou versions précédentes.

Cette option n'est pas effective lorsque la restauration vers une machine virtuelle est exécutée par l'agent pour VMware, l'agent pour Hyper-V, l'agent pour Scale Computing HC3 ou l'agent pour oVirt.

Le préréglage est le suivant : **Désactivé**.

Le logiciel peut générer un identificateur de sécurité unique (SID d'ordinateur) pour le système d'exploitation restauré. Vous avez uniquement besoin de cette option pour assurer le fonctionnement de logiciels tiers qui dépendent du SID d'ordinateur.

Microsoft ne prend pas officiellement en charge la modification de SID sur un système déployé ou restauré. Par conséquent, vous utilisez cette option à vos propres risques.

Gestion de l'alimentation des MV

Ces options sont effectives lorsque la restauration vers une machine virtuelle est exécutée par l'agent pour VMware, Hyper-V, Virtuozzo, Scale Computing HC3 ou oVirt.

Éteindre les machines virtuelles cibles lors du démarrage de la récupération

Le préréglage est le suivant : **Activé**.

Il n'est pas possible d'effectuer une restauration sur une machine virtuelle existante si la machine est en ligne ; la machine est donc éteinte automatiquement dès que la restauration démarre. Les utilisateurs seront déconnectés de la machine et toutes les données non enregistrées seront perdues.

Décochez la case correspondant à cette option si vous préférez éteindre les machines virtuelles manuellement avant la restauration.

Démarrer la machine virtuelle cible lorsque la récupération est complétée

Le préréglage est le suivant : **Désactivé**.

Après qu'une machine ait été restaurée à partir d'une sauvegarde sur une autre machine, il est possible que la réplique de la machine existante apparaisse sur le réseau. Par prudence, allumez manuellement la machine virtuelle restaurée, après avoir pris les précautions nécessaires.

Journal des événements Windows

Cette option est effective uniquement dans les systèmes d'exploitation Windows.

Cette option définit si les agents doivent consigner des événements des opérations de restauration dans journal des événements d'applications Windows (pour voir ce journal, exécutez eventvwr.exe ou sélectionnez **Panneau de configuration** > **Outils administratifs** > **Affichage des événements**). Vous pouvez filtrer les événements à consigner.

Le préréglage est le suivant : **Désactivé**.

Opérations avec des sauvegardes

L'onglet Stockage de sauvegarde

L'onglet **Stockage de sauvegarde** offre un accès à toutes les sauvegardes, notamment à celles d'ordinateurs hors ligne et d'ordinateurs qui ne sont plus enregistrés dans le service Cyber Protection, aux sauvegardes vers des clouds publics tels que Microsoft Azure et aux sauvegardes orphelines[1].

Les sauvegardes créées via `acrocmd` sont marquées comme orphelines. Les sauvegardes créées dans la version 12.5 de la solution sont également identifiées comme orphelines.

Remarque
Veuillez noter que les sauvegardes orphelines sont également facturées.

[1] Une sauvegarde orpheline est une sauvegarde qui n'est plus associée à un plan de protection.

Les sauvegardes stockées à un emplacement partagé (tel que partage SMB ou NFS) sont visibles de tous les utilisateurs bénéficiant d'un accès en lecture à l'emplacement en question.

Dans Windows, les fichiers de sauvegarde héritent des permissions d'accès de leur dossier parent. Par conséquent, nous vous recommandons de restreindre les permissions de lecture pour ce dossier.

Concernant le stockage dans le Cloud, les utilisateurs ont uniquement accès à leurs propres sauvegardes.

Un administrateur peut afficher les sauvegardes sur le Cloud pour tout compte appartenant à l'unité ou à la société donnée et à ses groupes enfants, en sélectionnant le stockage dans le Cloud du compte. Pour sélectionner le terminal que vous souhaitez utiliser pour obtenir les données depuis le Cloud, cliquez sur **Changer** sur la ligne **Machine à parcourir**. L'onglet **Stockage de sauvegarde** affiche les sauvegardes de l'ensemble des machines enregistrées dans le compte sélectionné.

Les sauvegardes créées par l'agent *Cloud* pour Microsoft 365 et les sauvegardes des données Google Workspace n'apparaissent pas dans l'emplacement de **Stockage dans le Cloud**, mais dans une section séparée appelée **Sauvegardes d'applications Cloud**.

Les emplacements de sauvegarde utilisés dans les plans de protection sont automatiquement ajoutés à l'onglet **Stockage de sauvegarde**. Pour ajouter un dossier personnalisé (par exemple, un périphérique USB amovible) à la liste des emplacements de sauvegarde, cliquez sur **Parcourir** et indiquez le chemin d'accès au dossier.

Si vous avez ajouté ou supprimé des sauvegardes à l'aide d'un gestionnaire de fichiers, cliquez sur l'icône en forme d'engrenage à côté du nom de l'emplacement, puis cliquez sur **Actualiser**.

Avertissement !
Ne tentez pas de modifier manuellement les fichiers de sauvegarde, car cela pourrait altérer les fichiers et rendre les sauvegardes inutilisables. Nous vous recommandons également d'utiliser la réplication de sauvegarde plutôt que de déplacer manuellement des fichiers de sauvegarde.

Un emplacement de sauvegarde (sauf pour le stockage dans le Cloud) disparaît de l'onglet **Stockage de sauvegarde** si toutes les machines qui ont été sauvegardées dans l'emplacement à un moment ou à un autre ont été supprimées du service Cyber Protection. Cela garantit que vous n'avez pas à payer pour les sauvegardes stockées dans cet emplacement. Dès qu'un élément est sauvegardé vers cet emplacement, ce dernier est de nouveau ajouté en même temps que toutes les sauvegardes qui y sont stockées.

Dans l'onglet **Stockage de sauvegarde**, vous pouvez filtrer les sauvegardes de la liste selon les critères suivants :

- **Uniquement avec les données d'investigation** : seules les sauvegardes qui possèdent des données d'investigation s'afficheront.

- **Effectuer une pré-mise à jour uniquement pour les sauvegardes créées par la gestion des correctifs** : uniquement les sauvegardes qui ont été créées lors de la gestion des correctifs avant l'installation des correctifs s'afficheront.

Pour sélectionner un point de reprise à l'aide de l'onglet Stockage de sauvegarde

1. Dans l'onglet **Stockage de sauvegarde**, sélectionnez l'emplacement de stockage des sauvegardes.
   Le logiciel présente toutes les sauvegardes que votre compte est autorisé à afficher dans l'emplacement sélectionné. Les sauvegardes sont placées dans des groupes. Les noms des groupes reposent sur l'exemple suivant :
   `<nom de machine> - <nom de plan de protection>`
2. Sélectionnez le groupe à partir duquel vous voulez restaurer les données.
3. [Facultatif] Cliquez sur **Modifier** en regard de **Machine à parcourir**, puis sélectionnez une autre machine. Certaines sauvegardes ne peuvent être explorées que par des agents spécifiques. Par exemple, vous devez sélectionner une machine exécutant l'agent pour SQL afin de parcourir les sauvegardes de bases de données Microsoft SQL Server.

   Important
   Notez que **Machine à parcourir** est une destination par défaut pour la restauration depuis une sauvegarde de machine physique. Après avoir sélectionné un point de récupération et cliqué sur **Restaurer**, vérifiez le paramètre **Machine cible** afin de vous assurer qu'il s'agit bien de la machine vers laquelle vous souhaitez effectuer une restauration. Pour modifier la destination de restauration, spécifiez une autre machine dans **Machine à parcourir**.

4. Cliquez sur **Afficher les sauvegardes**.
5. Sélectionnez le point de restauration.

Pour ajouter un emplacement pour une sauvegarde

Remarque
Cette opération est disponible uniquement si vous avez un agent en ligne.

Dans l'onglet **Stockage de sauvegarde**, cliquez sur **Ajouter un emplacement**.

Sélectionnez un emplacement dans l'un des types d'emplacements suivants, puis cliquez sur **Terminé** :

- Dossier local
- Dossier réseau
- Secure Zone
- Dossier NFS
- Cloud public

Montage de volumes à partir d'une sauvegarde

Monter des volumes à partir d'une sauvegarde de niveau disque vous permet d'accéder aux volumes comme s'il s'agissait de disques physiques.

Monter des volumes en mode lecture/écriture vous permet de modifier le contenu de la sauvegarde, c'est-à-dire enregistrer, déplacer, créer, supprimer des fichiers ou des dossiers, et lancer des fichiers exécutables consistant d'un seul fichier. Dans ce mode, le logiciel crée une sauvegarde incrémentielle contenant les modifications apportées au contenu de la sauvegarde. Veuillez noter qu'aucune des sauvegardes suivantes ne comprendra ces modifications.

Configuration requise

- Cette fonctionnalité est uniquement disponible sous Windows à l'aide de l'Explorateur de fichiers.
- L'agent pour Windows doit être installé sur la machine qui effectue l'opération de montage.
- Le système de fichiers de la sauvegarde doit être pris en charge par la version de Windows sous laquelle fonctionne la machine.
- La sauvegarde doit être stockée dans un dossier local, sur un partage réseau (SMB/CIFS) ou dans Secure Zone.

Scénarios d'utilisation

- Partage de données

  Les volumes montés peuvent facilement être partagés sur le réseau.
- Solution « sparadrap » de restauration de bases de données

  Montez un volume qui contient une base de données SQL d'une machine récemment tombée en panne. Cela donnera accès à la base de données jusqu'à ce que la machine qui a planté soit récupérée. Cette approche peut également être utilisée pour la restauration granulaire de données Microsoft SharePoint à l'aide de l'Explorateur SharePoint.
- Nettoyage des virus hors ligne

  Si une machine est infectée, montez sa sauvegarde, nettoyez-la avec un logiciel antivirus (ou retrouvez la dernière sauvegarde qui n'est pas infectée), puis restaurez la machine à partir de cette sauvegarde.
- Vérification des erreurs

  L'échec d'une restauration avec redimensionnement du volume peut provenir d'une erreur dans le système de fichiers de la sauvegarde. Montez la sauvegarde en mode lecture/écriture. Vérifiez ensuite le volume monté en utilisant la commande `chkdsk /r`. Une fois que les erreurs sont corrigées et qu'une nouvelle sauvegarde incrémentielle est créée, restaurez le système à partir de cette sauvegarde.

Pour monter un volume à partir d'une sauvegarde

1. Accédez à l'emplacement de la sauvegarde à l'aide de l'Explorateur de fichiers.
2. Double-cliquez sur le fichier de sauvegarde. Les noms des fichiers reposent sur l'exemple suivant :

   `<nom de machine> - <GUID du plan de protection>`
3. Si la sauvegarde est chiffrée, saisissez le mot de passe de chiffrement. Sinon, ignorez cette étape.

   L'Explorateur de fichiers affiche les points de restauration.
4. Double-cliquez sur le point de restauration.

   L'Explorateur de fichiers affiche les volumes sauvegardés.

   Remarque
   Double-cliquez sur un volume pour parcourir son contenu. Vous pouvez copier des fichiers et des dossiers à partir de la sauvegarde vers n'importe quel dossier du système de fichiers.
5. Effectuez un clic droit sur un volume pour le monter, puis cliquez sur une des options suivantes :
   a. **Monter**

      Remarque
      Seule la dernière sauvegarde de l'archive (chaîne de sauvegarde) peut être montée en mode lecture/écriture.

   b. **Monter en mode lecture seule**.
6. Si la sauvegarde est stockée sur un partage réseau, fournissez les informations d'identification. Sinon, ignorez cette étape.

   Le logiciel monte le volume sélectionné. La première lettre non utilisée est attribuée au volume.

Démontage d'un volume

1. Accédez à **Ordinateur** (**Ce PC** sous Windows 8.1 et versions ultérieures) à l'aide de l'Explorateur de fichiers.
2. Effectuez un clic droit sur le volume monté.
3. Cliquez sur **Démonter**.
4. [Facultatif] Si le volume était monté en mode lecture/écriture et que son contenu a été modifié, indiquez si vous souhaitez créer une sauvegarde incrémentielle avec les modifications. Sinon, ignorez cette étape.

Le logiciel démonte le volume sélectionné.

Validation des sauvegardes

En validant une sauvegarde, vous vérifiez que vous pouvez en restaurer les données. Pour en savoir plus sur cette opération, reportez-vous à "Validation" (p. 208).

Remarque
Cette fonctionnalité est disponible pour les tenants clients pour lesquels le quota **Advanced Backup - Serveurs** ou **Advanced Backup - NAS** est activé dans le cadre du pack Advanced Backup.

Pour valider une sauvegarde

1. Sélectionnez la ressource sauvegardée.
2. Cliquez sur **Restauration**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

   Si la ressource est hors ligne, les points de récupération ne s'affichent pas. Effectuez l'une des actions suivantes :
   - Si la sauvegarde est située sur le cloud ou à un emplacement de stockage partagé (c.-à-d. que d'autres agents peuvent y accéder), cliquez sur **Sélectionner la machine**, sélectionnez une ressource cible qui est en ligne, puis choisissez un point de récupération.
   - Sélectionnez un point de récupération dans l'onglet Stockage de sauvegarde. Pour en savoir plus sur ce type de sauvegarde, reportez-vous à "L'onglet Stockage de sauvegarde" (p. 552).
4. Cliquez sur l'icône en forme d'engrenage, puis sur **Valider**.
5. Sélectionnez l'agent qui exécutera la validation.
6. Sélectionnez la méthode de validation.
7. Si la sauvegarde est chiffrée, saisissez le mot de passe de chiffrement.
8. Cliquez sur **Démarrer**.

Exportation de sauvegardes

L'opération d'exportation crée une copie auto-suffisante d'une sauvegarde à l'emplacement spécifié par vos soins. La sauvegarde originale demeure intacte. L'exportation de sauvegardes vous permet de séparer une sauvegarde spécifique d'une chaîne de sauvegardes incrémentielles et différentielles pour une restauration rapide, une écriture sur support amovible ou détachable, ou pour d'autres raisons.

Remarque
Cette fonctionnalité est disponible pour les tenants clients pour lesquels le quota **Advanced Backup - Serveurs** ou **Advanced Backup - NAS** est activé dans le cadre du pack Advanced Backup.

Le résultat d'une opération d'exportation est toujours une sauvegarde complète. If vous souhaitez répliquer toute la chaîne de sauvegarde vers un autre emplacement et préserver de multiples points de récupération, utilisez un plan de réplication de sauvegarde. Pour en savoir plus sur ce plan, reportez-vous à "Réplication de sauvegarde" (p. 205).

Le nom du fichier de sauvegarde de la sauvegarde exportée est identique à celui de la sauvegarde d'origine, à l'exception du numéro séquentiel. Si de multiples sauvegardes issues de la même chaîne de sauvegarde sont exportées vers le même emplacement, un numéro de séquence à quatre chiffres est attaché aux noms de fichier de toutes les sauvegardes, sauf au premier.

La sauvegarde exportée hérite des paramètres de chiffrement et du mot de passe de la sauvegarde originale. Vous devez indiquer le mot de passe lorsque vous exportez une sauvegarde chiffrée.

Pour exporter une sauvegarde

1. Sélectionnez la ressource sauvegardée.
2. Cliquez sur **Restauration**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.
   Si la ressource est hors ligne, les points de récupération ne s'affichent pas. Effectuez l'une des actions suivantes :
   - Si la sauvegarde est située sur le cloud ou à un emplacement de stockage partagé (c.-à-d. que d'autres agents peuvent y accéder), cliquez sur **Sélectionner la machine**, sélectionnez une ressource cible qui est en ligne, puis choisissez un point de récupération.
   - Sélectionnez un point de récupération dans l'onglet Stockage de sauvegarde. Pour en savoir plus sur ce type de sauvegarde, reportez-vous à "L'onglet Stockage de sauvegarde" (p. 552).
4. Cliquez sur l'icône en forme d'engrenage, puis sur **Exporter**.
5. Sélectionnez l'agent qui exécutera l'exportation.
6. Si la sauvegarde est chiffrée, saisissez le mot de passe de chiffrement. Sinon, ignorez cette étape.
7. Spécifiez la destination de l'exportation.
8. Cliquez sur **Démarrer**.

Suppression de sauvegardes

Une archive de sauvegarde contient une ou plusieurs sauvegardes. Vous pouvez supprimer des sauvegardes spécifiques (points de restauration) dans une archive ou toute l'archive.

La suppression de l'archive de sauvegarde supprime toutes les sauvegardes qu'elle contient. La suppression de toutes les sauvegardes d'une ressource supprime les archives de sauvegarde qui contiennent ces sauvegardes.

Vous pouvez supprimer des sauvegardes en utilisant la console Cyber Protect, dans les onglets **Terminaux** et **Stockage des sauvegardes**. Vous pouvez également supprimer des sauvegardes du stockage dans le cloud à l'aide de la console Web Restore.

Avertissement !
Si le stockage immuable est désactivé, les données sauvegardées sont définitivement supprimées et ne peuvent pas être récupérées.

Pour supprimer des sauvegardes ou des archives de sauvegarde

Dans l'onglet Terminaux

Cette procédure ne s'applique qu'aux ressources en ligne.

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez les sauvegardes de ressources que vous souhaitez supprimer.
3. Cliquez sur **Restauration**.
4. [Si plusieurs emplacements de sauvegarde sont disponibles] Sélectionnez l'emplacement de sauvegarde.
5. [Pour supprimer toutes les sauvegardes de ressources] Cliquez sur **Supprimer tout**.
   La suppression de toutes les sauvegardes supprime également les archives de sauvegarde qui contiennent ces sauvegardes.
6. [Pour supprimer une sauvegarde spécifique] Sélectionnez la sauvegarde (point de restauration) que vous souhaitez supprimer, puis cliquez sur **Actions** > **Supprimer**.
7. [Lors de la suppression de toutes les sauvegardes] Cochez la case, puis cliquez sur **Supprimer** pour confirmer votre décision.
8. [Lors de la suppression d'une sauvegarde spécifique] Cliquez sur **Supprimer** pour confirmer votre décision.

Dans l'onglet Stockage de sauvegarde

Cette procédure s'applique aux ressources en ligne et hors ligne.

1. Sur la console Cyber Protect, accédez à **Stockage de sauvegarde**.
2. Sélectionnez l'emplacement à partir duquel vous souhaitez supprimer les sauvegardes.
3. Sélectionnez l'archive de sauvegarde à partir de laquelle vous souhaitez supprimer les sauvegardes.
   Le nom de l'archive utilise le modèle suivant :
   - Archives de sauvegarde non-cloud à cloud : <nom de la ressource> - <nom du plan de protection>
   - Archives de sauvegarde cloud à cloud : <nom de l'utilisateur> ou <nom du disque> ou <nom de l'équipe> - <service cloud> - <nom du plan de protection>
4. [Pour supprimer l'ensemble de l'archive de sauvegardes] Cliquez sur **Supprimer**.
   La suppression d'une archive de sauvegardes supprime toutes les sauvegardes de cette archive.
5. [Pour supprimer une sauvegarde spécifique dans l'archive de sauvegardes] Cliquez sur **Afficher les sauvegardes**.
   a. Sélectionnez la sauvegarde (point de restauration) que vous souhaitez supprimer.
   b. Cliquez sur **Actions** > **Supprimer**.
6. [Lors de la suppression d'une archive de sauvegardes] Cochez la case, puis cliquez sur **Supprimer** pour confirmer votre décision.
7. [Lors de la suppression d'une sauvegarde spécifique] Cliquez sur **Supprimer** pour confirmer votre décision.

Dans la console Web Restore

Cette procédure s'applique uniquement aux archives de sauvegardes dans le stockage dans le cloud.

1. Dans la console Cyber Protection, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez les sauvegardes de ressource que vous souhaitez supprimer, puis cliquez sur **Restauration**.
3. [Si plusieurs emplacements de sauvegarde sont disponibles] Sélectionnez l'emplacement de sauvegarde, puis cliquez sur **Autres méthodes de restauration**.
4. Cliquez sur **Télécharger les fichiers**.

   Vous êtes redirigé vers la console Web Restore.
5. Dans la console Web Restore, sous **Ordinateurs**, cliquez sur le nom de la ressource.
6. Sous **Dernière version**, cliquez sur la date, puis sur **Supprimer**.

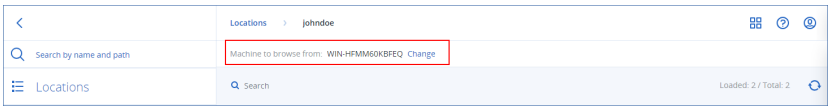
   Cette action n'est disponible qu'au niveau de l'archive de sauvegardes. Vous ne pouvez pas explorer l'archive et supprimer des sauvegardes spécifiques.
7. Cliquez sur **Supprimer** pour confirmer votre décision.

Suppression des sauvegardes en dehors de la console Cyber Protect

Nous vous recommandons de supprimer les sauvegardes à l'aide de la console Cyber Protect. Si vous supprimez des sauvegardes du stockage dans le cloud à l'aide de la console Web Restore ou si vous supprimez des sauvegardes locales à l'aide d'un gestionnaire de fichiers, vous devez actualiser l'emplacement de la sauvegarde pour synchroniser les modifications avec la console Cyber Protect.

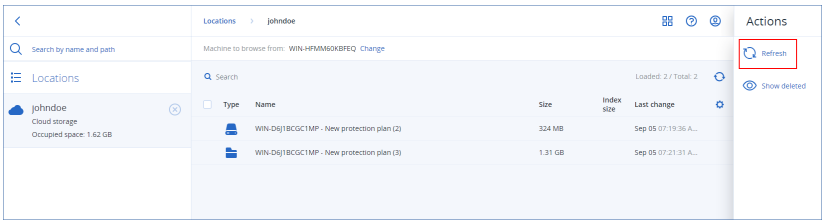
Prérequis

- Un agent en ligne qui peut accéder à l'emplacement de la sauvegarde doit être sélectionné comme **Machine à parcourir** dans la console Cyber Protect.



Pour actualiser un emplacement de sauvegarde

1. Sur la console Cyber Protect, accédez à **Stockage de sauvegarde**.
2. Sélectionnez l'emplacement de sauvegarde dans lequel les sauvegardes supprimées ont été stockées.
3. Dans le volet **Actions**, cliquez sur **Actualiser**.



Compréhension de la détection des goulots d'étranglement

La fonctionnalité de détection de goulots d'étranglement vous permet d'identifier l'endroit où vous pouvez améliorer les performances, car elle met en évidence le composant de votre système qui a été le plus lent pendant une sauvegarde ou une restauration.

Étant donné que les goulots d'étranglement se produisent *toujours* pendant un événement de transmission, ils ne doivent pas nécessairement être résolus. Vos sauvegardes sont peut-être déjà suffisamment rapides, s'intègrent déjà parfaitement dans vos créneaux de sauvegarde et sont conformes à vos accords de niveau de service (SLA) : il n'y a donc généralement pas de problème particulier à résoudre.

Vous pouvez afficher et suivre facilement les goulots d'étranglement dans l'onglet **Détails de l'activité**. Pour ce faire, accédez depuis la console Cyber Protect à **Surveillance > Activités**, puis cliquez sur l'activité pertinente. Pour plus d'informations sur l'affichage des goulots d'étranglement, voir "Affichage des détails d'un goulot d'étranglement" (p. 562) et "Sur quels agents, ressources et emplacements de sauvegarde les goulots d'étranglement sont-ils affichés ?" (p. 564).

Qu'est-ce qu'un goulot d'étranglement ?

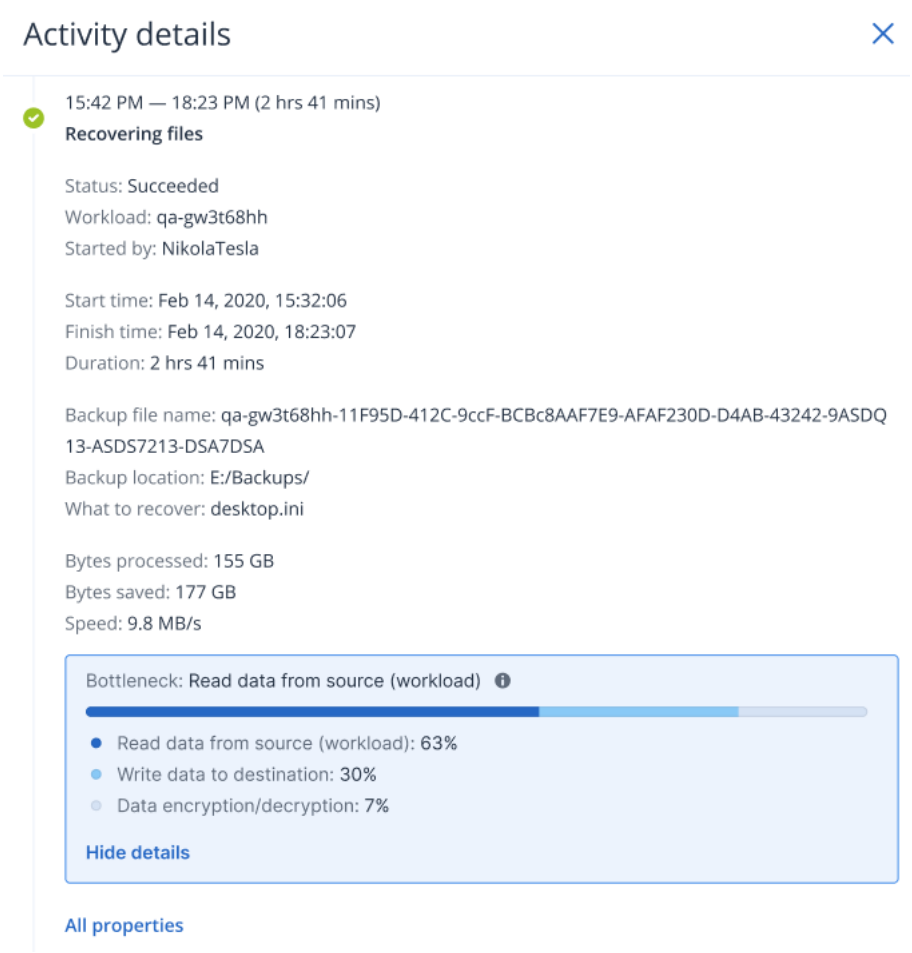
Les goulots d'étranglement sont généralement provoqués par la lenteur d'un composant de la chaîne de traitement, ce qui implique que d'autres composants attendent ce composant.

La fonctionnalité de détection des goulots d'étranglement vous permet de suivre des composants présentant des lenteurs pendant la sauvegarde et la restauration, et d'identifier parmi les types de composants suivants ceux qui sont les plus lents :

- **Source** : En un coup d'œil, vous pouvez déterminer si la vitesse de lecture à partir de la source de sauvegarde/restauration provoque un goulot d'étranglement.
- **Destination** : Compréhension des incidences sur les performances de la vitesse d'écriture sur la destination de sauvegarde/restauration.
- **Agent** : Examen de la vitesse de traitement des données par l'agent et détermination si elle est suffisante.

Le type de goulot d'étranglement, qu'il provienne de la source, de la destination ou de l'agent, peut évoluer selon les heures pendant la sauvegarde/restauration. Les pourcentages indiqués dans la section **Goulot d'étranglement** de l'onglet **Détails de l'activité** ci-dessous (par exemple, **Lire les données à partir de la source (ressource) : 63 %**) représentent le pourcentage de durée en cas de détection de ce type de goulot d'étranglement. Dans ce cas, pendant 63 % du temps d'activité de la restauration, le type de goulot d'étranglement concernait la lenteur de lecture des données depuis l'archive de sauvegarde par l'agent.

De la même manière, pendant 30 % du temps, le goulot d'étranglement était lié à la lenteur d'écriture des données dans la destination de la restauration (**Écrire les données sur la destination : 30 %**).



Remarque
Les statistiques sur le goulot d'étranglement sont disponibles dans l'onglet **Détails de l'activité**. Ces statistiques sont disponibles uniquement pour les tâches de plus d'une minute.

Comment réduire les goulots d'étranglement ?

Comme indiqué ci-dessus, la fonctionnalité de détection des goulots d'étranglement met en évidence le flux de données *en lecture* et *en écriture* entre les composants de sauvegarde. Les statistiques de *lecture* font référence au flux de données depuis la source de données vers l'agent qui effectue la sauvegarde/restauration. Quant aux statistiques d'*écriture*, elles font référence au flux de données entre l'agent et l'archive de sauvegarde (la destination).

Pour réduire les goulots d'étranglement et améliorer les performances des flux de données en lecture/écriture, vous devez analyser le canal entre l'agent et la source de données/l'archive de sauvegarde. Par exemple, vous pouvez essayer de réaliser un banc d'essai de vos disques durs si l'agent sauvegarde des fichiers locaux.

Affichage des détails d'un goulot d'étranglement

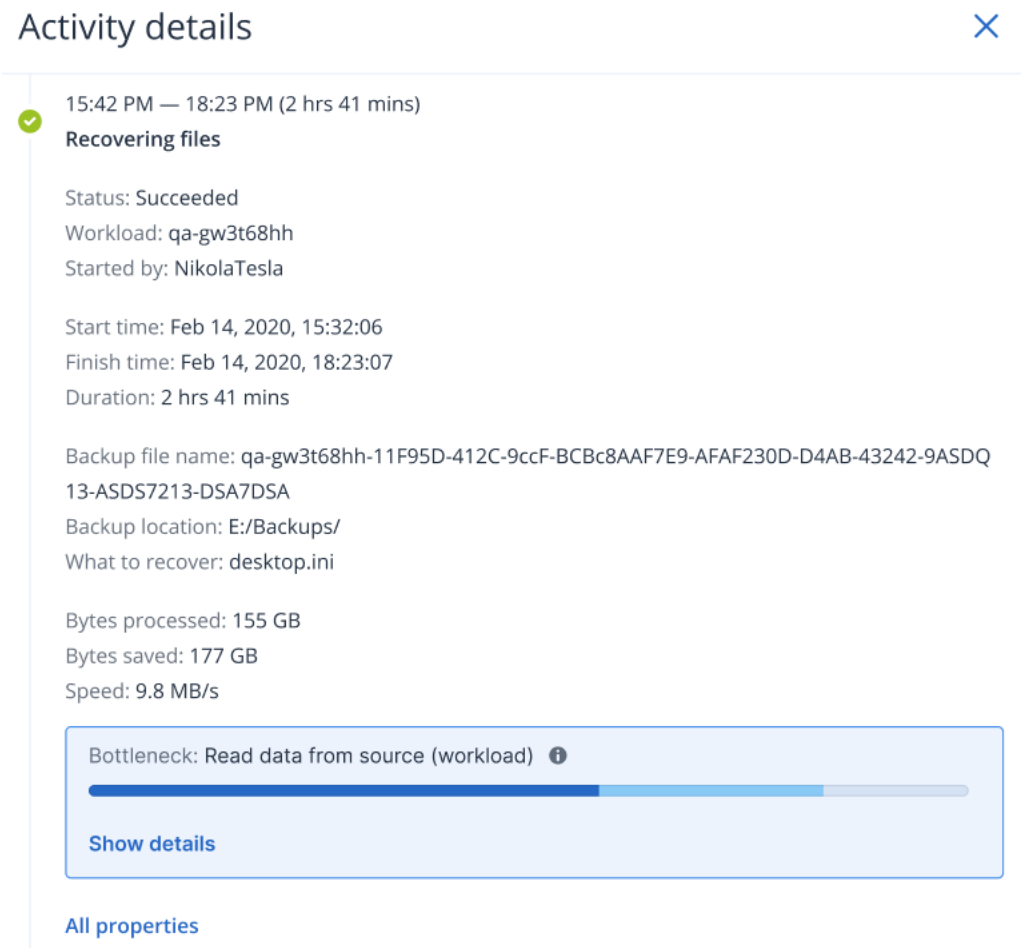
Vous pouvez visualiser les goulots d'étranglement détectés pour tout type de sauvegarde, réplication de sauvegarde ou restauration (vers un autre type de dossier ou d'emplacement de

destination), y compris les sauvegardes de machine virtuelle, d'ordinateur et de fichiers/dossiers. Vous pouvez également afficher les goulots d'étranglement des réplications et restaurations automatiques de machines virtuelles.

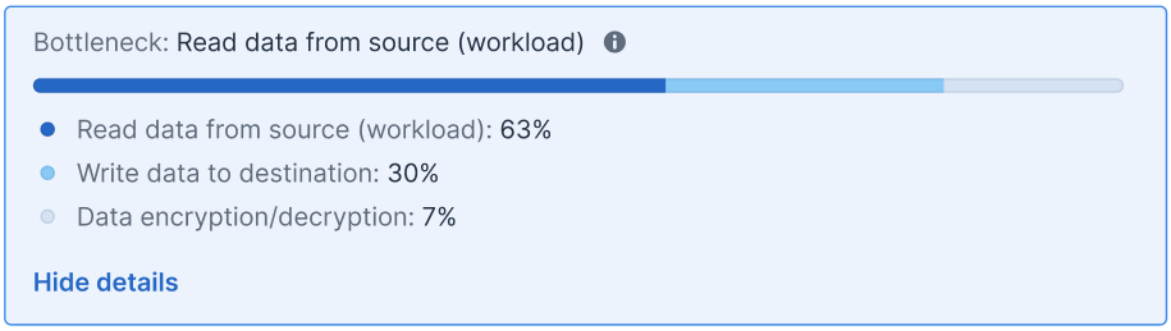
Pour plus d'informations sur la définition et les concepts essentiels des types de goulots d'étranglement, voir "Compréhension de la détection des goulots d'étranglement" (p. 561).

Pour afficher les détails d'un goulot d'étranglement

1. Dans la console Cyber Protect, accédez à **Surveillance > Activités**.
2. Cliquez sur l'activité pertinente.
   Dans l'onglet **Détails de l'activité**, la section **Goulot d'étranglement** apparaît en bleu.



3. Cliquez sur **Afficher les détails** pour afficher le goulot d'étranglement rencontré le plus fréquemment pendant la sauvegarde/restauration.
   La section **Goulot d'étranglement** se développe pour afficher la synthèse des types de goulot d'étranglement pertinents.



Dans l'exemple ci-dessus, le goulot d'étranglement qui représentait 63 % de la durée totale de l'opération a été provoqué par l'opération de *lecture* (effectuée par l'agent).

Remarque
Les valeurs de goulot d'étranglement se mettent à jour dynamiquement toutes les minutes pendant l'exécution de l'activité correspondante.

Sur quels agents, ressources et emplacements de sauvegarde les goulots d'étranglement sont-ils affichés ?

La détection des goulots d'étranglement est disponible pour les types suivants de ressources, agents et emplacements de sauvegarde :

- Sauvegardes de disque/d'image effectuées par :
  - Agent pour Azure
  - Agent pour Windows
  - Agent pour Linux
  - Agent pour Mac
  - Agent pour VMware (appliance virtuelle et Windows, y compris la réplication et la restauration automatique de VM à partir d'un réplica (activités de restauration à partir de réplicas))
  - Agent pour Hyper-V
  - Agent pour Scale Computing
  - Agent pour oVirt (KVM)
  - Plate-forme d'infrastructure de l'agent pour Virtuozzo
  - Agent pour Virtuozzo
  - Agent pour VMware Cloud Director (vCD-BA)
- Sauvegardes de niveau fichier
  - Agent pour Windows
  - Agent pour Linux
  - Agent pour Mac

- Sauvegardes de niveau application
  - Agent pour SQL
  - Agent pour Exchange
  - Agent pour MySQL/MariaDB
  - Agent pour Oracle
  - Agent pour SAP HANA
- Emplacements de sauvegardes
  - Acronis Cloud storage (y compris le stockage hébergé partenaire)
  - Stockage dans le cloud public
  - Partages réseau (SMB + NFS)
  - Dossiers locaux
  - Emplacements définis par script
  - Acronis Secure Zone

Sauvegarde de ressources dans des clouds publics

Remarque
Cette fonctionnalité fait partie du pack Advanced Backup, qui fait à son tour partie du service de Cyber Protection. Notez que, lorsque vous ajoutez cette fonctionnalité à un plan de protection, vous êtes susceptible de devoir vous acquitter de frais supplémentaires.

Vous pouvez sélectionner des services de cloud public tels que Microsoft Azure et Amazon S3 en tant que destinations de sauvegarde dans la console Cyber Protect.

Pour configurer des emplacements de sauvegarde dans Wasabi, vous devez être administrateur d'entreprise ou d'unité, ou disposer de l'un des rôles suivants définis dans le service de cyberprotection : cyberadministrateur, administrateur, utilisateur.

Définition d'un emplacement de sauvegarde dans Microsoft Azure

Remarque
Pour configurer les emplacements de sauvegarde dans Microsoft Azure, vous devez avoir l'un des rôles suivants définis dans le service de cyberprotection : administrateur d'entreprise, utilisateur, cyberadministrateur.

Pour sauvegarder une ressource dans Microsoft Azure, vous devez définir l'emplacement de sauvegarde Microsoft Azure dans la console Cyber Protect, puis vous connecter à l'abonnement Microsoft Azure pertinent. Cette opération peut être effectuée selon les méthodes suivantes :

- Lors de la création ou de la modification d'un plan de protection.
- Lors de la définition et de la gestion d'emplacements de stockage des sauvegardes.

Important
Les administrateurs et les utilisateurs non-administrateurs peuvent sauvegarder les ressources dans Microsoft Azure.

Les utilisateurs non-administrateurs peuvent ajouter l'accès à un abonnement Microsoft Azure (voir "Gestion de l'accès aux abonnements Microsoft Azure" (p. 577)), mais peuvent appliquer des plans de protection uniquement lorsque l'emplacement de sauvegarde est connecté à l'abonnement Microsoft Azure qu'ils ont eux-mêmes ajouté et pour la ressource enregistrée dans la console Cyber Protect sous leur nom.

Les administrateurs peuvent appliquer des plans de protection lorsque l'emplacement de sauvegarde est connecté aux abonnements Microsoft Azure qu'ils ont eux-mêmes ajoutés ou aux abonnements ajoutés par un autre administrateur, et pour les ressources enregistrées dans la console Cyber Protect sous le nom d'un utilisateur.

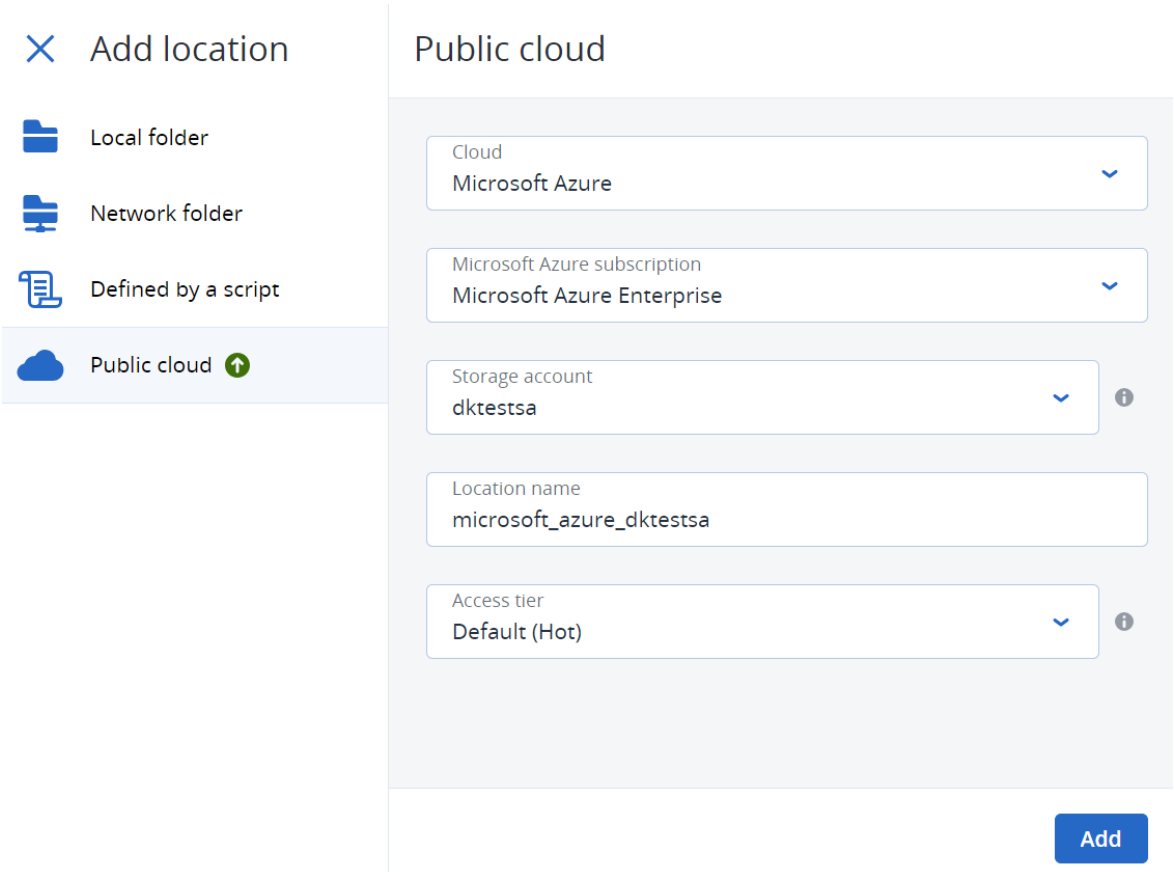
Pour définir un emplacement de sauvegarde dans Microsoft Azure

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - Si vous créez ou modifiez un plan de protection, accédez à **Terminaux** et sélectionnez la ressource que vous souhaitez sauvegarder dans Microsoft Azure. Dans la section **Sauvegarde** du plan de protection de la ressource sélectionnée, cliquez sur le lien dans la ligne **Où sauvegarder**.
     Pour plus d'informations sur l'utilisation des plans de protection, reportez-vous à "Plans et modules de protection" (p. 222).
   - S vous gérez vos emplacements de stockage des sauvegardes et souhaitez ajouter Microsoft Azure en tant que nouvel emplacement, accédez à **Stockage de sauvegarde**.
     Pour plus d'informations sur la gestion de vos emplacements de stockage des sauvegardes, reportez-vous à "L'onglet Stockage de sauvegarde" (p. 552).
2. Cliquez sur **Ajouter un emplacement**.
3. Dans la liste déroulante **Clouds publics**, sélectionnez **Microsoft Azure**.
4. Si l'abonnement Microsoft Azure pertinent est déjà enregistré dans la console Cyber Protect, sélectionnez-le dans la liste des abonnements.
   Si l'abonnement pertinent n'est pas enregistré dans la console Cyber Protect, cliquez sur **Ajouter** cliquez sur **Connexion** dans la boîte de dialogue qui s'affiche. Vous êtes redirigé vers la page de connexion Microsoft. Pour plus d'informations sur l'ajout et la définition de l'accès à un abonnement Microsoft Azure, voir "Ajout de l'accès à un abonnement Microsoft Azure" (p. 578).
5. Dans le champ **Compte de stockage**, sélectionnez le compte souhaité.

Remarque
Seuls les comptes de stockage Microsoft Azure avec suffixes de terminaux classiques contenant `core.windows.net` sont pris en charge actuellement. Par ailleurs, le compte de stockage sélectionné doit être de type StorageV2.

Par défaut, les champs **Nom de l'emplacement** et **Niveau d'accès** sont renseignés automatiquement en fonction du compte de stockage sélectionné. Le nom de l'emplacement affiché est `microsoft_azure_[compte de stockage]` et le niveau d'accès sélectionné est **Par défaut (chaud)**. Les deux champs peuvent être modifiés si nécessaire.

Remarque
Lorsque vous changez le nom de l'emplacement, saisissez un nom d'emplacement unique (ce nom doit être unique pour le tenant client). Si le nom que vous ajoutez existe déjà dans le compte de stockage, Acronis lui ajoute un numéro en suffixe. Par exemple, si le nom **Stockage Microsoft Azure** existe déjà, le nom est automatiquement mis à jour en **Stockage Microsoft Azure_01**.



6. Cliquez sur **Ajouter**.
   Si vous créez ou modifiez un plan de protection, l'emplacement de sauvegarde Microsoft Azure est défini comme étant l'emplacement sur la ligne **Où sauvegarder**. Lors de l'exécution de la

sauvegarde (manuelle ou en fonction d'une planification), la sauvegarde est enregistrée dans l'emplacement défini.

Si vous gérez vos emplacements de stockage de sauvegarde, vous pouvez afficher et mettre à jour les détails de l'emplacement si nécessaire. L'emplacement Microsoft Azure est également disponible lors de la définition d'un emplacement de sauvegarde pour les ressources. Pour plus d'informations, voir "Affichage et mise à jour des emplacements de sauvegarde dans le cloud public" (p. 572).

Définir un emplacement de sauvegarde dans Amazon S3

Remarque
Pour configurer les emplacements de sauvegarde dans Amazon S3, vous devez avoir l'un des rôles suivants définis dans le service de cyberprotection : administrateur d'entreprise, utilisateur, cyberadministrateur.

Pour sauvegarder une ressource dans Amazon S3, vous devez définir l'emplacement de sauvegarde Amazon S3 dans la console Cyber Protect, puis vous connecter à la connexion Amazon S3 correspondante. Vous pouvez procéder de la manière suivante :

- Lors de la création ou de la modification d'un plan de protection.
- Lors de la définition et de la gestion d'emplacements de stockage des sauvegardes.

Important
Les administrateurs et les utilisateurs non-administrateurs peuvent sauvegarder des ressources dans Amazon S3.

Les utilisateurs non-administrateurs peuvent ajouter un accès à une connexion Amazon S3 (voir "Gestion de l'accès à d'autres services de stockage dans le cloud public" (p. 581)), mais ils ne peuvent appliquer des plans de protection que lorsque l'emplacement de sauvegarde est connecté à la connexion Amazon S3 qu'ils ont eux-mêmes ajoutée, et pour les ressources enregistrées dans la console Cyber Protect sous leur nom.

Les administrateurs peuvent appliquer des plans de protection lorsque l'emplacement de sauvegarde est connecté aux connexions Amazon S3 qu'ils ont eux-mêmes ajoutées ou aux abonnements ajoutés par tout autre administrateur, et pour les ressources enregistrées dans la console Cyber Protect sous n'importe quel utilisateur.

Pour définir un emplacement de sauvegarde dans Amazon S3

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - Si vous créez ou modifiez un plan de protection, accédez à **Terminaux** et sélectionnez la ressource que vous souhaitez sauvegarder dans Amazon S3. Dans la section **Sauvegarde** du plan de protection de la ressource sélectionnée, cliquez sur le lien dans la ligne **Où sauvegarder**.

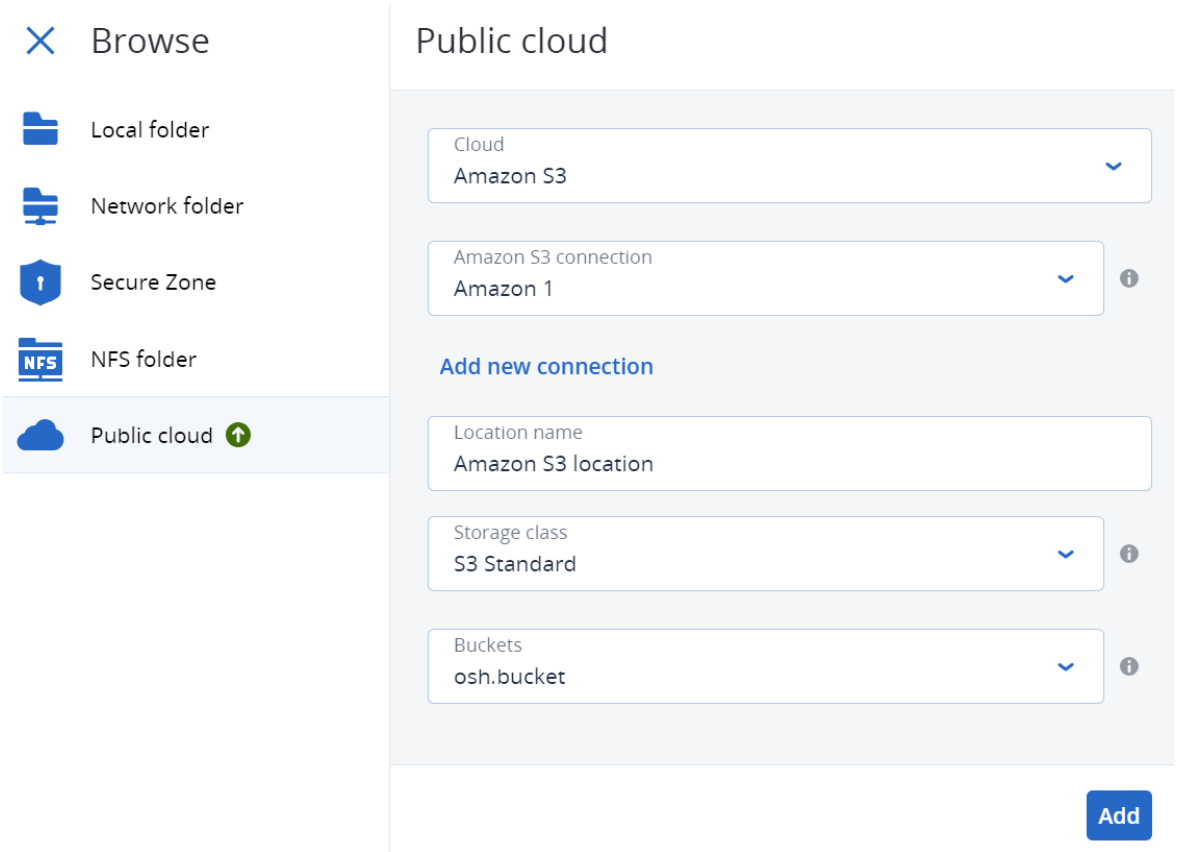
Pour plus d'informations sur l'utilisation des plans de protection, reportez-vous à "Plans et modules de protection" (p. 222).

- Si vous gérez vos emplacements de stockage des sauvegardes et souhaitez ajouter Amazon S3 en tant que nouvel emplacement, accédez à **Stockage de sauvegarde**.

  Pour plus d'informations sur la gestion de vos emplacements de stockage des sauvegardes, reportez-vous à "L'onglet Stockage de sauvegarde" (p. 552).

2. Cliquez sur **Ajouter un emplacement**.
3. Dans la liste déroulante **Clouds publics**, sélectionnez **Amazon S3**.
4. Si la connexion Amazon S3 concernée est déjà enregistrée dans la console Cyber Protect, sélectionnez-la dans la liste.

   Si la connexion concernée n'est pas enregistrée dans la console Cyber Protect, cliquez sur **Ajouter une nouvelle connexion**. Pour plus d'informations sur l'ajout et la définition de l'accès à une connexion Amazon S3, voir "Ajout d'un accès à une connexion au cloud public" (p. 581). Lorsque la connexion est ajoutée, passez à l'étape suivante.



5. Définissez ce qui suit :

- Dans le champ **Nom de l'emplacement**, saisissez le nom de l'emplacement de sauvegarde.

  Remarque
  Le nom de l'emplacement doit être unique pour le tenant client. Si le nom que vous ajoutez existe déjà dans la connexion, Acronis ajoute un numéro de suffixe au nom. Par exemple, si **Stockage Amazon S3** existe déjà, le nom sera automatiquement mis à jour en **Stockage Amazon S3 1**.

- Dans le champ **Classe de stockage**, sélectionnez l'une des classes de stockage prises en charge suivantes :
  - S3 Standard
  - Standard - Accès peu fréquent (S3 Standard-IA)
  - Une zone - Accès peu fréquent (S3 Une zone-IA)
  - S3 Hiérarchisation intelligente
- Dans le champ **Compartiment**, sélectionnez le compartiment Amazon S3 approprié.

6. Cliquez sur **Ajouter**.

   Si vous créez ou modifiez un plan de protection, l'emplacement de sauvegarde Amazon S3 est défini comme emplacement dans la ligne **Où sauvegarder**. Lorsque la sauvegarde est exécutée (manuellement ou automatiquement par planification), elle est enregistrée dans l'emplacement défini.

   Si vous gérez vos emplacements de stockage de sauvegarde, vous pouvez afficher et mettre à jour les détails de l'emplacement si nécessaire. L'emplacement Amazon S3 est également disponible lors de la définition d'un emplacement de sauvegarde pour les ressources. Pour plus d'informations, voir "Affichage et mise à jour des emplacements de sauvegarde dans le cloud public" (p. 572).

Définition d'un emplacement de sauvegarde dans Wasabi

Remarque
Pour configurer les emplacements de sauvegarde dans Wasabi, vous devez avoir l'un des rôles suivants définis dans le service de cyberprotection : administrateur d'entreprise, utilisateur, cyberadministrateur.

Pour sauvegarder une ressource dans Wasabi, vous devez définir l'emplacement de sauvegarde Wasabi dans la console Cyber Protect, puis vous connecter à la connexion Wasabi correspondante. Vous pouvez procéder de la manière suivante :

- Lors de la création ou de la modification d'un plan de protection.
- Lors de la définition et de la gestion d'emplacements de stockage des sauvegardes.

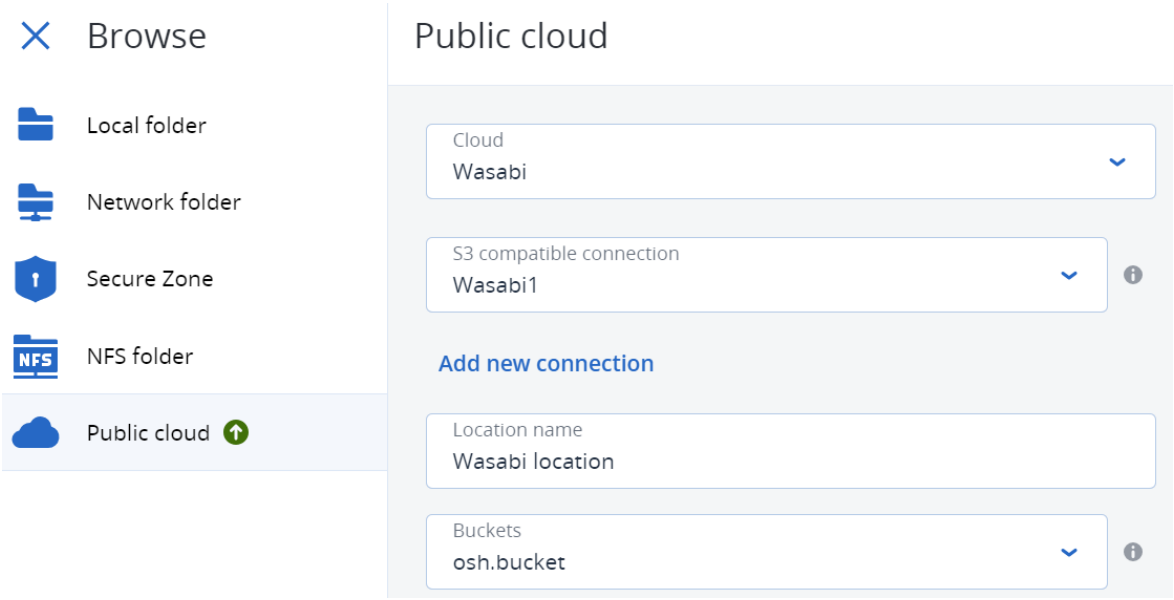
Important
Les administrateurs et les utilisateurs non-administrateurs peuvent sauvegarder des ressources dans Wasabi.

Les utilisateurs non-administrateurs peuvent ajouter un accès à une connexion Wasabi (voir "Gestion de l'accès à d'autres services de stockage dans le cloud public" (p. 581)), mais ils ne peuvent appliquer des plans de protection que lorsque l'emplacement de sauvegarde est connecté à la connexion Wasabi qu'ils ont eux-mêmes ajoutée, et pour les ressources enregistrées dans la console Cyber Protect sous leur nom.

Les administrateurs peuvent appliquer des plans de protection lorsque l'emplacement de sauvegarde est connecté aux connexions Wasabi qu'ils ont eux-mêmes ajoutées ou aux abonnements ajoutés par tout autre administrateur, et pour les ressources enregistrées dans la console Cyber Protect sous n'importe quel utilisateur.

Pour définir un emplacement de sauvegarde dans Wasabi

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - Si vous créez ou modifiez un plan de protection, accédez à **Terminaux** et sélectionnez la ressource que vous souhaitez sauvegarder dans Wasabi. Dans la section **Sauvegarde** du plan de protection de la ressource sélectionnée, cliquez sur le lien dans la ligne **Où sauvegarder**.
     Pour plus d'informations sur l'utilisation des plans de protection, reportez-vous à "Plans et modules de protection" (p. 222).
   - S vous gérez vos emplacements de stockage des sauvegardes et souhaitez ajouter Wasabi en tant que nouvel emplacement, accédez à **Stockage de sauvegarde**.
     Pour plus d'informations sur la gestion de vos emplacements de stockage des sauvegardes, reportez-vous à "L'onglet Stockage de sauvegarde" (p. 552).
2. Cliquez sur **Ajouter un emplacement**.
3. Dans la liste déroulante **Clouds publics**, sélectionnez **Wasabi**.
4. Si la connexion Wasabi concernée est déjà enregistrée dans la console Cyber Protect, sélectionnez-la dans la liste.
   Si la connexion concernée n'est pas enregistrée dans la console Cyber Protect, cliquez sur **Ajouter une nouvelle connexion**. Pour plus d'informations sur l'ajout et la définition de l'accès à une connexion Wasabi, voir "Ajout d'un accès à une connexion au cloud public" (p. 581).
   Lorsque la connexion est ajoutée, passez à l'étape suivante.



5. Définissez ce qui suit :
   - Dans le champ **Nom de l'emplacement**, saisissez le nom de l'emplacement de sauvegarde.

     Remarque
     Le nom de l'emplacement doit être unique pour le tenant client. Si le nom que vous ajoutez existe déjà dans la connexion, Acronis ajoute un numéro de suffixe au nom. Par exemple, si **Stockage Wasabi** existe déjà, le nom sera automatiquement mis à jour en **Stockage Wasabi 1**.

   - Dans le champ **Compartiment**, sélectionnez le compartiment Wasabi approprié.
6. Cliquez sur **Ajouter**.

   Si vous créez ou modifiez un plan de protection, l'emplacement de sauvegarde Wasabi est défini comme emplacement dans la ligne **Où sauvegarder**. Lorsque la sauvegarde est exécutée (manuellement ou automatiquement par planification), elle est enregistrée dans l'emplacement défini.

   Si vous gérez vos emplacements de stockage des sauvegardes, vous pouvez visualiser et mettre à jour les détails de l'emplacement si nécessaire. L'emplacement Wasabi est également disponible lors de la définition d'un emplacement de sauvegarde pour les ressources. Pour plus d'informations, voir "Affichage et mise à jour des emplacements de sauvegarde dans le cloud public" (p. 572).

Affichage et mise à jour des emplacements de sauvegarde dans le cloud public

Vous pouvez afficher et mettre à jour les emplacements de sauvegarde Microsoft Azure, Amazon S3 et Wasabi que vous définissez dans le module **Stockage des sauvegardes**, ou lors de la création ou de la modification d'un plan de protection.

Pour plus d'informations sur la suppression de l'accès à un abonnement Microsoft Azure à partir de la console Cyber Protect, voir "Suppression de l'accès à un abonnement Microsoft Azure" (p. 580). Pour plus d'informations sur la suppression de l'accès à d'autres connexions au cloud public, voir "Gestion de l'accès à d'autres services de stockage dans le cloud public" (p. 581).

Remarque
Vous ne pouvez ni actualiser ni supprimer manuellement un emplacement de sauvegarde dans le cloud public dans le module **Stockage des sauvegardes**. Le contenu de l'emplacement de sauvegarde est mis à jour automatiquement après chaque opération de sauvegarde ou de restauration.

Pour afficher les emplacements de sauvegarde dans le cloud public

1. Sur la console Cyber Protect, accédez à **Stockage de sauvegarde**.
   La liste des emplacements de sauvegarde s'affiche, avec des détails sur la capacité de stockage et le nombre de sauvegardes attribuées à chaque emplacement.
   Pour plus d'informations sur l'utilisation des emplacements de sauvegarde répertoriés, voir "L'onglet Stockage de sauvegarde" (p. 552).
2. Sélectionnez l'emplacement souhaité.
   Les sauvegardes en cours de l'emplacement sélectionné sont répertoriées.
3. (Facultatif) Cliquez sur une sauvegarde pour afficher d'autres informations la concernant.

Pour mettre à jour un emplacement de sauvegarde dans le cloud public dans un plan de protection

1. Accédez au plan de protection pertinent et sélectionnez **Modifier**.
2. Cliquez sur le lien dans la ligne **Où sauvegarder**.
3. Sélectionnez un emplacement de sauvegarde dans la liste ou cliquez sur **Ajouter un emplacement** pour ajouter un nouvel emplacement.
   Si l'abonnement Microsoft Azure ou la connexion au cloud public concernés sont déjà enregistrés dans la console Cyber Protect, sélectionnez-les dans la liste affichée.
   Si vous ajoutez un nouvel abonnement Microsoft Azure, vous êtes invité à authentifier les détails de votre compte Microsoft (voir "Ajout de l'accès à un abonnement Microsoft Azure" (p. 578)). Pour plus d'informations sur les autorisations requises lors de la connexion à Microsoft Azure, voir l'article Sécurité de la connexion à Microsoft Azure et audit (72684).

Gestion de l'accès du compte dans le cloud public

Pour activer les services Acronis Cyber Protection dans les plates-formes de cloud public, l'accès aux comptes de cloud public pertinents doit être configuré.

Par exemple, lorsque vous utilisez Microsoft Azure, l'accès à votre abonnement Microsoft Azure est nécessaire. Une fois ajouté dans la console Cyber Protect, l'abonnement peut être sélectionné lorsque vous configurez une sauvegarde directe vers Microsoft Azure. De la même manière, lorsque

vous travaillez avec Amazon S3 et Wasabi, les clés d'accès pertinentes associées à des politiques de sauvegarde spécifiques sont nécessaires.

L'accès aux clouds publics est géré par l'intermédiaire du menu **Infrastructure** de la console Cyber Protect.

Important
La validation des sauvegardes est désactivée pour les sauvegardes dans le stockage dans le cloud public, afin d'éviter des coûts de trafic de sortie excessifs. En outre, vous ne pouvez pas actuellement « rattacher » un emplacement de sauvegarde dans un cloud public au même tenant ou à un tenant différent si l'emplacement a été supprimé. Pour plus d'informations, contactez l'équipe de support.

Exigences d'accès pour la sauvegarde dans le stockage dans le cloud public

Lors de la sauvegarde directe dans des services de stockage dans le cloud public, vous devez prendre en compte un certain nombre de conditions d'accès pour chaque plate-forme :

- Microsoft Azure
- Amazon S3
- Wasabi

Sauvegarde dans Microsoft Azure

Pour vous connecter à un abonnement Microsoft Azure, vous devez disposer de plusieurs autorisations. Pour plus d'informations à ce sujet, voir l'article Sécurité et audit des connexions Microsoft Azure (72684).

Sauvegarde dans Amazon S3

Lorsque vous effectuez des sauvegardes dans Amazon S3, plusieurs conditions doivent être remplies pour que vous puissiez définir les emplacements de sauvegarde dans Amazon S3 :

- Classes de stockage prises en charge
- Autorisations de politiques
- Clés d'accès
- Paramètres de compartiment

Classes de stockage prises en charge

Les classes de stockage Amazon S3 prises en charge actuellement sont les suivantes :

- S3 Standard
- Standard - Accès peu fréquent (S3 Standard-IA)
- Une zone - Accès peu fréquent (S3 Une zone-IA)
- S3 Hiérarchisation intelligente

Autorisations de politiques

Lorsque vous effectuez des sauvegardes dans Amazon S3, les autorisations minimales doivent être appliquées à votre compte Amazon pour qu'Acronis puisse sauvegarder les ressources pertinentes dans Amazon S3. Cela signifie que les utilisateurs concernés doivent avoir accès à la console de gestion AWS et que la politique appropriée doit être appliquée aux groupes auxquels ils sont assignés.

Exemples

L'exemple de politique suivant indique l'ensemble minimum d'autorisations pour un large éventail de ressources. Notez que * indique toutes les ressources.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:GetBucketObjectLockConfiguration" ], "Resource": "*" },
{ "Effect": "Allow", "Action": "sts:GetFederationToken", "Resource": "*" }, {
"Effect": "Allow", "Action": [ "s3:GetBucketLocation", "s3:PutObject",
"s3:GetObject", "s3:DeleteObject" ], "Resource": "*" }, { "Effect": "Allow",
"Action": [ "s3:ListBucket" ], "Resource": "*" } ] }
```

L'exemple de politique suivant indique les autorisations minimales limitées à un compartiment spécifique. Notez que `[BUCKETNAME]` doit être remplacé par le nom du compartiment.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:GetBucketObjectLockConfiguration" ], "Resource":
"arn:aws:s3:::[BUCKETNAME]" }, { "Effect": "Allow", "Action":
"sts:GetFederationToken", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:PutObject", "s3:GetObject", "s3:DeleteObject" ],
"Resource": "arn:aws:s3:::[BUCKETNAME]/*" }, { "Effect": "Allow", "Action": [
"s3:ListBucket" ], "Resource": "arn:aws:s3:::[BUCKETNAME]" } ] }
```

Clés d'accès

Acronis exige les clés d'accès à chaque connexion à Amazon S3 et les utilise lors de la définition de la connexion à Amazon S3. Pour plus d'informations sur la génération de clés d'accès et de leurs identifiants, consultez la documentation d'Amazon S3.

Paramètres de compartiment

Lorsque vous utilisez les compartiments Amazon S3 comme emplacement de sauvegarde, assurez-vous que le compartiment est configuré avec les paramètres par défaut, y compris le blocage de tous les accès publics (par défaut, ce paramètre est **activé**). Pour plus d'informations sur l'utilisation des compartiments, consultez la documentation d'Amazon S3.

Remarque
Actuellement, Acronis ne prend pas en charge le versionnage des compartiments ni le verrouillage des objets dans Amazon S3, même s'ils sont activés dans le compartiment.

Sauvegarde dans Wasabi

Lorsque vous effectuez des sauvegardes dans Wasabi, vous devez tenir compte d'un certain nombre d'exigences lors de la définition des emplacements de sauvegarde :

- Autorisations de politiques
- Clés d'accès
- Paramètres de compartiment

Autorisations de politiques

Lorsque vous définissez un emplacement de sauvegarde dans Wasabi, assurez-vous que les politiques adéquates sont appliquées aux groupes et utilisateurs pertinents dans Wasabi.

Exemples

L'exemple de politique suivant indique l'ensemble minimum d'autorisations pour un large éventail de ressources. Notez que * indique toutes les ressources.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action":
"s3:GetBucketLocation", "Resource": "*" }, { "Effect": "Allow", "Action": [
"iam:CreateRole", "iam:AttachRolePolicy", "sts:GetCallerIdentity", "sts:AssumeRole"
], "Resource": "*" }, { "Effect": "Allow", "Action": [ "s3:PutObject",
"s3:GetObject", "s3:DeleteObject" ], "Resource": "*" }, { "Effect": "Allow",
"Action": "s3:ListBucket", "Resource": "*" } ] }
```

L'exemple de politique suivant indique des autorisations limitées pour une gamme limitée de ressources. Notez que `[BUCKETNAME]` doit être remplacé par le nom du compartiment et `[ACCOUNTID]`, par l'identifiant du compte Wasabi.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action":
"s3:GetBucketLocation", "Resource": "arn:aws:s3:::[BUCKETNAME]" }, { "Effect":
"Allow", "Action": [ "iam:CreateRole", "iam:AttachRolePolicy",
"sts:GetCallerIdentity", "sts:AssumeRole" ], "Resource": "arn:aws:iam::
[ACCOUNTID]:*" }, { "Effect": "Allow", "Action": [ "s3:PutObject", "s3:GetObject",
"s3:DeleteObject" ], "Resource": "arn:aws:s3:::[BUCKETNAME]/*" }, { "Effect":
"Allow", "Action": "s3:ListBucket", "Resource": "arn:aws:s3:::[BUCKETNAME]" } ] }
```

Clés d'accès

Acronis exige les clés d'accès à chaque connexion à Wasabi et les utilise lors de la définition de la connexion à Wasabi. Pour plus d'informations sur la génération de clés d'accès et de leurs identifiants, consultez la documentation de Wasabi.

Paramètres de compartiment

Lorsque vous utilisez les compartiments Wasabi comme emplacement de sauvegarde, assurez-vous que le compartiment est configuré avec les paramètres par défaut. Pour plus d'informations sur l'utilisation des compartiments, consultez la documentation Wasabi.

Remarque
Actuellement, Acronis ne prend pas en charge le versionnage des compartiments ni le verrouillage des objets dans Wasabi, même s'ils sont activés dans le compartiment.

Gestion de l'accès aux abonnements Microsoft Azure

En vous connectant aux abonnements Microsoft Azure pertinents dans la console Cyber Protect, vous pouvez sauvegarder les ressources pertinentes directement dans Microsoft Azure.

La connexion à un abonnement peut être configurée lors de la création d'un emplacement de sauvegarde via le menu **Terminaux** ou **Stockage de sauvegarde**, comme le décrit la section "Définition d'un emplacement de sauvegarde dans Microsoft Azure" (p. 565).

De la même manière, ces abonnements Microsoft Azure peuvent être configurés dans l'écran **Clouds publics** (accédez à **Infrastructure > Clouds publics**). Vous pouvez également gérer vos abonnements, y compris en renouvelant l'accès à l'abonnement, en affichant les propriétés et les activités d'abonnement, ou en supprimant l'abonnement.

En fonction du rôle d'utilisateur qui vous a été attribué, vous pouvez être en mesure de gérer les abonnements Microsoft Azure ajoutés par d'autres utilisateurs de votre organisation. Par exemple, si vous êtes administrateur d'entreprise ou d'unité, ou avez reçu le rôle de cyberadministrateur ou d'administrateur dans le service de cyberprotection, vous pouvez afficher et gérer les abonnements Microsoft Azure ajoutés par d'autres administrateurs et des utilisateurs non-administrateurs. Ces derniers peuvent uniquement afficher les abonnements Microsoft Azure qu'ils ont ajoutés à la console Cyber Protect.

Remarque
Les partenaires peuvent gérer les abonnements Microsoft Azure de clients de niveau hiérarchique inférieur. Toutefois, lorsqu'un partenaire sélectionne **Tous les clients**, le menu **Infrastructure** de la console Cyber Protect n'est pas disponible.

Important
Lors de la connexion à un abonnement Microsoft Azure, Acronis exige les autorisations minimales pour la connexion à l'abonnement. Pour plus d'informations sur les autorisations nécessaires, reportez-vous à l'article Microsoft Azure connection security and audit (72684).

Ajout de l'accès à un abonnement Microsoft Azure

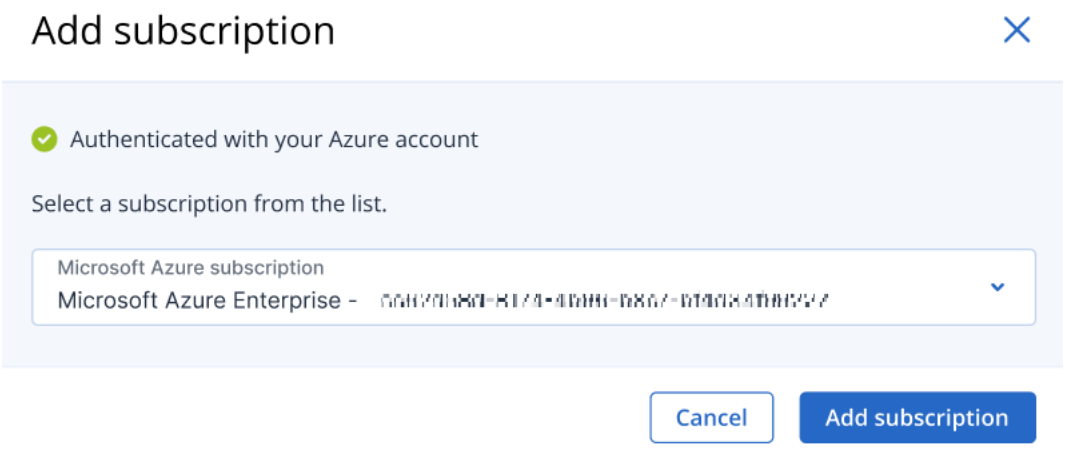
En ajoutant un abonnement Microsoft Azure dans la console Cyber Protect, Acronis peut accéder en toute sécurité à votre abonnement et sauvegarder directement les ressources pertinentes dans Microsoft Azure.

Pour ajouter l'accès à un abonnement Microsoft Azure

1. Dans la console Cyber Protect, accédez à **Infrastructure > Clouds publics**.
2. Cliquez sur **Ajouter**, puis sélectionnez **Microsoft Azure** dans la liste des options.
3. Dans la boîte de dialogue qui s'affiche, cliquez sur **Se connecter**. Vous êtes redirigé vers la page de connexion de Microsoft.

   Remarque
   Pour établir la connexion à l'abonnement, vous devez disposer de l'un des rôles suivants dans Microsoft Azure AD : Administrateur d'applications dans le cloud, administrateur d'applications ou administrateur global. Vous devez également recevoir le rôle de propriétaire pour chaque abonnement sélectionné.

4. Dans l'écran de connexion Microsoft, saisissez vos identifiants de connexion et acceptez les autorisations demandées. Le processus de connexion démarre et peut prendre plusieurs minutes.
   Pour plus d'informations sur l'accès sécurisé à votre abonnement Microsoft Azure, reportez-vous à l'article Microsoft Azure connection security and audit (72684).
5. Lorsque la connexion est établie, sélectionnez l'abonnement pertinent dans la liste déroulante de la boîte de dialogue, puis cliquez sur **Ajouter un abonnement**.



L'abonnement est ajouté à la liste des clouds publics.

Pour renouveler le certificat d'accès annuel de l'abonnement, voir "Renouvellement de l'accès à un abonnement Microsoft Azure" (p. 579).

Pour supprimer l'accès à l'abonnement, voir "Suppression de l'accès à un abonnement Microsoft Azure" (p. 580).

Remarque
Si le compte Microsoft Azure auquel vous êtes connecté comprend l'accès à plusieurs AD Microsoft Azure, y compris ceux dans lesquels vous avez été invité en tant qu'utilisateur invité, seul le répertoire utilisateur par défaut est sélectionné. Si vous souhaitez utiliser un répertoire dans lequel vous êtes utilisateur invité, vous devez créer un nouvel utilisateur dans cet AD Microsoft Azure spécifique. Vous pouvez alors vous connecter à ce compte et à l'abonnement pertinent.

Renouvellement de l'accès à un abonnement Microsoft Azure

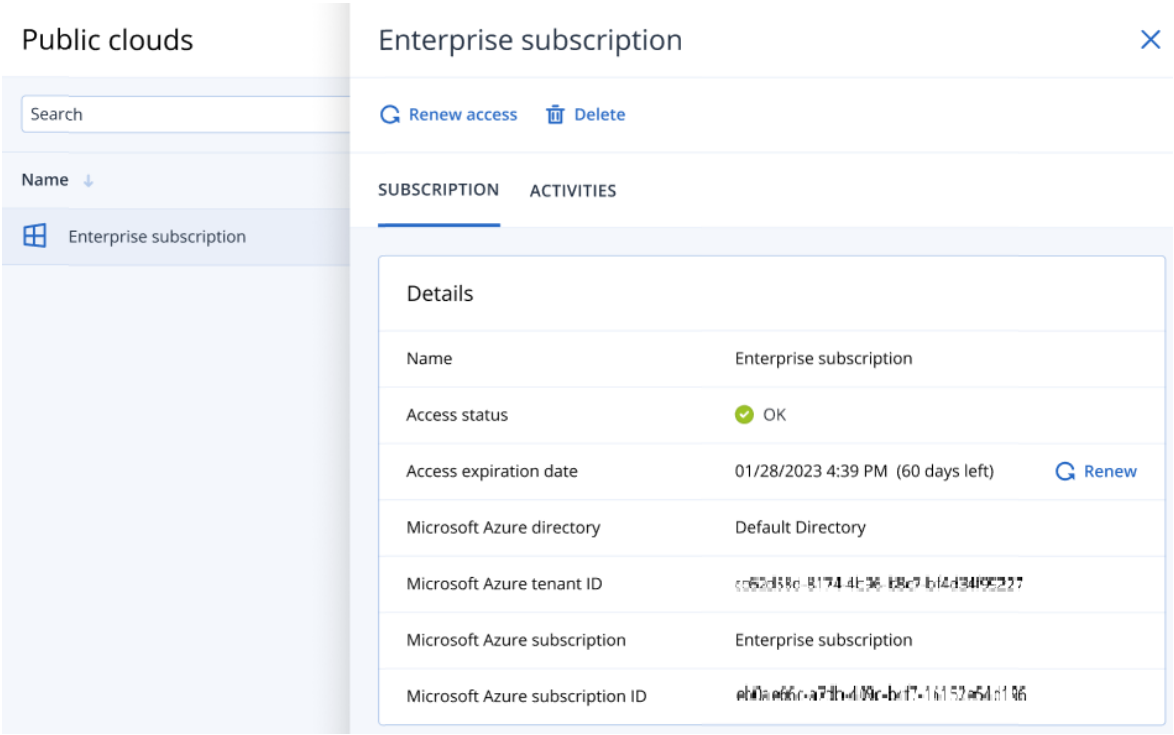
Une fois que vous êtes enregistré dans la console Cyber Protect, l'accès à un abonnement Microsoft Azure est défini automatiquement pour une année par Acronis à l'aide d'un certificat d'accès gratuit et unique. Lorsque le certificat s'approche de sa date d'expiration, vous pouvez le renouveler facilement et rapidement.

Pour renouveler le certificat d'accès de votre abonnement Microsoft Azure

1. Dans la console Cyber Protect, accédez à **Infrastructure > Clouds publics**.
2. Sélectionnez l'abonnement pertinent dans la liste affichée.

   Remarque
   La colonne **État de l'accès** indique le statut actuel du certificat d'accès pour chaque abonnement et indique l'un des deux statuts : **OK** ou **Expiré**.

3. Dans le volet de droite, cliquez sur **Renouveler l'accès**.
   Vous pouvez également cliquer sur l'onglet **Abonnement**, puis sur **Renouveler** dans le champ **Date d'expiration de l'accès**.



4. Dans l'écran de connexion Microsoft, saisissez vos identifiants de connexion et acceptez les autorisations demandées. Le processus de connexion démarre et peut prendre plusieurs minutes.

   Lorsque l'authentification est réussie, l'accès est renouvelé automatiquement pour une année.

   Pour plus d'informations sur les autorisations nécessaires, reportez-vous à l'article Microsoft Azure connection security and audit (72684).

Suppression de l'accès à un abonnement Microsoft Azure

Vous devez supprimer l'accès à l'abonnement Microsoft Azure si vous ne sauvegardez pas les ressources dans Microsoft Azure.

Pour supprimer l'accès à un abonnement Microsoft Azure

Important
Vous ne pouvez pas supprimer un abonnement s'il est en cours d'utilisation par une sauvegarde dans Microsoft Azure.

1. Dans la console Cyber Protect, accédez à **Infrastructure > Clouds publics**.
2. Sélectionnez l'abonnement pertinent dans la liste affichée.
3. Dans le volet de droite, cliquez sur **Supprimer**.

Remarque
Vous ne pouvez retirer qu'un abonnement que vous avez ajouté. Vous pouvez également supprimer un abonnement si vous êtes administrateur d'entreprise ou de division, ou avez reçu le rôle de cyberadministrateur ou d'administrateur du service de cyberprotection.

4. Dans le message de confirmation qui s'affiche, cliquez sur **Supprimer**.

Gestion de l'accès à d'autres services de stockage dans le cloud public

Remarque
Cette section concerne la gestion de l'accès à tous les services de stockage dans le cloud public autres que Microsoft Azure, qui est décrite ici : "Gestion de l'accès aux abonnements Microsoft Azure" (p. 577).

En vous connectant au compte de cloud public concerné dans la console Cyber Protect, vous pouvez sauvegarder les ressources directement dans le stockage de cloud public concerné.

Vous pouvez configurer les connexions aux comptes de stockage dans le cloud public lors de la création d'un emplacement de sauvegarde via le menu **Terminaux** ou **Stockage de sauvegarde**. Vous pouvez également configurer les connexions aux clouds publics dans l'écran **Clouds publics** (accédez à **Infrastructure > Clouds publics**). Vous pouvez également gérer votre connexion, notamment en renouvelant l'accès à la connexion, en affichant les propriétés et les activités de la connexion, ou en supprimant la connexion.

Selon le rôle d'utilisateur qui vous a été attribué, vous pouvez être en mesure de gérer les connexions dans le cloud public ajoutées par d'autres utilisateurs de votre organisation. Par exemple, si vous êtes administrateur d'entreprise ou d'unité, ou avez reçu le rôle de cyberadministrateur ou d'administrateur du service de cyberprotection, vous pouvez visualiser et gérer les connexions au cloud public ajoutées par d'autres administrateurs et les utilisateurs non-administrateurs. Les utilisateurs non-administrateurs peuvent uniquement afficher et utiliser les connexions au cloud public qu'ils ont ajoutés à la console Cyber Protect.

Remarque
Les partenaires peuvent gérer les connexions au cloud public des clients situés en dessous de leur niveau dans la hiérarchie. Toutefois, lorsqu'un partenaire sélectionne **Tous les clients**, le menu **Infrastructure** de la console Cyber Protect n'est pas disponible.

Important
Lors de la connexion à un cloud public, Acronis requiert un certain nombre d'autorisations. Pour plus d'informations, voir "Exigences d'accès pour la sauvegarde dans le stockage dans le cloud public" (p. 574).

Ajout d'un accès à une connexion au cloud public

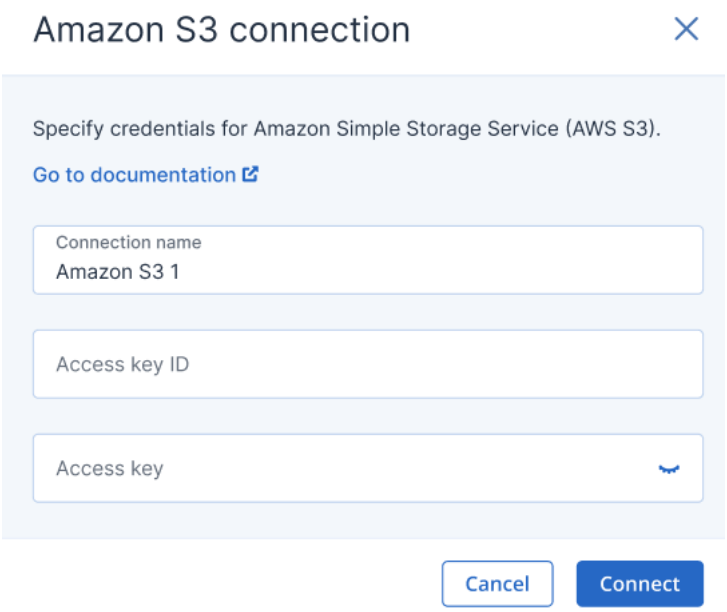
Après avoir ajouté une connexion au cloud public (Amazon S3 ou Wasabi, par exemple) dans la console Cyber Protect, Acronis peut accéder en toute sécurité à vos ressources dans le cloud et les sauvegarder directement dans le stockage dans le cloud public correspondant.

Pour ajouter un accès à une connexion au cloud public

1. Dans la console Cyber Protect, accédez à **Infrastructure > Clouds publics**.
2. Cliquez sur **Ajouter** et sélectionnez l'une des options suivantes :
   - **Amazon S3**

     Dans la boîte de dialogue qui s'affiche, définissez les options suivantes :
     - **Nom de la connexion** : nom de la connexion Amazon S3.
     - **Identifiant de la clé d'accès** : identifiant de la clé d'accès de l'utilisateur pour le service Amazon S3.
     - **Clé d'accès** : clé d'accès de l'utilisateur au service Amazon S3.

       La clé d'accès et son identifiant permettent à Acronis d'accéder aux classes et aux compartiments de stockage pour la connexion concernée. Pour plus d'informations sur les clés d'accès et les autorisations requises par Acronis, voir "Exigences d'accès pour la sauvegarde dans le stockage dans le cloud public" (p. 574).

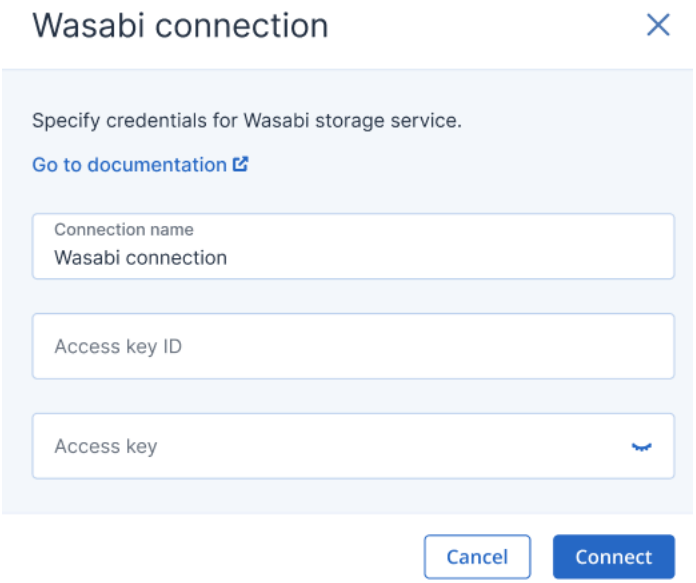


   - **Wasabi**

     Dans la boîte de dialogue qui s'affiche, définissez les options suivantes :
     - **Nom de la connexion** : nom de la connexion Wasabi.
     - **Identifiant de la clé d'accès** : identifiant de la clé d'accès de l'utilisateur pour le service Wasabi.
     - **Clé d'accès** : clé d'accès de l'utilisateur au service Wasabi.

       La clé d'accès et son identifiant permettent à Acronis d'accéder aux classes et aux compartiments de stockage pour la connexion concernée. Pour plus d'informations sur les clés d'accès et les autorisations requises par Acronis, voir "Exigences d'accès pour la

sauvegarde dans le stockage dans le cloud public" (p. 574).



3. Cliquez sur **Connexion**.

   Le processus de connexion démarre et peut durer plusieurs minutes. Une fois terminé, la connexion est ajoutée à la liste des clouds publics.

   Pour renouveler le certificat d'accès annuel à la connexion, voir "Renouvellement de l'accès à une connexion au cloud public" (p. 583).

   Pour supprimer l'accès à la connexion, voir "Suppression de l'accès à une connexion au cloud public" (p. 584).

Renouvellement de l'accès à une connexion au cloud public

Après l'enregistrement d'une connexion au cloud public dans la console Cyber Protect, Acronis attribue automatiquement un certificat d'accès gratuit et unique qui permet d'accéder à la connexion au cloud public. Le certificat est valable un an. Lorsque le certificat approche de sa date d'expiration, vous pouvez le renouveler.

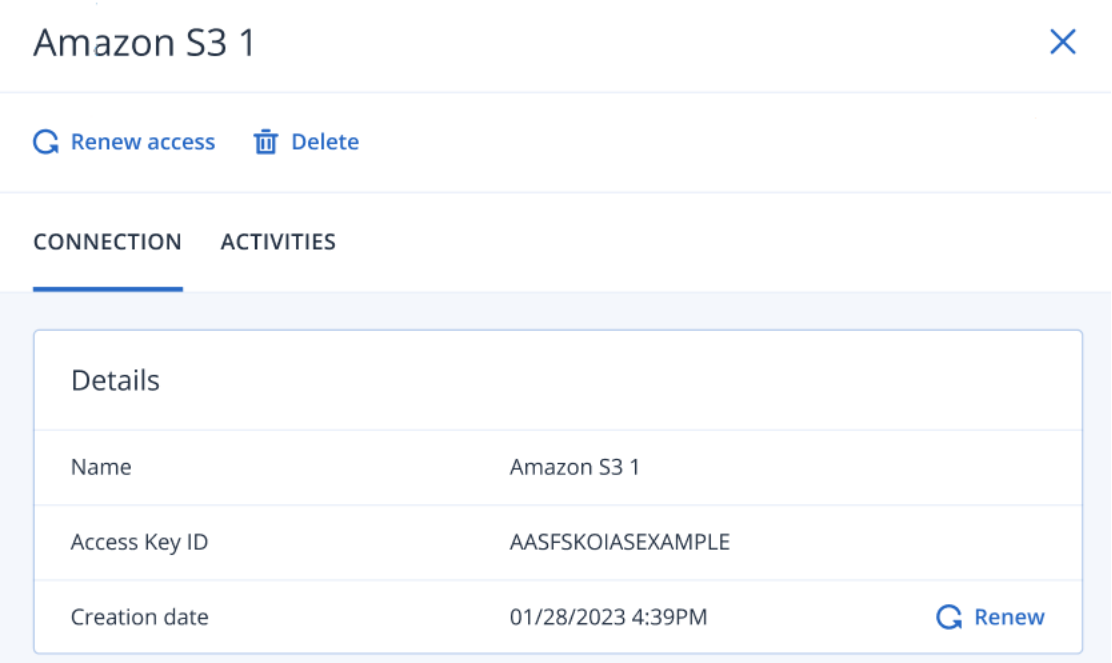
Pour renouveler le certificat d'accès à votre connexion au cloud public

1. Dans la console Cyber Protect, accédez à **Infrastructure > Clouds publics**.
2. Sélectionnez la connexion concernée dans la liste.

   Remarque
   La colonne **État d'accès** indique l'état actuel du certificat d'accès pour chaque connexion et présente l'un des deux états suivants : **OK** ou **Expiré**.

3. Dans le volet de droite, cliquez sur **Renouveler l'accès**.

   Vous pouvez également cliquer sur l'onglet **Connexion**, puis sur **Renouveler** dans la ligne **Date de création**.



Lorsque l'authentification est réussie, l'accès est renouvelé automatiquement pour une année.

Suppression de l'accès à une connexion au cloud public

Si vous ne sauvegardez pas de ressources dans des clouds publics, vous devez supprimer l'accès aux connexions au cloud public.

Pour supprimer l'accès à une connexion au cloud public

Important
Vous ne pouvez pas supprimer une connexion si elle est actuellement utilisée pour des sauvegardes vers un cloud public.

1. Dans la console Cyber Protect, accédez à **Infrastructure > Clouds publics**.
2. Sélectionnez la connexion dans la liste.
3. Dans le volet de droite, cliquez sur **Supprimer**.

   Remarque
   Vous ne pouvez retirer qu'une connexion que vous avez ajoutée. Vous pouvez également supprimer une connexion si vous êtes administrateur d'entreprise ou d'unité, ou avez reçu le rôle de cyberadministrateur ou d'administrateur du service de cyberprotection.

4. Dans le message de confirmation qui s'affiche, cliquez sur **Supprimer**.

Protection d'applications Microsoft

Protection des serveurs Microsoft SQL Server et Microsoft Exchange Server

Remarque
La sauvegarde de Microsoft SQL n'est prise en charge que pour les bases de données fonctionnant sur les systèmes de fichiers NFTS, REFS et FAT32. ExFat n'est pas pris en charge.

Il existe deux méthodes de protection pour les applications Microsoft :

- **Sauvegarde de base de données**
  Il s'agit d'une sauvegarde des bases de données et des métadonnées associées. Les bases de données peuvent être restaurées sur une application active ou en tant que fichiers.
- **Sauvegarde reconnaissant les applications**
  Il s'agit d'une sauvegarde de niveau disque qui collecte également les métadonnées des applications. Ces métadonnées permettent l'exploration et la restauration des données de l'application sans restaurer la totalité du disque ou du volume. Le disque et le volume peuvent également être restaurés intégralement. Cela signifie qu'une seule solution et un seul plan de protection peuvent être utilisés à la fois à des fins de reprise d'activité après sinistre et de protection des données.

Pour Microsoft Exchange Server, vous pouvez choisir **Sauvegarde de boîte de réception**. Il s'agit d'une sauvegarde de boîtes aux lettres individuelles via le protocole Services web Exchange. La ou les boîtes aux lettres peuvent être restaurée(s) sur Exchange Server en temps réel ou sur Microsoft 365. La sauvegarde des boîtes aux lettres est prise en charge pour Microsoft Exchange Server 2010 Service Pack 1 (SP1) et version ultérieure.

Protection de Microsoft SharePoint

Une batterie de serveurs Microsoft SharePoint contient des serveurs frontaux qui exécutent des services SharePoint, des serveurs de bases de données qui exécutent Microsoft SQL Server, et (facultativement) des serveurs d'applications qui déchargent certains services SharePoint des serveurs frontaux. Certains serveurs d'applications et serveurs frontaux peuvent être identiques l'un à l'autre.

Pour protéger une batterie de serveurs SharePoint dans son intégralité :

- Sauvegardez tous les serveurs de bases de données avec une sauvegarde reconnaissant les applications.
- Sauvegardez tous les serveurs d'applications et les serveurs frontaux uniques avec une sauvegarde de niveau disque habituelle.

Les sauvegardes de tous les serveurs doivent être effectuées en utilisant la même planification.

Pour protéger le contenu uniquement, vous pouvez sauvegarder les bases de données de contenu séparément.

Protection d'un contrôleur de domaine

Une machine exécutant les services de domaine Active Directory peut être protégée par une sauvegarde reconnaissant les applications. Si un domaine comprend plusieurs contrôleurs de domaine et que vous en restaurez un, une restauration ne faisant pas autorité est effectuée et une restauration USN n'a pas lieu par la suite.

Restauration d'applications

Le tableau suivant résume les méthodes de restauration d'applications disponibles.

	À partir d'une sauvegarde de base de données	**À partir d'une sauvegarde reconnaissant les applications**	**À partir d'une sauvegarde de disque**
Microsoft SQL Server	Bases de données sur une instance SQL Server distante active Bases de données en tant que fichiers	Toute la machine Bases de données sur une instance SQL Server distante active Bases de données en tant que fichiers	Toute la machine
Microsoft Exchange Server	Bases de données sur un serveur Exchange actif Bases de données en tant que fichiers Restauration granulaire sur un serveur Exchange ou Microsoft 365*	Toute la machine Bases de données sur un serveur Exchange actif Bases de données en tant que fichiers Restauration granulaire sur un serveur Exchange ou Microsoft 365*	Toute la machine
Serveurs de bases de données Microsoft SharePoint	Bases de données sur une instance SQL Server distante active Bases de données en tant que fichiers Restauration granulaire avec SharePoint Explorer	Toute la machine Bases de données sur une instance SQL Server distante active Bases de données en tant que fichiers Restauration granulaire avec SharePoint Explorer	Toute la machine
Serveurs Web frontaux Microsoft	-	-	Toute la machine

SharePoint			
Services de domaine Active Directory	-	Toute la machine	-

* La restauration granulaire est également disponible à partir d'une sauvegarde de boîte aux lettres. La récupération d'éléments de données Exchange vers Microsoft 365, et inversement, est prise en charge à la condition que l'agent pour Microsoft 365 soit installé localement.

Prérequis

Avant de configurer l'application de sauvegarde, assurez-vous que les exigences répertoriées ci-dessous sont remplies.

Pour vérifier l'état des enregistreurs VSS, utilisez la commande `vssadmin list writers`.

Exigences communes

Pour Microsoft SQL Server, assurez-vous que :

- Au moins une instance de Microsoft SQL Server est démarrée.
- L'enregistreur SQL pour VSS est activé.

Pour Microsoft Exchange Server, assurez-vous que :

- le service Microsoft Exchange Information Store est démarré.
- Windows PowerShell est installé. Pour Exchange 2010 ou version ultérieure, la version de Windows PowerShell doit être au moins la 2.0.
- Microsoft .NET Framework est installé.

  Pour Exchange 2007, la version de Microsoft .NET Framework doit être au moins la 2.0.

  Pour Exchange 2010 ou version ultérieure, la version de Microsoft .NET Framework doit être au moins la 3.5.
- L'enregistreur Exchange pour VSS est activé.

Remarque
L'agent pour Exchange requiert un stockage temporaire pour fonctionner. Par défaut, les fichiers temporaires sont situés dans `%ProgramData%\Acronis\Temp`. Veillez à disposer à l'emplacement du dossier `%ProgramData%` d'au moins autant d'espace que 15 % de la taille d'une base de données Exchange. Sinon, modifiez l'emplacement des fichiers temporaires avant la création des sauvegardes Exchange, comme décrit dans Changing Temp Files and Folder Location (40040).

Sur un contrôleur de domaine, assurez-vous que :

- L'enregistreur Active Directory pour VSS est activé.

Lors de la création d'un plan de protection, procédez aux vérifications suivantes :

- Pour les machines physiques et les machines sur lesquelles l'agent est installé, l'option de sauvegarde Service de cliché instantané des volumes (VSS) est activée.
- Pour les machines virtuelles, l'option de sauvegarde Service de cliché instantané des volumes (VSS) pour les machines virtuelles est activée.

Exigences supplémentaires pour les sauvegardes reconnaissant les applications

Lors de la création d'un plan de protection, assurez-vous que l'option **Toute la machine** est sélectionnée pour la sauvegarde. L'option de sauvegarde **secteur par secteur** sera désactivée dans un plan de protection. Dans le cas contraire, il sera impossible d'exécuter une restauration des données d'application à partir de ces sauvegardes. Si le plan est exécuté en mode **secteur par secteur** en raison d'un basculement automatique vers ce mode, la restauration des données d'application sera également impossible.

Exigences pour les machines virtuelles ESXi

Si l'application s'exécute sur une machine virtuelle sauvegardée par l'agent pour VMware, assurez-vous que :

- La machine virtuelle sauvegardée répond aux exigences de sauvegarde et de restauration en cohérence avec l'application qui sont répertoriées dans l'article Windows Backup Implementations de la documentation VMware : https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html.
- VMware Tools est installé et à jour sur la machine.
- Le contrôle de compte utilisateur (CCU) est désactivé sur la machine. Si vous ne souhaitez pas désactiver le CCU, vous devez fournir les identifiants de l'administrateur de domaine intégré (DOMAIN\Administrator) lors de l'activation d'une sauvegarde d'application.
  Si vous ne souhaitez pas désactiver le CCU, vous devez fournir les identifiants de l'administrateur de domaine intégré (DOMAIN\Administrator) lors de l'activation d'une sauvegarde d'application.

  Remarque
  Utilisez le compte administrateur du domaine intégré qui a été configuré lors de la création du domaine. Les comptes créés plus tard ne sont pas pris en charge.

Exigences pour les machines virtuelles Hyper-V

Si l'application s'exécute sur une machine virtuelle sauvegardée par l'agent pour Hyper-V, assurez-vous que :

- Le système d'exploitation invité est Windows Server 2008 ou version ultérieure.
- Pour Hyper-V 2008 R2 : le système d'exploitation invité est Windows Server 2008/2008 R2/2012.
- La machine virtuelle ne possède aucun disque dynamique.
- La connexion réseau existe entre l'hôte Hyper-V et le système d'exploitation invité. Ceci est requis pour exécuter des demandes WMI distantes au sein de la machine virtuelle.

- Le contrôle de compte utilisateur (CCU) est désactivé sur la machine. Si vous ne souhaitez pas désactiver le CCU, vous devez fournir les identifiants de l'administrateur de domaine intégré (DOMAIN\Administrator) lors de l'activation d'une sauvegarde d'application.
  Si vous ne souhaitez pas désactiver le CCU, vous devez fournir les identifiants de l'administrateur de domaine intégré (DOMAIN\Administrator) lors de l'activation d'une sauvegarde d'application.

  Remarque
  Utilisez le compte administrateur du domaine intégré qui a été configuré lors de la création du domaine. Les comptes créés plus tard ne sont pas pris en charge.

- La configuration de la machine virtuelle correspond aux critères suivants :
  - La technologie Hyper-V Integration Services est installée et à jour. La mise à jour critique est https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines
  - Dans les paramètres de votre machine virtuelle, l'option **Gestion** > **Services d'intégration** > **Sauvegarde (point de contrôle du volume)** est activée.
  - Pour Hyper-V 2012 et version ultérieure : la machine virtuelle ne possède aucun point de contrôle.
  - Pour Hyper-V 2012 R2 et version ultérieure : la machine virtuelle possède un contrôleur SCSI (consultez **Paramètres** > **Matériel**).

Sauvegarde de base de données

Avant de sauvegarder des bases de données, assurez-vous que les exigences répertoriées dans « Prérequis » sont respectées.

Sélectionnez les bases de données comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Sélection des bases de données SQL

Une sauvegarde de base de données SQL contient les fichiers de bases de données (.mdf, .ndf), les fichiers journaux (.ldf) et d'autres fichiers associés. Les fichiers sont sauvegardés à l'aide du service SQL Writer. Le service doit être exécuté au moment où le service de cliché instantané des volumes (VSS) nécessite une sauvegarde ou une restauration.

Les fichiers journaux des transactions SQL sont tronqués après chaque sauvegarde réussie. La troncation de journal SQL peut être désactivée dans les options du plan de protection.

Pour sélectionner des bases de données SQL

1. Cliquez sur **Terminaux** > **Microsoft SQL**.
   Le logiciel affiche l'arborescence des groupes de disponibilité AlwaysOn Microsoft SQL Server (AAG), les machines fonctionnant sous Microsoft SQL Server, les instances SQL Server et les bases de données.
2. Accédez aux données que vous voulez sauvegarder.

Développez les nœuds de l'arborescence ou double-cliquez sur les éléments de la liste à la droite de l'arborescence.

3. Sélectionnez les données que vous voulez sauvegarder. Vous pouvez sélectionner les AAG, les machines fonctionnant sous SQL Server, les instances SQL Server ou les bases de données individuelles.
   - Si vous sélectionnez un AAG, toutes les bases de données incluses dans l'AAG sélectionné seront sauvegardées. Pour plus d'informations sur la sauvegarde des AAG ou de bases de données AAG individuelles, consultez la section « Protection des groupes de disponibilité AlwaysOn (AAG) ».
   - Si vous sélectionnez une machine fonctionnant sous SQL Server, toutes les bases de données attachées aux instances SQL Server fonctionnant sur la machine sélectionnée seront sauvegardées.
   - Si vous sélectionnez une instance SQL Server, toutes les bases de données incluses dans l'instance sélectionnée seront sauvegardées.
   - Si vous sélectionnez directement les bases de données, seules les bases de données sélectionnées seront sauvegardées.
4. Cliquez sur **Protection**. Si vous y êtes invité, spécifiez les identifiants donnant accès aux données SQL Server.

   Si vous utilisez l'authentification Windows, le compte doit être membre des groupes **Opérateurs de sauvegarde** ou **Administrateurs** de la machine, et du rôle **sysadmin** de chacune des instances faisant l'objet d'une sauvegarde.

   Si vous utilisez l'authentification SQL Server, le compte doit être membre du rôle **sysadmin** de chacune des instances faisant l'objet d'une sauvegarde.

Sélection de données Exchange Server

Le tableau suivant résume les données de Microsoft Exchange Server que vous pouvez sélectionner pour leur sauvegarde, ainsi que les droits d'utilisateur nécessaires pour effectuer cette tâche.

Version d'Exchange	Eléments de données	Droits utilisateur
2007	Groupes de stockage	Appartenance au groupe de rôles **Gestion d'organisation Exchange**
2010/2013/2016/2019	Bases de données, Groupes de disponibilité de la base de données (DAG)	Appartenance au groupe de rôles **Gestion de serveur**.

Une sauvegarde complète inclut l'ensemble des données Exchange Server sélectionnées.

Une sauvegarde incrémentielle comprend les blocs modifiés des fichiers de la base de données, les fichiers de point de contrôle, ainsi que quelques fichiers journaux plus récents que le point de contrôle de la base de données correspondant. Puisque les modifications apportées aux fichiers de la base de données sont intégrées à la sauvegarde, il n'est pas nécessaire de sauvegarder tous les enregistrements des journaux de transaction depuis la sauvegarde précédente. Seul le fichier

journal ultérieur au point de contrôle doit être réutilisé après une restauration. Cela permet une restauration plus rapide et assure la réussite de la sauvegarde de la base de données, même lorsque l'enregistrement circulaire est activé.

Les fichiers journaux des transactions sont tronqués après chaque sauvegarde réussie.

Pour sélectionner des données Exchange Server

1. Cliquez sur **Terminaux** > **Microsoft Exchange**.
   Le logiciel affiche l'arborescence des groupes de disponibilité de la base de données (DAG) Exchange Server, les machines fonctionnant sous Microsoft Exchange Server et les bases de données Exchange Server. Si vous avez configuré l'agent pour Exchange tel que décrit dans "Sauvegarde de boîte de réception" (p. 598), les boîtes aux lettres s'affichent également dans cette arborescence.
2. Accédez aux données que vous voulez sauvegarder.
   Développez les nœuds de l'arborescence ou double-cliquez sur les éléments de la liste à la droite de l'arborescence.
3. Sélectionnez les données que vous voulez sauvegarder.
   - Si vous sélectionnez un DAG, une copie de chaque base de données en cluster sera sauvegardée. Pour plus d'informations sur la sauvegarde des DAG, reportez-vous à "Protection des groupes de disponibilité de la base de données (DAG)" (p. 593).
   - Si vous sélectionnez une machine fonctionnant sous Microsoft Exchange Server, toutes les bases de données montées sur Exchange Server fonctionnant sur la machine sélectionnée seront sauvegardées.
   - Si vous sélectionnez directement les bases de données, seules les bases de données sélectionnées seront sauvegardées.
   - Si vous avez configuré l'agent pour Exchange tel que décrit dans "Sauvegarde de boîte de réception" (p. 598), vous pouvez sélectionner les boîtes aux lettres pour la sauvegarde.

   Si votre sélection comporte plusieurs bases de données, deux d'entre elles sont traitées simultanément. Une fois la sauvegarde du premier groupe terminée, celle du groupe suivant commence.
4. Le cas échéant, spécifiez les identifiants donnant accès aux données.
5. Cliquez sur **Protection**.

Protection des groupes de disponibilité AlwaysOn (AAG)

Remarque
Cette fonctionnalité est disponible avec le pack Advanced Backup.

Présentation des solutions SQL Server haute disponibilité

La fonctionnalité de clustering de basculement Windows Server (WSFC) vous permet de configurer SQL Server pour qu'il soit à haute disponibilité en utilisant la redondance au niveau de l'instance

(instance de cluster de basculement, FCI) ou au niveau de la base de données (groupe de disponibilité AlwaysOn, AAG). Vous pouvez également combiner les deux méthodes.

Dans une instance de cluster de basculement, les bases de données SQL sont situées sur un stockage partagé. Ce stockage est accessible uniquement à partir du nœud cluster actif. Si le nœud actif échoue, un basculement se produit et un autre nœud devient actif.

Dans un groupe de disponibilité, chaque réplica de base de données réside sur un nœud différent. Si le réplica principal devient non disponible, le rôle principal est attribué à un réplica secondaire résidant sur un autre nœud.

Ainsi, les clusters sont déjà utilisés comme solution de reprise d'activité après sinistre. Toutefois, il peut arriver que les clusters ne puissent pas fournir de protection de données : par exemple, dans le cas d'un endommagement logique d'une base de données ou d'une panne du cluster entier. De plus, des solutions de cluster ne protègent pas contre les modifications dangereuses de contenu car elles sont immédiatement reproduites sur tous les nœuds de cluster.

Configurations de cluster prises en charge

Le logiciel de sauvegarde prend *uniquement* en charge les groupes de disponibilité AlwaysOn (AAG) pour SQL Server 2012 ou version ultérieure. Les autres configurations de cluster, comme les instances de cluster de basculement, la mise en miroir de base de données et l'envoi des journaux, *ne sont pas* prises en charge.

Combien d'agents sont nécessaires pour la sauvegarde et la restauration de données de cluster ?

Pour réussir la sauvegarde et la restauration de données d'un cluster, Agent pour SQL doit être installé sur chaque nœud du cluster WSFC.

Sauvegarde des bases de données incluses dans un AAG

1. Installez Agent pour SQL sur tous les nœuds du cluster WSFC.
2. Sélectionnez l'AAG à sauvegarder comme décrit dans la section « Sélection des bases de données SQL ».

   Vous devez sélectionner l'AAG lui-même pour sauvegarder toutes les bases de données qu'il contient. Pour sauvegarder un ensemble de bases de données, définissez cet ensemble de bases de données dans tous les nœuds de l'AAG.

   Avertissement !
   L'ensemble de bases de données doit être exactement le même dans tous les nœuds. Si le moindre ensemble est différent ou n'est pas défini dans tous les nœuds, la sauvegarde de cluster ne fonctionnera pas correctement.

3. Configurez l'option de sauvegarde « Mode de sauvegarde de cluster ».

Restauration de bases de données incluses dans un AAG

1. Sélectionnez les bases de données que vous voulez restaurer, puis sélectionnez le point de récupération à partir duquel vous voulez les restaurer.

   Quand vous sélectionnez une base de données en cluster sous **Terminaux** > **Microsoft SQL** > **Bases de données** et que vous cliquez sur **Restaurer**, le logiciel n'affiche que les points de récupération correspondant aux fois où la copie sélectionnée de la base de données a été sauvegardée.

   La façon la plus simple de voir tous les points de récupération d'une base de données en cluster est de sélectionner la sauvegarde de l'AAG entier dans l'onglet Stockage de sauvegarde. Les noms des sauvegardes d'AAG sont basés sur le modèle suivant : `<nom AAG> - <nom plan protection>` et sont dotés d'une icône spéciale.
2. Pour configurer la restauration, suivez les étapes décrites dans « Restauration de bases de données SQL », en commençant par l'étape 5.

   Le logiciel définit automatiquement un nœud cluster vers lequel les données seront restaurées. Le nom du nœud est affiché dans le champ **Récupérer vers**. Vous pouvez modifier le nœud cible manuellement.

   Important
   Une base de données incluse dans un groupe de disponibilité AlwaysOn ne peut pas être écrasée lors d'une restauration, car Microsoft SQL Server l'interdit. Vous devez exclure la base de données cible de l'AAG avant la restauration. Ou restaurez simplement la base de données en tant que nouvelle base de données non AAG. Lorsque la restauration est terminée, vous pouvez reconstruire la configuration AAG d'origine.

Protection des groupes de disponibilité de la base de données (DAG)

Remarque
Cette fonctionnalité est disponible avec le pack Advanced Backup.

Présentation des clusters Exchange Server

L'idée principale des clusters Exchange est d'offrir une disponibilité élevée des bases de données, avec un basculement rapide et sans aucune perte de données. Généralement, cela se réalise en conservant une ou plusieurs copies de bases de données ou de groupes de stockage sur les membres du cluster (nœuds de cluster). Si le nœud de cluster qui héberge la copie de base de données active ou si la copie de la base de données active elle-même échoue, l'autre nœud qui héberge la copie passive prend automatiquement la relève des opérations du nœud qui a échoué et fournit l'accès aux services Exchange avec un temps d'arrêt minimal. Ainsi, les clusters sont déjà utilisés comme solution de reprise d'activité après sinistre.

Toutefois, il y a des cas où les solutions de cluster de basculement ne peuvent pas fournir une protection des données : par exemple, dans le cas d'un endommagement logique d'une base de données, lorsqu'une base de données particulière d'un cluster n'a aucune copie (réplica) ou bien

lorsque le cluster entier est en panne. De plus, des solutions de cluster ne protègent pas contre les modifications dangereuses de contenu car elles sont immédiatement reproduites sur tous les nœuds de cluster.

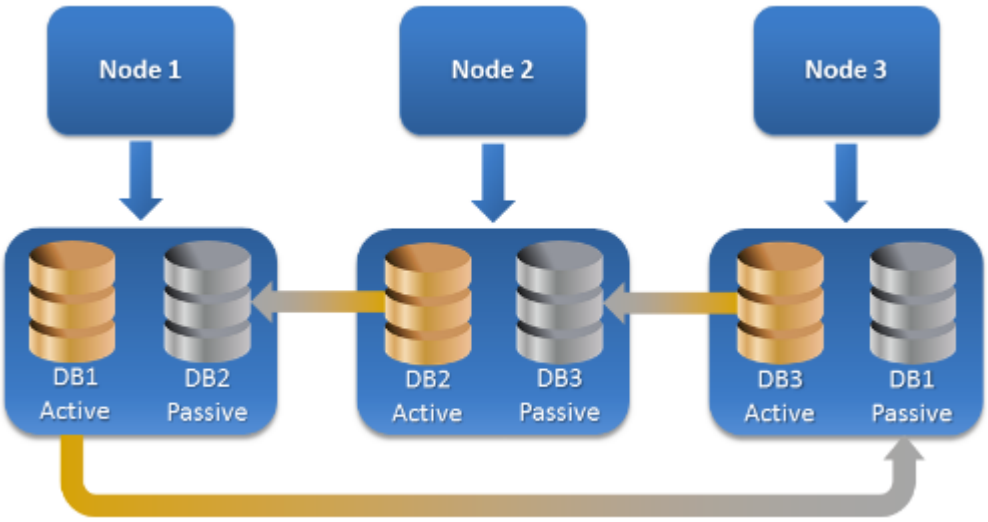
Sauvegarde prenant en charge les clusters

Grâce à la sauvegarde prenant en charge les clusters, vous sauvegardez seulement une copie des données du cluster. Si les données changent d'emplacement au sein du cluster (en raison d'un déplacement ou d'un basculement), le logiciel fait le suivi de toutes les relocalisations de ces données et les sauvegarde en toute sécurité.

Configurations de cluster prises en charge

La sauvegarde prenant en charge les clusters est prise en charge *uniquement* pour Database Availability Group (DAG) dans Exchange Server 2010 ou des versions plus récentes. Les autres configurations de cluster, comme Single Copy Cluster (SCC) et Cluster Continuous Replication (CCR) pour Exchange 2007 *ne sont pas* prises en charge.

DAG est un groupe pouvant contenir jusqu'à 16 serveurs de boîtes aux lettres Exchange. N'importe quel nœud peut accueillir une copie de base de données de boîtes aux lettres provenant de n'importe quel autre nœud. Chaque nœud peut héberger des copies de bases de données passives et actives. Jusqu'à 16 copies de chaque base de données peuvent être créées.



Combien d'agents sont nécessaires pour la sauvegarde et la restauration prenant en charge les clusters ?

Pour assurer le succès de la sauvegarde et de la restauration de bases de données en cluster, l'agent pour Exchange doit être installé sur chaque nœud du cluster Exchange.

Remarque
Une fois que vous avez installé l'agent sur l'un des nœuds, la console Cyber Protect affiche le DAG et ses nœuds sous **Terminaux** > **Microsoft Exchange** > **Bases de données**. Pour installer Agents pour Exchange sur les autres nœuds, sélectionnez le DAG et cliquez sur **Détails**, puis sur **Installer un agent** en regard de chaque nœud.

Sauvegarde des données de cluster Exchange

1. Lors de la création d'un plan de protection, sélectionnez le DAG comme décrit dans "Sélection de données Exchange Server" (p. 590).
2. Configurez l'option de sauvegarde "Mode de sauvegarde de cluster" (p. 478).
3. Spécifiez les autres paramètres du plan de protection, le cas échéant.

Important
Pour la sauvegarde prenant en compte les clusters, assurez-vous de bien sélectionner le DAG. Si vous sélectionnez des noeuds individuels ou des bases de données au sein du DAG, seuls les éléments sélectionnés seront sauvegardés et l'option **Mode de sauvegarde de cluster** sera ignorée.

Restauration des données du cluster Exchange

1. Sélectionnez le point de récupération de la base de données que vous voulez restaurer. Si ça n'est pas possible, sélectionnez un cluster complet pour la restauration.
   Quand vous sélectionnez la copie d'une base de données en cluster sous **Terminaux** > **Microsoft Exchange** > **Bases de données** > `<nom du cluster>` > `<nom du nœud` et cliquez sur **Restaurer**, le logiciel n'affiche que les points de récupération correspondant aux fois où la copie a été sauvegardée.
   La façon la plus simple d'afficher tous les points de récupération d'une base de données en cluster est de sélectionner sa sauvegarde dans l'onglet Stockage de sauvegarde.
2. Suivez les étapes décrites dans "Restauration de bases de données Exchange" (p. 609) à partir de l'étape 5.
   Le logiciel définit automatiquement un nœud cluster vers lequel les données seront restaurées. Le nom du nœud est affiché dans le champ **Récupérer vers**. Vous pouvez modifier le nœud cible manuellement.

Sauvegarde reconnaissant les applications

La sauvegarde de niveau disque reconnaissant les applications est disponible pour les machines physiques, les machines virtuelles ESXi et les machines virtuelles Hyper-V.

Lorsque vous sauvegardez une machine exécutant Microsoft SQL Server, Microsoft Exchange Server ou les services de domaine Active Directory, activez la **Sauvegarde d'application** pour une protection renforcée des données de ces applications.

Pourquoi utiliser la sauvegarde reconnaissant les applications ?

En utilisant la sauvegarde reconnaissant les applications, vous vous assurez que :

- Les applications sont sauvegardées dans un état cohérent et sont donc immédiatement disponibles après la restauration de la machine.
- Vous pouvez restaurer les bases de données, boîtes aux lettres et éléments de boîte aux lettres SQL et Exchange sans restaurer l'intégralité de la machine.
- Les fichiers journaux des transactions SQL sont tronqués après chaque sauvegarde réussie. La troncation de journal SQL peut être désactivée dans les options du plan de protection. Les fichiers journaux des transactions Exchange sont tronqués sur les machines virtuelles uniquement. Vous pouvez activer l'option de sauvegarde complète VSS si vous souhaitez tronquer les fichiers journaux des transactions Exchange sur une machine physique.
- Si un domaine comprend plusieurs contrôleurs de domaine et que vous en restaurez un, une restauration ne faisant pas autorité est effectuée et une restauration USN n'a pas lieu par la suite.

De quoi ai-je besoin pour utiliser la sauvegarde reconnaissant les applications ?

Sur une machine physique, l'agent pour SQL et/ou l'agent pour Exchange doivent être installés, en plus de l'agent pour Windows.

Sur une machine virtuelle, aucun agent d'installation n'est nécessaire ; on suppose que la machine est sauvegardée par l'agent pour VMware (Windows) ou l'agent pour Hyper-V.

Remarque
Pour les machines virtuelles Hyper-V et VMware ESXi exécutant Windows Server 2022, la sauvegarde reconnaissant les applications n'est pas prise en charge en mode sans agent, c'est-à-dire lorsque la sauvegarde est effectuée respectivement par l'agent pour Hyper-V et par l'agent pour VMware. Pour protéger les applications Microsoft sur ces ordinateurs, installez l'agent pour Windows dans le système d'exploitation invité.

L'agent pour VMware (appliance virtuelle) peut créer des sauvegardes reconnaissant les applications, mais il ne peut pas restaurer de données d'application provenant de ces sauvegardes. Pour restaurer des données d'application à partir de sauvegardes créées par cet agent, vous avez besoin d'un agent pour VMware (Windows), d'un agent pour SQL ou d'un agent pour Exchange sur une machine ayant accès à l'emplacement sur lequel les sauvegardes ont été stockées. Lors de la configuration de la restauration de données d'application, sélectionnez le point de récupération sur l'onglet **Stockage de sauvegarde**, puis sélectionnez cette machine dans **Machine à parcourir**.

Les autres critères sont répertoriés dans les sections « Prérequis » et « Droits utilisateurs requis ».

Remarque
Les sauvegardes reconnaissant les applications des machines virtuelles Hyper-V peuvent échouer avec l'erreur « La commande ExecQuery de WMI n'a pas réussi l'exécution de la demande. » ou « Échec de création d'un nouveau processus via WMI » si les sauvegardes sont exécutées sur un hôte présentant une charge élevée en raison de l'absence de réponse ou d'un retard de réponse depuis Windows Management Instrumentation. Retentez ces sauvegardes dans un créneau horaire où la charge sur l'hôte est réduite.

Droits utilisateur requis pour les sauvegardes reconnaissant les applications

Une sauvegarde reconnaissant les applications comprend des métadonnées d'applications compatibles VSS présentes sur le disque. Pour accéder à ces métadonnées, l'agent nécessite un compte avec les droits appropriés, répertoriés ci-dessous. Vous êtes invité à indiquer ce compte lors de l'activation de la sauvegarde d'applications.

- Pour SQL Server :
  Le compte doit être membre du groupe **Opérateurs de sauvegarde** ou **Administrateurs** sur l'ordinateur et membre du rôle **sysadmin** sur chacune des instances que vous allez sauvegarder.

  Remarque
  Seule l'authentification Windows est prise en charge.

- Pour Exchange Server :
  Exchange 2007 : Le compte doit être un membre du groupe **Administrateurs** sur la machine, et un membre du groupe de rôles **Gestion d'organisation Exchange**.
  Exchange 2010 et versions ultérieures : Le compte doit être un membre du groupe **Administrateurs** sur la machine, et un membre du groupe de rôles **Gestion d'organisation**.
- Pour Active Directory :
  Le compte doit être un administrateur de domaine.

Exigences supplémentaires pour les machines virtuelles

Si l'application s'exécute sur une machine virtuelle sauvegardée par l'agent pour VMware ou l'agent pour Hyper-V, assurez-vous que le contrôle de compte utilisateur (CCU) est désactivé sur la machine.

Si vous ne souhaitez pas désactiver le CCU, vous devez fournir les identifiants de l'administrateur de domaine intégré (DOMAIN\Administrator) lors de l'activation d'une sauvegarde d'application.

Remarque
Utilisez le compte administrateur du domaine intégré qui a été configuré lors de la création du domaine. Les comptes créés plus tard ne sont pas pris en charge.

Exigences supplémentaires pour les ordinateurs exécutant Windows

Pour toutes les versions Windows, vous devez désactiver les politiques de contrôle de compte utilisateur (CCU) afin d'autoriser les sauvegardes reconnaissant les applications.

Si vous ne souhaitez pas désactiver le CCU, vous devez fournir les identifiants de l'administrateur de domaine intégré (DOMAIN\Administrator) lors de l'activation d'une sauvegarde d'application.

Remarque
Utilisez le compte administrateur du domaine intégré qui a été configuré lors de la création du domaine. Les comptes créés plus tard ne sont pas pris en charge.

Pour désactiver les politiques CCU dans Windows

1. Dans l'Éditeur de la base de registre, localisez la clé de la base de registre suivante : `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`
2. Modifiez la valeur **EnableLUA** et définissez-la sur **0**.
3. Redémarrez la machine.

Sauvegarde de boîte de réception

La sauvegarde des boîtes aux lettres est prise en charge pour Microsoft Exchange Server 2010 Service Pack 1 (SP1) et version ultérieure.

La sauvegarde de boîte aux lettres est disponible si au moins un agent pour Exchange est enregistré sur le serveur de gestion. L'agent doit être installé sur une machine appartenant à la même forêt Active Directory que Microsoft Exchange Server.

Avant de sauvegarder des boîtes aux lettres, vous devez connecter l'agent pour Exchange à la machine exécutant le **serveur d'Accès Client** (CAS) de Microsoft Exchange Server. Dans Exchange 2016 et les versions ultérieures, le rôle CAS n'est pas disponible en tant qu'option d'installation séparée. Il est automatiquement installé dans le cadre du rôle serveur de boîtes aux lettres. Ainsi, vous pouvez connecter l'agent à n'importe quel serveur exécutant le **rôle de boîte aux lettres**.

Remarque
Vous pouvez restaurer les boîtes aux lettres et les éléments de boîte aux lettres également depuis des sauvegardes de bases de données et des sauvegardes reconnaissant les applications. Pour plus d'informations, voir "Restauration de boîtes aux lettres et éléments de boîtes aux lettres Exchange" (p. 612). Les sauvegardes de bases de données et les sauvegardes reconnaissant les applications ne vous permettent pas de créer des plans de protection pour des boîtes aux lettres indépendantes.

Pour connecter l'agent pour Exchange au CAS

1. Cliquez sur **Terminaux** > **Ajouter**.
2. Cliquez sur **Microsoft Exchange Server**.

3. Cliquez sur **Boîtes aux lettres Exchange**.

   S'il n'y a pas d'agent pour Exchange enregistré sur le serveur de gestion, le logiciel vous propose d'installer l'agent. Après l'installation, répétez cette procédure à partir de l'étape 1.
4. [Facultatif] Si plusieurs agents pour Exchange sont enregistrés sur le serveur de gestion, cliquez sur **Agent**, puis sélectionnez l'agent qui exécutera la sauvegarde.
5. Dans le **serveur d'accès client**, spécifiez le nom de domaine qualifié complet (FQDN) de la machine où le rôle **Accès Client** de Microsoft Exchange Server est activé.

   Dans Exchange 2016 et les versions ultérieures, les services d'accès au client sont automatiquement installés dans le cadre du rôle serveur de boîtes aux lettres. Ainsi, vous pouvez spécifier n'importe quel serveur exécutant le **rôle de boîte aux lettres**. Nous nous référons à ce serveur en tant que CAS plus loin dans cette section.
6. Dans **Type d'authentification**, sélectionnez le type d'authentification utilisé par le CAS. Vous pouvez sélectionner **Kerberos** (par défaut) ou **Basic**.
7. [Uniquement pour une authentification basique] Sélectionnez le protocole à utiliser. Vous pouvez sélectionner **HTTPS** (par défaut) ou **HTTP**.
8. [Uniquement pour une authentification basique avec le protocole HTTPS] Si le CAS utilise un certificat SSL obtenu à partir d'une autorité de certification, il faut que le logiciel vérifie le certificat SSL lors de la connexion au CAS. Pour cela, cochez **Vérifier le certificat SSL**. Sinon, ignorez cette étape.
9. Fournissez les informations d'identification d'un compte qui sera utilisé pour accéder au CAS. Les exigences pour ce compte sont répertoriées dans « Droits utilisateurs requis ».
10. Cliquez sur **Ajouter**.

Ainsi, les boîtes aux lettres apparaissent sous **Terminaux** > **Microsoft Exchange** > **Boîtes aux lettres**.

Sélectionner les boîtes aux lettres Exchange Server

Sélectionnez les boîtes aux lettres comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Pour sélectionner les boîtes aux lettres Exchange

1. Cliquez sur **Terminaux** > **Microsoft Exchange**.

   Le logiciel affiche l'arborescence des bases de données et boîtes aux lettres Exchange Server.
2. Cliquez sur **Boîtes aux lettres**, puis sélectionnez les boîtes aux lettres que vous voulez sauvegarder.
3. Cliquez sur **Protection**.

Droits utilisateurs requis

Pour accéder aux boîtes aux lettres, l'agent pour Exchange nécessite un compte doté des droits appropriés. Vous êtes invité à indiquer ce compte lors de la configuration de différentes opérations avec les boîtes aux lettres.

L'appartenance du compte au groupe de rôles **Gestion d'organisation** permet d'accéder à n'importe quelle boîte aux lettres, y compris celles créées à l'avenir.

Les droits utilisateurs minimums requis sont les suivants :

- Le compte doit être un membre du groupe de rôles **Gestion des serveurs** et **Gestion des destinataires**.
- Le compte doit avoir le rôle de gestion **ApplicationImpersonation** activé pour tous les utilisateurs ou groupes d'utilisateurs possédant les boîtes aux lettres auxquelles accédera l'agent.
  Pour en savoir plus sur la configuration du rôle de gestion **ApplicationImpersonation**, consultez l'article suivant de base de connaissances Microsoft : https://msdn.microsoft.com/en-us/library/office/dn722376.aspx.

Restauration de bases de données SQL

Vous pouvez restaurer les bases de données SQL depuis des sauvegardes de base de données et des sauvegardes reconnaissant les applications. Pour plus d'informations sur la différence entre les deux types de sauvegarde, voir "Protection des serveurs Microsoft SQL Server et Microsoft Exchange Server" (p. 585).

Vous pouvez restaurer les bases de données SQL vers l'instance d'origine, vers une autre instance sur l'ordinateur d'origine ou vers une instance sur un ordinateur différent de l'ordinateur d'origine. Lorsque vous effectuez une reprise vers un ordinateur différent de l'ordinateur d'origine, l'agent pour SQL doit être installé sur la machine cible.

Vous pouvez également restaurer les bases de données sous forme de fichiers.

Si vous utilisez l'authentification Windows pour l'instance SQL, vous devrez fournir les identifiants d'un compte membre du groupe **Opérateurs de sauvegarde** ou **Administrateurs** sur l'ordinateur, et membre du rôle **sysadmin** sur l'instance cible. Si vous utilisez l'authentification SQL Server, vous devez fournir les identifiants d'un compte membre du rôle **sysadmin** sur l'instance cible.

Les bases de données système sont restaurées en tant que bases de données utilisateur, avec certaines distinctions. Pour en savoir plus sur ces distinctions, voir "Restauration des bases de données système" (p. 608).

Lors d'une reprise, vous pouvez vérifier la progression de l'opération dans la console Cyber Protect, dans l'onglet **Surveillance** > **Activités**.

Restauration de bases de données SQL vers l'ordinateur d'origine

Vous pouvez restaurer les bases de données SQL vers leur instance d'origine, vers une autre instance sur l'ordinateur d'origine ou vers une instance sur une machine cible différente de la machine d'origine.

Pour restaurer des bases de données SQL vers l'ordinateur d'origine

À partir d'une sauvegarde de base de données

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Microsoft SQL**.
2. Sélectionnez l'instance SQL Server ou cliquez sur le nom de l'instance pour sélectionner les bases de données spécifiques que vous souhaitez restaurer, puis cliquez sur **Reprise**.

   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Pour restaurer les données vers une machine différente de la machine d'origine, voir "Restauration de bases de données SQL vers un ordinateur différent de l'ordinateur d'origine" (p. 603).
3. Sélectionnez un point de restauration.

   Les points de reprise sont filtrés en fonction de leur emplacement.
4. Cliquez sur **Restaurer** > **Bases de données vers une instance**.

   Par défaut, l'instance et les bases de données sont restaurées vers les machines d'origine. Vous pouvez également restaurer une base de données d'origine comme nouvelle base de données.
5. [Lors de la restauration vers une instance différente de l'instance d'origine sur la même machine] Cliquez sur **Instance SQL Server cible**, sélectionnez l'instance cible, puis cliquez sur **Terminé**.
6. [Lors de la restauration d'une base de données en tant que nouvelle base de données] Cliquez sur le nom de la base de données, puis, dans **Restaurer vers**, sélectionnez **Nouvelle base de données**.
   - Spécifiez le nom de la nouvelle base de données.
   - Spécifiez le chemin d'accès de la nouvelle base de données.
   - Spécifiez le chemin d'accès du journal.
7. [Facultatif] [Non disponible lors de la de la restauration d'une base de données en tant que nouvelle base de données] Pour changer l'état d'une base de données après reprise, cliquez sur le nom de la base de données, choisissez l'un des états suivants et cliquez sur **Terminé**.
   - **Prête à l'emploi (RESTORE WITH RECOVERY)** (par défaut)

     Après l'achèvement de la restauration, la base de données sera prête à l'emploi. Les utilisateurs y auront un accès complet. Le logiciel restaurera toutes les transactions non validées de la base de données restaurée qui sont stockées dans les journaux des transactions. Vous ne pourrez pas restaurer des journaux des transactions supplémentaires à partir des sauvegardes natives de Microsoft SQL.
   - **Non-opérationnelle (RESTORE WITH NORECOVERY)**

     Après l'achèvement de la restauration, la base de données sera non-opérationnelle. Les utilisateurs n'y auront aucun accès. Le logiciel conservera toutes les transactions non validées de la base de données restaurée. Vous pourrez restaurer des journaux des transactions supplémentaires à partir des sauvegardes natives de Microsoft SQL et ainsi atteindre le point de restauration nécessaire.
   - **En lecture seule (RESTORE WITH STANDBY)**

     Après l'achèvement de la restauration, les utilisateurs auront accès en lecture seule à la base de données. Le logiciel annulera les transactions non validées. Toutefois, il enregistrera les actions d'annulation dans un fichier de secours temporaire afin que les effets de la restauration puissent être annulés.

Cette valeur est principalement utilisée pour détecter le moment dans le temps où une erreur SQL Server s'est produite.

8. Cliquez sur **Démarrer la récupération**.

À partir d'une sauvegarde reconnaissant les applications

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez l'ordinateur qui contenait à l'origine les données que vous souhaitez restaurer, puis cliquez sur **Reprise**.

   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Pour restaurer les données vers une machine différente de la machine d'origine, voir "Restauration de bases de données SQL vers un ordinateur différent de l'ordinateur d'origine" (p. 603).
3. Sélectionnez un point de restauration.

   Les points de reprise sont filtrés en fonction de leur emplacement.
4. Cliquez sur **Restaurer** > **Bases de données SQL**.
5. Sélectionnez l'instance SQL Server ou cliquez sur le nom de l'instance pour sélectionner les bases de données spécifiques que vous souhaitez restaurer, puis cliquez sur **Restaurer**.

   Par défaut, l'instance et les bases de données sont restaurées vers les machines d'origine. Vous pouvez également restaurer une base de données d'origine comme nouvelle base de données.
6. [Lors de la restauration vers une instance différente de l'instance d'origine sur la même machine] Cliquez sur **Instance SQL Server cible**, sélectionnez l'instance cible, puis cliquez sur **Terminé**.
7. [Lors de la restauration d'une base de données en tant que nouvelle base de données] Cliquez sur le nom de la base de données, puis, dans **Restaurer vers**, sélectionnez **Nouvelle base de données**.
   - Spécifiez le nom de la nouvelle base de données.
   - Spécifiez le chemin d'accès de la nouvelle base de données.
   - Spécifiez le chemin d'accès du journal.
8. [Facultatif] [Non disponible lors de la de la restauration d'une base de données en tant que nouvelle base de données] Pour changer l'état d'une base de données après reprise, cliquez sur le nom de la base de données, choisissez l'un des états suivants et cliquez sur **Terminé**.
   - **Prête à l'emploi (RESTORE WITH RECOVERY)** (par défaut)

     Après l'achèvement de la restauration, la base de données sera prête à l'emploi. Les utilisateurs y auront un accès complet. Le logiciel restaurera toutes les transactions non validées de la base de données restaurée qui sont stockées dans les journaux des transactions. Vous ne pourrez pas restaurer des journaux des transactions supplémentaires à partir des sauvegardes natives de Microsoft SQL.
   - **Non-opérationnelle (RESTORE WITH NORECOVERY)**

     Après l'achèvement de la restauration, la base de données sera non-opérationnelle. Les utilisateurs n'y auront aucun accès. Le logiciel conservera toutes les transactions non validées de la base de données restaurée. Vous pourrez restaurer des journaux des transactions

supplémentaires à partir des sauvegardes natives de Microsoft SQL et ainsi atteindre le point de restauration nécessaire.

- **En lecture seule (RESTORE WITH STANDBY)**

  Après l'achèvement de la restauration, les utilisateurs auront accès en lecture seule à la base de données. Le logiciel annulera les transactions non validées. Toutefois, il enregistrera les actions d'annulation dans un fichier de secours temporaire afin que les effets de la restauration puissent être annulés.

  Cette valeur est principalement utilisée pour détecter le moment dans le temps où une erreur SQL Server s'est produite.

9. Cliquez sur **Démarrer la récupération**.

Restauration de bases de données SQL vers un ordinateur différent de l'ordinateur d'origine

Vous pouvez restaurer les sauvegardes reconnaissant les applications et les sauvegardes de bases de données dans des instances SQL Server sur des machines cibles différentes des ordinateurs d'origine sur lesquelles l'agent pour SQL est installé. Les sauvegardes doivent être localisées dans le stockage dans le cloud ou dans un stockage partagé accessible par la machine cible.

La version SQL Server sur la machine cible doit être identique à la version sur la machine source ou plus récente.

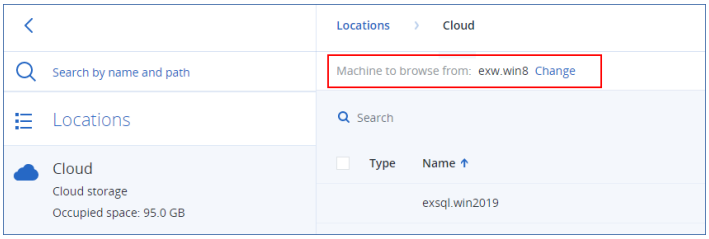
Pour restaurer les bases de données SQL vers un ordinateur différent de l'ordinateur d'origine

Depuis le stockage des sauvegardes

Cette procédure s'applique aux sauvegardes reconnaissant les applications et aux sauvegardes de bases de données.

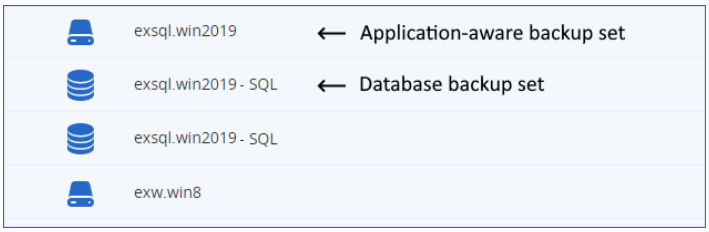
1. Sur la console Cyber Protect, accédez à **Stockage de sauvegarde**.
2. Sélectionnez l'emplacement de l'ensemble de sauvegardes à partir duquel vous souhaitez restaurer des données.
3. Dans **Machine à parcourir**, sélectionnez la machine cible.

   Il s'agit de la machine sur laquelle vous allez restaurer les données. La machine cible doit être en ligne.



4. Sélectionnez l'ensemble de sauvegardes et, dans le volet **Actions**, cliquez sur **Afficher les sauvegardes**.

   Les ensembles de sauvegardes reconnaissant les applications et les ensembles de sauvegardes de bases de données ont des icônes différentes.



5. Sélectionnez la point de reprise à partir duquel vous souhaitez restaurer des données.
6. [Pour les sauvegardes de base de données] Cliquez sur **Restaurer les bases de données SQL**.
7. [Pour les sauvegardes reconnaissant les applications] Cliquez sur **Restaurer** > **Bases de données SQL**.
8. Sélectionnez l'instance SQL Server ou cliquez sur le nom de l'instance pour sélectionner les bases de données spécifiques que vous souhaitez restaurer, puis cliquez sur **Restaurer**.
9. [Si la machine cible comprend plusieurs instances SQL] Cliquez sur **Instance SQL Server cible**, sélectionnez l'instance cible, puis cliquez sur **Terminé**.
10. Cliquez sur le nom de la base de données, spécifiez le chemin d'accès de la nouvelle base de données et des fichiers journaux, puis cliquez sur **Terminé**.

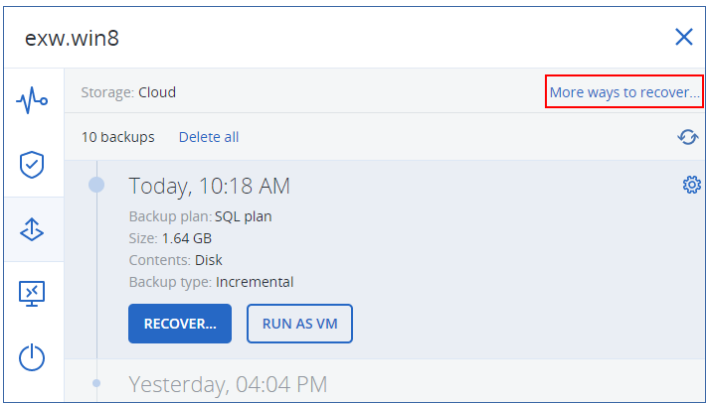
    Vous pouvez indiquer le même chemin d'accès dans les deux champs, par exemple :

    ```
    C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
    ```
11. Cliquez sur **Démarrer la récupération**.

À partir de terminaux

Cette procédure ne s'applique qu'aux sauvegardes reconnaissant les applications.

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez l'ordinateur qui contenait à l'origine les données que vous souhaitez restaurer, puis cliquez sur **Reprise**.
3. [Si la machine source est en ligne] Cliquez sur **Autres méthodes de restauration**.



4. Cliquez sur **Sélectionner la machine** pour sélectionner la machine cible, puis cliquez sur **OK**.

   Il s'agit de la machine sur laquelle vous allez restaurer les données. La machine cible doit être en ligne.
5. Sélectionnez un point de restauration.

Les points de reprise sont filtrés en fonction de leur emplacement.

6. Cliquez sur **Restaurer** > **Bases de données SQL**.
7. Sélectionnez l'instance SQL Server ou cliquez sur le nom de l'instance pour sélectionner les bases de données spécifiques que vous souhaitez restaurer, puis cliquez sur **Restaurer**.
8. [Si la machine cible comprend plusieurs instances SQL] Cliquez sur **Instance SQL Server cible**, sélectionnez l'instance cible, puis cliquez sur **Terminé**.
9. Cliquez sur le nom de la base de données, spécifiez le chemin d'accès de la nouvelle base de données et des fichiers journaux, puis cliquez sur **Terminé**.

   Vous pouvez indiquer le même chemin d'accès dans les deux champs, par exemple :

   ```
   C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
   ```

10. Cliquez sur **Démarrer la récupération**.

Restauration de bases de données SQL sous forme de fichiers

Vous pouvez restaurer les bases de données sous forme de fichiers. Cette option peut être utile si vous devez extraire des données pour l'exploration de données, un audit ou tout autre traitement ultérieur effectué par des outils tiers. Pour savoir comment joindre les fichiers de base de données SQL à une instance SQL Server, voir "Attacher des bases de données SQL Server" (p. 608).

Vous pouvez restaurer les bases de données sous forme de fichiers sur l'ordinateur d'origine ou sur d'autres ordinateurs sur lesquels l'agent pour SQL est installé. Lorsque vous restaurez des données sur d'autres ordinateurs que l'ordinateur d'origine, les sauvegardes doivent être localisées dans le stockage dans le cloud ou dans un stockage partagé accessible par la machine cible.

Remarque
La restauration de bases de données sous forme de fichiers est la seule méthode de reprise disponible si vous utilisez l'agent pour VMware (Windows). La restauration de bases de données à l'aide de l'agent pour VMware (appliance virtuelle) n'est pas possible.

Pour restaurer des bases de données SQL sous forme de fichiers

À partir d'une sauvegarde de base de données

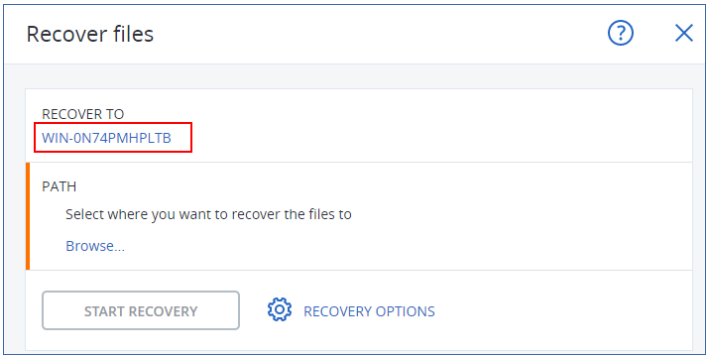
Cette procédure s'applique aux machines sources en ligne.

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Microsoft SQL**.
2. Sélectionnez les bases de données que vous souhaitez restaurer, puis cliquez sur **Reprise**.
3. Sélectionnez un point de restauration.

   Les points de reprise sont filtrés en fonction de leur emplacement.
4. Cliquez sur **Restaurer** > **Bases de données en tant que fichiers**.
5. [Lorsque de la restauration sur un ordinateur différent de l'ordinateur d'origine] Dans **Restaurer vers**, sélectionnez la machine cible.

Il s'agit de la machine sur laquelle vous allez restaurer les données. La machine cible doit être en ligne.

Pour modifier la sélection, cliquez sur le nom de l'ordinateur, sélectionnez un autre ordinateur, puis cliquez sur **OK**.



6. Dans **Chemin d'accès**, cliquez sur **Parcourir**, sélectionnez un dossier local ou réseau dans lequel enregistrer les fichiers, puis cliquez sur **Terminé**.
7. Cliquez sur **Démarrer la récupération**.

À partir d'une sauvegarde reconnaissant les applications

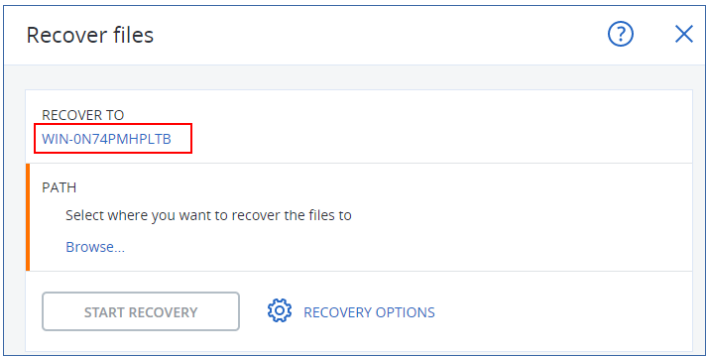
Cette procédure s'applique aux machines sources en ligne.

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez l'ordinateur qui contenait à l'origine les données que vous souhaitez restaurer, puis cliquez sur **Reprise**.
3. Sélectionnez un point de restauration.

   Les points de reprise sont filtrés en fonction de leur emplacement.
4. Cliquez sur **Restaurer** > **Bases de données SQL**, sélectionnez les bases de données que vous souhaitez restaurer, puis cliquez sur **Restaurer en tant que fichiers**.
5. [Lorsque de la restauration sur un ordinateur différent de l'ordinateur d'origine] Dans **Restaurer vers**, sélectionnez la machine cible.

   Il s'agit de la machine sur laquelle vous allez restaurer les données. La machine cible doit être en ligne.

   Pour modifier la sélection, cliquez sur le nom de l'ordinateur, sélectionnez un autre ordinateur, puis cliquez sur **OK**.

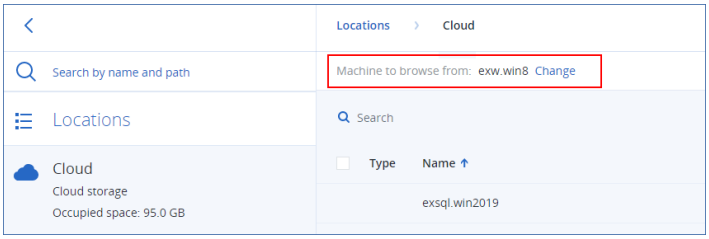


6. Dans **Chemin d'accès**, cliquez sur **Parcourir**, sélectionnez un dossier local ou réseau dans lequel enregistrer les fichiers, puis cliquez sur **Terminé**.
7. Cliquez sur **Démarrer la récupération**.

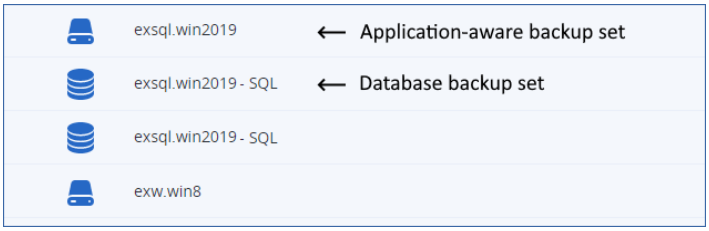
À partir d'une sauvegarde sur un ordinateur hors ligne

Cette procédure s'applique aux sauvegardes reconnaissant les applications et aux sauvegardes de bases de données sur les machines sources hors ligne.

1. Sur la console Cyber Protect, accédez à **Stockage de sauvegarde**.
2. Sélectionnez l'emplacement de l'ensemble de sauvegardes à partir duquel vous souhaitez restaurer des données.
3. Dans **Machine à parcourir**, sélectionnez la machine cible.
   Il s'agit de la machine sur laquelle vous allez restaurer les données. La machine cible doit être en ligne.



4. Sélectionnez l'ensemble de sauvegardes et, dans le volet **Actions**, cliquez sur **Afficher les sauvegardes**.
   Les ensembles de sauvegardes reconnaissant les applications et les ensembles de sauvegardes de bases de données ont des icônes différentes.



5. Sélectionnez la point de reprise à partir duquel vous souhaitez restaurer des données.
6. [Pour les sauvegardes de base de données] Cliquez sur **Restaurer les bases de données SQL**.
7. [Pour les sauvegardes reconnaissant les applications] Cliquez sur **Restaurer** > **Bases de données SQL**.
8. Sélectionnez l'instance SQL Server ou cliquez sur le nom de l'instance pour sélectionner les bases de données spécifiques que vous souhaitez restaurer, puis cliquez sur **Restaurer en tant que fichiers**.
9. Dans **Chemin d'accès**, cliquez sur **Parcourir**, sélectionnez un dossier local ou réseau dans lequel enregistrer les fichiers, puis cliquez sur **Terminé**.
10. Cliquez sur **Démarrer la récupération**.

Restauration des bases de données système

Toutes les bases de données système d'une même instance sont restaurées en une seule fois. Lors de la restauration de bases de données système, le logiciel redémarre automatiquement l'instance de destination dans le mode mono-utilisateur. Une fois la restauration terminée, le logiciel redémarre l'instance et restaure d'autres bases de données (le cas échéant).

Autres points à considérer lors de la restauration de bases de données système :

- Les bases de données système ne peuvent être restaurées que sur une instance de la même version que l'instance d'origine.
- Les bases de données système sont toujours restaurées dans l'état « prête à l'emploi ».

Restauration de la base de données MASTER

Les bases de données système contiennent la base de données **MASTER**. La base de données **MASTER** enregistre les informations sur toutes les bases de données de l'instance. Par conséquent, la base de données **MASTER** dans la sauvegarde contient des informations à propos des bases de données qui existaient dans l'instance au moment de la sauvegarde. Après la restauration de la base de données **MASTER**, vous devrez peut-être effectuer les opérations suivantes :

- Les bases de données qui sont apparues dans l'instance après que la sauvegarde a été effectuée ne sont pas visibles par l'instance. Pour amener ces bases de données en production, attachez-les manuellement à l'instance, en utilisant SQL Server Management Studio.
- Les bases de données qui ont été supprimées après que la sauvegarde a été effectuée sont affichées comme hors ligne dans l'instance. Supprimez ces bases de données en utilisant SQL Server Management Studio.

Attacher des bases de données SQL Server

Cette section décrit comment attacher une base de données dans SQL Server en utilisant SQL Server Management Studio. Une seule base de données peut être attachée à la fois.

Attacher une base de données requiert une des autorisations suivantes : **CREATE DATABASE**, **CREATE ANY DATABASE** ou **ALTER ANY DATABASE**. Normalement, ces autorisations sont accordées au rôle **sysadmin** de l'instance.

Pour attacher une base de données

1. Lancez Microsoft SQL Server Management Studio.
2. Connectez-vous à l'instance SQL Server, puis développez l'instance.
3. Cliquez avec le bouton droit de la souris sur **Bases de données** et cliquez sur **Attacher**.
4. Cliquez sur **Ajouter**.
5. Dans la boîte de dialogue **Localiser les fichiers de base de données**, trouvez et sélectionnez le fichier .mdf de la base de données.

6. Dans la section **Détails de la base de données**, assurez-vous que le reste des fichiers de base de données (fichiers .ndf et .ldf) sont trouvés.

   Détails. Les fichiers de base de données SQL Server peuvent ne pas être trouvés automatiquement si :

   - ils ne sont pas dans l'emplacement par défaut, ou ils ne sont pas dans le même dossier que le fichier de la base de données principale (.mdf). Solution : Spécifiez manuellement le chemin d'accès aux fichiers requis dans la colonne **Chemin d'accès du fichier actuel**.
   - Vous avez restauré un ensemble incomplet de fichiers qui composent la base de données. Solution : Restaurez les fichiers de base de données SQL Server manquants à partir de la sauvegarde.
7. Lorsque tous les fichiers sont trouvés, cliquez sur **OK**.

Restauration de bases de données Exchange

Cette section décrit la restauration depuis des sauvegardes de base de données et des sauvegardes reconnaissant les applications.

Vous pouvez restaurer des données Exchange Server sur un serveur Exchange actif. Il peut s'agir du serveur Exchange d'origine ou d'un serveur Exchange de la même version exécuté sur la machine avec le même nom de domaine complet (FQDN). L'agent pour Exchange doit être installé sur la machine.

Le tableau suivant résume les données d'Exchange Server que vous pouvez sélectionner pour leur restauration, ainsi que les droits d'utilisateur nécessaires pour effectuer cette tâche.

Version d'Exchange	Eléments de données	Droits utilisateur
2007	Groupes de stockage	Appartenance au groupe de rôles **Gestion d'organisation Exchange**.
2010/2013/2016/2019	Bases de données	Appartenance au groupe de rôles **Gestion de serveur**.

Parallèlement, vous pouvez restaurer les bases de données (groupes de stockage) en tant que fichiers. Les fichiers de bases de données, tout comme les fichiers journaux de transactions, seront extraits de la sauvegarde pour être placés dans le dossier de votre choix. Cela peut être utile si vous devez extraire des données pour un audit ou un autre traitement par des outils tiers, ou si la restauration échoue pour une raison quelconque et que vous recherchez une solution de rechange pour monter les bases de données manuellement.

Si vous utilisez uniquement l'agent pour VMware (Windows), la restauration de bases de données sous forme de fichiers est la seule méthode de restauration disponible. La restauration de bases de données à l'aide de l'agent pour VMware (appliance virtuelle) n’est pas possible.

Tout au long des procédures ci-après, nous utiliserons le terme « bases de données » pour se référer à la fois aux bases de données et aux groupes de stockage.

Pour restaurer des bases de données Exchange sur un serveur Exchange actif

1. Effectuez l'une des actions suivantes :
   - Lors d'une restauration à partir d'une sauvegarde reconnaissant les applications, sous **Terminaux**, sélectionnez la machine qui contenait à l'origine les données que vous voulez restaurer.
   - Lors d'une restauration à partir d'une sauvegarde de base de données, cliquez sur **Terminaux** > **Microsoft Exchange** > **Bases de données**, puis sélectionnez les bases de données que vous voulez restaurer.
2. Cliquez sur **Restauration**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Effectuez l'une des actions suivantes :
   - [Uniquement lors d'une restauration à partir d'une sauvegarde reconnaissant les applications]Si la sauvegarde est située sur le Cloud ou à un emplacement de stockage partagé (c'est-à-dire si d'autres agents peuvent y accéder), cliquez sur **Sélectionner une machine**, sélectionnez une machine en ligne avec Agent pour Exchange, puis choisissez un point de récupération.
   - Sélectionnez un point de récupération dans l'onglet Stockage de sauvegarde.

   La machine choisie pour la navigation dans l'une des actions ci-dessus devient une machine cible pour la récupération de données Exchange.
4. Effectuez l'une des actions suivantes :
   - Lors d'une restauration à partir d'une sauvegarde reconnaissant les applications, cliquez sur **Restaurer** > **Bases de données Exchange**, sélectionnez la base de données que vous souhaitez restaurer, puis cliquez sur **Restaurer**.
   - Lors d'une restauration depuis une sauvegarde de base de données, cliquez sur **Restaurer** > **Bases de données vers un serveur Exchange**.
5. Par défaut, les bases de données sont restaurées vers leur état d'origine. Si la base de données d'origine n'existe pas, elle sera recréée.

   Pour restaurer une base de données en tant que base de données différente :
   a. Cliquez sur le nom de la base de données.
   b. Dans **Restaurer vers**, sélectionnez **Nouvelle base de données**.
   c. Spécifiez le nom de la nouvelle base de données.
   d. Spécifiez le chemin de la nouvelle base de données et des fichiers journaux. Le dossier que vous spécifiez ne doit contenir ni la base de données initiale, ni les fichiers journaux.
6. Cliquez sur **Démarrer la récupération**.

La progression de la restauration sont affichées dans l'onglet Activités.

Pour restaurer des bases de données Exchange sous forme de fichiers

1. Effectuez l'une des actions suivantes :
   - Lors d'une restauration à partir d'une sauvegarde reconnaissant les applications, sous **Terminaux**, sélectionnez la machine qui contenait à l'origine les données que vous voulez restaurer.
   - Lors d'une restauration à partir d'une sauvegarde de base de données, cliquez sur **Terminaux** > **Microsoft Exchange** > **Bases de données**, puis sélectionnez les bases de données que vous voulez restaurer.
2. Cliquez sur **Restauration**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Effectuez l'une des actions suivantes :
   - [Uniquement lors d'une restauration à partir d'une sauvegarde reconnaissant les applications] Si la sauvegarde est située dans le Cloud ou à un emplacement de stockage partagé (c'est-à-dire si d'autres agents peuvent y accéder), cliquez sur **Sélectionner une machine**, sélectionnez une machine en ligne avec agent pour Exchange ou agent pour VMware, puis choisissez un point de récupération.
   - Sélectionnez un point de récupération dans l'onglet Stockage de sauvegarde.

   La machine choisie pour la navigation dans l'une des actions ci-dessus devient une machine cible pour la récupération de données Exchange.
4. Effectuez l'une des actions suivantes :
   - Lors d'une restauration à partir d'une sauvegarde reconnaissant les applications, cliquez sur **Restaurer** > **Bases de données Exchange**, sélectionnez la base de données que vous souhaitez restaurer, puis cliquez sur **Restaurer en tant que fichiers**.
   - Lors d'une restauration depuis une sauvegarde de base de données, cliquez sur **Restaurer** > **Bases de données en tant que fichiers**.
5. Cliquez sur **Parcourir**, puis sélectionnez un fichier local ou réseau où enregistrer les fichiers.
6. Cliquez sur **Démarrer la récupération**.

La progression de la restauration sont affichées dans l'onglet Activités.

Montage de bases de données Exchange Server

Après avoir restauré les fichiers de la base de données, vous pouvez mettre les bases de données en ligne en les montant. Le montage est exécuté en utilisant la console de gestion Exchange, le gestionnaire système Exchange ou l'environnement de ligne de commande Exchange Management Shell.

Les bases de données restaurées seront dans un état d'arrêt incorrect. Une base de données qui est dans un état d'arrêt incorrect peut être montée par le système si elle est restaurée sur son emplacement d'origine (cela signifie donc que les informations concernant la base de données d'origine sont présentes dans Active Directory). Lors de la restauration d'une base de données vers un autre emplacement (tel qu'une nouvelle base de données ou la base de données de

restauration), la base de données ne peut pas être montée tant qu'elle ne retourne pas dans un état d'arrêt normal à l'aide de la commande `Eseutil /r <Enn>`. <Enn> indique le préfixe du fichier journal pour la base de données (ou du groupe de stockage qui contient la base de données) dans laquelle vous devez appliquer les fichiers journaux des transactions.

Le compte que vous utilisez pour attacher une base de données doit être un délégué d'un rôle d'administrateur d'Exchange Server et d'un groupe d'administrateurs local sur le serveur cible.

Pour plus de détails sur la façon de monter des bases de données, reportez-vous aux articles suivants :

- Exchange 2010 ou versions plus récentes : http://technet.microsoft.com/en-us/library/aa998871.aspx
- Exchange 2007 : http://technet.microsoft.com/fr-fr/library/aa998871(v=EXCHG.80).aspx

Restauration de boîtes aux lettres et éléments de boîtes aux lettres Exchange

Vous pouvez restaurer des boîtes aux lettres et éléments de boîtes aux lettres Exchange à partir des sauvegardes suivantes :

- Sauvegardes de bases de données
- Sauvegardes reconnaissant les applications
- Sauvegardes de boîtes aux lettres

Vous pouvez restaurer les éléments suivants :

- Boîtes aux lettres (à l'exception des boîtes aux lettres archivées)
- Dossiers publics

> **Remarque**
> Disponible uniquement depuis les sauvegardes de base de données. Consultez "Sélection de données Exchange Server" (p. 590).

- Éléments de dossier Public
- Dossiers de courriers électroniques
- Messages de courriers électroniques
- Événements de calendrier
- Tâches
- Contacts
- Entrées de journal
- Notes

Vous pouvez utiliser la fonction de recherche pour trouver l'emplacement des éléments.

La ou les boîtes aux lettres peuvent être restaurée(s) sur Exchange Server en temps réel ou sur Microsoft 365.

Restauration sur Exchange Server

La restauration granulaire peut uniquement être réalisée sur Microsoft Exchange Server 2010 Service Pack 1 (SP1) et versions ultérieures. Il est possible que la sauvegarde source contienne des bases de données ou des boîtes aux lettres de toute autre version d'Exchange compatible.

La restauration granulaire peut être effectuée par l'agent pour Exchange ou l'agent pour VMware (Windows). Le serveur Exchange cible et la machine exécutant l'agent doivent appartenir à la même forêt Active Directory.

Lorsqu'une boîte aux lettres est restaurée sur une boîte aux lettres existante, les éléments existants dont les identifiants sont identiques sont écrasés.

La restauration des éléments de boîtes aux lettres n'écrase aucun élément. À la place, le chemin d'accès complet vers un élément de boîte aux lettres est recréé dans le dossier cible.

Exigences sur les comptes d'utilisateur

Une boîte aux lettres restaurée à partir d'une sauvegarde doit être associée à un compte d'utilisateur dans Active Directory.

Les boîtes aux lettres des utilisateurs et leur contenu peuvent être restaurés uniquement si les comptes d'utilisateur qui leur sont associés sont *activés*. Les boîtes aux lettres partagées, de salles et d'équipement peuvent être restaurées uniquement si leurs comptes d'utilisateur associés sont *désactivés*.

Une boîte aux lettres qui ne répond pas aux conditions énoncées ci-dessus est ignorée lors de la restauration.

Si certaines boîtes aux lettres sont ignorées, la restauration réussira avec des avertissements. Si toutes les boîtes aux lettres sont ignorées, la restauration échouera.

Restauration vers Microsoft 365

La récupération d'éléments de données Exchange vers Microsoft 365, et inversement, est prise en charge à la condition que l'agent pour Microsoft 365 soit installé localement.

La restauration peut être réalisée à partir de Microsoft Exchange Server 2010 et versions ultérieures.

Lorsqu'une boîte aux lettres est restaurée sur une boîte aux lettres Microsoft 365 existante, les éléments existants sont intacts et les éléments restaurés sont placés à leurs côtés.

Lors de la restauration d'une boîte aux lettres unique, vous devez d'abord sélectionner la boîte aux lettres Microsoft 365 cible. Lors de la restauration de plusieurs boîtes aux lettres en une seule opération de restauration, le logiciel essaiera de restaurer chaque boîte aux lettres vers la boîte aux lettres de l'utilisateur avec le même nom. Si l'utilisateur est introuvable, la boîte aux lettres est

ignorée. Si certaines boîtes aux lettres sont ignorées, la restauration réussira avec des avertissements. Si toutes les boîtes aux lettres sont ignorées, la restauration échouera.

Pour plus d'informations sur la restauration de Microsoft 365, consultez la section "Protection des données Microsoft 365" (p. 628).

Restauration de boîtes aux lettres

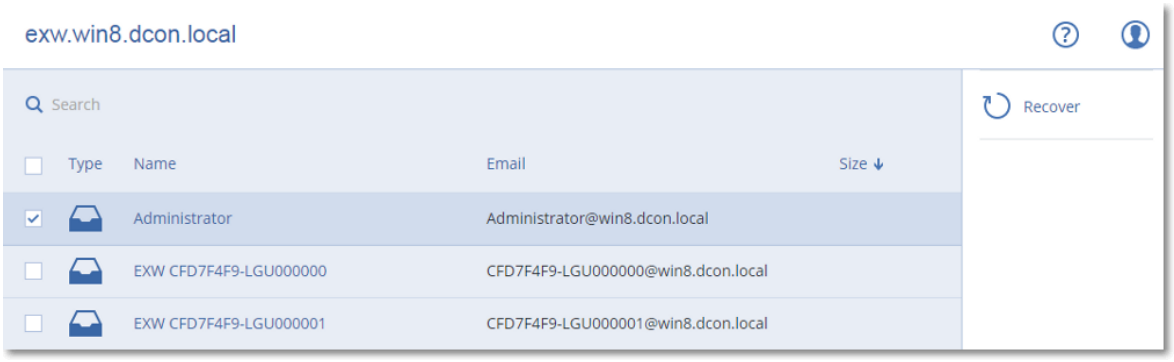
Pour restaurer des boîtes aux lettres à partir d'une sauvegarde de base de données ou d'une sauvegarde reconnaissant les applications

1. [Uniquement lors de la restauration à partir d'une sauvegarde de base de données vers Microsoft 365] Si l'agent pour Microsoft 365 n'est pas installé sur la machine exécutant Exchange Server qui était sauvegardée, effectuez l'une des actions suivantes :
   - S'il n'y a pas d'agent pour Microsoft 365 au sein de votre organisation, installez un agent pour Microsoft 365 sur la machine qui a été sauvegardée (ou sur une autre machine possédant la même version de Microsoft Exchange Server).
   - Si vous avez déjà un agent pour Microsoft 365 au sein de votre organisation, copiez des bibliothèques depuis la machine qui a été sauvegardée (ou à partir d'une autre machine possédant la même version de Microsoft Exchange Server) vers la machine avec l'agent pour Microsoft 365, comme décrit dans « Copier des bibliothèques Microsoft Exchange ».
2. Effectuez l'une des actions suivantes :
   - Lors d'une restauration à partir d'une sauvegarde reconnaissant les applications : sous **Terminaux**, sélectionnez la machine qui contenait à l'origine les données que vous voulez restaurer.
   - Lors d'une restauration à partir d'une sauvegarde de base de données, cliquez sur **Terminaux** > **Microsoft Exchange** > **Bases de données**, puis sélectionnez la base de données qui contenait à l'origine les données que vous voulez restaurer.
3. Cliquez sur **Restauration**.
4. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Utilisez d'autres méthodes de restauration :
   - [Uniquement lors d'une restauration à partir d'une sauvegarde reconnaissant les applications] Si la sauvegarde est située dans le Cloud ou à un emplacement de stockage partagé (c'est-à-dire si d'autres agents peuvent y accéder), cliquez sur **Sélectionner une machine**, sélectionnez une machine en ligne avec agent pour Exchange ou agent pour VMware, puis choisissez un point de récupération.
   - Sélectionnez un point de récupération dans l'onglet Stockage de sauvegarde.

   La machine choisie pour la navigation dans l'une des actions présentées ci-dessus effectuera la restauration des données à la place de la machine d'origine hors ligne.
5. Cliquez sur **Restaurer** > **Boîtes aux lettres Exchange**.
6. Sélectionnez les boîtes aux lettres que vous souhaitez restaurer.

Vous pouvez rechercher les boîtes aux lettres par nom. Les caractères génériques ne sont pas pris en charge.



7. Cliquez sur **Restaurer**.
8. [Uniquement lors de la restauration vers Microsoft 365] :
   a. Dans **Restaurer vers**, sélectionnez **Microsoft 365**.
   b. [Si vous avez sélectionné uniquement une boîte aux lettres à l'étape 6] Dans **Boîte aux lettres cible**, spécifiez la boîte aux lettres cible.
   c. Cliquez sur **Démarrer la récupération**.

   Les étapes suivantes de cette procédure ne sont pas nécessaires.

   Cliquez sur **Machine cible avec Microsoft Exchange Server** pour sélectionner ou modifier la machine cible. Cette étape permet la restauration d'une machine qui n'exécute par l'agent pour Exchange.

   Spécifiez le nom de domaine qualifié complet (FQDN) de la machine où le rôle **Accès client** (dans Microsoft Exchange Server 2010/2013) ou le **rôle de boîte aux lettres** (dans Microsoft Exchange Server 2016 ou version ultérieure) est activé. La machine doit appartenir à la même forêt Active Directory que la machine qui effectue la restauration.
9. Si vous y êtes invité, fournissez les informations d'identification d'un compte qui sera utilisé pour accéder à la machine. Les exigences pour ce compte sont répertoriées dans « Droits utilisateurs requis ».
10. [Facultatif] Cliquez sur **Base de données pour recréer toutes boîtes aux lettres manquantes** pour modifier la base de données automatiquement sélectionnée.
11. Cliquez sur **Démarrer la récupération**.

La progression de la restauration sont affichées dans l'onglet **Activités**.

Pour restaurer une boîte aux lettres à partir d'une sauvegarde de boîte aux lettres

1. Cliquez sur **Terminaux** > **Microsoft Exchange** > **Boîtes aux lettres**.
2. Sélectionnez la boîte aux lettres à restaurer, puis cliquez sur **Restaurer**.

   Vous pouvez rechercher les boîtes aux lettres par nom. Les caractères génériques ne sont pas pris en charge.

   Si la boîte aux lettres a été supprimée, sélectionnez-la dans l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.
4. Cliquez sur **Restaurer** > **Boîte aux lettres**.
5. Exécutez les étapes 8-11 de la procédure ci-dessus.

Restauration d'éléments de boîte aux lettres

Pour restaurer des boîtes aux lettres à partir d'une sauvegarde de base de données ou d'une sauvegarde reconnaissant les applications

1. [Uniquement lors de la restauration à partir d'une sauvegarde de base de données vers Microsoft 365] Si l'agent pour Microsoft 365 n'est pas installé sur la machine exécutant Exchange Server qui était sauvegardée, effectuez l'une des actions suivantes :
   - S'il n'y a pas d'agent pour Microsoft 365 au sein de votre organisation, installez un agent pour Microsoft 365 sur la machine qui a été sauvegardée (ou sur une autre machine possédant la même version de Microsoft Exchange Server).
   - Si vous avez déjà un agent pour Microsoft 365 au sein de votre organisation, copiez des bibliothèques depuis la machine qui a été sauvegardée (ou à partir d'une autre machine possédant la même version de Microsoft Exchange Server) vers la machine avec l'agent pour Microsoft 365, comme décrit dans « Copier des bibliothèques Microsoft Exchange ».
2. Effectuez l'une des actions suivantes :
   - Lors d'une restauration à partir d'une sauvegarde reconnaissant les applications : sous **Terminaux**, sélectionnez la machine qui contenait à l'origine les données que vous voulez restaurer.
   - Lors d'une restauration à partir d'une sauvegarde de base de données, cliquez sur **Terminaux** > **Microsoft Exchange** > **Bases de données**, puis sélectionnez la base de données qui contenait à l'origine les données que vous voulez restaurer.
3. Cliquez sur **Restauration**.
4. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Utilisez d'autres méthodes de restauration :
   - [Uniquement lors d'une restauration à partir d'une sauvegarde reconnaissant les applications] Si la sauvegarde est située dans le Cloud ou à un emplacement de stockage partagé (c'est-à-dire si d'autres agents peuvent y accéder), cliquez sur **Sélectionner une machine**, sélectionnez une machine en ligne avec agent pour Exchange ou agent pour VMware, puis choisissez un point de récupération.
   - Sélectionnez un point de récupération dans l'onglet Stockage de sauvegarde.

   La machine choisie pour la navigation dans l'une des actions présentées ci-dessus effectuera la restauration des données à la place de la machine d'origine hors ligne.
5. Cliquez sur **Restaurer** > **Boîtes aux lettres Exchange**.

6. Cliquez sur la boîte aux lettres dans laquelle les éléments que vous souhaitez restaurer étaient initialement présents.
7. Sélectionnez les éléments que vous souhaitez restaurer.

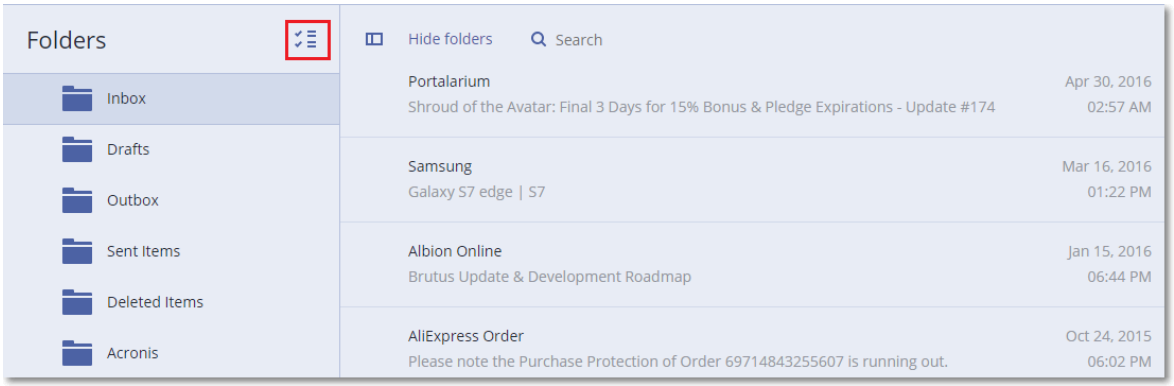
   Les options de recherche suivantes sont disponibles. Les caractères génériques ne sont pas pris en charge.

   - Pour les messages de courrier électronique : recherche par sujet, expéditeur, destinataire et date.
   - Pour les événements : recherche par titre et date.
   - Pour les tâches : recherche par sujet et date.
   - Pour les contacts : recherche par nom, adresse e-mail et numéro de téléphone.

   Lorsqu'un message de courrier électronique est sélectionné, vous pouvez cliquer sur **Afficher le contenu** pour afficher son contenu, y compris les pièces jointes.

   Remarque
   Cliquez sur le nom d'un fichier de pièce jointe pour le télécharger.

   Pour pouvoir sélectionner les dossiers, cliquez sur l'icône des dossiers de restauration.

8. Cliquez sur **Restaurer**.
9. Pour restaurer Microsoft 365, sélectionnez **Microsoft 365** dans **Restaurer vers**.

   Pour effectuer une restauration vers un serveur Exchange, conservez la valeur par défaut **Microsoft Exchange** dans **Restaurer vers**.

   [Uniquement lors de la restauration vers Exchange Server] Cliquez sur **Machine cible avec Microsoft Exchange Server** pour sélectionner ou modifier la machine cible. Cette étape permet la restauration d'une machine qui n'exécute par l'agent pour Exchange.

   Spécifiez le nom de domaine qualifié complet (FQDN) de la machine où le rôle **Accès client** (dans Microsoft Exchange Server 2010/2013) ou le **rôle de boîte aux lettres** (dans Microsoft Exchange Server 2016 ou version ultérieure) est activé. La machine doit appartenir à la même forêt Active Directory que la machine qui effectue la restauration.
10. Si vous y êtes invité, fournissez les informations d'identification d'un compte qui sera utilisé pour accéder à la machine. Les exigences pour ce compte sont répertoriées dans « Droits utilisateurs requis ».
11. Dans **Boîte aux lettres cible**, afficher, modifier ou spécifier la boîte aux lettres cible.

Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas ou si une machine cible non d'origine est sélectionnée, vous devez spécifier la boîte aux lettres cible.

12. [Uniquement lors de la restauration de messages électroniques] Dans **Dossier cible**, affichez ou modifiez le dossier cible dans la boîte aux lettres cible. Par défaut, le dossier **Éléments restaurés** est sélectionné. En raison des limites de Microsoft Exchange, les évènements, tâches, notes et contacts sont restaurés dans leur emplacement d'origine, quel que soit le **dossier cible** spécifié.
13. Cliquez sur **Démarrer la récupération**.

La progression de la restauration sont affichées dans l'onglet **Activités**.

Pour restaurer un élément de boîte aux lettres à partir d'une sauvegarde de boîte aux lettres

1. Cliquez sur **Terminaux** > **Microsoft Exchange** > **Boîtes aux lettres**.
2. Sélectionnez la boîte aux lettres d'origine des éléments à restaurer, puis cliquez sur **Restauration**.

   Vous pouvez rechercher les boîtes aux lettres par nom. Les caractères génériques ne sont pas pris en charge.

   Si la boîte aux lettres a été supprimée, sélectionnez-la dans l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.
4. Cliquez sur **Restaurer** > **Messages électroniques**.
5. Sélectionnez les éléments que vous souhaitez restaurer.

   Les options de recherche suivantes sont disponibles. Les caractères génériques ne sont pas pris en charge.

   - Pour les messages de courrier électronique : recherche par sujet, expéditeur, destinataire et date.
   - Pour les événements : recherche par titre et date.
   - Pour les tâches : recherche par sujet et date.
   - Pour les contacts : recherche par nom, adresse e-mail et numéro de téléphone.

   Lorsqu'un message de courrier électronique est sélectionné, vous pouvez cliquer sur **Afficher le contenu** pour afficher son contenu, y compris les pièces jointes.

   Remarque
   Cliquez sur le nom d'un fichier de pièce jointe pour le télécharger.

   Lorsqu'un message de courrier électronique est sélectionné, vous pouvez cliquer sur **Envoyer sous forme de message électronique** pour l'envoyer à une adresse électronique. Le message est envoyé à partir de l'adresse électronique de votre compte d'administrateur.

   Pour pouvoir sélectionner les dossiers, cliquez sur l'icône des dossiers à restaurer : 

6. Cliquez sur **Restaurer**.
7. Exécutez les étapes 9-13 de la procédure ci-dessus.

Copier les bibliothèques Microsoft Exchange Server

Lors de la restauration de boîtes aux lettres Exchange ou d'éléments de boîte aux lettres vers Microsoft 365, vous aurez peut-être besoin de copier les bibliothèques suivantes depuis la machine qui a été sauvegardée (ou depuis une autre machine possédant la même version de Microsoft Exchange Server) vers la machine avec l'agent pour Microsoft 365.

Copiez les fichiers suivants, en fonction de la version de Microsoft Exchange Server sauvegardée.

Version Microsoft Exchange Server	Bibliothèques	Emplacement par défaut

Microsoft Exchange Server 2010	`ese.dll`
	`esebcli2.dll`
	`store.exe`
		`%ProgramFiles%\Microsoft\Exchange Server\V14\bin`

Microsoft Exchange Server 2013	`ese.dll`	`%ProgramFiles%\Microsoft\Exchange Server\V15\bin`
	`msvcr110.dll`	`%WINDIR%\system32`
Microsoft Exchange Server 2016, 2019	`ese.dll`	`%ProgramFiles%\Microsoft\Exchange Server\V15\bin`
	`msvcr110.dll` `msvcp110.dll`	`%WINDIR%\system32`

Les bibliothèques doivent être placées dans le dossier `%ProgramData%\Acronis\ese`. Si ce dossier n'existe pas, créez-le manuellement.

Modification des informations d'identification de SQL Server ou d'Exchange Server

Vous pouvez modifier les informations d'identification de SQL Server ou Exchange Server sans réinstaller l'agent.

Pour modifier les informations d'identification de SQL Server ou Exchange Server

1. Cliquez sur **Terminaux**, puis sur **Microsoft SQL** ou **Microsoft Exchange**.
2. Sélectionnez le groupe de disponibilité AlwaysOn, le groupe de disponibilité de la base de données, l'instance SQL Server ou l'instance Exchange Server dont vous voulez modifier les identifiants d'accès.

3. Cliquez sur **Indiquer l'identifiant**.
4. Indiquez les nouvelles informations d'identification, puis cliquez sur **OK**.

Pour modifier les informations d'identification d'Exchange Server pour la sauvegarde de boîte aux lettres

1. Cliquez sur **Terminaux** > **Microsoft Exchange**, puis développez **Boîtes aux lettres**.
2. Sélectionnez l'Exchange Server dont vous souhaitez modifier les informations d'identification.
3. Cliquez sur **Paramètres**.
4. Indiquez les nouvelles informations d'identification sous **Compte administrateur Exchange**, puis cliquez sur **OK**.

Protection des terminaux mobiles

L'application Cyber Protect vous permet de sauvegarder vos données mobiles dans le Stockage dans le Cloud, puis de les restaurer en cas de perte ou d'endommagement. Veuillez noter que pour effectuer une sauvegarde vers le stockage dans le Cloud, vous devez posséder un compte et un abonnement au Cloud.

Terminaux mobiles pris en charge

Vous pouvez installer l'application Cyber Protect sur un terminal mobile fonctionnant sur l'un des systèmes d'exploitation suivants :

- iOS 14 à iOS 16 (iPhone, iPod, iPad)
- Android 9 à Android 13

Ce que vous pouvez sauvegarder

- Contacts (nom, numéro de téléphone et adresse e-mail)
- Photos (la taille et le format d'origine de vos photos sont préservés)
- Vidéos
- Calendriers
- Rappels (iOS uniquement)

Ce que vous devez savoir

- Vous pouvez uniquement sauvegarder les données dans le stockage sur le Cloud.
- Lorsque vous ouvrez l'application, le résumé des changements dans les données s'affiche et vous pouvez démarrer une sauvegarde manuellement.
- La fonctionnalité **Sauvegarde en continu** est activée par défaut. Si ce paramètre est activé, l'application Cyber Protect détecte automatiquement les nouvelles données à la volée et les transfère dans le cloud.

- L'option **Utiliser le Wi-Fi uniquement** est activée par défaut dans les paramètres de l'application. Si ce paramètre est activé, l'application Cyber Protect sauvegarde vos données uniquement si une connexion Wi-Fi est disponible. Si la connexion est perdue, le processus de sauvegarde ne se lance pas. Si vous souhaitez que l'application utilise également les données cellulaires, désactivez cette option.
- L'optimisation de la batterie sur votre terminal peut empêcher l'application Cyber Protect de fonctionner correctement. Pour exécuter les sauvegardes dans les temps, vous devez arrêter l'optimisation de la batterie de l'application.
- Vous pouvez économiser de l'énergie de deux façons :
  - La fonctionnalité **Sauvegarder pendant la charge**, qui est désactivée par défaut. Si ce paramètre est activé, l'application Cyber Protect sauvegarde vos données uniquement lorsque votre terminal est connecté à une source d'alimentation. Si le terminal n'est pas connecté à une source d'alimentation lors du processus de sauvegarde continu, la sauvegarde est mise en pause.
  - L'option **Mode d'économie d'énergie**, qui est activée par défaut. Si ce paramètre est activé, l'application Cyber Protect sauvegarde vos données uniquement lorsque la batterie de votre terminal est suffisamment chargée. Lorsque le niveau de charge de la batterie baisse, la sauvegarde continue est mise en pause.
- Vous pouvez accéder aux données sauvegardées à partir de tous les terminaux mobiles enregistrés sur votre compte. Cela vous permet de transférer les données d'un ancien terminal mobile à un nouveau. Les contacts et les photos d'un terminal Android peuvent être récupérés sur un terminal iOS, et inversement. Vous pouvez également télécharger une photo, une vidéo ou un contact sur n'importe quel terminal à l'aide de la console Cyber Protect.
- Les données sauvegardées à partir des terminaux mobiles associés à votre compte sont uniquement disponible sous ce compte. Personne d'autre que vous ne peut visualiser et restaurer vos données.
- Dans l'application Cyber Protect, vous pouvez restaurer uniquement la version des données la plus récente. Si vous souhaitez effectuer une restauration à partir d'une version de sauvegarde en particulier, utilisez la console Cyber Protect sur une tablette ou sur un ordinateur.
- Les règles de rétention ne s'appliquent pas aux sauvegardes de terminaux mobiles.
- [Pour les terminaux Android uniquement] Si une carte SD est présente lors d'une sauvegarde, les données stockées sur cette carte sont également sauvegardées. Ces données seront restaurées sur la carte SD, vers le dossier **Restauré par la sauvegarde**, si la carte est présente lors de la restauration. À défaut, l'application demandera un autre emplacement vers lequel restaurer les données.

Où obtenir l'application Cyber Protect

Selon le terminal mobile que vous possédez, installez l'application depuis l'App Store ou sur Google Play.

Comment commencer à sauvegarde vos données

1. Ouvrez l'application.
2. Connectez-vous à votre compte.
3. Appuyez sur **Configurer** pour créer votre sauvegarde. Veuillez noter que ce bouton apparaît uniquement lorsqu'aucune sauvegarde n'est présente sur votre terminal mobile.
4. Sélectionnez les catégories de données que vous voulez sauvegarder. Par défaut, toutes les catégories sont sélectionnées.
5. [étape facultative] Activez **Chiffrer la sauvegarde** pour protéger votre sauvegarde par chiffrage. Dans ce cas, vous devrez également :
   a. Saisir un mot de passe de chiffrement deux fois.

      Remarque
      Assurez-vous de vous souvenir du mot de passe, car il est impossible de le restaurer ou de le modifier en cas d'oubli.

   b. Appuyez sur **Chiffrer**.
6. Sélectionnez **Sauvegarder**.
7. Autorisez l'application à accéder à vos données personnelles. Si vous refusez l'accès à certaines catégories de données, celles-ci ne seront pas sauvegardées.

La sauvegarde commence.

Comment restaurer les données vers un terminal mobile

Avertissement !
Pour restaurer des données mobiles, vous devez utiliser le compte de l'utilisateur final.

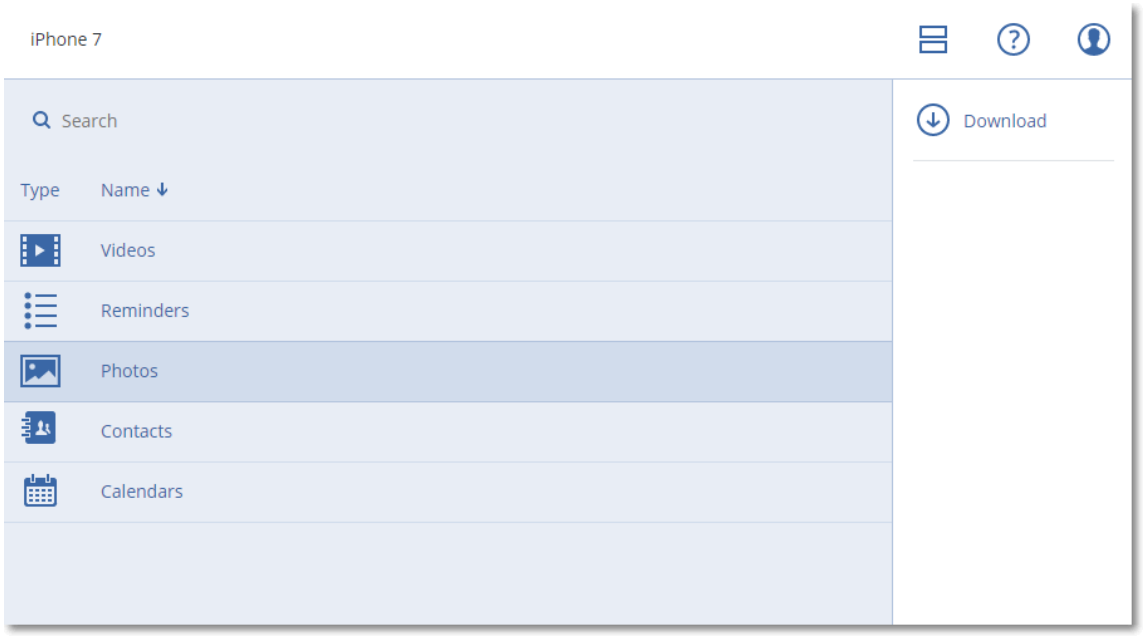
1. Ouvrez l'application Cyber Protect.
2. Appuyez sur **Parcourir**.
3. Entrez le nom du terminal.
4. Effectuez l'une des actions suivantes :
   - Pour restaurer toutes les données sauvegardées, appuyez sur **Tout restaurer**. Aucune autre action n'est requise.
   - Pour restaurer une ou plusieurs catégories de données, appuyez sur **Sélectionner**, puis sélectionnez les cases à cocher correspondant aux catégories de données requises. Appuyez sur **Restaurer**. Aucune autre action n'est requise.
   - Pour restaurer un ou plusieurs éléments de données appartenant à une même catégorie de données, sélectionnez la catégorie de données requise. Continuez avec les étapes ci-après.
5. Effectuez l'une des actions suivantes :

- Pour restaurer un seul élément de données, sélectionnez-le en appuyant dessus.
- Pour restaurer plusieurs éléments de données, appuyez sur **Sélectionner**, puis sélectionnez les cases correspondant aux éléments de données requis.

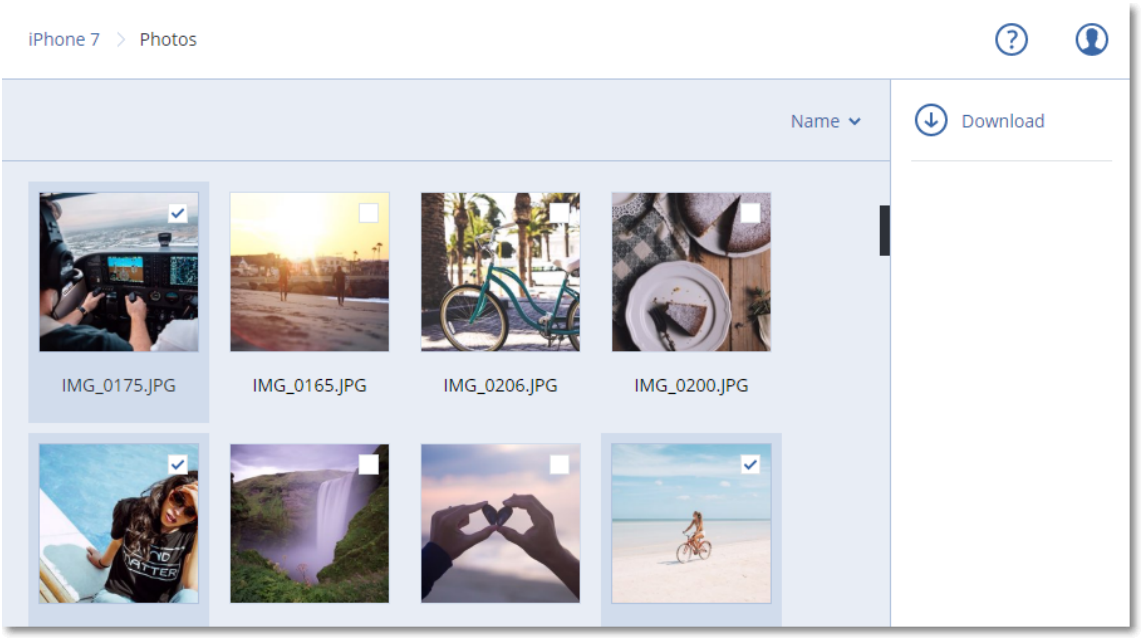
6. Appuyez sur **Restaurer**.

Comment examiner des données à partir de la console Cyber Protect

1. Sur un ordinateur, ouvrez un navigateur et saisissez l'URL de la console Cyber Protect.
2. Connectez-vous à votre compte.
3. Dans **Tous les terminaux**, cliquez sur **Restaurer** sous le nom de votre terminal mobile.
4. Effectuez l'une des actions suivantes :
   - Pour télécharger l'ensemble des photos, vidéos, contacts, calendriers ou rappels, sélectionnez les catégories de données correspondantes. Cliquez sur **Télécharger**.



   - Pour télécharger des photos, vidéos, contacts, calendriers ou rappels particuliers, cliquez sur les catégories de données correspondantes, puis sélectionnez les éléments de données requis. Cliquez sur **Télécharger**.



- Pour afficher l'aperçu d'une photo ou d'un contact, cliquez sur le nom de la catégorie de données correspondante, puis sélectionnez l'élément de données requis.

Protection des données Exchange hébergées

Quels éléments peuvent être sauvegardés ?

Vous pouvez sauvegarder des boîtes aux lettres utilisateur, communes et de groupe. Vous pouvez aussi choisir de sauvegarder les boîtes aux lettres d'archive (**Archives permanentes**) des boîtes aux lettres sélectionnées.

Quels éléments de données peuvent être restaurés ?

Les éléments suivants peuvent être restaurés à partir de sauvegardes de boîte aux lettres :

- Boîtes aux lettres
- Dossiers de courriers électroniques
- Messages de courriers électroniques
- Événements de calendrier
- Tâches
- Contacts
- Entrées de journal
- Notes

Vous pouvez utiliser la fonction de recherche pour trouver l'emplacement des éléments.

Lorsque vous restaurez des boîtes aux lettres, des éléments de boîte aux lettres, des dossiers publics et des éléments de dossiers publics, vous pouvez choisir d'écraser ou non les éléments de l'emplacement de destination.

Lorsqu'une boîte aux lettres est restaurée sur une boîte aux lettres existante, les éléments existants dont les identifiants sont identiques sont écrasés.

La restauration des éléments de boîtes aux lettres n'écrase aucun élément. À la place, le chemin d'accès complet vers un élément de boîte aux lettres est recréé dans le dossier cible.

Sélection des boîtes aux lettres Exchange Online

Sélectionnez les boîtes aux lettres comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Sélection de boîtes aux lettres Exchange Online

1. Cliquez sur **Terminaux > Exchange hébergé**.
2. Si plusieurs organisations Exchange hébergé ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez sauvegarder les données utilisateur. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour sauvegarder les boîtes aux lettres de tous les utilisateurs et toutes les boîtes aux lettres communes (y compris celles qui seront créées à l'avenir), développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, puis cliquez sur **Sauvegarde de groupe**.
   - Pour sauvegarder des boîtes aux lettres utilisateur ou communes, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez sauvegarder les boîtes aux lettres, puis cliquez sur **Sauvegarde**.
   - Pour sauvegarder toutes les boîtes aux lettres de groupe (y compris celles des groupes qui seront créés à l'avenir), développez le nœud **Groupes**, sélectionnez **Tous les groupes**, puis cliquez sur **Sauvegarde de groupe**.
   - Pour sauvegarder des boîtes aux lettres de groupe en particulier, développez le nœud **Groupes**, sélectionnez **Tous les groupes**, sélectionnez les groupes dont vous souhaitez sauvegarder les boîtes aux lettres, puis cliquez sur **Sauvegarde**.

Restauration de boîtes aux lettres et d'éléments de boîte aux lettres

Restauration de boîtes aux lettres

1. Cliquez sur **Terminaux > Exchange hébergé**.
2. Si plusieurs organisations Exchange hébergé ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :

- Pour restaurer une boîte aux lettres utilisateur, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez restaurer la boîte aux lettres, puis cliquez sur **Restauration**.
- Pour restaurer une boîte aux lettres commune, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez la boîte aux lettres commune que vous souhaitez restaurer, puis cliquez sur **Restauration**.
- Pour restaurer une boîte aux lettres de groupe, développez le nœud **Groupes**, sélectionnez **Tous les groupes**, sélectionnez le groupe dont vous souhaitez restaurer la boîte aux lettres, puis cliquez sur **Restauration**.
- Si la boîte aux lettres utilisateur, de groupe ou commune a été supprimée, sélectionnez-la dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

Vous pouvez rechercher les utilisateurs et les groupes par nom. Les caractères génériques ne sont pas pris en charge.

4. Sélectionnez un point de restauration.
5. Cliquez sur **Restaurer** > **Intégralité de la boîte aux lettres**.
6. Si plusieurs organisations Exchange hébergé sont ajoutées au service Cyber Protection, cliquez sur **Organisation Exchange hébergé** pour afficher, modifier ou spécifier l'organisation cible.
   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
7. Dans **Restaurer vers la boîte aux lettres**, affichez, modifiez ou spécifiez la boîte aux lettres cible.
   Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier la boîte aux lettres cible.
8. Cliquez sur **Démarrer la récupération**.
9. Sélectionnez l'une des options d'écrasement :
   - **Écraser les éléments existants**
   - **Ne pas écraser les éléments existants**
10. Cliquez sur **Continuer** pour confirmer votre choix.

Restauration d'éléments de boîte aux lettres

1. Cliquez sur **Terminaux > Exchange hébergé**.
2. Si plusieurs organisations Exchange hébergé ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour restaurer des éléments d'une boîte aux lettres utilisateur, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont la boîte aux lettres contenait à l'origine les éléments à restaurer, puis cliquez sur **Restauration**.

- Pour restaurer les éléments d'une boîte aux lettres commune, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez la boîte aux lettres commune qui contenait à l'origine les éléments que vous souhaitez restaurer, puis cliquez sur **Restauration**.
- Pour restaurer des éléments d'une boîte aux lettres de groupe, développez le nœud **Groupes**, sélectionnez **Tous les groupes**, sélectionnez le groupe dont la boîte aux lettres contenait à l'origine les éléments à restaurer, puis cliquez sur **Restauration**.
- Si la boîte aux lettres utilisateur, de groupe ou commune a été supprimée, sélectionnez-la dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

Vous pouvez rechercher les utilisateurs et les groupes par nom. Les caractères génériques ne sont pas pris en charge.

4. Sélectionnez un point de restauration.
5. Cliquez sur **Restaurer** > **Messages électroniques**.
6. Parcourez le dossier requis ou utilisez la fonction de recherche pour obtenir la liste des éléments requis.

   Les options de recherche suivantes sont disponibles. Les caractères génériques ne sont pas pris en charge.
   - Pour les messages de courrier électronique : recherche par sujet, expéditeur, destinataire, nom de la pièce jointe et date.
   - Pour les événements : recherche par titre et date.
   - Pour les tâches : recherche par sujet et date.
   - Pour les contacts : recherche par nom, adresse e-mail et numéro de téléphone.
7. Sélectionnez les éléments que vous souhaitez restaurer. Pour pouvoir sélectionner les dossiers, cliquez sur l'icône des dossiers à restaurer : 

   Par ailleurs, vous pouvez effectuer l'une des opérations suivantes :
   - Lorsqu'un élément est sélectionné, cliquez sur **Afficher le contenu** pour afficher son contenu, y compris les pièces jointes. Cliquez sur le nom d'un fichier de pièce jointe pour le télécharger.
   - Lorsqu'un message de courrier électronique ou un élément de calendrier est sélectionné, vous pouvez cliquer sur **Envoyer sous forme de message électronique** pour l'envoyer aux adresses électroniques spécifiées. Vous pouvez sélectionner l'expéditeur et rédiger un message qui sera ajouté à l'élément transféré.
   - Uniquement si la sauvegarde n'est pas chiffrée, que vous avez utilisé la fonction de recherche et que vous avec sélectionné un seul élément dans les résultats de recherche : cliquez sur **Afficher les versions** pour sélectionner la version de l'élément à restaurer. Vous pouvez choisir n'importe quelle version sauvegardée, avant ou après le point de récupération sélectionné.
8. Cliquez sur **Restaurer**.

9. Si plusieurs organisations Exchange hébergé ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Exchange hébergé** pour afficher, modifier ou spécifier l'organisation cible.

   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
10. Dans **Restaurer vers la boîte aux lettres**, affichez, modifiez ou spécifiez la boîte aux lettres cible.

    Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier la boîte aux lettres cible.
11. [Uniquement lors de la restauration vers une boîte aux lettres utilisateur ou commune] Dans **Chemin d'accès**, affichez ou modifiez le dossier cible dans la boîte aux lettres cible. Par défaut, le dossier **Éléments restaurés** est sélectionné.

    Les éléments d'une boîte aux lettres de groupe sont toujours restaurés dans le dossier **Boîte de réception**.
12. Cliquez sur **Démarrer la récupération**.
13. Sélectionnez l'une des options d'écrasement :
    - **Écraser les éléments existants**
    - **Ne pas écraser les éléments existants**
14. Cliquez sur **Continuer** pour confirmer votre choix.

Protection des données Microsoft 365

Pourquoi sauvegarder les données Microsoft 365 ?

Bien que Microsoft 365 soit un ensemble de services Cloud, l'exécution de sauvegardes régulières offre une couche de protection supplémentaire contre les erreurs des utilisateurs et les actions malveillantes intentionnelles. Il est possible de restaurer les éléments supprimés d'une sauvegarde même après expiration de la période de rétention de Microsoft 365. Par ailleurs, pour des raisons de conformité à d'éventuelles réglementations, il est possible de conserver une copie locale des boîtes aux lettres Exchange Online.

Les données sauvegardées sont automatiquement compressées et utilisent moins d'espace dans l'emplacement de sauvegarde que dans leur emplacement d'origine. Le niveau de compression des sauvegardes cloud à cloud est fixe et correspond au niveau **Normal** des sauvegardes non-cloud à cloud. Pour en savoir plus sur ces niveaux, reportez-vous à "Niveau de compression" (p. 479).

Agent cloud et agent local

Pour les ressources Microsoft 365, deux agents sont disponibles :

- Agent cloud

L'agent cloud offre des fonctionnalités de sauvegarde étendues, directement accessibles dans la console Cyber Protect. Aucune installation n'est nécessaire. Pour plus d'informations, voir "Utilisation de l'agent Cloud pour Microsoft 365" (p. 638).

- Agent local

  L'agent local n'assure que la sauvegarde des boîtes aux lettres Exchange Online. Cet agent doit être installé sur une machine Windows connectée à Internet. Pour plus d'informations, voir "Utilisation de l'agent pour Office 365 installé localement" (p. 633).

Azure Information Protection (AIP) est pris en charge par les deux agents.

Remarque
Pour les tenants en mode Conformité, seul l'agent local est disponible. Ces tenants ne peuvent sauvegarder que les boîtes aux lettres Microsoft 365. Ils ne peuvent pas utiliser les fonctionnalités étendues fournies par l'agent cloud.

Le tableau suivant résume les fonctionnalités des agents.

	Agent local	Agent cloud
Éléments de données qui peuvent être sauvegardés	**Exchange Online** : boîtes aux lettres utilisateur et partagées (y compris les boîtes aux lettres des utilisateurs possédant un plan Kiosk et les boîtes aux lettres bloquées pour cause de litige)	• **Exchange Online** : ◦ boîtes aux lettres utilisateur et partagées (y compris les boîtes aux lettres des utilisateurs possédant un plan Kiosk et les boîtes aux lettres bloquées pour cause de litige) ◦ boîtes aux lettres de groupe ◦ dossiers publics • **OneDrive :** fichiers et dossiers utilisateur • **SharePoint Online** : ◦ collections de sites classiques ◦ sites de groupe (équipe) ◦ sites de communication ◦ éléments de données • **Microsoft 365 Teams** : ◦ équipes complètes ◦ canaux d'équipe ◦ fichiers de canal ◦ boîtes aux lettres d'équipe ◦ fichiers et e-mails dans les boîtes aux lettres d'équipe ◦ réunions

	Agent local	Agent cloud
		◦ sites d'équipe • **Bloc-notes OneNote** : dans le cadre de sauvegardes OneDrive, SharePoint Online et Microsoft 365 Teams
Sauvegarde de boîtes aux lettres d'archive (**Archives permanentes**)	Non	Oui
Planification de sauvegarde	Définie par l'utilisateur	Jusqu'à six fois par jour*
Emplacements de sauvegardes	Stockage dans le Cloud, dossier local, dossier réseau	Stockage dans le Cloud uniquement (stockage hébergé par le partenaire compris)
Protection automatique des nouveaux utilisateurs, groupes, sites et équipes Microsoft 365	Non	Oui, en appliquant un plan de protection aux groupes **Tous les utilisateurs**, **Tous les groupes**, **Tous les sites**, **Toutes les équipes**
Protection de plus d'une organisation Microsoft 365	Non	Oui
Restauration granulaire	Oui	Oui
Restauration vers un autre utilisateur au sein d'une même organisation	Oui	Oui
Restauration vers une autre organisation	Non	Oui
Restauration vers un serveur Microsoft Exchange Server sur site	Non	Non
Nombre maximum d'éléments pouvant être sauvegardés sans dégradation des performances	Lors d'une sauvegarde sur le stockage dans le Cloud : 5 000 boîtes aux lettres par entreprise Lorsque vous effectuez une sauvegarde vers d'autres destinations : 2 000 boîtes aux lettres par plan de protection (aucune limite du nombre de boîtes aux lettres par entreprise)	10 000 éléments protégés (boîtes aux lettres, instances OneDrive, ou sites) par entreprise**

	Agent local	Agent cloud
Nombre maximal d'exécutions de sauvegardes manuelles	Non	10 exécutions manuelles en une heure
Nombre maximal d'opérations de récupération simultanées	Non	10 opérations, y compris les opérations de récupération Google Workspace

* L'option par défaut est **Une fois par jour**. Grâce au pack Advanced Backup, vous pouvez planifier jusqu'à six sauvegardes par jour. Les sauvegardes démarrent à des intervalles approximatifs qui dépendent de la charge actuelle de l'agent cloud desservant les nombreux clients d'un centre de données. De cette manière, la charge est égale toute la journée, ce qui garantit une qualité de service équivalente pour tous les clients.

Remarque
Le calendrier de protection peut être affecté par le fonctionnement de services tiers, par exemple, l'accessibilité des serveurs Microsoft 365, les paramètres de limitation sur les serveurs Microsoft, et autres. Voir également https://docs.microsoft.com/en-us/graph/throttling.

** Nous vous recommandons de sauvegarder vos éléments protégés de manière graduelle et dans l'ordre suivant :

1. Boîtes aux lettres.
2. Une fois toutes les boîtes aux lettres sauvegardées, passez aux instances OneDrive.
3. Une fois la sauvegarde des instances OneDrive terminée, passez aux sites SharePoint Online.

La première sauvegarde complète peut prendre plusieurs jours, en fonction du nombre d'éléments protégés et de leur taille.

Droits utilisateurs requis

Dans Cyber Protection

L'agent local doit être enregistré sous un compte d'administrateur d'entreprise et utilisé au niveau du tenant client. Les administrateurs d'entreprise agissant au niveau de l'unité, les administrateurs d'unité et les utilisateurs ne peuvent pas sauvegarder ou récupérer les données Microsoft 365.

L'agent cloud peut être utilisé à la fois au niveau du tenant client et au niveau de l'unité. Pour plus d'informations sur ces niveaux et leurs administrateurs respectifs, voir "Administration d'organisations Microsoft 365 organisations ajoutées à différents niveaux" (p. 639).

Dans Microsoft 365

Votre compte doit bénéficier du rôle d'administrateur global dans Microsoft 365.

Pour découvrir, sauvegarder et restaurer des dossiers publics Microsoft 365, au moins un de vos comptes d'administrateur Microsoft 365 doit disposer d'une boîte aux lettres et de droits d'accès en lecture/écriture aux dossiers publics que vous souhaitez sauvegarder.

- L'agent local se connectera à Microsoft 365 en utilisant ce compte. Pour permettre à l'agent d'accéder au contenu de toutes les boîtes aux lettres, ce compte se verra attribuer le rôle de gestion **ApplicationImpersonation**. Si vous modifiez le mot de passe du compte, mettez-le à jour dans la console Cyber Protect, comme décrit dans "Modification des identifiants de Microsoft 365" (p. 636).
- L'agent cloud ne se connecte pas à Microsoft 365. Vous devez vous connecter une fois à Microsoft 365 en tant qu'administrateur global, afin d'accorder à l'agent cloud les autorisations nécessaires à son fonctionnement.

  Les autorisations suivantes sont requises dans Microsoft 365 :
  - Se connecter et lire les profils des utilisateurs
  - Lire et écrire des fichiers dans toutes les collections de sites
  - Lire et écrire les profils complets de tous les utilisateurs
  - Lire et écrire tous les groupes
  - Lire les données du répertoire
  - Lire tous les messages du canal
  - Lire et écrire des métadonnées gérées
  - Lire et écrire des éléments et des listes dans toutes les collections de sites
  - Contrôle total de toutes les collections de sites
  - Lire et écrire des éléments dans toutes les collections de sites
  - Utiliser les services Web d'Exchange avec un accès complet à toutes les boîtes aux lettres
- L'agent cloud ne stocke pas les identifiants de votre compte et ne les utilise pas pour effectuer des sauvegardes et des restaurations. La modification des identifiants, la désactivation ou la suppression du compte n'affectent pas le fonctionnement de l'agent cloud.

Limites

- Avec l'agent local, vous pouvez protéger jusqu'à 5 000 ressources. Avec l'agent cloud, vous pouvez protéger jusqu'à 50 000 ressources.
- Tous les utilisateurs ayant une boîte aux lettres ou un OneDrive s'affichent dans la console Cyber Protect, y compris les utilisateurs qui ne possèdent pas de licence Microsoft 365 et les utilisateurs dont la connexion aux services Microsoft 365 est bloquée.
- Une sauvegarde de boîte aux lettres inclut uniquement des dossiers visibles pour les utilisateurs. Le dossier **Éléments récupérables** et ses sous-dossiers (**Suppressions**, **Versions**, **Purges**, **Audits**, **DiscoveryHold**, **Journalisation du calendrier**) ne sont pas inclus dans une sauvegarde de boîte aux lettres.

- La création automatique d'utilisateurs, de dossiers publics, de groupes ou de sites lors d'une restauration est impossible. Par exemple, si vous souhaitez restaurer un site SharePoint Online supprimé, commencez par créer un site manuellement, puis choisissez-le en tant que site cible lors d'une restauration.
- Vous ne pouvez pas simultanément restaurer des éléments depuis différents points de récupération, même si vous pouvez sélectionner ces éléments dans les résultats de recherche.
- Lors d'une sauvegarde, toute étiquette de confidentialité appliquée au contenu sera préservée. Par conséquent, le contenu sensible ne s'affichera peut-être pas s'il est restauré vers un emplacement autre que l'emplacement d'origine et si l'utilisateur dispose de droits d'accès différents.
- Vous ne pouvez pas appliquer plusieurs plans de sauvegarde à la même ressource.
- Lorsqu'un plan de sauvegarde et un plan de sauvegarde de groupe sont appliqués à la même ressource, les paramètres du plan isolé sont prioritaires.

Rapport des licences de poste Microsoft 365

Les administrateurs de l'entreprise peuvent télécharger un rapport au sujet des postes Microsoft 365 protégés et de leurs licences. Le rapport est au format CSV, et comprend des informations sur la licence d'un poste ainsi que sur la raison de l'utilisation d'une licence. Il inclut aussi le nom du poste protégé, l'e-mail associé, le groupe, l'organisation Microsoft 365, le nom et le type de la ressource protégée.

Ce rapport est disponible uniquement pour les tenants dans lesquels une organisation Microsoft 365 a été enregistrée.

Pour télécharger le rapport des licences de poste Microsoft 365

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur de l'entreprise.
2. Cliquez sur l'icône de compte dans l'angle supérieur droit.
3. Cliquez sur le **rapport des licences de poste Microsoft 365**.

Journalisation

Actions concernant les ressources de cloud à cloud telles que l'affichage du contenu d'e-mails sauvegardés, le téléchargement de pièces jointes ou de fichiers, la restauration d'e-mails sur des boîtes aux lettres autres que les boîtes aux lettres d'origine, ou l'envoi de tels contenus par e-mail pouvant constituer une violation de la confidentialité des utilisateurs. Ces actions sont consignées dans le portail de gestion accessible par **Surveillance** > **Journal d'audit**.

Utilisation de l'agent pour Office 365 installé localement

Ajout d'une organisation Microsoft 365

Pour ajouter une organisation Microsoft 365

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur de l'entreprise.
2. Cliquez sur l'icône de compte dans l'angle supérieur droit, puis cliquez sur **Téléchargements** > **Agent pour Office 365**.
3. Téléchargez l'agent et installez-le sur une machine Windows connectée à Internet.
4. Dans la console Cyber Protect, accédez à **Terminaux** > **Microsoft Office 365 (agent local)**.
5. Dans la fenêtre qui s'ouvre, saisissez l'identifiant et le secret de l'application, ainsi que l'identifiant du tenant Microsoft 365. Pour plus informations sur leur recherche, reportez-vous à "Obtention de l'identifiant et du secret d'application" (p. 634).
6. Cliquez sur **OK**.

Les éléments de données de votre organisation apparaissent ensuite dans la console Cyber Protect, dans l'onglet **Microsoft Office 365 (agent local)**.

Important
Il ne peut y avoir qu'un seul agent pour Office 365 installé localement au sein d'une organisation (groupe de sociétés).

Obtention de l'identifiant et du secret d'application

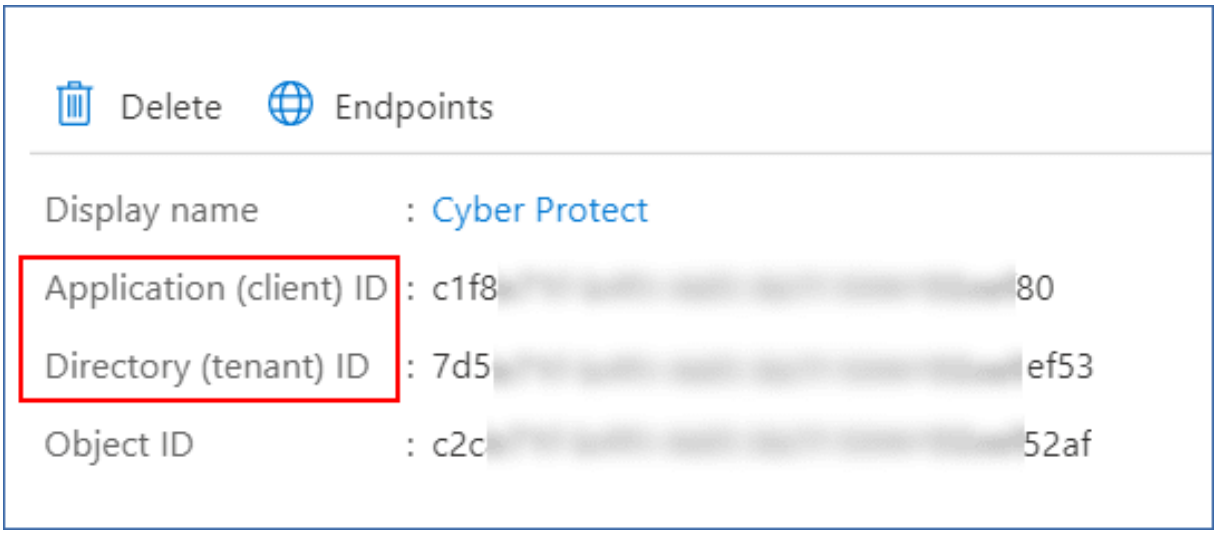
Pour utiliser l'authentification moderne pour Office 365, vous devez créer une application personnalisée dans le centre d'administration d'Entra et lui attribuer une permission d'API spécifiques. Vous obtiendrez ensuite l'**identifiant de l'application**, le **secret de l'application** et l'**identifiant du répertoire (tenant)** que vous devez saisir dans la console Cyber Protect .

Remarque
Sur l'ordinateur sur lequel Agent pour Office 365 est installé, vérifiez que vous autorisez l'accès à graph.microsoft.com par l'intermédiaire du port 443.

Pour créer une application dans le centre d'administration d'Entra

1. Connectez-vous au centre d'administration d'Entra en tant qu'administrateur.
2. Accédez à **Azure Active Directory** > **Inscriptions de l'application**, puis cliquez sur **Nouvelle inscription**.
3. Spécifiez un nom pour votre application personnalisée, par exemple Cyber Protection.
4. Dans **Types de comptes pris en charge**, sélectionnez **Comptes dans ce répertoire organisationnel uniquement**.
5. Cliquez sur **Enregistrer**.

Votre application est maintenant créée. Dans le centre d'administration d'Entra, accédez à la page d'**Vue d'ensemble** de l'application, puis vérifiez l'identifiant de votre application (client) et celui du répertoire (tenant).



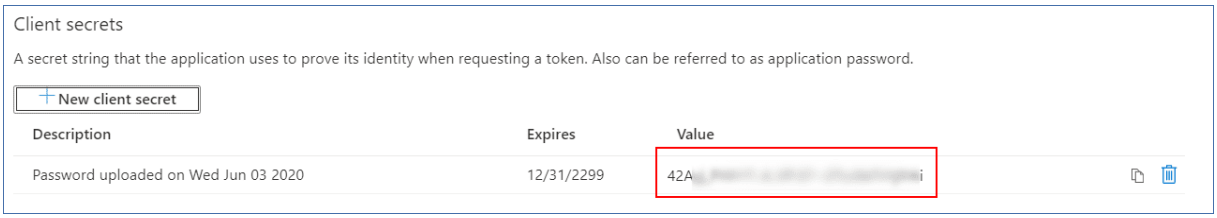
Pour plus d'informations sur la création d'une application dans le centre d'administration d'Entra, référez-vous à la documentation Microsoft.

Pour accorder à l'application les permissions d'API nécessaires

1. Dans le centre d'administration d'Entra, accédez aux **permissions API** de l'application, puis cliquez sur **Ajouter une autorisation**.
2. Sélectionnez l'onglet **API utilisées par mon organisation**, puis recherchez **Office 365 Exchange Online**.
3. Cliquez sur **Office 365 Exchange Online**, puis sur **Permissions d'application**.
4. Cochez la case **full_access_as_app**, puis cliquez sur **Ajouter des permissions**.
5. Dans **Permissions d'API**, cliquez sur **Ajouter une permission**.
6. Sélectionnez **Microsoft Graph**.
7. Sélectionnez **Permissions d'application**.
8. Développez l'onglet **Répertoire**, puis cochez la case **Directory.Read.All**. Cliquez sur **Ajouter des permissions**.
9. Vérifiez toutes les permissions, puis cliquez sur **Accorder des permissions d'administrateur pour <nom de votre application>**.
10. Confirmez votre choix en cliquant sur **Oui**.

Pour créer un secret d'application

1. Dans le centre d'administration d'Entra, accédez au **Certificats et secrets de** votre application > **Nouveau secret client**.
2. Dans la boîte de dialogue qui s'ouvre, sélectionnez Expire : **Jamais**, puis cliquez sur **Ajouter**.
3. Vérifiez le secret de votre application dans le champ **Valeur**, puis mémorisez-le.



Pour plus d'informations sur le secret d'application, reportez-vous à la documentation Microsoft.

Modification des identifiants de Microsoft 365

Vous pouvez modifier les identifiants de Microsoft 365 sans réinstaller l'agent.

Modification des identifiants de Microsoft 365

1. Cliquez sur **Terminaux** > **Microsoft Office 365 (agent local)**.
2. Sélectionnez l'organisation Microsoft 365.
3. Cliquez sur **Indiquer l'identifiant**.
4. Saisissez l'identifiant et le secret de l'application, ainsi que l'identifiant du tenant Microsoft 365. Pour plus informations sur leur recherche, reportez-vous à "Obtention de l'identifiant et du secret d'application" (p. 634).
5. Cliquez sur **OK**.

Protection des boîtes aux lettres Exchange Online

Quels éléments peuvent être sauvegardés ?

Vous pouvez sauvegarder des boîtes aux lettres utilisateur et communes. Les boîtes aux lettres de groupe et les boîtes aux lettres d'archive (**Archives permanentes**) ne peuvent pas être sauvegardées.

Quels éléments de données peuvent être restaurés ?

Les éléments suivants peuvent être restaurés à partir de sauvegardes de boîte aux lettres :

- Boîtes aux lettres
- Dossiers de courriers électroniques
- Messages de courriers électroniques
- Événements de calendrier
- Tâches
- Contacts
- Entrées de journal
- Notes

Vous pouvez utiliser la fonction de recherche pour trouver l'emplacement des éléments.

Lorsqu'une boîte aux lettres est restaurée sur une boîte aux lettres existante, les éléments existants dont les identifiants sont identiques sont écrasés.

La restauration des éléments de boîtes aux lettres n'écrase aucun élément. À la place, le chemin d'accès complet vers un élément de boîte aux lettres est recréé dans le dossier cible.

Sélection des boîtes aux lettres Microsoft 365

Sélectionnez les boîtes aux lettres comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Pour sélectionner des boîtes aux lettres

1. Cliquez sur **Microsoft Office 365 (agent local)**.
2. Sélectionnez les boîtes aux lettres que vous voulez sauvegarder.
3. Cliquez sur **Sauvegarder**.

Restauration de boîtes aux lettres et d'éléments de boîte aux lettres

Restauration de boîtes aux lettres

1. Cliquez sur **Microsoft Office 365 (agent local)**.
2. Sélectionnez la boîte aux lettres à restaurer, puis cliquez sur **Restaurer**.
   Vous pouvez rechercher les boîtes aux lettres par nom. Les caractères génériques ne sont pas pris en charge.
   Si la boîte aux lettres a été supprimée, sélectionnez-la dans l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.
4. Cliquez sur **Restaurer** > **Boîte aux lettres**.
5. Dans **Boîte aux lettres cible**, afficher, modifier ou spécifier la boîte aux lettres cible.
   Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas, vous devez spécifier la boîte aux lettres cible.
6. Cliquez sur **Démarrer la récupération**.

Restauration d'éléments de boîte aux lettres

1. Cliquez sur **Microsoft Office 365 (agent local)**.
2. Sélectionnez la boîte aux lettres d'origine des éléments à restaurer, puis cliquez sur **Restauration**.
   Vous pouvez rechercher les boîtes aux lettres par nom. Les caractères génériques ne sont pas pris en charge.
   Si la boîte aux lettres a été supprimée, sélectionnez-la dans l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.
4. Cliquez sur **Restaurer** > **Messages électroniques**.
5. Sélectionnez les éléments que vous souhaitez restaurer.

   Les options de recherche suivantes sont disponibles. Les caractères génériques ne sont pas pris en charge.

   - Pour les messages de courrier électronique : recherche par sujet, expéditeur, destinataire, nom de la pièce jointe et date.
   - Pour les événements : recherche par titre et date.
   - Pour les tâches : recherche par sujet et date.
   - Pour les contacts : recherche par nom, adresse e-mail et numéro de téléphone.

   Lorsqu'un message de courrier électronique est sélectionné, vous pouvez cliquer sur **Afficher le contenu** pour afficher son contenu, y compris les pièces jointes.

   Remarque
   Cliquez sur le nom d'un fichier de pièce jointe pour le télécharger.

   Lorsqu'un message de courrier électronique est sélectionné, vous pouvez cliquer sur **Envoyer sous forme de message électronique** pour l'envoyer à une adresse électronique. Le message est envoyé à partir de l'adresse électronique de votre compte d'administrateur.

   Pour pouvoir sélectionner les dossiers, cliquez sur l'icône des dossiers à restaurer : 
6. Cliquez sur **Restaurer**.
7. Dans **Boîte aux lettres cible**, afficher, modifier ou spécifier la boîte aux lettres cible.

   Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas, vous devez spécifier la boîte aux lettres cible.
8. Cliquez sur **Démarrer la récupération**.
9. Confirmez votre choix.

Les éléments de boîte aux lettres sont toujours restaurés dans le dossier **Éléments restaurés** de la boîte aux lettres cible.

Utilisation de l'agent Cloud pour Microsoft 365

Ajout d'une organisation Microsoft 365

Un administrateur peut ajouter une ou plusieurs organisations Microsoft 365 à un tenant client ou à une unité dans ce tenant.

Les administrateurs d'entreprise ajoutent des organisations aux tenants clients. Les administrateurs d'unité et les administrateurs client agissant au niveau unité ajoutent des organisations aux unités.

Pour ajouter une organisation Microsoft 365

1. En fonction de l'endroit où vous devez ajouter l'organisation, connectez-vous à la console Cyber Protect en tant qu'administrateur d'entreprise ou d'unité.
2. [Pour les administrateurs d'entreprise agissant au niveau unité] Dans le portail de gestion, accédez à l'unité souhaitée.
3. Cliquez sur **Terminaux** > **Ajouter** > **Microsoft 365 Business**.
   Le logiciel vous redirige vers la page de connexion de Microsoft 365.
4. Connectez-vous à l'aide des informations d'identification de l'administrateur global Microsoft 365.
   Microsoft 365 affiche une liste des permissions nécessaires pour sauvegarder et restaurer les données de votre organisation.
5. Confirmez que vous donnez ces permissions au service Cyber Protection.

Votre organisation Microsoft 365 apparaît alors sous l'onglet **Terminaux** dans la console Cyber Protect.

Conseils utiles

- L'agent Cloud se synchronise avec Microsoft 365 toutes les 24 heures, à compter du moment où l'organisation est ajoutée au service Cyber Protection. Si vous ajoutez ou supprimez un utilisateur, un groupe ou un site, ce changement ne sera pas immédiatement visible dans la console Cyber Protect. Pour synchroniser la modification immédiatement, sélectionnez l'organisation sur la page **Microsoft 365**, puis cliquez sur **Actualiser**.
  Pour plus d'informations sur la synchronisation des ressources d'une organisation Microsoft 365 et de la console Cyber Protect, voir "Découverte de ressources Microsoft 365" (p. 641).
- Si vous avez appliqué un plan de protection au groupe **Tous les utilisateurs**, **Tous les groupes** ou **Tous les sites**, les éléments récemment ajoutés ne seront inclus dans la sauvegarde que lorsque la synchronisation aura été effectuée.
- Conformément à la politique de Microsoft, lorsqu'un utilisateur, un groupe ou un site est supprimé de l'interface graphique de Microsoft 365, il reste encore disponible pendant quelques jours via l'API. Pendant cette période, l'élément supprimé est inactif (grisé) dans la console Cyber Protect et n'est pas sauvegardé. Lorsque l'élément supprimé ne sera plus disponible via l'API, il disparaîtra de la console Cyber Protect. Ses sauvegardes (s'il y en a) se trouvent sous **Stockage de sauvegarde** > **Sauvegardes d'applications Cloud**.

Administration d'organisations Microsoft 365 organisations ajoutées à différents niveaux

Les administrateurs d'entreprise disposent d'un accès complet aux organisations Microsoft 365 ajoutées au niveau tenant client.

Les administrateurs d'entreprise disposent d'un accès limité aux organisations ajoutées à une unité. Dans ces organisations, qui s'affichent avec le nom d'unité entre crochets, les administrateurs d'entreprise peuvent effectuer les actions suivantes :

- Restaurer des données à partir de sauvegardes
  Les administrateurs d'entreprise peuvent restaurer des données dans toutes les organisations du tenant, quel que soit le niveau auquel ces organisations sont ajoutées.
- Parcourir des sauvegardes et des points de restauration dans des sauvegardes
- Supprimer des sauvegardes et des points de restauration dans des sauvegardes
- Afficher les alertes et les activités

Les administrateurs d'entreprise, lorsqu'ils agissent au niveau tenant client, ne peuvent effectuer les tâches suivantes :

- Ajouter des organisations Microsoft 365 à des unités
- Supprimer des organisations Microsoft 365 dans des unités
- Synchroniser des organisations Microsoft 365 qui ont été ajoutées une unité
- Afficher, créer, modifier, supprimer, applique, exécuter ou révoquer des plans de protection pour des éléments de données d'organisations Microsoft 365 qui ont été ajoutées à une unité

Les administrateurs d'unité et les administrateurs d'entreprise agissant au niveau unité disposent d'un accès complet aux organisations ajoutées à une unité. Toutefois, ils n'ont pas accès aux éventuelles ressources provenant du tenant client parent, y compris aux plans de protection créés au sein de ce dernier.

Suppression d'une organisation Microsoft 365

La suppression d'une organisation Microsoft 365 n'affecte pas les sauvegardes existantes des données de cette organisation. Si vous n'avez plus besoin de ces sauvegardes, commencez par les supprimer, puis supprimez l'organisation Microsoft 365. Sinon, les sauvegardes utiliseront toujours de l'espace de stockage dans le Cloud, qui est susceptible de vous être facturé.

Pour plus d'informations sur la suppression des sauvegardes, reportez-vous à "Pour supprimer des sauvegardes ou des archives de sauvegarde" (p. 558).

Pour supprimer une organisation Microsoft 365

1. En fonction de l'endroit où l'organisation est ajoutée, connectez-vous à la console Cyber Protect en tant qu'administrateur d'entreprise ou d'unité.
2. [Pour les administrateurs d'entreprise agissant au niveau unité] Dans le portail de gestion, accédez à l'unité souhaitée.
3. Accédez à **Terminaux** > **Microsoft 365.**
4. Sélectionnez l'organisation, puis cliquez sur **Supprimer le groupe**.

Par conséquent, les plans de sauvegarde appliqués à ce groupe seront révoqués.

Toutefois, vous devriez également révoquer manuellement les droits d'accès de l'application de service de sauvegarde aux données d'organisation Microsoft 365.

Pour révoquer des droits d'accès

1. Connectez-vous à Microsoft 365 en tant qu'administrateur général.
2. Accédez à **Centre administratif** > **Azure Active Directory** > **Applications d'entreprise** > **Toutes les applications**.
3. Sélectionnez l'application de **service de sauvegarde** et explorez-la.
4. Accédez à l'onglet **Propriétés**, puis, sur le panneau d'action, cliquez sur **Supprimer**.
5. Confirmez l'opération de suppression.

Par conséquent, les droits d'accès aux données d'organisation Microsoft 365 seront révoqués de l'application de service de sauvegarde.

Découverte de ressources Microsoft 365

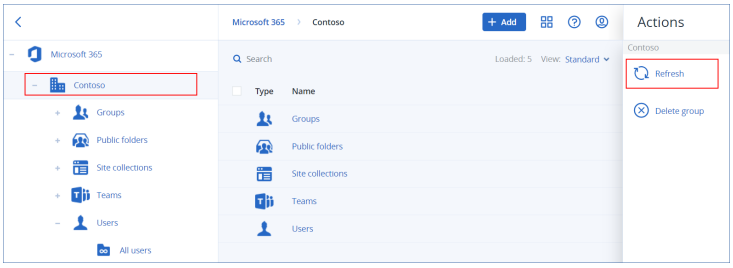
Lorsque vous ajoutez une organisation Microsoft 365 au service Cyber Protection, les ressources de cette organisation (boîtes aux lettres, stockages OneDrive, Microsoft Teams et sites SharePoint, par exemple) sont synchronisées avec la console Cyber Protect. Cette opération est appelée découverte et elle est consignée dans **Surveillance** > **Activités**.

Une fois la découverte terminée, vous pouvez voir les ressources de l'organisation Microsoft 365 dans l'onglet **Terminaux** > **Microsoft 365** de la console Cyber Protect et pouvez leur appliquer des plans de sauvegarde.

Une opération de découverte automatique est exécutée une fois par jour afin que la liste des ressources dans la console Cyber Protect soit à jour. Vous pouvez également synchroniser cette liste à la demande en réexécutant une opération de découverte manuellement.

Pour réexécuter une opération de découverte manuellement

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Microsoft 365**.
2. Sélectionnez votre organisation Microsoft 365, puis cliquez dans le panneau **Actions** sur **Actualiser**.



Remarque
Vous pouvez exécuter manuellement jusqu'à 10 découvertes par heure. Lorsque ce nombre est atteint, le nombre d'exécutions autorisé est réinitialisé à un par heure, puis une exécution supplémentaire est alors disponible toutes les heures jusqu'à ce qu'un total de 10 exécutions par heure soit atteint.

Configuration de la fréquence des sauvegardes Microsoft 365

Par défaut, les sauvegardes Microsoft 365 s'exécutent une fois par jour et aucune autre option de planification n'est disponible.

Si le pack Advanced Backup est activé dans votre tenant, vous pouvez configurer des sauvegardes plus fréquentes. Vous pouvez sélectionner le nombre de sauvegardes par jour, mais vous ne pouvez pas configurer l'heure de leur démarrage. Les sauvegardes démarrent automatiquement à des intervalles approximatifs qui dépendent de la charge actuelle de l'agent cloud desservant les nombreux clients d'un centre de données. De cette manière, la charge est égale toute la journée, ce qui garantit une qualité de service équivalente pour tous les clients.

Les options suivantes sont disponibles.

Planification des options	Intervalle approximatif entre chaque sauvegarde
Une fois par jour	24 heures
Deux fois par jour (par défaut)	12 heures
Trois fois par jour	8 heures
Six fois par jour	4 heures

Remarque
Selon la charge sur l'agent cloud et les limitations possibles côté Microsoft 365, une sauvegarde peut démarrer plus tard ou prendre plus de temps que prévu. Si une sauvegarde est plus longue que l'intervalle moyen entre deux sauvegardes, la sauvegarde suivante est replanifiée, ce qui peut avoir pour résultat un nombre de sauvegardes quotidiennes inférieur au nombre sélectionné. Par exemple, il est possible que deux sauvegardes par jour seulement puissent s'effectuer, même si vous en avez sélectionné six.

Les sauvegardes de boîtes aux lettres de groupe ne peuvent être exécutées qu'une fois par jour.

Protection des données Exchange Online

Quels éléments peuvent être sauvegardés ?

Vous pouvez sauvegarder des boîtes aux lettres utilisateur, communes et de groupe. (Facultatif) Vous pouvez également choisir de sauvegarder les boîtes aux lettres d'archive en ligne (**Archives permanentes**) des boîtes aux lettres sélectionnées.

À partir de la version 8.0 du service Cyber Protection, vous pouvez sauvegarder des dossiers publics. Si votre organisation a été ajoutée au service Cyber Protection avant la sortie de la version 8.0, vous devez rajouter l'organisation pour obtenir cette fonctionnalité. Ne supprimez pas l'organisation, répétez simplement les étapes décrites dans "Ajout d'une organisation Microsoft 365" (p. 638). Par conséquent, le service Cyber Protection obtient la permission d'utiliser l'API correspondante.

Quels éléments de données peuvent être restaurés ?

Les éléments suivants peuvent être restaurés à partir de sauvegardes de boîte aux lettres :

- Boîtes aux lettres
- Dossiers de courriers électroniques
- Messages de courriers électroniques
- Événements de calendrier
- Tâches
- Contacts
- Entrées de journal
- Notes

Les éléments suivants peuvent être restaurés à partir d'une sauvegarde de dossier public :

- Sous-dossiers
- Publications
- Messages de courriers électroniques

Vous pouvez utiliser la fonction de recherche pour trouver l'emplacement des éléments.

Lorsque vous restaurez des boîtes aux lettres, des éléments de boîte aux lettres, des dossiers publics et des éléments de dossiers publics, vous pouvez choisir d'écraser ou non les éléments de l'emplacement de destination.

Sélection de boîtes aux lettres

Sélectionnez les boîtes aux lettres comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Sélection de boîtes aux lettres Exchange Online

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données utilisateur. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour sauvegarder les boîtes aux lettres de tous les utilisateurs et toutes les boîtes aux lettres communes (y compris celles qui seront créées à l'avenir), développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, puis cliquez sur **Sauvegarde de groupe**.
   - Pour sauvegarder des boîtes aux lettres utilisateur ou communes, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez sauvegarder les boîtes aux lettres, puis cliquez sur **Sauvegarde**.

- Pour sauvegarder toutes les boîtes aux lettres de groupe (y compris celles des groupes qui seront créés à l'avenir), développez le nœud **Groupes**, sélectionnez **Tous les groupes**, puis cliquez sur **Sauvegarde de groupe**.
- Pour sauvegarder des boîtes aux lettres de groupe en particulier, développez le nœud **Groupes**, sélectionnez **Tous les groupes**, sélectionnez les groupes dont vous souhaitez sauvegarder les boîtes aux lettres, puis cliquez sur **Sauvegarde**.

Remarque
L'agent Cloud pour Microsoft 365 accède à une boîte aux lettres de groupe à l'aide d'un compte doté des droits appropriés. Par conséquent, pour sauvegarder une boîte aux lettres de groupe, au moins un des propriétaires du groupe doit être un utilisateur Microsoft 365 disposant d'une licence avec une boîte aux lettres. Si le groupe est privé ou à appartenance masquée, le propriétaire doit également être membre du groupe.

4. Dans le volet du plan de protection :
   - Dans **Quoi sauvegarder**, assurez-vous que **Boîtes aux lettres Microsoft 365** est sélectionné.
     Si certains des utilisateurs sélectionnés individuellement n'ont pas le service Exchange inclus dans leur plan Microsoft 365, vous ne pourrez pas sélectionner cette option.
     Si certains des utilisateurs sélectionnés pour la sauvegarde de groupe n'ont pas le service Exchange inclus dans leur plan Microsoft 365, vous pourrez sélectionner cette option, mais le plan de protection ne sera pas appliqué à ces utilisateurs.
   - Si vous ne souhaitez pas sauvegarder les boîtes aux lettres d'archive, désactivez l'interrupteur **Boîte aux lettres d'archive**.

Sélection de dossiers publics

Sélectionnez les dossiers publics comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Remarque
Les dossiers publics utilisent les licences de votre quota de sauvegarde pour les postes Microsoft 365.

Pour sélectionner des dossiers publics Exchange Online

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, développez l'organisation pour laquelle vous souhaitez restaurer les données. Sinon, ignorez cette étape.
3. Étendez le nœud **Dossiers publics**, puis sélectionnez **Tous les dossiers publics**.
4. Effectuez l'une des actions suivantes :
   - Pour sauvegarder tous les dossiers publics (y compris les dossiers publics qui seront créés à l'avenir), cliquez sur **Sauvegarde de groupe**.

- Pour sauvegarder des dossiers publics en particulier, sélectionnez ceux que vous souhaitez sauvegarder, puis cliquez sur **Sauvegarder**.

5. Dans le volet du plan de protection, assurez-vous que **Boîtes aux lettres Microsoft 365** est sélectionné dans **Quoi sauvegarder**.

Restauration de boîtes aux lettres et d'éléments de boîte aux lettres

Restauration de boîtes aux lettres

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour restaurer une boîte aux lettres utilisateur, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez restaurer la boîte aux lettres, puis cliquez sur **Restauration**.
   - Pour restaurer une boîte aux lettres commune, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez la boîte aux lettres commune que vous souhaitez restaurer, puis cliquez sur **Restauration**.
   - Pour restaurer une boîte aux lettres de groupe, développez le nœud **Groupes**, sélectionnez **Tous les groupes**, sélectionnez le groupe dont vous souhaitez restaurer la boîte aux lettres, puis cliquez sur **Restauration**.
   - Si la boîte aux lettres utilisateur, de groupe ou commune a été supprimée, sélectionnez-la dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les utilisateurs et les groupes par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.

   Remarque
   Pour afficher uniquement les points de récupération qui contiennent des boîtes aux lettres, sélectionnez **Boîtes aux lettres** dans **Filtre par contenu**.

5. Cliquez sur **Restaurer** > **Intégralité de la boîte aux lettres**.
6. Si plusieurs organisations Microsoft 365 sont ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.
   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
7. Dans **Restaurer vers la boîte aux lettres**, affichez, modifiez ou spécifiez la boîte aux lettres cible.

Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier la boîte aux lettres cible.

Vous ne pouvez pas créer une nouvelle boîte aux lettres cible pendant la restauration. Pour restaurer une boîte aux lettres vers une nouvelle, vous devez d'abord créer la boîte aux lettres cible dans l'organisation Microsoft 365 souhaitée, puis laisser l'agent cloud synchroniser le changement. L'agent cloud se synchronise automatiquement avec Microsoft 365 toutes les 24 heures. Pour synchroniser la modification immédiatement, sélectionnez dans la console Cyber Protect l'organisation sur la page **Microsoft 365**, puis cliquez sur **Actualiser**.

8. Cliquez sur **Démarrer la récupération**.
9. Sélectionnez l'une des options d'écrasement :
   - **Écraser les éléments existants**
   - **Ne pas écraser les éléments existants**
10. Cliquez sur **Continuer** pour confirmer votre choix.

Restauration d'éléments de boîte aux lettres

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour restaurer des éléments d'une boîte aux lettres utilisateur, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont la boîte aux lettres contenait à l'origine les éléments à restaurer, puis cliquez sur **Restauration**.
   - Pour restaurer les éléments d'une boîte aux lettres commune, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez la boîte aux lettres commune qui contenait à l'origine les éléments que vous souhaitez restaurer, puis cliquez sur **Restauration**.
   - Pour restaurer des éléments d'une boîte aux lettres de groupe, développez le nœud **Groupes**, sélectionnez **Tous les groupes**, sélectionnez le groupe dont la boîte aux lettres contenait à l'origine les éléments à restaurer, puis cliquez sur **Restauration**.
   - Si la boîte aux lettres utilisateur, de groupe ou commune a été supprimée, sélectionnez-la dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les utilisateurs et les groupes par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.

Remarque
Pour afficher uniquement les points de récupération qui contiennent des boîtes aux lettres, sélectionnez **Boîtes aux lettres** dans **Filtre par contenu**.

5. Cliquez sur **Restaurer** > **Messages électroniques**.
6. Parcourez le dossier requis ou utilisez la fonction de recherche pour obtenir la liste des éléments requis.

   Les options de recherche suivantes sont disponibles. Les caractères génériques ne sont pas pris en charge.

   - Pour les e-mails : recherche par objet, expéditeur, destinataire, nom de la pièce jointe et date. Vous pouvez sélectionner une date de début ou une date de fin (toutes deux incluses), ou les deux dates pour effectuer une recherche dans un intervalle de temps.
   - Pour les événements : recherche par titre et date.
   - Pour les tâches : recherche par sujet et date.
   - Pour les contacts : recherche par nom, adresse e-mail et numéro de téléphone.
7. Sélectionnez les éléments que vous souhaitez restaurer. Pour pouvoir sélectionner les dossiers, cliquez sur l'icône des dossiers à restaurer : 

   Vous ne pouvez pas créer de nouvelle boîte aux lettres cible pendant la restauration. Pour restaurer un nouvel élément de boîte aux lettres vers une nouvelle boîte aux lettres, vous devez d'abord créer le nouvel élément de boîte aux lettres cible dans l'organisation Microsoft 365, puis laisser l'agent cloud synchroniser la modification. L'agent cloud se synchronise automatiquement avec Microsoft 365 toutes les 24 heures. Pour synchroniser la modification immédiatement, sélectionnez dans la console Cyber Protect l'organisation sur la page **Microsoft 365**, puis cliquez sur **Actualiser**.

   Par ailleurs, vous pouvez effectuer l'une des opérations suivantes :

   - Lorsqu'un élément est sélectionné, cliquez sur **Afficher le contenu** pour afficher son contenu, y compris les pièces jointes. Cliquez sur le nom d'un fichier joint pour le télécharger.
   - Lorsqu'un message de courrier électronique ou un élément de calendrier est sélectionné, vous pouvez cliquer sur **Envoyer sous forme de message électronique** pour l'envoyer aux adresses électroniques spécifiées. Vous pouvez sélectionner l'expéditeur et rédiger un message qui sera ajouté à l'élément transféré.
   - Uniquement si la sauvegarde n'est pas chiffrée, que vous avez utilisé la fonction de recherche et que vous avec sélectionné un seul élément dans les résultats de recherche : cliquez sur **Afficher les versions** pour sélectionner la version de l'élément à restaurer. Vous pouvez choisir n'importe quelle version sauvegardée, avant ou après le point de récupération sélectionné.
8. Cliquez sur **Restaurer**.
9. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.

   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
10. Dans **Restaurer vers la boîte aux lettres**, affichez, modifiez ou spécifiez la boîte aux lettres cible.

Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier la boîte aux lettres cible.

11. [Uniquement lors de la restauration vers une boîte aux lettres utilisateur ou commune] Dans **Chemin d'accès**, affichez ou modifiez le dossier cible dans la boîte aux lettres cible. Par défaut, le dossier **Éléments restaurés** est sélectionné.

    Les éléments d'une boîte aux lettres de groupe sont toujours restaurés dans le dossier **Boîte de réception**.
12. Cliquez sur **Démarrer la récupération**.
13. Sélectionnez l'une des options d'écrasement :
    - **Écraser les éléments existants**
    - **Ne pas écraser les éléments existants**
14. Cliquez sur **Continuer** pour confirmer votre choix.

Restauration de l'intégralité de boîtes aux lettres dans des fichiers de données PST

Remarque
L'archive en place ne peut pas être restaurée dans le cadre de la restauration vers des fichiers PST. Pour restaurer l'archive en place avec la boîte aux lettres, reportez-vous à "Restauration de boîtes aux lettres" (p. 645).

Restaurer une boîte aux lettres

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour restaurer une boîte aux lettres utilisateur dans un fichier de données PST, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez restaurer la boîte aux lettres, puis cliquez sur **Reprise**.
   - Pour restaurer une boîte aux lettres partagée dans un fichier de données PST, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez la boîte aux lettres que vous souhaitez restaurer, puis cliquez sur **Restauration**.
   - Pour restaurer une boîte aux lettres de groupe dans un fichier de données PST, développez le nœud **Groupes**, sélectionnez **Tous les groupes**, sélectionnez le groupe dont vous souhaitez restaurer la boîte aux lettres, puis cliquez sur **Restauration**.

   Vous pouvez rechercher les utilisateurs et les groupes par nom. Les caractères génériques ne sont pas pris en charge.

   Si le fichier de données Outlook utilisateur, de groupe ou partagées a été supprimé, sélectionnez l'élément dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.
4. Cliquez sur **Restaurer** > **En tant que fichiers PST**.

5. Définissez le mot de passe pour chiffrer l'archive avec le fichier PST.
   Le mot de passe doit contenir au moins un symbole.
6. Confirmez le mot de passe et cliquez sur **Terminé**.
7. Les éléments de boîte aux lettres sélectionnés seront restaurés sous la forme de fichiers de données PST et archivés au format ZIP. La taille maximale d'un fichier PST est limitée à 2 Go. Si la quantité de données que vous restaurez dépasse 2 Go, les données seront divisées en plusieurs fichiers PST. L'archive ZIP sera protégée par le mot de passe que vous avez défini.
8. Vous recevrez un e-mail avec un lien vers l'archive ZIP contenant les fichiers PST créés.
9. L'administrateur recevra une notification par e-mail l'informant que vous avez exécuté la procédure de restauration.

Remarque
La reprise d'une boîte aux lettres dans des fichiers PST peut prendre du temps, car elle suppose non seulement le transfert de données, mais également leur transformation à l'aide d'algorithmes complexes.

Télécharger l'archive contenant les fichiers PST et effectuer la restauration

1. Effectuez l'une des actions suivantes :
   - Pour télécharger l'archive depuis l'e-mail, suivez le lien **Téléchargement des fichiers**. L'archive est disponible au téléchargement sous 24 heures. Si le lien expire, répétez la procédure de restauration.
   - Télécharger l'archive à partir de la console Cyber Protect :
     a. Accédez à **Stockage de sauvegarde** > **Fichiers PST**.
     b. Sélectionnez la dernière archive mise en évidence.
     c. Cliquez sur **Télécharger** dans le volet de droite.

   L'archive sera téléchargée dans le répertoire de téléchargement par défaut sur votre ordinateur.
2. Extrayez les fichiers PST depuis l'archive à l'aide du mot de passe que vous avez défini pour chiffrer l'archive.
3. Ouvrez les fichiers PST avec Microsoft Outlook.
   Les fichiers PST résultants peuvent être beaucoup plus petits que la boîte aux lettres d'origine. C'est un comportement normal.

   Important
   N'importez pas ces fichiers dans Microsoft Outlook à l'aide de l'**assistant d'importation et d'exportation**.
   Ouvrez les fichiers : double-cliquez dessus, ou cliquez avec le bouton droit et sélectionnez **Ouvrir avec...** > **Microsoft Outlook** dans le menu contextuel.

Restauration d'éléments de boîte aux lettres vers des fichiers PST

Remarque
L'archive en place ne peut pas être restaurée dans le cadre de la restauration vers des fichiers PST. Pour restaurer l'archive en place avec la boîte aux lettres, reportez-vous à "Restauration de boîtes aux lettres" (p. 645).

Restaurer des éléments de boîte aux lettres

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour restaurer des éléments d'une boîte aux lettres utilisateur, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont la boîte aux lettres contenait à l'origine les éléments à restaurer, puis cliquez sur **Restauration**.
   - Pour restaurer les éléments d'une boîte aux lettres commune, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez la boîte aux lettres commune qui contenait à l'origine les éléments que vous souhaitez restaurer, puis cliquez sur **Restauration**.
   - Pour restaurer des éléments d'une boîte aux lettres de groupe, développez le nœud **Groupes**, sélectionnez **Tous les groupes**, sélectionnez le groupe dont la boîte aux lettres contenait à l'origine les éléments à restaurer, puis cliquez sur **Restauration**.
   - Si la boîte aux lettres utilisateur, de groupe ou commune a été supprimée, sélectionnez-la dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les utilisateurs et les groupes par nom. Les caractères génériques ne sont pas pris en charge.
4. Cliquez sur **Restaurer** > **Messages électroniques**.
5. Parcourez le dossier requis ou utilisez la fonction de recherche pour obtenir la liste des éléments requis.

   Les options de recherche suivantes sont disponibles. Les caractères génériques ne sont pas pris en charge.
   - Pour les messages de courrier électronique : recherche par sujet, expéditeur, destinataire, nom de la pièce jointe et date.
   - Pour les événements : recherche par titre et date.
   - Pour les tâches : recherche par sujet et date.
   - Pour les contacts : recherche par nom, adresse e-mail et numéro de téléphone.

6. Sélectionnez les éléments que vous souhaitez restaurer. Pour pouvoir sélectionner les dossiers, cliquez sur l'icône des dossiers à restaurer : 

   Par ailleurs, vous pouvez effectuer l'une des opérations suivantes :
   - Lorsqu'un élément est sélectionné, cliquez sur **Afficher le contenu** pour afficher son contenu, y compris les pièces jointes. Cliquez sur le nom d'un fichier de pièce jointe pour le télécharger.
   - Lorsqu'un message de courrier électronique ou un élément de calendrier est sélectionné, vous pouvez cliquer sur **Envoyer sous forme de message électronique** pour l'envoyer aux adresses électroniques spécifiées. Vous pouvez sélectionner l'expéditeur et rédiger un message qui sera ajouté à l'élément transféré.
   - Uniquement si la sauvegarde n'est pas chiffrée, que vous avez utilisé la fonction de recherche et que vous avec sélectionné un seul élément dans les résultats de recherche : cliquez sur **Afficher les versions** pour sélectionner la version de l'élément à restaurer. Vous pouvez choisir n'importe quelle version sauvegardée, avant ou après le point de récupération sélectionné.
7. Cliquez sur **Restaurer en tant que fichiers PST**.
8. Définissez le mot de passe pour chiffrer l'archive avec le fichier PST.

   Le mot de passe doit contenir au moins un symbole.
9. Confirmez le mot de passe et cliquez sur **TERMINÉ**.

Les éléments de boîte aux lettres sélectionnés seront restaurés sous la forme de fichiers de données PST et archivés au format ZIP. La taille maximale d'un fichier PST est limitée à 2 Go. Si la quantité de données que vous restaurez dépasse 2 Go, les données seront divisées en plusieurs fichiers PST. L'archive ZIP sera protégée par le mot de passe que vous avez défini.

Vous recevrez un e-mail avec un lien vers l'archive ZIP contenant les fichiers PST créés.

L'administrateur recevra une notification par e-mail l'informant que vous avez exécuté la procédure de restauration.

Télécharger l'archive contenant les fichiers PST et effectuer la restauration

1. Effectuez l'une des actions suivantes :
   - Pour télécharger l'archive depuis l'e-mail, suivez le lien **Téléchargement des fichiers**. L'archive est disponible au téléchargement sous 24 heures. Si le lien expire, répétez la procédure de restauration.
   - Télécharger l'archive à partir de la console Cyber Protect :
     a. Accédez à **Stockage de sauvegarde** > **Fichiers PST**.
     b. Sélectionnez la dernière archive mise en évidence.
     c. Cliquez sur **Télécharger** dans le volet de droite.

   L'archive sera téléchargée dans le répertoire de téléchargement par défaut sur votre ordinateur.
2. Extrayez les fichiers PST depuis l'archive à l'aide du mot de passe que vous avez défini pour chiffrer l'archive.

3. Ouvrez les fichiers PST avec Microsoft Outlook.

   Les fichiers PST résultants peuvent être beaucoup plus petits que la boîte aux lettres d'origine. C'est un comportement normal.

   Important
   N'importez pas ces fichiers dans Microsoft Outlook à l'aide de l'**assistant d'importation et d'exportation**.

   Ouvrez les fichiers en double-cliquant dessus, ou en cliquant dessus avec le bouton droit de la souris et en sélectionnant **Ouvrir avec...** > **Microsoft Outlook** dans le menu contextuel.

Restauration de dossiers publics et d'éléments de dossier

Pour restaurer un dossier public ou des éléments de dossier public, au moins un administrateur de l'organisation Microsoft 365 cible doit posséder les droits **Propriétaire** pour le dossier public cible. Si la restauration échoue en affichant une erreur concernant un accès refusé, affectez ces droits dans les propriétés du dossier cible, sélectionnez l'organisation cible dans la console Cyber Protect, cliquez sur **Actualiser**, puis répétez la restauration.

Pour restaurer un dossier public ou des éléments de dossier

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 sont ajoutées au service Cyber Protection, développez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Développez le nœud **Dossiers publics**, sélectionnez **Tous les dossiers publics**, sélectionnez le dossier public que vous souhaitez restaurer ou qui contenait à l'origine les éléments à restaurer, puis cliquez sur **Restauration**.
   - Si le dossier public a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher des dossiers publics par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.
5. Cliquez sur **Récupérer des données**.
6. Parcourez le dossier requis ou utilisez la fonction de recherche pour obtenir la liste des éléments requis.

   Vous pouvez rechercher les e-mails et publications par sujet, expéditeur, destinataire et date. Les caractères génériques ne sont pas pris en charge.
7. Sélectionnez les éléments que vous souhaitez restaurer. Pour pouvoir sélectionner les dossiers, cliquez sur l'icône des dossiers à restaurer : 

   Par ailleurs, vous pouvez effectuer l'une des opérations suivantes :

- Lorsqu'un e-mail ou une publication est sélectionné, cliquez sur **Afficher le contenu** pour afficher son contenu, y compris les pièces jointes. Cliquez sur le nom d'un fichier de pièce jointe pour le télécharger.
- Lorsqu'un e-mail ou une publication est sélectionné, cliquez sur **Envoyer sous forme d'e-mail** pour l'envoyer aux adresses e-mail spécifiées. Vous pouvez sélectionner l'expéditeur et rédiger un message qui sera ajouté à l'élément transféré.
- Uniquement si la sauvegarde n'est pas chiffrée, que vous avez utilisé la fonction de recherche et que vous avec sélectionné un seul élément dans les résultats de recherche : cliquez sur **Afficher les versions** pour sélectionner la version de l'élément à restaurer. Vous pouvez choisir n'importe quelle version sauvegardée, avant ou après le point de récupération sélectionné.

8. Cliquez sur **Restaurer**.
9. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.
   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
10. Dans **Restaurer dans un dossier public**, affichez, modifiez ou spécifiez le dossier public cible.
    Le dossier d'origine est sélectionné par défaut. Si ce dossier n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier le dossier cible.
    Vous ne pouvez pas créer de nouveau dossier public pendant la restauration. Pour restaurer un dossier public vers un nouveau, vous devez d'abord créer le dossier public cible dans l'organisation Microsoft 365 souhaitée, puis laisser l'agent cloud synchroniser la modification. L'agent cloud se synchronise automatiquement avec Microsoft 365 toutes les 24 heures. Pour synchroniser la modification immédiatement, sélectionnez dans la console Cyber Protect l'organisation sur la page **Microsoft 365**, puis cliquez sur **Actualiser**.
11. Dans **Chemin d'accès**, affichez ou modifiez le sous-dossier cible dans le dossier public cible. Par défaut, le chemin d'accès d'origine sera recréé.
12. Cliquez sur **Démarrer la récupération**.
13. Sélectionnez l'une des options d'écrasement :

Option	Description
Écraser les éléments existants	Tous les fichiers existants dans l'emplacement de destination sont remplacés.
Ne pas écraser les éléments existants	Si l'emplacement de destination comporte un fichier de même nom, ce fichier n'est pas écrasé et le fichier source n'est pas enregistré dans l'emplacement de destination.

14. Cliquez sur **Continuer** pour confirmer votre choix.

Protection des fichiers OneDrive

Quels éléments peuvent être sauvegardés ?

Vous pouvez sauvegarder l'intégralité de OneDrive, ou des fichiers et dossiers en particulier.

Une option distincte dans le plan de sauvegarde permet de sauvegarder des blocs-notes OneNote.

Les fichiers sont sauvegardés avec les permissions de partage associées. Les niveaux de permission avancés (**Création**, **Complet**, **Contribution**) ne sont pas sauvegardés.

Certains fichiers sont susceptibles de contenir des informations sensibles, et l'accès à ces derniers peut être bloqué par une règle DLP (prévention de perte de données) dans Microsoft 365. Ces fichiers ne sont pas sauvegardés, et aucun avertissement n'est affiché une fois l'opération de sauvegarde terminée.

Limites

La sauvegarde de contenu OneDrive Contenu n'est pas prise en charge pour les boîtes aux lettres partagées. Pour sauvegarder ce contenu, convertissez la boîte aux lettres partagée en compte utilisateur standard et vérifiez que OneDrive est activé pour ce compte.

Quels éléments de données peuvent être restaurés ?

Vous pouvez restaurer l'intégralité de OneDrive, ou tout fichier ou dossier sauvegardé.

Vous pouvez utiliser la fonction de recherche pour trouver l'emplacement des éléments.

Vous pouvez choisir de restaurer les permissions de partage ou de laisser les fichiers hériter des permissions du dossier vers lequel ils sont restaurés.

Les liens de partage des fichiers et des dossiers ne sont pas restaurés.

Sélection de fichiers OneDrive

Sélectionnez les fichiers comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Sélection de fichiers OneDrive

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données utilisateur. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour sauvegarder les fichiers de tous les utilisateurs (y compris des utilisateurs qui seront créés à l'avenir), développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, puis cliquez sur **Sauvegarde de groupe**.

- Pour sauvegarder les fichiers d'utilisateurs en particulier, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez sauvegarder les fichiers, puis cliquez sur **Sauvegarde**.

4. Dans le volet du plan de protection :
   - Dans **Quoi sauvegarder**, assurez-vous que **OneDrive** est sélectionné.

     Si certains des utilisateurs sélectionnés individuellement n'ont pas le service OneDrive inclus dans leur plan Microsoft 365, vous ne pourrez pas sélectionner cette option.

     Si certains des utilisateurs sélectionnés pour la sauvegarde de groupe n'ont pas le service OneDrive inclus dans leur plan Microsoft 365, vous pourrez sélectionner cette option, mais le plan de protection ne sera pas appliqué à ces utilisateurs.
   - Dans **Éléments à sauvegarder**, effectuez l'une des actions suivantes :
     - Conservez le paramètre par défaut **[Tous]** (tous les fichiers).
     - Spécifiez les fichiers et dossiers à sauvegarder en ajoutant leur nom ou leur chemin d'accès.

       Vous pouvez utiliser des caractères génériques (*, ** et ?). Pour en savoir plus sur la définition de chemin d'accès et sur l'utilisation de caractères génériques, consultez la section « Filtres de fichiers ».
     - Spécifiez les fichiers et dossiers à sauvegarder en cliquant sur Parcourir.

       Le lien **Parcourir** est disponible uniquement lors de la création d'un plan de protection pour un seul utilisateur.
   - [Facultatif] Dans **Éléments à sauvegarder**, cliquez sur **Afficher les exclusions** pour spécifier les fichiers et dossiers à ignorer lors de la sauvegarde.

     Les exclusions ont priorité sur la sélection de fichiers, c'est-à-dire que si vous spécifiez le même fichier dans les deux champs, ce fichier sera ignoré lors de la sauvegarde.
   - [Facultatif] Pour sauvegarder des blocs-notes OneNote, activez l'interrupteur **Inclure OneNote**.

Restauration de OneDrive et de fichiers OneDrive

Restauration de l'intégralité de OneDrive

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez restaurer le OneDrive, puis cliquez sur **Restauration**.

   Si l'utilisateur a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les utilisateurs par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.

Remarque
Pour afficher uniquement les points de récupération qui contiennent des fichiers OneDrive, sélectionnez **OneDrive** dans **Filtre par contenu**.

5. Cliquez sur **Restaurer** > **Intégralité de OneDrive**.
6. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.
   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
   Vous ne pouvez pas créer une nouvelle cible OneDrive pendant la récupération. Pour restaurer un OneDrive sur un nouveau, vous devez d'abord créer le OneDrive cible dans l'organisation Microsoft 365, puis laisser l'agent cloud synchroniser le changement. L'agent cloud se synchronise automatiquement avec Microsoft 365 toutes les 24 heures. Pour synchroniser la modification immédiatement, sélectionnez dans la console Cyber Protect l'organisation sur la page **Microsoft 365**, puis cliquez sur **Actualiser**.
7. Dans **Restaurer vers le lecteur**, affichez, modifiez ou spécifiez l'utilisateur cible.
   L'utilisateur d'origine est sélectionné par défaut. Si cet utilisateur n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier l'utilisateur cible.
8. Choisissez de restaurer ou non les permissions de partage associées aux fichiers.
9. Cliquez sur **Démarrer la récupération**.
10. Sélectionnez l'une des options d'écrasement :

Option	Description
Écraser un fichier existant s'il est plus ancien	Si l'emplacement de destination comporte un fichier de même nom, mais plus ancien que le fichier source, le fichier source est enregistré dans l'emplacement de destination et remplace l'ancienne version.
Écraser les fichiers existants	Tous les fichiers existants dans l'emplacement de destination sont remplacés, quelle que soit la date de leur dernière modification.
Ne pas écraser les fichiers existants	Si l'emplacement de destination comporte un fichier de même nom, aucune modification ne lui est appliquée et le fichier source n'est pas enregistré dans l'emplacement de destination.

Remarque
Lorsque vous restaurez des blocs-notes OneNote, les options **Écraser un fichier existant s'il est plus ancien** et **Écraser les fichiers existants** remplaceront les blocs-notes OneNote existants.

11. Cliquez sur **Continuer** pour confirmer votre choix.

Restauration de fichiers OneDrive

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez restaurer les fichiers OneDrive, puis cliquez sur **Restauration**.

   Si l'utilisateur a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les utilisateurs par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.

   Remarque
   Pour afficher uniquement les points de récupération qui contiennent des fichiers OneDrive, sélectionnez **OneDrive** dans **Filtre par contenu**.
5. Cliquez sur **Restaurer** > **Fichiers/dossiers**.
6. Recherchez le dossier requis ou utilisez la fonction de recherche pour obtenir la liste des fichiers et des dossiers requis.
7. Sélectionnez les fichiers que vous voulez restaurer.

   Si la sauvegarde n'est pas chiffrée et que vous avez sélectionné un seul fichier, vous pouvez cliquer sur **Afficher les versions** pour sélectionner la version du fichier à restaurer. Vous pouvez choisir n'importe quelle version sauvegardée, avant ou après le point de récupération sélectionné.
8. Si vous souhaitez télécharger un fichier, sélectionnez-le, cliquez sur **Télécharger**, sélectionnez l'emplacement dans lequel le sauvegarder, puis cliquez sur **Sauvegarder**. Sinon, ignorez cette étape.
9. Cliquez sur **Restaurer**.
10. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.

    L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.

    Vous ne pouvez pas créer de nouveau OneDrive pendant la restauration. Pour restaurer un fichier vers un nouveau OneDrive, vous devez d'abord créer le OneDrive cible dans l'organisation Microsoft 365 souhaitée, puis laisser l'agent cloud synchroniser la modification. L'agent cloud se synchronise automatiquement avec Microsoft 365 toutes les 24 heures. Pour synchroniser la modification immédiatement, sélectionnez dans la console Cyber Protect l'organisation sur la page **Microsoft 365**, puis cliquez sur **Actualiser**.
11. Dans **Restaurer vers le lecteur**, affichez, modifiez ou spécifiez l'utilisateur cible.

L'utilisateur d'origine est sélectionné par défaut. Si cet utilisateur n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier l'utilisateur cible.

12. Dans **Chemin d'accès**, affichez ou modifiez le dossier cible dans le OneDrive de l'utilisateur cible. L'emplacement d'origine est sélectionné par défaut.
13. Choisissez de restaurer ou non les permissions de partage associées aux fichiers.
14. Cliquez sur **Démarrer la récupération**.
15. Sélectionnez l'une des options d'écrasement de fichier :

Option	Description
Écraser un fichier existant s'il est plus ancien	Si l'emplacement de destination comporte un fichier de même nom, mais plus ancien que le fichier source, le fichier source est enregistré dans l'emplacement de destination et remplace l'ancienne version.
Écraser les fichiers existants	Tous les fichiers existants dans l'emplacement de destination sont remplacés, quelle que soit la date de leur dernière modification.
Ne pas écraser les fichiers existants	Si l'emplacement de destination comporte un fichier de même nom, aucune modification ne lui est appliquée et le fichier source n'est pas enregistré dans l'emplacement de destination.

Remarque
Lorsque vous restaurez des blocs-notes OneNote, les options **Écraser un fichier existant s'il est plus ancien** et **Écraser les fichiers existants** remplaceront les blocs-notes OneNote existants.

16. Cliquez sur **Continuer** pour confirmer votre choix.

Protection de sites SharePoint Online

Quels éléments peuvent être sauvegardés ?

Vous pouvez sauvegarder les collections de sites classiques, les sites de groupe (équipe moderne) et les sites de communication de SharePoint. Vous pouvez également sélectionner des sous-sites, listes et bibliothèques particuliers pour les sauvegarder.

Une option distincte dans le plan de sauvegarde permet de sauvegarder des blocs-notes OneNote.

Les éléments suivants sont *exclus* lors d'une sauvegarde :

- Les paramètres de **Vue d'ensemble** du site (à l'exception du **titre, de la description et du logo**).
- Les commentaires des pages du site et les paramètres de commentaire des pages (commentaires **Activés**/**Désactivés**).
- Le **Site comprend** les paramètres du site.

- Les pages de composants WebPart et les composants WebPart intégrés aux pages wiki (en raison des limitations de l'API de SharePoint Online).
- Fichiers extraits : fichiers extraits manuellement pour être modifiés, et tous les fichiers créés ou transférés dans des bibliothèques et pour lesquels l'option **Nécessite une extraction** a été activée. Pour sauvegarder ces fichiers, vous devez d'abord les archiver.
- Les types de colonnes Données externes et Métadonnées gérées.
- La collection de sites par défaut « domain-my.sharepoint.com ». Il s'agit d'une collection dans laquelle sont stockés les fichiers OneDrive de tous les utilisateurs de l'organisation.
- Le contenu de la corbeille.

Limites

- Les titres et descriptions des sites/sous-sites/listes/colonnes sont tronqués lors d'une sauvegarde si la taille du titre/de la description dépasse 10 000 octets.
- Vous ne pouvez pas sauvegarder des versions précédentes de fichiers créés dans SharePoint Online. Seules les dernières versions des fichiers sont protégées.
- Vous ne pouvez pas sauvegarder la bibliothèque de conservation.
- Vous ne pouvez pas sauvegarder les sites créés dans Business Productivity Online Suite (BPOS), le prédécesseur de Microsoft 365.
- Vous ne pouvez pas sauvegarder les paramètres des sites qui utilisent le chemin d'accès géré/les `portails` gérés (par exemple, `https://<tenant>.sharepoint.com/portals/...`).
- Vous pouvez restaurer les paramètres de gestion des droits relatifs à l'information (Information Rights Gestion – IRM) d'une liste ou d'une bibliothèque uniquement si l'IRM est activée dans l'organisation Microsoft 365 cible.

Quels éléments de données peuvent être restaurés ?

Les éléments suivants peuvent être restaurés à partir de sauvegardes de site :

- Site entier
- Sous-sites
- Listes
- Éléments de liste
- Bibliothèques de documents
- Documents
- Pièces jointes d'éléments de liste
- Pages de site et pages de Wiki

Vous pouvez utiliser la fonction de recherche pour trouver l'emplacement des éléments.

Les éléments peuvent être restaurés vers le site d'origine ou vers un autre site. Le chemin d'accès à un élément restauré est identique au chemin d'accès d'origine. Si le chemin d'accès n'existe pas, il sera créé.

Vous pouvez choisir de restaurer les permissions de partage ou de laisser les éléments hériter des permissions de l'objet parent après la restauration.

Quels éléments ne peuvent pas être restaurés ?

- Sous-sites basés sur le modèle de **Référentiel de processus dans Visio**.
- Les listes de types suivants : **Liste de sondages**, **Liste de tâches**, **Bibliothèque d'images**, **Liens**, **Calendrier**, **Forum de discussion**, **Externe** et **Feuilles de calcul d'import**.
- Les listes pour lesquelles plusieurs types de contenu sont activés.

Sélection de données SharePoint Online

Sélectionnez les données comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Pour sélectionner des données SharePoint Online

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données utilisateur. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour sauvegarder tous les sites SharePoint classiques de l'organisation, y compris les sites qui seront créés à l'avenir, développez le nœud **Collections de sites**, sélectionnez **Toutes les collections de sites**, puis cliquez sur **Sauvegarde de groupe**.
   - Pour sauvegarder des sites classiques en particulier, développez le nœud **Collections de sites**, sélectionnez **Toutes les collections de sites**, sélectionnez les sites que vous souhaitez sauvegarder, puis cliquez sur **Sauvegarde**.
   - Pour sauvegarder tous les sites de groupe (équipe moderne), y compris les sites qui seront créés à l'avenir, développez le nœud **Groupes**, sélectionnez **Tous les groupes**, puis cliquez sur **Sauvegarde de groupe**.
   - Pour sauvegarder des sites de groupe (équipe moderne) en particulier, développez le nœud **Groupes**, sélectionnez **Tous les groupes**, sélectionnez les groupes dont vous souhaitez sauvegarder les sites, puis cliquez sur **Sauvegarde**.
4. Dans le volet du plan de protection :
   - Dans **Quoi sauvegarder**, assurez-vous que **Sites SharePoint** est sélectionné.
   - Dans **Éléments à sauvegarder**, effectuez l'une des actions suivantes :
     - Conservez le paramètre par défaut **[Tous]** (tous les éléments des sites sélectionnés).
     - Spécifiez les sous-sites, listes, et bibliothèques à sauvegarder en ajoutant leur nom ou leur chemin d'accès.

       Pour sauvegarder un sous-site ou une liste/bibliothèque de sites de premier niveau, spécifiez son nom affiché au format suivant : `/nom affiché/**`

Pour sauvegarder une liste/bibliothèque de sous-sites, spécifiez son nom affiché au format suivant : `/nom affiché du sous-site/nom affiché de la liste/**`

Le nom affiché des sous-sites, des listes et des bibliothèques est disponible à la page **Contenu du site** du site ou sous-site SharePoint.

- Spécifiez les sous-sites à sauvegarder en cliquant sur Parcourir.

  Le lien **Parcourir** est disponible uniquement lors de la création d'un plan de protection pour un seul site.

- [Facultatif] Dans **Éléments à sauvegarder**, cliquez sur **Afficher les exclusions** pour spécifier les sous-sites, les listes et les bibliothèques à ignorer lors de la sauvegarde.

  Les exclusions ont la priorité sur la sélection d'éléments, c'est-à-dire que si vous spécifiez le même sous-site dans les deux champs, ce sous-site sera ignoré lors de la sauvegarde.
- [Facultatif] Pour sauvegarder des blocs-notes OneNote, activez l'interrupteur **Inclure OneNote**.

Restauration de données de SharePoint Online

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour restaurer des données depuis un site de groupe (équipe moderne), développez le nœud **Groupes**, sélectionnez **Tous les groupes**, sélectionnez le groupe dont le site contenait à l'origine les éléments à restaurer, puis cliquez sur **Restauration**.
   - Pour restaurer des données depuis un site classique, développez le nœud **Collections de sites**, sélectionnez **Toutes les collections de sites**, sélectionnez le groupe dont le site contenait à l'origine les éléments à restaurer, puis cliquez sur **Restauration**.
   - Si le site a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les groupes et les sites par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.

   Remarque
   Pour afficher uniquement les points de récupération qui contiennent des sites SharePoint, sélectionnez **Sites SharePoint** dans **Filtre par contenu**.
5. Cliquez sur **Restaurer les fichiers SharePoint**.
6. Parcourez le dossier requis ou utilisez la fonction de recherche pour obtenir la liste des éléments de données requis.
7. Sélectionnez les éléments que vous souhaitez restaurer.

Si la sauvegarde n'est pas chiffrée, que vous avez utilisé la fonction de recherche et que vous avec sélectionné un seul élément dans les résultats de recherche, vous pouvez cliquer sur **Afficher les versions** pour sélectionner la version de l'élément à restaurer. Vous pouvez choisir n'importe quelle version sauvegardée, avant ou après le point de récupération sélectionné.

8. [Facultatif] Pour télécharger un élément, sélectionnez-le, cliquez sur **Télécharger**, sélectionner l'emplacement dans lequel vous souhaitez le sauvegarder, puis cliquez sur **Enregistrer**.
9. Cliquez sur **Restaurer**.
10. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.
    L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
11. Dans **Restaurer vers le site**, affichez, modifiez ou spécifiez le site cible.
    Vous ne pouvez pas créer de nouveau site SharePoint pendant la restauration. Pour restaurer un site SharePoint vers un nouveau site, vous devez d'abord créer le site cible dans l'organisation Microsoft 365 souhaitée, puis laisser l'agent cloud synchroniser le changement. L'agent cloud se synchronise automatiquement avec Microsoft 365 toutes les 24 heures. Pour synchroniser la modification immédiatement, sélectionnez dans la console Cyber Protect l'organisation sur la page **Microsoft 365**, puis cliquez sur **Actualiser**.
12. Choisissez de restaurer ou non les permissions de partage associées aux éléments restaurés.
13. Cliquez sur **Démarrer la récupération**.
14. Sélectionnez l'une des options d'écrasement :

Option	Description
Écraser un fichier existant s'il est plus ancien	Si l'emplacement de destination comporte un fichier de même nom, mais plus ancien que le fichier source, le fichier source est enregistré dans l'emplacement de destination et remplace l'ancienne version.
Écraser les fichiers existants	Tous les fichiers existants dans l'emplacement de destination sont remplacés, quelle que soit la date de leur dernière modification.
Ne pas écraser les fichiers existants	Si l'emplacement de destination comporte un fichier de même nom, aucune modification ne lui est appliquée et le fichier source n'est pas enregistré dans l'emplacement de destination.

Remarque
Lorsque vous restaurez des blocs-notes OneNote, les options **Écraser un fichier existant s'il est plus ancien** et **Écraser les fichiers existants** remplaceront les blocs-notes OneNote existants.

15. Cliquez sur **Continuer** pour confirmer votre choix.

Protection des données Microsoft 365 Teams

Quels éléments peuvent être sauvegardés ?

Vous pouvez sauvegarder des équipes entières. Cela inclut le nom de l'équipe, la liste des membres de l'équipe, les canaux d'équipe et leur contenu, la boîte aux lettres et les réunions de l'équipe, et le site de l'équipe.

Une option distincte dans le plan de sauvegarde permet de sauvegarder des blocs-notes OneNote.

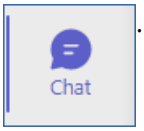
Quels éléments de données peuvent être restaurés ?

- Toute l'équipe
- Canaux d'équipe
- Fichiers de canal
- Boîte aux lettres d'équipe
- Dossiers d'e-mail dans la boîte aux lettres de l'équipe
- E-mails dans la boîte aux lettres de l'équipe
- Réunions
- Site d'équipe

Il est impossible de restaurer des conversations dans les canaux d'équipe, mais vous pouvez les télécharger en tant que fichier html unique.

Limites

Les éléments suivants ne sont pas sauvegardés :

- Les paramètres du canal général (préférence de modération), en raison d'une restriction de l'API bêta de Microsoft Teams.
- Les paramètres des canaux personnalisés (préférence de modération), en raison d'une restriction de l'API bêta de Microsoft Teams.
- Notes de réunion.
- Messages de la section de chat 

. Cette section contient des chats privés en tête-à-tête et des chats de groupe.
- Badges et éloges.

La sauvegarde et la restauration sont prises en charge pour les onglets de canal suivants :

- Word
- Excel

- PowerPoint
- PDF
- Bibliothèque de documents

Sélection des équipes

Sélectionnez les équipes comme décrit ci-dessous, puis indiquez d'autres paramètres du plan de protection au besoin.

Pour sélectionner des équipes

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez sauvegarder les équipes. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour sauvegarder toutes les équipes de l'organisation (y compris les équipes qui seront créées à l'avenir), développez le nœud **Équipes**, sélectionnez **Toutes les équipes**, puis cliquez sur **Sauvegarde de groupe**.
   - Pour sauvegarder des équipes individuelles, développez le nœud **Équipes**, sélectionnez **Toutes les équipes**, sélectionnez les équipes que vous souhaitez sauvegarder, puis cliquez sur **Sauvegarde**.

   Vous pouvez rechercher les équipes par nom. Les caractères génériques ne sont pas pris en charge.
4. Dans le volet du plan de protection :
   - Dans **Quoi sauvegarder**, assurez-vous que **Microsoft Teams** est sélectionné.
   - [Facultatif] Dans **Durée de conservation**, définissez les options de nettoyage.
   - [Facultatif] Si vous souhaitez chiffrer votre sauvegarde, activez le commutateur **Chiffrement**, puis définissez votre mot de passe et sélectionnez l'algorithme de chiffrement.
   - [Facultatif] Pour sauvegarder des blocs-notes OneNote, activez l'interrupteur **Inclure OneNote**.

Restauration de l'intégralité d'une équipe

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les équipes sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Équipes**, sélectionnez **Toutes les équipes**, sélectionnez l'équipe que vous souhaitez restaurer, puis cliquez sur **Restauration**.

   Vous pouvez rechercher les équipes par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.

5. Cliquez sur **Restaurer** > **Toute l'équipe**.

   Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.

   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
6. Dans **Restaurer vers l'équipe**, consultez l'équipe cible ou sélectionnez-en une autre.

   L'équipe d'origine est sélectionnée par défaut. Si cette équipe n'existe pas (par exemple, si elle a été supprimée) ou si vous avez sélectionné une organisation qui ne contient pas l'équipe d'origine, vous devez sélectionner une équipe cible dans la liste déroulante.

   Vous pouvez restaurer une équipe uniquement dans une équipe existante. Vous ne pouvez pas créer d'équipes pendant les opérations de restauration.
7. Cliquez sur **Démarrer la récupération**.
8. Sélectionnez l'une des options d'écrasement :
   - **Écraser le contenu existant s'il est plus ancien**
   - **Écraser le contenu existant**
   - **Ne pas écraser le contenu existant**

   Remarque
   Lorsque vous restaurez des blocs-notes OneNote, les options **Écraser le contenu existant s'il est plus ancien** et **Écraser le contenu existant** remplaceront les blocs-notes OneNote existants.
9. Cliquez sur **Continuer** pour confirmer votre choix.

Lorsque vous supprimez un canal d'une interface graphique de Microsoft Teams, il n'est pas immédiatement supprimé du système. Ainsi, lorsque vous restaurez l'intégralité de l'équipe, le nom de ce canal ne peut pas être utilisé et un suffixe y sera ajouté.

Les conversations sont restaurées en tant que fichier html unique dans l'onglet **Fichiers** du canal. Vous pouvez trouver ce fichier dans un dossier nommé selon le modèle suivant : `<Nom de l'équipe>_<Nom du canal>_sauvegarde_des_conversations_<date de la restauration>T<heure de la restauration>Z`.

Remarque
Après avoir restauré une équipe ou des canaux d'équipe, accédez à Microsoft Teams, sélectionnez les canaux restaurés, puis cliquez sur leur onglet **Fichiers**. Autrement, les sauvegardes suivantes de ces canaux n'incluront pas le contenu de cet onglet, en raison d'une restriction de l'API bêta de Microsoft Teams.

Restaurer des canaux ou des fichiers d'équipe dans les canaux d'équipe

Pour restaurer des canaux d'équipe

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les équipes sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Équipes**, sélectionnez **Toutes les équipes**, sélectionnez l'équipe dont vous souhaitez restaurer les canaux, puis cliquez sur **Restauration**.
4. Sélectionnez un point de restauration.
5. Cliquez sur **Restaurer** > **Canaux**.
6. Sélectionnez les canaux que vous souhaitez restaurer, puis cliquez sur **Restaurer**. Pour sélectionner un canal dans le volet principal, sélectionnez la case en face de son nom.

   Les options de recherche suivantes sont disponibles :
   - Pour **Conversations** : expéditeur, objet, contenu, langue, nom de la pièce jointe, date ou plage de dates.
   - Pour **Fichiers** : nom du fichier ou nom du dossier, type de fichier, taille, date ou plage de dates de la dernière modification.

   Remarque
   Vous pouvez aussi télécharger les fichiers localement, au lieu de les restaurer.
7. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.

   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
8. Dans **Restaurer vers l'équipe**, affichez, modifiez ou indiquez l'équipe cible.

   L'équipe d'origine est sélectionnée par défaut. Si cette équipe n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez indiquer l'équipe cible.
9. Dans **Restaurer vers le canal**, affichez, modifiez ou indiquez le canal cible.
10. Cliquez sur **Démarrer la récupération**.
11. Sélectionnez l'une des options d'écrasement :
    - **Écraser le contenu existant s'il est plus ancien**
    - **Écraser le contenu existant**
    - **Ne pas écraser le contenu existant**

    Remarque
    Lorsque vous restaurez des blocs-notes OneNote, les options **Écraser le contenu existant s'il est plus ancien** et **Écraser le contenu existant** remplaceront les blocs-notes OneNote existants.
12. Cliquez sur **Continuer** pour confirmer votre choix.

Les conversations sont restaurées en tant que fichier html unique dans l'onglet **Fichiers** du canal. Vous pouvez trouver ce fichier dans un dossier nommé selon le modèle suivant : `<Nom de l'équipe>_<Nom du canal>_sauvegarde_des_conversations_<date de la restauration>T<heure de la restauration>Z`.

Remarque
Après avoir restauré une équipe ou des canaux d'équipe, accédez à Microsoft Teams, sélectionnez les canaux restaurés, puis cliquez sur leur onglet **Fichiers**. Autrement, les sauvegardes suivantes de ces canaux n'incluront pas le contenu de cet onglet, en raison d'une restriction de l'API bêta de Microsoft Teams.

Restaurer des fichiers dans un canal d'équipe

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les équipes sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Équipes**, sélectionnez **Toutes les équipes**, sélectionnez l'équipe dont vous souhaitez restaurer les canaux, puis cliquez sur **Restauration**.
4. Sélectionnez un point de restauration.
5. Cliquez sur **Restaurer** > **Canaux**.
6. Sélectionnez le canal souhaité, puis ouvrez le dossier **Fichiers**.
   Parcourez les éléments requis ou utilisez la fonction de recherche pour les obtenir. Les options de recherche suivantes sont disponibles : nom du fichier ou nom du dossier, type de fichier, taille, date ou plage de dates de la dernière modification.
7. [Facultatif] Pour télécharger un élément, sélectionnez-le, cliquez sur **Télécharger**, sélectionner l'emplacement dans lequel vous souhaitez le sauvegarder, puis cliquez sur **Enregistrer**.
8. Sélectionnez les éléments que vous souhaitez restaurer, puis cliquez sur **Restaurer**
9. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur Organisation Microsoft 365 pour afficher, modifier ou indiquer l'organisation cible.
   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
10. Dans **Restaurer vers l'équipe**, affichez, modifiez ou indiquez l'équipe cible.
    L'équipe d'origine est sélectionnée par défaut. Si cette équipe n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez indiquer l'équipe cible.
11. Dans **Restaurer vers le canal**, affichez, modifiez ou indiquez le canal cible.
12. Choisissez de restaurer ou non les permissions de partage associées aux éléments restaurés.
13. Cliquez sur **Démarrer la récupération**.
14. Sélectionnez l'une des options d'écrasement :

- **Écraser le contenu existant s'il est plus ancien**
- **Écraser le contenu existant**
- **Ne pas écraser le contenu existant**

Remarque
Lorsque vous restaurez des blocs-notes OneNote, les options **Écraser le contenu existant s'il est plus ancien** et **Écraser le contenu existant** remplaceront les blocs-notes OneNote existants.

15. Cliquez sur **Continuer** pour confirmer votre choix.

Vous ne pouvez pas restaurer de conversations individuelles. Dans votre volet principal, vous pouvez uniquement parcourir le dossier **Conversation** ou télécharger son contenu en tant que fichier html unique. Pour cela, cliquez sur l'icône « Restaurer les dossiers »  , sélectionnez le dossier **Conversations** souhaité, puis cliquez sur **Télécharger**.

Vous pouvez rechercher les messages dans le dossier **Conversation** par :

- Expéditeur
- Contenu
- Nom de la pièce jointe
- Date

Restaurer une boîte aux lettres d'équipe

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les équipes sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Équipes**, sélectionnez **Toutes les équipes**, sélectionnez l'équipe dont vous souhaitez restaurer la boîte aux lettres, puis cliquez sur **Restauration**.
   Vous pouvez rechercher les équipes par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.
5. Cliquez sur **Restaurer** > **Messages électroniques**.
6. Cliquez sur l'icône « Restaurer les dossiers »  , sélectionnez le dossier de boîte aux lettres racine, puis cliquez sur **Restaurer**.

Remarque
Vous pouvez également récupérer des dossiers individuels dans la boîte aux lettres sélectionnée.

7. Cliquez sur **Restaurer**.
8. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.
   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
9. Dans **Restaurer vers la boîte aux lettres**, affichez, modifiez ou spécifiez la boîte aux lettres cible.
   Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier la boîte aux lettres cible.
10. Cliquez sur **Démarrer la récupération**.
11. Sélectionnez l'une des options d'écrasement :
    - **Écraser les éléments existants**
    - **Ne pas écraser les éléments existants**
12. Cliquez sur **Continuer** pour confirmer votre choix.

Restauration d'éléments de boîte aux lettres d'équipe vers des fichiers PST

Restaurer des éléments de boîte aux lettres d'équipe

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Vous pouvez rechercher les utilisateurs et les groupes par nom. Les caractères génériques ne sont pas pris en charge.
4. Développez le nœud **Équipes**, sélectionnez **Toutes les équipes**, sélectionnez une équipe dont la boîte aux lettres contenait à l'origine les éléments que vous souhaitez restaurer, puis cliquez sur **Restauration**.
5. Cliquez sur **Restaurer** > **Messages électroniques**.
6. Parcourez le dossier requis ou utilisez la fonction de recherche pour obtenir la liste des éléments requis.
   Les options de recherche suivantes sont disponibles. Les caractères génériques ne sont pas pris en charge.
   - Pour les messages de courrier électronique : recherche par sujet, expéditeur, destinataire, nom de la pièce jointe et date.
   - Pour les événements : recherche par titre et date.
   - Pour les tâches : recherche par sujet et date.
   - Pour les contacts : recherche par nom, adresse e-mail et numéro de téléphone.
7. Sélectionnez les éléments que vous souhaitez restaurer. Pour pouvoir sélectionner les dossiers, cliquez sur l'icône des dossiers à restaurer : 

Par ailleurs, vous pouvez effectuer l'une des opérations suivantes :

- Lorsqu'un élément est sélectionné, cliquez sur **Afficher le contenu** pour afficher son contenu, y compris les pièces jointes. Cliquez sur le nom d'un fichier de pièce jointe pour le télécharger.
- Lorsqu'un message de courrier électronique ou un élément de calendrier est sélectionné, vous pouvez cliquer sur **Envoyer sous forme de message électronique** pour l'envoyer aux adresses électroniques spécifiées. Vous pouvez sélectionner l'expéditeur et rédiger un message qui sera ajouté à l'élément transféré.
- Lorsque la sauvegarde n'est pas chiffrée, que vous avez utilisé la recherche et que vous avez sélectionné un seul élément dans les résultats de recherche : cliquez sur **Afficher les versions** pour afficher la version de l'élément. Vous pouvez sélectionner n'importe quelle version sauvegardée, qu'elle soit antérieure ou postérieure au point de reprise sélectionné.

8. Cliquez sur **Restaurer en tant que fichiers PST**.
9. Définissez le mot de passe pour chiffrer l'archive avec le fichier PST.
   Le mot de passe doit contenir au moins un symbole.
10. Confirmez le mot de passe et cliquez sur **TERMINÉ**.

Les éléments de boîte aux lettres sélectionnés seront restaurés sous la forme de fichiers de données PST et archivés au format ZIP. La taille maximale d'un fichier PST est limitée à 2 Go. Si la quantité de données que vous restaurez dépasse 2 Go, les données seront divisées en plusieurs fichiers PST. L'archive ZIP sera protégée par le mot de passe que vous avez défini.

Vous recevrez un e-mail avec un lien vers l'archive ZIP contenant les fichiers PST créés.

L'administrateur recevra une notification par e-mail l'informant que vous avez exécuté la procédure de restauration.

Télécharger l'archive contenant les fichiers PST et effectuer la restauration

1. Effectuez l'une des actions suivantes :
   - Pour télécharger l'archive depuis l'e-mail, suivez le lien **Téléchargement des fichiers**. L'archive est disponible au téléchargement sous 24 heures. Si le lien expire, répétez la procédure de restauration.
   - Télécharger l'archive à partir de la console Cyber Protect :
     a. Accédez à **Stockage de sauvegarde** > **Fichiers PST**.
     b. Sélectionnez la dernière archive mise en évidence.
     c. Cliquez sur **Télécharger** dans le volet de droite.

   L'archive sera téléchargée dans le répertoire de téléchargement par défaut sur votre ordinateur.
2. Extrayez les fichiers PST depuis l'archive à l'aide du mot de passe que vous avez défini pour chiffrer l'archive.
3. Dans Microsoft Outlook, ouvrez ou importez les fichiers PST. Pour savoir comment procéder, reportez-vous à la documentation Microsoft.

Restaurer les messages électroniques et les réunions

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les équipes sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Équipes**, sélectionnez **Toutes les équipes**, sélectionnez l'équipe dont vous souhaitez restaurer les e-mails ou les réunions, puis cliquez sur **Restauration**.

   Vous pouvez rechercher les équipes par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.
5. Cliquez sur **Restaurer** > **Messages électroniques**.
6. Parcourez l'élément requis ou utilisez la fonction de recherche pour l'obtenir.

   Les options de recherche suivantes sont disponibles :
   - Pour les messages de courrier électronique : recherche par sujet, expéditeur, destinataire et date.
   - Pour les réunions : recherchez par nom d'événement et date.
7. Sélectionnez les éléments que vous souhaitez restaurer, puis cliquez sur **Restaurer**.

   Remarque
   Vous pouvez trouver les réunions dans le dossier **Calendrier**.

   Par ailleurs, vous pouvez effectuer l'une des opérations suivantes :
   - Lorsqu'un élément est sélectionné, cliquez sur **Afficher le contenu** pour afficher son contenu, y compris les pièces jointes. Cliquez sur le nom d'un fichier de pièce jointe pour le télécharger.
   - Lorsqu'un e-mail ou une réunion sont sélectionnés, vous pouvez cliquer sur **Envoyer sous forme de message électronique** pour l'envoyer aux adresses électroniques spécifiées. Vous pouvez sélectionner l'expéditeur et rédiger un message qui sera ajouté à l'élément transféré.
8. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.

   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
9. Dans **Restaurer vers la boîte aux lettres**, affichez, modifiez ou spécifiez la boîte aux lettres cible.

   Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier la boîte aux lettres cible.
10. Cliquez sur **Démarrer la récupération**.
11. Sélectionnez l'une des options d'écrasement :

- **Écraser les éléments existants**
- **Ne pas écraser les éléments existants**

12. Cliquez sur **Continuer** pour confirmer votre choix.

Restaurer un site d'équipe ou des éléments précis d'un site

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les équipes sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Équipes**, sélectionnez **Toutes les équipes**, sélectionnez l'équipe dont vous souhaitez restaurer le site, puis cliquez sur **Restauration**.

   Vous pouvez rechercher les équipes par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.
5. Cliquez sur **Restaurer** > **Site d'équipe**.
6. Parcourez l'élément requis ou utilisez la fonction de recherche pour l'obtenir.
7. [Facultatif] Pour télécharger un élément, sélectionnez-le, cliquez sur **Télécharger**, sélectionner l'emplacement dans lequel vous souhaitez le sauvegarder, puis cliquez sur **Enregistrer**.
8. Sélectionnez les éléments que vous souhaitez restaurer, puis cliquez sur **Restaurer**.
9. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.

   L'organisation et l'équipe d'origine sont sélectionnées par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
10. Dans **Restaurer vers l'équipe**, affichez, modifiez ou indiquez l'équipe cible.

    L'équipe d'origine est sélectionnée par défaut. Si cette équipe n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez indiquer le dossier cible.
11. Choisissez de restaurer ou non les permissions de partage associées aux éléments restaurés.
12. Cliquez sur **Démarrer la récupération**.
13. Sélectionnez l'une des options d'écrasement :
    - **Écraser le contenu existant s'il est plus ancien**
    - **Écraser le contenu existant**
    - **Ne pas écraser le contenu existant**

    Remarque
    Lorsque vous restaurez des blocs-notes OneNote, les options **Écraser le contenu existant s'il est plus ancien** et **Écraser le contenu existant** remplaceront les blocs-notes OneNote existants.
14. Cliquez sur **Continuer** pour confirmer votre choix.

Protection des blocs-notes OneNote

Par défaut, les blocs-notes OneNote sont inclus dans les sauvegardes de fichiers OneDrive, de Microsoft Teams et de sites SharePoint.

Pour exclure les blocs-notes OneNote de ces sauvegardes, désactivez l'interrupteur **Inclure OneNote** dans le plan de sauvegarde correspondant.

Restauration de blocs-notes OneNote sauvegardés

Pour apprendre à restaurer un bloc-notes OneNote sauvegardé, reportez-vous à la rubrique suivante :

- Pour les sauvegardes OneDrive, reportez-vous à "Restauration de l'intégralité de OneDrive" (p. 655) ou à "Restauration de fichiers OneDrive" (p. 657).
- Pour les sauvegardes Teams, reportez-vous à "Restauration de l'intégralité d'une équipe" (p. 664), à "Restaurer des canaux ou des fichiers d'équipe dans les canaux d'équipe" (p. 665) ou à "Restaurer un site d'équipe ou des éléments précis d'un site" (p. 672).
- Pour les sauvegardes de site SharePoint, reportez-vous à "Restauration de données de SharePoint Online" (p. 661).

Versions prises en charge

- OneNote (OneNote 2016 et versions ultérieures)
- OneNote pour Windows 10

Limitations et problèmes connus

- Les blocs-notes OneNote enregistrés dans OneDrive ou SharePoint sont limités à 2 Go. Vous ne pouvez pas restaurer des blocs-notes OneNote plus volumineux sur des cibles OneDrive ou SharePoint.
- Les blocs-notes OneNote comprenant des groupes de sections ne sont pas pris en charge.
- Dans les blocs-notes OneNote sauvegardés qui contiennent des sections avec des noms différents de ceux par défaut, la première section s'affiche avec le nom par défaut (comme `Nouvelle section` ou `Section sans titre`). Cela peut affecter l'ordre des sections dans les blocs-notes contenant plusieurs sections.
- Lorsque vous restaurez des blocs-notes OneNote, les options **Écraser le contenu existant s'il est plus ancien** et **Écraser le contenu existant** remplaceront les blocs-notes OneNote existants.
- Lorsque vous restaurez une équipe complète, un site d'équipe ou le dossier `SiteAssets` d'un site d'équipe, et que vous avez sélectionné l'option **Écraser le contenu existant s'il est plus ancien** ou **Écraser le contenu existant**, le bloc-notes OneNote par défaut de l'équipe n'est pas écrasé. La reprise réussit avec l'avertissement *Échec de la mise à jour des propriétés du fichier « /sites/<nom équipe>/SiteAssets/<nom bloc-notes OneNote> »*.

Protection des postes avec application de collaboration Microsoft 365

Vous pouvez utiliser le pack Advanced Email Security qui fournit une protection en temps réel pour vos boîtes aux lettres Microsoft 365, Google Workspace ou Open-Xchange :

- Anti-malware et antispam
- Analyse d'URL dans les e-mails
- Analyse DMARC
- Anti-hameçonnage
- Protection contre l'usurpation d'identité
- Analyse des pièces jointes
- Désarmement et reconstruction du contenu
- Schéma de confiance

Vous pouvez également activer les postes d'application de collaboration Microsoft 365, ce qui permet de protéger les applications de collaboration cloud Microsoft 365 contre les menaces de sécurité liées au contenu. Ces applications comprennent OneDrive, SharePoint et Teams.

Advanced Email Security peut être activé par ressource ou par gigaoctet, et aura un impact sur votre modèle de licence.

Pour accéder à l'intégration d'Advanced Email Security depuis la console Cyber Protect Cloud

1. Cliquez sur **Terminaux** > **Microsoft 365**.
2. Cliquez sur le nœud **Utilisateurs**, puis sur le lien **Accédez à Email Security** en haut à droite.

Pour en savoir plus sur Advanced Email Security dans la fiche solution Advanced Email Security.

Pour obtenir des instructions de configuration, voir Advanced Email Security avec Perception Point.

Protection des données Google Workspace

Remarque
Cette fonctionnalité n'est pas disponible pour les tenants en mode Conformité. Pour plus d'informations, consultez le site "Mode de conformité" (p. 1147).

Que signifie la protection Google Workspace ?

- Service de sauvegarde et de restauration de Cloud à Cloud des données utilisateur de Google Workspace (boîtes aux lettres Gmail, Agendas, Contacts, Google Drives) et Drive partagés Google Workspace.
- Restauration granulaire d'e-mails, fichiers, contacts et autres éléments.

- Assistance pour plusieurs organisations Google Workspace et restauration entre les organisations.
- Notarisation facultative des fichiers sauvegardés au moyen de la base de données blockchain Ethereum. Lorsqu'elle est activée, elle vous permet de prouver qu'un fichier est authentique et inchangé depuis sa sauvegarde.
- Recherche en texte intégral facultative. Lorsque cette fonction est activée, vous pouvez rechercher du contenu dans les e-mails.
- Vous pouvez protéger jusqu'à 5 000 éléments (boîtes aux lettres, instances Google Drive et Drive partagés) par entreprise, sans dégradation des performances.
- Les données sauvegardées sont automatiquement compressées et utilisent moins d'espace dans l'emplacement de sauvegarde que dans leur emplacement d'origine. Le niveau de compression des sauvegardes cloud à cloud est fixe et correspond au niveau **Normal** des sauvegardes non-cloud à cloud. Pour en savoir plus sur ces niveaux, reportez-vous à "Niveau de compression" (p. 479).

Droits utilisateurs requis

Dans Cyber Protection

Dans Cyber Protection, vous devez être un administrateur d'entreprise agissant au niveau tenant client. Les administrateurs d'entreprise agissant au niveau d'une unité, les administrateurs d'unité et les utilisateurs ne peuvent pas sauvegarder ou récupérer les données de Google Workspace.

Dans Google Workspace

Pour ajouter votre organisation Google Workspace au service Cyber Protection, vous devez être connecté en tant que super administrateur, avec l'accès aux API activé (**Security** > **Document de référence sur les API** > **Activer l'accès aux API** dans la console d'administration Google).

Le mot de passe du super administrateur n'est stocké nulle part et n'est pas utilisé pour effectuer la sauvegarde et la restauration. La modification de ce mot de passe dans Google Workspace n'affecte pas le fonctionnement du service Cyber Protection.

Si le super administrateur qui a ajouté l'organisation Google Workspace est supprimé de Google Workspace ou se voit attribuer un rôle avec des privilèges moindres, les sauvegardes échoueront avec une erreur telle que « Accès refusé ». Dans ce cas, répétez la procédure décrite à l'adresse "Ajouter une organisation Google Workspace" (p. 676) et indiquez des identifiants valides pour le super administrateur. Pour éviter ce problème, nous vous recommandons de créer un utilisateur super administrateur dédié à la sauvegarde et à la restauration.

À propos de la planification de sauvegarde

Étant donné que l'agent Cloud sert plusieurs clients, il détermine seul l'heure de début de chaque plan de protection, pour garantir une charge égale dans une journée et une qualité de service égale pour tous les clients.

Chaque plan de protection s'exécute tous les jours à la même heure.

L'option par défaut est **Une fois par jour**. Grâce au pack Advanced Backup, vous pouvez planifier jusqu'à six sauvegardes par jour. Les sauvegardes démarrent à des intervalles approximatifs qui dépendent de la charge actuelle de l'agent cloud desservant les nombreux clients d'un centre de données. De cette manière, la charge est égale toute la journée, ce qui garantit une qualité de service équivalente pour tous les clients.

Limites

- La console montre uniquement les utilisateurs qui ont une licence Google Workspace affectée, et une boîte aux lettres ou un espace Google Drive.
- Les documents aux formats Google natifs sont sauvegardés en tant que documents Office génériques et s'affichent avec une extension différente dans la console Cyber Protect, .docx ou .pptx par exemple. Ces documents sont reconvertis dans leur format d'origine lors de la restauration.
- Pas plus de 10 exécutions de sauvegarde manuelle en une heure.
- Pas plus de 10 opérations de récupération en même temps (ce nombre comprend aussi bien la restauration Microsoft 365 que Google Workspace).
- Vous ne pouvez pas simultanément restaurer des éléments depuis différents points de récupération, même si vous pouvez sélectionner ces éléments dans les résultats de recherche.
- Les sauvegardes des comptes utilisateur Google Workspace supprimés ne sont pas supprimées automatiquement du stockage dans le cloud. Ces sauvegardes sont facturées en fonction de l'espace de stockage qu'elles utilisent.
- Vous ne pouvez pas appliquer plusieurs plans de sauvegarde à la même ressource.
- Lorsqu'un plan de sauvegarde et un plan de sauvegarde de groupe sont appliqués à la même ressource, les paramètres du plan isolé sont prioritaires.

Journalisation

Actions concernant les ressources de cloud à cloud telles que l'affichage du contenu d'e-mails sauvegardés, le téléchargement de pièces jointes ou de fichiers, la restauration d'e-mails sur des boîtes aux lettres autres que les boîtes aux lettres d'origine, ou l'envoi de tels contenus par e-mail pouvant constituer une violation de la confidentialité des utilisateurs. Ces actions sont consignées dans le portail de gestion accessible par **Surveillance** > **Journal d'audit**.

Ajouter une organisation Google Workspace

Pour ajouter une organisation Google Workspace au service Cyber Protection, vous devez disposer d'un projet Google Cloud personnel dédié. Pour plus d'informations sur le processus de création et de configuration d'un tel projet, consultez "Création d'un projet Google Cloud personnel" (p. 677).

Pour ajouter une organisation Google Workspace en utilisant un projet Google Cloud personnel dédié

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur de l'entreprise.
2. Cliquez sur **Terminaux** > **Ajouter** > **Google Workspace**.
3. Saisissez l'adresse e-mail d'un super administrateur de votre compte Google Workspace.
   Pour cette procédure, il est utile de savoir si la vérification en 2 étapes est activée pour le compte e-mail de Super administrateur.
4. Recherchez le fichier JSON qui contient la clé privée du compte de service que vous avez créé dans votre projet Google Cloud.
   Vous pouvez également coller le contenu du fichier en tant que texte.
5. Cliquez sur **Confirmer**.

Votre organisation Google Workspace apparaît alors sous l'onglet **Terminaux** dans la console Cyber Protect.

Conseils utiles

- Après l'ajout d'une organisation Google Workspace, les données utilisateurs et les Drive partagés qui se trouvent dans le domaine principal et dans tous les domaines secondaires (s'il y en a) seront sauvegardés. Les ressources sauvegardées s'afficheront sous la forme d'une liste, et ne seront pas regroupées par domaine.
- L'agent Cloud se synchronise avec Google Workspace toutes les 24 heures, à compter du moment où l'organisation est ajoutée au service Cyber Protection. Si vous ajoutez ou supprimez un utilisateur ou un lecteur partagé, ce changement ne sera pas immédiatement visible dans la console Cyber Protect. Pour synchroniser la modification immédiatement, sélectionnez l'organisation sur la page **Google Workspace**, puis cliquez sur **Actualiser**.
  Pour plus d'informations sur la synchronisation des ressources d'une organisation Google Workspace et de la console Cyber Protect, voir "Découverte des ressources Google Workspace" (p. 681).
- Si vous avez appliqué un plan de protection au groupe **Tous les utilisateurs** ou **Tous les Drive partagés**, les éléments récemment ajoutés ne seront inclus dans la sauvegarde que lorsque la synchronisation aura été effectuée.
- Conformément à la politique de Google, lorsqu'un utilisateur ou un Drive partagé est supprimé de l'interface utilisateur graphique de Google Workspace, il reste encore disponible pendant quelques jours via l'API. Pendant cette période, l'élément supprimé est inactif (grisé) dans la console Cyber Protect et n'est pas sauvegardé. Lorsque l'élément supprimé ne sera plus disponible via l'API, il disparaîtra de la console Cyber Protect. Ses sauvegardes (s'il y en a) se trouvent sous **Stockage de sauvegarde** > **Sauvegardes d'applications Cloud**.

Création d'un projet Google Cloud personnel

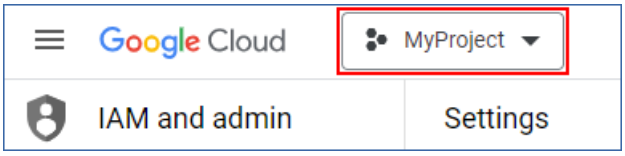
Pour ajouter votre organisation Google Workspace au service Cyber Protection à l'aide d'un projet Google Cloud personnel dédié, procédez comme suit :

1. Créez un nouveau projet Google Cloud.
2. Activez les API nécessaires pour ce projet.
3. Configurez les informations d'identification pour ce projet :
   a. Configurez l'écran d'autorisation OAuth.
   b. Créez et configurez le compte de service pour le service Cyber Protection.
4. Accordez à votre nouveau projet l'accès à votre compte Google Workspace.

Remarque
Cette rubrique contient une description d'une interface utilisateur tierce, susceptible d'être modifiée sans préavis.

Pour créer un nouveau projet Google Cloud

1. Connectez-vous à la plate-forme Google Cloud (console.cloud.google.com) en tant que super administrateur.
2. Dans la console de la plate-forme Google Cloud, cliquez sur le sélecteur de projets en haut à gauche.



3. Dans l'écran qui s'affiche, sélectionnez une organisation, puis cliquez sur **Nouveau projet**.

4. Spécifiez un nom pour votre nouveau projet.
5. Cliquez sur **Créer**.

Un nouveau projet Google Cloud est alors créé.

Pour activer les API nécessaires pour ce projet

1. Dans la console de la plate-forme Google Cloud, sélectionnez votre nouveau projet.
2. Dans le menu de navigation, sélectionnez **API et services** > **API et services activés**.
3. Désactivez toutes les API activées par défaut dans ce projet, une par une :
   a. Faites défiler la page **API et services activés** vers le bas, puis cliquez sur le nom d'une API activée.
      La page **Détails de l'API/du service** de l'API sélectionnée s'ouvre.
   b. Cliquez sur **Désactiver l'API**, puis confirmez votre choix en cliquant sur **Désactiver**.
   c. [Si vous y êtes invité] Confirmez votre choix en cliquant sur **Confirmer**.
   d. Revenez à la page **API et services** > **API et services activés**, puis désactivez l'API suivante.
4. Dans le menu de navigation, sélectionnez **API et services** > **Bibliothèque**.

5. Dans la bibliothèque d'API, activez les API suivantes, une par une :
   - Admin SDK API
   - Gmail API
   - Google Calendar API
   - API Google Drive
   - Google People API

   Trouvez les API requises à l'aide de la barre de recherche. Pour activer une API, cliquez sur son nom, puis sur **Activer**. Pour rechercher l'API suivante, revenez à la bibliothèque d'API en sélectionnant **API et services** > **Bibliothèque** dans le menu de navigation.

Pour configurer l'écran d'autorisation OAuth

1. Dans le menu de navigation de Google Cloud Platform, sélectionnez **API et services** > **Écran d'autorisation OAuth**.
2. Dans la fenêtre qui s'ouvre, sélectionnez le type d'utilisateur **Interne**, puis cliquez sur **Créer**.
3. Dans le champ **Nom de l'appli**, spécifiez un nom pour votre application.
4. Dans le champ **Adresse e-mail d'assistance utilisateur**, saisissez l'adresse e-mail du super administrateur.
5. Dans le champ **Coordonnées du développeur**, saisissez l'adresse e-mail du super administrateur.
6. Laissez tous les autres champs vides, puis cliquez sur **Enregistrer et continuer**.
7. Sur la page **Niveau d'accès**, cliquez sur **Enregistre et continuer**, sans rien modifier.
8. Sur la page **Résumé**, vérifiez vos paramètres, puis cliquez sur **Revenir au tableau de bord**.

Pour créer et configurer le compte de service pour le service Cyber Protection

1. Dans le menu de navigation de Google Cloud Platform, sélectionnez **API et services** > **Comptes de service**.
2. Cliquez sur **Créer un compte de service**.
3. Spécifiez un nom pour le compte de service.
4. [Facultatif] Spécifiez une description pour le compte de service.
5. Cliquez sur **Créer et continuer**.
6. Ne modifiez rien dans les étapes **Autoriser ce compte de service à accéder au projet** et **Autoriser les utilisateurs à accéder à ce compte de service**.
7. Cliquez sur **Valider**.
   La page **Comptes de service** s'ouvre.
8. Sur la page **Comptes de service**, sélectionnez le nouveau compte de service, puis sous **Actions**, cliquez sur **Gérer les clés**.
9. Sous **Clés**, cliquez sur **Ajouter une clé** > **Créer clé**, puis sélectionnez le type de clé **JSON**.
10. Cliquez sur **Créer**.

Un fichier JSON contenant la clé privée du compte de service est automatiquement téléchargé sur votre ordinateur. Conservez ce fichier précieusement, car vous en aurez besoin pour ajouter votre organisation Google Workspace au service Cyber Protection.

Pour accorder l'accès à votre compte Google Workspace à votre nouveau projet

1. Dans le menu de navigation de Google Cloud Platform, sélectionnez **IAM et Admin** > **Comptes de service**.
2. Dans la liste, recherchez le compte de service que vous avez créé, puis copiez l'identifiant client indiqué dans la colonne **ID client OAuth 2.0**.
3. Connectez-vous à la console d'administration de Google (admin.google.com) en tant que super administrateur.
4. Dans le menu de navigation, sélectionnez **Sécurité** > **Contrôles d'accès et de données** > **Contrôles d'API**.
5. Faites défiler la page **Contrôles d'API**, puis sous **Délégation au niveau du domaine**, cliquez sur **Gérer la délégation au niveau du domaine**.
   La page **Délégation au niveau du domaine** s'affiche.
6. Sur la page **Délégation au niveau du domaine**, cliquez sur **Ajouter nouveau**.
   La fenêtre **Ajouter un identifiant client** s'ouvre.
7. Dans le champ **Identifiant du client**, entrez l'ID du client de votre compte de service.
8. Dans le champ **Champs d'application OAuth**, copiez et collez la liste des champs d'application délimités par des virgules suivante :

   ```
   https://mail.google.com,https://www.googleapis.com/auth/contacts,https://www.googlea
   pis.com/auth/calendar,https://www.googleapis.com/auth/admin.directory.user.readonly,
   https://www.googleapis.com/auth/admin.directory.domain.readonly,https://www.googleap
   is.com/auth/drive,https://www.googleapis.com/auth/gmail.modify
   ```

   Vous pouvez également ajouter des champs d'application, un par ligne :
   - https://mail.google.com
   - https://www.googleapis.com/auth/contacts
   - https://www.googleapis.com/auth/calendar
   - https://www.googleapis.com/auth/admin.directory.user.readonly
   - https://www.googleapis.com/auth/admin.directory.domain.readonly
   - https://www.googleapis.com/auth/drive
   - https://www.googleapis.com/auth/gmail.modify
9. Cliquez sur **Autoriser**.

Votre nouveau projet Google Cloud peut alors accéder aux données de votre compte Google Workspace. Pour sauvegarder les données, vous devez lier ce projet au service Cyber Protection. Pour en savoir plus sur la façon de procéder, reportez-vous à "Pour ajouter une organisation Google Workspace en utilisant un projet Google Cloud personnel dédié" (p. 676).

Si vous devez révoquer l'accès de votre projet Google Cloud à votre compte Google Workspace, et respectivement, l'accès au service Cyber Protection, supprimez le client API que votre projet utilise.

Pour révoquer l'accès à votre compte Google Workspace

1. Dans la console d'administration de Google (admin.google.com), connectez-vous en tant que super administrateur.
2. Dans le menu de navigation, sélectionnez **Sécurité** > **Contrôles d'accès et de données** > **Contrôles d'API**.
3. Faites défiler la page **Contrôles d'API**, puis sous **Délégation au niveau du domaine**, cliquez sur **Gérer la délégation au niveau du domaine**.
   La page **Délégation au niveau du domaine** s'affiche.
4. Sur la page **Délégation au niveau du domaine**, sélectionnez le client API que votre projet utilise, puis cliquez sur **Supprimer**.
   Votre projet Google Cloud et le service Cyber Protection ne seront alors plus en mesure d'accéder à votre compte Google Workspace ni de sauvegarder les données qu'il contient.

Découverte des ressources Google Workspace

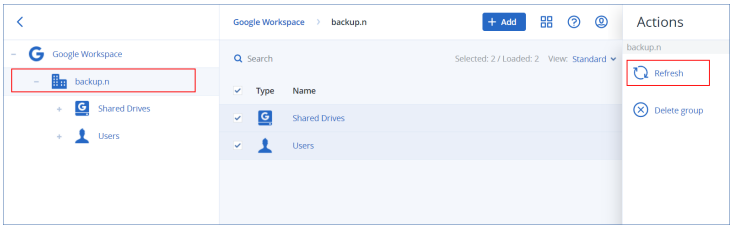
Lorsque vous ajoutez une organisation Google Workspace au service Cyber Protection, les ressources de cette organisation (boîtes aux lettres et services Google Drive, par exemple) sont synchronisées avec la console Cyber Protect. Cette opération est appelée découverte et elle est consignée dans **Surveillance** > **Activités**.

Une fois la découverte terminée, vous pouvez voir les ressources de l'organisation Google Workspace dans l'onglet **Terminaux** > **Google Workspace** de la console Cyber Protect et pouvez leur appliquer des plans de sauvegarde.

Une opération de découverte automatique est exécutée une fois par jour afin que la liste des ressources dans la console Cyber Protect soit à jour. Vous pouvez également synchroniser cette liste à la demande en réexécutant une opération de découverte manuellement.

Pour réexécuter une opération de découverte manuellement

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Google Workspace**.
2. Sélectionnez votre organisation Google Workspace, puis cliquez dans le panneau **Actions** sur **Actualiser**.



Remarque
Vous pouvez exécuter manuellement jusqu'à 10 découvertes par heure. Lorsque ce nombre est atteint, le nombre d'exécutions autorisé est réinitialisé à un par heure, puis une exécution supplémentaire est alors disponible toutes les heures jusqu'à ce qu'un total de 10 exécutions par heure soit atteint.

Configuration de la fréquence des sauvegardes Google Workspace

Par défaut, les sauvegardes Google Workspace s'exécutent une fois par jour et aucune autre option de planification n'est disponible.

Si le pack Advanced Backup est activé dans votre tenant, vous pouvez configurer des sauvegardes plus fréquentes. Vous pouvez sélectionner le nombre de sauvegardes par jour, mais vous ne pouvez pas configurer l'heure de leur démarrage. Les sauvegardes démarrent automatiquement à des intervalles approximatifs qui dépendent de la charge actuelle de l'agent cloud desservant les nombreux clients d'un centre de données. De cette manière, la charge est égale toute la journée, ce qui garantit une qualité de service équivalente pour tous les clients.

Les options suivantes sont disponibles.

Planification des options	Intervalle approximatif entre chaque sauvegarde
Une fois par jour	24 heures
Deux fois par jour (par défaut)	12 heures
Trois fois par jour	8 heures
Six fois par jour	4 heures

Remarque
Selon la charge sur l'agent cloud et les limitations possibles côté Google Workspace, une sauvegarde peut démarrer plus tard ou prendre plus de temps que prévu. Si une sauvegarde est plus longue que l'intervalle moyen entre deux sauvegardes, la sauvegarde suivante est replanifiée, ce qui peut avoir pour résultat un nombre de sauvegardes quotidiennes inférieur au nombre sélectionné. Par exemple, il est possible que deux sauvegardes par jour seulement puissent s'effectuer, même si vous en avez sélectionné six.

Protéger des données Gmail

Quels éléments peuvent être sauvegardés ?

Vous pouvez sauvegarder les boîtes aux lettres des utilisateurs Gmail. Une sauvegarde de boîte aux lettres inclut également des données d'Agenda et de Contacts. Vous pouvez également choisir de sauvegarder les agendas partagés.

Les éléments suivants sont *exclus* lors d'une sauvegarde :

- Les agendas **Anniversaires**, **Rappels**, **Tâches**
- Dossiers joints aux événements d'agenda
- Le dossier **Répertoire** des Contacts

Les éléments d'Agenda suivants sont *ignorés,* en raison des restrictions de l'API Google Agenda :

- Plages de rendez-vous
- Le champ Conférence d'un événement
- Le paramètre d'agenda **Notifications des événements « Toute la journée »**
- Le paramètre d'agenda **Accepter automatiquement les invitations** (dans les agendas pour les salons ou les espaces partagés)

Les éléments de Contacts suivants sont *ignorés,* en raison des restrictions de l'API Google People :

- Le dossier **Autres contacts**
- Les profils externes d'un contact (**Profil du répertoire**, **Profil Google**)
- Le champ de contact **Classer en tant que**

Quels éléments de données peuvent être restaurés ?

Les éléments suivants peuvent être restaurés à partir de sauvegardes de boîte aux lettres :

- Boîtes aux lettres
- Dossiers d'e-mail (selon la terminologie Google, « libellés ». Les **libellés** sont présentés dans le logiciel de sauvegarde en tant que dossiers, pour être cohérents avec la présentation d'autres données.)
- Messages de courriers électroniques
- Événements de calendrier
- Contacts

Vous pouvez utiliser la recherche pour localiser des éléments dans une sauvegarde.

Lorsque vous restaurez des boîtes aux lettres et des éléments de boîte aux lettres, vous pouvez choisir d'écraser ou non les éléments de l'emplacement de destination.

Limites

- Les photos des contacts ne peuvent pas être restaurées
- L'élément d'agenda **Absent du bureau** est restauré en tant qu'événement d'agenda régulier, en raison des restrictions de l'API Google Agenda

Sélection des boîtes aux lettres Gmail

Sélectionnez les boîtes aux lettres comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Pour sélectionner des boîtes aux lettres Gmail

1. Cliquez sur **Google Workspace**.
2. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez sauvegarder les données utilisateur. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour sauvegarder les boîtes aux lettres de tous les utilisateurs (y compris celles qui seront créés à l'avenir), développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, puis cliquez sur **Sauvegarde de groupe**.
   - Pour sauvegarder des boîtes aux lettres utilisateur en particulier, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez sauvegarder les boîtes aux lettres, puis cliquez sur **Sauvegarde**.
4. Dans le volet du plan de protection :
   - Dans **Quoi sauvegarder**, assurez-vous que **Gmail** est sélectionné.
   - Si vous souhaitez sauvegarder des calendriers partagés avec des utilisateurs sélectionnés, activez le commutateur **Inclure les calendriers partagés**.
   - Décidez de si vous avez besoin d'effectuer une recherche en texte intégral dans les e-mails sauvegardés. Pour accéder à cette option, cliquez sur l'icône en forme d'engrenage, puis sur **Options de sauvegarde** > **Recherche en texte intégral**.

Restauration de boîtes aux lettres et d'éléments de boîte aux lettres

Restauration de boîtes aux lettres

1. Cliquez sur **Google Workspace**.
2. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez restaurer la boîte aux lettres, puis cliquez sur **Restauration**.

   Si l'utilisateur a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les utilisateurs et les groupes par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.

Remarque
Pour afficher uniquement les points de récupération qui contiennent des boîtes aux lettres, sélectionnez **Gmail** dans **Filtre par contenu**.

5. Cliquez sur **Restaurer** > **Intégralité de la boîte aux lettres**.
6. Si plusieurs organisations Google Workspace sont ajoutées au service Cyber Protection, cliquez sur **Organisation Google Workspace** pour afficher, modifier ou spécifier l'organisation cible.
   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez sélectionner une nouvelle organisation cible parmi les organisations enregistrées disponibles.
7. Dans **Restaurer vers la boîte aux lettres**, affichez, modifiez ou spécifiez la boîte aux lettres cible.
   Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier la boîte aux lettres cible.
   Vous ne pouvez pas créer de nouvelle boîte aux lettres cible pendant la restauration. Pour restaurer une boîte aux lettres vers une nouvelle, vous devez d'abord créer la boîte aux lettres cible dans l'organisation Google Workspace souhaitée, puis laisser l'agent synchroniser le changement. L'agent Cloud se synchronise automatiquement avec Google Workspace toutes les 24 heures. Pour synchroniser la modification immédiatement, sélectionnez l'organisation sur la page **Google Workspace** de la console Cyber Protect, puis cliquez sur **Actualiser**.
8. Cliquez sur **Démarrer la récupération**.
9. Sélectionnez l'une des options d'écrasement :
   - **Écraser les éléments existants**
   - **Ne pas écraser les éléments existants**
10. Cliquez sur **Continuer** pour confirmer votre choix.

Restauration d'éléments de boîte aux lettres

1. Cliquez sur **Google Workspace**.
2. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont la boîte aux lettres contenait à l'origine les éléments à restaurer, puis cliquez sur **Restauration**.
   Si l'utilisateur a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.
   Vous pouvez rechercher les utilisateurs et les groupes par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.

Remarque
Pour afficher uniquement les points de récupération qui contiennent des boîtes aux lettres, sélectionnez **Gmail** dans **Filtre par contenu**.

5. Cliquez sur **Restaurer** > **Messages électroniques**.
6. Accédez au dossier requis. Si la sauvegarde n'est pas chiffrée, vous pouvez utiliser la recherche pour obtenir la liste des éléments requis.
   Les options de recherche suivantes sont disponibles. Les caractères génériques ne sont pas pris en charge.
   - Pour les e-mails : recherche par sujet, expéditeur, destinataire, date, nom de pièce jointe et contenu du message.
     Lors d'une recherche par date, vous pouvez sélectionner une date de début ou une date de fin (toutes deux incluses), ou les deux dates pour effectuer une recherche dans un intervalle de temps.
     La recherche par nom de pièce jointe ou dans le contenu du message ne donne des résultats que si l'option de **Recherche en texte intégral** a été activée lors de la sauvegarde. Vous pouvez spécifier la langue du fragment de message qui sera recherché en tant que paramètre supplémentaire.
   - Pour les événements : recherche par titre et date.
   - Pour les contacts : recherche par nom, adresse e-mail et numéro de téléphone.
7. Sélectionnez les éléments que vous souhaitez restaurer. Pour pouvoir sélectionner les dossiers, cliquez sur l'icône des dossiers à restaurer : 
   Par ailleurs, vous pouvez effectuer l'une des opérations suivantes :
   - Lorsqu'un élément est sélectionné, cliquez sur **Afficher le contenu** pour afficher son contenu, y compris les pièces jointes. Cliquez sur le nom d'un fichier de pièce jointe pour le télécharger.
   - Uniquement si la sauvegarde n'est pas chiffrée, que vous avez utilisé la fonction de recherche et que vous avec sélectionné un seul élément dans les résultats de recherche : cliquez sur **Afficher les versions** pour sélectionner la version de l'élément à restaurer. Vous pouvez choisir n'importe quelle version sauvegardée, avant ou après le point de récupération sélectionné.
8. Cliquez sur **Restaurer**.
9. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Google Workspace** pour afficher, modifier ou spécifier l'organisation cible.
   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez sélectionner une nouvelle organisation cible parmi les organisations enregistrées disponibles.

10. Dans **Restaurer vers la boîte aux lettres**, affichez, modifiez ou spécifiez la boîte aux lettres cible.

    Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier la boîte aux lettres cible.
11. Dans **Chemin d'accès**, affichez ou modifiez le dossier cible dans la boîte aux lettres cible. Le dossier d'origine est sélectionné par défaut.
12. Cliquez sur **Démarrer la récupération**.
13. Sélectionnez l'une des options d'écrasement :
    - **Écraser les éléments existants**
    - **Ne pas écraser les éléments existants**
14. Cliquez sur **Continuer** pour confirmer votre choix.

Protéger des fichiers Google Drive

Quels éléments peuvent être sauvegardés ?

Vous pouvez sauvegarder l'intégralité d'une instance Google Drive, ou des fichiers et dossiers en particulier. Les fichiers sont sauvegardés avec les permissions de partage associées.

Important
Les éléments suivants ne sont pas sauvegardés :

- Dossier **Partagé avec moi**
- Le dossier **Ordinateurs** (créé par le client Sauvegarde et synchronisation)

Limites

De tous les formats de fichiers spécifiques à Google, les formats Google Docs, Google Sheets et Google Slides sont totalement pris en charge pour la sauvegarde et la reprise. Les autres formats propres à Google risquent de n'être pris en charge que partiellement, voire pas du tout. Par exemple, les fichiers Google Drawings sont restaurés sous forme de fichiers `.svg`, les fichiers Google Sites, sous forme de fichiers `.txt` et les fichiers Google Jamboard, sous forme de fichiers `.pdf`. Quant aux fichiers Google My Maps, ils sont ignorés pendant la sauvegarde.

Remarque
Les formats de fichiers qui ne sont pas propres à Google, par exemple, `.txt`, `.docx`, `.pptx`, `.pdf`, `.jpg`, `.png`, `.zip`, sont totalement pris en charge pour la sauvegarde et la reprise.

Quels éléments de données peuvent être restaurés ?

Vous pouvez restaurer l'intégralité d'une instance Google Drive, ou tout fichier ou dossier sauvegardé.

Vous pouvez choisir de restaurer les permissions de partage ou de laisser les fichiers hériter des permissions du dossier vers lequel ils sont restaurés.

Limites

- Les commentaires des fichiers ne sont pas restaurés.
- Les liens de partage des fichiers et des dossiers ne sont pas restaurés.
- Les **paramètres de propriété** en lecture seule pour les fichiers partagés (**Empêcher les éditeurs de modifier l'accès et d'ajouter des personnes** et **Désactiver les options permettant de télécharger, imprimer et copier pour les commentateurs et les lecteurs**) ne peuvent pas être modifiés lors d'une restauration.
- Vous ne pouvez pas modifier la propriété d'un dossier partagé lors de la restauration si l'option **Empêcher les éditeurs de modifier l'accès et d'ajouter des personnes** est activée pour ce dossier. Ce paramètre empêche l'API Gogle Drive de lister les permissions de dossiers. La propriété des fichiers de ce dossier est correctement restaurée.

Sélectionner des fichiers Google Drive

Sélectionnez les fichiers comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Pour sélectionner des fichiers Google Drive

1. Cliquez sur **Google Workspace**.
2. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez sauvegarder les données utilisateur. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour sauvegarder les fichiers de tous les utilisateurs (y compris des utilisateurs qui seront créés à l'avenir), développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, puis cliquez sur **Sauvegarde de groupe**.
   - Pour sauvegarder les fichiers d'utilisateurs en particulier, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez sauvegarder les fichiers, puis cliquez sur **Sauvegarde**.
4. Dans le volet du plan de protection :
   - Dans **Quoi sauvegarder**, assurez-vous que **Google Drive** est sélectionné.
   - Dans **Éléments à sauvegarder**, effectuez l'une des actions suivantes :
     - Conservez le paramètre par défaut **[Tous]** (tous les fichiers).
     - Spécifiez les fichiers et dossiers à sauvegarder en ajoutant leur nom ou leur chemin d'accès.

       Vous pouvez utiliser des caractères génériques (*, ** et ?). Pour en savoir plus sur la définition de chemin d'accès et sur l'utilisation de caractères génériques, consultez la section « Filtres de fichiers ».

- Spécifiez les fichiers et dossiers à sauvegarder en cliquant sur Parcourir.

  Le lien **Parcourir** est disponible uniquement lors de la création d'un plan de protection pour un seul utilisateur.

- [Facultatif] Dans **Éléments à sauvegarder**, cliquez sur **Afficher les exclusions** pour spécifier les fichiers et dossiers à ignorer lors de la sauvegarde.

  Les exclusions ont priorité sur la sélection de fichiers, c'est-à-dire que si vous spécifiez le même fichier dans les deux champs, ce fichier sera ignoré lors de la sauvegarde.
- Si vous souhaitez activer la notarisation de tous les fichiers sélectionnés pour la sauvegarde, activez le commutateur **Notarisation**. Pour plus d'informations sur la notarisation, consultez la section « Notarisation ».

Restaurer une instance et des fichiers Google Drive

Restauration de l'intégralité d'une instance Google Drive

1. Cliquez sur **Google Workspace**.
2. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez restaurer les fichiers Google Drive, puis cliquez sur **Restauration**.

   Si l'utilisateur a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les utilisateurs par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.

   Remarque
   Pour afficher uniquement les points de récupération qui contiennent des fichiers Google Drive, sélectionnez **Google Drive** dans **Filtre par contenu**.
5. Cliquez sur **Restaurer** > **Tout le Drive**.
6. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Google Workspace** pour afficher, modifier ou spécifier l'organisation cible.

   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez sélectionner une nouvelle organisation cible parmi les organisations enregistrées disponibles.
7. Dans **Restaurer vers un Drive**, affichez, modifiez ou spécifiez l'utilisateur ou le Drive partagé cibles.

L'utilisateur d'origine est sélectionné par défaut. Si cet utilisateur n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier l'utilisateur cible ou le Drive partagé cible.

Si la sauvegarde contient des fichiers partagés, ces derniers seront restaurés vers le dossier racine du Drive cible.

8. Choisissez de restaurer ou non les permissions de partage associées aux fichiers.
9. Cliquez sur **Démarrer la récupération**.
10. Sélectionnez l'une des options d'écrasement :

Option	Description
Écraser un fichier existant s'il est plus ancien	Si l'emplacement de destination comporte un fichier de même nom, mais plus ancien que le fichier source, le fichier source est enregistré dans l'emplacement de destination et remplace l'ancienne version.
Écraser les fichiers existants	Tous les fichiers existants dans l'emplacement de destination sont remplacés, quelle que soit la date de leur dernière modification.
Ne pas écraser les fichiers existants	Si l'emplacement de destination comporte un fichier de même nom, aucune modification ne lui est appliquée et le fichier source n'est pas enregistré dans l'emplacement de destination.

11. Cliquez sur **Continuer** pour confirmer votre choix.

Restauration de fichiers Google Drive

1. Cliquez sur **Google Workspace**.
2. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez restaurer les fichiers Google Drive, puis cliquez sur **Restauration**.

   Si l'utilisateur a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les utilisateurs par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.

   Remarque
   Pour afficher uniquement les points de récupération qui contiennent des fichiers Google Drive, sélectionnez **Google Drive** dans **Filtre par contenu**.

5. Cliquez sur **Restaurer** > **Fichiers/dossiers**.

6. Recherchez le dossier requis ou utilisez la fonction de recherche pour obtenir la liste des fichiers et des dossiers requis.
7. Sélectionnez les fichiers que vous voulez restaurer.

   Si la sauvegarde n'est pas chiffrée et que vous avez sélectionné un seul fichier, vous pouvez cliquer sur **Afficher les versions** pour sélectionner la version du fichier à restaurer. Vous pouvez choisir n'importe quelle version sauvegardée, avant ou après le point de récupération sélectionné.
8. Si vous souhaitez télécharger un fichier, sélectionnez-le, cliquez sur **Télécharger**, sélectionnez l'emplacement dans lequel le sauvegarder, puis cliquez sur **Sauvegarder**. Sinon, ignorez cette étape.
9. Cliquez sur **Restaurer**.
10. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Google Workspace** pour afficher, modifier ou spécifier l'organisation cible.

    L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez sélectionner une nouvelle organisation cible parmi les organisations enregistrées disponibles.
11. Dans **Restaurer vers un Drive**, affichez, modifiez ou spécifiez l'utilisateur ou le Drive partagé cibles.

    L'utilisateur d'origine est sélectionné par défaut. Si cet utilisateur n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier l'utilisateur cible ou le Drive partagé cible.
12. Dans **Chemin d'accès**, affichez ou modifiez le dossier cible dans l'instance Google Drive de l'utilisateur cible ou dans le Drive partagé cible. L'emplacement d'origine est sélectionné par défaut.
13. Choisissez de restaurer ou non les permissions de partage associées aux fichiers.
14. Cliquez sur **Démarrer la récupération**.
15. Sélectionnez l'une des options d'écrasement de fichier :

Option	Description
Écraser un fichier existant s'il est plus ancien	Si l'emplacement de destination comporte un fichier de même nom, mais plus ancien que le fichier source, le fichier source est enregistré dans l'emplacement de destination et remplace l'ancienne version.
Écraser les fichiers existants	Tous les fichiers existants dans l'emplacement de destination sont remplacés, quelle que soit la date de leur dernière modification.
Ne pas écraser les fichiers existants	Si l'emplacement de destination comporte un fichier de même nom, aucune modification ne lui est appliquée et le fichier source n'est pas enregistré dans l'emplacement de destination.

16. Cliquez sur **Continuer** pour confirmer votre choix.

Protection des fichiers de Drive partagés

Quels éléments peuvent être sauvegardés ?

Vous pouvez sauvegarder l'intégralité d'un Drive partagé, ou des fichiers et dossiers en particulier. Les fichiers sont sauvegardés avec les permissions de partage associées.

Important
Le dossier **Partagé avec moi** n'est pas sauvegardé.

Limites

- Un Drive partagé qui ne comprend aucun membre ne peut pas être sauvegardé, en raison des restrictions de l'Google Drive API.
- De tous les formats de fichiers spécifiques à Google, les formats Google Docs, Google Sheets et Google Slides sont totalement pris en charge pour la sauvegarde et la reprise. Les autres formats propres à Google risquent de n'être pris en charge que partiellement, voire pas du tout. Par exemple, les fichiers Google Drawings sont restaurés sous forme de fichiers `.svg`, les fichiers Google Sites, sous forme de fichiers `.txt` et les fichiers Google Jamboard, sous forme de fichiers `.pdf`. Quant aux fichiers Google My Maps, ils sont ignorés pendant la sauvegarde.

  Remarque
  Les formats de fichiers qui ne sont pas propres à Google, par exemple, `.txt`, `.docx`, `.pptx`, `.pdf`, `.jpg`, `.png`, `.zip`, sont totalement pris en charge pour la sauvegarde et la reprise.

Quels éléments de données peuvent être restaurés ?

Vous pouvez restaurer l'intégralité d'un Drive partagé, ou tout fichier ou dossier sauvegardé.

Vous pouvez choisir de restaurer les permissions de partage ou de laisser les fichiers hériter des permissions du dossier vers lequel ils sont restaurés.

Les éléments suivants ne sont pas restaurés :

- Les permissions de partage d'un fichier ayant été partagé avec un utilisateur externe à l'organisation ne sont pas restaurées si le partage en dehors de l'organisation est désactivé dans le Drive partagé cible.
- Les permissions de partage d'un fichier ayant été partagé avec un utilisateur qui n'est pas membre du Drive partagé cible ne sont pas restaurées si **Partage avec des non-membres** est désactivé dans le Drive partagé cible.

Limites

- Les commentaires des fichiers ne sont pas restaurés.
- Les liens de partage des fichiers et des dossiers ne sont pas restaurés.

Sélection de fichiers de Drive partagés

Sélectionnez les fichiers comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Pour sélectionner des fichiers de Drive partagés

1. Cliquez sur **Google Workspace**.
2. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez sauvegarder les données utilisateur. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour sauvegarder les fichiers de tous les Drive partagés (y compris des Drive partagés qui seront créés à l'avenir), développez le nœud **Drive partagé**, sélectionnez **Tous les Drive partagés**, puis cliquez sur **Sauvegarde de groupe**.
   - Pour sauvegarder les fichiers de Drive partagés individuels, développez le nœud **Drive partagé**, sélectionnez **Tous les Drive partagés**, sélectionnez les Drive partagés à sauvegarder, puis cliquez sur **Sauvegarde**.
4. Dans le volet du plan de protection :
   - Dans **Éléments à sauvegarder**, effectuez l'une des actions suivantes :
     - Conservez le paramètre par défaut **[Tous]** (tous les fichiers).
     - Spécifiez les fichiers et dossiers à sauvegarder en ajoutant leur nom ou leur chemin d'accès.

       Vous pouvez utiliser des caractères génériques (*, ** et ?). Pour en savoir plus sur la définition de chemin d'accès et sur l'utilisation de caractères génériques, consultez la section « Filtres de fichiers ».
     - Spécifiez les fichiers et dossiers à sauvegarder en cliquant sur Parcourir.

       Le lien **Parcourir** est disponible uniquement lors de la création d'un plan de protection pour un seul Drive partagé.
   - [Facultatif] Dans **Éléments à sauvegarder**, cliquez sur **Afficher les exclusions** pour spécifier les fichiers et dossiers à ignorer lors de la sauvegarde.

     Les exclusions ont priorité sur la sélection de fichiers, c'est-à-dire que si vous spécifiez le même fichier dans les deux champs, ce fichier sera ignoré lors de la sauvegarde.
   - Si vous souhaitez activer la notarisation de tous les fichiers sélectionnés pour la sauvegarde, activez le commutateur **Notarisation**. Pour plus d'informations sur la notarisation, consultez la section « Notarisation ».

Restauration des Drives partagés et des fichiers de Drive partagés

Restauration de l'intégralité d'un Drive partagé

1. Cliquez sur **Google Workspace**.
2. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Drive partagé**, sélectionnez **Tous les Drive partagés**, sélectionnez le Drive partagé que vous souhaitez restaurer, puis cliquez sur **Restauration**.

   Si le Drive partagé a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les Drive partagés par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.
5. Cliquez sur **Restaurer** > **Drive partagé complet**.
6. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Google Workspace** pour afficher, modifier ou spécifier l'organisation cible.

   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez sélectionner une nouvelle organisation cible parmi les organisations enregistrées disponibles.
7. Dans **Restaurer vers le Drive**, affichez, modifiez ou spécifiez le Drive partagé ou l'utilisateur cibles. Si vous précisez un utilisateur, les données seront restaurées vers l'instance Google Drive de cet utilisateur.

   Le Drive partagé d'origine est sélectionné par défaut. Si ce Drive partagé n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier le Drive partagé cible ou l'utilisateur cible.
8. Choisissez de restaurer ou non les permissions de partage associées aux fichiers.
9. Cliquez sur **Démarrer la récupération**.

10. Sélectionnez l'une des options d'écrasement :

Option	Description
Écraser un fichier existant s'il est plus ancien	Si l'emplacement de destination comporte un fichier de même nom, mais plus ancien que le fichier source, le fichier source est enregistré dans l'emplacement de destination et remplace l'ancienne version.
Écraser les fichiers existants	Tous les fichiers existants dans l'emplacement de destination sont remplacés, quelle que soit la date de leur dernière modification.
Ne pas écraser les fichiers existants	Si l'emplacement de destination comporte un fichier de même nom, aucune modification ne lui est appliquée et le fichier source n'est pas enregistré dans l'emplacement de destination.

11. Cliquez sur **Continuer** pour confirmer votre choix.

Restauration des fichiers de Drive partagés

1. Cliquez sur **Google Workspace**.
2. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Drive partagé**, sélectionnez **Tous les Drive partagés**, sélectionnez le Drive partagé qui contenait à l'origine les fichiers que vous souhaitez restaurer, puis cliquez sur **Restauration**.

   Si le Drive partagé a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les Drive partagés par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.
5. Cliquez sur **Restaurer** > **Fichiers/dossiers**.
6. Recherchez le dossier requis ou utilisez la fonction de recherche pour obtenir la liste des fichiers et des dossiers requis.
7. Sélectionnez les fichiers que vous voulez restaurer.

   Si la sauvegarde n'est pas chiffrée et que vous avez sélectionné un seul fichier, vous pouvez cliquer sur **Afficher les versions** pour sélectionner la version du fichier à restaurer. Vous pouvez choisir n'importe quelle version sauvegardée, avant ou après le point de récupération sélectionné.
8. Si vous souhaitez télécharger un fichier, sélectionnez-le, cliquez sur **Télécharger**, sélectionnez l'emplacement dans lequel le sauvegarder, puis cliquez sur **Sauvegarder**. Sinon, ignorez cette étape.
9. Cliquez sur **Restaurer**.

10. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Google Workspace** pour afficher, modifier ou spécifier l'organisation cible.

    L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez sélectionner une nouvelle organisation cible parmi les organisations enregistrées disponibles.
11. Dans **Restaurer vers le Drive**, affichez, modifiez ou spécifiez le Drive partagé ou l'utilisateur cibles. Si vous précisez un utilisateur, les données seront restaurées vers l'instance Google Drive de cet utilisateur.

    Le Drive partagé d'origine est sélectionné par défaut. Si ce Drive partagé n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier le Drive partagé cible ou l'utilisateur cible.
12. Dans **Chemin d'accès**, affichez ou modifiez le dossier cible dans le Drive partagé cible ou dans le Google Drive de l'utilisateur cible. L'emplacement d'origine est sélectionné par défaut.
13. Choisissez de restaurer ou non les permissions de partage associées aux fichiers.
14. Cliquez sur **Démarrer la récupération**.
15. Sélectionnez l'une des options d'écrasement de fichier :

Option	Description
Écraser un fichier existant s'il est plus ancien	Si l'emplacement de destination comporte un fichier de même nom, mais plus ancien que le fichier source, le fichier source est enregistré dans l'emplacement de destination et remplace l'ancienne version.
Écraser les fichiers existants	Tous les fichiers existants dans l'emplacement de destination sont remplacés, quelle que soit la date de leur dernière modification.
Ne pas écraser les fichiers existants	Si l'emplacement de destination comporte un fichier de même nom, aucune modification ne lui est appliquée et le fichier source n'est pas enregistré dans l'emplacement de destination.

16. Cliquez sur **Continuer** pour confirmer votre choix.

Notarisation

La notarisation vous permet de prouver qu'un fichier est authentique et inchangé depuis sa sauvegarde. Nous vous recommandons d'activer la notarisation lors de la sauvegarde de vos fichiers juridiques ou tout autre fichier requérant une authentification.

La notarisation est disponible uniquement pour les sauvegardes de fichiers Google Drive et de Drive partagés Google Workspace.

Comment utiliser la notarisation

Pour activer la notarisation de tous les fichiers sélectionnés pour la sauvegarde, activez le commutateur **Notarisation** lors de la création d'un plan de protection.

Lors de la configuration de la restauration, les fichiers notariés seront marqués d'une icône spéciale. Vous pourrez ainsi vérifier l'authenticité du fichier.

Fonctionnement

Lors d'une sauvegarde, l'agent calcule les code de hachage des fichiers sauvegardés, crée un arbre de hachage (basé sur la structure du dossier), enregistre l'arbre dans la sauvegarde, puis envoie la racine de l'arbre de hachage au service Notary. Le service Notary enregistre la racine de l'arbre de hachage dans la base de données blockchain Ethereum pour s'assurer que cette valeur ne change pas.

Lors de la vérification de l'authenticité d'un fichier, l'agent calcule le hachage du fichier, puis le compare avec le hachage stocké dans l'arbre de hachage sauvegardé. Si ces hachages ne correspondent pas, le fichier n'est pas authentique. Sinon, l'authenticité du fichier est garantie par l'arbre de hachage.

Pour vérifier que l'arbre de hachage n'a pas été compromis, l'agent envoie la racine de l'arbre de hachage au service Notary. Le service Notary la compare avec celle stockée dans la base de données blockchain. Si les hachages correspondent, le fichier sélectionné est authentique. Sinon, le logiciel affiche un message indiquant que le fichier n'est pas authentique.

Vérification de l'authenticité d'un fichier grâce à Notary Service

Si la notarisation a été activée lors de la sauvegarde, vous pouvez vérifier l'authenticité d'un fichier sauvegardé.

Pour vérifier l'authenticité d'un fichier

1. Effectuez l'une des actions suivantes :
   - Pour vérifier l'authenticité d'un fichier Google Drive, sélectionnez le fichier tel que décrit dans les étapes 1 à 7 de la section « Restaurer des fichiers Google Drive ».
   - Pour vérifier l'authenticité d'un fichier de Drive partagé Google Workspace, sélectionnez le fichier tel que décrit dans les étapes 1 à 7 de la section « Restaurer des fichiers de Drive partagés ».
2. Assurez-vous que le fichier sélectionné possède l'icône suivante :  . Cela signifie que le fichier est notarié.
3. Effectuez l'une des actions suivantes :
   - Cliquez sur **Vérifier**.
     Le logiciel vérifie l'authenticité du fichier et affiche le résultat.
   - Cliquez sur **Obtenir certificat**.

Un certificat confirmant la notarisation du fichier est ouvert dans une fenêtre de navigateur Web. La fenêtre contient également les instructions qui vous permettent de vérifier l'authenticité d'un fichier manuellement.

Recherche dans les sauvegardes cloud à cloud

Lors de la restauration des données, vous pouvez effectuer une recherche d'éléments spécifiques sauvegardés au lieu de parcourir l'archive de sauvegarde.

Dans les sauvegardes non chiffrées, la recherche est toujours disponible. Seule la recherche améliorée (basée sur l'index) est prise en charge.

La recherche basée sur l'index est plus rapide et offre des options supplémentaires telles que l'affichage des versions des éléments sauvegardés, la recherche dans les noms des pièces jointes et la recherche en texte intégral dans les sauvegardes Gmail.

Dans les sauvegardes chiffrées, vous pouvez également activer la recherche améliorée (basée sur l'index). Si vous n'activez pas la recherche améliorée, la recherche de base est disponible pour les sauvegardes des boîtes aux lettres Microsoft 365. Pour toutes les autres ressources, la recherche n'est pas disponible.

Le tableau ci-dessous récapitule les options disponibles pour les sauvegardes chiffrées.

Type de ressource	Quoi restaurer	La recherche améliorée est désactivée	La recherche améliorée est activée
Ressources Microsoft 365			
Boîte de réception	Messages de courriers électroniques	La recherche de base (non basée sur l'index) est disponible	La recherche améliorée (basée sur l'index) est disponible
OneDrive	Fichiers/dossiers	La recherche n'est pas disponible	La recherche améliorée (basée sur l'index) est disponible
Site SharePoint	Fichiers SharePoint	La recherche n'est pas disponible	La recherche améliorée (basée sur l'index) est disponible
Teams	Canaux	La recherche n'est pas disponible	La recherche améliorée (basée sur l'index) est disponible
	Messages de courriers électroniques	La recherche de base (non basée sur l'index) est disponible	La recherche améliorée (basée sur l'index) est disponible
	Site d'équipe	La recherche n'est pas disponible	La recherche améliorée (basée sur l'index) est disponible
Ressources Google Workspace			
Boîte de	Messages de	La recherche n'est pas disponible	La recherche améliorée (basée

Type de ressource	Quoi restaurer	La recherche améliorée est désactivée	La recherche améliorée est activée
réception	courriers électroniques		sur l'index) est disponible
Google Drive	Fichiers/dossiers	La recherche n'est pas disponible	La recherche améliorée (basée sur l'index) est disponible
Lecteurs partagés	Fichiers/dossiers	La recherche n'est pas disponible	La recherche améliorée (basée sur l'index) est disponible

Recherche en texte intégral

La recherche en texte intégral est disponible uniquement pour les sauvegardes Gmail et est activée par défaut. Elle vous permet d'effectuer des recherches dans le corps du texte des e-mails sauvegardés. Si cette option est désactivée, vous ne pouvez effectuer des recherches que par objet, expéditeur, destinataire et date.

Un index de recherche en texte intégral prend entre 10 et 30 pour cent de l'espace de stockage occupé par la sauvegarde de Gmail. Un index sans données de recherche en texte intégral est nettement plus petit. Pour économiser de l'espace de stockage, vous pouvez désactiver la recherche en texte intégral et effacer la partie de l'index qui contient les données de recherche en texte intégral.

Index de recherche

Les index de recherche permettent d'effectuer des recherches améliorées dans les archives de sauvegarde cloud à cloud.

Les archives sont indexées automatiquement après chaque opération de sauvegarde. Le processus d'indexation n'a aucune incidence sur les performances de sauvegarde, car l'indexation et la sauvegarde sont effectuées par des composants logiciels distincts.

Les résultats de recherche sont disponibles une fois l'opération d'indexation terminée, ce qui peut prendre jusqu'à 24 heures. L'indexation de la première sauvegarde, qui est complète, prend généralement plus de temps que l'indexation des sauvegardes incrémentielles successives.

Tous les index contiennent des métadonnées qui soutiennent la fonctionnalité de recherche principale : recherche par objet, expéditeur, destinataire ou date. Les index des sauvegardes Gmail contiennent des données supplémentaires si la recherche en texte intégral est activée.

Vérification de la taille d'un index de recherche

La taille des index de recherche augmente avec le temps. Les index des archives de sauvegarde dans lesquelles la recherche en texte intégral est activée peuvent occuper jusqu'à 30 pour cent de la taille de l'archive.

Pour vérifier la taille d'un index de recherche

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Dans l'onglet **Stockage de sauvegarde**, cliquez sur **Sauvegarde des applications cloud**.
3. Vérifiez la valeur figurant dans la colonne **Taille de l'index**.

Mise à jour, reconstruction ou suppression des index

Pour résoudre les problèmes liés à la recherche dans les sauvegardes cloud à cloud, vous pouvez mettre à jour, reconstruire ou supprimer les index de recherche.

Remarque
Nous vous recommandons de contacter l'équipe de support avant de mettre à jour, de reconstruire ou de supprimer un index.

Pour mettre à jour, reconstruire ou supprimer un index

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Dans l'onglet **Stockage de sauvegarde**, cliquez sur **Sauvegarde des applications cloud**. Sélectionnez l'archive dont vous souhaitez mettre à jour, reconstruire ou supprimer l'index.
   La disponibilité de ces actions dépend du niveau et du rôle de l'administrateur, comme suit :

Niveau du compte	Rôle	Peut mettre à jour l'index	Peut reconstruire l'index	Peut supprimer l'index
Tenant partenaire	Administrateur d'entreprise	+	+	+
	Administrateur de cyberprotection	+	-	-
	Administrateur de protection	+	-	-
	Administrateur de protection en lecture seule	-	-	-
Tenant client	Administrateur d'entreprise	+	-	-
	Administrateur de protection	+	-	-
	Administrateur de protection en lecture seule	-	-	-
Unité	Administrateur de l'unité	+	-	-
	Administrateur de protection	+	-	-
	Administrateur de protection en lecture seule	-	-	-

3. Dans le volet **Actions**, sélectionnez l'action à effectuer :
   - **Mettre à jour l'index** : les points de restauration dans l'archive sont vérifiés et les index manquants sont ajoutés.

- **Reconstruire l'index** : les index de tous les points de restauration de l'archive sont supprimés, puis sont recréés.
- **Supprimer l'index** : les index de tous les points de restauration de l'archive sont supprimés.

4. [Pour les archives chiffrées] Spécifiez le mot de passe de chiffrement, puis cliquez sur **OK**.
5. Sélectionnez le champ d'application de l'action, puis cliquez sur **OK**.
   En fonction de l'archive et de l'action sélectionnée, une ou plusieurs des options suivantes sont disponibles :
   - **Métadonnées uniquement**
   - **Contenu seulement**
   - **Métadonnées et recherche de contenu**

Activation de la recherche améliorée dans les sauvegardes chiffrées

Lors de la création d'un plan de sauvegarde pour la sauvegarde cloud à cloud chiffrée, vous pouvez activer une recherche améliorée (basée sur l'index).

Si vous n'activez pas la recherche améliorée, la recherche de base est disponible pour les sauvegardes des boîtes aux lettres Microsoft 365. Pour toutes les autres ressources, la recherche n'est pas disponible. Pour plus d'informations sur les options disponibles, voir "Recherche dans les sauvegardes cloud à cloud" (p. 698).

Remarque
Cette fonctionnalité est disponible dans certains centres de données et peut ne pas être accessible à tous les clients.

Pour activer la recherche dans les sauvegardes chiffrées

1. Lors de la création d'un plan de sauvegarde, activez le commutateur **Chiffrement**.
2. Indiquez et confirmez le mot de passe de chiffrement.
3. Cochez la case **Permettez une recherche améliorée dans les sauvegardes chiffrées**.
4. Cliquez sur **Valider**.

Remarque
Vous ne pourrez ni désactiver le chiffrement ni modifier le mot de passe de chiffrement ultérieurement. Pour créer une sauvegarde non chiffrée ou modifier le mot de passe de chiffrement, créez un nouveau plan de sauvegarde.

Activation ou désactivation de la recherche améliorée dans les plans existants

Vous pouvez modifier un plan existant de sauvegarde chiffrée pour activer ou désactiver la recherche améliorée (basée sur l'index).

Si vous n'activez pas la recherche améliorée, la recherche de base est disponible pour les sauvegardes des boîtes aux lettres Microsoft 365. Pour toutes les autres ressources, la recherche n'est pas disponible. Pour plus d'informations sur les options disponibles, voir "Recherche dans les sauvegardes cloud à cloud" (p. 698).

Dans les sauvegardes non chiffrées, la recherche améliorée est toujours disponible. Cette option ne peut pas être désactivée.

Pour activer ou désactiver la recherche améliorée dans les sauvegardes chiffrées

1. Lors de la modification d'un plan de sauvegarde dans lequel le chiffrement est activé, cliquez sur l'icône d'engrenage dans l'angle supérieur droit.
2. Dans l'onglet **Options de recherche**, activez ou désactivez le commutateur selon les besoins.
3. Cliquez sur **Valider**.
4. Cliquez sur **Enregistrer les paramètres**.

Remarque
Si vous réactivez la recherche améliorée, toutes les archives créées par ce plan de sauvegarde seront à nouveau indexées. Cette opération prend un certain temps.

Désactivation de la recherche en texte intégral pour les sauvegardes Gmail

La recherche en texte intégral est disponible uniquement pour les sauvegardes Gmail et est activée par défaut. Elle vous permet d'effectuer des recherches dans le corps du texte des e-mails sauvegardés. Si cette option est désactivée, vous ne pouvez effectuer des recherches que par objet, expéditeur, destinataire et date.

Vous souhaiterez peut-être désactiver la recherche en texte intégral si la taille de l'index de recherche doit rester à son niveau minimal.

Pour désactiver la recherche en texte intégral

1. Lors de la création ou de la modification d'un plan de sauvegarde, cliquez sur l'icône d'engrenage dans l'angle supérieur droit.
2. Dans l'onglet **Recherche en texte intégral**, désactivez le commutateur.
3. Cliquez sur **Valider**.
4. [Lors de la création d'un plan] Cliquez sur **Appliquer**.
5. [Lors de la modification d'un plan] Cliquez sur **Enregistrer les paramètres**.

Remarque
Si vous réactivez la recherche en texte intégral, toutes les archives créées par ce plan de sauvegarde sont à nouveau indexées. Cette opération prend un certain temps.

Sauvegarde d'Oracle Database

Remarque
Cette fonctionnalité est disponible avec le pack Advanced Backup.

La protection d'Oracle Database est décrite dans un autre document, disponible à l'adresse https://dl.managed-protection.com/u/pdf/OracleBackup_whitepaper_en-US.pdf

Protection de SAP HANA

Remarque
Cette fonctionnalité est disponible avec le pack Advanced Backup.

La protection de SAP HANA est décrite dans un document distinct disponible à cette adresse : https://dl.managed-protection.com/u/pdf/SAP_HANA_backup_whitepaper_en-US.pdf

Protection des données MySQL et MariaDB

Vous pouvez protéger les données MySQL ou MariaDB à l'aide d'une sauvegarde reconnaissant les applications. Elle collecte les métadonnées des applications et permet une restauration granulaire au niveau de l'instance, de la base de données ou de la table.

Remarque
La sauvegarde reconnaissant les applications de données MySQL ou MariaDB est disponible avec le pack Advanced Backup.

Pour protéger une machine physique ou virtuelle qui exécute des instances MySQL ou MariaDB avec la sauvegarde reconnaissant les applications, vous devez installer l'agent pour MySQL/MariaDB sur cette machine. L'agent pour MySQL/MariaDB est fourni avec l'agent pour Linux (64 bits) ; par conséquent, il ne peut être installé que sur des systèmes d'exploitation Linux 64 bits. Consultez "Systèmes d'exploitation et environnements pris en charge" (p. 23).

Télécharger le fichier d'installation de l'agent pour Linux (64 bits)

1. Connectez-vous à la console Cyber Protect.
2. Cliquez sur l'icône de compte dans l'angle supérieur droit, puis sélectionnez **Téléchargements**.
3. Cliquez sur **Agent pour Linux (64 bits)**.

Le fichier d'installation est téléchargé sur votre ordinateur. Pour installer l'agent, procédez tel que décrit dans les sections "Installation des agents de protection sous Linux" (p. 82) ou "Installation ou désinstallation sans assistance sous Linux" (p. 109). Veillez à sélectionner Agent pour MySQL/MariaDB, qui est un composant optionnel.

Pour restaurer des bases de données et des tables vers une instance active, l'agent pour MySQL/MariaDB a besoin d'un stockage temporaire pour fonctionner. Par défaut, le répertoire `/tmp` est utilisé. Vous pouvez modifier ce répertoire en configurant la variable d'environnement `ACRONIS_MYSQL_RESTORE_DIR`.

Limites

- Les clusters MySQL ou MariaDB ne sont pas pris en charge.
- Les instances MySQL ou MariaDB exécutées dans des conteneurs Docker ne sont pas prises en charge.
- Les instances MySQL ou MariaDB exécutées sur des systèmes d'exploitation utilisant le système de fichiers BTRFS ne sont pas prises en charge.
- Les bases de données système (`sys`, `mysql`, `information-schema` et `performance_schema`) et les bases de données qui ne contiennent aucune table ne peuvent pas être restaurées sur des instances actives. Toutefois, ces bases de données ne peuvent pas être restaurées en tant que fichiers lors de la restauration de l'instance complète.
- La restauration est prise en charge uniquement vers les instances cibles dont la version est identique à celle de l'instance sauvegardée, avec les restrictions suivantes :
  - La restauration d'instances MySQL 5.x vers des instances MySQL 8.x n'est pas prise en charge.
  - La reprise vers une version MySQL 5.x ultérieure (y compris les versions mineures) est prise en charge uniquement via une reprise de l'instance complète sous forme de fichiers. Avant de tenter une reprise, consultez le guide officiel de mise à niveau MySQL pour la version cible, par exemple, le Guide de mise à niveau MySQL 5.7.
- La restauration de sauvegardes stockées sur Secure Zone n'est pas prise en charge.
- Les bases de données et les tables ne peuvent pas être restaurées par l'agent pour MySQL/MariaDB qui est encore en cours d'exécution sur un ordinateur sur lequel AppArmor est installé. Vous pouvez toujours restaurer une instance sous forme de fichiers, ou bien la machine entière.
- La restauration vers des bases de données cibles configurées avec des liens symboliques n'est pas prise en charge. Vous pouvez restaurer les bases de données sauvegardées en tant que nouvelles bases de données en modifiant leur nom.

Problèmes connus

Si vous rencontrez des problèmes lors de la restauration de données depuis des partages Samba protégés par mot de passe, déconnectez-vous de la console Cyber Protect, puis reconnectez-vous à cette dernière. Sélectionnez le point de récupération désiré, puis cliquez sur **Bases de données MySQL/MariaDB**.Ne cliquez pas sur **Toute la machine** ni sur **Fichiers/dossiers**.

Configuration d'une sauvegarde reconnaissant les applications

Prérequis

- Au moins une instance MySQL ou MariaDB doit être en cours d'exécution sur l'ordinateur sélectionné.
- Sur l'ordinateur sur lequel l'instance MySQL ou MariaDB est en cours d'exécution, l'agent de protection doit être lancé à l'aide de l'utilisateur root (superutilisateur).
- La sauvegarde reconnaissant les applications n'est disponible que lorsque l'option **Toute la machine** est sélectionnée en tant que source de sauvegarde dans le plan de protection.
- L'option de sauvegarde **Secteur par secteur** doit être désactivée dans les options du plan de protection. Dans le cas contraire, la restauration des donnes d'application est impossible.

Configurer une sauvegarde reconnaissant les applications

1. Dans la console Cyber Protect, sélectionnez un ou plusieurs ordinateurs sur lesquels une instance MySQL ou MariaDB est en cours d'exécution.
   Vous pouvez disposer d'une ou plusieurs instances sur le même ordinateur.
2. Créez un plan de protection avec le module de sauvegarde activé.
3. Dans **Quoi sauvegarder**, sélectionnez **Toute la machine**.
4. Cliquez sur **Sauvegarde d'applications**, puis activez l'interrupteur à côté de **MySQL/MariaDB Server**.
5. Sélectionnez comment spécifier les instances MySQL ou MariaDB :
   - **Pour toutes les ressources**
     Choisissez cette option si vous exécutez des instances dont la configuration est identique sur plusieurs serveurs. Les mêmes paramètres et identifiants de connexion seront utilisés pour toutes les instances.
   - **Pour des ressources spécifiques**
     Choisissez cette option pour spécifier les paramètres et identifiants de connexion pour chaque instance.
6. Cliquez sur **Ajouter une instance** pour configurer les paramètres et identifiants de connexion pour chaque instance.
   a. Sélectionnez le type de connexion, puis spécifiez les éléments suivants :
      - [Pour socket TCP] Adresse IP et port.
      - [Pour socket Unix] Chemin d'accès du socket.
   b. Spécifiez les identifiants d'un compte utilisateur possédant les autorisations suivantes pour l'instance :
      - `FLUSH_TABLES` ou `RELOAD` pour toutes les bases de données et tables (`*.*`)
      - `SELECT` pour `information_schema.tables`

c. Cliquez sur **OK**.

7. Cliquez sur **Valider**.

Restauration à partir d'une sauvegarde reconnaissant les applications

À partir d'une sauvegarde reconnaissant les applications, vous pouvez restaurer des instances, bases de données et tables MySQL ou MariaDB. Vous pouvez aussi restaurer le serveur tout entier sur lequel ces instances sont en cours d'exécution, ou des fichiers et dossiers de ce serveur.

Le tableau ci-dessous résume toutes les options de restauration.

Quoi restaurer	Restaurer en tant que	Récupérer vers
Serveur MySQL Serveur MariaDB	Toute la machine	Machine* sur laquelle l'agent pour Linux est installé
Serveur MySQL Serveur MariaDB	Fichiers ou dossiers	Machine* sur laquelle l'agent pour Linux est installé
Instance	Fichiers	Machine* sur laquelle l'agent pour MySQL/MariaDB est installé
Base de données	La même base de données Nouvelle base de données	Machine* sur laquelle l'agent pour MySQL/MariaDB est installé • Instance d'origine • Une autre instance • Base de données d'origine • Nouvelle base de données
Table	La même table Une nouvelle table	Machine* sur laquelle l'agent pour MySQL/MariaDB est installé • Instance d'origine • Une autre instance • Base de données d'origine • La table d'origine • Une nouvelle table

* Une machine virtuelle contenant un agent est traitée comme une machine physique du point de vue de la sauvegarde.

Restauration du serveur tout entier

Pour apprendre à restaurer l'ensemble du serveur sur lequel des instances MySQL ou MariaDB sont en cours d'exécution, reportez-vous à "Restauration d'une machine" (p. 522).

Restauration d'instances

À partir d'une sauvegarde reconnaissant les applications, vous pouvez restaurer des instances MySQL ou MariaDB sous la forme de fichiers.

Restaurer une instance

1. Dans la console Cyber Protect, sélectionnez l'ordinateur sur lequel les données que vous souhaitez restaurer étaient initialement présentes.
2. Cliquez sur **Restauration**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Effectuez l'une des actions suivantes :

   - Si la sauvegarde est située sur le Cloud ou à un emplacement de stockage partagé (c.-à-d. que d'autres agents peuvent y accéder), cliquez sur **Sélectionner un ordinateur**, sélectionnez un ordinateur en ligne avec agent pour MySQL/MariaDB, puis choisissez un point de récupération.
   - Sélectionnez un point de récupération dans l'onglet **Stockage de sauvegarde**.

   La machine choisie pour la navigation avec l'une des actions ci-dessus devient une machine cible pour la restauration.
4. Cliquez sur **Restaurer** > **Bases de données MySQL/MariaDB**.
5. Sélectionnez l'instance à restaurer, puis cliquez sur **Restaurer en tant que fichiers**.
6. Sous **Chemin d'accès**, sélectionnez le répertoire vers lequel les fichiers seront restaurés.
7. Cliquez sur **Démarrer la récupération**.

Restauration de bases de données

À partir d'une sauvegarde reconnaissant les applications, vous pouvez restaurer des bases de données vers des instances MySQL ou MariaDB.

1. Dans la console Cyber Protect, sélectionnez l'ordinateur sur lequel les données que vous souhaitez restaurer étaient initialement présentes.
2. Cliquez sur **Restauration**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Effectuez l'une des actions suivantes :

- Si la sauvegarde est située sur le Cloud ou à un emplacement de stockage partagé (c.-à-d. que d'autres agents peuvent y accéder), cliquez sur **Sélectionner un ordinateur**, sélectionnez un ordinateur en ligne avec agent pour MySQL/MariaDB, puis choisissez un point de récupération.
- Sélectionnez un point de récupération dans l'onglet **Stockage de sauvegarde**.

La machine choisie pour la navigation avec l'une des actions ci-dessus devient une machine cible pour la restauration.

4. Cliquez sur **Restaurer** > **Bases de données MySQL/MariaDB**.
5. Cliquez sur le nom de l'instance désirée pour explorer ses bases de données.
6. Sélectionnez une ou plusieurs bases de données à restaurer.
7. Cliquez sur **Restaurer**.
8. Cliquez sur **Instance MySQL/MariaDB cible** pour spécifier les paramètres et identifiants de connexion pour l'instance cible.
   - Vérifiez l'instance sur laquelle vous voulez restaurer les données. Par défaut, l'instance d'origine est sélectionnée.
   - Spécifiez les identifiants d'un compte utilisateur capable d'accéder à l'instance cible. Les privilèges suivants doivent être attribués à ce compte utilisateur pour toutes les bases de données et tables (`*.*`) :
     - `INSERT`
     - `CREATE`
     - `DROP`
     - `LOCK_TABLES`
     - `ALTER`
     - `SELECT`
   - Cliquez sur **OK**.
9. Vérifiez la base de données cible.

   Par défaut, la base de données d'origine est sélectionnée.

   Pour restaurer une base de données en tant que nouvelle base de données, cliquez sur le nom de la base de données cible et modifiez-le. Cette action n'est disponible que si vous restaurez une seule base de données.
10. Sous **Écraser les bases de données existantes**, sélectionnez le mode d'écrasement.

    Par défaut, l'écrasement est activé et la base de données sauvegardée remplace la base de données cible qui possède le même nom.

    Si l'écrasement est désactivé, la base de données sauvegardée est ignorée lors de l'opération de récupération et ne remplace pas la base de données cible qui possède le même nom.
11. Cliquez sur **Démarrer la récupération**.

Restauration de tables

À partir d'une sauvegarde reconnaissant les applications, vous pouvez restaurer des tables vers des instances MySQL ou MariaDB actives.

1. Dans la console Cyber Protect, sélectionnez l'ordinateur sur lequel les données que vous souhaitez restaurer étaient initialement présentes.
2. Cliquez sur **Restauration**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Effectuez l'une des actions suivantes :

   - Si la sauvegarde est située sur le Cloud ou à un emplacement de stockage partagé (c.-à-d. que d'autres agents peuvent y accéder), cliquez sur **Sélectionner un ordinateur**, sélectionnez un ordinateur en ligne avec agent pour MySQL/MariaDB, puis choisissez un point de récupération.
   - Sélectionnez un point de récupération dans l'onglet **Stockage de sauvegarde**.

   La machine choisie pour la navigation avec l'une des actions ci-dessus devient une machine cible pour la restauration.
4. Cliquez sur **Restaurer** > **Bases de données MySQL/MariaDB**.
5. Cliquez sur le nom de l'instance désirée pour explorer ses bases de données.
6. Cliquez sur le nom de la base de données désirée pour explorer ses tables.
7. Sélectionnez une ou plusieurs tables à restaurer.
8. Cliquez sur **Restaurer**.
9. Cliquez sur **Instance MySQL/MariaDB cible** pour spécifier les paramètres et identifiants de connexion pour l'instance cible.
   - Vérifiez l'instance sur laquelle vous voulez restaurer les données. Par défaut, l'instance d'origine est sélectionnée.
   - Spécifiez les identifiants d'un compte utilisateur capable d'accéder à l'instance cible. Les privilèges suivants doivent être attribués à ce compte utilisateur pour toutes les bases de données et tables (`*.*`) :
     - `INSERT`
     - `CREATE`
     - `DROP`
     - `LOCK_TABLES`
     - `ALTER`
     - `SELECT`
   - Cliquez sur **OK**.

10. Vérifiez la base cible.

    Par défaut, la table d'origine est sélectionnée.

    Pour restaurer une table en tant que nouvelle table, cliquez sur le nom de la table cible et modifiez-le. Cette action n'est disponible que si vous restaurez une seule table.
11. Sous **Écraser les tables existantes**, sélectionnez le mode d'écrasement.

    Par défaut, l'écrasement est activé et la table sauvegardée remplace la table cible qui possède le même nom.

    Si l'écrasement est désactivé, la table sauvegardée est ignorée lors de l'opération de récupération et ne remplace pas la table cible qui possède le même nom.
12. Cliquez sur **Démarrer la récupération**.

Récupération des routines stockées

Lorsque vous récupérez une instance MySQL complète, les routines stockées sont automatiquement restaurées.

Lorsque vous récupérez une base de données individuelle vers une instance non originale ou que vous la récupérez en tant que nouvelle base de données, les routines stockées ne sont pas automatiquement restaurées. Vous pouvez les restaurer manuellement, en les exportant dans un fichier SQL, puis en les ajoutant à la base de données restaurée.

Pour exporter les routines stockées et les ajouter à une base de données restaurée

1. Sur la machine où se trouve l'instance MySQL d'origine, ouvrez Terminal.
2. Exécutez la commande suivante pour exporter les routines stockées.
3. ```
   mysqldump -p [source_database_name] --routines --no-create-info --no-data > [exported_db_routines.sql]
   ```
4. Sur la machine où la base de données est restaurée, ouvrez le client MySQL en ligne de commande .
5. Exécutez les commandes suivantes pour ajouter les routines à la base de données restaurée.

   ```
   mysql>  use [recovered_database_name];
   ```

   ```
   mysql>  source [path_to_exported_db_routines.sql];
   ```

Protection des sites Web et hébergement des serveurs

Protection des sites Web

Un site Web peut être corrompu à la suite d'un accès non autorisé ou d'une attaque de logiciel malveillant. Sauvegardez votre site Web si vous souhaitez rétablir facilement son état de santé, en cas de corruption.
   ```

De quoi ai-je besoin pour effectuer une sauvegarde de site Web ?

Le site Web doit être accessible via le protocole SFTP ou SSH. Vous n'avez pas d'agent à installer, ajoutez simplement un site Web, comme décrit plus loin dans cette section.

Quels éléments peuvent être sauvegardés ?

Vous pouvez sauvegarder les éléments suivants :

- **Les fichiers de contenu du site Web**
  Tous les fichiers accessibles au compte que vous indiquez pour la connexion SFTP ou SSH.
- **Les bases de données associées (le cas échéant) hébergées sur des serveurs MySQL.**
  Toutes les bases de données accessibles au compte MySQL que vous aurez indiqué.

Si votre site Web utilise des bases de données, nous vous recommandons de sauvegarder aussi bien les fichiers que les bases de données, afin de pouvoir les récupérer dans un état cohérent.

Limites

- Le seul emplacement de sauvegarde disponible pour la sauvegarde d'un site Web est le stockage dans le Cloud.
- Il est possible d'appliquer plusieurs plans de protection à un site Web, mais un seul d'entre eux peut s'exécuter selon une planification. Les autres plans doivent être lancés manuellement.
- La seule option de sauvegarde disponible est « Nom de fichier de la sauvegarde ».
- Les plans de protection de site Web ne s'affichent pas dans l'onglet **Gestion** > **Plans de protection**.

Sauvegarder un site Web

Pour ajouter un site Web

1. Cliquez sur **Terminaux** > **Ajouter**.
2. Cliquez sur **Site Web**.
3. Configurez les paramètres d'accès suivants pour le site Web :
   - Dans **Nom du site Web**, créez et saisissez un nom pour votre site Web. Ce nom s'affichera dans la console Cyber Protect.
   - Dans **Hôte**, indiquez le nom de l'hôte ou l'adresse IP qui sera utilisé pour accéder au site Web via SFTP ou SSH. Par exemple, `my.server.com` ou `10.250.100.100`.
   - Dans **Port**, indiquez le numéro de port.
   - Dans **Nom d'utilisateur** et **Mot de passe**, indiquez les informations d'identification du compte qui peuvent être utilisées pour accéder au site Web via SFTP ou SSH.

Important
Seuls les fichiers accessibles au compte indiqué seront sauvegardés.

Au lieu d'un mot de passe, vous pouvez indiquer votre clé privée SSH. Pour cela, cochez la case **Utiliser une clé privée SSH au lieu du mot de passe**, puis indiquer la clé.

4. Cliquez sur **Suivant**.
5. Si votre site Web utilise des bases de données MySQL, configurez les paramètres d'accès pour les bases de données. Sinon, cliquez sur **Ignorer**.
   a. Dans **Type de connexion**, sélectionnez comment accéder aux bases de données depuis le Cloud :
      - **Via SSH depuis l'hôte**—Vous accèderez aux bases de données depuis l'hôte indiqué à l'étape 3.
      - **Connexion directe**—Vous accèderez aux bases de données directement. Choisissez ce paramètre uniquement si les bases de données sont accessibles depuis Internet.
   b. Dans **Hôte**, indiquez le nom ou l'adresse IP de l'hôte dans lequel le serveur MySQL fonctionne.
   c. Dans **Port**, indiquez le numéro de port pour la connexion TCP/IP au serveur. Le numéro de port par défaut est 3306.
   d. Dans **Nom d'utilisateur** et **Mot de passe**, indiquez les informations d'identification du compte MySQL.

      Important
      Seules les bases de données accessibles au compte indiqué seront sauvegardées.

   e. Cliquez sur **Créer**.

   Le site Web apparaît dans la console Cyber Protect sous **Terminaux** > **Sites Web**.

Pour modifier les paramètres de connexion

1. Sélectionnez le site Web sous **Terminaux** > **Sites Web**.
2. Cliquez sur **Détails**.
3. Cliquez sur l'icône en forme de crayon à côté du site Web ou des paramètres de connexion à la base de données.
4. Effectuez les modifications nécessaires, puis cliquez sur **Enregistrer**.

Créer un plan de protection pour des sites Web

1. Sélectionnez un ou plusieurs sites Web sous **Terminaux** > **Sites Web**.
2. Cliquez sur **Protection**.
3. [Facultatif] Activez la sauvegarde des bases de données.

   Si plusieurs sites Web ont été sélectionnés, la sauvegarde des bases de données est désactivée par défaut.

4. [Facultatif] Modifiez les règles de rétention.
5. [Facultatif] Activez le chiffrement des sauvegardes.
6. [Facultatif] Cliquez sur l'icône en forme d'engrenage pour modifier l'option **Sauvegarde du nom de fichier**. Cela s'avère utile dans deux cas :
   - Si vous avez déjà sauvegardé ce site Web et que vous souhaitez continuer la séquence de sauvegardes existante.
   - Si vous souhaitez voir le nom personnalisé dans l'onglet **Stockage de sauvegarde**
7. Cliquez sur **Appliquer**.

Vous pouvez modifier, révoquer et supprimer les plans de protection pour les sites Web de la même façon que pour les machines. Ces opérations sont décrites dans la section « Opérations avec les plans de protection ».

Restauration d'un site Web

Pour récupérer un site Web

1. Effectuez l'une des actions suivantes :
   - Sous **Terminaux** > **Sites Web**, sélectionnez le site Web que vous souhaitez récupérer, puis cliquez sur **Récupération**.

     Vous pouvez rechercher les sites Web par nom. Les caractères génériques ne sont pas pris en charge.
   - Si le site Web a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

     Pour récupérer un site Web supprimé, vous devez ajouter le site cible en tant que terminal.
2. Sélectionnez le point de restauration.
3. Cliquez sur **Restaurer**, puis sélectionnez ce que vous souhaitez récupérer : **Site Web entier**, **Bases de données** (le cas échéant) ou **Fichiers/dossiers**.

   Pour que votre site Web soit dans un état cohérent, nous vous recommandons de restaurer les fichiers et les bases de données, dans n'importe quel ordre.
4. En fonction de votre choix, suivez l'une des procédures décrites ci-dessous.

Pour récupérer le site Web entier

1. Dans **Récupérer sur un site Web**, affichez ou modifiez le site Web cible.

   Le site Web d'origine est sélectionné par défaut. Si celui-ci n'existe pas, vous devez sélectionner le site Web cible.
2. Choisissez de restaurer ou non les permissions de partage associées aux éléments restaurés.
3. Cliquez sur **Démarrer la récupération**, puis confirmez l'action.

Pour récupérer les bases de données

1. Sélectionnez les bases de données que vous voulez restaurer.
2. Si vous souhaitez télécharger une base de données en tant que fichier, cliquez sur **Télécharger**, sélectionnez l'emplacement dans lequel la sauvegarder, puis cliquez sur **Enregistrez**. Sinon, ignorez cette étape.
3. Cliquez sur **Restaurer**.
4. Dans **Récupérer sur un site Web**, affichez ou modifiez le site Web cible.
   Le site Web d'origine est sélectionné par défaut. Si celui-ci n'existe pas, vous devez sélectionner le site Web cible.
5. Cliquez sur **Démarrer la récupération**, puis confirmez l'action.

Pour récupérer les fichiers/dossiers du site Web

1. Sélectionnez les fichiers/dossiers que vous souhaitez récupérer.
2. Si vous souhaitez enregistrer un fichier, cliquez sur **Télécharger**, sélectionnez l'emplacement dans lequel le sauvegarder, puis cliquez sur **Enregistrer**. Sinon, ignorez cette étape.
3. Cliquez sur **Restaurer**.
4. Dans **Récupérer sur un site Web**, affichez ou modifiez le site Web cible.
   Le site Web d'origine est sélectionné par défaut. Si celui-ci n'existe pas, vous devez sélectionner le site Web cible.
5. Choisissez de restaurer ou non les permissions de partage associées aux éléments restaurés.
6. Cliquez sur **Démarrer la récupération**, puis confirmez l'action.

Protéger les serveurs d'hébergement Web

Vous pouvez protéger les serveurs d'hébergement Web Linux qui exécutent des panneaux de configuration cPanel, Plesk, DirectAdmin, VirtualMin ou ISPManager. Les serveurs qui exécutent des panneaux de configuration d'hébergement Web d'autres fournisseurs sont protégés comme des ressources classiques.

Quotas

Les serveurs qui exécutent des panneaux de configuration cPanel, Plesk, DirectAdmin, VirtualMin ou ISPManager sont considérés comme des serveurs d'hébergement Web. Chaque serveur d'hébergement Web sauvegardé consomme le quota des **serveurs d'hébergement Web**. Si ce quota est désactivé ou si la surconsommation pour ce quota est dépassée, un quota sera attribué comme suit ou la sauvegarde échouera :

- Si le serveur est physique, le quota des **serveurs** sera utilisé. Si ce quota est désactivé ou dépassé, la sauvegarde échouera.
- Si le serveur est virtuel, le quota des **machines virtuelles** sera utilisé. Si ce quota est désactivé ou dépassé, la sauvegarde échouera.

Intégration de DirectAdmin, de cPanel et de Plesk

Les administrateurs d'hébergement Web qui utilisent DirectAdmin, Plesk ou cPanel peuvent intégrer ces panneaux de configuration au service Cyber Protection afin d'accéder à différentes fonctionnalités très utiles :

- Sauvegarde de l'intégralité d'un serveur d'hébergement Web dans le stockage dans le cloud, avec sauvegarde de disque
- Restauration de l'intégralité d'un serveur, y compris tous les comptes et sites Web
- Exécution d'une restauration granulaire et téléchargement de comptes, de sites Web, de fichiers, de boîtes aux lettres ou de bases de données
- Activation de revendeurs et de clients pour qu'ils exécutent la reprise en libre-service de leurs propres données

Pour exécuter l'intégration, vous devez utiliser une extension de service Cyber Protection. Pour plus d'informations, reportez-vous aux guides d'intégration correspondants :

- Guide d'intégration de DirectAdmin
- Guide d'intégration de WHM et cPanel
- Guide d'intégration de Plesk

Opérations spéciales avec les machines virtuelles

Exécution d'une machine virtuelle à partir d'une sauvegarde (restauration instantanée)

Vous pouvez exécuter une machine virtuelle depuis une sauvegarde de niveau disque contenant un système d'exploitation. Cette opération, aussi appelée restauration instantanée, vous permet de lancer un serveur virtuel en quelques secondes. Les disques virtuels sont émulés directement depuis la sauvegarde et n'utilisent pas d'espace dans le magasin de données (stockage). Seule la conservation des modifications des disques virtuels nécessite de l'espace de stockage.

Nous vous recommandons de laisser cette machine virtuelle temporaire fonctionner pendant un maximum de trois jours. Vous pourrez alors la supprimer entièrement ou la convertir en machine virtuelle standard (finalisation) sans temps d'arrêt du système.

Tant que la machine virtuelle temporaire existe, les règles de rétention ne peuvent être appliquées à la sauvegarde utilisée par celle-ci. L'exécution des sauvegardes de la machine d'origine se poursuit.

Exemples d'utilisation

- **Reprise d'activité après sinistre**
  Mettez instantanément en ligne une copie d'une machine qui a planté.

- **Test d'une sauvegarde**

  Exécutez la machine depuis la sauvegarde et assurez-vous que le SE invité et les applications fonctionnent correctement.
- **Accès aux données d'application**

  Tant que la machine est en cours d'exécution, utilisez les outils de gestion natifs de l'application pour accéder aux données nécessaires et les extraire.

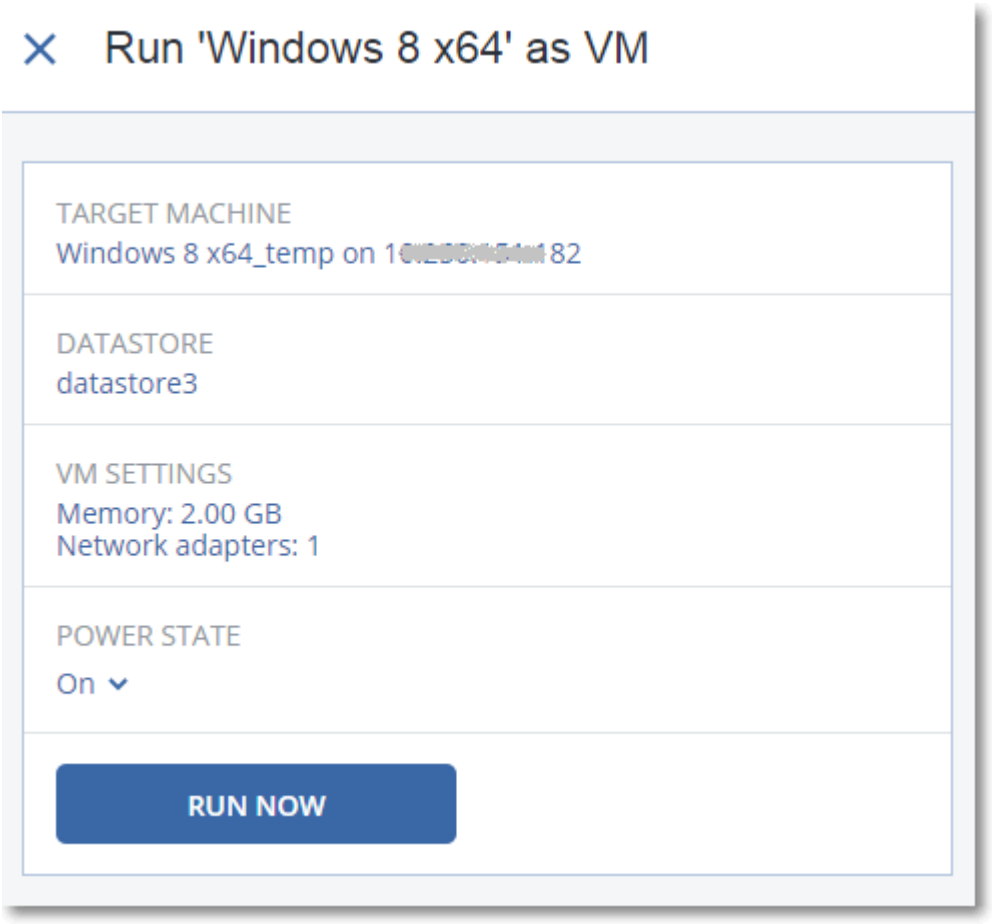
Prérequis

- Au moins un agent pour VMware ou Hyper-V doit être enregistré dans le service Cyber Protection.
- La sauvegarde peut être stockée dans un dossier réseau ou local de la machine sur laquelle l'agent pour VMware ou Hyper-V est installé. Si vous sélectionnez un dossier réseau, il doit être accessible depuis cette machine. Il est possible d'exécuter une machine virtuelle à partir d'une sauvegarde stockée sur le Cloud, mais celle-ci sera plus lente, car l'opération nécessite d'importantes lectures en accès aléatoire à partir de la sauvegarde.
- La sauvegarde doit contenir une machine entière ou l'ensemble des volumes requis pour le démarrage du système d'exploitation.
- Des sauvegardes de machines à la fois physiques et virtuelles peuvent être utilisées. Les sauvegardes de *conteneurs* Virtuozzo ne peuvent pas être utilisées.
- Les sauvegardes qui contiennent des volumes logiques Linux (LVM) doivent être créées par l'agent pour VMware ou l'agent pour Hyper-V. La machine virtuelle doit être du même type que la machine d'origine (ESXi ou Hyper-V).

Exécution de la machine

1. Effectuez l'une des actions suivantes :
   - Sélectionnez une machine sauvegardée, cliquez sur **Restauration**, puis sélectionnez un point de restauration.
   - Sélectionnez un point de récupération dans l'onglet Stockage de sauvegarde.
2. Cliquez sur **Exécuter en tant que MV**.

   Le logiciel sélectionne automatiquement l'hôte et les autres paramètres requis.



3. [Facultatif] Cliquez sur **Machine cible**, puis modifiez le type de machine virtuelle (ESXi ou Hyper-V), l'hôte ou le nom de machine virtuelle.
4. [Facultatif] Cliquez sur **Magasin de données** pour ESXi ou **Chemin d'accès** pour Hyper-V, puis sélectionnez le magasin de données pour la machine virtuelle.

   Les modifications des disques virtuels s'accumulent tant que la machine est en cours d'exécution. Assurez-vous que le magasin de données sélectionné dispose d'un espace libre suffisant. Si vous prévoyez de conserver ces modifications en rendant la machine virtuelle permanente, sélectionnez un magasin de données adapté à la machine en production.
5. [Facultatif] Cliquez sur **Paramètres de MV** pour modifier la taille de la mémoire et les connexions réseau de la machine virtuelle.
6. [Facultatif] Sélectionnez l'état d'alimentation de la MV (**Activé**/**Arrêt**).
7. Cliquez sur **Exécuter maintenant**.

La machine apparaît alors dans l'interface Web avec une des icônes suivantes :  ou 

. Ces machines virtuelles ne peuvent pas être sélectionnées pour la sauvegarde.

Remarque
Vous pouvez exécuter l'opération Exécuter en tant que machine virtuelle (restauration instantanée) avec des sauvegardes dans Microsoft Azure. Toutefois, cette opération engendre un trafic considérable pour le transfert de données vers des emplacements externes qui sera ajouté à votre facture d'abonnement Microsoft Azure. En général, le trafic pour le transfert de données vers des emplacements externes d'un ordinateur Windows s'exécutant à partir d'une sauvegarde Microsoft Azure est d'environ 5 Go, depuis le démarrage de la machine virtuelle jusqu'à la connexion.

Suppression de la machine

Nous vous recommandons de ne pas supprimer une machine virtuelle temporaire directement dans vSphere/Hyper-V, car cela peut créer des artefacts dans l'interface Web. De plus, la sauvegarde depuis laquelle s'exécutait la machine peut rester verrouillée pendant un certain temps (elle ne peut pas être supprimée par les règles de rétention).

Suppression d'une machine virtuelle s'exécutant depuis une sauvegarde

1. Dans l'onglet **Tous les terminaux**, sélectionnez une machine virtuelle s'exécutant depuis une sauvegarde.
2. Cliquez sur **Supprimer**.

La machine est supprimée de l'interface Web. Elle est également supprimée du magasin de données (stockage) et de l'inventaire vSphere ou Hyper-V. Toutes les modifications des données pendant l'exécution de la machine sont perdues.

Finalisation de la machine

Tant qu'une machine virtuelle s'exécute depuis une sauvegarde, le contenu des disques virtuels est obtenu directement de cette sauvegarde. De ce fait, la machine devient inaccessible, voire endommagée, si la connexion avec l'emplacement de sauvegarde ou l'agent de protection est perdue.

Vous pouvez rendre cette machine permanente, c'est-à-dire restaurer l'ensemble de tous les disques virtuels, y compris les modifications effectuées lors de l'exécution de la machine, dans le magasin de données stockant ces modifications. Ce processus s'appelle la finalisation.

La finalisation s'effectue sans indisponibilité du système. La machine virtuelle n'est *pas* mise hors tension lors de la finalisation.

L'emplacement des disques virtuels finaux est défini dans les paramètres de l'opération **Exécuter en tant que MV** (**Magasin de données** pour ESXi ou **Chemin d'accès** pour Hyper-V). Avant de commencer la finalisation, assurez-vous que l'espace disponible, les capacités de partage et les performances de ce magasin de données sont adaptés à l'exécution de la machine en production.

Remarque
La finalisation n'est pas prise en charge pour l'Hyper-V qui s'exécute sous Windows Server 2008/2008 R2 et Microsoft Hyper-V Server 2008/2008 R2, car l'API nécessaire manque dans ces versions d'Hyper-V.

Finalisation d'une machine virtuelle s'exécutant depuis une sauvegarde

1. Dans l'onglet **Tous les terminaux**, sélectionnez une machine virtuelle s'exécutant depuis une sauvegarde.
2. Cliquez sur **Finaliser**.
3. [Facultatif] Indiquez un nouveau nom pour la machine.
4. [Facultatif] Modifiez le mode d'allocation du disque. Le paramètre par défaut est **Dynamique**.
5. Cliquez sur **Finaliser**.

Le nom de la machine est immédiatement modifié. La progression de la restauration sont affichées dans l'onglet **Activités**. Une fois la restauration terminée, l'icône de la machine devient celle d'une machine virtuelle standard.

Ce que vous devez savoir à propos de la finalisation

Finalisation vs. récupération normale

Le processus de finalisation est plus lent qu'une récupération normale pour les raisons suivantes :

- Lors d'une finalisation, l'agent accède aléatoirement aux différentes parties de la sauvegarde. Lorsqu'une machine entière est restaurée, l'agent lit de manière séquentielle les données de la sauvegarde.
- Si la machine virtuelle est exécutée pendant la finalisation, l'agent lit les données de la sauvegarde plus souvent, afin de maintenir les deux processus simultanément. Lors d'une récupération normale, la machine virtuelle est arrêtée.

Finalisation des machines exécutées depuis des sauvegardes Cloud

En raison de l'accès intensif aux données sauvegardées, la vitesse de finalisation dépend fortement de la bande passante de connexion entre l'emplacement de la sauvegarde et l'agent. La finalisation sera plus lente pour les sauvegardes situées dans le Cloud que pour les sauvegardes locales. Si la connexion Internet est très lente ou instable, la finalisation d'une machine exécutée depuis une sauvegarde Cloud peut échouer. Nous vous recommandons d'exécuter des machines virtuelles à partir de sauvegardes locales si vous prévoyez d'effectuer la finalisation et que vous avez le choix.

Remarque
La vitesse de finalisation varie selon que l'agent est connecté à un hôte VMware ESXi ou à vCenter, comme le décrit l'étape 3 de "Configuration de l'appliance virtuelle" (p. 143). La connexion à un VMware vCenter peut ralentir la finalisation en raison des spécificités des API VMware. Pour accélérer la finalisation, utilisez un agent pour VMware distinct pour l'opération **Exécuter en tant que MV** qui est suivie de la finalisation et dans laquelle cet agent est connecté à un hôte ESXi au lieu d'un vCenter.

Fonctionnement dans VMware vSphere

Cette section décrit les opérations spécifiques aux environnements VMware vSphere.

Réplication de machines virtuelles

La réplication est uniquement disponible pour les machines virtuelles VMware ESXi.

La réplication est un processus visant à créer une copie exacte (réplica) d'une machine virtuelle, puis à conserver la synchronisation du réplica avec la machine d'origine. En répliquant une machine virtuelle critique, vous disposerez toujours d'une copie de cette machine et qui sera toujours prête à démarrer.

La réplication peut être démarrée manuellement ou selon la planification que vous définissez. La première réplication est complète (elle copie la machine en entier). Toutes les réplications subséquentes sont incrémentielles et effectuées avec Suivi des blocs modifiés, sauf si cette option est désactivée.

Réplication vs. sauvegarde

Contrairement aux sauvegardes planifiées, un réplica conserve l'état le plus récent de la machine virtuelle. Un réplica consomme de l'espace au sein du magasin de données, tandis que les sauvegardes peuvent être conservées dans un espace de stockage plus abordable.

Toutefois, recourir à un réplica est beaucoup plus rapide qu'une restauration et que l'exécution d'une machine virtuelle depuis une sauvegarde. Lorsqu'il est utilisé, un réplica travaille plus rapidement qu'une machine virtuelle exécutée depuis une sauvegarde et ne charge pas l'agent pour VMware.

Exemples d'utilisation

- **Répliquer des machines virtuelles sur un site distant.**
  La réplication vous permet de faire face aux défaillances des centres de données partielles ou complètes, en clonant les machines virtuelles depuis un site secondaire. Le site secondaire se trouve habituellement dans emplacement à distance qui est susceptible d'être affecté par l'environnement, l'infrastructure ou d'autres facteurs qui pourraient provoquer la défaillance du premier site.

- **Répliquer des machines virtuelles au sein d'un site unique (depuis un hôte/magasin de données vers un autre).**

  La réplication sur site peut être utilisée pour des scénarios de reprise d'activité après sinistre et de haute disponibilité.

Ce qu'un réplica vous permet de faire

- **Tester un réplica**

  Le réplica sera mis sur tension pour le test. Utilisez vSphere Client ou d'autres outils pour vérifier si le réplica fonctionne correctement. La réplication est suspendue pendant que le test est en cours.
- **Basculement sur un réplica**

  Le basculement est une transition de la ressource depuis la machine virtuelle d'origine vers le réplica. La réplication est suspendue pendant que le basculement est en cours.
- **Sauvegarder le réplica**

  La sauvegarde et la réplication requièrent l'accès aux disques virtuels, ce qui a une incidence sur les performances de l'hôte sur lequel la machine virtuelle s'exécute. Si vous souhaitez à la fois un réplica et des sauvegardes pour une machine virtuelle, mais que vous ne souhaitez pas ajouter de charge sur l'hôte de production, répliquez la machine sur un hôte différent et configurez des sauvegardes du réplica.

Limites

- Les types de machines virtuelles suivants ne peuvent pas être répliqués :
  - Machines insensibles aux défaillances s'exécutant sur ESXi 5.5 et versions ultérieures
  - Machines s'exécutant à partir de sauvegardes
  - Réplicas de machines virtuelles
- Certaines modifications matérielles, telles que l'ajout d'une carte d'interface réseau (NIC) à l'hôte ESXi ou la suppression d'une NIC, entraînent une modification des identifiants internes de l'hôte. Ce changement affecte les plans de réplication des VM. Après une telle modification, vous devez recréer les plans de réplication de VM dans lesquels l'hôte ESXi est sélectionné comme source ou cible. Sinon, les plans de réplication de VM échoueront.

Création d'un plan de réplication

Un plan de réplication doit être créé individuellement pour chaque machine. Il est impossible d'appliquer un plan existant à d'autres machines.

Pour créer un plan de réplication

1. Sélectionnez une machine virtuelle à répliquer.
2. Cliquez sur **Réplication**.

   Le logiciel affiche un nouveau modèle de plan de réplication.
3. [Facultatif] Pour modifier le nom du plan de réplication, cliquez sur le nom par défaut.

4. Cliquez sur **Machine cible**, puis suivez les instructions suivantes :
   a. Choisissez de créer un nouveau réplica ou d'utiliser un réplica existant sur la machine d'origine.
   b. Sélectionnez l'hôte ESXi et spécifiez le nouveau nom du réplica ou sélectionnez un réplica existant.
      Le nom par défaut d'un nouveau réplica est **[Nom d'origine de la machine]_réplica**.
   c. Cliquez sur **OK**.
5. [Uniquement en cas de réplication sur une nouvelle machine] Cliquez sur **Magasin de données**, puis sélectionnez le magasin de données pour la machine virtuelle.
6. [Facultatif] Cliquez sur **Planification** pour modifier la planification de réplication.
   Par défaut, la réplication s'effectue de manière quotidienne, du lundi au vendredi. Vous pouvez sélectionner l'heure de démarrage de la réplication.
   Si vous souhaitez modifier la fréquence des réplications, faites glisser le curseur, puis indiquez la planification.
   Vous pouvez également procéder comme suit :
   - Définir une période au cours de laquelle la planification sera effective. Cochez la case **Exécuter le plan dans une plage de dates**, puis indiquez la plage de dates.
   - Désactiver la planification. Dans ce cas, la réplication peut commencer manuellement.
7. [Facultatif] Cliquez sur l'icône en forme d'engrenage pour modifier les options de réplication.
8. Cliquez sur **Appliquer**.
9. [Facultatif] Pour exécuter le plan manuellement, cliquez sur **Exécuter maintenant** dans le volet du plan.

À la suite de l'exécution d'un plan de réplication, le réplica de la machine virtuelle apparaît dans la liste **Tous les terminaux** avec l'icône suivante : 

Test d'un réplica

Pour préparer un réplica à des fins de test

1. Sélectionnez un réplica à tester.
2. Cliquez sur **Tester un réplica**.
3. Cliquez sur **Démarrer le test**.
4. Sélectionnez si le réplica sous tension doit être connecté à un réseau. Par défaut, le réplica ne sera pas connecté à un réseau.
5. [Facultatif] Si vous choisissez de connecter le réplica au réseau, cochez la case **Arrêter la machine virtuelle d'origine** pour arrêter la machine d'origine avant de mettre le réplica sous tension.
6. Cliquez sur **Démarrer**.

Pour arrêter le test d'un réplica

1. Sélectionnez un réplica en cours de test.
2. Cliquez sur **Tester un réplica**.
3. Cliquez sur **Arrêter le test**.
4. Confirmez votre choix.

Basculement sur un réplica

Pour basculer une machine sur un réplica

1. Sélectionnez un réplica sur lequel basculer.
2. Cliquez sur **Actions de réplica**.
3. Cliquez sur **Basculement**.
4. Sélectionnez si le réplica sous tension doit être connecté à un réseau. Par défaut, le réplica sera connecté au même réseau que la machine d'origine.
5. [Facultatif] Si vous choisissez de connecter le réplica au réseau, décochez la case **Arrêter la machine virtuelle** pour conserver la machine d'origine en ligne.
6. Cliquez sur **Démarrer**.

Lorsque le réplica est en état de basculement, vous pouvez choisir une des options suivantes :

- **Arrêter le basculement**
  Arrêtez le basculement si la machine d'origine a été réparée. Le réplica sera mis hors tension. La réplication sera reprise.
- **Effectuer un basculement permanent sur le réplica**
  Cette opération instantanée supprime la marque « réplica » de la machine virtuelle, et la réplication n'est alors plus possible. Si vous souhaitez reprendre la réplication, modifiez le plan de réplication pour sélectionner cette machine en tant que source.
- **Restauration automatique**
  Effectuez une restauration automatique si vous avez basculé sur le site qui n'est pas destiné aux opérations continues. Le réplica sera restauré sur la machine d'origine ou sur une nouvelle machine virtuelle. Une fois la restauration effectuée sur la machine d'origine, celle-ci est mise sous tension et la réplication reprend. Si vous choisissez de restaurer sur une nouvelle machine, modifiez le plan de réplication pour sélectionner cette machine en tant que source.

Arrêt du basculement

Pour arrêter le basculement

1. Sélectionnez un réplica en état de basculement.
2. Cliquez sur **Actions de réplica**.
3. Cliquez sur **Arrêter le basculement**.
4. Confirmez votre choix.

Effectuer un basculement permanent

Pour effectuer un basculement permanent

1. Sélectionnez un réplica en état de basculement.
2. Cliquez sur **Actions de réplica**.
3. Cliquez sur **Basculement permanent**.
4. [Facultatif] Modifiez le nom de la machine virtuelle.
5. [Facultatif] Cochez la case **Arrêter la machine virtuelle d'origine**.
6. Cliquez sur **Démarrer**.

Restauration automatique

Pour restaurer automatiquement depuis un réplica

1. Sélectionnez un réplica en état de basculement.
2. Cliquez sur **Actions de réplica**.
3. Cliquez sur **Restauration automatique depuis un réplica**.
   Le logiciel sélectionne automatiquement la machine d'origine comme machine cible.
4. [Facultatif] Cliquez sur **Machine cible**, puis suivez les instructions suivantes :
   a. Sélectionnez si vous souhaitez restaurer automatiquement sur une machine nouvelle ou existante.
   b. Sélectionnez l'hôte ESXi et spécifiez le nouveau nom de machine ou sélectionnez une machine existante.
   c. Cliquez sur **OK**.
5. [Facultatif] Lors de la restauration automatique sur une nouvelle machine, vous pouvez également procéder comme suit :
   - Cliquez sur **Magasin de données** pour sélectionner le magasin de données pour la machine virtuelle.
   - Cliquez sur **Paramètres de MV** pour modifier la taille de mémoire, le nombre de processeurs et les connexions réseau de la machine virtuelle.
6. [Facultatif] Cliquez sur **Options de restauration** pour modifier les options de restauration automatique.
7. Cliquez sur **Démarrer la récupération**.
8. Confirmez votre choix.

Options de réplication

Pour modifier les options de réplication, cliquez sur l'icône en forme d'engrenage située à côté du nom du plan de réplication, puis cliquez sur **Options de réplication**.

Suivi des blocs modifiés (CBT)

Cette option est identique à l'option de sauvegarde « Suivi des blocs modifiés (CBT) ».

Provisionnement du disque

Cette option définit les paramètres de provisionnement du disque pour le réplica.

Le préréglage est le suivant : **Allocation dynamique**.

Les valeurs suivantes sont disponibles : **Thin provisioning**, **Thick provisioning**, **Conserver les paramètres d'origine**.

Gestion erreurs

Cette option est identique à l'option de sauvegarde « Gestion des erreurs ».

Commandes Pré/Post

Cette option est identique à l'option de sauvegarde « Commandes Pré/Post ».

Service de cliché instantané des volumes (VSS) pour les machines virtuelles

Cette option est identique à l'option de sauvegarde « Service de cliché instantané des volumes (VSS) pour les machines virtuelles ».

Options de restauration automatique

Pour modifier les options de restauration automatique, cliquez sur **Options de restauration** lors de la configuration de la restauration automatique.

Gestion erreurs

Cette option est identique à l'option de restauration « Gestion des erreurs ».

Performance

Cette option est identique à l'option de restauration « Performance ».

Commandes Pré/Post

Cette option est identique à l'option de restauration « Commandes Pré/Post ».

Gestion de l'alimentation des MV

Cette option est identique à l'option de restauration « Gestion de l'alimentation des MV ».

Amorçage d'un réplica initial

Pour accélérer la réplication vers un emplacement distant et économiser de la bande passante réseau, vous pouvez effectuer un amorçage du réplica.

Important
Pour réaliser l'amorçage d'un réplica, l'agent pour VMware (appliance virtuelle) doit être exécuté sur l'ESXi cible.

Pour réaliser l'amorçage initial d'un réplica

1. Effectuez l'une des actions suivantes :
   - si la machine virtuelle d'origine peut être mise hors tension, éteignez-la, puis passez à l'étape 4.
   - Si la machine virtuelle d'origine ne peut pas être mise hors tension, passez à l'étape suivante.
2. Créez un plan de réplication.
   Lorsque vous créez le plan, sous **Machine cible**, sélectionnez **Nouveau réplica** et l'ESXi qui héberge la machine d'origine.
3. Exécutez une fois le plan.
   Un réplica est créé sur l'ESXi d'origine.
4. Exportez les fichiers de la machine virtuelle (ou du réplica) sur un disque dur externe.
   a. Connectez le disque dur externe à la machine exécutant vSphere Client.
   b. Connectez vSphere Client au vCenter/ESXi d'origine.
   c. Sélectionnez le réplica nouvellement créé dans l'inventaire.
   d. Cliquez sur **Fichier** > **Exporter** > **Exporter le modèle OVF**.
   e. Dans **Répertoire**, spécifiez le dossier sur le disque dur externe.
   f. Cliquez sur **OK**.
5. Transférez le disque dur à l'emplacement distant.
6. Importez le réplica sur l'ESXi cible.
   a. Connectez le disque dur externe à la machine exécutant vSphere Client.
   b. Connectez vSphere Client au vCenter/ESXi cible.
   c. Cliquez sur **Fichier** > **Déployer le modèle OVF**.
   d. Dans **Déployer à partir d'un fichier ou d'une URL**, spécifiez le modèle que vous avez exporté lors de l'étape 4.
   e. Terminez la procédure d'importation.
7. Modifiez le plan de réplication que vous avez créé dans l'étape 2. Sous **Machine cible**, sélectionnez **Réplica existant**, puis sélectionnez le réplica importé.

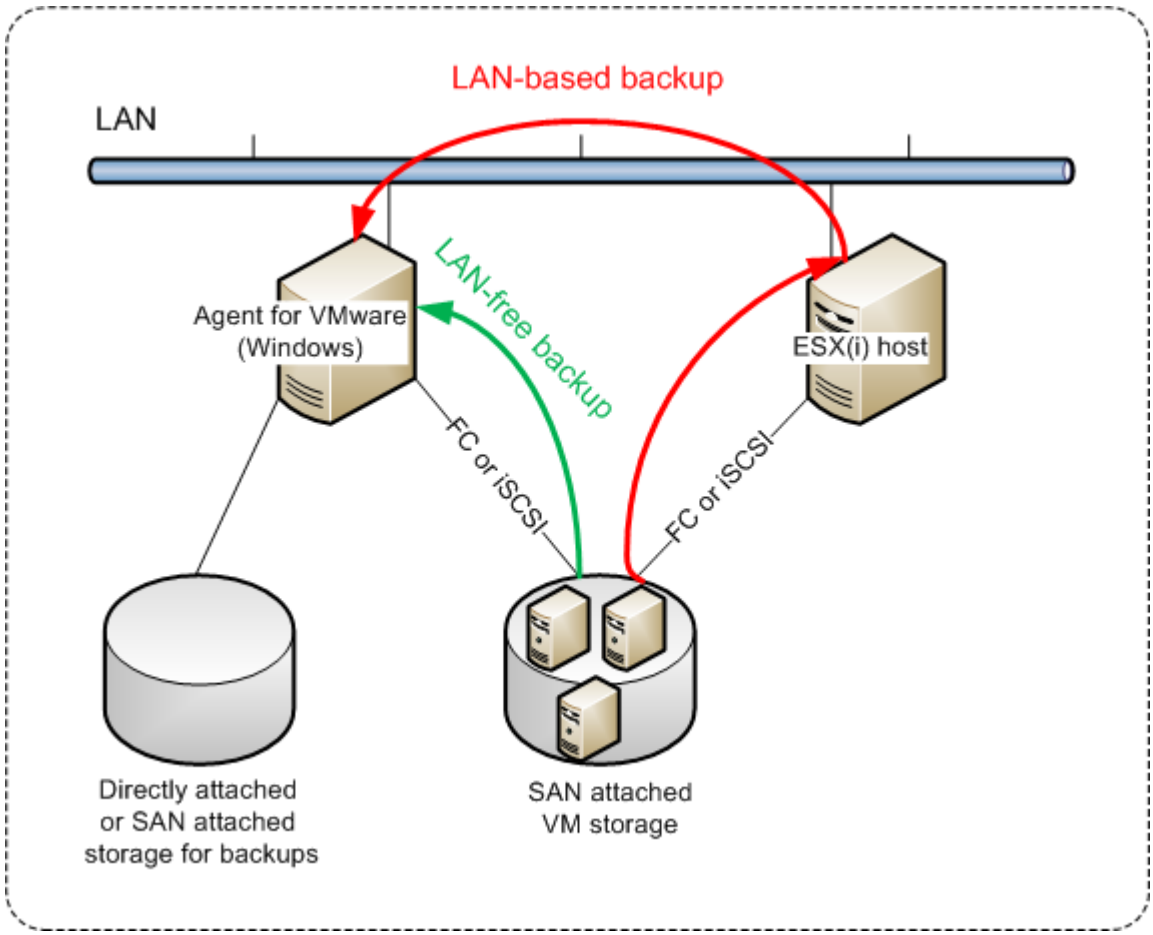
En conséquence, le logiciel continuera à mettre à jour le réplica. Toutes les réplications seront incrémentielles.

Agent pour VMware - Sauvegarde sans réseau local

Si votre ESXi utilise un stockage SAN, installez l'agent sur une machine connectée au même SAN. L'agent sauvegardera les machines virtuelles directement à partir du stockage plutôt que via l'hôte

ESXi et le réseau local. Cette fonctionnalité s'appelle une sauvegarde sans réseau local.

Le diagramme ci-dessous montre une sauvegarde basée sur un réseau local et une sauvegarde sans réseau local. L'accès aux machines virtuelles sans utiliser le réseau local est possible si vous utilisez fibre channel (FC) ou un réseau de zone de stockage iSCSI. Pour éliminer complètement le transfert des données sauvegardées via le LAN, stockez les sauvegardes sur un disque local de la machine de l'agent ou sur un stockage connecté au SAN.



Pour activer l'agent de sorte qu'il puisse accéder directement à un magasin de données

1. Installez l'agent pour VMware sur une machine Windows possédant un accès réseau au vCenter Server.
2. Connectez à la machine le numéro d'unité logique (LUN) qui héberge le magasin de données. Considérez ce qui suit :
   - Utilisez le même protocole (par ex. iSCSI ou FC) que celui utilisé pour connecter le magasin de données au système ESXi.
   - Le LUN *ne doit pas* être initialisé et doit apparaître comme disque « hors ligne » sous **Gestion de disque**. Si Windows initialise le LUN, celui-ci risque d'être corrompu et illisible par VMware vSphere.

Par conséquent, l'agent utilisera le mode de transport SAN pour accéder aux disques virtuels, c'est-à-dire qu'il lira les secteurs LUN bruts via iSCSI/FC sans reconnaître le système de fichiers VMFS (dont Windows n'a pas connaissance).

Limites

- Dans vSphere 6.0 et versions ultérieures, l'agent ne peut pas utiliser le mode de transport SAN si certains des disques VM se trouvent sur un volume VVol (VMware Virtual Volume) et d'autres non. La sauvegarde de telles machines virtuelles échouera.
- Les machines virtuelles chiffrées, introduites dans VMware vSphere 6.5, sont sauvegardées via LAN, même si vous configurez le mode de transport SAN pour l'agent. L'agent revient au transport NBD, car VMware ne prend pas en charge le transport SAN pour la sauvegarde de disques virtuels chiffrés.

Exemple

Si vous utilisez un réseau de zone de stockage (SAN) iSCSI, configurez l'initiateur iSCSI sur la machine Windows où l'agent pour VMware est installé.

Pour configurer la stratégie SAN

1. Connectez-vous en tant qu'administrateur, ouvrez l'invite de commande, saisissez `diskpart`, puis appuyez sur **Entrée**.
2. Saisissez `san`, puis appuyez sur **Entrée**. Assurez-vous que **Stratégie SAN : Tout hors ligne** s'affiche.
3. Si une autre valeur est définie pour la stratégie SAN :
   a. Saisissez `san policy=offlineall`.
   b. Appuyez sur **Entrée**.
   c. Pour vérifier si le paramètre a bien été appliqué, exécutez l'étape 2.
   d. Redémarrez la machine.

Pour configurer un initiateur iSCSI

1. Accédez à **Panneau de configuration** > **Outils administratifs** > **Initiateur iSCSI**.

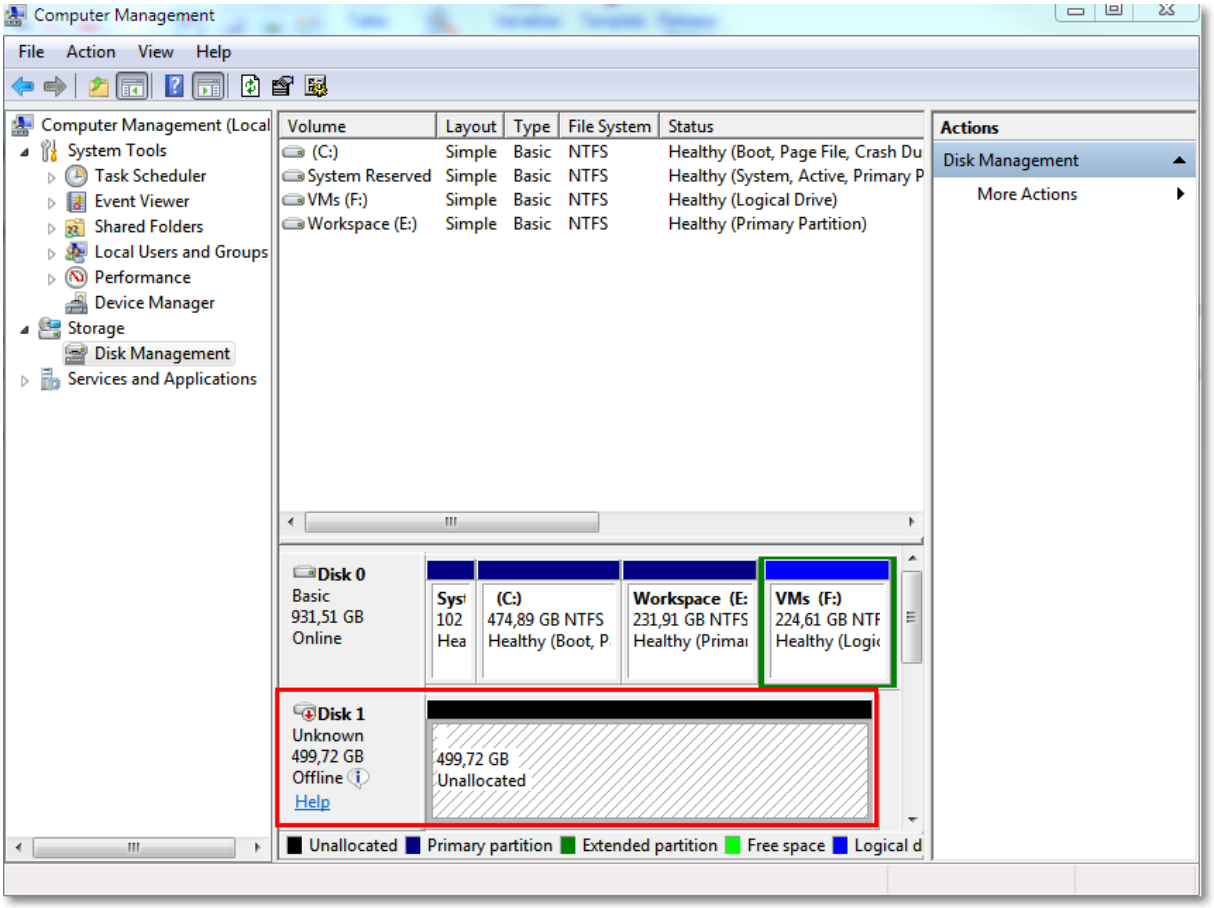
   Remarque
   Pour trouvez l'applet **Outils administratifs**, vous devrez peut-être définir l'affichage du **panneau de configuration** sur autre chose que **Accueil** ou **Catégorie**, ou utiliser la fonction de recherche.

2. Si c'est la première fois que vous lancez l'initiateur Microsoft iSCSI, confirmez votre choix.
3. Sous l'onglet **Cibles**, entrez le nom de domaine complet (FQDN) ou l'adresse IP du périphérique SAN cible, puis cliquez sur **Connexion rapide**.
4. Sélectionnez le LUN qui héberge le magasin de données, puis cliquez sur **Connexion**.

Si le LUN ne s'affiche pas, assurez-vous que la zone de la cible iSCSI permet bien à la machine exécutant l'agent d'accéder au LUN. La machine doit être ajoutée à la liste d'initiateurs iSCSI autorisés sur cette cible.

5. Cliquez sur **OK**.

Le LUN du SAN prêt doit apparaître sous **Gestion de disque**, comme illustré dans la capture d'écran ci-dessous.



Utilisation d'un stockage attaché localement

Vous pouvez connecter un disque supplémentaire à un agent pour VMware (appliance virtuelle) pour que l'agent puisse effectuer des sauvegardes sur ce stockage connecté localement. Cette approche élimine le trafic réseau entre l'agent et l'emplacement de sauvegarde.

Une appliance virtuelle en cours d'exécution sur le même hôte ou cluster avec les machines virtuelles ont un accès direct au(x) magasin(s) de données où se trouvent les machines. Cela signifie que le matériel peut attacher les disques sauvegardés via le transport HotAdd. Par conséquent, le trafic de sauvegarde est dirigé d'un disque local à l'autre. Si le magasin de données est connecté comme **Disque/LUN** plutôt que **NFS**, la sauvegarde sera entièrement sans réseau local. Dans le cas d'un magasin de données NFS, il y aura du trafic réseau entre le magasin de données et l'hôte.

L'utilisation d'un stockage attaché localement présume que l'agent sauvegarde toujours les mêmes machines. Si plusieurs agents travaillent au sein de vSphere, et qu'un ou plusieurs d'entre eux

utilisent des stockages attachés localement, vous devez manuellement lier chaque agent à toutes les machines qu'ils doivent sauvegarder. Autrement, si les machines sont redistribuées parmi les agents par serveur de gestion, les sauvegardes d'une machine pourraient être dispersées dans plusieurs stockages.

Vous pouvez ajouter le stockage à un agent qui fonctionne déjà ou lorsque vous déployez l'agent à partir d'un modèle OVF.

Pour connecter un stockage à un agent qui fonctionne déjà

1. Dans l'inventaire de VMware vSphere, faites un clic droit sur l'agent pour VMware (appliance virtuelle).
2. Ajoutez le disque en modifiant les paramètres de la machine virtuelle. La taille du disque doit être d'au moins 10 Go.

   Avertissement !
   Faites bien attention lorsque vous ajoutez un disque déjà existant. Dès que le stockage est créé, toutes les données précédemment contenues sur ce disque sont perdues.

3. Allez à la console de l'appliance virtuelle. Le lien **Créer un stockage** est disponible au bas de l'écran. S'il ne l'est pas, cliquez sur **Actualiser**.
4. Cliquez sur le lien **Créer un stockage**, sélectionnez le disque et donnez-lui un nom. La longueur du nom est limitée à 16 caractères à cause des limites du système de fichiers.

Pour sélectionner un stockage attaché localement comme une destination de sauvegarde

- Lors de la création d'un plan de protection, dans **Où sauvegarder**, sélectionnez **Dossiers locaux**, puis tapez la lettre correspondant au stockage attaché localement, par exemple, **D:**.

Remarque
Le stockage connecté localement est conçu pour des environnements relativement petits avec un seul agent (appliance virtuelle). Nous avons testé des unités de stockage connecté localement d'une taille maximale de 5 To. Vous pouvez connecter des disques plus volumineux à vos risques et périls, mais de telles configurations ne sont pas prises en charge. Pour plus de 5 To de données de sauvegarde, nous vous recommandons d'utiliser d'autres types de stockage. Par exemple, vous pouvez créer et connecter un disque virtuel VMware à n'importe quelle machine virtuelle et créer un partage réseau sur ce disque, qui sera alors utilisé comme destination de sauvegarde à la place du stockage connecté localement.

Liaison de machine virtuelle

Cette section vous donne un aperçu de la façon dont le service Cyber Protection organise l'opération de plusieurs agents dans VMware vCenter.

L'algorithme de distribution ci-dessous fonctionne à la fois pour les appliances virtuelles et les agents installés dans Windows.

Algorithme de distribution

Les machines virtuelles sont automatiquement distribuées de façon égale entre les Agents pour VMware. Par uniformément, nous voulons dire que chaque agent gère un nombre égal de machines. La quantité d'espace de stockage occupée par une machine virtuelle n'est pas comptée.

Toutefois, lors du choix d'un agent pour une machine, le logiciel essaie d'optimiser les performances générales du système. En particulier, le logiciel considère l'emplacement de l'agent et de la machine virtuelle. Un agent hébergé sur le même hôte est préféré. S'il n'y a aucun agent sur le même hôte, un agent du même cluster est préféré.

Quand une machine virtuelle est assignée à un agent, toutes les sauvegardes de cette machine sont déléguées à cet agent.

Redistribution

La redistribution prend place chaque fois que l'équilibre établi se brise ou, plus précisément, lorsqu'un déséquilibre de charge entre les agents atteint 20 pour cent. Cela peut se produire lorsqu'une machine ou un agent est ajouté ou supprimé, ou qu'une machine migre vers un autre hôte ou cluster, ou si vous liez manuellement une machine à un agent. Si cela se produit, le service Cyber Protection redistribue les machines en utilisant le même algorithme.

Par exemple, vous réalisez que vous avez besoin de plus d'agents pour aider avec le débit et déployez une appliance virtuelle supplémentaire au cluster. Le service Cyber Protection assignera les machines les plus adaptées au nouvel agent. La charge des anciens agents sera réduite.

Lorsque vous supprimez un agent du service Cyber Protection, les machines assignées à l'agent sont distribuées parmi les agents restants. Cependant, cela ne se produira pas si un agent est endommagé ou est supprimé manuellement de vSphere. La redistribution démarrera seulement après que vous ayez supprimé cet agent de l'interface Web.

Affichage du résultat de la distribution

Vous pouvez voir le résultat de la distribution automatique :

- dans la colonne **Agent** pour chaque machine virtuelle dans la section **Tous les terminaux**
- dans la section **machines virtuelles attribuées** du volet **Détails** lorsqu'un agent est sélectionné dans la section **Paramètres** > **Agents**

Liaison manuelle

La liaison de l'Agent pour VMware vous permet d'exclure une machine virtuelle de ce processus de distribution en spécifiant l'agent qui doit toujours sauvegarder cette machine. L'équilibre général sera maintenu, mais cette machine en particulier peut être passée à un agent différent uniquement si l'agent d'origine est supprimé.

Pour lier une machine avec un agent

1. Sélectionnez la machine.
2. Cliquez sur **Détails**.
   Dans la section **Agent attribué**, le logiciel affiche l'agent qui gère actuellement la machine sélectionnée.
3. Cliquez sur **Modifier**.
4. Sélectionnez **Manuel**.
5. Sélectionnez l'agent auquel vous souhaitez lier la machine.
6. Cliquez sur **Enregistrer**.

Pour annuler la liaison d'une machine avec un agent

1. Sélectionnez la machine.
2. Cliquez sur **Détails**.
   Dans la section **Agent attribué**, le logiciel affiche l'agent qui gère actuellement la machine sélectionnée.
3. Cliquez sur **Modifier**.
4. Sélectionnez **Automatique**.
5. Cliquez sur **Enregistrer**.

Désactivation de l'attribution automatique pour un agent

Vous pouvez désactiver l'attribution automatique pour un Agent pour VMware dans le but de l'exclure du processus de distribution en spécifiant la liste des machines que cet agent doit sauvegarder. L'équilibre général sera maintenu entre les autres agents.

L'attribution automatique ne peut pas être désactivée pour un agent s'il n'y a aucun autre agent enregistré, ou si l'attribution automatique est désactivée pour tous les autres agents.

Pour désactiver l'attribution automatique pour un agent

1. Cliquez sur **Paramètres** > **Agents**.
2. Sélectionnez l'Agent pour VMware pour lequel vous souhaitez désactiver l'attribution automatique.
3. Cliquez sur **Détails**.
4. Désactivez le commutateur **Attribution automatique**.

Exemples d'utilisation

- La liaison manuelle est pratique si vous voulez qu'une machine en particulier (de très grande capacité) soit sauvegardée par l'Agent pour VMware (Windows) via fibre channel, tandis que les autres machines sont sauvegardées par des appliances virtuelles.
- Il est nécessaire de lier les MV à un agent si l'agent possède un stockage attaché localement.

- Désactiver l'attribution automatique vous permet de vous assurer qu'une machine en particulier est sauvegardée de façon prévisible selon le calendrier que vous avez spécifié. L'agent qui ne sauvegarde qu'une seule MV ne peut pas se charger de sauvegarder d'autres MV à l'heure planifiée.
- Désactiver l'attribution automatique est utile si vous avez plusieurs hôtes ESXi séparés géographiquement. Si vous désactivez l'attribution automatique puis liez les MV de chaque hôte à l'agent s'exécutant sur le même hôte, vous pouvez vous assurer que l'agent ne sauvegardera jamais aucune machine s'exécutant sur des hôtes ESXi distants, réduisant ainsi le trafic réseau.

Exécution automatique de scripts pre-freeze et post-thaw

Avec VMware Tools, vous pouvez exécuter automatiquement des scripts pre-freeze et post-thaw personnalisés sur des machines virtuelles que vous sauvegardez en mode sans agent. Ainsi, vous pouvez exécuter des scripts de suspension personnalisés et créer des sauvegardes cohérentes avec les applications pour les machines virtuelles qui exécutent des applications compatibles VSS.

Prérequis

Les scripts pre-freeze et post-thaw doivent se trouver dans un dossier spécifique sur la machine virtuelle.

- Pour les machines virtuelles Windows, l'emplacement de ce dossier dépend de la version ESXi de l'hôte.

  Par exemple, pour les machines virtuelles exécutées sur un hôte ESXi 6.5, ce dossier est `C:\Program Files\VMware\VMware Tools\backupScripts.d\`. Vous devez créer le dossier `backupScripts.d` manuellement. N'archivez pas d'autres types de fichiers dans ce dossier, parce que cela pourrait rendre l'outil VMware Tools instable.

  Pour plus d'informations sur l'emplacement des scripts pre-freeze et post-thaw pour d'autres extensions ESXi, reportez-vous à la documentation VMware.
- Pour les machines virtuelles Linux, copiez respectivement vos scripts dans les répertoires `/usr/sbin/pre-freeze-script` et `/usr/sbin/post-thaw-script`. Les scripts sous `/usr/sbin/pre-freeze-script` sont exécutés lorsque vous créez un instantané et ceux sous `/usr/sbin/post-thaw-script` sont exécutés une fois l'instantané terminé. Les scripts doivent pouvoir être exécutés par l'utilisateur de VMware Tools.

Pour exécuter automatiquement des scripts pre-freeze et post-thaw

1. Assurez-vous que VMware Tools est installé sur la machine virtuelle.
2. Sur la machine virtuelle, ajoutez vos scripts personnalisés aux dossiers appropriés.
3. Dans le plan de protection de cette machine, activez l'option **Service de cliché instantané des volumes (VSS) pour les machines virtuelles**.

   Cela crée un instantané VMware avec l'option **Suspendre le système de fichiers invité**, ce qui déclenche à son tour les scripts de pre-freeze et de post-thaw sur la machine virtuelle.

Vous n'avez pas besoin d'exécuter de scripts de suspension sur les machines virtuelles qui exécutent des applications compatibles VSS, telles que Microsoft SQL Server ou Microsoft Exchange.

Pour créer une sauvegarde cohérente avec les applications pour de telles machines, activez l'option **Service de cliché instantané des volumes (VSS) pour les machines virtuelles** dans le plan de protection.

Support pour la migration d'une machine virtuelle

Cette section vous renseigne sur ce qui vous attend lors de la migration de machines virtuelles au sein d'un environnement vSphere, y compris lors de la migration entre des hôtes ESXi appartenant à un cluster vSphere.

vMotion déplace l'état et la configuration d'une machine virtuelle vers un autre hôte alors que les disques de l'ordinateur demeurent dans le même emplacement dans le stockage partagé. Storage vMotion déplace les disques d'une machine virtuelle d'un magasin de données vers un autre.

- La migration avec vMotion, y compris Storage vMotion, n'est pas prise en charge pour une machine virtuelle qui exécute un agent pour VMware (appliance virtuelle) et est automatiquement désactivée. Cette machine virtuelle est ajoutée à la liste **Remplacements de VM** dans la configuration des clusters vSphere.
- Lorsque la sauvegarde d'une machine virtuelle démarre, la migration avec vMotion, y compris Storage vMotion, est automatiquement désactivée. Cette machine virtuelle est temporairement ajoutée à la liste **Remplacements de VM** dans la configuration des clusters vSphere. Une fois la sauvegarde terminée, les paramètres **Remplacements de VM** sont automatiquement rétablis à l'état précédent.
- Il n'est pas possible de lancer la sauvegarde d'une machine virtuelle pendant si sa migration avec vMotion, y compris Storage vMotion, est en cours. La sauvegarde démarrera une fois la migration terminée.

Gestion des environnements de virtualisation

Vous pouvez afficher les environnements vSphere, Hyper-V et Virtuozzo dans leur présentation native. Une fois l'agent correspondant installé et enregistré, l'onglet **VMware**, **Hyper-V** ou **Virtuozzo** apparaît sous **Terminaux**.

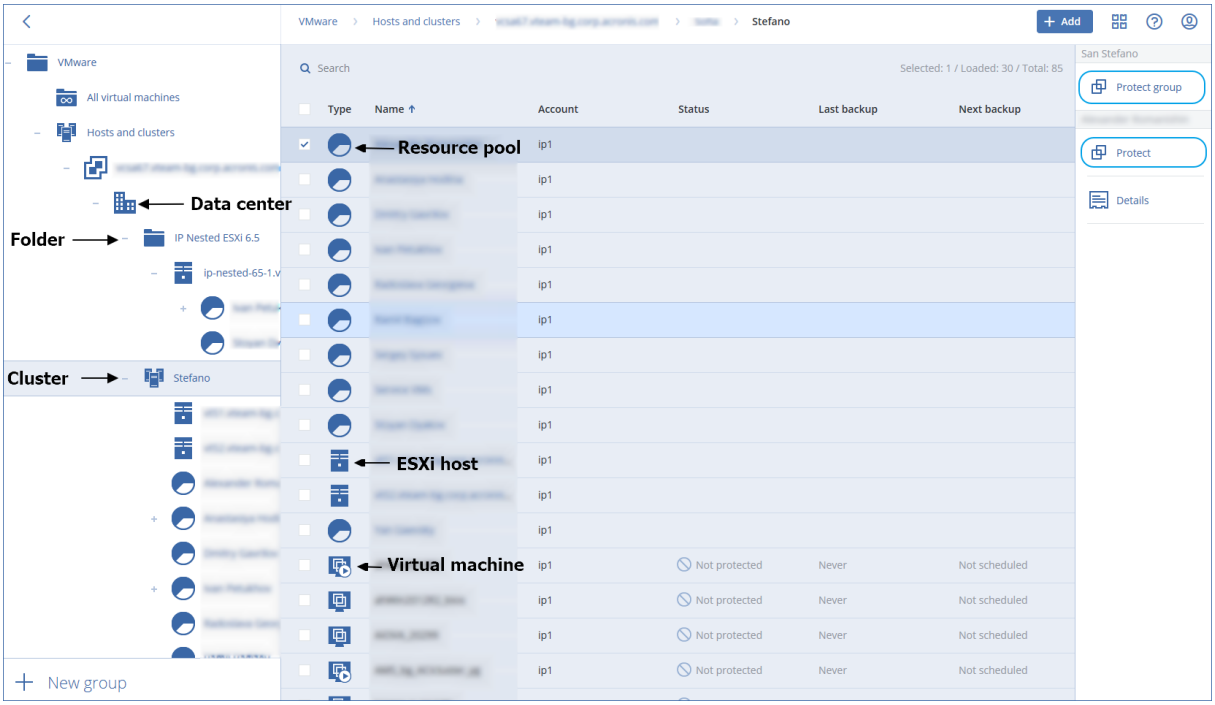
Dans l'onglet **VMware**, vous pouvez sauvegarder les objets d'infrastructure VMware suivants :

- Centre de données
- Dossier
- Cluster
- Hôte ESXi
- Liste des ressources

Chacun de ces objets d'infrastructure fonctionne comme un objet de groupe pour les machines virtuelles. Lorsque vous appliquez un plan de protection à l'un de ces objets de groupe, toutes les machines virtuelles qui y sont incluses seront sauvegardées. Vous pouvez sauvegarder soit les

machines de groupes sélectionnées en cliquant sur **Protection**, soit les machines de groupe parentes dans lesquelles le groupe sélectionné est inclus en cliquant sur **Protéger le groupe**.

Par exemple, vous avez sélectionné le cluster Stefano, puis le pool de ressources qui s'y trouve. Si vous cliquez sur **Protection**, toutes les machines virtuelles incluses dans le pool de ressources sélectionné seront sauvegardées. Si vous cliquez sur **Protéger un groupe**, toutes les machines virtuelles incluses dans le cluster Stefano seront sauvegardées.



L'onglet **VMware** vous permet de modifier les informations d'identification pour le vCenter Server ou l'hôte ESXi autonome sans réinstaller l'agent.

Modification des informations d'identification d'accès au vCenter Server ou à l'hôte ESXi

1. Dans **Terminaux**, cliquez sur **VMware**.
2. Cliquez sur **Hôtes et clusters**.
3. Dans la liste **Hôtes et clusters** (à droite de l'arborescence **Hôtes et clusters**), sélectionnez le vCenter Server ou l'hôte ESXi autonome indiqué lors de l'installation de l'agent pour VMware.
4. Cliquez sur **Détails**.
5. Dans **Informations d'identification**, cliquez sur le nom d'utilisateur.
6. Indiquez les nouvelles informations d'identification, puis cliquez sur **OK**.

Affichage de l'état de la sauvegarde dans vSphere Client

Vous pouvez afficher l'état de la sauvegarde et la dernière heure de sauvegarde d'une machine virtuelle dans vSphere Client.

Cette information apparaît dans le résumé de la machine virtuelle (**Résumé** > **Attributs personnalisés**/**Annotations**/**Remarques**, en fonction du type de client et de la version de

vSphere). Vous pouvez également activer les colonnes **Dernière sauvegarde** et **État de la sauvegarde** sur l'onglet **Machines virtuelles** pour tous les hôtes, centres de données, dossiers, pools de ressources ou le serveur vCenter entier.

Pour fournir ces attributs, l'agent pour VMware doit disposer des privilèges suivants en plus de ceux décrits dans la section « Agent pour VMware - privilèges nécessaires » :

- **Global** > **Gérer les rapports personnalisés**
- **Global** > **Définir un attribut personnalisé**

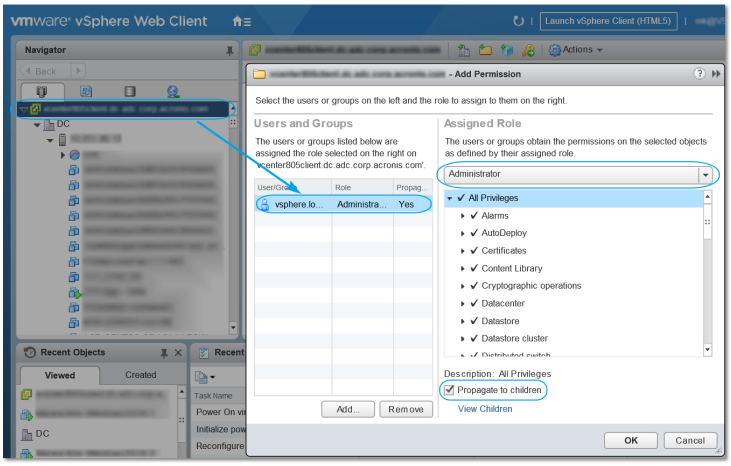
Agent pour VMware – privilèges nécessaires

Pour exécuter une opération avec des objets vCenter, comme les machines virtuelles, les hôtes ESXi, les clusters, vCenter et plus encore, l'agent pour VMware s'authentifie sur vCenter ou l'hôte ESXi à l'aide des identifiants vSphere fournis par un utilisateur. Le compte vSphere utilisé par l'agent pour VMware pour se connecter à vSphere doit disposer des privilèges nécessaires à tous les niveaux de l'infrastructure vSphere, à commencer par le niveau vCenter.

Précisez le compte vSphere disposant des privilèges nécessaires pendant l'installation ou la configuration de l'agent pour VMware. Si vous devez modifier le compte ultérieurement, reportez-vous à la section "Gestion des environnements de virtualisation" (p. 734).

Attribuer des permissions à un utilisateur vSphere au niveau de vCenter

1. Connectez-vous au client Web vSphere.
2. Faites un clic droit sur vCenter, puis cliquez sur **Ajouter une autorisation**.
3. Sélectionnez ou ajoutez un nouvel utilisateur ayant le rôle nécessaire (ce rôle doit inclure toutes les autorisations requises du tableau ci-dessous).
4. Sélectionnez l'option **Propager vers les enfants**.



Objet	Droit	Opération			
		Sauvegarder une MV	Restaurer sur une nouvelle MV	Restaurer sur une MV existante	Exécuter une MV à partir d'une sauvegarde
Opérations de chiffrement (à partir de vSphere 6.5)	**Ajouter un disque**	+*			
	Accès direct	+*			
Magasin de données	**Allouer de l'espace**		+	+	+
	Parcourir le magasin de données				+
	Configurer un magasin de données	+	+	+	+
	Opérations de bas niveau sur les fichiers				+
Global	**Licences**	+	+	+	+
	Désactiver les méthodes	+	+	+	
	Activer les méthodes	+	+	+	
	Gérer les rapports personnalisés	+	+	+	
	Définir un attribut personnalisé	+	+	+	
Hôte > **Configuration**	**Configuration de la partition de stockage**				+
Hôte > **Opérations locales**	**Créer une MV**				+

	Supprimer une MV				+
	Reconfigurer une MV				+
Réseau	**Attribuer un réseau**		+	+	+
Ressource	**Attribuer une MV à un pool de ressources**		+	+	+
Machine virtuelle > **Configuration**	**Ajouter un disque existant**	+	+		+
	Ajouter un nouveau disque		+	+	+
	Ajouter ou supprimer un terminal		+		+
	Advanced	+	+	+	
	Modifier le nombre de processeurs		+		
	Suivi de changement de disque	+		+	
	Location de disque	+		+	
	Mémoire		+		
	Supprimer un disque	+	+	+	+
	Renommer		+		
	Définir une annotation				+
	Param.		+	+	+
Machine virtuelle > **Opérations invité**	**Exécution de programme d'opération invité**	+**			
	Requêtes	+**			

	d'opération invité				
	Modifications des opérations invité	+**			
Machine virtuelle > **Interaction**	**Obtenir le ticket de contrôle invité** (dans vSphere 4.1 et 5.0)				+
	Configurer le support CD		+	+	
	Gestion du système d'exploitation invité par VIX API (dans vSphere 5.1 et versions ultérieures)				+
	Mise hors tension			+	+
	Mettre sous tension		+	+	+
Machine virtuelle > **Inventaire**	**Créer à partir d'une machine existante**		+	+	+
	Créer une nouvelle		+	+	+
	Enregistrer				+
	Supprimer		+	+	+
	Désinscrire				+
Machine virtuelle > **Allocation**	**Autoriser l'accès au disque**		+	+	+
	Autoriser l'accès au disque en lecture seule	+		+	
	Autoriser le téléchargement de machine virtuelle	+	+	+	+
Machine virtuelle > **État Machine**	**Créer un instantané**	+		+	+

virtuelle > **Gestion des instantanés** (vSphere 6.5 et versions ultérieures)					
	Supprimer l'instantané	+		+	+
vApp	**Ajouter une machine virtuelle**				+

* Ce droit est uniquement obligatoire pour les sauvegardes de machines chiffrées.

** Ce droit est uniquement obligatoire pour les sauvegardes reconnaissant les applications.

Sauvegarde de machines Hyper-V en cluster.

Dans un cluster Hyper-V, les machines virtuelles peuvent migrer entre les nœuds cluster. Suivez ces recommandations pour configurer une sauvegarde correcte de machines Hyper-V en cluster :

1. Une machine doit être disponible pour la sauvegarde quel que soit le nœud sur lequel elle migre. Pour garantir que l'agent pour Hyper-V puisse accéder à une machine sur n'importe quel nœud, le service de l'agent doit être exécuté sous un compte utilisateur de domaine qui dispose de privilèges administratifs sur chacun des nœuds cluster.
   Nous vous conseillons de spécifier un tel compte pour le service de l'agent pendant l'installation de l'agent pour Hyper-V.
2. Installez l'agent pour Hyper-V sur chaque nœud du cluster.
3. Enregistrez tous les agents dans le service Cyber Protection.

Haute disponibilité d'une machine restaurée

Lorsque vous restaurez des disques sauvegardés vers une machine virtuelle Hyper-V *existante*, la propriété de haute disponibilité de la machine reste inchangée.

Lorsque vous récupérez des disques sauvegardés sur une *nouvelle* machine virtuelle Hyper-V, la machine résultante n'est pas hautement disponible. Elle est considéré comme une machine de rechange et est normalement désactivée. Si vous devez utiliser la machine dans l'environnement de production, vous pouvez la configurer pour la haute disponibilité à partir du composant logiciel enfichable **Gestion du cluster de basculement**.

Limite le nombre total de machines virtuelles sauvegardées simultanément.

Dans l'option de sauvegarde **Planification**, vous pouvez limiter le nombre de machines virtuelles sauvegardées simultanément par plan de protection.

Lorsqu'un agent exécute plusieurs plans simultanément, le nombre de machines sauvegardées simultanément s'incrémente. Cela peut avoir une incidence sur les performances de sauvegarde et surcharger aussi bien l'hébergeur que le stockage de la machine virtuelle. Vous pouvez éviter ces problèmes en configurant une limite au niveau de l'agent.

Pour limiter le nombre de sauvegardes simultanées au niveau de l'agent

Agent pour VMware (Windows)

1. Sur l'ordinateur avec l'agent, créez un nouveau document texte et ouvrez-le dans un éditeur de texte.
2. Copiez et collez les lignes suivantes dans le fichier.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Remplacez `00000001` par la valeur hexadécimale de la limite que vous souhaitez définir.
   Par exemple, `00000001` est 1 et `0000000A` est 10.
4. Enregistrez le document sous **limit.reg**.
5. Exécutez le fichier en tant qu'administrateur.
6. Confirmez que vous souhaitez modifier le registre Windows.
7. Redémarrez l'agent.
   a. Dans le menu **Démarrer**, cliquez sur **Exécuter**.
   b. Saisissez **cmd**, puis cliquez sur **OK**.
   c. Dans la ligne de commande, exécutez les commandes suivantes :

```
net stop mms
net start mms
```

Agent pour Hyper-V

1. Sur l'ordinateur avec l'agent, créez un nouveau document texte et ouvrez-le dans un éditeur de texte.
2. Copiez et collez les lignes suivantes dans le fichier.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Remplacez `00000001` par la valeur hexadécimale de la limite que vous souhaitez définir.
   Par exemple, `00000001` est 1 et `0000000A` est 10.

4. Enregistrez le document sous **limit.reg**.
5. Exécutez le fichier en tant qu'administrateur.
6. Confirmez que vous souhaitez modifier le registre Windows.
7. Redémarrez l'agent.
   a. Dans le menu **Démarrer**, cliquez sur **Exécuter**.
   b. Saisissez **cmd**, puis cliquez sur **OK**.
   c. Dans la ligne de commande, exécutez les commandes suivantes :

```
net stop mms
net start mms
```

Appliances virtuelles

Cette procédure s'applique aux agents pour VMware (appliance virtuelle), pour Scale Computing, pour Virtuozzo Hybrid Infrastructure et pour oVirt.

1. Dans la console de l'appliance virtuelle, appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.
2. Ouvrez le fichier `/etc/Acronis/MMS.config` dans un éditeur de texte.
3. Localisez la section suivante :

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Remplacez `10` par le nombre maximal de sauvegardes simultanées que vous souhaitez définir.
5. Enregistrez le fichier.
6. Redémarrez l'agent en exécutant la commande `reboot`.

Migration de machine

Vous pouvez effectuer une migration de machine en restaurant sa sauvegarde sur une machine autre que celle d'origine.

Le tableau suivant résume les options de migration disponibles.

Type de machine sauvegardée	Destinations de restauration disponibles

	Machine physique	Machine virtuelle ESXi	Machine virtuelle Hyper-V	Virtuozzo		Machine virtuelle Virtuozzo Hybrid Infrastructure	Machine virtuelle Scale Computing HC3	Machine virtuelle RHV/oVirt
				Machine virtuelle	Conteneur			
Machine physique	+	+	+	-	-	+	+*	+
Machine virtuelle VMware ESXi	+	+	+	-	-	+	+*	+
Machine virtuelle Hyper-V	+	+	+	-	-	+	+*	+
Machine virtuelle Virtuozzo	+	+	+	+	-	+	+*	+
Conteneur Virtuozzo	-	-	-	-	+	-	-	-
Machine virtuelle Virtuozzo Hybrid Infrastructure	+	+	+	-	-	+	+*	+
Machine virtuelle Scale Computing HC3	+	+	+	-	-	+	+	+
Machine virtuelle Red Hat Virtualization/oVirt	+	+	+	-	-	+	+*	+

*Si Secure Boot est activé sur la machine source, la machine virtuelle restaurée ne peut plus démarrer, sauf si vous désactivez Secure Boot dans la console de la machine virtuelle après la reprise.

Remarque
Vous ne pouvez pas restaurer des machines virtuelles macOS sur des hôtes Hyper-V, car Hyper-V ne prend pas en charge macOS. Vous pouvez restaurer des machines virtuelles macOS sur un hôte VMware installé sur un matériel Mac.

Pour en savoir plus sur les opérations de migration, consultez les rubriques suivantes :

- Pour la migration physique à virtuelle, voir "Machine physique à virtuelle" (p. 525).
- Pour la migration virtuelle à virtuelle, voir "Restauration d'une machine virtuelleVous pouvez restaurer des machines virtuelles avec leurs sauvegardes.Vous ne pouvez pas restaurer les sauvegardes dans la console Cyber Protect pour les tenants en mode Conformité. Pour plus d'informations sur la restauration de ces sauvegardes, voir "Restauration de sauvegardes pour les tenants en mode Conformité" (p. 1).PrérequisLors de la restauration sur cette machine, vous devez arrêter la machine virtuelle. Par défaut, le logiciel stoppe la machine sans invite. Une fois la restauration terminée, vous devrez redémarrer manuellement la machine. Vous pouvez modifier ce comportement par défaut à l'aide de l'option de restauration de gestion de l'alimentation de MV (cliquez sur Options de récupération > Gestion de l'alimentation de MV).ProcédureEffectuez l'une des actions suivantes :Sélectionnez une machine sauvegardée, cliquez sur Restauration, puis sélectionnez un point de restauration.Sélectionnez un point de récupération dans l'onglet Stockage de sauvegarde.Cliquez sur Restaurer > Toute la machine.Si vous souhaitez effectuer la restauration vers une machine physique, sélectionnez Machine physique dans Restaurer vers. Sinon, ignorez cette étape.La restauration vers une machine physique est uniquement possible si la configuration de disque de la machine cible correspondant exactement à celle de la sauvegarde.Dans ce cas, poursuivez avec l’étape 4 dans « Machine physique ». Sinon, nous vous recommandons d’effectuer une migration V2P à l’aide d’un support de démarrage.[Facultatif] Par défaut, le logiciel sélectionne automatiquement la machine d'origine comme machine cible. Pour effectuer la restauration vers une autre machine virtuelle, cliquez sur Machine cible, puis procédez comme suit :Sélectionnez l'hyperviseur (VMware ESXi, Hyper-V, Virtuozzo Virtuozzo Hybrid Infrastructure, Scale Computing HC3 ou oVirt).Seules les machines virtuelles Virtuozzo peuvent être restaurées sur Virtuozzo. Pour plus d'informations sur la migration V2V, consultez « Migration de machine ».Sélectionnez si vous souhaitez restaurer sur une machine nouvelle ou existante.Sélectionnez l'hôte et spécifiez le nouveau nom de machine ou sélectionnez une machine cible existante.Cliquez sur OK.Configurez les options de récupération supplémentaires dont vous avez besoin.[Non disponible pour Virtuozzo Hybrid Infrastructure et Scale Computing HC3] Pour sélectionner le magasin de données pour la machine virtuelle, cliquez sur Magasin de données pour ESXi, Chemin d'accès pour Hyper-V et Virtuozzo, ou Domaine de stockage pour Red Hat Virtualization (oVirt), puis sélectionnez le magasin de données (stockage) pour la machine virtuelle.Pour afficher le magasin de données (stockage), l'interface et le mode de provisionnement de chaque disque virtuel, cliquez sur Mappage de disque. Vous pouvez modifier ces paramètres, à moins que vous ne restauriez un conteneur Virtuozzo ou une machine virtuelle de Virtuozzo Hybrid Infrastructure.Pour Virtuozzo Hybrid Infrastructure, vous pouvez uniquement sélectionner la stratégie de stockage pour les disques de destination. Pour cela, sélectionnez le disque de destination souhaité, puis cliquez sur Modifier. Dans la lame qui

s'ouvre, cliquez sur l'icône en forme d'engrenage, sélectionnez la stratégie de stockage, puis cliquez sur Terminé.La section Mappage permet également de choisir les disques individuels à restaurer.[Disponible pour VMware ESXi, Hyper-V et Virtuozzo] Cliquez sur Paramètres de MV pour modifier la taille de mémoire, le nombre de processeurs et les connexions réseau de la machine virtuelle.[Pour Virtuozzo Hybrid Infrastructure] Cliquez sur Variété pour modifier la taille de mémoire et le nombre de processeurs ou les connexions réseau de la machine virtuelle.[Disponible uniquement pour les ordinateurs Windows sur lesquels un agent de protection est installé] Activez le curseur Restauration sûre afin de vous assurer que les données restaurées sont exemptes de malware. Pour plus d'informations sur le fonctionnement de la restauration sécurisée, voir "Restauration sûre" (p. 1).Cliquez sur Démarrer la récupération.Lors de la restauration sur une machine virtuelle existante, confirmez que vous souhaitez écraser les disques.La progression de la restauration sont affichées dans l'onglet Activités." (p. 1).

- Pour la migration virtuelle à physique, voir "Restauration d'une machine virtuelleVous pouvez restaurer des machines virtuelles avec leurs sauvegardes.Vous ne pouvez pas restaurer les sauvegardes dans la console Cyber Protect pour les tenants en mode Conformité. Pour plus d'informations sur la restauration de ces sauvegardes, voir "Restauration de sauvegardes pour les tenants en mode Conformité" (p. 1).PrérequisLors de la restauration sur cette machine, vous devez arrêter la machine virtuelle. Par défaut, le logiciel stoppe la machine sans invite. Une fois la restauration terminée, vous devrez redémarrer manuellement la machine. Vous pouvez modifier ce comportement par défaut à l'aide de l'option de restauration de gestion de l'alimentation de MV (cliquez sur Options de récupération > Gestion de l'alimentation de MV).ProcédureEffectuez l'une des actions suivantes :Sélectionnez une machine sauvegardée, cliquez sur Restauration, puis sélectionnez un point de restauration.Sélectionnez un point de récupération dans l'onglet Stockage de sauvegarde.Cliquez sur Restaurer > Toute la machine.Si vous souhaitez effectuer la restauration vers une machine physique, sélectionnez Machine physique dans Restaurer vers. Sinon, ignorez cette étape.La restauration vers une machine physique est uniquement possible si la configuration de disque de la machine cible correspondant exactement à celle de la sauvegarde.Dans ce cas, poursuivez avec l’étape 4 dans « Machine physique ». Sinon, nous vous recommandons d’effectuer une migration V2P à l’aide d’un support de démarrage.[Facultatif] Par défaut, le logiciel sélectionne automatiquement la machine d'origine comme machine cible. Pour effectuer la restauration vers une autre machine virtuelle, cliquez sur Machine cible, puis procédez comme suit :Sélectionnez l'hyperviseur (VMware ESXi, Hyper-V, Virtuozzo Virtuozzo Hybrid Infrastructure, Scale Computing HC3 ou oVirt).Seules les machines virtuelles Virtuozzo peuvent être restaurées sur Virtuozzo. Pour plus d'informations sur la migration V2V, consultez « Migration de machine ».Sélectionnez si vous souhaitez restaurer sur une machine nouvelle ou existante.Sélectionnez l'hôte et spécifiez le nouveau nom de machine ou sélectionnez une machine cible existante.Cliquez sur OK.Configurez les options de récupération supplémentaires dont vous avez besoin.[Non disponible pour Virtuozzo Hybrid Infrastructure et Scale Computing HC3] Pour sélectionner le magasin de données pour la machine virtuelle, cliquez sur Magasin de données pour ESXi, Chemin d'accès pour Hyper-V et Virtuozzo, ou Domaine de stockage pour Red Hat Virtualization (oVirt), puis sélectionnez le magasin de données (stockage) pour la machine virtuelle.Pour afficher le magasin de données (stockage), l'interface et le mode de provisionnement de chaque disque virtuel, cliquez sur Mappage de disque. Vous pouvez

modifier ces paramètres, à moins que vous ne restauriez un conteneur Virtuozzo ou une machine virtuelle de Virtuozzo Hybrid Infrastructure.Pour Virtuozzo Hybrid Infrastructure, vous pouvez uniquement sélectionner la stratégie de stockage pour les disques de destination. Pour cela, sélectionnez le disque de destination souhaité, puis cliquez sur Modifier. Dans la lame qui s'ouvre, cliquez sur l'icône en forme d'engrenage, sélectionnez la stratégie de stockage, puis cliquez sur Terminé.La section Mappage permet également de choisir les disques individuels à restaurer.[Disponible pour VMware ESXi, Hyper-V et Virtuozzo] Cliquez sur Paramètres de MV pour modifier la taille de mémoire, le nombre de processeurs et les connexions réseau de la machine virtuelle.[Pour Virtuozzo Hybrid Infrastructure] Cliquez sur Variété pour modifier la taille de mémoire et le nombre de processeurs ou les connexions réseau de la machine virtuelle.[Disponible uniquement pour les ordinateurs Windows sur lesquels un agent de protection est installé] Activez le curseur Restauration sûre afin de vous assurer que les données restaurées sont exemptes de malware. Pour plus d'informations sur le fonctionnement de la restauration sécurisée, voir "Restauration sûre" (p. 1).Cliquez sur Démarrer la récupération.Lors de la restauration sur une machine virtuelle existante, confirmez que vous souhaitez écraser les disques.La progression de la restauration sont affichées dans l'onglet Activités." (p. 1) et "Restauration de disques via un support de démarrage" (p. 530).

Migration par l'intermédiaire d'un support de démarrage

En remplacement de la migration d'ordinateurs que vous effectuez dans la console Cyber Protect, vous pouvez restaurer un ordinateur à l'aide d'un support de démarrage.

Nous vous recommandons d'utiliser un support de démarrage dans les cas suivants :

- Exécution d'une migration non prise en charge de manière native.
  Par exemple, utilisez un support de démarrage pour restaurer une machine physique ou une machine virtuelle non-Virtuozzo en tant que machine virtuelle Virtuozzo sur un hôte Virtuozzo.
- Exécution de la migration d'une machine Linux contenant des volumes logiques.
  Utilisez l'agent pour Linux ou un support de démarrage pour créer la sauvegarde, puis employez un support de démarrage pour restaurer la sauvegarde.
- Fourniture de pilotes pour du matériel spécifique, essentiel pour la capacité de démarrage du système.
  Concevez un support de démarrage qui peut utiliser les lecteurs requis. Pour plus d'informations, voir "Bootable Media Builder" (p. 749).

Machines virtuelles Microsoft Azure et Amazon EC2

Pour sauvegarder une machine virtuelle Microsoft Azure ou Amazon EC2, installez un agent de protection sur la machine. Les opérations de sauvegarde et de restauration sont les mêmes que pour une machine physique. La machine est toutefois considérée comme une machine virtuelle lorsque vous définissez les quotas pour le nombre de machines.

Par rapport aux machines physiques, les machines virtuelles Microsoft Azure et Amazon EC2 ne peuvent pas être démarrées à partir de supports de démarrage. Si vous souhaitez effectuer une

restauration vers une nouvelle machine virtuelle Microsoft Azure ou Amazon EC2, suivez la procédure ci-dessous.

Remarque
La procédure de reprise suivante s'applique uniquement aux sauvegardes d'ordinateurs contenant tous les pilotes nécessaires pour s'exécuter dans Microsoft Azure de manière native (sauvegardes créées d'une machine virtuelle Azure, ordinateur Hyper-V local ou machine source Windows Server 2016 et versions ultérieures). Pour la reprise inter-plate-forme, consultez cet article de la base de connaissances.

Pour restaurer une machine en tant que machine virtuelle Microsoft Azure ou Amazon EC2

1. Créez une nouvelle machine virtuelle à partir d'une image/d'un modèle dans Microsoft Azure ou Amazon EC2. La nouvelle machine doit avoir la même configuration de disque que la machine que vous souhaitez restaurer.
2. Installez l'agent pour Windows ou l'agent pour Linux sur la nouvelle machine.
3. Restaurez la machine sauvegardée, comme décrit dans « Machine physique ». Lorsque vous configurez la restauration, sélectionnez la nouvelle machine en tant que machine cible.

Création d'un support de démarrage afin de restaurer des systèmes d'exploitation

Un support de démarrage est un support physique (CD, DVD, lecteur flash USB ou autre support amovible) qui vous permet d'exécuter l'agent de protection dans un environnement Linux, WinPE (Windows Preinstallation Environment) ou WinRE (Windows Recovery Environment), sans l'aide d'un système d'exploitation. La fonction première d'un support de démarrage est de restaurer les systèmes d'exploitation qui ne démarrent pas.

Remarque
Le support de démarrage n'est pas compatible avec les lecteurs hybrides.

Support de démarrage personnalisé ou tout prêt ?

Avec Bootable Media Builder, vous pouvez créer un support de démarrage personnalisé (basé sur Linux ou WinPE) pour ordinateurs Windows, Linux ou macOS. Dans votre support de démarrage personnalisé basé sur Linux ou WinPE/WinRE, vous pouvez configurer des paramètres supplémentaires, comme l'enregistrement automatique, les paramètres réseau ou les paramètres de serveur proxy. Dans les supports de démarrage personnalisés basés sur WinPE/WinRE, vous pouvez aussi ajouter des pilotes supplémentaires.

Si vous préférez, vous pouvez aussi télécharger un support de démarrage tout prêt (basé sur Linux uniquement). Le support de démarrage tout prêt ne peut être utilisé que pour les opérations de récupération et l'accès à la fonctionnalité Universal Restore.

Support de démarrage basé sur Linux ou sur WinPE/WinRE ?

Basé sur Linux

Un support de démarrage basé sur Linux contient un agent de protection basé sur un noyau Linux. L'agent peut démarrer et réaliser des opérations sur n'importe quel matériel compatible PC, y compris un système vierge et des machines avec des systèmes de fichiers corrompus ou incompatibles.

Basé sur WinPE/WinRE

Un support de démarrage basé sur WinPE contient un système Windows minimal appelé Windows Preinstallation Environment (WinPE) et un plug-in Cyber Protection pour WinPE, qui est une modification de l'agent de protection qui peut être exécutée dans l'environnement de préinstallation. Un support de démarrage basé sur WinRE utilise Windows Recovery Environment et ne nécessite pas l'installation de paquets Windows supplémentaires.

WinPE se révèle être la solution de démarrage la plus pratique dans les grands environnements avec un matériel hétérogène.

Avantages :

- L'utilisation de Cyber Protection dans Windows Preinstallation Environment offre plus de fonctionnalités que l'utilisation d'un support de démarrage basé sur un environnement Linux. Après avoir démarré un matériel compatible PC sous WinPE, vous pouvez non seulement utiliser l'agent de protection, mais aussi les commandes et scripts de l'environnement de préinstallation (PE), ainsi que les autres plug-ins que vous y avez ajoutés.
- Un support de démarrage PE aide à résoudre certains problèmes de support de démarrage liés à un environnement Linux tels que la prise en charge de certains contrôleurs RAID ou certains niveaux de piles RAID seulement. Un support basé sur WinPE 2.x ou ultérieur permet le chargement dynamique des pilotes des périphériques nécessaires.

Limites :

- Un support de démarrage basé sur une version de WinPE antérieure à 4.0 ne peut pas démarrer sur des machines qui utilisent le Unified Extensible Firmware Interface (UEFI).

Création d'un support de démarrage physique

Nous vous recommandons vivement de créer un support de démarrage et de le tester dès que vous commencez à utiliser une sauvegarde de niveau disque. En outre, il est également recommandé de recréer le support à chaque nouvelle mise à jour importante de l'agent de protection.

Vous pouvez restaurer Windows et Linux à partir du même support. Pour restaurer macOS, créez un support à part à partir d'une machine sous macOS.

Pour créer un support de démarrage physique sous Windows ou Linux

1. Créez un fichier ISO de support de démarrage personnalisé ou téléchargez le fichier ISO tout prêt.

   Pour créer un fichier ISO personnalisé, utilisez "Bootable Media Builder" (p. 749).

   Pour télécharger le fichier ISO tout prêt, accédez à la console Cyber Protect, sélectionnez un ordinateur, puis cliquez sur **Restaurer** > **Autres méthodes de restauration...** > **Télécharger l'image ISO**.
2. [Facultatif] Dans la console Cyber Protect, générez un jeton d'enregistrement. Le jeton d'enregistrement s'affiche automatiquement lorsque vous téléchargez un fichier ISO tout prêt.

   Ce jeton permet au support de démarrage d'accéder au stockage Cloud, sans vous demander de saisir d'identifiant ni de mot de passe.
3. Créez un support de démarrage physique de l'une des manières suivantes :
   - Gravez le fichier ISO sur un CD/DVD.
   - Créez un lecteur flash USB de démarrage avec le fichier ISO et l'un des outils gratuits disponibles en ligne.

     Utilisez `ISO vers USB` ou `RUFUS` pour démarrer une machine UEFI et `Win32DiskImager` pour une machine BIOS. Sous Linux, l'utilisation de la commande `dd` est toute indiquée.

   Pour les machines virtuelles, vous pouvez connecter le fichier ISO en tant que lecteur CD/DVD à la machine virtuelle que vous souhaitez restaurer.

Pour créer un support de démarrage physique sous macOS

1. Sur les machines où l'agent pour Mac est installé, cliquez sur **Applications** > **Rescue Media Builder**.
2. Le logiciel affiche les supports amovibles connectés. Sélectionnez celui que vous désirez utiliser.

   Avertissement !
   Toutes les données sur le disque seront effacées.

3. Cliquez sur **Créer**.
4. Patientez pendant que le logiciel crée le support de démarrage.

Bootable Media Builder

Bootable Media Builder permet de créer des supports de démarrage. Il est installé sous la forme d'un composant optionnel sur l'ordinateur sur lequel l'agent de protection est installé.

Pourquoi utiliser Bootable Media Builder ?

Le support de démarrage tout prêt et disponible au téléchargement dans la console Cyber Protect se base sur un noyau Linux. Contrairement à Windows PE, il ne permet pas d'implanter des pilotes personnalisés à la volée.

Bootable Media Builder vous permet de créer des images de support de démarrage personnalisées basées sur Linux ou WinPE.

32 bits ou 64 bits ?

Bootable Media Builder crée un support de démarrage avec des composants 32 bits et 64 bits. Dans la plupart des cas, vous avez besoin d'un support 64 bits pour démarrer une machine qui utilise l'interface UEFI (Unified Extensible Firmware Interface).

Support de démarrage basé sur un environnement Linux

Pour créer un support de démarrage basé sur Linux

1. Démarrez **Bootable Media Builder**.
2. Dans **Type de support de démarrage**, sélectionnez **Défaut (support basé sur Linux)**.
3. Sélectionnez la manière dont les volumes et les ressources réseau seront représentés :
   - Un support de démarrage avec une représentation de volume de type Linux affiche les volumes comme suit : hda1 et sdb2, par exemple. Il essaye de reconstruire les périphériques MD et les volumes logiques (LVM) avant de démarrer une restauration.
   - Un support de démarrage avec une représentation de volume de type Windows affiche les volumes comme suit : C: et D:, par exemple. Il permet d'accéder aux volumes dynamiques (LDM).
4. [Facultatif] Spécifiez les paramètres du noyau Linux. Séparez des paramètres multiples par des espaces.

   Par exemple, pour pouvoir sélectionner un mode d'affichage pour l'agent de démarrage chaque fois que le support démarre, saisissez : **vga=ask**. Pour plus d'informations sur les paramètres disponibles, reportez-vous à "Paramètres du noyau" (p. 751).
5. [Facultatif] Sélectionnez la langue du support de démarrage.
6. [Facultatif] Sélectionnez le mode de démarrage (BIOS ou UEFI) que Windows utilisera après la restauration.
7. Sélectionnez le composant à placer sur le support : l'agent de démarrage Cyber Protection.
8. [Facultatif] Spécifiez l'intervalle d'arrêt pour le menu de démarrage. Si ce paramètre n'est pas configuré, le chargeur attendra que vous choisissiez quoi démarrer entre le système d'exploitation (s'il est présent) ou le composant.
9. [Facultatif] Si vous souhaitez automatiser les opérations de l'agent de démarrage, cochez la case **Utiliser le script suivant**. Sélectionnez ensuite l'un des scripts et définissez les paramètres du script. Pour plus d'informations sur les scripts, reportez-vous à "Scripts sur un support de démarrage" (p. 753).
10. [Facultatif] Sélectionnez le mode d'enregistrement du support de démarrage dans le service Cyber Protection lors du démarrage. Pour plus d'informations sur les paramètres d'enregistrement, reportez-vous à "Enregistrement du support de démarrage" (p. 762).
11. Spécifiez les paramètres réseau des adaptateurs réseau de l'ordinateur démarré ou gardez la configuration DHCP automatique.
12. [Facultatif] Si un serveur proxy est activé sur votre réseau, spécifiez son nom d'hôte/adresse IP et le port.

13. Sélectionnez le type de fichier du support de démarrage :
    - Image ISO
    - Fichier ZIP
14. Spécifiez un nom de fichier pour le fichier de support de démarrage.
15. Vérifiez vos paramètres sur l'écran Résumé et cliquez sur **Continuer**.

Paramètres du noyau

Vous pouvez spécifier un ou plusieurs paramètres du noyau Linux qui seront automatiquement appliqués au lancement du support de démarrage. Ces paramètres sont généralement utilisés en cas de problème d'utilisation du support de démarrage. Normalement, vous pouvez laisser ce champ vide.

Vous pouvez également spécifier n'importe lequel de ces paramètres en appuyant sur F11 dans le menu de démarrage.

Paramètres

Lorsque vous spécifiez plusieurs paramètres, séparez-les avec des espaces.

- **acpi=off**
  Désactive ACPI (Advanced Configuration and Power Interface). Vous pouvez utiliser ce paramètre lorsque vous rencontrez un problème avec une configuration matérielle spécifique.
- **noapic**
  Désactive APIC (Advanced Programmable Interrupt Controller). Vous pouvez utiliser ce paramètre lorsque vous rencontrez un problème avec une configuration matérielle spécifique.
- **vga=ask**
  Invite à spécifier le mode vidéo que doit utiliser l'interface graphique utilisateur du support de démarrage. Sans le paramètre **vga**, le mode vidéo est détecté automatiquement.
- **vga=** *mode_number*
  Spécifie le mode vidéo à utiliser dans l'interface utilisateur graphique du support de démarrage. Le numéro de mode est donné par *mode_number* sous forme hexadécimale, par exemple : **vga=0x318**
  La résolution de l'écran et le nombre de couleurs correspondant à un numéro de mode peuvent être différents sur des ordinateurs différents. Nous vous recommandons de commencer par utiliser le paramètre **vga=ask** afin de choisir une valeur pour *numéro_mode*.
- **quiet**
  Désactive l'affichage des messages de démarrage quand le noyau Linux est en cours de chargement, et démarre la console d'administration dès que le noyau est chargé.
  Ce paramètre est implicitement spécifié lors de la création du support de démarrage, mais vous pouvez le supprimer dans le menu de démarrage.

Si ce paramètre est supprimé, tous les messages de démarrage s'affichent, suivis d'une invite de commandes. Pour démarrer la console de gestion à partir de l'invite de commandes, exécutez la commande suivante : **/bin/product**

- **nousb**

  Désactive le chargement du sous-système USB (Universal Serial Bus).
- **nousb2**

  Désactive la prise en charge USB 2.0. Ce paramètre n'affecte pas le fonctionnement des périphériques USB 1.1. Ce paramètre vous permet d'utiliser certains lecteurs USB en mode USB 1.1 s'ils ne fonctionnent pas en mode USB 2.0.
- **nodma**

  Désactive l'accès direct à la mémoire (DMA) pour tous les disques durs IDE. Empêche le noyau de se figer pour certains matériels.
- **nofw**

  Désactive la prise en charge de l'interface FireWire (IEEE1394).
- **nopcmcia**

  Désactive la détection du matériel PCMCIA.
- **nomouse**

  Désactive la prise en charge de la souris.
- *module_name* **=off**

  Désactive le module dont le nom est donné par *module_name*. Par exemple, pour désactiver l'utilisation du module SATA, saisissez : **sata_sis=off**
- **pci=bios**

  Force l'utilisation du BIOS PCI au lieu d'accéder directement au terminal matériel. Vous pouvez utiliser ce paramètre si la machine possède un pont d'hôte PCI non standard.
- **pci=nobios**

  Désactive l'utilisation du BIOS PCI. Seules les méthodes d'accès direct au matériel seront autorisées. Vous pouvez utiliser ce paramètre quand le support de démarrage ne démarre pas, ce qui peut être causé par le BIOS.
- **pci=biosirq**

  Utilise des appels BIOS PCI pour obtenir la table de routage d'interruptions Vous pouvez utiliser ce paramètre si le noyau ne parvient pas à allouer les requêtes d'interruption (IRQ) ou à découvrir les bus PCI secondaires sur la carte-mère.

  Il se peut que ces appels ne fonctionnent pas correctement sur certaines machines. Mais ceci pourrait être la seule façon d'obtenir la table de routage d'interruptions.
- **STRUCTURES=en-US, de-DE, fr-FR, ...**

  Spécifie la structure du clavier qui peut être utilisée dans l'interface utilisateur graphique du support de démarrage.

  Sans ce paramètre, seules deux structures peuvent être utilisées : Anglais (USA) et la structure correspondant à la langue sélectionnée dans le menu de démarrage de votre support.

  Vous pouvez indiquer l'une des structures suivantes :

  Belge : **be-BE**

Tchèque : **cz-CZ**
Anglais : **en-GB**
Anglais (USA) : **en-US**
Français : **fr-FR**
Français (Suisse) : **fr-CH**
Allemand : **de-DE**
Allemand (Suisse) : **de-CH**
Italien : **it-IT**
Polonais : **pl-PL**
Portugais : **pt-PT**
Portugais (Brésil) : **pt-BR**
Russe : **ru-RU**
Serbe (cyrillique) : **sr-CR**
Serbe (latin) : **sr-LT**
Espagnol : **es-ES**
En cas d'utilisation avec le support de démarrage, utilisez CTRL + SHIFT pour parcourir les structures disponibles.

Scripts sur un support de démarrage

Si vous voulez que le support de démarrage exécute un ensemble prédéfini d'opérations, vous pouvez spécifier un script lors de la création du support avec Bootable Media Builder. Ainsi, chaque fois qu'un ordinateur démarrera à partir du support, le script spécifié sera exécuté et l'interface utilisateur ne s'affichera pas.

Vous pouvez sélectionner l'un des scripts prédéfinis ou créer un script personnalisé en suivant les conventions de script.

Scripts prédéfinis

Le support de démarrage fournit les scripts prédéfinis suivants :

- Restauration du stockage dans le Cloud (**entire_pc_cloud**)
- Restauration depuis un partage réseau (**entire_pc_share**)

Les scripts se trouvent dans les répertoires suivants sur l'ordinateur où Bootable Media Builder est installé :

- Sous Windows : %**ProgramData%\Acronis\MediaBuilder\scripts**
- Sous Linux : **/var/lib/Acronis/MediaBuilder/scripts/**

Restauration du stockage Cloud

Dans le support de démarrage, spécifiez les paramètres de script suivants :

1. Le nom du fichier de sauvegarde.
2. [Facultatif] Un mot de passe que le script utilisera pour accéder aux sauvegardes chiffrées.

Restauration depuis un partage réseau

Dans le support de démarrage, spécifiez les paramètres de script suivants :

- Le chemin d'accès au partage réseau.
- Les nom d'utilisateur et mot de passe du partage réseau.
- Le nom du fichier de sauvegarde. Pour trouver le nom du fichier de sauvegarde :
  a. Dans la console Cyber Protect, accédez à **Stockage de sauvegarde** > **Emplacements**.
  b. Sélectionnez le partage réseau (cliquez sur **Ajouter un emplacement** si le partage n'est pas répertorié).
  c. Sélectionnez la sauvegarde.
  d. Cliquez sur **Détails**. Le nom du fichier s'affiche sous **Nom de fichier de la sauvegarde**.
- [Facultatif] Un mot de passe que le script utilisera pour accéder aux sauvegardes chiffrées.

Scripts personnalisés

Important
La création de scripts personnalisés requiert la connaissance du langage de commande Bash et de JavaScript Object Notation (JSON). Si vous ne connaissez pas Bash, il existe un bon site pour le découvrir : http://www.tldp.org/LDP/abs/html. La spécification JSON est disponible à l'adresse http://www.json.org

Fichiers d'un script

Votre Un script doit se trouver dans les répertoires suivants sur la machine où Bootable Media Builder est installé :

- Sous Windows : %**ProgramData%\Acronis\MediaBuilder\scripts**
- Sous Linux : **/var/lib/Acronis/MediaBuilder/scripts/**

Le script doit être composé d'au moins trois fichiers :

- **<script_file>.sh** : fichier avec votre script Bash. Lors de la création du script, utilisez uniquement un ensemble limité de commandes, que vous trouverez à l'adresse : https://busybox.net/downloads/BusyBox.html. Les commandes suivantes peuvent également être utilisées :
  - `acrocmd` : utilitaire de ligne de commande pour la sauvegarde et la restauration
  - `product` : commande qui lance l'interface utilisateur du support de démarrage

Ce fichier et tous les fichiers supplémentaires inclus dans le script (par exemple, en utilisant la commande dot) doivent être situés dans le sous-dossier **bin**. Dans ce script, indiquez les chemins de fichier supplémentaires sous la forme **/ConfigurationFiles/bin/<some_file>**.

- **autostart** : fichier pour démarrer **<script_file>.sh**. Le contenu du fichier doit être comme suit :

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** : fichier JSON contenant les éléments suivants :
  - Nom et description du script à afficher dans Bootable Media Builder.
  - Noms des variables de script à configurer via Bootable Media Builder.
  - Paramètres des contrôles qui seront affichés dans le support de démarrage pour chaque variable.

Structure d'autostart.json

Objet Toplevel

Paire		Requis	Description
Nom	**Type de valeur**		
`displayName`	string	Oui	Nom du script affiché dans le support de démarrage.
`description`	string	Non	Description du script affiché dans le support de démarrage.
`timeout`	number	Non	Délai d'expiration (en secondes) pour le menu de démarrage avant de lancer le script. Si la paire n'est pas indiquée, le délai d'expiration sera de dix secondes.
`variables`	objet	Non	Toute variable pour **<script_file>.sh** que vous voulez configurer via le support de démarrage. La valeur doit être un ensemble des paires suivantes : l'identificateur de chaîne d'une variable et l'objet de la variable (voir tableau ci-dessous).

Objet de variable

Paire		Requis	Description
Nom	**Type de valeur**		
`displayName`	string	Oui	Nom de variable utilisé dans **<script_file>.sh**.
`type`	string	Oui	Type de contrôle affiché dans le support de démarrage. Ce contrôle est utilisé pour configurer la valeur de la variable. Pour connaître tous les types pris en charge, consultez le tableau ci-dessous.
`description`	string	Oui	Étiquette de contrôle affichée au-dessus du contrôle dans le support de démarrage.
`default`	chaîne si `type` est `string`, `multiString`, `password` ou `enum` nombre si `type` est `number`, `spinner` ou `checkbox`	Non	Valeur par défaut du contrôle. Si la paire n'est pas indiquée, la valeur par défaut sera une chaîne vide ou un zéro en fonction du type de contrôle. La valeur par défaut d'une case à cocher peut être `0` (l'état effacé) ou `1` (l'état sélectionné).
`order`	number (non négatif)	Oui	Ordre de contrôle dans le support de démarrage. Plus la valeur est élevée, plus le contrôle est placé bas par rapport aux autres contrôles définis dans **autostart.json**. La valeur initiale doit être `0`.
`min` (pour `spinner` uniquement)	number	Non	Valeur minimale de la toupie dans une zone de sélection numérique. Si la paire n'est pas indiquée, la valeur sera `0`.
`max` (pour `spinner` uniquement)	number	Non	Valeur minimale de la toupie dans une zone de sélection numérique. Si la paire n'est pas indiquée, la valeur sera `100`.
`étape` (pour `spinner` uniquement)	number	Non	Valeur de pas de la toupie dans une zone de sélection numérique. Si la paire n'est pas indiquée, la valeur sera `1`.
`items`	grappe de	Oui	Valeurs d'une liste déroulante.

(pour `enum` uniquement)	chaînes		
`required` (pour `string`, `multiString`, `password` et `enum`)	number	Non	Indique si la valeur de contrôle peut être vide (`0`) ou non (`1`). Si la paire n'est pas indiquée, la valeur de contrôle peut être vide.

Type de contrôle

Nom	Description
`string`	Zone de texte sans contrainte d'une seule ligne, utilisée pour saisir ou modifier des chaînes courtes.
`multiString`	Zone de texte sans contrainte de plusieurs lignes, utilisée pour saisir ou modifier des chaînes longues.
`password`	Zone de texte sans contrainte d'une seule ligne, utilisée pour saisir des mots de passe en toute sécurité.
`number`	Zone de texte numérique uniquement et d'une seule ligne, utilisée pour saisir ou modifier des nombres.
`spinner`	Zone de texte numérique uniquement et d'une seule ligne, utilisée pour saisir ou modifier des nombres, avec une toupie. Également appelée zone de sélection numérique.
`enum`	Liste déroulante standard, avec un ensemble fixe de valeurs prédéterminées.
`checkbox`	Case à cocher avec deux états : l'état effacé ou l'état sélectionné.

L'échantillon **autostart.json** ci-dessous contient tous les types possibles de contrôle pouvant être utilisés pour configurer des variables pour **<script_file>.sh**.

```
{
        "displayName": "Autostart script name",
        "description": "This is an autostart script description.",
        "variables": {
                "var_string": {
                        "displayName": "VAR_STRING",
                        "type": "string", "order": 1,
                        "description": "This is a 'string' control:", "default": "Hello,
world!"
```

```
},
"var_multistring": {
        "displayName": "VAR_MULTISTRING",
        "type": "multiString", "order": 2,
        "description": "This is a 'multiString' control:",
        "default": "Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
},
"var_number": {
        "displayName": "VAR_NUMBER",
        "type": "number", "order": 3,
        "description": "This is a 'number' control:", "default": 10
},
"var_spinner": {
        "displayName": "VAR_SPINNER",
        "type": "spinner", "order": 4,
        "description": "This is a 'spinner' control:",
        "min": 1, "max": 10, "step": 1, "default": 5
},
"var_enum": {
        "displayName": "VAR_ENUM",
        "type": "enum", "order": 5,
        "description": "This is an 'enum' control:",
        "items": ["first", "second", "third"], "default": "second"
},
"var_password": {
        "displayName": "VAR_PASSWORD",
        "type": "password", "order": 6,
        "description": "This is a 'password' control:", "default": "qwe"
},
"var_checkbox": {
        "displayName": "VAR_CHECKBOX",
```

```
                    "type": "checkbox", "order": 7,
                    "description": "This is a 'checkbox' control", "default": 1
                }
        }
}
```

Support de démarrage basé sur WinPE et WinRE

Vous pouvez créer des images WinRE sans préparation supplémentaire, ou créer des images WinPE après avoir installé le kit d'installation automatisée Windows (AIK) ou le kit de déploiement et d'évaluation Windows (ADK).

Images WinRE

La création d'images WinRE est prise en charge pour les systèmes d'exploitation suivants :

- Windows 7 (64 bits)
- Windows 8 (32 bits et 64 bits)
- Windows 8.1 (32 bits et 64 bits)
- Windows 10 (32 bits et 64 bits)
- Windows 11 (64 bits)
- Windows Server 2012 (64 bits)
- Windows Server 2016 (64 bits)
- Windows Server 2019 (64 bits)
- Windows Server 2022 (64 bits)

Images WinPE

Après l'installation du kit d'installation automatisée Windows (AIK) ou du kit de déploiement et d'évaluation Windows (ADK), Bootable Media Builder prend en charge les distributions WinPE qui sont basées sur n'importe lequel des noyaux suivants :

- Windows Vista (PE 2.0)
- Windows Vista SP1 et Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0) avec ou sans le supplément pour Windows 7 SP1 (PE 3.1)
- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)
- Windows 10 (PE 10.0.1xxx)
- Windows 11 (PE 10.0.2xxx)

Bootable Media Builder prend en charge les distributions WinPE 32 bits et 64 bits. Les distributions WinPE 32 bits peuvent également fonctionner sur un matériel 64 bits. Cependant, vous avez besoin d'une distribution 64 bits pour démarrer une machine qui utilise le Unified Extensible Firmware Interface (UEFI).

Remarque
Les images PE basées sur WinPE 4 et versions plus récentes nécessitent environ 1 Go de RAM pour fonctionner.

Création d'un support de démarrage WinPE ou WinRE

Bootable Media Builder offre deux méthodes pour intégrer Cyber Protection avec WinPE et WinRE :

- Création d'un fichier ISO avec le plug-in Cyber Protection à partir de zéro.
- Ajout du plug-in Cyber Protection à un fichier WIM pour n'importe quel usage ultérieur (création manuelle d'ISO, ajout d'autres outils à l'image et ainsi de suite).

Pour créer un support de démarrage WinPE ou WinRE

1. Sur l'ordinateur sur lequel l'agent de protection est installé, exécutez Bootable Media Builder.
2. Dans **Bootable media type**, sélectionnez **Windows PE** ou **Windows PE (64-bit)**. Un support 64 bits est nécessaire pour démarrer une machine qui utilise l'interface micrologicielle extensible unifiée (Unified Extensible Firmware Interface) (UEFI).
3. Sélectionnez le sous-type du support de démarrage : **WinRE** ou **WinPE**.
   La création d'un support de démarrage WinRE ne nécessite l'installation d'aucun paquet supplémentaire.
   Pour créer un support WinPE 64 bits, vous devez télécharger le kit d'installation automatisée Windows (AIK) ou le kit de déploiement et d'évaluation Windows (ADK). Pour créer un support WinPE 32 bits, en plus de télécharger le kit AIK ou ADK, vous devez procéder comme suit :
   a. Cliquez sur **Télécharger le plug-in pour WinPE (32 bits)**.
   b. Enregistrez le plug-in à l'emplacement **%PROGRAM_ FILES%\BackupClient\BootableComponents\WinPE32**.
4. [Facultatif] Sélectionnez la langue du support de démarrage.
5. [Facultatif] Sélectionnez le mode de démarrage (BIOS ou UEFI) que Windows utilisera après la restauration.
6. Spécifiez les paramètres réseau des adaptateurs réseau de l'ordinateur démarré ou gardez la configuration DHCP automatique.
7. [Facultatif] Sélectionnez le mode d'enregistrement du support de démarrage dans le service Cyber Protection lors du démarrage. Pour plus d'informations sur les paramètres d'enregistrement, reportez-vous à "Enregistrement du support de démarrage" (p. 762).
8. [Facultatif] Spécifiez les pilotes Windows à ajouter au support de démarrage.
   Après avoir démarré un ordinateur avec Windows PE ou Windows RE, les pilotes peuvent vous aider à accéder au terminal où se trouve la sauvegarde. Ajoutez les pilotes 32 bits si vous utilisez

une distribution WinPE ou WinRE 32 bits ou les pilotes 64 bits si vous utilisez une distribution WinPE ou WinRE 64 bits.

Pour ajouter des pilotes :

- Cliquez sur **Ajouter**, puis spécifiez le chemin d'accès au fichier .inf nécessaire pour un terminal SCSI, un disque RAID, un contrôleur SATA, une carte réseau, un lecteur de bandes ou un autre terminal.
- Répétez cette procédure pour chaque pilote que vous souhaitez inclure dans le support WinPE ou WinRE obtenu.

9. Sélectionnez le type de fichier du support de démarrage :
   - Image ISO
   - Image WIM
10. Indiquez le chemin complet au fichier image obtenu, y compris le nom de fichier.
11. Vérifiez vos paramètres sur l'écran Résumé et cliquez sur **Continuer**.

Pour créer une image PE (fichier ISO) à partir du fichier WIM obtenu

- Remplacez le fichier boot.wim par défaut dans votre dossier Windows PE par le fichier WIM nouvellement créé. Pour l'exemple ci-dessus, saisissez :

```
copy c:\RecoveryWIMMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- Utiliser l'outil **Oscdimg**. Pour l'exemple ci-dessus, saisissez :

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso
```

Avertissement !
Ne pas copier/coller cet exemple. Pour qu'elle fonctionne, saisissez manuellement la commande.

Préparation : WinPE 2.x et 3.x

Pour pouvoir créer ou modifier des images PE 2.x ou 3.x, installez Bootable Media Builder et Windows Automated Installation Kit (AIK) sur le même ordinateur.

Pour préparer un ordinateur

1. Téléchargez le fichier image AIK à partir du site Web de Microsoft, comme suit :
   - Pour Windows Vista (PE 2.0) : https://www.microsoft.com/en-us/download/details.aspx?id=10333
   - Pour Windows Vista SP1 et Windows Server 2008 (PE 2.1) : https://www.microsoft.com/fr-fr/download/details.aspx?id=9085
   - Pour Windows 7 (PE 3.0) : https://www.microsoft.com/fr-fr/download/details.aspx?id=5753

     Pour Windows 7 SP1 (PE 3.1), vous avez également besoin du supplément AIK disponible à l'adresse https://www.microsoft.com/fr-fr/download/details.aspx?id=5188.
2. Gravez le fichier image sur un disque DVD ou une clé USB.

3. À partir du fichier image, installez les éléments suivants :
   - Microsoft .NET Framework (NETFXx86 ou NETFXx64, en fonction de votre matériel)
   - MSXML (analyseur XML de Microsoft)
   - Windows AIK
4. Installez Bootable Media Builder sur la même machine.

Préparation : WinPE 4.0 et versions ultérieures

Pour pouvoir créer ou modifier des images PE 4 ou ultérieures, installez Bootable Media Builder et Windows Assessment and Deployment Kit (ADK) sur le même ordinateur.

Pour préparer un ordinateur

1. Téléchargez le programme d'installation ADK à partir du site Web de Microsoft.
   Les versions suivantes de Windows sont prises en charge :
   - Windows 11 (PE 10.0.2xxx)
   - Windows 10 (PE 10.0.1xxx)
   - Windows 8.1 (PE 5.0)
   - Windows 8 (PE 4.0)
2. Installez le kit d'évaluation et de déploiement.
3. Installez Bootable Media Builder.

Enregistrement du support de démarrage

L'enregistrement du support de démarrage auprès du service Cyber Protection vous permet d'accéder au stockage dans le Cloud pour vos sauvegardes. Vous pouvez préconfigurer l'enregistrement lors de la création du support de démarrage. Si l'enregistrement n'est pas préconfiguré, vous pouvez enregistrer le support après l'avoir utilisé pour démarrer un ordinateur.

Pour préconfigurer l'enregistrement auprès du service Cyber Protection

1. Dans Bootable Media Builder, accédez à **Enregistrement du support de démarrage**.
2. Dans **URL du service**, spécifiez l'adresse du service Cyber Protection.
3. [Facultatif] Dans **Nom affiché**, spécifiez un nom pour l'ordinateur démarré.
4. Pour définir l'enregistrement automatique dans le service Cyber Protection, cochez la case **Enregistrer automatiquement le support de démarrage**, puis sélectionnez le niveau d'enregistrement automatique :
   - **Demander le jeton d'enregistrement lors du démarrage**
     Le jeton doit être fourni chaque fois qu'un ordinateur démarre à partir de ce support de démarrage.
   - **Utiliser le jeton suivant**

L'ordinateur est enregistré automatiquement lorsqu'il démarre à partir du support de démarrage.

Pour enregistrer le support de démarrage après l'avoir utilisé pour démarrer un ordinateur

1. Démarrez la machine à partir du support de démarrage.
2. Dans la fenêtre de démarrage, cliquez sur **Enregistrer le support**.
3. Dans **Serveur**, spécifiez l'adresse du service Cyber Protection.
4. Dans **Jeton d'enregistrement**, saisissez le jeton d'enregistrement.
5. Cliquez sur **Enregistrer**.

Paramètres réseau

Lors de la création d'un support de démarrage, vous pouvez préconfigurer les connexions réseau qui seront utilisées par l'agent de démarrage. Les paramètres suivants peuvent être préconfigurés :

- Adresse IP
- Masque de sous-réseau
- Passerelle
- Serveur DNS
- Serveur WINS

Une fois que l'agent de démarrage a démarré sur un ordinateur, sa configuration est appliquée sur la carte réseau (Network Interface Card - NIC) de l'ordinateur. Si les paramètres n'ont pas été préconfigurés, l'agent utilise la configuration automatique DHCP.

Vous pouvez aussi configurer les paramètres réseau manuellement lorsque l'agent de démarrage est en cours d'exécution sur l'ordinateur.

Préconfiguration de plusieurs connexions réseau

Vous pouvez préconfigurer les paramètres TCP/IP pour dix cartes réseau au maximum. Pour vous assurer que les paramètres appropriés seront affectés à chaque NIC, créez le support sur le serveur pour lequel le support est personnalisé. Lorsque vous sélectionnez une carte réseau existante dans la fenêtre de l'assistant, ses paramètres sont sélectionnés et enregistrés sur le support. L'adresse MAC de chaque NIC existante est également enregistrée sur le support.

Vous pouvez modifier les paramètres, sauf l'adresse MAC, ou configurer les paramètres pour une carte réseau inexistante.

Une fois que l'agent de démarrage a démarré sur le serveur, il récupère la liste des cartes réseau disponibles. La liste est classée en fonction du logement occupé par les cartes réseau : la plus proche du processeur est en haut.

L'agent de démarrage affecte les paramètres appropriés à chaque carte réseau connue, et identifie les cartes réseau par leur adresse MAC. Une fois que les cartes réseau ayant une adresse MAC

connue sont configurées, les paramètres que vous avez créés pour les cartes réseau inexistantes sont affectés aux cartes réseau restantes en commençant par la carte réseau la plus haute.

Vous pouvez personnaliser le support de démarrage pour n'importe quel ordinateur, et pas seulement pour l'ordinateur sur lequel le support est créé. Pour cela, configurez les NIC en fonction de l'ordre de leur case sur cette machine : NIC1 occupe le logement le plus proche du processeur, NIC2 est dans le logement suivant et ainsi de suite. Lorsque l'agent de démarrage démarrera sur cet ordinateur, il ne trouvera pas de carte réseau ayant une adresse MAC connue et il configurera les cartes réseau dans le même ordre que vous l'avez fait précédemment.

Exemple

L'agent de démarrage pourrait utiliser l'un des adaptateurs réseau pour la communication avec la console de gestion au travers du réseau de production. Une configuration automatique peut être effectuée pour cette connexion. Une quantité assez importante de données à restaurer peut être transférée à travers la seconde carte réseau, incluse dans le réseau de sauvegarde dédié au moyen de paramètres TCP/IP statiques.

Connexion à un ordinateur démarré à partir d'un support de démarrage

Connexion locale

Pour travailler directement sur la machine démarrée à partir du support de démarrage, cliquez sur **Gérer cette machine localement** dans la fenêtre de démarrage.

Quand un ordinateur est démarré à partir d'un support de démarrage, le terminal de l'ordinateur affiche une fenêtre système avec les adresses IP obtenues à partir de DHCP ou configurées à partir de valeurs préétablies.

Configuration des paramètres réseau

Pour modifier les paramètres réseau pour une session en cours, cliquez sur **Configurer le réseau** dans la fenêtre de démarrage. La fenêtre **Paramètres réseau** vous permet de configurer les paramètres réseau pour chaque carte réseau (NIC) de l'ordinateur.

Les modifications apportées pendant une session seront perdues après le redémarrage de l'ordinateur.

Ajout de VLAN

Dans la fenêtre **Paramètres réseau**, vous pouvez ajouter des réseaux locaux virtuels (VLAN). Utilisez cette fonctionnalité si vous devez accéder à un emplacement de sauvegarde qui est inclus dans un VLAN spécifique.

Les VLAN sont principalement utilisés pour diviser un réseau local en plusieurs segments. Une carte d'interface réseau qui est connectée à un port *d'accès* du commutateur a toujours accès au VLAN spécifié dans la configuration du port. Une carte réseau connectée à un port en mode *trunk* du

commutateur peut accéder aux VLAN autorisés dans la configuration du port uniquement si vous spécifiez les VLAN dans les paramètres réseau.

Pour activer l'accès à un VLAN via un port en mode trunk

1. Cliquez sur **Ajouter un VLAN**.
2. Sélectionnez la carte réseau qui donne accès au réseau local qui inclut le VLAN requis.
3. Spécifiez l'identificateur du VLAN.

Après avoir cliqué sur **OK**, une nouvelle entrée apparaît dans la liste des cartes réseau.

Si vous devez supprimer un VLAN, cliquez sur l'entrée VLAN, puis cliquez sur **Supprimer le VLAN**.

Opérations locales avec support de démarrage

Les opérations avec le support de démarrage sont semblables aux opérations de récupération exécutées sur un système d'exploitation en cours d'exécution. Les différences sont les suivantes :

1. Sous un support de démarrage avec représentation des volumes de type Windows, un volume a la même lettre de lecteur que sous Windows. Pour les volumes qui n'ont pas de lettre de lecteur sous Windows (comme le volume System Reserved), des lettres sont affectées librement dans leur ordre séquentiel sur le disque.
   Si le support de démarrage ne peut pas détecter Windows sur l'ordinateur ou s'il en détecte plusieurs, tous les volumes, y compris ceux sans lettre de lecteur, reçoivent une lettre dans leur ordre de séquence sur le disque. Par conséquent, les lettres des volumes peuvent différer de celles affichées dans Windows. Par exemple, le lecteur D: sous le support de démarrage peut correspondre au lecteur E: dans Windows.

   Remarque
   Il est conseillé d'assigner des noms uniques aux volumes.

2. Le support de démarrage avec une représentation des volumes de type Linux affiche les disques et volumes locaux comme n'étant pas montés (sda1, sda2...).
3. Les tâches ne peuvent pas être planifiées. Si vous devez répéter une opération, configurez-la de toutes pièces.
4. La durée de vie du journal est limitée à la durée de la session actuelle. Vous pouvez enregistrer le journal entier ou les entrées de journal filtrées dans un fichier.

Définition d'un mode d'affichage

Lorsque vous démarrez un ordinateur à partir d'un support de démarrage Linux, un mode d'affichage vidéo est détecté automatiquement en fonction de la configuration matérielle (spécifications du moniteur et de la carte graphique). Si le mode d'affichage vidéo est incorrectement détecté, procédez comme suit :

1. Lors de l'affichage du menu de démarrage, appuyez sur F11.
2. Dans l'interface de ligne de commande, saisissez **vga=ask**, puis continuez le démarrage.
3. Choisissez le mode vidéo approprié pris en charge à partir de la liste en entrant son numéro (**318**, par exemple), puis appuyez sur **Entrée**.

Si vous ne souhaitez pas suivre cette procédure à chaque démarrage d'une configuration matérielle donnée, recréez le support de démarrage avec le numéro de mode approprié (dans notre exemple, **vga=0x318**) spécifié dans le champ **Paramètres du noyau**.

Reprise avec support de démarrage sur site

1. Démarrez votre ordinateur à partir du support de démarrage.
2. Cliquez sur **Gérer cette machine localement**.
3. Cliquez sur **Restaurer**.
4. Dans **Quoi restaurer**, cliquez sur **Sélectionner les données**.
5. Sélectionnez le fichier de sauvegarde à restaurer.
6. Dans le volet inférieur gauche, sélectionnez les lecteurs/volumes (ou fichiers/dossiers) que vous souhaitez restaurer, puis cliquez sur **OK**.
7. Configurez les règles d'écrasement.
8. Configurez les exclusions de récupération.
9. Configurez les options de récupération.
10. Vérifiez que les paramètres sont corrects, puis cliquez sur **OK**.

Opérations à distance avec un support de démarrage

Remarque
Cette fonctionnalité est disponible avec le pack Advanced Backup.

Pour voir le support de démarrage dans la console Cyber Protect, vous devez d'abord l'enregistrer en suivant les indications de "Enregistrement du support de démarrage" (p. 762).

Une fois le support enregistré dans la console Cyber Protect, il apparaît dans l'onglet **Terminaux** > **Support de démarrage**. Un support de démarrage disparaît de cet onglet lorsqu'il est hors ligne depuis plus de 30 jours.

Vous pouvez gérer le support de démarrage à distance dans la console Cyber Protect. Par exemple, vous pouvez restaurer des données, redémarrer ou arrêter l'ordinateur démarré avec le support, ou encore afficher des informations, des activités et des alertes concernant le support.

Important
Vous ne pouvez pas mettre à jour le support de démarrage à distance, depuis l'onglet **Paramètres** > **Agents** de la console Cyber Protect.

Pour mettre à jour le support de démarrage, créez-en un nouveau en suivant les indications de la section "Bootable Media Builder" (p. 749). Vous pouvez également télécharger le support tout prêt en cliquant sur l'icône de votre compte, puis sur **Téléchargements** > **Support de démarrage** dans la console Cyber Protect.

Pour restaurer à distance des fichiers ou des dossiers à l'aide d'un support de démarrage

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Support de démarrage**.
1. Sélectionnez le support que vous souhaitez utiliser pour la restauration de données.
2. Cliquez sur **Restauration**.
3. Sélectionnez l'emplacement, puis la sauvegarde dont vous avez besoin. Vous remarquerez que les sauvegardes sont filtrées en fonction de leur emplacement.
4. Sélectionnez le point de reprise, puis cliquez sur **Restaurer des fichiers/dossiers**.
5. Accédez au dossier requis ou servez-vous de la barre de recherche pour obtenir la liste des fichiers et dossiers requis.
   La recherche ne dépend pas de la langue.
   Vous pouvez utiliser un ou plusieurs caractères génériques (* et ?). Pour plus de détails sur l'utilisation de caractères génériques, voir "Filtres de fichiers (Inclusions/Exclusions)" (p. 481).
6. Cliquez sur les fichiers que vous souhaitez restaurer, puis sur **Restaurer**.
7. Dans **Chemin d'accès**, sélectionnez la destination de la restauration.
8. [Facultatif] Pour définir la configuration avancée de la reprise, cliquez sur **Options de restauration**. Pour obtenir plus d'informations, consultez l'article "Options de restauration" (p. 543).
9. Cliquez sur **Démarrer la récupération**.
10. Sélectionnez l'une des options d'écrasement de fichier :
    - **Écraser les fichiers existants**
    - **Écraser un fichier existant s'il est plus ancien**
    - **Ne pas écraser les fichiers existants**

    Choisissez si vous souhaitez redémarrer automatiquement la machine.
11. Cliquez sur **Poursuivre** pour lancer la reprise. La progression de la restauration sont affichées dans l'onglet **Activités**.

Pour restaurer à distance des disques, volumes, ou ordinateurs complets à l'aide d'un support de démarrage

1. Dans l'onglet **Terminaux**, accédez au groupe **Support de démarrage**, puis sélectionnez le support que vous souhaitez utiliser pour la restauration de données.

2. Cliquez sur **Restauration**.
3. Sélectionnez l'emplacement, puis la sauvegarde dont vous avez besoin. Vous remarquerez que les sauvegardes sont filtrées en fonction de leur emplacement.
4. Sélectionnez le point de reprise, puis cliquez sur **Restaurer** > **Toute la machine**.

   Si nécessaire, configurez la machine cible et le mappage de volume en suivant les indications de "Restauration de machines physiquesCette section décrit la restauration des machines physiques via l'interface Web.Utilisez un support de démarrage plutôt que l'interface Web pour restaurer :Un ordinateur fonctionnant sous macOSUn ordinateur d'un tenant en mode ConformitéTout système d'exploitation de manière complète ou sur une machine hors ligneLa structure des volumes logiques (volumes créés par Logical Volume Manager sous Linux). Le support vous permet de recréer automatiquement la structure des volumes logique.Vous ne pouvez pas restaurer les sauvegarde de disque d'ordinateurs Mac Intel sur des Mac utilisant des puces silicone Apple, et inversement. Vous pouvez restaurer des fichiers et des dossiers.Restauration avec redémarrageLa restauration d'un système d'exploitation et de volumes chiffrés avec BitLocker nécessite un redémarrage. Vous pouvez choisir de redémarrer automatiquement la machine ou de lui attribuer le statut Intervention nécessaire. Le système d'exploitation restauré est automatiquement mis en ligne.Les volumes chiffrés et sauvegardés sont restaurés comme volumes non chiffrés.La reprise des volumes chiffrés par BitLocker nécessite la présence sur la même machine d'un volume non chiffré disposant d'au moins 1 Go d'espace disponible. Si aucune de ces conditions n'est remplie, la reprise échoue.La reprise d'un volume système chiffré ne requiert aucune action supplémentaire. Pour restaurer un volume non-système chiffré, vous devez d'abord le verrouiller, par exemple en ouvrant un fichier qui y réside. Dans le cas contraire, la reprise se poursuit sans redémarrage et le volume récupéré risque de ne pas être reconnu par Windows.Si la reprise échoue et que votre machine redémarre avec l'erreur Impossible d'obtenir le fichier de la partition, essayez de désactiver le démarrage sécurisé. Pour en savoir plus sur la façon de procéder, consultez la section Désactivation du démarrage sécurisé dans la documentation Microsoft.Pour restaurer une machine physiqueSélectionnez la machine sauvegardée.Cliquez sur Restauration.Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Effectuez l'une des actions suivantes :Si la sauvegarde est située sur le Cloud ou à un emplacement de stockage partagé (c.-à-d. que d'autres agents peuvent y accéder), cliquez sur Sélectionner une machine, sélectionnez une machine cible qui est en ligne, puis choisissez un point de restauration.Sélectionnez un point de récupération dans l'onglet Stockage de sauvegarde.Restaurez la machine comme décrit dans « Restauration de disques via un support de démarrage ».Cliquez sur Restaurer > Toute la machine.Le logiciel mappe automatiquement les disques depuis la sauvegarde vers les disques de la machine cible.Pour effectuer une restauration sur une autre machine physique, cliquez sur Machine cible, puis sélectionnez une machine cible en ligne.Si vous n'êtes pas satisfait du résultat du mappage ou si le mappage du disque échoue, cliquez sur Mappage de volume pour re-mapper les disques manuellement.La section Mappage permet également de choisir les disques ou volumes à restaurer. Vous pouvez passer de la restauration de disques à la restauration de volumes, et vice-versa, à l'aide du lien

Basculer vers... dans l'angle supérieur droit.[Disponible uniquement pour les ordinateurs Windows sur lesquels un agent de protection est installé] Activez le curseur Restauration sûre afin de vous assurer que les données restaurées sont exemptes de malware. Pour plus d'informations sur le fonctionnement de la restauration sécurisée, voir "Restauration sûre" (p. 1).Cliquez sur Démarrer la récupération.Confirmez que vous souhaitez écraser les données du disque avec leurs versions sauvegardées. Choisissez si vous souhaitez redémarrer automatiquement la machine.La progression de la restauration sont affichées dans l'onglet Activités." (p. 1).

5. Pour définir la configuration avancée de la reprise, cliquez sur **Options de restauration**. Pour obtenir plus d'informations, consultez l'article "Options de restauration" (p. 543).
6. Cliquez sur **Démarrer la récupération**.
7. Confirmez que vous souhaitez écraser les données du disque avec leurs versions sauvegardées. Choisissez si vous souhaitez redémarrer automatiquement la machine.
8. La progression de la restauration sont affichées dans l'onglet **Activités**.

Pour redémarrer à distance l'ordinateur démarré

1. Dans l'onglet **Terminaux**, accédez au groupe **Support de démarrage**, puis sélectionnez le support que vous souhaitez utiliser pour la restauration de données.
2. Cliquez sur **Redémarrer**.
3. Confirmez que vous souhaitez redémarrer l'ordinateur démarré avec le support.

Pour arrêter à distance l'ordinateur démarré

1. Dans l'onglet **Terminaux**, accédez au groupe **Support de démarrage**, puis sélectionnez le support que vous souhaitez utiliser pour la restauration de données.
2. Cliquez sur **Arrêt du système**.
3. Confirmez que vous souhaitez arrêter l'ordinateur démarré avec le support.

Pour afficher les informations concernant le support de démarrage

1. Dans l'onglet **Terminaux**, accédez au groupe **Support de démarrage**, puis sélectionnez le support que vous souhaitez utiliser pour la restauration de données.
2. Cliquez sur **Détails**, **Activités** ou **Alertes** pour voir les informations correspondantes.

Pour supprimer à distance le support de démarrage

1. Dans l'onglet **Terminaux**, accédez au groupe **Support de démarrage**, puis sélectionnez le support que vous souhaitez utiliser pour la restauration de données.
2. Cliquez sur **Supprimer** pour supprimer le support de démarrage de la console Cyber Protect.
3. Confirmez que vous souhaitez supprimer le support de démarrage.

Startup Recovery Manager

Startup Recovery Manager est un composant amorçable qui réside sur le disque dur. Avec Startup Recovery Manager, vous pouvez lancer l'utilitaire de secours amorçable sans utiliser de support d'amorçage distinct.

En cas d'échec, redémarrez l'ordinateur, attendez que le message **Appuyez sur F11 pour Acronis Startup Recovery Manager** apparaisse, puis appuyez sur F11 ou sélectionnez Startup Recovery Manager dans le menu de démarrage (si vous utilisez le chargeur de démarrage GRUB). Startup Recovery Manager démarre et vous pouvez effectuer une restauration.

Limites

- [Ne s'applique pas à GRUB installé dans le secteur de démarrage principal] L'activation de Startup Recovery Manager écrase le secteur de démarrage principal (MBR) avec son propre code de démarrage. Par conséquent, vous devrez peut-être réactiver les chargeurs de démarrage tiers après l'activation.
- [Ne s'applique par à GRUB] Avant d'activer Startup Recovery Manager sous Linux, nous vous recommandons d'installer le chargeur de démarrage dans l'enregistrement de démarrage de la partition racine ou des partitions /boot au lieu de l'installer dans l'enregistrement de démarrage principal. Sinon, reconfigurez manuellement le chargeur de démarrage après l'activation.

Activation de Startup Recovery Manager

Pour activer l'invite de démarrage **Appuyez sur F11 pourAcronis Startup Recovery Manager** (ou pour ajouter l'élément **Startup Recovery Manager** au menu GRUB), vous devez activer Startup Recovery Manager.

Remarque
L'activation de Startup Recovery Manager sur un ordinateur avec un volume système non chiffré nécessite au moins 100 Mo d'espace libre sur cet ordinateur. La restauration avec redémarrage nécessite 100 Mo supplémentaires.

Pour que l'élément Startup Recovery Manager puisse être activé sur un ordinateur ayant un volume chiffré par BitLocker, cet ordinateur doit avoir au moins un volume non chiffré avec un espace libre minimal de 500 Mo. La restauration avec redémarrage nécessite 500 Mo d'espace libre supplémentaires.

Les opérations de sauvegarde qui créent des sauvegardes de restauration en un clic échouent si Startup Recovery Manager n'est pas activé.

Pour activer Startup Recovery Manager

Sur un ordinateur Windows ou Linux avec un agent

1. Dans la console Cyber Protect, sélectionnez l'ordinateur sur lequel vous souhaitez activer Startup Recovery Manager.

2. Cliquez sur **Détails**.
3. Activez le commutateur **Startup Recovery Manager** .

Sur un ordinateur sans agent

1. Démarrez l'ordinateur en utilisant un support de démarrage.
2. Dans l'interface graphique du support de démarrage, cliquez sur **Outils** > **Activer Startup Recovery Manager**.
3. Sélectionnez **Activer**.
4. Cliquez sur **OK**.
5. Dans l'onglet **Détails**, vérifiez dans la ligne **Résultat** si l'activation a réussi, puis cliquez sur **Fermer**.

Désactivation de Startup Recovery Manager

La désactivation porte sur l'invite de démarrage **Appuyez sur F11 pourAcronis Startup Recovery Manager** (ou supprime l'élément **Startup Recovery Manager** du menu GRUB).

Si Startup Recovery Manager n'est pas activé, vous pouvez toujours récupérer un ordinateur qui ne démarre pas en utilisant un support de démarrage distinct.

Remarque
Les opérations de sauvegarde qui créent des sauvegardes de restauration en un clic échouent si Startup Recovery Manager n'est pas activé.

Pour désactiver Startup Recovery Manager

Sur un ordinateur Windows ou Linux avec un agent

1. Dans la console Cyber Protect, sélectionnez l'ordinateur sur lequel vous voulez désactiver Startup Recovery Manager.
2. Cliquez sur **Détails**.
3. Désactivez le commutateur **Startup Recovery Manager**.

Sur un ordinateur sans agent

1. Démarrez l'ordinateur en utilisant un support de démarrage.
2. Dans l'interface graphique du support de démarrage, cliquez sur **Outils** > **Désactiver Startup Recovery Manager**.
3. Sélectionnez **Désactiver**.
4. Cliquez sur **OK**.
5. Dans l'onglet **Détails**, vérifiez dans la ligne **Résultat** si la désactivation a réussi, puis cliquez sur **Fermer**.

Implémentation de la reprise d'activité après sinistre

Remarque
- Cette fonctionnalité ne prend pas en charge les emplacements de sauvegarde Microsoft Azure.

À propos de Cyber Disaster Recovery Cloud

Cyber Disaster Recovery Cloud (DR) : partie de Cyber Protection, qui fournit une reprise d'activité après sinistre en tant que service (DRaaS). Cyber Disaster Recovery Cloud vous fournit une solution rapide et stable pour lancer les copies exactes de vos machines sur le site dans le Cloud et basculer la ressource des machines d'origine corrompues vers les serveurs de restauration dans le Cloud, en cas de catastrophe naturelle ou causée par l'homme.

Vous pouvez définir et configurer la reprise d'activité après sinistre de différentes manières :

- Créez un plan de protection qui inclut un module de reprise d'activité après sinistre et appliquez-le à tous vos terminaux. Cela permet de définir automatiquement une infrastructure de reprise d'activité après sinistre par défaut. Voir la section Créer un plan de protection de reprise d'activité après sinistre.
- Configurez manuellement l'infrastructure Cloud de reprise d'activité après sinistre et contrôlez chaque étape. Consultez "Configuration des serveurs de restauration" (p. 819).

Les fonctionnalités clés

Remarque
Certaines fonctionnalités peuvent nécessiter une licence supplémentaire, en fonction du modèle de gestion de licences appliqué.

- Gérez le service Cyber Disaster Recovery Cloud depuis une console unique
- Étendez jusqu'à 23 réseaux locaux au Cloud à l'aide d'un tunnel VPN sécurisé
- Établissez une connexion vers le site dans le Cloud sans aucun déploiement de appliance VPN (le mode « sur Cloud uniquement »)
- Établissez une connexion de point à site vers vos sites locaux et dans le Cloud
- Protégez vos machines en utilisant des serveurs de restauration dans le Cloud
- Protégez vos applications et matériels en utilisant des serveurs primaires dans le Cloud
- Exécutez des opérations automatisées de reprise d'activité après sinistre pour des sauvegardes chiffrées
- Réalisez un basculement test dans le réseau isolé
- Utilisez des runbooks pour lancer l'environnement de production dans le Cloud

Exigences logicielles

Systèmes d'exploitation pris en charge

La protection à l'aide d'un serveur de restauration a été testée pour les systèmes d'exploitation suivants :

- CentOS 6.6, 7.x, 8.x
- Debian 9.x, 10.x, 11.x
- Red Hat Enterprise Linux 6.6, 7.x, 8.x
- Ubuntu 16.04, 18.04, 20.x, 21.x
- Oracle Linux 7.3 and 7.9 with Unbreakable Enterprise Kernel
- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – toutes les options d'installation, excepté Nano Server
- Windows Server 2019 – toutes les options d'installation, excepté Nano Server
- Windows Server 2022 – toutes les options d'installation, excepté Nano Server

Le logiciel peut fonctionner avec d'autres systèmes d'exploitation Windows ou d'autres distributions Linux, mais cela n'est pas garanti.

Remarque
La protection à l'aide d'un serveur de restauration a été testée pour les machines virtuelles Microsoft Azure avec les systèmes d'exploitation suivants.

- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – toutes les options d'installation, excepté Nano Server
- Windows Server 2019 – toutes les options d'installation, excepté Nano Server
- Windows Server 2022 – toutes les options d'installation, excepté Nano Server
- Ubuntu Server 20.04 LTS - Gen2 (Canonical) Pour plus d'informations sur l'accès à la console du serveur de restauration, consultez l'article https://kb.acronis.com/content/71616.

Plates-formes de virtualisation prises en charge

La protection de machines virtuelles à l'aide d'un serveur de restauration a été testée pour les plates-formes de virtualisation suivantes :

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
- Windows Server 2008 R2 avec Hyper-V

- Windows Server 2012/2012 R2 avec Hyper-V
- Windows Server 2016 avec Hyper-V – toutes les options d'installation, excepté Nano Server
- Windows Server 2019 avec Hyper-V – toutes les options d'installation, excepté Nano Server
- Windows Server 2022 avec Hyper-V – toutes les options d'installation, excepté Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- Machines virtuelles basées sur un noyau (KVM) — Invités entièrement virtualisés (HVM) uniquement. Les invités paravirtualisés (PV) ne sont pas pris en charge.
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2

L'application VPN a été testée pour les plates-formes de virtualisation suivantes :

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2 avec Hyper-V
- Windows Server 2012/2012 R2 avec Hyper-V
- Windows Server 2016 avec Hyper-V – toutes les options d'installation, excepté Nano Server
- Windows Server 2019 avec Hyper-V – toutes les options d'installation, excepté Nano Server
- Windows Server 2022 avec Hyper-V – toutes les options d'installation, excepté Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

Le logiciel peut fonctionner avec d'autres plates-formes de virtualisation ou d'autres versions, mais cela n'est pas garanti.

Limites

Les plate-formes et configurations suivantes ne sont pas prises en charge dans Cyber Disaster Recovery Cloud :

1. Plateformes non prises en charge :
   - Agents pour Virtuozzo
   - macOS
   - Les systèmes d'exploitation Windows de bureau ne sont pas pris en charge en raison des conditions générales relatives aux produits Microsoft.
   - Windows Server Azure Edition

     Azure Edition est une version particulière de Windows Server conçue spécifiquement pour fonctionner en tant que machine virtuelle Azure IaaS (VM) dans Azure ou en tant que VM dans un cluster HCI Azure Stack. Contrairement aux éditions Standard et Datacenter, Azure Edition

n'a pas la licence nécessaire pour fonctionner sur un système nu, Windows Client Hyper-V, Windows Server Hyper-V, des hyperviseurs tiers ou dans des clouds tiers.

2. Configurations non prises en charge :

   Microsoft Windows

   - Les disques dynamiques ne sont pas pris en charge
   - Les systèmes d'exploitation Windows de bureau ne sont pas pris en charge en raison des conditions générales relatives aux produits Microsoft.
   - Le service Active Directory avec réplication FRS n'est pas pris en charge
   - Les supports amovibles sans formatage GPT ou MBR (dits « super disquettes ») ne sont pas pris en charge

   Linux

   - Systèmes de fichiers sans table de partition
   - Les ressources Linux qui sont sauvegardées avec un agent d'un SE invité et dont les volumes ont les configurations Logical Volume Manager avancées suivantes : volumes agrégés par bandes, volumes en miroir, volumes RAID 0, RAID 4, RAID 5, RAID 6 ou RAID 10.

   Remarque
   Les ressources ayant plusieurs systèmes d'exploitation installés ne sont pas prises en charge.

3. Types de sauvegarde non pris en charge :
   - Les points de reprise de la protection continue des données (CDP) sont incompatibles.

     Important
     Si vous créez un serveur de restauration à partir d'une sauvegarde disposant d'un point de récupération CDP, lors de la restauration automatique ou lors de la création d'une sauvegarde d'un serveur de restauration, vous perdrez les données contenues dans le point de récupération CDP.

   - Les sauvegardes d'investigation ne peuvent pas être utilisées pour créer des serveurs de restauration.

Un serveur de restauration possède une interface réseau. Si la machine d'origine possède plusieurs interfaces réseau, une seule est émulée.

Les serveurs Cloud ne sont pas chiffrés.

Version d'évaluation Cyber Disaster Recovery Cloud

Vous pouvez utiliser une version d'évaluation de Acronis Cyber Disaster Recovery Cloud pour une période de 30 jours. Dans ce cas, la reprise d'activité après sinistre présente les limitations suivantes pour les tenants partenaires :

- Aucun accès à l'Internet public pour les serveurs primaires et de reprise. Vous ne pouvez pas attribuer d'adresses IP aux serveurs.

- Le VPN multisite Ipsec n'est pas disponible.

Limites d'utilisation du stockage géoredondant dans le cloud

Le stockage géoredondant dans le cloud fournit un emplacement secondaire pour vos données de sauvegarde. L'emplacement secondaire se trouve dans une région distincte géographiquement de l'emplacement de stockage principal. La séparation géographique des régions garantit que, en cas de sinistre ayant des conséquences sur l'une des régions et rendant les données de stockage non récupérables, l'autre région ne sera pas affectée et les opérations pourront se poursuivre.

Important
Le service Reprise d'activité après sinistre n'est pas pris en charge si l'emplacement de stockage des sauvegardes passe de l'emplacement principal à l'emplacement secondaire géoredondant.

Compatibilité de la reprise d'activité après sinistre avec le logiciel de chiffrement

La reprise d'activité après sinistre est compatible avec les logiciels de chiffrement de disque suivants :

- Microsoft BitLocker Drive Encryption
- Chiffrement McAfee Endpoint
- Chiffrement PGP de disque complet

Remarque
- Pour les ressources avec chiffrement au niveau du disque, nous vous recommandons d'installer l'agent de protection dans le système d'exploitation invité de la ressource, et d'effectuer des sauvegardes avec agent.
- Le basculement et la restauration automatique ne sont pas pris en charge pour les sauvegardes sans agent de ressources chiffrées.

Pour plus d'informations sur la compatibilité de Cyber Protection avec le logiciel de chiffrement, voir "Compatibilité avec le logiciel de chiffrage" (p. 43).

Points de calcul

Dans Disaster Recovery, es points de calcul sont utilisés pour les serveurs primaires et les serveurs de restauration pendant le basculement en environnement de test et en environnement de production. Les points de calcul reflètent les ressources de calcul utilisées pour l'exécution des serveurs (machines virtuelles) dans le cloud.

La consommation des points de calcul pendant la reprise d'activité après sinistre dépend des paramètres du serveur et de la durée pendant laquelle le serveur se trouve dans l'état de basculement. Plus le serveur est puissant et plus cette période est longue, plus le nombre de points de calcul consommés est élevé. Et plus le nombre de points de calcul consommés est élevé, plus le prix que vous payez est important.

Tous les serveurs qui fonctionnent dans le cloud Acronis seront facturés pour les points de calcul, en fonction de leur version configurée, et indépendamment de leur état (sous tension ou hors tension).

Les serveurs de restauration en état de veille ne consomment pas de points de calcul et ne seront pas facturés pour les points de calcul.

Dans le tableau ci-dessous, vous pouvez voir un exemple de huit serveurs dans le cloud avec différentes configurations, et les points de calcul correspondants qu'ils consommeront par heure. Vous pouvez modifier les configurations des serveurs dans l'onglet **Détails**.

Type	CPU	RAM	Points de calcul
F1	1 vCPU	2 Go	1
F2	1 vCPU	4 Go	2
F3	2 vCPU	8 Go	4
F4	4 vCPU	16 Go	8
F5	8 vCPU	32 Go	16
F6	16 vCPU	64 Go	32
F7	16 vCPU	128 Go	64
F8	16 vCPU	256 Go	128

Grâce aux informations du tableau, vous pouvez estimer facilement le nombre de points de calcul consommés par un serveur (machine virtuelle).

Par exemple, si vous souhaitez protéger avec la reprise d'activité après sinistre une machine virtuelle comportant 4 vCPU* de 16 Go de mémoire RAM et une machine virtuelle comportant 2 vCPU avec 8 Go de mémoire RAM, la première machine virtuelle consomme 8 points de calcul par heure et la seconde machine virtuelle, 4 points de calcul par heure. Si les deux machines virtuelles se trouvent dans une situation de basculement, la consommation totale est de 12 points de calcul par heure, soit 288 points de calcul pour la journée complète (12 points de calcul x 24 heures = 288 points de calcul).

* vCPU fait référence à un processeur (CPU) physique affecté à une machine virtuelle et dépendant de l'heure.

Remarque
Si le quota de **Points de calcul** est dépassé, tous les serveurs primaires et de restauration seront arrêtés. Il ne sera plus possible d'utiliser ces serveurs jusqu'au début de la période de facturation suivante ou jusqu'à ce que vous augmentiez le quota. La période de facturation par défaut est un mois complet.

Configuration de la fonctionnalité de reprise d'activité après sinistre

Remarque
Certaines fonctionnalités peuvent nécessiter une licence supplémentaire, en fonction du modèle de gestion de licences appliqué.

Pour configurer la fonctionnalité de reprise d'activité après sinistre

1. Configurer le type de connectivité vers le site dans le Cloud :
   - Connexion de point à site
   - Connexion OpenVPN de site à site
   - Connexion VPN IPsec multi-site
   - Mode « sur Cloud uniquement »
2. Créez un plan de protection avec le module de sauvegarde activé et sélectionnez la machine ou le système entier, ainsi que les volumes de démarrage, pour la sauvegarde. Au moins un plan de protection est nécessaire pour créer un serveur de restauration.
3. Appliquez le plan de protection aux serveurs locaux à protéger.
4. Créez des serveurs de restauration pour chacun des serveurs locaux que vous souhaitez protéger.
5. Réalisez un basculement test pour vérifier le fonctionnement.
6. [Facultatif] Créez les serveurs primaires pour la réplication de l'application.

En conséquence, vous avez configuré la fonctionnalité de reprise d'activité après sinistre destinée à protéger vos serveurs locaux d'un sinistre.

Si un sinistre se produit, vous pouvez basculer la ressource vers les serveurs de restauration dans le Cloud. Vous devez créer au moins un point de récupération avant de basculer vers des serveurs de restauration. Lorsque votre site local est restauré après un sinistre, vous pouvez rebasculer la ressource vers votre site local en procédant à une restauration automatique. Pour plus d'informations sur le processus de restauration automatique, reportez-vous à "Prérequis" (p. 834) et "Prérequis" (p. 839).

Créer un plan de protection de reprise d'activité après sinistre

Créez un plan de protection qui inclut un module de reprise d'activité après sinistre et appliquez-le à tous vos terminaux.

Par défaut, lors de la création d'un plan de protection, le module de reprise d'activité après sinistre est désactivé. Une fois que vous avez activé la fonctionnalité de reprise d'activité après sinistre et appliqué le plan à vos terminaux, l'infrastructure réseau dans le cloud est créée et se compose notamment d'un *serveur de restauration* pour chaque terminal protégé. Le *serveur de restauration* est une machine virtuelle dans le Cloud qui est une copie du terminal sélectionné. Pour chacun des terminaux sélectionnés, un serveur de restauration avec les paramètres par défaut est créé en mode Veille (machine virtuelle non exécutée). Le serveur de restauration est automatiquement dimensionné en fonction du processeur et de la mémoire RAM du terminal protégé. L'infrastructure du réseau Cloud par défaut est également créée automatiquement : la passerelle VPN et les réseaux sur le site dans le Cloud auxquels les serveurs de restauration seront connectés.

Si vous révoquez, supprimez ou désactivez le module de reprise d'activité après sinistre d'un plan de protection, les serveurs de restauration et les réseaux cloud ne sont pas automatiquement supprimés. Vous pouvez retirer manuellement l'infrastructure de reprise d'activité après sinistre, si nécessaire.

Remarque

- Une fois que vous aurez configuré la reprise d'activité après sinistre, vous serez en mesure d'effectuer un basculement test ou un basculement de la production depuis n'importe quel point de reprise généré après la création du serveur de restauration pour le terminal. Les points de reprise qui ont été générés avant qu'un terminal ne soit protégé par la reprise d'activité après sinistre (p. ex., avant que le serveur de restauration ne soit créé) ne pourront pas être utilisés pour le basculement.
- Un plan de protection de reprise d'activité après sinistre ne peut pas être activé si l'adresse IP d'un terminal ne peut pas être détectée. Par exemple lorsque des machines virtuelles sont sauvegardées sans agent, et qu'aucune adresse IP ne leur a été affectée.
- Lorsque vous appliquez un plan de protection, les mêmes réseaux et adresses IP sont attribués au site dans le Cloud. La connectivité VPN IPsec nécessite que les segments réseau du site local et du site dans le Cloud ne se chevauchent pas. Si une connectivité VPN IPsec multi-site est configurée et que vous appliquez un plan de protection ultérieurement à un ou plusieurs terminaux, vous devez en plus mettre à jour les réseaux Cloud et réaffecter les adresses IP des serveurs Cloud. Pour plus d'informations, voir "Réaffectation d'adresses IP" (p. 809).

Pour créer un plan de protection de reprise d'activité après sinistre

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez les machines que vous souhaitez protéger.

3. Cliquez sur **Protection**, puis sur **Création d'un plan**.
   Les paramètres par défaut du plan de protection s'affichent.
4. Configurez les options de sauvegarde.
   Pour utiliser la fonctionnalité de reprise d'activité après sinistre, le plan doit sauvegarder l'intégralité de la machine ou uniquement les disques requis pour le démarrage et la fourniture des services nécessaires à un stockage dans le Cloud.
5. Activez le module de reprise d'activité après sinistre en cliquant à côté du nom du module.
6. Cliquez sur **Créer**.
   Le plan est créé et appliqué aux ordinateurs sélectionnés.

Que faire ensuite

- Vous pouvez modifier la configuration par défaut du serveur de restauration. Pour plus d'informations, voir "Configuration des serveurs de restauration" (p. 819).
- Vous pouvez modifier la configuration de mise en réseau par défaut. Pour plus d'informations, voir "Configuration de la connectivité" (p. 782).
- Vous pouvez en apprendre plus à propos des paramètres par défaut du serveur de restauration et de l'infrastructure de réseau Cloud. Pour plus d'informations, voir "Modification des paramètres par défaut du serveur de restauration" (p. 780) et "Infrastructure du réseau Cloud" (p. 782).

Modification des paramètres par défaut du serveur de restauration

Lorsque vous créez et appliquez un plan de protection de reprise d'activité après sinistre, un serveur de restauration est créé avec des paramètres par défaut. Vous pouvez modifier ces paramètres par défaut ultérieurement.

Remarque
Un serveur de restauration est créé seulement s'il n'existe pas. Les serveurs de restauration existants ne sont pas modifiés ni recréés.

Pour modifier les paramètres par défaut du serveur de restauration

1. Accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez un terminal, puis cliquez sur **Reprise d'activité après sinistre**.
3. Modifiez les paramètres par défaut du serveur de restauration.
   Ces paramètres sont décrits dans le tableau suivant :

Serveur de restauration paramètre	**Défaut valeur**	**Description**
CPU et RAM	auto	Nombre de processeurs virtuels et la quantité de mémoire RAM pour le serveur de restauration. Les

		paramètres par défaut seront automatiquement déterminés en fonction du processeur du terminal et de la configuration de la mémoire RAM.
Réseau dans le Cloud	auto	Le serveur Cloud auquel le serveur sera connecté. Pour plus de détails sur la configuration des réseaux dans le Cloud, voir Infrastructure de réseau Cloud.
Adresse IP en réseau de production	auto	Adresse IP que le serveur aura dans le réseau de production. Par défaut, l'adresse IP de la machine d'origine est sélectionnée.
Adresse IP test	désactivé	Cela vous permettra de tester un basculement dans le réseau de test isolé et de vous connecter au serveur de restauration via RDP ou SSH lors d'un basculement test. En mode de basculement test, la passerelle VPN remplace l'adresse IP test par l'adresse IP de production au moyen du protocole NAT. Si vous n'activez pas la case à cocher, la console sera le seul moyen d'accéder au serveur lors d'un basculement test.
Accès Internet	activé	Cela permettra au serveur de restauration d'accéder à Internet lors d'un vrai basculement ou d'un basculement test. Par défaut, le port TCP 25 est refusé pour les connexions sortantes.
Utiliser une adresse publique	désactivé	Disposer d'une adresse IP publique permet au serveur de restauration d'être accessible depuis Internet lors d'un basculement ou d'un basculement test. Si vous n'utilisez pas une adresse IP publique, le serveur sera disponible uniquement sur votre réseau de production. Pour utiliser une adresse IP publique, vous devez activer l'accès Internet. L'adresse IP publique s'affichera une fois la configuration terminée. Par défaut, le port TCP 443 est ouvert pour les connexions entrantes.
Définir le seuil des objectifs de point de récupération	désactivé	Le seuil des objectifs de point de récupération (RPO) définit l'intervalle de temps maximum autorisé entre le dernier point de récupération pour un basculement et l'heure actuelle. La valeur peut être définie entre 15 et 60 minutes, 1 et 24 heures, 1 et 14 jours.

Infrastructure du réseau Cloud

L'infrastructure du réseau Cloud se compose de la passerelle VPN sur le site dans le Cloud et des réseaux Cloud auxquels les serveurs de restauration seront connectés.

Remarque
L'application d'un plan de protection de reprise d'activité après sinistre crée une infrastructure de réseau Cloud uniquement si elle n'existe pas. Les réseaux Cloud existants ne sont pas modifiés ni recréés.

Le système vérifie les adresses IP des terminaux et, s'il n'existe pas de réseaux Cloud correspondant à l'adresse IP, crée automatiquement les réseaux Cloud qui conviennent. Si vous disposez déjà de réseaux Cloud existants où les adresses IP des serveurs de restauration correspondent, ceux-ci ne seront ni modifiés ni recréés.

- Si vous ne disposez pas de réseaux Cloud existants ou si vous définissez une configuration de reprise d'activité après sinistre pour la première fois, les réseaux Cloud seront créés avec les plages maximales recommandées par IANA pour un usage privé (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) en fonction de votre plage d'adresses IP de terminaux. Vous pouvez restreindre l'accès réseau en modifiant le masque de réseau.
- Si vous avez des terminaux sur plusieurs réseaux locaux, le réseau sur le site dans le Cloud peut devenir un super-ensemble de réseaux locaux. Vous pouvez reconfigurer les réseaux dans la section **Connectivité**. Consultez "Gestion des réseaux" (p. 803).
- Si vous devez configurer la connectivité OpenVPN de site à site, téléchargez l'appliance VPN et configurez-la. Consultez "Configuration OpenVPN de site à site" (p. 793). Assurez-vous que les plages des réseaux Cloud correspondent aux plages de vos réseaux locaux connectés au matériel VPN.
- Pour modifier la configuration du réseau par défaut, cliquez sur le lien **Accéder à Connectivité** dans le module de reprise d'activité après sinistre du plan de protection ou accédez à **Reprise d'activité après sinistre** > **Connectivité**.

Configuration de la connectivité

Cette section explique les concepts de réseau nécessaires pour que vous compreniez comment tout fonctionne dans Cyber Disaster Recovery Cloud. Vous découvrirez comment configurer différents types de connectivité vers le site dans le Cloud, selon vos besoins. Enfin, vous découvrirez comment gérer vos réseaux dans le Cloud et gérer les paramètres du matériel VPN et de la passerelle VPN.

Concepts de réseau

Remarque
Certaines fonctionnalités peuvent nécessiter une licence supplémentaire, en fonction du modèle de gestion de licences appliqué.

Cyber Disaster Recovery Cloud vous permet de définir les types suivants de connectivité au site dans le Cloud :

- **Mode « sur Cloud uniquement »**

  Ce type de connexion ne nécessite pas de déploiement de matériel VPN sur le site local.

  Les réseaux locaux et dans le Cloud sont des réseaux indépendants. Ce type de connexion implique soit le basculement de tous les serveurs protégés du site local ou le basculement partiel de serveurs indépendants qui ne nécessitent pas de communiquer avec le site local.

  Les serveurs Cloud sur le site dans le Cloud sont accessibles via le VPN de point à site et les adresses IP publiques (si attribuées).
- **Connexion OpenVPN de site à site**

  Ce type de connexion requiert le déploiement d'un matériel VPN vers le site local.

  La connexion OpenVPN de site à site vous permet d'étendre vos réseaux au Cloud et de conserver les adresses IP.

  Votre site local est connecté au site dans le Cloud au moyen d'un tunnel VPN sécurisé. Ce type de connexion est adapté en cas de serveurs hautement dépendants sur le site local, tels qu'un serveur Web et un serveur de bases de données. En cas de basculement partiel, quand l'un de ces serveurs est recréé sur le site dans le Cloud alors que l'autre reste dans le site local, ils pourront toujours communiquer entre eux via un tunnel VPN.

  Les serveurs Cloud sur le site dans le Cloud sont accessibles via le réseau local, le VPN de point à site, et les adresses IP publiques (si attribuées).
- **Connexion VPN IPsec multi-site**

  Ce type de connexion nécessite un terminal VPN local compatible avec le protocole IPsec IKE v2.

  Lorsque vous commencez à configurer la connexion VPN IPsec multi-site, Cyber Disaster Recovery Cloud crée automatiquement une passerelle VPN Cloud avec une adresse IP publique.

  Avec le VPN IPsec multi-site, vos sites locaux sont connectés au site dans le Cloud au moyen d'un tunnel VPN IPsec sécurisé.

  Ce type de connexion est adapté aux scénarios de reprise d'activité après sinistre lorsque vous disposez d'un ou plusieurs sites locaux hébergeant des ressources critiques ou de services qui dépendent étroitement les uns des autres.

  En cas de basculement partiel de l'un des serveurs, le serveur est recréé sur le site dans le Cloud alors que les autres sont conservés dans le site local. Ils pourront toutefois toujours communiquer entre eux via un tunnel VPN IPsec.

  En cas de basculement partiel de l'un des sites locaux, les autres sites locaux restent opérationnels et pourront toujours communiquer entre eux via un tunnel VPN IPsec.
- **Accès VPN à distance de point à site**

  Un accès VPN à distance de point à site sécurisé vers les ressources de votre site Cloud et local provenant de l'extérieur en utilisant votre terminal.

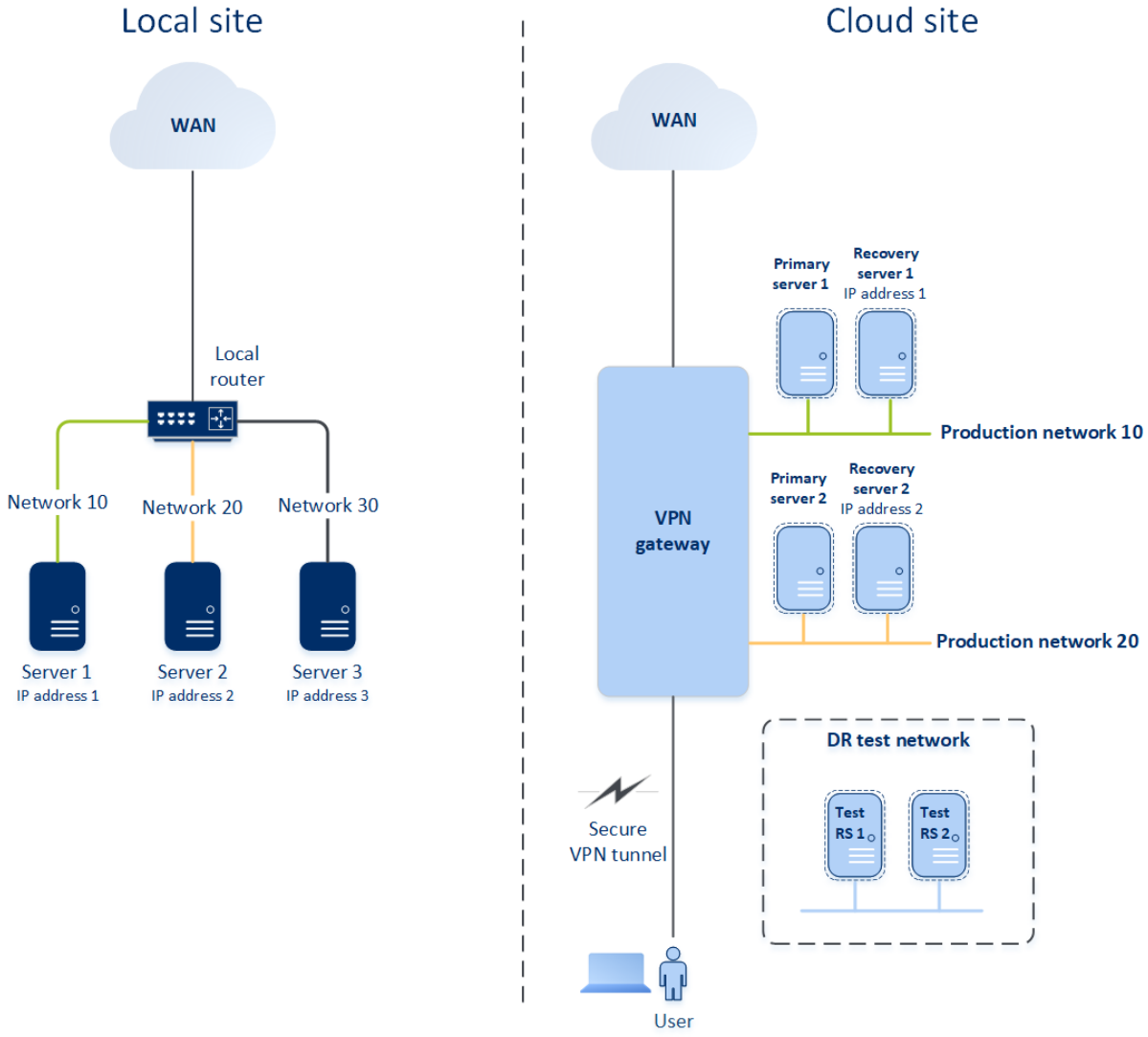
  Pour accéder à un site local, ce type de connexion requiert le déploiement d'un matériel VPN vers le site local.

Mode « sur Cloud uniquement »

Le mode « sur Cloud uniquement » ne nécessite pas de déploiement d'une appliance VPN sur le site local. Cela implique que vous possédez deux réseaux indépendants : l'un sur le site local, l'autre sur le site dans le Cloud. Le routage est effectué avec le routeur sur le site dans le Cloud.

Fonctionnement du routage

Si le mode « sur Cloud uniquement » est activé, le routage est effectué avec le routeur sur le site Cloud, afin que les serveurs des différents réseaux Cloud puissent communiquer les uns avec les autres.



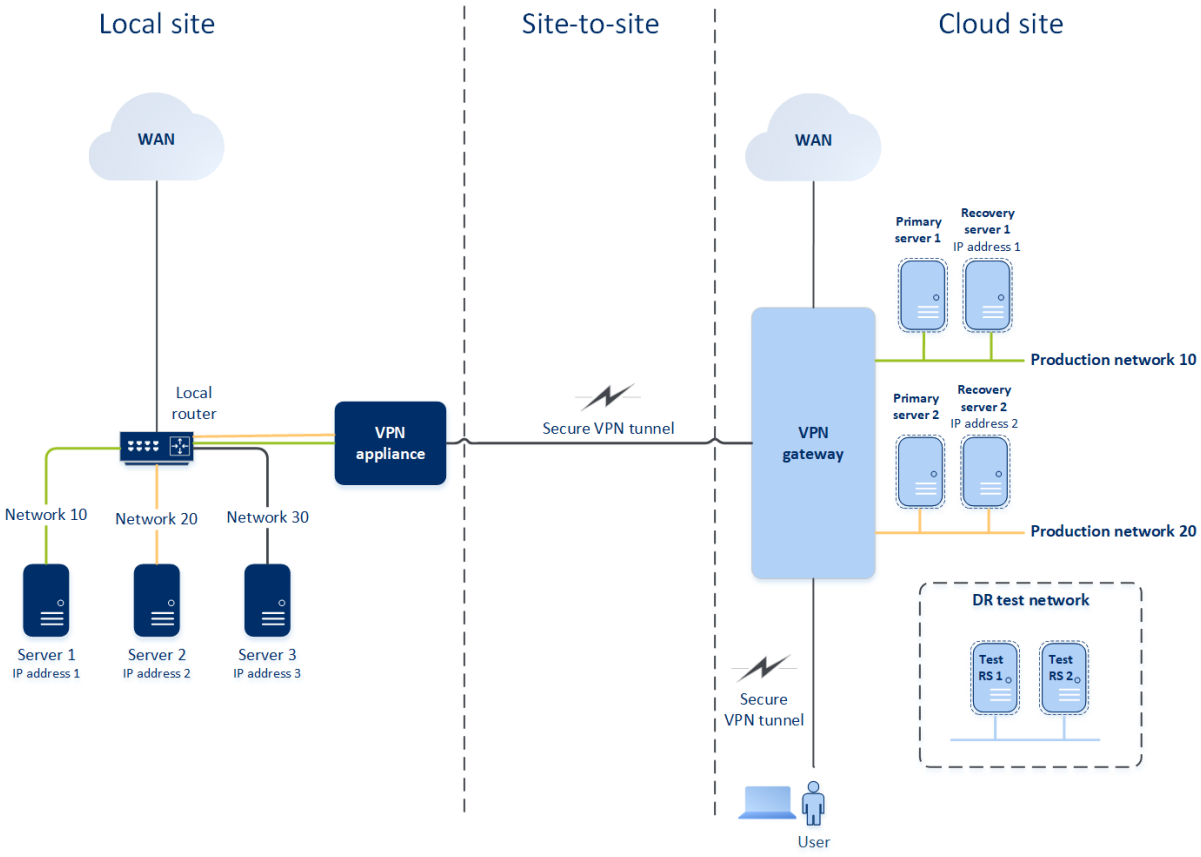
Connexion OpenVPN de site à site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Pour comprendre comment le système de réseau fonctionne dans Cyber Disaster Recovery Cloud, nous examinerons un cas dans lequel vous possédez trois réseaux dotés chacun d'une machine sur le site local. Vous allez configurer la protection contre un sinistre pour les deux réseaux : le Réseau 10 et le Réseau 20.

Dans le diagramme ci-dessous, vous pouvez voir le site local dans lequel vos ordinateurs sont hébergés ainsi que le site dans le Cloud, où vos serveurs Cloud sont lancés en cas de sinistre.

La solution Cyber Disaster Recovery Cloud vous permet de basculer toute la ressource des ordinateurs corrompus du site local vers les serveurs Cloud. Vous pouvez protéger jusqu'à 23 réseaux dans le cloud avec Cyber Disaster Recovery Cloud.



Pour établir une communication OpenVPN de site à site entre le site local et le site dans le Cloud, une **appliance VPN** et une **passerelle VPN** sont utilisées. Lorsque vous commencez à configurer la connexion OpenVPN de site à site dans la console Cyber Protect, la passerelle VPN est automatiquement déployée sur le site dans le cloud. Vous devez ensuite déployer le matériel VPN dans votre site local, ajouter les réseaux à protéger et enregistrer le matériel dans le Cloud. Cyber Disaster Recovery Cloud crée un réplica de votre réseau local dans le Cloud. Un tunnel VPN sécurisé est établi entre l'appliance VPN et la passerelle VPN. Il fournit à votre réseau local une extension vers le Cloud. Les réseaux de production dans le Cloud sont comblés par vos réseaux locaux. Les serveurs locaux et dans le Cloud peuvent communiquer via ce tunnel VPN comme s'ils se trouvaient tous dans le même segment Ethernet. Le routage est effectué avec votre routeur local.

Pour chaque machine source à protéger, vous devez créer un serveur de restauration dans le site dans le Cloud. Il reste en mode **Veille** jusqu'à ce qu'un événement de basculement se produise. Si un sinistre se produit et que vous lancez un processus de basculement (en **mode production**), le serveur de restauration représentant la copie exacte de votre machine protégée est lancé dans le Cloud. Il se peut que la même adresse IP que celle de la machine source lui soit attribuée, et qu'il soit lancé dans le même segment Ethernet. Vos clients peuvent continuer à travailler avec le serveur, sans remarquer de changement de fond.

Vous pouvez également démarrer un processus de basculement en **mode test**. Cela signifie que la machine source fonctionne toujours, et que le serveur de restauration associé doté de la même adresse IP est lancé en même temps dans le Cloud. Pour éviter les conflits d'adresse IP, un réseau virtuel spécial est créé dans le **réseau test** dans le Cloud. Le réseau test est isolé pour éviter la duplication de l'adresse IP de la machine source dans un segment Ethernet. Pour accéder au serveur de restauration en mode de basculement test, vous devez affecter l'**Adresse IP test** au serveur de restauration lorsque vous créez ce dernier. Vous pouvez indiquer d'autres paramètres pour le serveur de restauration, qui seront pris en compte dans les sections respectives ci-dessous.

Fonctionnement du routage

Lorsqu'une connexion de site à site est établie, le routage entre réseaux Cloud s'effectue avec votre routeur local. Le serveur VPN n'effectue pas de routage entre des serveurs Cloud situés dans différents réseaux Cloud. Si un serveur Cloud sur l'un des réseaux souhaite communiquer avec un serveur d'un autre réseau Cloud, le trafic est acheminé au routeur local sur le site local via le tunnel VPN, le routeur local l'achemine vers un autre réseau, puis le trafic revient au serveur de destination sur le site Cloud via le tunnel.

Passerelle VPN

La **passerelle VPN** est le composant majeur qui permet la communication entre les sites locaux et dans le Cloud. Il s'agit d'une machine virtuelle dans le Cloud sur laquelle le logiciel spécial est installé et le réseau spécifiquement configuré. La passerelle VPN possède les fonctions suivantes :

- Connecte les segments Ethernet de votre réseau local et de votre réseau de production dans le Cloud en mode couche 2.
- Fournit des règles iptables et ebtables.
- Agit comme routeur et NAT par défaut pour les ordinateurs des réseaux de test et de production.
- Agit comme serveur DHCP. Toutes les machines des réseaux de production et de test doivent obtenir la configuration réseau (adresses IP, paramètres DNS) via DHCP. À chaque fois, un serveur Cloud obtiendra la même adresse IP auprès du serveur DHCP. Si vous avez besoin de configurer un DNS personnalisé, nous vous invitons à contacter l'équipe d'assistance.
- Agit comme DNS de mise en cache.

Configuration réseau de la passerelle VPN

La passerelle VPN possède plusieurs interfaces réseau :

- Une interface externe, connectée à Internet
- Des interfaces de production, connectées aux réseaux de production
- Une interface de test, connectée au réseau test

Par ailleurs, deux interfaces virtuelles sont ajoutées pour les connexions de point à site et de site à site.

Lorsque la passerelle VPN est déployée et initialisée, les ponts sont créés : un pour l'interface externe et un pour les interfaces client et de production. Bien que le pont client-production et l'interface de test utilisent les mêmes adresses IP, la passerelle VPN peut router des packages correctement en utilisant une technique spécifique.

Application VPN

L'**appliance VPN** est une machine virtuelle dans le site local sur laquelle Linux et le logiciel spécial sont installés, et qui dispose d'une configuration réseau spéciale. Il permet la communication entre les sites locaux et dans le Cloud.

Serveurs de restauration

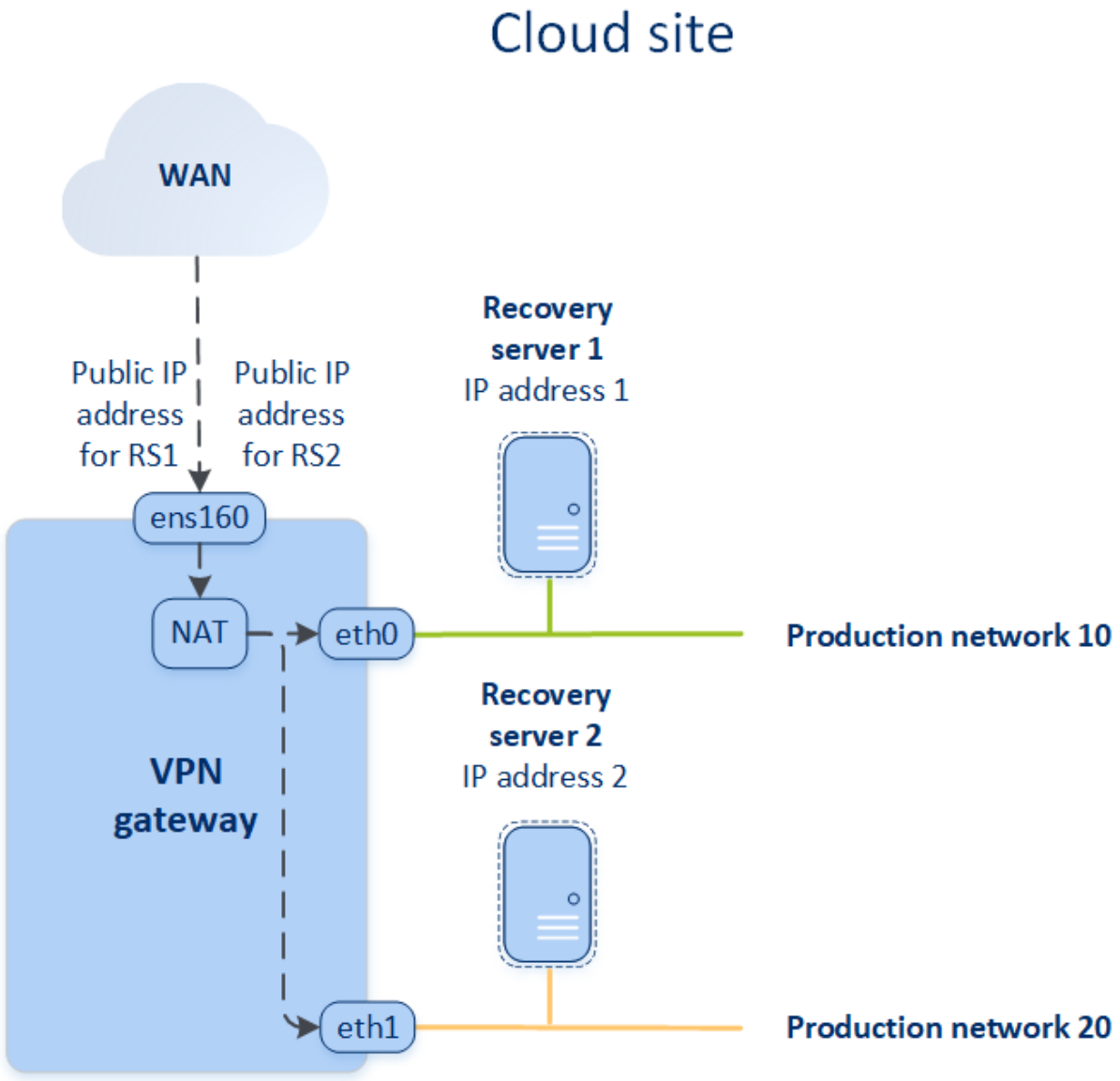
Un **serveur de restauration** : un réplica de la machine d'origine, basé sur les sauvegardes de serveur protégées stockées dans le Cloud. Les serveurs de restauration sont utilisés pour remplacer les ressources depuis les serveurs originaux en cas de sinistre.

Lorsque vous créez un serveur de restauration, vous devez préciser les paramètres de réseau suivants :

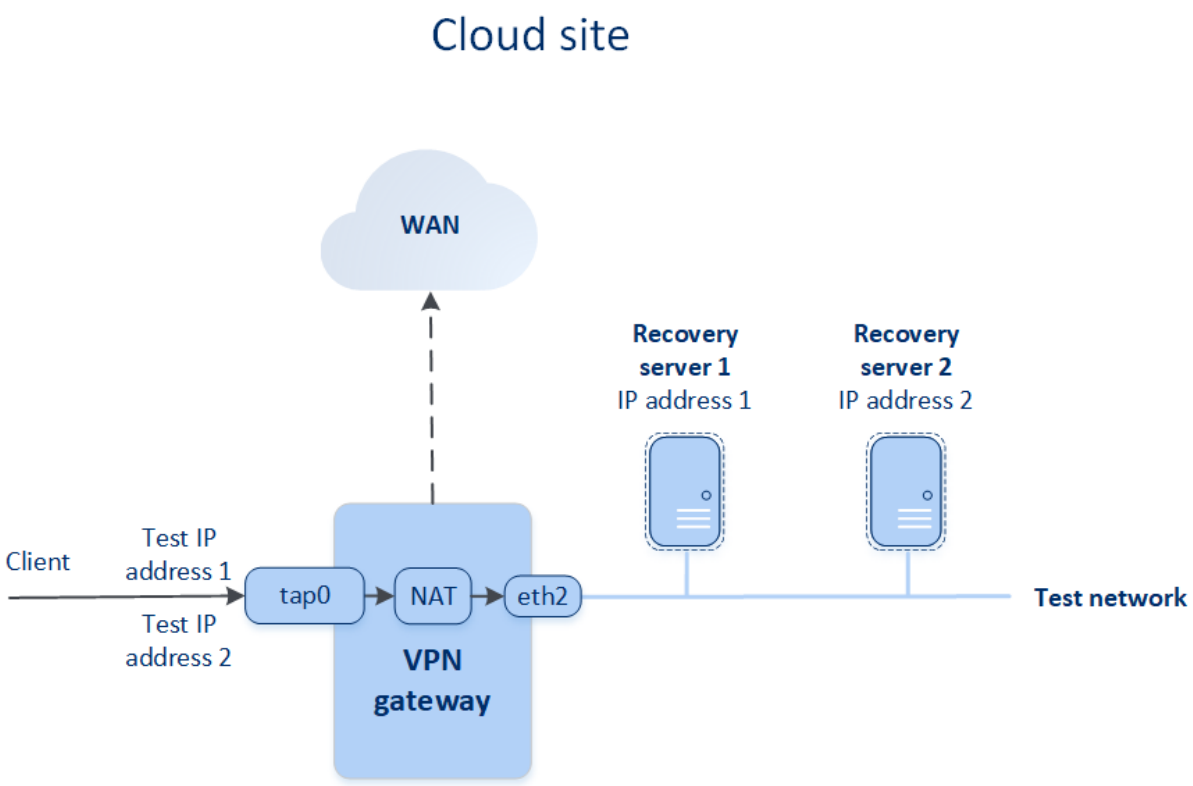
- **Réseau Cloud** (obligatoire) : un réseau Cloud auquel un serveur de restauration sera connecté.
- **Adresse IP dans le réseau de production** (obligatoire) : une adresse IP avec laquelle une machine virtuelle sera lancée pour un serveur de récupération. Cette adresse est utilisée dans les réseaux de test et de production. Avant le lancement, la machine virtuelle est configurée de façon à récupérer l'adresse IP via DHCP.
- **Adresse IP de test** (facultatif) : une adresse IP est nécessaire pour accéder au serveur de restauration depuis le réseau client-production lors du basculement test, afin d'éviter que l'adresse IP de test ne soit dupliquée dans le même réseau. Cette adresse IP est différente de l'adresse IP du réseau de production. Les serveurs du site local peuvent accéder aux serveurs de restauration lors du basculement test via l'adresse IP de test. L'accès inverse n'est cependant pas disponible. Une connexion Internet depuis le serveur de restauration dans le réseau de test est disponible si l'option **Accès Internet** a été choisie lors de la création du serveur de restauration.
- **Adresse IP publique** (facultatif) : une adresse IP permettant d'accéder au serveur de restauration depuis Internet. Si un serveur ne possède pas d'adresse IP publique, vous pouvez y accéder uniquement depuis le réseau local.
- **Accès Internet** (facultatif) : elle permet au serveur de restauration d'accéder à Internet (aussi bien dans les cas de basculement test qu'en production).

Adresse IP publique et de test

Si vous affectez l'adresse IP publique lors de la création d'un serveur de restauration, celui-ci devient disponible depuis Internet via cette adresse IP. Lorsqu'un paquet provenant d'Internet contient l'adresse IP publique de destination, la passerelle VPN le remappe à l'adresse IP de production associée en utilisant NAT, puis l'envoie au serveur de restauration correspondant.



Si vous affectez l'adresse IP test lors de la création d'un serveur de restauration, celui-ci devient disponible dans le réseau de test via cette adresse IP. Lorsque vous effectuez le basculement test, la machine d'origine fonctionne toujours pendant que le serveur de restauration doté de la même adresse IP est lancé en même temps dans le Cloud. Il n'existe aucun conflit d'adresse IP, car le réseau de test est isolé. Les serveurs de restauration du réseau de test sont accessibles avec leur adresse IP test, qui est remappée aux adresses IP de production via NAT.



Pour plus d'informations à propos de l'Open VPN de site à site, consultez "OpenVPN de site à site – Informations complémentaires" (p. 195).

Serveurs primaires

Un **serveur primaire** : une machine virtuelle qui ne possède pas d'ordinateur associé sur le site local, par rapport à un serveur de restauration. Les serveurs primaires servent à protéger une application par réplication, ou à exécuter divers services auxiliaires (tels qu'un serveur Web).

Généralement, un serveur primaire est utilisé pour la réplication des données en temps réel entre des serveurs exécutant des applications cruciales. Vous configurez vous-même la réplication à l'aide des outils natifs de l'application. Par exemple, la réplication Active Directory ou la réplication SQL peuvent être configurées entre les serveurs locaux et le serveur primaire.

Un serveur primaire peut également être inclus dans un groupe AlwaysOn Availability Group (AAG) ou dans un groupe de disponibilité de la base de données (DAG).

Ces méthodes nécessitent toutes les deux une connaissance approfondie de l'application, ainsi que les droits d'administrateur correspondants. Un serveur primaire consomme en continu des ressources de calcul et de l'espace sur le stockage rapide pour reprise d'activité après sinistre. Il nécessite une maintenance de votre côté : suivi de la réplication, installation des mises à jour logicielles et sauvegarde. Les avantages sont des RTO et RPO minimales, avec une faible charge sur l'environnement de production (comparé à la sauvegarde de serveurs entiers dans le Cloud).

Les serveurs primaires sont toujours lancés uniquement dans le réseau de production et possèdent les paramètres réseau suivants :

- **Réseau Cloud** (obligatoire) : un réseau Cloud auquel un serveur primaire sera connecté.
- **Adresse IP dans le réseau de production** (obligatoire) : une adresse IP que le serveur primaire aura dans le réseau de production. Par défaut, la première adresse IP gratuite issue de votre réseau de production est définie.
- **Adresse IP publique** (facultatif) : une adresse IP permettant d'accéder au serveur primaire depuis Internet. Si un serveur ne possède pas d'adresse IP publique, vous pouvez y accéder uniquement depuis le réseau local, pas via Internet.
- **Connexion à Internet** (facultatif) : permet au serveur primaire d'accéder à Internet.

Connexion VPN IPsec multi-site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez utiliser la connectivité VPN IPsec multi-site pour connecter un site local ou plusieurs sites locaux à Cyber Disaster Recovery Cloud via une connexion VPN IPsec de couche 3 sécurisée.

Ce type de connectivité est utile pour les scénarios de reprise d'activité après sinistre avec les cas d'utilisation suivants :

- Vous disposez d'un site local hébergeant des ressources critiques.
- Vous disposez de plusieurs sites locaux hébergeant des ressources critiques, par exemple des bureaux à différents endroits.
- Vous utilisez des sites de logiciels tiers ou des sites de fournisseurs de services managés et vous êtes connectés à eux via un tunnel VPN IPsec.

Pour établir une communication VPN IPsec multi-site entre le site local et le site dans le Cloud, une **passerelle VPN** est utilisée. Lorsque vous commencez à configurer la connexion VPN IPsec multisite dans la console Cyber Protect, la passerelle VPN est déployée automatiquement sur le site dans le cloud. Vous devez configurer les segments réseau dans le Cloud et vous assurer qu'ils ne se chevauchent pas avec les segments réseau locaux. Un tunnel VPN sécurisé est établi entre les sites locaux et le site dans le Cloud. Les serveurs locaux et dans le Cloud peuvent communiquer via ce tunnel VPN comme s'ils se trouvaient tous dans le même segment Ethernet.

Pour chaque machine source à protéger, vous devez créer un serveur de restauration dans le site dans le Cloud. Il reste en mode **Veille** jusqu'à ce qu'un événement de basculement se produise. Si un sinistre se produit et que vous lancez un processus de basculement (en **mode production**), le serveur de restauration représentant la copie exacte de votre machine protégée est lancé dans le Cloud. Vos clients peuvent continuer à travailler avec le serveur, sans remarquer de changement de fond.

Vous pouvez également lancer un processus de basculement en **mode test**. Cela signifie que la machine source fonctionne toujours, et que le serveur de restauration associé doté de la même adresse IP est lancé en même temps dans le Cloud, dans un réseau privé spécial créé dans le

Cloud - **réseau test**. Le réseau test est isolé pour éviter la duplication des adresses IP dans les autres segments de réseau Cloud.

Passerelle VPN

La **passerelle VPN** est le composant majeur qui permet la communication entre les sites locaux et le site dans le Cloud. Il s'agit d'une machine virtuelle dans le Cloud sur laquelle le logiciel spécial est installé et le réseau spécifiquement installé. La passerelle VPN a les fonctions suivantes :

- Connecte les segments Ethernet de votre réseau local et de votre réseau de production dans le Cloud en mode IPsec de couche 3.
- Agit comme routeur et NAT par défaut pour les ordinateurs des réseaux de test et de production.
- Agit comme serveur DHCP. Toutes les machines des réseaux de production et de test doivent obtenir la configuration réseau (adresses IP, paramètres DNS) via DHCP. À chaque fois, un serveur Cloud obtiendra la même adresse IP auprès du serveur DHCP.

  Si vous préférez, vous pouvez définir une configuration DNS personnalisée. Pour plus d'informations, voir "Configuration de serveurs DNS personnalisés" (p. 810).
- Agit comme DNS de mise en cache.

Fonctionnement du routage

Le routage entre les réseaux dans le Cloud est effectué avec le routeur sur le site Cloud, afin que les serveurs des différents réseaux Cloud puissent communiquer les uns avec les autres.

Accès VPN à distance de point à site

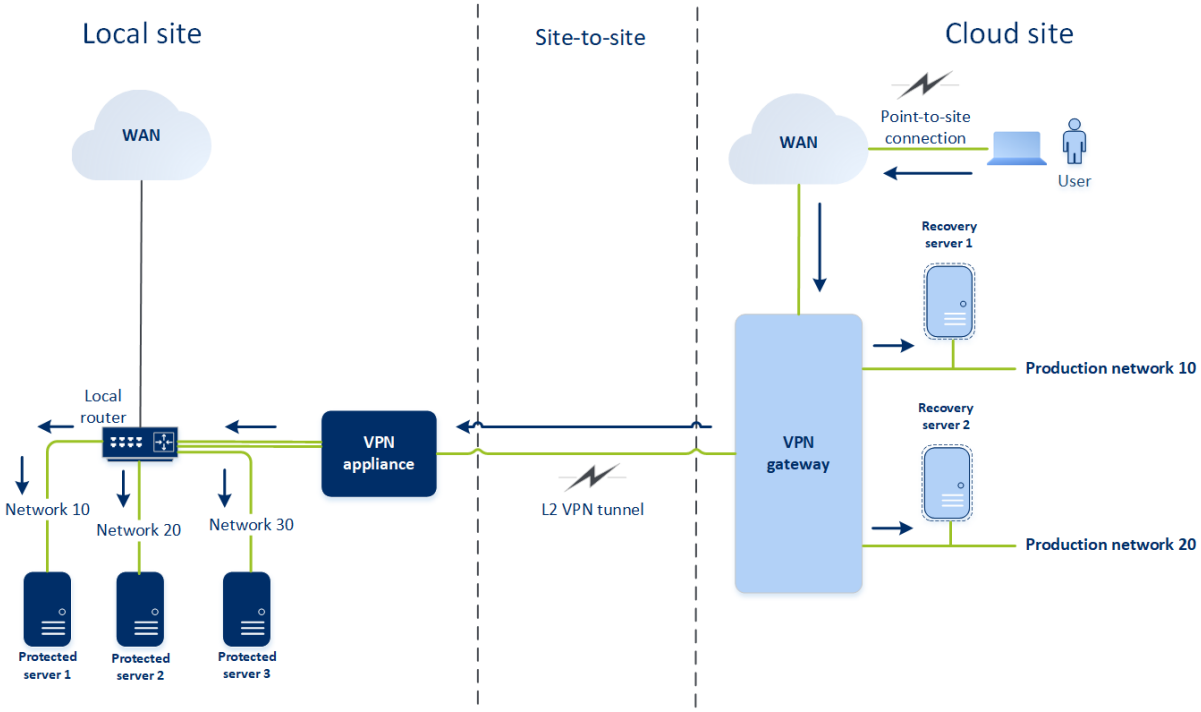
Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Une connexion de point à site est une connexion sécurisée extérieure à l'aide de vos terminaux (comme un ordinateur de bureau ou un ordinateur portable) vers le site dans le Cloud et les sites locaux via VPN. Elle est disponible après avoir établi une connexion OpenVPN de site à site au site Cyber Disaster Recovery Cloud. Ce type de connexion est utile dans les situations suivantes :

- Dans de nombreuses sociétés, les services d'entreprise et les ressources Web ne sont disponibles que sur le réseau d'entreprise. La connexion de point à site vous permet de vous connecter de façon sécurisée au site local.
- En cas de sinistre, lorsqu'une ressource bascule vers le site dans le Cloud et que votre réseau local est en panne, il se peut que vous deviez accéder directement à vos serveurs Cloud. Cela est possible via la connexion de point à site au site dans le Cloud.

Pour la connexion de point à site au site local, vous devez installer l'appliance VPN sur le site local, configurer la connexion site à site, puis la connexion de point à site au site local. Ainsi, vos employés travaillant à distance auront accès au réseau d'entreprise via le VPN de couche 2.

Le schéma ci-dessous montre le site local, le site dans le Cloud et les communications entre les serveurs surlignées en vert. Le tunnel VPN L2 relie vos sites locaux et dans le Cloud. Quand un utilisateur établit une connexion de point à site, les communications vers le site local sont réalisées par l'intermédiaire du site dans le Cloud.



La configuration de point à site utilise des certificats pour s'authentifier auprès du client VPN. Les autres identifiants utilisateur servent à l'authentification. Prenez connaissance des informations suivantes concernant la connexion de point à site au site local :

- Les utilisateurs doivent utiliser leurs identifiants Cyber Protect Cloud pour s'authentifier sur le client VPN. Ils doivent avoir le rôle utilisateur « Administrateur d'entreprise » ou « Cyberprotection ».
- Si vous avez régénéré la configuration OpenVPN, vous devez fournir la configuration mise à jour à tous les utilisateurs qui utilisent la connexion de point à site pour accéder au site dans le Cloud.

Suppression automatique des environnements clients non utilisés sur un site dans le Cloud

Le service Reprise d'activité après sinistre suit l'utilisation des environnements client créés à des fins de reprise après sinistre, et les supprime automatiquement s'ils ne sont pas utilisés.

Les critères suivants permettent de définir si le tenant client est actif :

- Au moins un serveur Cloud est actuellement présent, ou un ou plusieurs serveurs Cloud étaient présents au cours des sept derniers jours.
  OU

- L'option **Accès VPN au site local** est activée et soit le tunnel OpenVPN site à site est établi, soit des données en provenance de l'appliance VPN ont été signalées au cours des 7 derniers jours.

Les autres tenants restants sont considérés comme des tenants inactifs. Pour ces tenants, le système effectue les opérations suivantes :

- La passerelle VPN et toutes les ressources Cloud liées à ce tenant sont supprimées.
- L'enregistrement de l'appliance VPN est annulé.

Les tenants inactifs sont ramenés à leur état antérieur à la configuration de la connectivité.

Configuration de la connectivité initiale

Cette section décrit les scénarios de configuration de la connectivité.

Configuration du mode « sur Cloud uniquement »

Pour configurer une connexion dans le mode « sur Cloud uniquement »

1. Dans la console Cyber Protect, accédez à **Reprise d'activité après sinistre** > **Connectivité**.
2. Sélectionnez **Cloud uniquement** et cliquez sur **Configurer**.
   En conséquence, la passerelle VPN et le réseau Cloud contenant l'adresse et le masque définis seront déployés sur le site dans le Cloud.

Pour découvrir comment gérer vos réseaux dans le Cloud et configurer les paramètres de la passerelle VPN, consultez la section « Gérer les réseaux Cloud ».

Configuration OpenVPN de site à site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Exigences relatives à l'appliance VPN

Configuration requise

- 1 processeur
- 1 Go de RAM
- 8 Go d'espace disque

Ports

- TCP 443 (sortant) : pour la connexion VPN
- TCP 80 (sortant) : pour la mise à jour automatique de l'application

Assurez-vous que vos pare-feux et les autres composants de votre système de sécurité réseau autorisent les connexions sur ces ports vers n'importe quelle adresse IP.

Configuration d'une connexion OpenVPN de site à site

L'appliance VPN étend votre réseau local au Cloud via un tunnel VPN sécurisé. Ce type de connexion est souvent appelé connexion de « site à site » (S2S). Vous pouvez suivre la procédure ci-dessous ou regarder le tutoriel vidéo.

Pour configurer une connexion via l'appliance VPN

1. Dans la console Cyber Protect, accédez à **Reprise d'activité après sinistre** > **Connectivité**.
2. Sélectionnez **Connexion OpenVPN de site à site**, puis cliquez sur **Configurer**.
   Le système commence à déployer la passerelle VPN dans le Cloud. Cela peut prendre un certain temps. En attendant, vous pouvez passer à l'étape suivante.

   Remarque
   La passerelle VPN est fournie sans frais supplémentaires. Elle sera supprimée si la fonctionnalité de reprise d'activité après sinistre n'est pas utilisée, c'est-à-dire si aucun serveur primaire ni serveur de restauration n'est présent dans le Cloud pendant sept jours.

3. Dans le bloc **appliance VPN**, cliquez sur **Télécharger et déployer**. En fonction de la plate-forme de virtualisation que vous utilisez, téléchargez l'appliance VPN pour VMware vSphere ou Microsoft Hyper-V.
4. Déployez le matériel et connectez-le aux réseaux de production.
   Dans vSphere, vérifiez que le **mode Promiscuité** et l'option **Fausses transmissions** sont activés et configurés sur **Accepter** pour tous les commutateurs virtuels qui connectent l'appliance VPN aux réseaux de production. Pour accéder à ces paramètres, dans vSphere Client, sélectionnez l'hôte > **Résumé** > **Réseau**, puis sélectionnez le commutateur > **Modifier les paramètres...** > **Sécurité**.
   Dans Hyper-V, créez une machine virtuelle **Génération 1** avec 1 024 Mo de mémoire. Nous vous recommandons également d'activer la **mémoire dynamique** de l'ordinateur. Une fois la machine créée, accédez à **Paramètres** > **Matériel** > **Adaptateur réseau** > **Fonctionnalités avancées** et activez la case à cocher **Activer l'usurpation des adresses MAC**.
5. Démarrez l'application.
6. Ouvrez la console de l'application et connectez-vous à l'aide du nom d'utilisateur et du mot de passe « admin/admin ».
7. [Facultatif] Modifiez le mot de passe.
8. [Facultatif] Modifiez les paramètres réseau au besoin. Définissez l'interface qui sera utilisée comme WAN pour la connexion Internet.
9. Enregistrez le matériel dans le service Cyber Protection à l'aide des identifiants de l'administrateur de l'entreprise.
   Ces identifiants ne sont utilisés qu'une seule fois pour récupérer le certificat. L'URL du centre de données est prédéfinie.

Remarque
Si l'authentification à deux facteurs est configurée pour votre compte, vous serez également invité à saisir le code TOTP. Si l'authentification à deux facteurs est activée, mais pas configurée pour votre compte, vous ne pouvez pas enregistrer votre appliance VPN. Vous devez d'abord accéder à la page de connexion de la console Cyber Protect et terminer la configuration de l'authentification à deux facteurs pour votre compte. Pour en savoir plus sur l'authentification à deux facteurs, accédez au Guide de l'administrateur du portail de gestion.

Une fois la configuration terminée, l'application affiche le statut **En ligne**. Le matériel se connecte à la passerelle VPN et commence à communiquer des informations concernant les réseaux de toutes les interfaces actives au service Cyber Disaster Recovery Cloud. La console Cyber Protect affiche les interfaces en fonction des informations de l'appliance VPN.

Configuration d'un VPN IPsec multi-site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez configurer une connexion VPN IPsec multi-site de deux manières différentes :

- depuis l'onglet **Reprise d'activité après sinistre** > **Connectivité**.
- en appliquant un plan de protection sur ou un plusieurs terminaux, puis en basculant manuellement de la connexion OpenVPN site à site vers une connexion VPN IPsec multi-site, en configurant les paramètres du VPN IPsec multi-site et en réaffectant les adresses IP.

Pour configurer une connexion VPN IPsec multi-site depuis l'onglet Connectivité.

1. Dans la console Cyber Protect, accédez à **Reprise d'activité après sinistre** > **Connectivité**.
2. Dans la section **Connexion VPN multi-site**, cliquez sur **Configurer**.
   Une passerelle VPN est déployée sur le site dans le Cloud.
3. Configurez les paramètres du VPN IPsec multi-site.

Pour configurer une connexion VPN IPsec multi-site depuis un plan de protection

1. Dans la console Cyber Protect, accédez à **Terminaux**.
2. Appliquez un plan de protection à un ou plusieurs terminaux dans la liste.
   Les paramètres du serveur de restauration et de l'infrastructure Cloud sont automatiquement configurés pour la connectivité OpenVPN site à site.
3. Accédez à **Reprise d'activité après sinistre** > **Connectivité**.
4. Cliquez sur **Afficher les propriétés**.
5. Cliquez sur **Basculer sur un VPN IPsec multi-site**.
6. Configurez les paramètres du VPN IPsec multi-site.
7. Réaffectez les adresses IP du réseau Cloud et des serveurs dans le Cloud.

Configuration des paramètres du VPN IPsec multi-site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Une fois que vous avez configuré un VPN IPsec multi-site, vous devez configurer les paramètres du site dans le Cloud et des sites locaux dans l'onglet **Reprise d'activité après sinistre** > **Connectivité**.

Prérequis

- La connectivité VPN IPsec multi-site est configurée. Pour plus d'informations sur la configuration de la connectivité VPN IPsec multisite, reportez-vous à "Configuration d'un VPN IPsec multi-site" (p. 795).
- Chaque passerelle VPN IPsec locale a une adresse IP publique.
- Votre réseau Cloud dispose d'un nombre suffisant d'adresses IP pour les serveurs Cloud qui sont des copies de vos machines protégées (dans le réseau de production) et pour les serveurs de restauration (avec une ou deux adresses IP selon vos besoins).
- [Si vous utilisez un pare-feu entre les sites locaux et le site dans le cloud] Les protocoles IP et les ports UDP suivants sont autorisés sur les sites locaux : ID de protocole IP 50 (ESP), Port UDP 500 (IKE) et Port UDP 4500.
- La configuration NAT-T sur les sites locaux est désactivée.

Pour configurer une connexion VPN IPsec multi-site

1. Ajoutez un ou plusieurs réseaux au site dans le Cloud.
   a. Cliquez sur **Ajouter un réseau**.

      Remarque
      Lorsque vous ajoutez un réseau dans le Cloud, un réseau de test correspondant sera ajouté automatiquement à la même adresse et au même masque de réseau pour effectuer des basculements tests. Les serveurs Cloud dans le réseau test auront les mêmes adresses IP que dans le réseau de production dans le Cloud. Si vous avez besoin d'accéder à un serveur Cloud depuis le réseau de production pendant un basculement test, attribuez-lui une seconde adresse IP test lorsque vous créez le serveur de restauration.

   b. Dans le champ **Adresse réseau**, tapez l'adresse IP du réseau.
   c. Dans le champ **Masque réseau**, tapez le masque du réseau.
   d. Cliquez sur **Ajouter**.
2. Configurez les paramètres pour chaque site local que vous souhaitez connecter au site dans le Cloud, en suivant les recommandations pour les sites locaux. Pour plus d'informations sur ces recommandations, reportez-vous à "Recommandations générales pour les sites locaux" (p. 797).

a. Cliquez sur **Ajouter une connexion**.

b. Saisissez un nom pour la passerelle VPN locale.

c. Entrez l'adresse IP publique de la passerelle VPN locale.

d. [Facultatif] Saisissez une description de la passerelle VPN locale.

e. Cliquez sur **Suivant**.

f. Dans le champ **Clé prépartagée**, tapez la clé prépartagée, ou cliquez sur **Générer une nouvelle clé prépartagée** pour utiliser une valeur générée automatiquement.

Remarque
Vous devez utiliser la même clé prépartagée pour les passerelles VPN locales et dans le Cloud.

g. Cliquez sur **Paramètres de sécurité IPsec/IKE** pour les configurer. Pour plus d'informations sur les paramètres que vous pouvez configurer, reportez-vous à "Paramètres de sécurité IPsec/IKE" (p. 798).

Remarque
Vous pouvez utiliser les paramètres par défaut, qui sont remplis automatiquement, ou utiliser des valeurs personnalisées. Seules les connexions de protocole IKEv2 sont prises en charge. L'**Action de démarrage** par défaut lors de l'établissement du VPN est **Ajouter** (votre passerelle VPN locale démarre la connexion), mais vous pouvez la modifier en **Démarrer** (la passerelle VPN dans le Cloud démarre la connexion) ou **Route** (adaptée pour les pare-feux qui prennent en charge les options de routage).

h. Configurez les **Politiques réseau**.
Les politiques réseau spécifient les réseaux auxquels se connecte le VPN IPsec. Tapez l'adresse IP et le masque du réseau au format CIDR. Les segments réseau locaux et dans le Cloud ne doivent pas se chevaucher.

i. Cliquez sur **Enregistrer**.

Recommandations générales pour les sites locaux

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Lorsque vous configurez les sites locaux pour votre connectivité VPN IPsec multi-site, tenez compte des recommandations suivantes :

- Pour chaque phase d'IKE, définissez les paramètres suivants pour au moins une des valeurs configurées sur le site dans le Cloud : Algorithme de chiffrement, algorithme de hachage et numéros de groupes Diffie-Hellman.
- Activez la confidentialité persistante avec au moins une des valeurs pour les numéros de groupes Diffie-Hellman configurée sur le site dans le Cloud pour la phase 2 d'IKE.

- Configurez la même valeur **Durée de vie** que celle du site dans le cloud pour les phases 1 et 2 d'IKE.
- Les configurations avec NAT-T (NAT trasversal) ne sont pas prises en charge. Désactivez la configuration NAT-T sur le site local. Dans le cas contraire, aucune autre encapsulation UDP ne peut être négociée.
- La configuration **Action de démarrage** définit le côté où démarre la connexion. La valeur par défaut **Ajouter** signifie que le site local démarre la connexion et que le site dans le Cloud attend le démarrage de la connexion. Modifier la valeur sur **Démarrer** si vous souhaitez que le site dans le Cloud démarre la connexion ou sur **Route** si vous souhaitez que les deux côtés soient capables de démarrer la connexion (cette option est adaptée pour les pare-feux compatibles avec l'option de routage).

Pour en savoir plus et obtenir des exemples de configuration pour différentes solutions, consultez :

- Cette série d'articles de la base de connaissances
- Cet exemple de vidéo

Paramètres de sécurité IPsec/IKE

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Le tableau suivant fournit plus de détails sur les paramètres de sécurité IPsec/IKE.

Paramètre	Description
Algorithme de chiffrement	L'algorithme de chiffrement qui sera utilisé pour s'assurer que les données ne peuvent pas être consultées pendant leur transit. Par défaut, tous les algorithmes sont sélectionnés. Vous devez configurer au moins un des algorithmes sélectionnés sur votre terminal de passerelle local pour chaque phase d'IKE.
Algorithme de hachage	L'algorithme de hachage qui sera utilisé pour vérifier l'intégrité et l'authenticité des données. Par défaut, tous les algorithmes sont sélectionnés. Vous devez configurer au moins un des algorithmes sélectionnés sur votre terminal de passerelle local pour chaque phase d'IKE.
Numéros de groupes Diffie-Hellman	Les numéros de groupes Diffie-Hellman définissent la fiabilité de la clé utilisée dans le processus Internet Key Exchange (IKE). Les numéros de groupes plus élevés sont plus sécurisés, mais nécessitent un temps de calcul plus long pour la clé.

Paramètre	Description
	Par défaut, tous les groupes sont sélectionnés. Vous devez configurer au moins un des groupes sélectionnés sur votre terminal de passerelle local pour chaque phase d'IKE.
Durée de vie (secondes)	La valeur de Durée de vie détermine la durée d'une instance de connexion avec un ensemble de clés de chiffrement/d'authentification pour les paquets utilisateur, de la négociation réussie à l'expiration. Plage pour la phase 1 : 900-28 800 secondes avec par défaut 28 800. Plage pour la phase 2 : 900-3 600 secondes avec par défaut 3 600. La durée de vie de la phase 2 doit être inférieure à celle de la phase 1. La connexion est renégociée via le canal de clés avant son expiration, voir **Durée de marge du changement de clé**. Si une divergence de durée de vie a lieu entre le site local et le site distant, un encombrement de connexions substituées se produira du côté où la durée de vie est la plus longue. Voir aussi **Durée de marge du changement de clé** et **Fuzz du changement de clé**.
Durée de marge du changement de clé (secondes)	La durée de marge avant l'expiration de la connexion ou l'expiration du canal de changement de clé, au cours de laquelle le côté local de la connexion VPN essaie de négocier un remplacement. L'heure exacte du changement de clé est sélectionnée aléatoirement en fonction de la valeur de **Fuzz du changement de clé**. Pertinent uniquement au niveau local, le côté à distance n'a pas besoin de l'accepter. Plage : 900 à 3 600 secondes. La valeur par défaut est 3 600.
Taille de la fenêtre de réexécution (paquets)	La taille de la fenêtre de réexécution IPsec pour cette connexion. La valeur par défaut -1 utilise la valeur configurée avec charon.replay_window dans le fichier strongswan.conf. Les valeurs supérieures à 32 sont prises en charge uniquement lors de l'utilisation du back-end

Paramètre	Description
	Netlink. Une valeur de 0 désactive la protection contre les attaques par rejeu d'IPsec.
Fuzz du changement de clé (%)	Le pourcentage maximum pour lequel les valeurs marginbytes, marginpackets et margintime sont augmentées aléatoirement pour randomiser les intervalles de changement de clé (primordial pour les hôtes avec de nombreuses connexions). La valeur fuzz du changement de clé peut dépasser 100 %. La valeur de marginTYPE, après l'augmentation aléatoire, ne doit pas dépasser celle de lifeTYPE, où TYPE correspond à Octets, Paquets ou Heure. La valeur 0 % annule la randomisation. Pertinent uniquement au niveau local, le côté à distance n'a pas besoin de l'accepter.
Expiration du délai d'attente DPD (secondes)	Durée après laquelle une expiration du délai d'attente de la fonction Dead peer detection (DPD) se produit. Vous pouvez spécifier la valeur 30 ou une valeur supérieure. La valeur par défaut est 30.
Action d'expiration du délai d'attente de la fonction Dead peer detection (DPD)	L'action à effectuer après l'expiration du délai d'attente de la fonction dead peer detection (DPD). **Redémarrer** : redémarrage de la session lors de l'expiration du délai d'attente DPD. **Effacer** : fin de la session lors de l'expiration du délai d'attente DPD. **Aucun** : aucune action lors de l'expiration du délai d'attente DPD.
Action de démarrage	Détermine quel côté démarre la connexion et établit le tunnel pour la connexion VPN. **Ajouter** : votre passerelle VPN locale démarre la connexion. **Démarrer** : la passerelle VPN dans le Cloud démarre la connexion. **Route** : option adaptée aux passerelles VPN compatibles avec l'option de routage. Le tunnel est activé uniquement quand il y a un trafic provenant de la passerelle VPN locale ou la passerelle VPN dans le Cloud.

Recommandations pour la disponibilité des services de domaine Active Directory

Si vos ressources protégées ont besoin d'une authentification dans un contrôleur de domaine, nous vous recommandons de disposer d'une instance de contrôleur de domaine Active Directory sur le site de reprise d'activité après sinistre.

Contrôleur de domaine Active Directory pour la connectivité OpenVPN de couche 2

Avec la connectivité OpenVPN de couche 2, les adresses IP des ressources protégées sont conservées sur le site dans le Cloud lors d'un basculement test ou d'un basculement de la production. Par conséquent, lors d'un basculement test ou d'un basculement de la production, le contrôleur de domaine Active Directory possède la même adresse IP que dans le site local.

Grâce aux DNS personnalisés, vous pouvez définir votre propre serveur DNS personnalisé pour tous les serveurs Cloud. Pour plus d'informations, voir "Configuration de serveurs DNS personnalisés" (p. 810).

Contrôleur de domaine Active Directory pour la connectivité VPN IPsec de couche 3

Avec la connectivité VPN IPsec de couche 3, les adresses IP des ressources protégées ne sont pas conservées sur le site dans le Cloud. Par conséquent, nous vous recommandons de disposer d'une instance de contrôleur de domaine Active Directory supplémentaire en tant que serveur primaire sur le site dans le Cloud avant d'effectuer un basculement de la production.

Les recommandations pour une instance de contrôleur de domaine Active Directory dédiée et configurée en tant que serveur primaire sur le site dans le Cloud sont les suivantes :

- Désactivez le pare-feu Windows.
- Associez le serveur primaire au service Active Directory.
- Assurez-vous que le serveur primaire dispose d'un accès à Internet.
- Ajoutez la fonctionnalité Active Directory.

Grâce aux DNS personnalisés, vous pouvez définir votre propre serveur DNS personnalisé pour tous les serveurs Cloud. Pour plus d'informations, voir "Configuration de serveurs DNS personnalisés" (p. 810).

Configuration de l'accès VPN à distance de point à site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Si vous devez vous connecter à distance à votre site local, vous pouvez configurer la connexion de point à site au site local. Vous pouvez suivre la procédure ci-dessous ou regarder le tutoriel vidéo.

Prérequis

- Une connectivité OpenVPN de site à site est configurée.
- L'appliance VPN est installée sur le site local.

Pour configurer la connexion de point à site au site local

1. Dans la console Cyber Protect, accédez à **Reprise d'activité après sinistre** > **Connectivité**.
2. Cliquez sur **Afficher les propriétés**.
3. Activez l'option **Accès VPN au site local**.
4. Assurez-vous que l'utilisateur qui doit établir la connexion de point à site au site local dispose des éléments suivants :
   - Un compte utilisateur dans Cyber Protect Cloud. Les autres identifiants utilisateur servent à l'authentification dans le client VPN. Sinon, créez un compte utilisateur dans Cyber Protect Cloud.
   - Un rôle utilisateur « Administrateur d'entreprise » ou « Cyberprotection ».
5. Configurer le client OpenVPN :
   a. Téléchargez le client OpenVPN v2.4.0 ou version ultérieure depuis l'emplacement suivant https://openvpn.net/community-downloads/.
   b. Installez le client OpenVPN sur la machine que vous souhaitez connecter au site local.
   c. Cliquez sur **Télécharger la configuration pour OpenVPN**. Le fichier de configuration est valide pour les utilisateurs de votre organisation possédant le rôle utilisateur « Administrateur d'entreprise » ou « Cyberprotection ».
   d. Importez la configuration téléchargée dans OpenVPN.
   e. Connectez-vous au client OpenVPN grâce à vos identifiants utilisateur Cyber Protect Cloud (voir l'étape 4 ci-dessus).
   f. [Facultatif] Si l'authentification à deux facteurs est activée pour votre organisation, alors vous devez fournir le code TOTP unique généré.

Important
Si vous activez l'authentification à deux facteurs pour votre compte, vous devez régénérer le fichier de configuration et le renouveler pour vos clients OpenVPN existants. Les utilisateurs doivent se reconnecter à Cyber Protect Cloud pour configurer l'authentification à deux facteurs pour leur compte.

Ainsi, votre utilisateur pourra se connecter à des machines sur le site local.

Gestion du réseau

Cette section décrit les scénarios de gestion des réseaux.

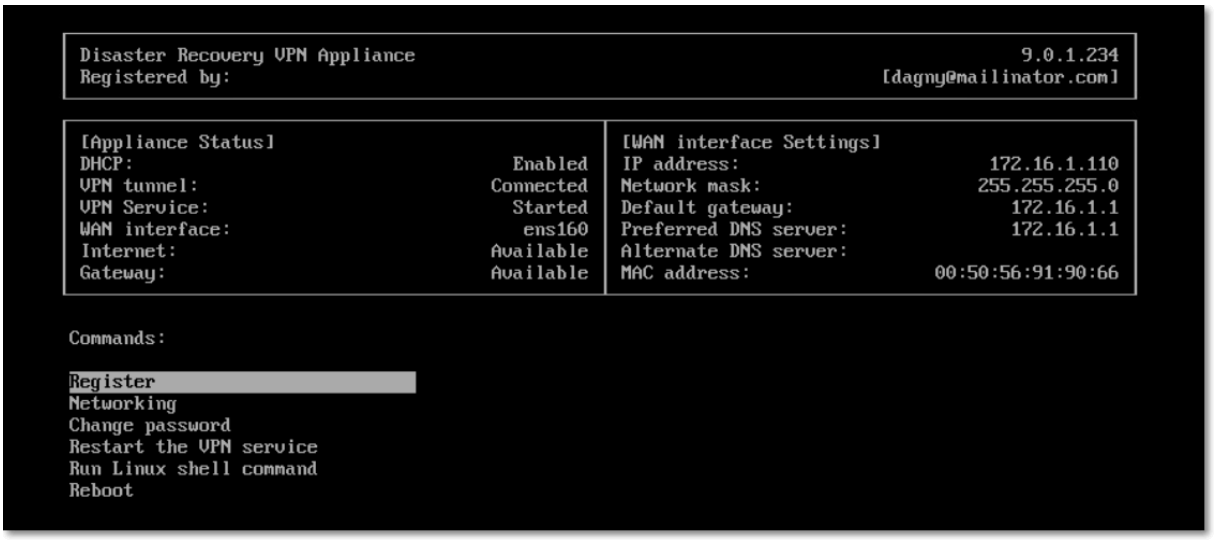
Gestion des réseaux

Remarque
Certaines fonctionnalités peuvent nécessiter une licence supplémentaire, en fonction du modèle de gestion de licences appliqué.

Connexion OpenVPN de site à site

Pour ajouter un réseau sur le site local et l'étendre au Cloud

1. Sur le matériel VPN, configurez la nouvelle interface réseau avec le réseau local que vous souhaitez étendre dans le Cloud.
2. Connectez-vous à la console du matériel VPN.
3. Dans la section **Réseau**, configurez les paramètres réseau de la nouvelle interface.



Le matériel VPN commence à communiquer des informations concernant les réseaux de toutes les interfaces actives à Cyber Disaster Recovery Cloud. La console Cyber Protect affiche les interfaces en fonction des informations de l'appliance VPN.

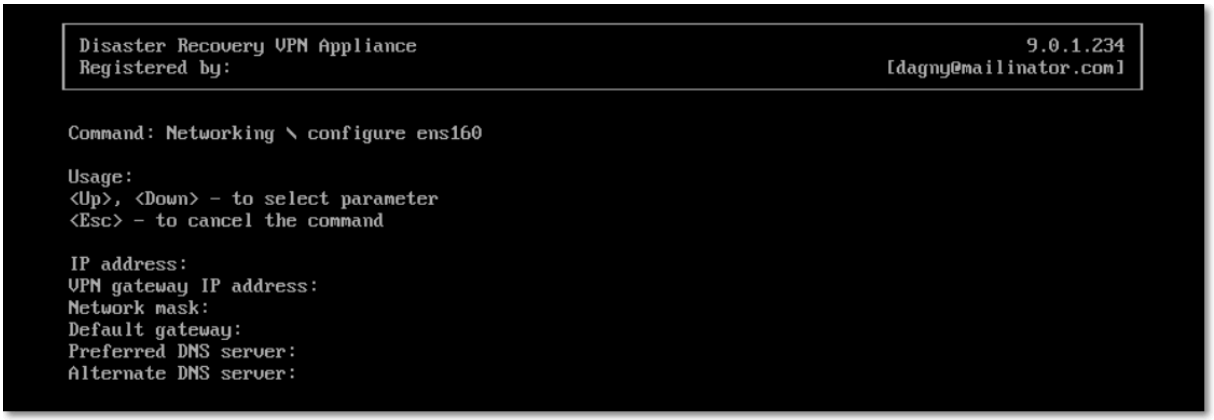
Pour supprimer un réseau étendu au Cloud

1. Connectez-vous à la console du matériel VPN.
2. Dans la section **Réseau**, sélectionnez l'interface que vous souhaitez supprimer, puis cliquez sur **Effacer les paramètres réseau**.
3. Confirmez l'opération.

Par conséquent, l'extension du réseau local au Cloud via un tunnel VPN sécurisé sera arrêtée. Le réseau fonctionnera en tant que segment Cloud indépendant. Si cette interface est utilisée pour faire passer le trafic depuis (vers) le site dans le Cloud, toutes vos connexions réseau depuis (vers) le site dans le Cloud seront déconnectées.

Pour changer les paramètres réseau

1. Connectez-vous à la console du matériel VPN.
2. Dans la section **Réseau**, sélectionnez l'interface que vous souhaitez modifier.
3. Cliquez sur **Modifier les paramètres réseau**.
4. Sélectionnez l'une des deux options suivantes :
   - Pour une configuration automatique du réseau via DHCP, cliquez sur **Utiliser DHCP**. Confirmez l'opération.
   - Pour une configuration manuelle du réseau, cliquez sur **Définir une adresse IP statique**. Les paramètres suivants peuvent être modifiés :
     - **Adresse IP** : adresse IP de l'interface dans le réseau local.
     - **Adresse IP de la passerelle VPN** : adresse IP spéciale réservée au segment de Cloud du réseau pour le bon fonctionnement du service Cyber Disaster Recovery Cloud.
     - **Masque réseau** : masque réseau du réseau local.
     - **Passerelle par défaut** : passerelle par défaut sur le site local.
     - **Serveur DNS préféré** : serveur DNS principal sur le site local.
     - **Serveur DNS alternatif** : serveur DNS secondaire sur le site local.



- Effectuez les modifications nécessaires et confirmez-les en appuyant sur Entrée.

Mode « sur Cloud uniquement »

Vous pouvez avoir jusqu'à 23 réseaux dans le cloud.

Pour ajouter un nouveau réseau Cloud

1. Accédez à **Reprise d'activité après sinistre** > **Connectivité**.
2. Sous **Site dans le Cloud**, cliquez sur **Ajouter un réseau dans le Cloud**.
3. Définissez les paramètres du réseau Cloud : l'adresse et le masque du réseau. Lorsque vous avez terminé, cliquez sur **Terminé**.

En conséquence, le réseau Cloud supplémentaire contenant l'adresse et le masque définis seront créés dans le site dans le Cloud.

Pour supprimer un réseau Cloud

Remarque
Vous ne pouvez pas supprimer un réseau Cloud s'il contient au moins un serveur Cloud. Commencez par supprimer le serveur Cloud, puis supprimez le réseau.

1. Accédez à **Reprise d'activité après sinistre** > **Connectivité**.
2. Dans **Site dans le Cloud**, cliquez sur l'adresse réseau que vous souhaitez supprimer.
3. Cliquez sur **Supprimer** pour confirmer l'opération.

Pour modifier les paramètres réseau

1. Accédez à **Reprise d'activité après sinistre** > **Connectivité**.
2. Dans **Site dans le Cloud**, cliquez sur l'adresse réseau que vous souhaitez modifier.
3. Cliquez sur **Modifier.**
4. Définissez l'adresse et le masque du réseau, puis cliquez sur **Terminé**.

Reconfiguration d'une adresse IP

Pour obtenir de bonnes performances de la reprise d'activité après sinistre, les adresses IP attribuées aux serveurs locaux et dans le Cloud doivent être cohérentes. S'il existe la moindre incohérence ou incompatibilité dans les adresses IP, vous verrez le point d'exclamation à côté du réseau correspondant dans **Reprise d'activité après sinistre** > **Connectivité**.

Certains motifs connus d'incohérences d'adresses IP sont répertoriés ci-dessous :

1. Un serveur de restauration a été migré d'un réseau vers un autre, ou le masque du réseau ou le réseau Cloud a été modifié. En conséquence, les serveurs Cloud possèdent les adresses IP de réseaux auxquels ils ne sont pas connectés.
2. Le type de connectivité a été basculé de « sans connexion de site à site » à « connexion de site à site ». En conséquence, un serveur local est placé dans le réseau différent de celui ayant été créé pour le serveur de restauration dans le site dans le Cloud.
3. Le type de connectivité a été basculé de « OpenVPN de site à site » à « VPN IPsec multi-site » ou de « VPN IPsec multi-site » à « OpenVPN de site à site ». Pour plus d'informations sur ce scénario, consultez Basculement de connexions et Réaffectation d'adresses IP.
4. Modification des paramètres de réseau suivants sur le site du matériel VPN :
   - Ajout d'une interface via les paramètres du réseau
   - Modification manuelle du masque du réseau via les paramètres de l'interface
   - Modification du masque et de l'adresse du réseau via DHCP
   - Modification manuelle de l'adresse et du masque du réseau via les paramètres de l'interface
   - Modification du masque et de l'adresse du réseau via DHCP

   En conséquence des actions répertoriées ci-dessus, le réseau du site dans le Cloud peut devenir un sous-ensemble ou un super-ensemble du réseau local, ou l'interface du matériel VPN peut rapporter les mêmes paramètres réseau pour différentes interfaces.

Pour résoudre le problème à l'aide de paramètres réseau

1. Cliquez sur le réseau nécessitant la reconfiguration d'une adresse IP.
   Vous verrez une liste des serveurs dans le réseau sélectionné, leur statut et leur adresse IP. Les serveurs dont les paramètres réseau sont incohérents sont marqués par un point d'exclamation.
2. Pour modifier les paramètres réseau d'un serveur, cliquez sur **Accéder au serveur**. Pour modifier les paramètres réseau de tous les serveurs en même temps, cliquez sur **Modifier** dans le bloc de notification.
3. Modifiez les adresses IP au besoin en les définissant dans les champs **Nouvelle adresse IP** et **Nouvelle adresse IP test**.
4. Lorsque vous avez terminé, cliquez sur **Confirmer**.

Déplacer des serveurs vers un réseau approprié

Lorsque vous créez un plan de protection de reprise d'activité après sinistre et que vous l'appliquez aux terminaux sélectionnés, le système vérifie les adresses IP des terminaux et crée automatiquement des réseaux Cloud s'il n'existe pas de réseaux Cloud correspondant à l'adresse IP. Par défaut, les réseaux Cloud sont configurés avec les plages maximales recommandées par IANA pour un usage privé (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Vous pouvez restreindre la taille de votre réseau en modifiant le masque de réseau.

Dans le cas où les terminaux sélectionnés se trouvaient sur plusieurs réseaux locaux, le réseau sur le site dans le Cloud peut devenir un super-ensemble de réseaux locaux. Dans ce cas, pour reconfigurer les réseaux Cloud :

1. Cliquez sur le réseau Cloud qui requiert la reconfiguration de la taille du réseau, puis cliquez sur **Modifier**.
2. Reconfigurez la taille du réseau à l'aide des paramètres corrects.
3. Créez les autres réseaux requis.
4. Cliquez sur l'icône de notification à côté du nombre de terminaux connectés au réseau.
5. Cliquez sur **Déplacer vers un réseau approprié**.
6. Sélectionnez les serveurs que vous souhaitez déplacer, puis cliquez sur **Déplacer**.

Gestion des paramètres de l'appliance VPN

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Dans la console Cyber Protect (**Reprise d'activité après sinistre** > **Connectivité**), vous pouvez effectuer les actions suivantes :

- Télécharger les fichiers journaux
- Désinscrire le matériel (si vous devez réinitialiser les paramètres de l'appliance VPN ou basculer vers le mode « sur Cloud uniquement »)

Pour accéder à ces paramètres, cliquez sur l'icône **i** dans le bloc de **appliance VPN**.

Dans la console du matériel VPN, vous pouvez :

- Modifier le mot de passe de l'appliance
- Afficher/modifier les paramètres réseau et définir l'interface à utiliser comme WAN pour la connexion Internet
- Enregistrer/modifier le compte d'enregistrement (en répétant le processus d'enregistrement)
- Redémarrer le service VPN
- Redémarrer l'appliance VPN
- Exécuter la commande shell Linux (uniquement pour les cas de dépannage avancés)

Réinstallation de la passerelle VPN

En cas de problème de passerelle VPN que vous ne parvenez pas à résoudre, vous souhaiterez peut-être réinstaller la passerelle. Voici quelques problèmes possibles :

- La passerelle VPN est dans l'état **Erreur**.
- La passerelle VPN est dans l'état **En attente** depuis longtemps.
- La passerelle VPN est dans un état indéterminé depuis longtemps.

La réinstallation de la passerelle VPN comprend les actions automatiques suivantes : suppression totale de la machine virtuelle de la passerelle VPN existante ; installation d'une nouvelle machine virtuelle à partir du modèle et application des paramètres de la passerelle VPN précédente sur la nouvelle machine virtuelle.

Pré-requis :

Vous devez définir au moins un type de connectivité vers le site dans le Cloud.

Pour réinstaller la passerelle VPN

1. Dans la console Cyber Protect, accédez à **Reprise d'activité après sinistre** > **Connectivité**.
2. Cliquez sur l'icône en forme d'engrenage de la passerelle VPN, puis sélectionnez **Réinstaller la passerelle VPN**.
3. Dans la boîte de dialogue **Réinstaller la passerelle VPN**, saisissez votre identifiant.
4. Cliquez sur **Réinstaller**.

Activation et désactivation de la connexion de site à site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez activer la connexion de site à site dans les cas suivants :

- Si vous avez besoin que les serveurs Cloud du site dans le Cloud communiquent avec les serveurs du site local.

- Après un basculement vers le Cloud, l'infrastructure est restaurée et vous souhaitez restaurer automatiquement vos serveurs vers le site local.

Pour activer la connexion de site à site

1. Accédez à **Reprise d'activité après sinistre** > **Connectivité**.
2. Cliquez sur **Afficher les propriétés**, puis activez l'option **Connexion de site à site**.

En conséquence, la connexion VPN de site à site est activée entre les sites locaux et dans le Cloud. Le service Cyber Disaster Recovery Cloud obtient les paramètres réseau à partir du matériel VPN et étend les réseaux locaux au site dans le Cloud.

Si vous n'avez pas besoin que les serveurs Cloud du site dans le Cloud communiquent avec les serveurs du site local, vous pouvez désactiver la connexion de site à site.

Pour désactiver la connexion de site à site

1. Accédez à **Reprise d'activité après sinistre** > **Connectivité**.
2. Cliquez sur **Afficher les propriétés**, puis désactivez l'option **Connexion de site à site**.

En conséquence, le site local est déconnecté du site dans le Cloud.

Basculement du type de connexion de site à site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez facilement basculer d'une connexion OpenVPN de site à site à une connexion VPN IPsec multi-site, et vice-versa.

Lorsque vous basculez le type de connexion, les connexions VPN actives sont supprimées, mais les serveurs dans le Cloud et les configurations réseau sont préservés. Toutefois, vous devrez quand même réaffecter les adresses IP du réseau et des serveurs dans le Cloud.

Le tableau suivant compare les caractéristiques de base de la connexion OpenVPN de site à site et de la connexion VPN IPsec multi-site.

	Open VPN de site à site	VPN IPsec multi-site
Prise en charge de sites locaux	Site unique	Un ou plusieurs sites
Mode de passerelle VPN	L2 Open VPN	L3 IPsec VPN
Segments du réseau	Étend le réseau local au réseau dans le Cloud	Les segments réseau locaux et dans le Cloud ne doivent pas se chevaucher
Prise en charge de l'accès	Oui	Non

	Open VPN de site à site	VPN IPsec multi-site
point à site au site local		
Prise en charge de l'accès point à site au site dans le Cloud	Oui	Oui
Nécessite une offre d'IP publique	Non	Oui

Pour basculer d'une connexion OpenVPN de site à site à une connexion VPN IPsec multi-site

1. Dans la console Cyber Protect, accédez à **Reprise d'activité après sinistre** > **Connectivité**.
2. Cliquez sur **Afficher les propriétés**.
3. Cliquez sur **Basculer sur un VPN IPsec multi-site**.
4. Cliquez sur **Reconfigurer**.
5. Réaffectez les adresses IP du réseau Cloud et des serveurs dans le Cloud.
6. Configurez les paramètres de connexion IPsec multi-site.

Pour basculer d'une connexion VPN IPsec multi-site à une connexion OpenVPN de site à site

1. Dans la console Cyber Protect, accédez à **Reprise d'activité après sinistre** > **Connectivité**.
2. Cliquez sur **Afficher les propriétés**.
3. Cliquez sur **Basculer sur un OpenVPN de site à site**.
4. Cliquez sur **Reconfigurer**.
5. Réaffectez les adresses IP du réseau Cloud et des serveurs dans le Cloud.
6. Configurez les paramètres de connexion de site à site.

Réaffectation d'adresses IP

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous devez réaffecter les adresses IP des réseaux Clouds, ainsi que les serveurs Cloud, afin de terminer la configuration dans les cas suivants :

- Après être passé d'une connectivité OpenVPN de site à site à une connectivité VPN IPsec multi-site ou vice-versa.
- Après avoir appliqué un plan de protection (si la connectivité VPN IPsec multi-site est configurée).

Pour réaffecter l'adresse IP d'un réseau Cloud

1. Dans l'onglet **Connectivité**, cliquez sur l'adresse IP du réseau Cloud.
2. Dans la fenêtre contextuelle **Réseau**, cliquez sur **Modifier**.
3. Tapez la nouvelle adresse et le nouveau masque du réseau.
4. Cliquez sur **Valider**.

Une fois que vous avez réaffecté l'adresse IP d'un réseau Cloud, vous devez réaffecter les serveurs Cloud qui appartiennent au réseau Cloud réaffecté.

Pour réaffecter l'adresse IP d'un serveur

1. Dans l'onglet **Connectivité**, cliquez sur l'adresse IP du serveur dans le réseau Cloud.
2. Dans la fenêtre contextuelle **Serveurs**, cliquez sur **Changer l'adresse IP**.
3. Dans la fenêtre contextuelle **Changer l'adresse IP**, tapez la nouvelle adresse IP du serveur, ou utilisez l'adresse IP générée automatiquement et qui fait partie du réseau Cloud réaffecté.

   Remarque
   Cyber Disaster Recovery Cloud affecte automatiquement les adresses IP du réseau Cloud à tous les serveurs Cloud qui en font partie, avant la réaffectation de l'adresse IP du réseau. Vous pouvez vous servir des adresses IP suggérées pour réaffecter simultanément l'adresse IP de tous les serveurs Cloud.

4. Cliquez sur **Confirmer**.

Configuration de serveurs DNS personnalisés

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Lorsque vous configurez une connectivité, Cyber Disaster Recovery Cloud crée l'infrastructure de votre réseau Cloud. Le serveur DHCP Cloud assigne automatiquement les serveurs DNS par défaut aux serveurs de restauration et aux serveurs primaires, mais vous pouvez modifier les paramètres par défaut et configurer des serveurs DNS personnalisés. Les nouveaux paramètres DNS seront appliqués au moment de la prochaine demande au serveur DHCP.

Pré-requis :

Vous devez définir au moins un type de connectivité vers le site dans le Cloud.

Pour configurer un serveur DNS personnalisé

1. Dans la console Cyber Protect, accédez à **Reprise d'activité après sinistre** > **Connectivité**.
2. Cliquez sur **Afficher les propriétés**.
3. Cliquez sur **Par défaut (fourni par le site dans le Cloud)**.
4. Sélectionnez **Serveurs personnalisés**.

5. Saisissez l'adresse IP du serveur DNS.
6. [Facultatif] Si vous souhaitez ajouter un autre serveur DNS, cliquez sur **Ajouter**, puis saisissez l'adresse IP du serveur DNS.

   Remarque
   Une fois que vous avez ajouté les serveurs DNS personnalisés, vous pouvez aussi ajouter les serveurs DNS par défaut. De cette manière, si les serveurs DNS personnalisés sont indisponibles, Cyber Disaster Recovery Cloud utilisera les serveurs DNS par défaut.

7. Cliquez sur **Valider**.

Suppression de serveurs DNS personnalisés

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez supprimer des serveurs DNS à partir de la liste des DNS personnalisés.

Pré-requis :

Des serveurs DNS personnalisés sont configurés.

Pour supprimer un serveur DNS personnalisé

1. Dans la console Cyber Protect, accédez à **Reprise d'activité après sinistre** > **Connectivité**.
2. Cliquez sur **Afficher les propriétés**.
3. Cliquez sur **Serveurs personnalisés**.
4. Cliquez sur l'icône de suppression à côté du serveur DNS.

   Remarque
   L'option de suppression est désactivée lorsqu'un seul serveur DNS est disponible. Si vous souhaitez supprimer tous les serveurs DNS personnalisés, sélectionnez **Par défaut (fourni par le site dans le Cloud)**.

5. Cliquez sur **Valider**.

Configuration du routage local

En plus d'étendre vos réseaux locaux au Cloud via l'appliance VPN, vous pouvez posséder d'autres réseaux locaux qui ne sont pas enregistrés dans l'appliance VPN, mais qui possèdent des serveurs qui doivent communiquer avec les serveurs Cloud. Pour établir la connectivité entre ces serveurs locaux et les serveurs dans le Cloud, vous devez configurer les paramètres de routage local.

Pour configurer le routage local

1. Accédez à **Reprise d'activité après sinistre** > **Connectivité**.
2. Cliquez sur **Afficher les propriétés**, puis sur **Routage local**.
3. Indiquez les réseaux locaux dans la notation CIDR.
4. Cliquez sur **Enregistrer**.

En conséquence, les serveurs des réseaux locaux indiqués pourront communiquer avec les serveurs dans le Cloud.

Autoriser le trafic DHCP via un VPN de couche 2

Si des terminaux sur votre site local obtiennent leur adresse IP depuis un serveur DHCP, vous pouvez protéger le serveur DHCP à l'aide de la reprise d'activité après sinistre, le faire basculer vers le cloud, puis autoriser le trafic DHCP à passer par un VPN de couche 2. Ainsi, votre serveur DHCP fonctionnera dans le cloud, mais continuera à affecter des adresses IP à vos terminaux locaux.

Pré-requis :

Un type de connectivité site à site via un VPN de couche 2 doit être défini vers le site dans le cloud.

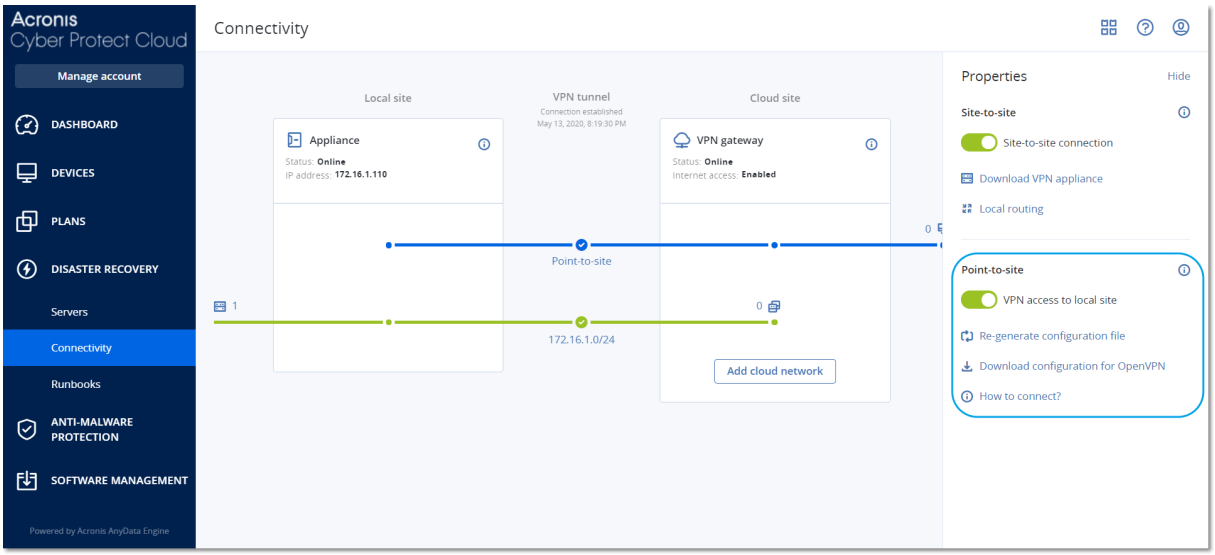
Pour autoriser le trafic DHCP à passer par la connexion VPN de couche 2

1. Accédez à **Reprise d'activité après sinistre** > onglet **Connectivité**.
2. Cliquez sur **Afficher les propriétés**.
3. Activez le commutateur **Autoriser le trafic DHCP via un VPN de couche 2**.

Gestion des paramètres de la connexion de point à site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Dans la console Cyber Protect, accédez à **Reprise d'activité après sinistre** > **Connectivité**, puis cliquez sur **Afficher les propriétés** en haut à droite.



Accès VPN au site local

Cette option est utilisée pour gérer l'accès VPN au site local. Par défaut, elle est activée. Si elle est désactivée, l'accès point à site au site local ne sera pas autorisé.

Téléchargez la configuration pour OpenVPN

Cela lancera le téléchargement du fichier de configuration pour le client OpenVPN. Ce fichier est requis pour établir une connexion de point à site vers le site dans le Cloud.

Régénération de la configuration

Vous pouvez générer à nouveau le fichier de configuration pour le client OpenVPN.

Cela est nécessaire dans les cas suivants :

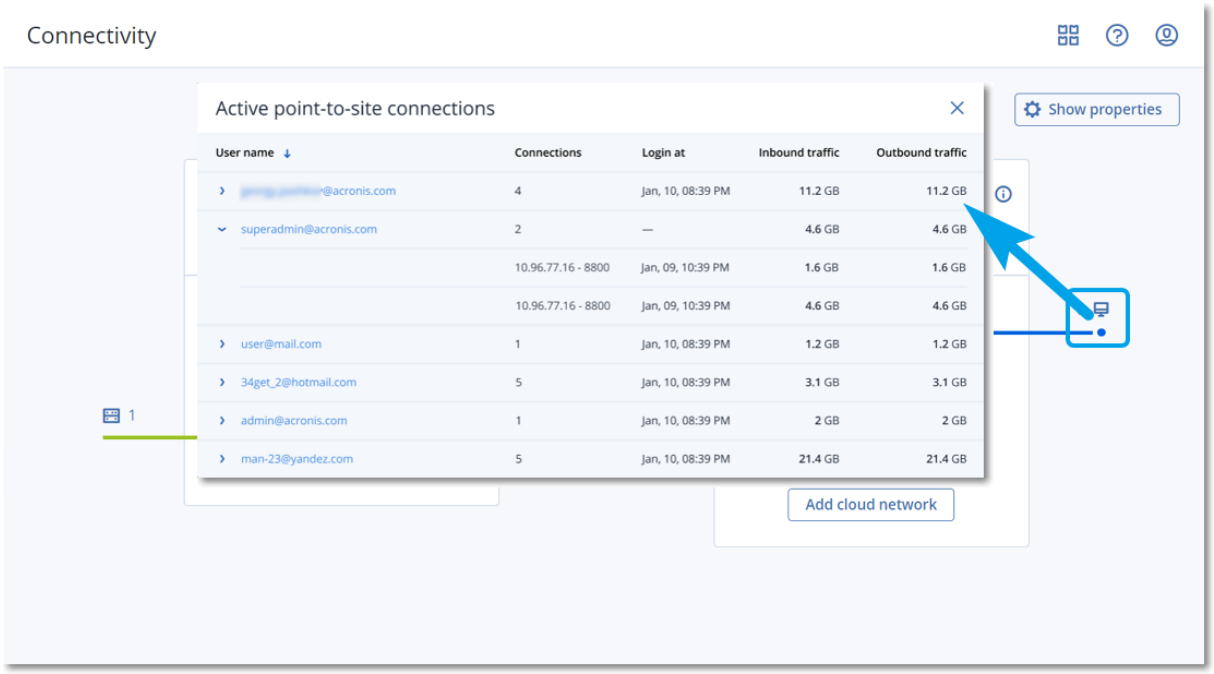
- Si vous pensez que le fichier de configuration est corrompu.
- L'authentification à deux facteurs a été activée pour votre compte.

Dès que le fichier de configuration est mis à jour, il n'est plus possible de se connecter à l'aide de l'ancien fichier de configuration. Veillez à fournir le nouveau fichier aux utilisateurs autorisés à utiliser la connexion de point à site.

Connexions de point à site actives

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez consulter toutes les connexions point à point actives dans **Reprise d'activité après sinistre** > **Connectivité**. Cliquez sur l'icône de la machine sur la ligne bleue **Point à site** et vous pourrez consulter les informations détaillées sur les connexions point-à-site actives, groupées par nom d'utilisateur.



Utilisation des journaux

La reprise d'activité après sinistre collecte les fichiers journaux pour l'appliance VPN et la passerelle VPN. Ces journaux sont enregistrés sous forme de fichiers .txt, qui sont compressés dans une archive .zip. Vous pouvez télécharger et extraire l'archive, puis vous servir des informations qu'elle contient à des fins de dépannage et de surveillance.

La liste suivante décrit les fichiers journaux qui font partie de l'archive zip, et les informations qu'ils contiennent.

`dnsmasq.config.txt` : le fichier contient des informations sur la configuration du service qui fournit les adresses DNS et DHCP.

`dnsmsq.leases.txt` : le fichier contient des informations sur les locations d'adresses DHCP actuelles.

`dnsmasq_log.txt` : le fichier contient les journaux du service dnsmasq.

`ebtables.txt` : le fichier contient des informations sur les tables de pare-feu.

`free.txt` : le fichier contient des informations sur la mémoire libre.

`ip.txt` : le fichier contient les journaux de la configuration des interfaces réseau, y compris leur nom pouvant être utilisé dans la configuration des paramètres **Capturer des paquets réseau**.

`NetworkManager_log.txt` : le fichier contient les journaux du service NetworkManager.

`NetworkManager_status.txt` : le fichier contient des informations sur l'état du service NetworkManager.

`openvpn@p2s_log.txt` : le fichier contient les journaux du service OpenVPN.

`openvpn@p2s_status.txt` : le fichier contient des informations sur l'état des tunnels VPN.

`ps.txt` : le fichier contient des informations sur les processus en cours d'exécution de la passerelle VPN ou de l'appliance VPN.

`resolf.conf.txt` : le fichier contient des informations sur la configuration des serveurs DNS.

`routes.txt` : le fichier contient des informations de routage réseau.

`uname.txt` : le fichier contient des informations sur la version actuelle du noyau du système d'exploitation.

`uptime.txt` : le fichier contient des informations sur la durée pendant laquelle le système d'exploitation n'a pas été redémarré.

`vpnserver_log.txt` : le fichier contient les journaux du service VPN.

`vpnserver_status.txt` : le fichier contient des informations sur l'état du serveur VPN.

Pour plus d'informations sur les fichiers journaux propres à la connectivité VPN IPsec, reportez-vous à "Fichiers journaux VPN IPsec multi-site" (p. 819).

Téléchargement des journaux de l'appliance VPN

Vous pouvez télécharger et extraire l'archive qui contient les journaux de l'appliance VPN, puis vous servir des informations qu'elle contient à des fins de dépannage et de surveillance.

Télécharger les journaux de l'appliance VPN

1. Sur la page **Connectivité**, cliquez sur l'icône en forme d'engrenage à côté de l'appliance VPN.
2. Cliquez sur le bouton **Télécharger le journal**.
3. [Facultatif] Sélectionnez **Capturer des paquets réseau**, puis configurez les paramètres. Pour plus d'informations, voir "Capture des paquets réseau" (p. 816).
4. Cliquez sur **Valider**.
5. Lorsque l'archive .zip est prête à être téléchargée, cliquez sur **Télécharger le journal**, puis enregistrez-la au niveau local.

Téléchargement des journaux de la passerelle VPN

Vous pouvez télécharger et extraire l'archive qui contient les journaux de la passerelle VPN, puis vous servir des informations qu'elle contient à des fins de dépannage et de surveillance.

Télécharger les journaux de la passerelle VPN

1. Sur la page **Connectivité**, cliquez sur l'icône en forme d'engrenage à côté de la passerelle VPN.
2. Cliquez sur le bouton **Télécharger le journal**.
3. [Facultatif] Sélectionnez **Capturer des paquets réseau**, puis configurez les paramètres. Pour plus d'informations, voir "Capture des paquets réseau" (p. 816).
4. Cliquez sur **Valider**.
5. Lorsque l'archive .zip est prête à être téléchargée, cliquez sur **Télécharger le journal**, puis enregistrez-la au niveau local.

Capture des paquets réseau

Pour dépanner et analyser la communication entre le site de production local et un serveur principal ou de restauration, vous pouvez choisir de collecter les paquets réseau sur la passerelle VPN ou sur l'appliance VPN.

Après avoir collecté 32 000 paquets réseau, ou atteint la limite de temps, la capture des paquets réseaux s'arrête, et les résultats sont écrits dans un fichier .libpcap ajouté dans l'archive .zip des journaux.

Le tableau suivant fournit plus de détails sur les paramètres **Capturer des paquets réseau** que vous pouvez configurer.

Paramètre	Description
Nom de l'interface réseau	L'interface réseau sur laquelle capturer des paquets réseau. Si vous souhaitez capturer des paquets réseau sur toutes les interfaces réseau, sélectionnez **Toutes**.
Limite de temps (secondes)	La limite de temps pour la capture des paquets réseau. La valeur maximale que vous pouvez définir est 1 800.
Filtrage	Un filtre supplémentaire à appliquer aux paquets réseau capturés. Vous pouvez saisir une chaîne contenant des protocoles, des ports, des instructions et leurs combinaisons, séparés par une espace, par exemple : « and », « or », « not », « (« , ») », « src », « dst », « net », « host », « port », « ip », « tcp », « udp », « icmp », « arp » et « esp ». Si vous souhaitez utiliser des parenthèses, entourez-les d'espaces. Vous pouvez également saisir des adresses IP et des adresses réseau, par exemple : « icmp or arp » et « port 67 or 68 ». Pour plus d'informations sur les valeurs que vous pouvez saisir, consultez l'aide Linux tpcdump.

Dépannage de la configuration VPN IPsec

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Lorsque vous configurez ou utilisez la connexion VPN IPsec, il est possible que vous rencontriez des problèmes.

Pour en savoir plus sur les problèmes rencontrés, reportez-vous aux fichiers journaux IPsec, et consultez les rubriques de problèmes de configuration VPN IPsec pour obtenir des solutions à certains des problèmes courants susceptibles de se produire.

Dépannage des problèmes de configuration VPN IPsec

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Le tableau suivant décrit les problèmes de configuration VPN IPsec les plus courants, et explique comment les résoudre.

Problème	Solution possible
Le message d'erreur suivant s'affiche : **Erreur de négociation IKE phase 1. Vérifiez les paramètres IKE IPsec sur les sites Cloud et locaux.**	Cliquez sur **Réessayer** et vérifiez si un message d'erreur plus spécifique apparaît. Par exemple, il peut s'agir d'un message concernant une incompatibilité de l'algorithme ou une clé prépartagée incorrecte. **Remarque** Pour des raisons de sécurité, les restrictions suivantes s'appliquent à la connectivité VPN IPsec : • IKEv1 sera déprécié dans RFC8247 et n'est pas pris en charge pour des raisons de sécurité. Seules les connexions de protocole IKEv2 sont prises en charge. • Les algorithmes de chiffrement suivants ne sont pas considérés comme sécurisés et ne sont donc pas pris en charge : DES et 3DES. • Les algorithmes de hachage suivants ne sont pas considérés comme sécurisés et ne sont donc pas pris en charge : SHA1 et MD5. • Le groupe Diffie-Hellman 2 n'est pas considéré comme sécurisé et n'est donc pas pris en charge.
L'état **Connexion en cours** persiste lors de la connexion entre mon site local et le site dans le Cloud.	Vérifiez les points suivants : • Si le port UDP 500 est ouvert (lorsque vous utilisez un pare-feu). • La connectivité entre le site local et le site dans le Cloud. • Si l'adresse IP du site local est correcte.
L'état **En attente de connexion** persiste lors de la connexion entre mon site local et le site dans le Cloud.	Cet état apparaît lorsque l'**action de démarrage** pour le site dans le Cloud est définie sur **Ajouter**, ce qui signifie que le site dans le Cloud attend que le site local démarre la connexion. Démarrez la connexion depuis le site local.

Problème	Solution possible
L'état **En attente de trafic** persiste lors de la connexion entre mon site local et le site dans le Cloud.	Cet état apparaît lorsque l'**action de démarrage** pour le site dans le Cloud est définie sur **Route**. Si vous attendez une connexion depuis le site local, procédez comme suit : • Depuis le site local, essayez d'envoyer un ping à la machine virtuelle sur le site dans le Cloud. Ce comportement standard est nécessaire pour établir un tunnel pour certains terminaux, par exemple les terminaux Cisco ASA. (Mode de routage) • Assurez-vous que le site local a établi un tunnel en définissant l'**action de démarrage** du site local sur **Démarrer**.
La connexion entre mon site local et le site dans le Cloud est établie, mais je vois qu'une ou plusieurs politiques réseau sont désactivées.	Ce problème peut avoir plusieurs causes : • Le mappage réseau sur le site IPsec dans le Cloud est différent du mappage réseau sur le site local. Vérifiez que les mappages réseau et que la séquence des politiques réseau sur le site local et sur le site dans le Cloud correspondent. • Cet état est correct lorsque l'**action de démarrage** du site local et/ou du site dans le Cloud est définie sur **Route** (par exemple, sur les terminaux Cisco ASA), et qu'il n'y a pas de trafic actuellement. Vous pouvez essayer d'envoyer un ping pour vous assurer que le tunnel est établi. Si le ping ne fonctionne pas, vérifiez le mappage réseau sur le site local et sur le site dans le Cloud.
Je veux redémarrer une connexion IPsec spécifique.	Pour redémarrer une connexion IPsec spécifique : 1. Depuis l'écran **Reprise d'activité après sinistre** > **Connectivité**, cliquez sur la connexion IPsec. 2. Cliquez sur **Désactiver la connexion**. 3. Cliquez à nouveau sur la connexion IPsec. 4. Cliquez sur **Activer la connexion**.

Téléchargement des fichiers journaux VPN IPsec

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous trouverez des informations supplémentaires sur la connectivité IPsec dans les fichiers journaux sur le serveur VPN. Les fichiers journaux sont compressés sous la forme d'une archive .zip que vous pouvez télécharger et extraire.

Prérequis

La connectivité VPN IPsec multi-site est configurée.

Pour télécharger et extraire l'archive .zip avec les fichiers journaux

1. Dans la console Cyber Protect, accédez à **Reprise d'activité après sinistre** > **Connectivité**.
2. Cliquez sur l'icône en forme d'engrenage située à côté de la passerelle VPN du site dans le Cloud.
3. Cliquez sur **Télécharger le journal**.
4. Cliquez sur **Valider**.
5. Lorsque l'archive .zip est prête à être téléchargée, cliquez sur **Télécharger le journal**, puis enregistrez-la au niveau local.

Fichiers journaux VPN IPsec multi-site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

La liste suivante décrit les fichiers journaux VPN IPsec qui font partie de l'archive zip, et les informations qu'ils contiennent.

- `ip.txt` : le fichier contient les journaux issus de la configuration des interfaces réseau. Vous devez voir deux adresses IP : une adresse IP publique et une adresse IP locale. Si vous ne voyez pas ces deux adresses IP dans le fichier journal, il y a un problème. Dans ce cas, contactez l'équipe d'assistance.

  Remarque
  Le masque pour l'adresse IP publique doit être 32.

- `swanctl-list-loaded-config.txt` : le fichier contient des informations concernant tous les sites IPsec.

  Si vous ne voyez pas un site dans le fichier, la configuration IPsec n'a pas été appliquée. Essayez de mettre à jour la configuration et de l'enregistrer, ou contacter l'équipe d'assistance.
- `swanctl-list-active-sas.txt` : le fichier contient des connexions et des politiques dont l'état est actif ou en cours de connexion.

Configuration des serveurs de restauration

Cette section décrit les concepts de basculement et de restauration automatique, la création d'un serveur de restauration, et les opérations de reprise d'activité après sinistre.

Création d'un serveur de restauration

Pour créer un serveur de restauration qui sera une copie de votre ressource, procédez comme suit. Vous pouvez aussi regarder le tutoriel vidéo qui présente le processus.

Important
Lorsque vous effectuez un basculement, vous ne pouvez sélectionner que les points de reprise qui ont été créés après la création du serveur de restauration.

Prérequis

- Un plan de protection doit être appliqué à la machine d'origine que vous souhaitez protéger. Ce plan peut sauvegarder l'intégralité de la machine ou uniquement les disques requis pour le démarrage et la fourniture des services nécessaires à un stockage dans le Cloud.
- Vous devez définir au moins un type de connectivité vers le site dans le Cloud.

Pour créer un serveur de restauration

1. Dans l'onglet **Tous les terminaux**, sélectionnez l'ordinateur que vous voulez protéger.
2. Cliquez sur **Reprise d'activité après sinistre**, puis sur **Créer un serveur de restauration**.
3. Sélectionnez le nombre de cœurs virtuels et la taille de la RAM.

   Remarque
   Vous pouvez voir les points de calcul de chaque option. Le nombre de points de calcul traduit le coût horaire de l'exécution du serveur de restauration. Pour plus d'informations, voir "Points de calcul" (p. 776).

4. Indiquez le serveur Cloud auquel le serveur sera connecté.
5. Sélectionnez l'option **DHCP**.

Option DHCP	Description
Fourni par le site dans le cloud	Paramètre par défaut. L'adresse IP du serveur sera fournie par un serveur DHCP configuré automatiquement dans le cloud.
Personnalisé	L'adresse IP du serveur sera fournie par votre propre serveur DHCP dans le cloud.

6. [Facultatif] Spécifiez l'**Adresse MAC**.

   L'adresse MAC est un identificateur unique attribué à l'adaptateur réseau du serveur. Si vous utilisez un DHCP personnalisé, vous pouvez le configurer pour toujours attribuer des adresses IP spécifiques à une adresse MAC donnée. De cette façon, vous vous assurerez que le serveur de restauration aura toujours la même adresse IP. Vous pouvez exécuter des applications possédant des licences enregistrées avec l'adresse MAC.

7. Indiquez l'adresse IP que le serveur aura dans le réseau de production. Par défaut, l'adresse IP de la machine d'origine est sélectionnée.

   Remarque
   Si vous utilisez un serveur DHCP, ajoutez cette adresse IP à la liste d'exclusion du serveur, afin d'éviter les conflits d'adresse IP.
   Si vous utilisez un serveur DHCP personnalisé, l'adresse IP que vous spécifiez dans **Adresse IP en réseau de production** doit être la même que celle configurée dans le serveur DHCP. Dans le cas contraire, le basculement test ne fonctionnera pas correctement, et il ne sera pas possible d'accéder au serveur via une adresse IP publique.

8. [Facultatif] Activez la case à cocher **Adresse IP test**, puis saisissez l'adresse IP.
   Cela vous permettra de tester un basculement dans le réseau de test isolé et de vous connecter au serveur de restauration via RDP ou SSH lors d'un basculement test. En mode de basculement test, la passerelle VPN remplace l'adresse IP test par l'adresse IP de production au moyen du protocole NAT.
   Si vous n'activez pas la case à cocher, la console sera le seul moyen d'accéder au serveur lors d'un basculement test.

   Remarque
   Si vous utilisez un serveur DHCP, ajoutez cette adresse IP à la liste d'exclusion du serveur afin d'éviter les conflits d'adresse IP.

   Vous pouvez sélectionner l'une des adresses IP proposées ou en saisir une autre.
9. [Facultatif] Activez la case à cocher **Accès Internet**.
   Cela permettra au serveur de restauration d'accéder à Internet lors d'un vrai basculement ou d'un basculement test. Par défaut, le port TCP 25 est ouvert pour les connexions sortantes vers des adresses IP publiques.
10. [Facultatif] Définissez le **seuil des objectifs de point de récupération**.
    Le seuil des objectifs de point de récupération définit l'intervalle de temps maximum autorisé entre le dernier point de récupération pour un basculement et l'heure actuelle. La valeur peut être définie entre 15 et 60 minutes, 1 et 24 heures, 1 et 14 jours.
11. [Facultatif] Activez la case à cocher **Utiliser une adresse IP publique**.
    Disposer d'une adresse IP publique permet au serveur de restauration d'être accessible depuis Internet lors d'un basculement ou d'un basculement test. Si vous n'activez pas la case à cocher, le serveur sera accessible uniquement dans votre réseau de production.
    L'option **Utiliser une adresse IP publique** nécessite que l'option **Accès Internet** soit activée.
    L'adresse IP publique s'affichera une fois la configuration terminée. Par défaut, le port TCP 443 est ouvert pour les connexions entrantes vers des adresses IP publiques.

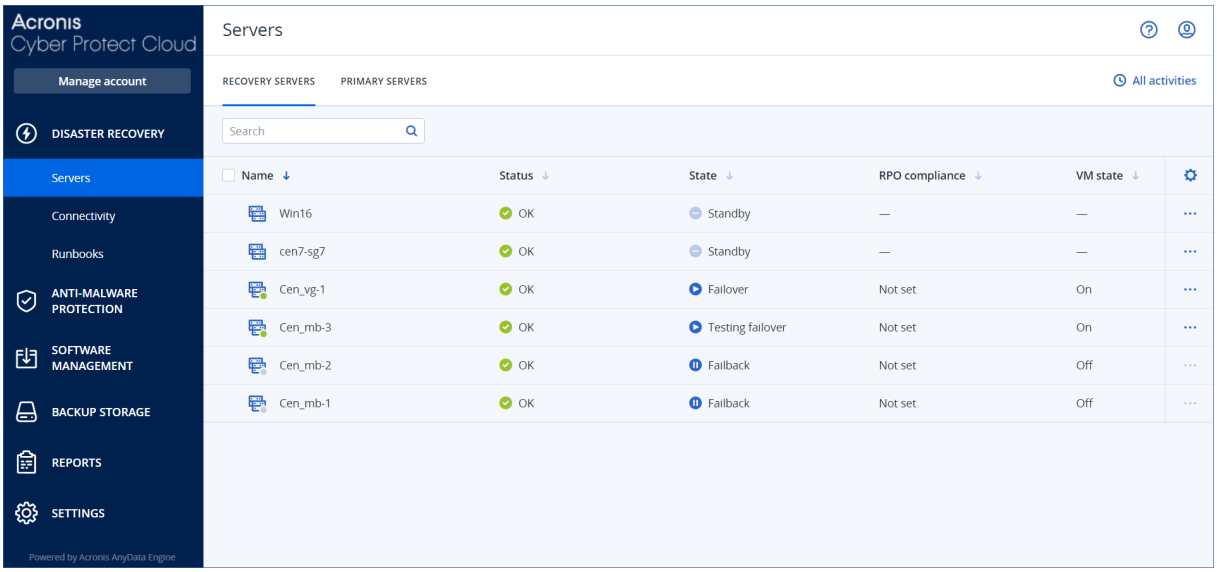
Remarque
Si vous désélectionnez la case **Utiliser une adresse IP publique** ou supprimez le serveur de restauration, son adresse IP publique n'est pas réservée.

12. [Facultatif] [Si les sauvegardes pour l'ordinateur sélectionné sont chiffrées à l'aide du chiffrement comme propriété de l'ordinateur] Spécifiez le mot de passe qui sera utilisé automatiquement lors de la création d'une machine virtuelle pour le serveur de restauration à partir de la sauvegarde chiffrée.
    a. Cliquez sur **Spécifier**, puis saisissez le mot de passe de la sauvegarde chiffrée et définissez un nom pour les identifiants.
    Par défaut, la liste affiche la sauvegarde la plus récente.
    b. [Facultatif] Pour afficher toutes les sauvegardes, sélectionnez **Afficher toutes les sauvegardes**.
    c. Cliquez sur **Valider**.

Remarque
Le mot de passe que vous spécifiez sera stocké dans un magasin d'identifiants sécurisé, mais l'enregistrement des mots de passe peut être contraire à vos obligations de conformité.

13. [Facultatif] Modifiez le nom du serveur de restauration.
14. [Facultatif] Saisissez une description pour le serveur de restauration.
15. [Facultatif] Cliquez sur l'onglet **Règles de pare-feu du Cloud** pour modifier les règles de pare-feu par défaut. Pour plus d'informations, voir "Définition de règles de pare-feu pour les serveurs Cloud" (p. 849).
16. Cliquez sur **Créer**.

Le serveur de restauration apparaît dans l'onglet **Reprise d'activité après sinistre** > **Serveurs** > **Serveurs de restauration** de la console Cyber Protect. Vous pouvez consulter ses paramètres en sélectionnant l'ordinateur d'origine et en cliquant sur **Reprise d'activité après sinistre**.



Fonctionnement du basculement

Basculement de la production

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Lorsqu'un serveur de restauration est créé, il reste en mode **En attente**. La machine virtuelle correspondante n'existe pas avant que vous ayez démarré un basculement. Avant de démarrer un processus de basculement, vous devez créer au moins une sauvegarde d'image de disque (avec volume amorçable) de la machine d'origine.

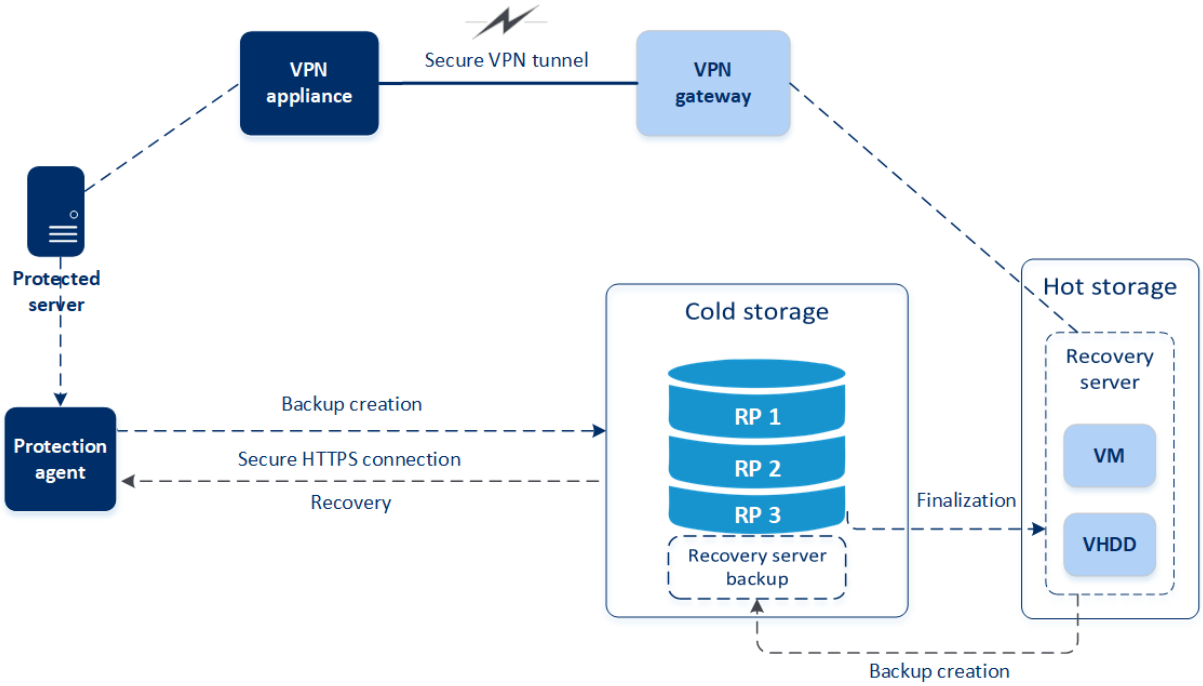
Lors du démarrage du processus de basculement, vous sélectionnez le point de restauration (sauvegarde) de l'ordinateur d'origine depuis lequel une machine virtuelle avec les paramètres prédéfinis sera créée. L'opération de basculement utilise la fonctionnalité « exécution d'une machine virtuelle à partir d'une sauvegarde ». Le serveur de restauration reçoit l'état de transition **Finalisation**. Ce processus implique le transfert des disques virtuels du serveur depuis le stockage des sauvegardes (stockage « froid ») vers le stockage pour reprise d'activité après sinistre (stockage « chaud »).

Remarque
Lors de la **Finalisation**, le serveur est accessible et opérationnel bien que ses performances soient inférieures à la normale. Vous pouvez ouvrir la console du serveur en cliquant sur le lien **La console est prête**. Le lien est disponible dans la colonne **État de la MV** de l'écran **Reprise d'activité après sinistre** > **Serveurs**, et dans la vue **Détails** du serveur.

Une fois la **Finalisation** terminée, les performances du serveur sont rétablies. L'état du serveur est modifié en **Basculement**. La ressource est désormais basculée de l'ordinateur d'origine vers le serveur de restauration du site dans le Cloud.

Si le composant de restauration possède un agent de protection, le service de l'agent est interrompu pour éviter toute interférence (notamment le démarrage d'une sauvegarde ou le signalement de statuts obsolètes au composant de sauvegarde).

Dans le diagramme ci-dessous, vous pouvez voir les processus de basculement et de restauration automatique.



Tester le basculement

Lors d'un **basculement test**, la machine virtuelle n'est pas finalisée. Cela signifie que l'agent lit le contenu des disques virtuels directement depuis la sauvegarde et accède aléatoirement aux différentes parties de la sauvegarde, si bien que ses performances peuvent être plus lentes que la normale. Ses performances peuvent être plus lentes que d'habitude. Pour plus d'informations sur le processus de basculement test, reportez-vous à "Réalisation d'un basculement test" (p. 824).

Basculement test automatisé

Lorsque le basculement test automatisé est configuré, il est exécuté une fois par mois, sans aucune interaction manuelle. Pour plus d'informations, voir "Basculement test automatisé" (p. 827) et "Configuration du basculement test automatisé" (p. 828).

Réalisation d'un basculement test

Un basculement test consiste à démarrer un serveur de restauration dans un VLAN de test isolé de votre réseau de production. Vous pouvez tester plusieurs serveurs de restauration à la fois et vérifier leur interaction. Dans le réseau de test, les serveurs communiquent à l'aide de leur adresse IP de production, mais ils ne peuvent pas démarrer de connexions TCP ou UDP à des ressources situées sur votre réseau local.

Lors du basculement test, la machine virtuelle (serveur de restauration) n'est pas finalisée. L'agent lit le contenu des disques virtuels directement depuis la sauvegarde et accède de façon aléatoire aux différentes parties de la sauvegarde. Le risque est que les performances du serveur de restauration dans l'état de basculement test soient plus lentes que d'habitude.

Bien que le basculement test soit facultatif, nous vous recommandons d'en exécuter régulièrement, à une fréquence adéquate pour vous en matière de coût et de fiabilité. Une bonne pratique consiste à créer un runbook (dossier d'exploitation), c'est-à-dire un ensemble d'instructions décrivant comment lancer l'environnement de production dans le Cloud.

Important
Vous devez créer un serveur de restauration à l'avance afin de protéger vos terminaux d'un sinistre.

Vous ne pouvez effectuer un basculement que depuis des points de reprise créés après la création du serveur de restauration du terminal.

Vous devez créer au moins un point de récupération avant de basculer vers un serveur de restauration. Le nombre maximal de points de reprise pris en charge est de 100.

Pour effectuer un basculement test

1. Sélectionnez la machine d'origine ou le serveur de restauration que vous souhaitez tester.
2. Cliquez sur **Reprise d'activité après sinistre**.
   La description du serveur de restauration s'ouvre.
3. Cliquez sur **Basculement**.
4. Sélectionnez le type de basculement **Basculement test**.
5. Sélectionnez le point de restauration (sauvegarde), puis cliquez sur **Démarrer**.
6. Si la sauvegarde sélectionnée est chiffrée à l'aide du chiffrement comme propriété de l'ordinateur :
   a. Saisissez le mot de passe de chiffrement pour l'ensemble de sauvegardes.

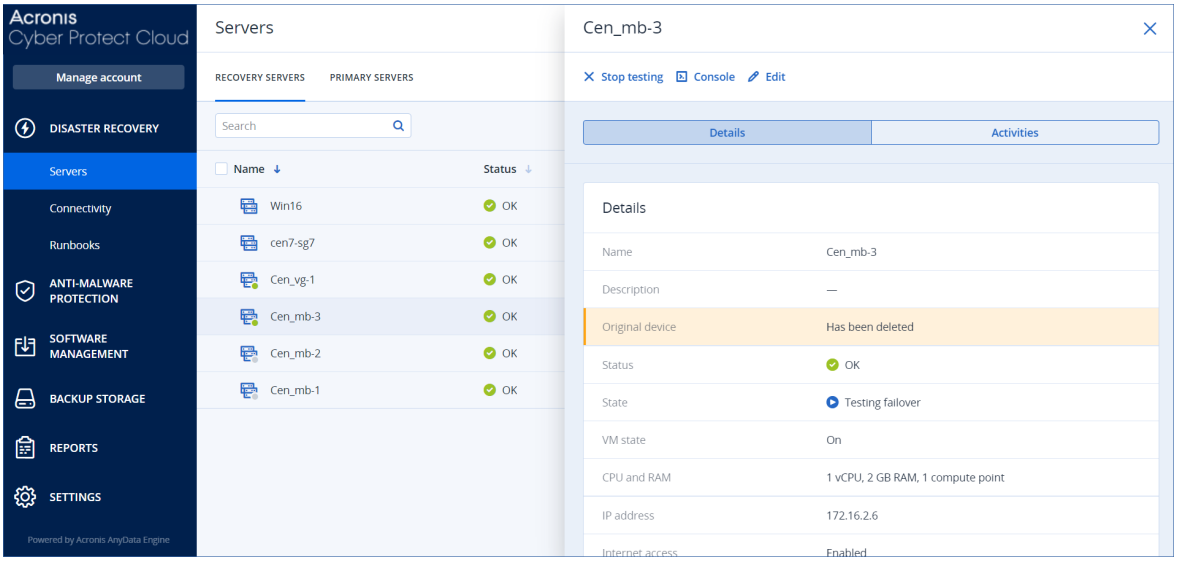
      Remarque
      Le mot de passe ne sera enregistré que temporairement et utilisé uniquement pour le basculement test en cours. Le mot de passe est supprimé automatiquement du magasin des identifiants si le basculement test est arrêté ou une fois que le basculement test est terminé.

   b. [Facultatif] Pour enregistrer le mot de passe de l'ensemble de sauvegardes et l'utiliser dans les opérations de basculement ultérieures, cochez la case **Stocker le mot de passe dans un magasin d'identifiants sécurisé** et saisissez un nom pour les identifiants dans le champ **Nom des identifiants**.

Important
Le mot de passe sera stocké dans un magasin d'identifiants sécurisé et sera appliqué automatiquement dans les opérations de basculement ultérieures. Toutefois, l'enregistrement des mots de passe peut entrer en conflit avec vos obligations de conformité.

c. Cliquez sur **Valider**.

Quand le serveur de restauration démarre, son état est modifié en **Test de basculement**.



7. Testez le serveur de restauration à l'aide de l'une des méthodes suivantes :
   - Dans **Reprise d'activité après sinistre** > **Serveurs**, sélectionnez le serveur de restauration, puis cliquez sur **Console**.
   - Connectez-vous au serveur de restauration via RDP ou SSH, à l'aide de l'IP de production que vous avez indiquée lors de la création du serveur de restauration. Testez la connexion de l'intérieur et de l'extérieur du réseau de production (comme décrit dans « Connexion de point à site »).
   - Exécutez un script au sein du serveur de restauration.

     Le script peut vérifier l'écran de connexion, le démarrage des applications, la connexion Internet, et la capacité d'autres machines à se connecter au serveur de restauration.
   - Si le serveur de restauration a accès à Internet et à une adresse IP publique, vous voudrez peut-être utiliser TeamViewer.
8. Une fois le test terminé, cliquez sur **Arrêter le test**.

   Le serveur de restauration est arrêté. Toutes les modifications apportées au serveur de restauration lors du basculement test ne sont pas conservées.

Remarque
Les actions **Démarrer le serveur** et **Arrêter le serveur** ne sont pas applicables aux opérations de basculement test, que ce soit dans un runbook ou lors d'un démarrage de basculement test manuel. Si vous essayez d'exécuter une telle action, elle échouera et le message d'erreur suivant sera renvoyé :
Échec : l'action n'est pas applicable à l'état actuel du serveur.

Basculement test automatisé

Avec le basculement test automatisé, le serveur de restauration est testé automatiquement une fois par mois, sans aucune interaction manuelle.

Le processus de basculement test automatisé se compose des étapes suivantes :

1. Création d'une machine virtuelle à partir du dernier point de reprise
2. Prise d'instantané de la machine virtuelle
3. Analyse visant à déterminer si le système d'exploitation de la machine virtuelle démarre correctement
4. Envoi d'une notification pour vous informer de statut du basculement test

Remarque
Le basculement test automatisé consomme des points de calcul.

Vous pouvez configurer le basculement test automatisé dans les paramètres du serveur de restauration. Pour plus d'informations, voir "Configuration du basculement test automatisé" (p. 828).

Veuillez noter que, dans de très rares cas, le basculement test automatisé peut être ignoré et ne pas être exécuté à l'heure planifiée. Cela s'explique par le fait que le basculement de la production est prioritaire sur le basculement test automatisé. Par conséquent, les ressources matérielles (processeur et mémoire RAM) allouées au basculement test automatisé peuvent être temporairement limitées afin de garantir que les ressources nécessaires à un basculement de production simultané soient suffisantes.

Si le basculement test automatisé est ignoré, quelle qu'en soit la raison, une alerte est générée.

Remarque
Le basculement de test automatisé échoue si les sauvegardes de l'ordinateur original sont chiffrées à l'aide du chiffrement comme propriété de l'ordinateur, et que le mot de passe de chiffrement n'est pas spécifié lors de la création du serveur de restauration. Pour plus d'informations sur la spécification du mot de passe de chiffrement, voir "Création d'un serveur de restauration" (p. 820).

Configuration du basculement test automatisé

En configurant le basculement test automatisé, vous pouvez tester votre serveur de restauration tous les mois, sans aucune intervention manuelle.

Pour configurer le basculement test automatisé

1. Dans la console, accédez à **Reprise d'activité après sinistre** > **Serveurs** > **Serveurs de restauration**, puis sélectionnez le serveur de restauration.
2. Cliquez sur **Modifier**.
3. Dans la section **Basculement test automatisé**, dans le champ **Planification**, sélectionnez **Tous les mois**.
4. [Facultatif] Dans la zone **Délai d'attente de capture d'écran**, changez la valeur par défaut de la durée maximale (en minutes) pendant laquelle le système essaie d'effectuer un basculement test automatisé.
5. [Facultatif] Si vous souhaitez conserver la valeur **Délai d'attente de capture d'écran** par défaut et souhaitez qu'elle soit renseignée automatiquement lorsque vous activez le basculement test automatisé des autres serveurs de restauration, sélectionnez **Définir comme délai d'attente par défaut**.
6. Cliquez sur **Enregistrer**.

Affichage du statut du basculement test automatisé

Vous pouvez afficher les détails d'un basculement test automatisé effectué, notamment son statut, ses heures de début et de fin, sa durée et l'instantané de la machine virtuelle.

Pour afficher le statut du basculement test automatisé d'un serveur de restauration

1. Dans la console, accédez à **Reprise d'activité après sinistre** > **Serveurs** > **Serveurs de restauration**, puis sélectionnez le serveur de restauration.
2. Dans la section **Basculement test automatisé**, vérifiez les détails du dernier basculement test automatisé.
3. [Facultatif] Cliquez sur **Afficher l'instantané** pour visualiser l'instantané de la machine virtuelle.

Désactivation du basculement test automatisé

Vous pouvez désactiver le basculement test automatisé si vous souhaitez économiser les ressources n'avez pas besoin d'exécuter le basculement test automatisé pour un serveur de restauration donné.

Pour désactiver le basculement test automatisé

1. Dans la console, accédez à **Reprise d'activité après sinistre** > **Serveurs** > **Serveurs de restauration**, puis sélectionnez le serveur de restauration.
2. Cliquez sur **Modifier**.

3. Dans la section **Basculement test automatisé**, dans le champ **Planification**, sélectionnez **Jamais**.
4. Cliquez sur **Enregistrer**.

Réalisation d'un basculement

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Un basculement est le processus consistant à déplacer une ressource de vos locaux vers le Cloud. Il s'agit aussi de l'état où la ressource reste dans le Cloud.

Lorsque vous démarrez un basculement, le serveur de restauration démarre dans le réseau de production. Pour éviter tout problème et interférence, assurez-vous que la ressource originale n'est pas en ligne et qu'il est impossible d'y accéder via VPN.

Pour éviter toute interférence de sauvegarde dans la même archive dans le cloud, révoquez manuellement le plan de protection de la ressource ayant l'état **Basculement**. Pour plus d'informations sur la révocation de plans, reportez-vous à Révocation d'un plan de protection.

Important
Vous devez créer un serveur de restauration à l'avance afin de protéger vos terminaux d'un sinistre.

Vous ne pouvez effectuer un basculement que depuis des points de reprise créés après la création du serveur de restauration du terminal.

Vous devez créer au moins un point de récupération avant de basculer vers un serveur de restauration. Le nombre maximal de points de reprise pris en charge est de 100.

Vous pouvez suivre les instructions ci-dessous ou regarder le tutoriel vidéo.

Pour réaliser un basculement

1. Vérifiez que la machine d'origine n'est pas disponible sur le réseau.
2. Dans la console Cyber Protect, accédez à **Reprise d'activité après sinistre** > **Serveurs** > **Serveurs de restauration**, puis sélectionnez le serveur de restauration.
3. Cliquez sur **Basculement**.
4. Sélectionnez le type de basculement **Basculement de la production**.
5. Sélectionnez le point de restauration (sauvegarde), puis cliquez sur **Démarrer**.
6. [Si la sauvegarde sélectionnée est chiffrée à l'aide du chiffrement comme propriété de l'ordinateur]

a. Saisissez le mot de passe de chiffrement pour l'ensemble de sauvegardes.

Remarque
Le mot de passe ne sera enregistré que temporairement et utilisé uniquement pour le basculement en cours. Le mot de passe est supprimé automatiquement du magasin des identifiants une fois que l'opération de basculement est terminée et que le serveur revient à l'état de **veille**.

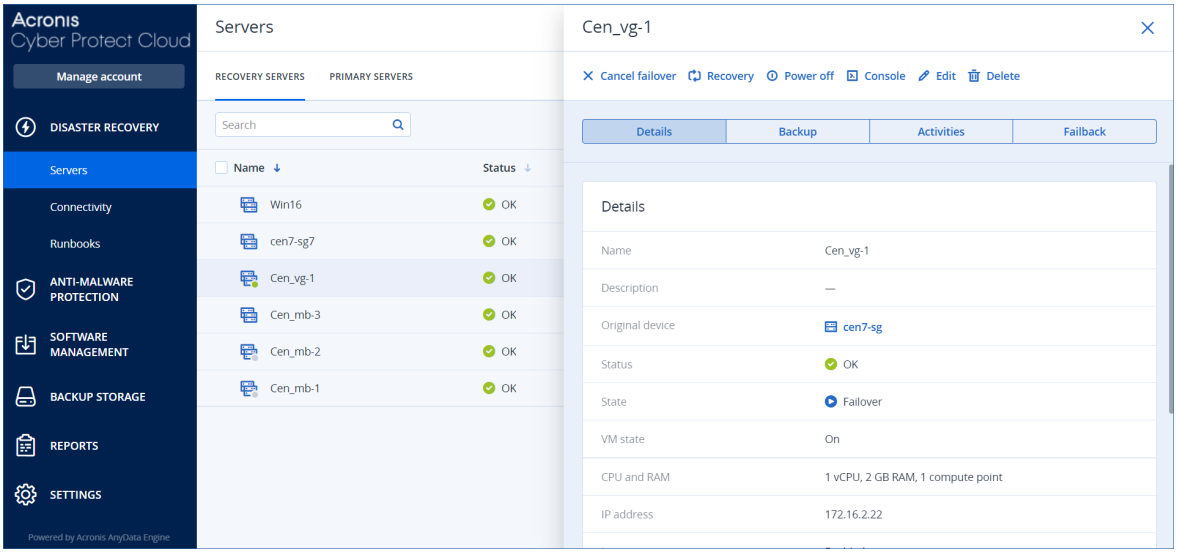
b. [Facultatif] Pour enregistrer le mot de passe de l'ensemble de sauvegardes et l'utiliser dans les opérations de basculement ultérieures, cochez la case **Stocker le mot de passe dans un magasin d'identifiants sécurisé** et saisissez un nom pour les identifiants dans le champ **Nom des identifiants**.

Important
Le mot de passe sera stocké dans un magasin d'identifiants sécurisé et sera appliqué automatiquement dans les opérations de basculement ultérieures. Toutefois, l'enregistrement des mots de passe peut entrer en conflit avec vos obligations de conformité.

c. Cliquez sur **Valider**.

Lorsque le serveur de restauration démarre, son état est modifié en **Finalisation**, puis, au bout d'un certain temps, en **Basculement.**

Important
Il est essentiel de comprendre que le serveur est disponible aussi bien dans l'état **Finalisation** que **Basculement**. Lors de la **Finalisation**, vous pouvez accéder à la console du serveur en cliquant sur le lien **La console est prête**. Le lien est disponible dans la colonne **État de la MV** de l'écran **Reprise d'activité après sinistre** > **Serveurs**, et dans la vue **Détails** du serveur. Pour plus de détails, voir "Fonctionnement du basculement" (p. 823).



7. Assurez-vous que le serveur de restauration est démarré en consultant sa console. Cliquez sur **Reprise d'activité après sinistre** > **Serveurs**, sélectionnez le serveur de restauration, puis cliquez sur **Console**.
8. Assurez-vous que le serveur de restauration est accessible à l'aide de l'adresse IP de production que vous avez indiquée lors de la création du serveur de restauration.

Une fois le serveur de restauration finalisé, un nouveau plan de protection est automatiquement créé et lui est appliqué. Ce plan de protection se base sur le plan de protection utilisé pour créer le serveur de restauration, avec certaines limitations. Dans ce plan, vous ne pouvez modifier que la planification et les règles de rétention. Pour en savoir plus, consultez « Sauvegarde des serveurs Cloud ».

Si vous souhaitez annuler le basculement, sélectionnez le serveur de restauration, puis cliquez sur **Annuler le basculement**. Toutes les modifications apportées à partir du basculement, à l'exception des sauvegardes du serveur de récupération, seront perdues. Le serveur de restauration repassera à l'état **En attente**.

Si vous souhaitez effectuer une restauration automatique, sélectionnez le serveur de restauration, puis cliquez sur **Restauration automatique**.

Comment exécuter un basculement des serveurs à l'aide d'un DNS local

Si vous utilisez des serveurs DNS sur le site local pour convertir les noms de machines, les serveurs de restauration correspondant aux machines qui dépendent du DNS n'arriveront alors plus à communiquer après le basculement, car les serveurs DNS utilisés dans le Cloud sont différents. Par défaut, les serveurs DNS du site dans le Cloud sont utilisés pour les serveurs Cloud nouvellement créés. Si vous avez besoin d'appliquer des paramètres DNS personnalisés, contactez l'équipe d'assistance.

Comment exécuter un basculement à l'aide d'un serveur DHCP

Il se peut que le serveur DHCP de votre infrastructure locale se situe sur un hôte Windows ou Linux. Lorsqu'un tel hôte est basculé vers le site dans le Cloud, un problème de duplication du serveur DHCP survient, car la passerelle VPN dans le Cloud joue également le rôle de DHCP. Pour résoudre ce problème, effectuez l'une des actions suivantes :

- Si seul l'hôte DHCP a été basculé vers le Cloud, mais que les autres serveurs locaux se trouvent toujours dans le site local, vous devez alors vous connecter à l'hôte DHCP et désactiver le serveur DHCP qui s'y trouve. Il n'y aura ainsi aucun conflit et seule la passerelle VPN fera office de serveur DHCP.
- Si vos serveurs dans le Cloud ont déjà obtenu leurs adresses auprès de l'hôte DHCP, vous devez alors vous connecter à l'hôte DHCP et désactiver le serveur DHCP qui s'y trouve. Vous devez également vous connecter aux serveurs Cloud et renouveler le bail DHCP pour attribuer de nouvelles adresses IP allouées par le bon serveur DHCP (hébergé sur la passerelle VPN).

Remarque
Les instructions ne sont pas valides lorsque votre serveur DHCP dans le cloud est configuré avec l'option **DHCP personnalisé**, et que certains des serveurs principaux ou de restauration obtiennent leur adresse IP depuis ce serveur DHCP.

Fonctionnement de la restauration automatique

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Une restauration automatique est un processus consistant à déplacer la ressource du Cloud vers une machine physique ou virtuelle sur votre site local. Vous pouvez exécuter une restauration automatique sur un serveur de restauration dont l'état est **Basculement**, et continuer d'utiliser le serveur sur votre site local.

Vous pouvez exécuter un basculement automatique vers une machine cible virtuelle ou physique sur votre site local. Lors du processus de restauration automatique, vous pouvez transférer les données de sauvegarde vers votre site local alors que la machine virtuelle dans le cloud continue à s'exécuter. Cette technologie vous permet de bénéficier d'une période d'interruption d'activité très courte, qui est estimée et affichée dans la console Cyber Protect. Vous pouvez consulter cette information et l'utiliser pour planifier vos activités et, si nécessaire, avertir vos clients d'une période d'interruption d'activité à venir.

Les processus de restauration automatique vers des machines cibles virtuelles et physiques sont légèrement différents. Pour plus d'informations sur les différentes phases du processus de restauration automatique, reportez-vous à "Restauration automatique sur une machine virtuelle cible" (p. 832) et "Restauration automatique vers une machine physique cible" (p. 838).

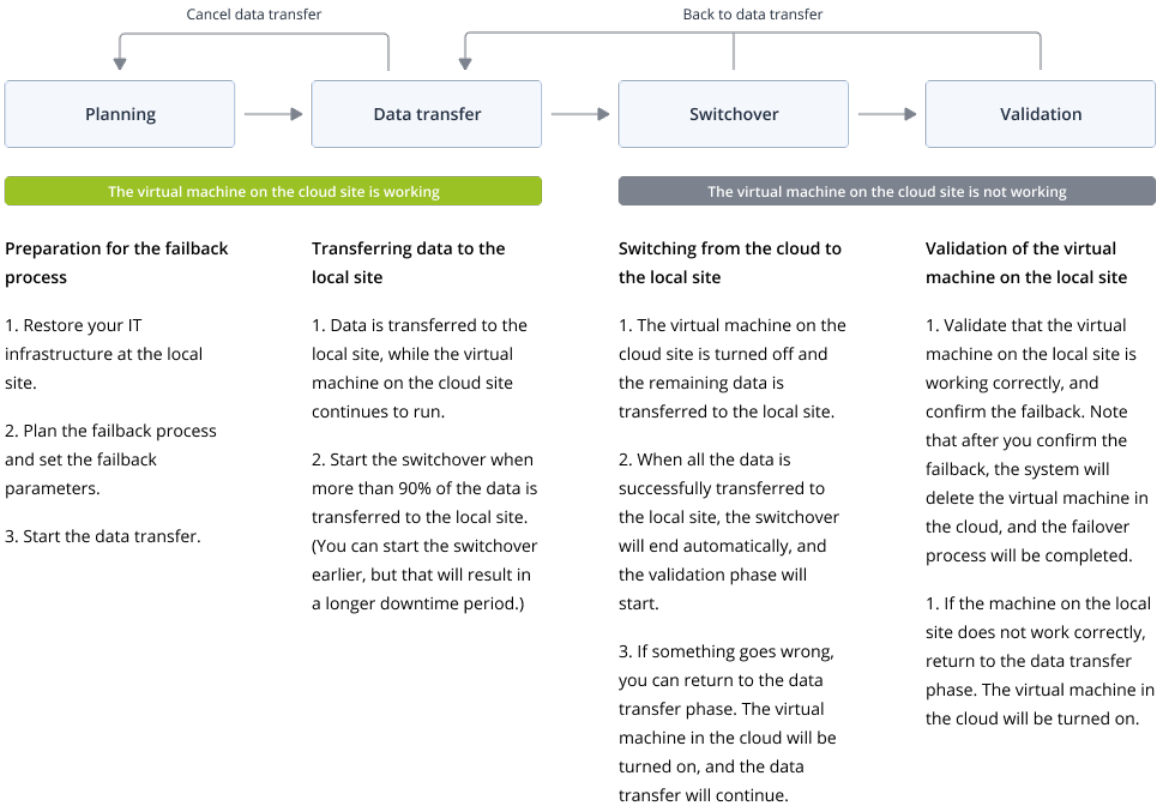
Dans des cas précis où vous ne pouvez pas utiliser la procédure de restauration automatique en mode automatisé, vous pouvez exécuter une restauration automatique en mode manuel. Pour plus d'informations, voir "Restauration automatique en mode manuel" (p. 842).

Remarque
Les opérations de runbook prennent en charge la restauration automatique en mode manuel uniquement. Cela signifie que si vous démarrez le processus de restauration automatique en exécutant un runbook qui inclut une étape **Serveur de restauration automatique**, la procédure nécessitera une interaction manuelle : vous devez restaurer l'ordinateur manuellement, et confirmer ou annuler le processus de restauration automatique à partir de l'onglet **Reprise d'activité après sinistre** > **Serveurs**.

Restauration automatique sur une machine virtuelle cible

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Le processus de restauration automatique vers une machine virtuelle cible se compose de quatre phases.



1. **Planification**. Lors de cette phase, vous restaurez l'infrastructure informatique sur votre site local (configuration des hôtes et du réseau), configurez les paramètres de restauration automatique et planifiez le moment où démarrer le transfert de données.

   Remarque
   Pour diminuer la durée totale du processus de restauration automatique, nous vous recommandons de démarrer la phase de transfert de données immédiatement après avoir configuré vos serveurs locaux, puis de poursuivre avec la configuration du réseau et le reste de l'infrastructure locale lors de la phase de transfert de données.

2. **Transfert de données**. Lors de cette phase, l'exécution de la machine virtuelle dans le Cloud est maintenue pendant que les données sont transférées du site dans le Cloud vers le site local. Vous pouvez démarrer la phase suivante, le basculement, à tout moment durant la phase de transfert de données, mais vous devriez tenir compte des relations suivantes.
   Plus vous restez longtemps dans la phase Transfert de données,
   - plus longtemps la machine virtuelle dans le cloud continue à s'exécuter ;
   - plus la quantité de données qui sera transférée à votre site local sera importante ;

- plus cela vous coûtera cher (vous dépensez plus de points de calcul) ;
- plus la période d'interruption d'activité lors de la phase de basculement sera courte.

  Si vous souhaitez réduire l'interruption d'activité au minimum, démarrez la phase de basculement une fois que 90 % au moins des données ont été transférés sur le site local.

  Si vous pouvez vous permettre une période d'interruption d'activité plus longue et que vous ne souhaitez pas dépenser plus de points de calcul pour l'exécution de la machine virtuelle dans le Cloud, vous pouvez démarrer la phase de basculement plus tôt.

  Si vous annulez le processus de restauration automatique lors de la phase Transfert de données, les données transférées ne seront pas supprimées du site local. Pour éviter d'éventuels problèmes, supprimez manuellement les données transférées avant de lancer un nouveau processus de restauration automatique. Le processus de transfert de données suivant reprendra au début.

3. **Basculement**. Lors de cette phrase, la machine virtuelle dans le cloud est arrêtée et les données restantes, y compris le dernier incrément de sauvegarde, sont transférées sur le site local. Si aucun plan de sauvegarde n'est appliqué au serveur de restauration, une sauvegarde sera effectuée automatiquement pendant la phase de basculement, ce qui ralentit le processus.

   Vous pouvez consulter le temps estimé pour finir cette phase (période d'interruption d'activité) dans la console Cyber Protect. Lorsque toutes les données sont transférées sur le site local (il n'y a aucune perte de données et la machine virtuelle située sur le site local est une copie parfaite de la machine virtuelle dans le cloud), la phase de basculement est terminée. La machine virtuelle sur le site local est restaurée et la phase de validation démarre automatiquement.
4. **Validation**. Pendant cette phase, la machine virtuelle sur le site local est prête et démarre automatiquement. Vous pouvez vérifier si elle fonctionne correctement et :
   - Si tout fonctionne comme prévu, vous pouvez confirmer la restauration automatique. Après la confirmation de la restauration automatique, la machine virtuelle dans le Cloud est supprimée, et le serveur de restauration revient à l'état **En attente**. Le processus de restauration automatique est alors terminé.
   - En cas d'anomalie, vous pouvez annuler le basculement et revenir à la phase de transfert de données.

Exécution d'une restauration automatique vers une machine virtuelle

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez exécuter une restauration automatique vers une machine virtuelle cible sur votre site local.

Prérequis

- L'agent que vous allez utiliser pour exécuter une restauration automatique est en ligne et n'est pas actuellement utilisé pour une autre opération de restauration automatique.

- Votre connexion Internet est stable.
- Il existe au moins une sauvegarde complète de la machine virtuelle dans le cloud.

Pour effectuer une restauration automatique vers une machine virtuelle

1. Dans la console Cyber Protect, accédez à **Reprise d'activité après sinistre** > **Serveurs**.
2. Sélectionnez le serveur de restauration en état de **basculement**.
3. Cliquez sur l'onglet **Restauration automatique**.
4. Dans la section **Paramètres de restauration automatique**, sélectionnez **Machine virtuelle** en guise de **Cible**, puis configurez les autres paramètres.
   Notez que par défaut, certains des **paramètres de restauration automatique** sont remplis automatiquement avec des valeurs suggérées, mais vous pouvez les modifier.
   Le tableau suivant fournit plus de détails sur les **paramètres de restauration automatique**.

Paramètre	Description
Taille de la sauvegarde	Quantité de données qui sera transférée à votre site local lors du processus de restauration automatique. Une fois que vous aurez lancé le processus de restauration automatique vers une machine virtuelle cible, la **Taille de la sauvegarde** augmentera lors de la phase de transfert de données, car la machine virtuelle dans le cloud continuera à s'exécuter et à générer de nouvelles données. Pour calculer l'interruption d'activité estimée qui surviendra lors du processus de restauration automatique vers une machine virtuelle cible, partez de 10 % de la **Taille de la sauvegarde** (puisque nous vous recommandons de démarrer la phase de basculement quand 90 % des données ont été transférés vers votre site local) et divisez cette valeur par celle de la vitesse de votre connexion Internet. **Remarque** La valeur de la vitesse de votre connexion Internet diminuera quand vous exécuterez simultanément plusieurs processus de restauration automatique.
Cible	Type de ressource sur votre site local vers laquelle vous allez restaurer le serveur Cloud : **Machine virtuelle** ou **Machine physique**.
Emplacement de machine cible	Emplacement de restauration automatique : hôte VMware ESXi ou Microsoft Hyper-V. Vous pouvez faire votre choix parmi tous les hôtes qui possèdent un agent enregistré avec le service de cyberprotection.
Agent	Agent qui exécutera l'opération de restauration automatique. Vous pouvez utiliser un agent pour effectuer une opération de

Paramètre	Description
	restauration automatique à la fois. Vous pouvez sélectionner un agent qui est en ligne et qui n'est pas actuellement utilisé pour un autre processus de restauration automatique, qui possède une version compatible avec la fonctionnalité de restauration automatique, et qui dispose des droits d'accès à la sauvegarde. Notez que vous pouvez installer plusieurs agents sur des hôtes VMware ESXi, et démarrer un processus de restauration automatique séparé sur chacun d'eux. Ces processus de restauration automatique peuvent être exécutés simultanément.
Paramètres de machine cible	Paramètres de machine virtuelle : • **Processeurs virtuels**. Sélectionnez le nombre de processeurs virtuels. • **Mémoire**. Sélectionnez la quantité de mémoire dont disposera la machine virtuelle. • **Unités**. Sélectionnez les unités pour la mémoire. • [Facultatif] **Adaptateurs réseau**. Pour ajouter un adaptateur réseau, cliquez sur **Ajouter**, puis sélectionnez un réseau dans le champ **Réseau**. Quand les changements vous conviennent, cliquez sur **Terminé**.
Chemin d'accès	(Pour les hôtes Microsoft Hyper-V) Dossier sur l'hôte où votre machine sera stockée. Assurez-vous que l'espace disponible sur l'hôte est suffisant pour la machine.
Magasin de données	(Pour les hôtes VMware ESXi) Magasin de données sur l'hôte où votre machine sera stockée. Assurez-vous que l'espace disponible sur l'hôte est suffisant pour la machine.
Mode de provisionnement	Méthode d'allocation du disque virtuel. Pour les hôtes Microsoft Hyper-V : • **En expansion dynamique** (Valeur par défaut). • **Taille fixe**. Pour les hôtes Microsoft Hyper-V : • **Dynamique** (Valeur par défaut). • **Statique**.
Nom de machine cible	Le nom de la machine cible. Par défaut, le nom de la machine cible est le même que celui du serveur de restauration. Le nom de la machine cible doit être spécifique à l'**emplacement de la machine cible** sélectionné.

5. Cliquez sur **Démarrer le transfert de données** et, dans la fenêtre de confirmation, cliquez sur **Démarrer**.

   Remarque
   S'il n'y a pas de sauvegarde de la machine virtuelle dans le cloud, le système effectuera une sauvegarde automatiquement avant la phase de transfert des données.

   La phase **Transfert de données** démarre. La console affiche les informations suivantes :

Champs	Description
Progression	Ce paramètre affiche la quantité de données déjà transférées vers le site local, ainsi que la quantité totale de données à transférer. La quantité totale de données comprend les données de la dernière sauvegarde avant le démarrage de la phase de transfert de données, ainsi que les sauvegardes des données nouvellement générées (incréments de sauvegarde), car la machine virtuelle continue à s'exécuter lors de la phase de transfert de données. Pour cette raison, les deux valeurs du paramètre **Progression** augmentent au fil du temps.
Estimation de l'interruption d'activité	Ce paramètre indique la durée d'indisponibilité de la machine virtuelle dans le cloud si vous démarrez la phase de basculement maintenant. La valeur est calculée en fonction des valeurs du paramètre **Progression** et diminue au fil du temps.

6. Cliquez sur **Basculement**, puis cliquez une nouvelle fois sur **Basculement** dans la fenêtre de confirmation.
   La phase de basculement commence. La console affiche les informations suivantes :

Champs	Description
Progression	Ce paramètre montre la progression de la restauration de la machine sur le site local.
Temps restant estimé	Ce paramètre indique l'heure approximative à laquelle la phase de basculement sera terminée et où vous pourrez démarrer la machine virtuelle sur le site local.

   Remarque
   Si aucun plan de sauvegarde n'est appliqué à la machine virtuelle dans le cloud, une sauvegarde sera effectuée automatiquement pendant la phase de basculement, ce qui ralentit le processus.

7. Une fois que la phase de **basculement** est terminée et que la machine virtuelle de votre site local est démarrée automatiquement, vérifiez qu'elle fonctionne comme prévu.
8. Cliquez sur **Confirmer la restauration automatique** et, dans la fenêtre de confirmation, cliquez sur **Confirmer** pour finaliser le processus.
   La machine virtuelle dans le Cloud est supprimée, et le serveur de restauration revient à l'état **En attente**.

Remarque

Appliquer un plan de protection sur le serveur restauré ne fait pas partie du processus de restauration automatique. Une fois le processus de restauration automatique terminé, appliquez un plan de protection sur le serveur restauré pour vous assurer qu'il est de nouveau protégé. Vous pouvez appliquer le même plan de protection que celui qui était appliqué sur le serveur d'origine ou un nouveau plan de protection pour lequel le module **Reprise d'activité après sinistre** est activé.

Restauration automatique vers une machine physique cible

Remarque

La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Le processus de restauration automatique en mode automatique vers une machine physique cible se compose des phases suivantes :

1. **Planification**. Lors de cette phase, vous restaurez l'infrastructure informatique sur votre site local (configuration des hôtes et du réseau), configurez les paramètres de restauration automatique et planifiez le moment où démarrer le transfert de données.
2. **Transfert de données**. Lors de cette phase, l'exécution de la machine virtuelle dans le Cloud est maintenue pendant que les données sont transférées du site dans le Cloud vers le site local. Vous pouvez démarrer la phase suivante, le basculement, à tout moment durant la phase de transfert de données, mais vous devriez tenir compte des relations suivantes.

   Plus vous restez longtemps dans la phase Transfert de données,

   - plus longtemps la machine virtuelle dans le cloud continue à s'exécuter ;
   - plus la quantité de données qui sera transférée à votre site local sera importante ;
   - plus cela vous coûtera cher (vous dépensez plus de points de calcul) ;
   - plus la période d'interruption d'activité lors de la phase de basculement sera courte.

   Si vous souhaitez réduire l'interruption d'activité au minimum, démarrez la phase de basculement une fois que 90 % au moins des données ont été transférés sur le site local.

   Si vous pouvez vous permettre une période d'interruption d'activité plus longue et que vous ne souhaitez pas dépenser plus de points de calcul pour l'exécution de la machine virtuelle dans le Cloud, vous pouvez démarrer la phase de basculement plus tôt.

Remarque

Le processus de transfert de données utilise une technologie de flashback. Cette technologie compare les données disponibles sur la machine cible aux données de la machine virtuelle dans le cloud. Si une partie des données est déjà disponible sur la machine cible, elles ne sont pas retransférées. Cette technologie accélère la phase de transfert de données.

C'est la raison pour laquelle nous vous recommandons de restaurer le serveur sur la machine d'origine sur votre site local.

3. **Basculement**. Lors de cette phrase, la machine virtuelle dans le cloud est arrêtée et les données restantes, y compris le dernier incrément de sauvegarde, sont transférées sur le site local. Si aucun plan de sauvegarde n'est appliqué au serveur de restauration, une sauvegarde sera effectuée automatiquement pendant la phase de basculement, ce qui ralentit le processus.
4. **Validation**. Lors de cette phrase, la machine physique sur le site local est prête et vous pouvez la redémarrer à l'aide d'un support de démarrage Linux. Vous pouvez vérifier que la machine virtuelle fonctionne correctement et :
   - Si tout fonctionne comme prévu, vous pouvez confirmer la restauration automatique. Après la confirmation de la restauration automatique, la machine virtuelle dans le Cloud est supprimée, et le serveur de restauration revient à l'état **En attente**. Le processus de restauration automatique est alors terminé.
   - En cas d'anomalie, vous pouvez annuler le basculement et revenir à la phase de planification.

   Remarque
   Une fois que le support de démarrage a été redémarré, vous ne pourrez plus le réutiliser. Si vous détectez une anomalie au cours de la phase de validation, vous devez enregistrer un nouveau support de démarrage et redémarrer le processus de restauration automatique.
   Toutefois, étant donné qu'une technologie de flashback est utilisée, les données figurant déjà sur le site local ne seront pas retransférées et le processus de restauration automatique sera accéléré.

Exécution d'une restauration automatique vers une machine physique

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez exécuter une restauration automatique en mode automatique vers une machine physique cible sur votre site local.

Remarque
Le processus de transfert de données utilise une technologie de flashback. Cette technologie compare les données disponibles sur la machine cible aux données de la machine virtuelle dans le cloud. Si une partie des données est déjà disponible sur la machine cible, elles ne sont pas retransférées. Cette technologie accélère la phase de transfert de données.

C'est la raison pour laquelle nous vous recommandons de restaurer le serveur sur la machine d'origine sur votre site local.

Prérequis

- L'agent que vous allez utiliser pour exécuter une restauration automatique est en ligne et n'est pas actuellement utilisé pour une autre opération de restauration automatique.
- Votre connexion Internet est stable.

- Un support de démarrage enregistré est disponible. Pour plus d'informations, voir Création d'un support de démarrage afin de restaurer des systèmes d'exploitation dans le Guide de l'utilisateur Cyber Protection.
- La machine physique cible est la machine d'origine sur votre site local ou une autre machine dont le firmware est identique à celui de la machine d'origine.
- Il existe au moins une sauvegarde complète de la machine virtuelle dans le cloud.

Pour effectuer une restauration automatique vers une machine physique

1. Dans la console Cyber Protect, accédez à **Reprise d'activité après sinistre** > **Serveurs**.
2. Sélectionnez le serveur de restauration en état de **basculement**.
3. Cliquez sur l'onglet **Restauration automatique**.
4. Dans le champ **Cible**, sélectionnez **Machine physique**.
5. Dans le champ **Support de démarrage cible**, cliquez sur **Spécifier**, sélectionnez le support de démarrage, puis cliquez sur **Terminé**.

   Remarque
   Nous vous recommandons d'utiliser un support de démarrage prêt à l'emploi, car il est déjà configuré. Pour plus d'informations, voir Création d'un support de démarrage afin de restaurer des systèmes d'exploitation dans le Guide de l'utilisateur Cyber Protection.

6. [Facultatif] Pour modifier le mappage de disque par défaut, cliquez dans le champ **Mappage de disque** sur **Spécifier**, mappez les disques de la sauvegarde vers les disques de la machine cible, puis cliquez sur **Terminé**.
7. Cliquez sur **Démarrer le transfert de données**, puis sur **Démarrer** dans la fenêtre de confirmation.

   Remarque
   S'il n'y a pas de sauvegarde de la machine virtuelle dans le cloud, le système effectuera une sauvegarde automatiquement avant la phase de transfert des données.

   La phase transfert de données démarre. La console affiche les informations suivantes :

Champs	Description
Progression	Ce paramètre affiche la quantité de données déjà transférées vers le site local, ainsi que la quantité totale de données à transférer. La quantité totale de données comprend les données de la dernière sauvegarde avant le démarrage de la phase de transfert de données, ainsi que les sauvegardes des données nouvellement générées (incréments de sauvegarde), car la machine virtuelle continue à s'exécuter lors de la phase de transfert de données. C'est la raison pour laquelle les valeurs **Progression** augmentent au fil du temps. Étant donné que le système utilise une technologie de flashback

Champs	Description
	pendant le transfert de données et ne transfère pas les données déjà disponibles sur la machine cible, la progression peut être plus rapide que dans le calcul initial effectué par la console.
Estimation de l'interruption d'activité	Ce paramètre indique la durée d'indisponibilité de la machine virtuelle dans le cloud si vous démarrez la phase de basculement maintenant. La valeur est calculée en fonction des valeurs du paramètre **Progression** et diminue au fil du temps. Étant donné que le système utilise une technologie de flashback pendant le transfert de données et ne transfère pas les données déjà disponibles sur la machine cible, l'interruption d'activité peut être plus courte que la valeur affichée initialement dans la console.

8. Cliquez sur **Basculement**, puis cliquez une nouvelle fois sur **Basculement** dans la fenêtre de confirmation.

   La phase de basculement commence. La console affiche les informations suivantes :

Champs	Description
Progression	Ce paramètre montre la progression de la restauration de la machine sur le site local.
Temps restant estimé	Ce paramètre indique l'heure approximative à laquelle la phase de basculement sera terminée et où vous pourrez démarrer la machine virtuelle sur le site local.

Remarque
Si aucun plan de sauvegarde n'est appliqué à la machine virtuelle dans le cloud, une sauvegarde sera effectuée automatiquement pendant la phase de basculement, ce qui ralentit le processus.

9. Une fois la phase de **basculement** terminée, redémarrez le support de démarrage, puis vérifiez que la machine physique sur votre site local fonctionne comme prévu.

   Pour plus d'informations, voir Récupération de disques à l'aide d'un support de démarrage dans le Guide de l'utilisateur Cyber Protection.

10. Cliquez sur **Confirmer la restauration automatique**, puis sur **Confirmer** dans la fenêtre de confirmation pour finaliser le processus.

    La machine virtuelle dans le Cloud est supprimée, et le serveur de restauration revient à l'état **En attente**.

Remarque
Appliquer un plan de protection sur le serveur restauré ne fait pas partie du processus de restauration automatique. Une fois le processus de restauration automatique terminé, appliquez un plan de protection sur le serveur restauré pour vous assurer qu'il est de nouveau protégé. Vous pouvez appliquer le même plan de protection que celui qui était appliqué sur le serveur d'origine ou un nouveau plan de protection pour lequel le module **Reprise d'activité après sinistre** est activé.

Restauration automatique en mode manuel

Remarque
Nous vous recommandons d'utiliser le processus de restauration automatique en mode manuel uniquement lorsque l'équipe de support vous l'indique.

Vous pouvez également démarrer un processus de restauration automatique en mode manuel. Dans ce cas, le transfert de données depuis la sauvegarde dans le cloud vers le site local n'est pas effectué automatiquement. Il doit être effectué manuellement après l'arrêt de la machine virtuelle dans le cloud. Le processus de restauration automatique en mode manuel est beaucoup plus lent et vous devez vous attendre à une interruption d'activité plus longue.

Le processus de restauration automatique en mode manuel se compose des phases suivantes :

1. **Planification**. Lors de cette phase, vous restaurez l'infrastructure informatique sur votre site local (configuration des hôtes et du réseau), configurez les paramètres de restauration automatique et planifiez le moment où démarrer le transfert de données.
2. **Basculement**. Lors de cette phrase, la machine virtuelle dans le cloud est arrêtée et les données générées récemment sont sauvegardées. Si aucun plan de sauvegarde n'est appliqué au serveur de restauration, une sauvegarde sera effectuée automatiquement pendant la phase de basculement, ce qui ralentit le processus. Lorsque la sauvegarde est terminée, restaurez manuellement la machine sur le site local. Vous pouvez restaurer le disque à l'aide d'un support de démarrage, ou restaurer la machine tout entière à partir du stockage de sauvegarde dans le Cloud.
3. **Validation**. Lors de cette phase, vous vérifiez que la machine physique ou virtuelle sur le site local fonctionne correctement, et confirmez la restauration automatique. Après la confirmation, la machine virtuelle sur le site dans le Cloud est supprimée, et le serveur de restauration revient à l'état **En attente**.

Réalisation d'une restauration automatique en mode manuel

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez exécuter une restauration automatique en mode manuel vers une machine cible physique ou virtuelle sur votre site local.

Pour effectuer une restauration automatique en mode manuel

1. Dans la console Cyber Protect, accédez à **Reprise d'activité après sinistre** > **Serveurs**.
2. Sélectionnez le serveur de restauration en état de **basculement**.
3. Cliquez sur l'onglet **Restauration automatique**.
4. Dans le champ **Cible**, sélectionnez **Machine physique**.
5. Cliquez sur l'icône en forme d'engrenage, puis activer le paramètre **Utiliser le mode manuel**.
6. [Facultatif] Calculez le temps d'arrêt estimé qui surviendra lors du processus de restauration automatique en divisant la valeur **Taille de la sauvegarde** par la vitesse de votre connexion Internet.

   Remarque
   La valeur de la vitesse de votre connexion Internet diminuera quand vous exécuterez simultanément plusieurs processus de restauration automatique.

7. Cliquez sur **Basculement** et, dans la fenêtre de confirmation, cliquez une nouvelle fois sur **Basculement**.
   La machine virtuelle sur le site dans le Cloud est désactivée.

   Remarque
   Si aucun plan de sauvegarde n'est appliqué à la machine virtuelle dans le cloud, une sauvegarde sera effectuée automatiquement pendant la phase de basculement, ce qui ralentit le processus.

8. Restaurez le serveur depuis la sauvegarde dans le cloud vers la machine physique ou virtuelle sur votre site local. Pour plus d'informations, voir Restauration d'une machine dans le Guide de l'utilisateur Cyber Protection.
9. Assurez-vous que la restauration est terminée et que la machine restaurée fonctionne correctement, puis cliquez sur **La machine a été restaurée**.
10. Si tout fonctionne comme prévu, cliquez sur **Confirmer la restauration automatique** et, dans la fenêtre de confirmation, cliquez une nouvelle fois sur **Confirmer**.
    Le serveur de restauration et le point de récupération sont disponibles pour le prochain basculement. Pour créer de nouveaux points de récupération, appliquez un plan de protection au nouveau serveur local.

    Remarque
    Appliquer un plan de protection sur le serveur restauré ne fait pas partie du processus de restauration automatique. Une fois le processus de restauration automatique terminé, appliquez un plan de protection sur le serveur restauré pour vous assurer qu'il est de nouveau protégé. Vous pouvez appliquer le même plan de protection que celui qui était appliqué sur le serveur d'origine ou un nouveau plan de protection pour lequel le module **Reprise d'activité après sinistre** est activé.

Travailler avec des sauvegardes chiffrées

Vous pouvez créer des serveurs de restauration provenant de sauvegardes chiffrées. Pour votre commodité, vous pouvez définir une application de mot de passe automatique sur une sauvegarde chiffrée lors du basculement vers un serveur de restauration.

Lors de la création d'un serveur de restauration vous pouvez indiquer le mot de passe à utiliser pour les opérations automatiques de reprise d'activité après sinistre. Il sera enregistré dans le magasin d'informations d'identification, un espace de stockage sécurisé des identifiants, que vous pouvez trouver dans la section **Paramètres** > **Informations d'identification**.

Un identifiant peut être associé à plusieurs sauvegardes.

Pour gérer les mots de passe enregistrés dans le magasin d'informations d'identification

1. Accédez à **Paramètres** > **Informations d'identification**.
2. Pour gérer un identifiant précis, cliquez sur l'icône dans la dernière colonne. Vous pouvez visualiser les éléments associés à cet identifiant.
   - Pour dissocier la sauvegarde des informations d'identification sélectionnées, cliquez sur l'icône de la corbeille à côté de la sauvegarde. En conséquence, vous devrez indiquer le mot de passe manuellement lors du basculement vers le serveur de restauration.
   - Pour modifier les informations d'identification, cliquez sur **Modifier**, puis indiquez le nom ou le mot de passe.
   - Pour supprimer les informations d'identification, cliquez sur **Supprimer**. Veuillez noter que vous devrez indiquer le mot de passe manuellement lors du basculement vers le serveur de restauration.

Opérations réalisées avec les machines virtuelles Microsoft Azure

Remarque
Certaines fonctionnalités peuvent nécessiter une licence supplémentaire, en fonction du modèle de gestion de licences appliqué.

Vous pouvez effectuer le basculement des machines virtuelles Microsoft Azure vers le cloud Acronis Cyber Protect. Pour plus d'informations, voir "Réalisation d'un basculement" (p. 829).

Vous pouvez ensuite exécuter la restauration automatique depuis le cloud Acronis Cyber Protect vers les machines virtuelles Azure. La restauration automatique vers une machine physique est identique à celle vers une machine virtuelle. Pour plus d'informations, voir "Prérequis" (p. 839).

Remarque
Pour enregistrer une nouvelle machine virtuelle Azure pour la restauration automatique, vous pouvez utiliser l'extension de machine virtuelle de sauvegarde Acronis qui est disponible dans Azure.

Vous pouvez configurer une connectivité VPN IPsec multisite entre le cloud Acronis Cyber Protect et la passerelle VPN Azure. Pour plus d'informations, voir "Configuration d'un VPN IPsec multi-site" (p. 795).

Configuration des serveurs primaires

Cette section décrit comment créer et gérer vos serveurs primaires.

Création d'un serveur primaire

Prérequis

- Vous devez définir au moins un type de connectivité vers le site dans le Cloud.

Pour créer un serveur primaire

1. Accédez à l'onglet **Reprise d'activité après sinistre** > **Serveurs** > **Serveurs primaires**.
2. Cliquez sur **Créer**.
3. Sélectionnez un modèle pour la nouvelle machine virtuelle.
4. Sélectionnez le type de configuration (nombre de cœurs virtuels et taille de la RAM). Le tableau suivant indique la quantité maximale d'espace disque (en Go) pour chaque configuration.

Type	vCPU	RAM (Go)	Quantité maximale d'espace disque (Go)
F1	1	2	500
F2	1	4	1000
F3	2	8	2000
F4	4	16	4000
F5	8	32	8000
F6	16	64	16000
F7	16	128	32000
F8	16	256	64000

Remarque
Vous pouvez voir les points de calcul de chaque option. Le nombre de points de calcul traduit le coût horaire de l'exécution du serveur primaire. Pour plus d'informations, voir "Points de calcul" (p. 776).

5. [Facultatif] Modifiez la taille du disque virtuel. Si vous avez besoin de plus d'un disque dur, cliquez sur **Ajouter un disque**, puis indiquez la taille du nouveau disque. Actuellement, vous ne pouvez pas ajouter plus de 10 disques pour un serveur primaire.

6. Indiquez le réseau Cloud dans lequel le serveur primaire sera inclus.
7. Sélectionnez l'option **DHCP**.

Option DHCP	Description
Fourni par le site dans le cloud	Paramètre par défaut. L'adresse IP du serveur sera fournie par un serveur DHCP configuré automatiquement dans le cloud.
Personnalisé	L'adresse IP du serveur sera fournie par votre propre serveur DHCP dans le cloud.

8. [Facultatif] Spécifiez l'**Adresse MAC**.

   L'adresse MAC est un identificateur unique attribué à l'adaptateur réseau du serveur. Si vous utilisez un DHCP personnalisé, vous pouvez le configurer pour toujours attribuer des adresses IP spécifiques à une adresse MAC donnée. Le serveur primaire obtient ainsi toujours la même adresse IP. Vous pouvez exécuter des applications possédant des licences enregistrées avec l'adresse MAC.
9. Indiquez l'adresse IP que le serveur aura dans le réseau de production. Par défaut, la première adresse IP gratuite issue de votre réseau de production est définie.

   Remarque

   Si vous utilisez un serveur DHCP, ajoutez cette adresse IP à la liste d'exclusion du serveur, afin d'éviter les conflits d'adresse IP.

   Si vous utilisez un serveur DHCP personnalisé, l'adresse IP que vous spécifiez dans **Adresse IP en réseau de production** doit être la même que celle configurée dans le serveur DHCP. Dans le cas contraire, le basculement test ne fonctionnera pas correctement, et il ne sera pas possible d'accéder au serveur via une adresse IP publique.
10. [Facultatif] Activez la case à cocher **Accès Internet**.

    Cela permettra au serveur primaire d'accéder à Internet. Par défaut, le port TCP 25 est ouvert pour les connexions sortantes vers des adresses IP publiques.
11. [Facultatif] Activez la case à cocher **Utiliser une adresse IP publique**.

    Disposer d'une adresse IP publique permet au serveur primaire d'être accessible depuis Internet. Si vous n'activez pas la case à cocher, le serveur sera accessible uniquement dans votre réseau de production.

    L'adresse IP publique s'affichera une fois la configuration terminée. Par défaut, le port TCP 443 est ouvert pour les connexions entrantes vers des adresses IP publiques.

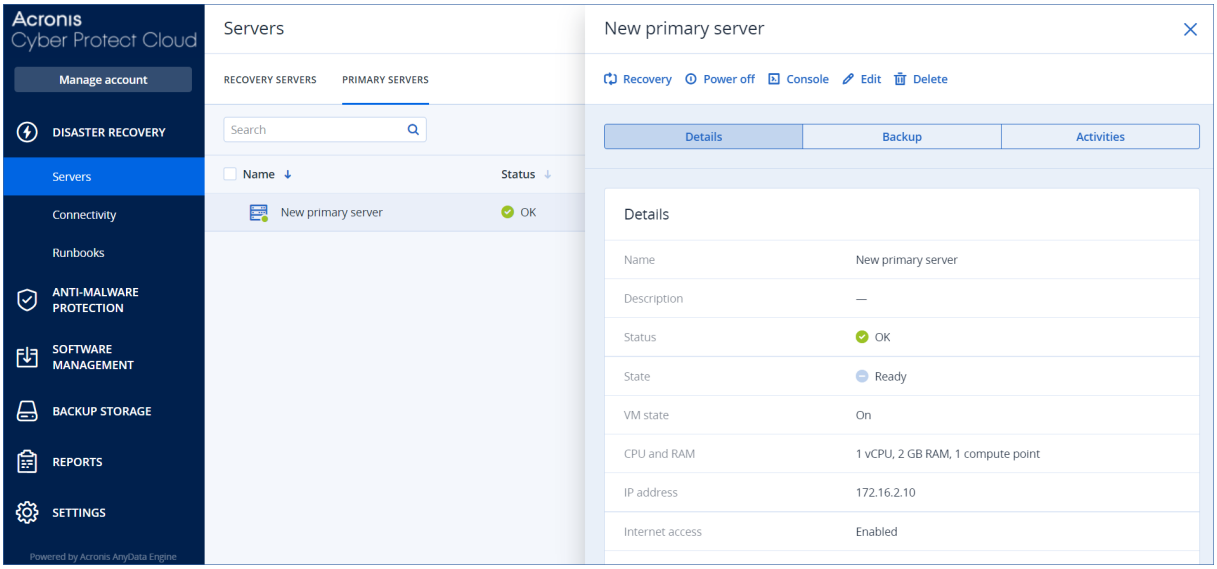
    Remarque

    Si vous désélectionnez la case **Utiliser une adresse IP publique** ou supprimez le serveur de restauration, son adresse IP publique n'est pas réservée.
12. [Facultatif] Sélectionnez **Définir le seuil des objectifs de point de récupération**.

Le seuil des objectifs de point de récupération (RPO) définit l'intervalle de temps maximum autorisé entre le dernier point de récupération pour un basculement et l'heure actuelle. La valeur peut être définie entre 15 et 60 minutes, 1 et 24 heures, 1 et 14 jours.

13. Définissez le nom du serveur primaire.
14. [Facultatif] Indiquez une description pour le serveur primaire.
15. [Facultatif] Cliquez sur l'onglet **Règles de pare-feu du Cloud** pour modifier les règles de pare-feu par défaut. Pour plus d'informations, voir "Définition de règles de pare-feu pour les serveurs Cloud" (p. 849).
16. Cliquez sur **Créer**.

Le serveur primaire devient accessible dans le réseau de production. Vous pouvez gérer le serveur à l'aide de sa console, de RDP, de SSH ou de TeamViewer.



Opérations sur un serveur primaire

Le serveur primaire apparaît dans l'onglet **Reprise d'activité après sinistre** > **Serveurs** > **Serveurs primaires** de la console Cyber Protect.

Pour démarrer ou arrêter le serveur, cliquez sur **Mettre sous tension** ou sur **Mise hors tension** dans le volet du serveur primaire.

Pour modifier les paramètres du serveur primaire, arrêtez le serveur, puis cliquez sur **Modifier**.

Pour appliquer un plan de protection au serveur primaire, sélectionnez-le et cliquez sur **Créer** dans l'onglet **Plan**. Vous verrez un plan de protection prédéfini dans lequel vous ne pouvez modifier que la planification et les règles de rétention. Pour en savoir plus, consultez « Sauvegarde des serveurs Cloud ».

Gestion des serveurs Cloud

Pour gérer les serveurs Cloud, accédez à **Reprise d'activité après sinistre** > **Serveurs**. Vous y verrez deux onglets : **Serveurs de restauration** et **Serveurs primaires**. Pour afficher toutes les colonnes facultatives, cliquez sur l'icône en forme d'engrenage.

Sélectionnez un serveur dans le Cloud pour afficher les informations suivantes le concernant.

Nom de la colonne	Description
Nom	Un nom de serveur Cloud que vous avez défini
Statut	Le statut reflétant le problème le plus grave au sein d'un serveur Cloud (basé sur les alertes actives)
État	L'état d'un serveur Cloud
État de la MV	L'état de l'alimentation d'une machine virtuelle associée au serveur Cloud
Emplacement actif	L'emplacement où le serveur dans le Cloud est hébergé. Par exemple, **Cloud**.
Seuil des objectifs de point de récupération	L'intervalle de temps maximum autorisé entre le dernier point de récupération pour un basculement et l'heure actuelle. La valeur peut être définie entre 15 et 60 minutes, 1 et 24 heures, 1 et 14 jours.
Conformité des objectifs de point de récupération	La conformité des objectifs de point de récupération (RPO) est le rapport entre les RPO réels et le seuil des RPO. La conformité des RPO s'affiche lorsque le seuil des RPO est défini. Elle est calculée comme suit : **Conformité RPO = RPO réels/Seuil des RPO** où **RPO réels = heure actuelle – heure du dernier point de récupération** **États de conformité des RPO** Selon la valeur du rapport entre les RPO réels et le seuil des RPO, les statuts suivants sont utilisés : • **Conformité**. La conformité des RPO < 1x. Un serveur définit le seuil des RPO. • **Dépassé**. La conformité des RPO <= 2x. Un serveur enfreint le seuil des RPO. • **Dépassement grave**. La conformité des RPO <= 4x. Un serveur enfreint le seuil de RPO plus de deux fois. • **Dépassement critique**. La conformité des RPO > 4x. Un serveur enfreint le seuil des RPO plus de quatre fois. • **En attente (aucune sauvegarde)**. Le serveur est protégé par le plan de protection, mais la sauvegarde est en cours de création et n'est pas encore terminée.

Objectifs de point de récupération (RPO) réels	Le temps passé depuis la création du dernier point de récupération
Dernier point de récupération	Date et heure auxquelles le dernier point de récupération a été créé

Règles de pare-feu pour les serveurs Cloud

Vous pouvez configurer les règles de pare-feu pour contrôler le trafic entrant et sortant des serveurs primaire et de restauration sur votre site dans le Cloud.

Vous pouvez configurer des règles entrantes après avoir provisionné une adresse IP publique pour le serveur Cloud. Le port TCP 443 est autorisé par défaut, et toutes les autres connexions entrantes sont refusées. Vous pouvez modifier les règles de pare-feu par défaut, et ajouter ou supprimer des exceptions entrantes. Si une adresse IP n'est pas provisionnée, vous pouvez uniquement consulter les règles entrantes, mais pas les configurer.

Vous pouvez configurer des règles sortantes après avoir provisionné une connexion Internet pour le serveur Cloud. Le port TCP 25 est refusé par défaut, et toutes les autres connexions sortantes sont refusées. Vous pouvez modifier les règles de pare-feu par défaut, et ajouter ou supprimer des exceptions sortantes. Si une connexion Internet n'est pas provisionnée, vous pouvez uniquement consulter les règles sortantes, mais pas les configurer.

Remarque
Pour des raisons de sécurité, certaines règles de pare-feu prédéfinies ne sont pas modifiables.

Pour les connexions entrantes et sortantes :

- Ping de permis : Demande d'écho ICMP (type 8, code 0) et réponse par écho ICMP (type 0, code 0)
- ICMP de permis besoin de fragmenter (type 3, code 4)
- TTL de permis dépassé (type 11, code 0)

Pour les connexions entrantes uniquement :

- Partie non configurable : Tout refuser

Pour les connexions sortantes uniquement :

- Partie non configurable : Tout rejeter

Définition de règles de pare-feu pour les serveurs Cloud

Vous pouvez modifier les règles de pare-feu par défaut pour les serveurs primaire et de restauration dans le Cloud.

Pour modifier les règles de pare-feu d'un serveur sur votre site dans le Cloud

1. Dans la console Cyber Protect, accédez à **Reprise d'activité après sinistre** > **Serveurs**.
2. Si vous souhaitez modifier les règles de pare-feu d'un serveur de restauration, cliquez sur **Serveurs de restauration**. Si vous souhaitez également modifier les règles de pare-feu d'un serveur primaire, cliquez sur l'onglet **Serveurs primaires**.
3. Cliquez sur le serveur, puis sur **Modifier**.
4. Cliquez sur l'onglet **Règles de pare-feu du Cloud**.
5. Si vous souhaitez modifier l'action par défaut pour les connexions entrantes :
   a. Dans le champ à liste déroulante **Entrantes**, sélectionnez l'action par défaut.

Action	Description
Tout refuser	Refuse tout le trafic entrant. Vous pouvez ajouter des exceptions et autoriser le trafic depuis des adresses IP, protocoles et ports spécifiques.
Tout autoriser	Autorise l'ensemble du trafic TCP et UDP entrant. Vous pouvez ajouter des exceptions et refuser le trafic depuis des adresses IP, protocoles et ports spécifiques.

Remarque
La modification de l'action par défaut invalide et supprime la configuration des règles entrantes existantes.

   b. [Facultatif] Si vous souhaitez sauvegarder les exceptions existantes, sélectionnez **Sauvegarder les exceptions remplies** dans la fenêtre de confirmation.
   c. Cliquez sur **Confirmer**.
6. Si vous souhaitez ajouter une exception :
   a. Cliquez sur **Ajouter une exception**.
   b. Spécifiez les paramètres de pare-feu.

Paramètre de pare-feu	Description
Protocole	Sélectionnez le protocole de connexion. Les options suivantes sont prises en charge : • **TCP** • **UDP** • **TCP+UDP**
Port de serveur	Sélectionnez les ports auxquels la règle s'applique. Vous pouvez spécifier les valeurs suivantes : • un numéro de port spécifique (par exemple, `2298`) • une plage de numéros de port (par exemple, `6000 à 6700`) • n'importe quel numéro de port. Utilisez `*` si vous souhaitez que la

Paramètre de pare-feu	Description
	règle s'applique à n'importe quel numéro de port.
Adresse IP du client	Sélectionnez les adresses IP auxquelles la règle s'applique. Vous pouvez spécifier les valeurs suivantes : • une adresse IP spécifique (par exemple, `192.168.0.0`) • une plage d'adresses IP qui utilisent la notation CIDR notation (par exemple, `192.168.0.0/24`) • n'importe quelle adresse IP. Utilisez `*` si vous souhaitez que la règle s'applique à n'importe quelle adresse IP.

7. Si vous souhaitez supprimer une exception entrante existante, cliquez sur l'icône de corbeille à côté de l'exception.
8. Si vous souhaitez modifier l'action par défaut pour les connexions sortantes :
   a. Dans le champ à liste déroulante **Sortantes**, sélectionnez l'action par défaut.

Action	Description
Tout refuser	Refuse tout le trafic sortant. Vous pouvez ajouter des exceptions et autoriser le trafic vers des adresses IP, protocoles et ports spécifiques.
Tout autoriser	Autorise tout le trafic sortant. Vous pouvez ajouter des exceptions et refuser le trafic depuis des adresses IP, protocoles et ports spécifiques.

Remarque
La modification de l'action par défaut invalide et supprime la configuration des règles sortantes existantes.

   b. [Facultatif] Si vous souhaitez sauvegarder les exceptions existantes, sélectionnez **Sauvegarder les exceptions remplies** dans la fenêtre de confirmation.
   c. Cliquez sur **Confirmer**.
9. Si vous souhaitez ajouter une exception :
   a. Cliquez sur **Ajouter une exception**.
   b. Spécifiez les paramètres de pare-feu.

Paramètre de pare-feu	Description
Protocole	Sélectionnez le protocole de connexion. Les options suivantes sont prises en charge : • **TCP** • **UDP**

Paramètre de pare-feu	Description
	• **TCP+UDP**
Port de serveur	Sélectionnez les ports auxquels la règle s'applique. Vous pouvez spécifier les valeurs suivantes : • un numéro de port spécifique (par exemple, `2298`) • une plage de numéros de port (par exemple, `6000 à 6700`) • n'importe quel numéro de port. Utilisez `*` si vous souhaitez que la règle s'applique à n'importe quel numéro de port.
Adresse IP du client	Sélectionnez les adresses IP auxquelles la règle s'applique. Vous pouvez spécifier les valeurs suivantes : • une adresse IP spécifique (par exemple, `192.168.0.0`) • une plage d'adresses IP qui utilisent la notation CIDR notation (par exemple, `192.168.0.0/24`) • n'importe quelle adresse IP. Utilisez `*` si vous souhaitez que la règle s'applique à n'importe quelle adresse IP.

10. Si vous souhaitez supprimer une exception sortante existante, cliquez sur l'icône de corbeille à côté de l'exception.
11. Cliquez sur **Enregistrer**.

Vérification des activités de pare-feu dans le Cloud

Après la mise à jour de la configuration des règles du pare-feu d'un serveur cloud, un journal de l'activité de mise à jour devient disponible dans la console Cyber Protect. Vous pouvez le consulter et vérifier les informations suivantes :

- le nom d'utilisateur de la personne ayant mis la configuration à jour
- la date et l'heure de la mise à jour
- les paramètres de pare-feu des connexions entrantes et sortantes
- les actions par défaut des connexions entrantes et sortantes
- les protocoles, ports et adresses IP des exceptions pour les connexions entrantes et sortantes

Pour consulter les détails d'un changement de configuration des règles d'un pare-feu dans le Cloud

1. Dans la console Cyber Protect, cliquez sur **Surveillance** > **Activités**.
2. Cliquez sur l'activité correspondante, puis sur **Toutes les propriétés**.

La description d'une activité doit être **Mise à jour de la configuration du serveur dans le Cloud**.

3. Dans le champ **Contexte**, examinez les informations qui vous intéressent.

Sauvegarde des serveurs Cloud

Les serveurs primaires et de restauration sont sauvegardés sans agent sur le site dans le cloud. Ces sauvegardes ont les restrictions suivantes.

- Le seul emplacement de sauvegarde possible est le stockage dans le cloud. Les serveurs primaires sont sauvegardés dans le **stockage de sauvegarde des serveurs primaires**.

  Remarque
  Les emplacements de sauvegarde Microsoft Azure ne sont pas pris en charge.

- Il n'est pas possible d'appliquer un plan de sauvegarde à plusieurs serveurs. Chaque serveur doit disposer de son propre plan de sauvegarde, même si tous les plans de sauvegarde ont les mêmes paramètres.
- Un seul plan de sauvegarde peut être appliqué à un serveur.
- La sauvegarde reconnaissant les applications n'est pas prise en charge.
- Le chiffrement n'est pas disponible.
- Aucune option de sauvegarde n'est disponible.

Lorsque vous supprimez un serveur primaire, ses sauvegardes sont également supprimées.

Un serveur de restauration est sauvegardé uniquement lorsqu'il se trouve en état de basculement. Sa sauvegarde poursuit la séquence de sauvegarde du serveur d'origine. Lorsqu'une restauration automatique est effectuée, le serveur d'origine peut poursuivre sa séquence de sauvegarde. Par conséquent, les sauvegardes du serveur de restauration peuvent uniquement être supprimées manuellement ou via l'application des règles de rétention. Lorsqu'un serveur de restauration est supprimé, ses sauvegardes sont toujours conservées.

Remarque
Les plans de sauvegarde pour les serveurs cloud s'exécutent en fonction de l'heure UTC.

Orchestration (runbooks)

Remarque
Certaines fonctionnalités peuvent nécessiter une licence supplémentaire, en fonction du modèle de gestion de licences appliqué.

Un runbook est un ensemble d'instructions décrivant le lancement de l'environnement de production dans le cloud. Vous pouvez créer des runbooks dans la console Cyber Protect. Pour accéder à l'écran **Runbooks**, sélectionnez **Reprise d'activité après sinistre** > **Runbooks**.

Pourquoi utiliser des runbooks ?

Les runbooks vous permettent d'effectuer les opérations suivantes :

- Automatiser le basculement d'un ou plusieurs serveurs
- Vérifier automatiquement le résultat du basculement en envoyant un ping à l'adresse IP et en vérifiant la connexion au port que vous spécifiez
- Définir la séquence d'opérations pour les serveurs exécutant des applications distribuées
- Inclure des opérations manuelles dans votre workflow
- Vérifier l'intégrité de votre solution de reprise d'activité après sinistre en exécutant des runbooks en mode test

Création d'un runbook

Un runbook se compose d'étapes exécutées consécutivement. Une étape se compose d'actions qui commencent simultanément.

Vous pouvez suivre les instructions ci-dessous ou regarder le tutoriel vidéo.

Pour créer un runbook

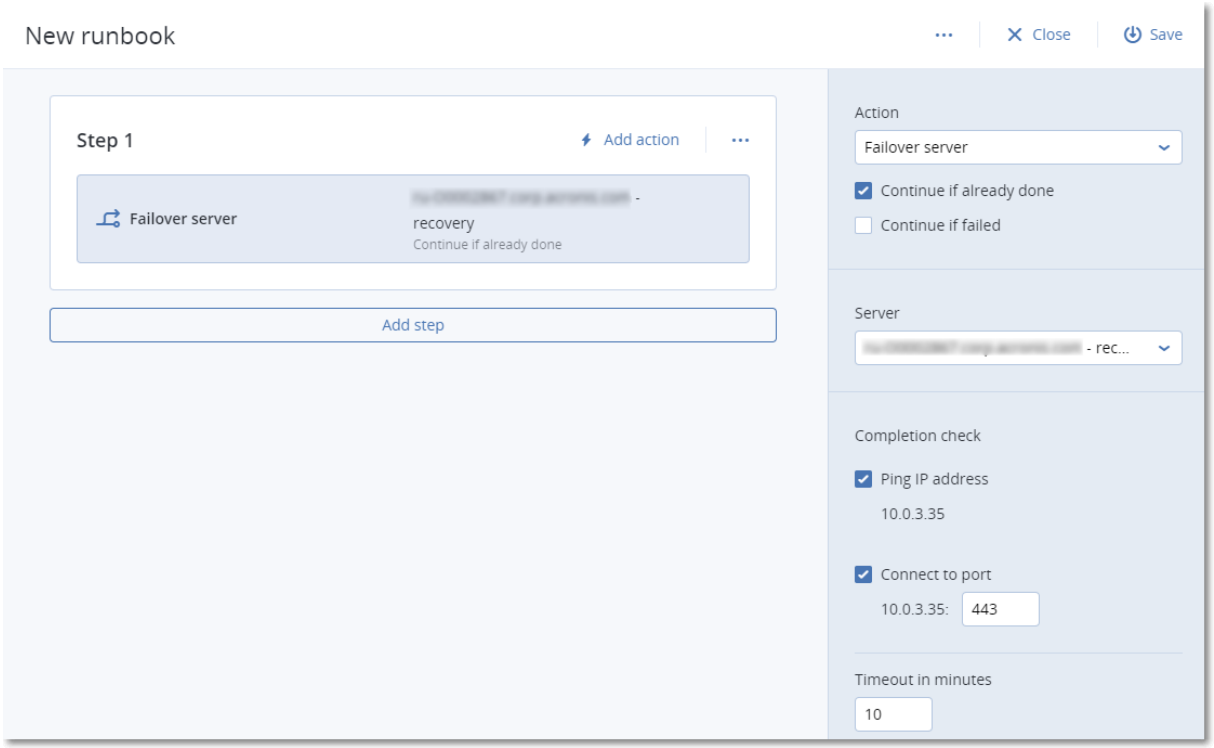
1. Dans la console Cyber Protection, accédez à **Reprise d'activité après sinistre** > **Runbooks**.
2. Cliquez sur **Créer un runbook**.
3. Cliquez sur **Ajouter une étape**.
4. Cliquez sur **Ajouter une action**, puis sélectionnez l'action que vous souhaitez ajouter à l'étape.

Action	Description
Basculer le serveur	Effectue le basculement d'un serveur cloud. Pour définir cette action, vous devez sélectionner un serveur cloud et configurer les paramètres du runbook disponibles pour cette action. Pour plus d'informations sur ces paramètres, voir "Paramètres du runbook" (p. 856). **Remarque** Si la sauvegarde du serveur que vous sélectionnez est chiffrée à l'aide du chiffrement comme propriété de l'ordinateur, l'action de **Basculer le serveur** est mise en pause et passe automatiquement à **Interaction requise**. Pour poursuivre l'exécution du runbook, vous devez fournir le mot de passe de la sauvegarde chiffrée.
Restaurer le serveur automatiquement	Effectue la restauration automatique d'un serveur cloud. Pour définir cette action, vous devez sélectionner un serveur cloud et configurer les paramètres du runbook disponibles pour cette action. Pour plus d'informations sur ces paramètres, voir "Paramètres du runbook" (p. 856).

Action	Description
	Remarque Les opérations de runbook prennent en charge la restauration automatique en mode manuel uniquement. Cela signifie que si vous démarrez le processus de restauration automatique en exécutant un runbook qui inclut une étape **Restaurer le serveur automatiquement**, la procédure nécessitera une interaction manuelle : vous devez restaurer l'ordinateur manuellement, et confirmer ou annuler le processus de restauration automatique à partir de l'onglet **Reprise d'activité après sinistre** > **Serveurs**.
Démarrer le serveur	Démarre un serveur cloud. Pour définir cette action, vous devez sélectionner un serveur cloud et configurer les paramètres du runbook disponibles pour cette action. Pour plus d'informations sur ces paramètres, voir "Paramètres du runbook" (p. 856). **Remarque** L'action **Démarrer le serveur** ne s'applique qu'aux opérations de basculement de test dans les runbooks. Si vous essayez d'exécuter une telle action, elle échoue et affiche le message d'erreur suivant : Échec : l'action ne s'applique pas à l'état actuel du serveur.
Arrêter le serveur	Arrête un serveur cloud. Pour définir cette action, vous devez sélectionner un serveur cloud et configurer les paramètres du runbook disponibles pour cette action. Pour plus d'informations sur ces paramètres, voir "Paramètres du runbook" (p. 856). **Remarque** L'action **Arrêter le serveur** ne s'applique pas aux opérations de basculement de test dans les runbooks. Si vous essayez d'exécuter une telle action, elle échoue et affiche le message d'erreur suivant : Échec : l'action ne s'applique pas à l'état actuel du serveur.
Opération manuelle	Une opération manuelle nécessite une interaction de la part de l'utilisateur. Pour définir cette action, vous devez entrer une description. Lorsqu'une séquence de runbook atteint une opération manuelle, le runbook est mis en pause et ne reprend que lorsqu'un utilisateur effectue l'opération manuelle requise, par exemple, clique sur le bouton de confirmation.
Exécuter le runbook	Exécute un autre runbook. Pour définir cette action, vous devez choisir un runbook. Un runbook ne peut contenir qu'une seule exécution d'un runbook donné. Par exemple, si vous avez ajouté l'action « Exécuter le runbook A », vous pouvez ajouter l'action « Exécuter le runbook B », mais vous ne pouvez pas ajouter une autre action « Exécuter le runbook A ».

5. Définissez les paramètres de runbook de l'action. Pour plus d'informations sur ces paramètres, voir "Paramètres du runbook" (p. 856).

6. [Facultatif] Pour ajouter une description de l'étape :
   a. Cliquez sur l'icône représentant des points de suspension, puis cliquez sur **Description**.
   b. Entrez une description de l'étape.
   c. Cliquez sur **Valider**.
7. Répétez les étapes 3 à 6 jusqu'à ce que vous ayez créé la séquence d'étapes et d'actions souhaitée.
8. [Facultatif] Pour changer le nom par défaut du runbook :
   a. Cliquez sur l'icône représentant des points de suspension.
   b. Entrez le nom du runbook.
   c. Entrez une description du runbook.
   d. Cliquez sur **Valider**.
9. Cliquez sur **Enregistrer**.
10. Cliquez sur **Fermer**.



Paramètres du runbook

Les paramètres du runbook sont des paramètres spécifiques que vous devez configurer pour définir une action de runbook. Il existe deux catégories de paramètres de runbook : les paramètres d'action et les paramètres de vérification d'achèvement.

Les paramètres d'action définissent le comportement du runbook en fonction de l'état initial de l'action ou du résultat.

Les paramètres de vérification d'achèvement garantissent que le serveur est disponible et fournit les services nécessaires. En cas d'échec de la vérification d'achèvement, l'action est considérée comme ayant échoué.

Le tableau suivant décrit les paramètres de runbook configurables pour chaque action.

Paramètre de runbook	Catégorie	Disponible pour l'action	Description
Continuer si l'action a déjà été effectuée	Paramètre d'action	• **Basculer le serveur** • **Démarrer le serveur** • **Arrêter le serveur** • **Restaurer le serveur automatiquement**	Ce paramètre définit le comportement du runbook lorsque l'action requise est déjà effectuée (par exemple, lorsqu'un basculement a déjà été effectué ou qu'un serveur est déjà en fonctionnement). Lorsqu'il est activé, le runbook émet un avertissement et continue le processus. Lorsqu'il est désactivé, l'action échoue et le runbook échoue également. Par défaut, ce paramètre est activé.
Continuer si l'action a échoué	Paramètre d'action	• **Basculer le serveur** • **Démarrer le serveur** • **Arrêter le serveur** • **Restaurer le serveur automatiquement**	Ce paramètre définit le comportement du runbook lorsque l'action requise échoue. Lorsqu'il est activé, le runbook affiche un avertissement, puis continue. Lorsqu'il est désactivé, l'action et le runbook échouent. Par défaut, ce paramètre est désactivé.
Ping adresse IP	Vérification de l'achèvement	• **Démarrer le serveur**	Le logiciel va procéder au ping de l'adresse IP de production du serveur Cloud jusqu'à ce que le serveur réponde ou que le délai d'expiration soit dépassé, selon la première éventualité.
Se connecter au port (443 par défaut)	Vérification de l'achèvement	• **Basculer le serveur** • **Démarrer le serveur**	Le logiciel va essayer de se connecter au serveur Cloud à l'aide de son adresse IP de production et du port que vous indiquez, jusqu'à ce qu'une connexion soit établie ou que le délai d'expiration soit dépassé, selon la première éventualité. De cette manière, vous pouvez vérifier la bonne exécution de l'application qui

Paramètre de runbook	Catégorie	Disponible pour l'action	Description
			écoute le port indiqué.
Délai d'expiration en minutes	Vérification de l'achèvement	• **Basculer le serveur** • **Démarrer le serveur**	Le délai d'expiration par défaut est de 10 minutes.

Opérations avec les runbooks

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Pour accéder à la liste des opérations, survolez un runbook, puis cliquez sur l'icône en forme de points de suspension. Lorsqu'un runbook n'est pas en cours d'exécution, les opérations suivantes sont disponibles :

- **Exécuter**
- **Modifier**
- **Cloner**
- **Supprimer**

Exécution d'un runbook

À chaque fois que vous cliquez sur **Exécuter**, vous êtes invité à saisir les paramètres d'exécution. Ces paramètres s'appliquent à toutes les opérations de basculement ou de restauration automatique incluses dans le runbook. Les runbooks indiqués dans les opérations **Exécuter le runbook** héritent de ces paramètres du runbook principal.

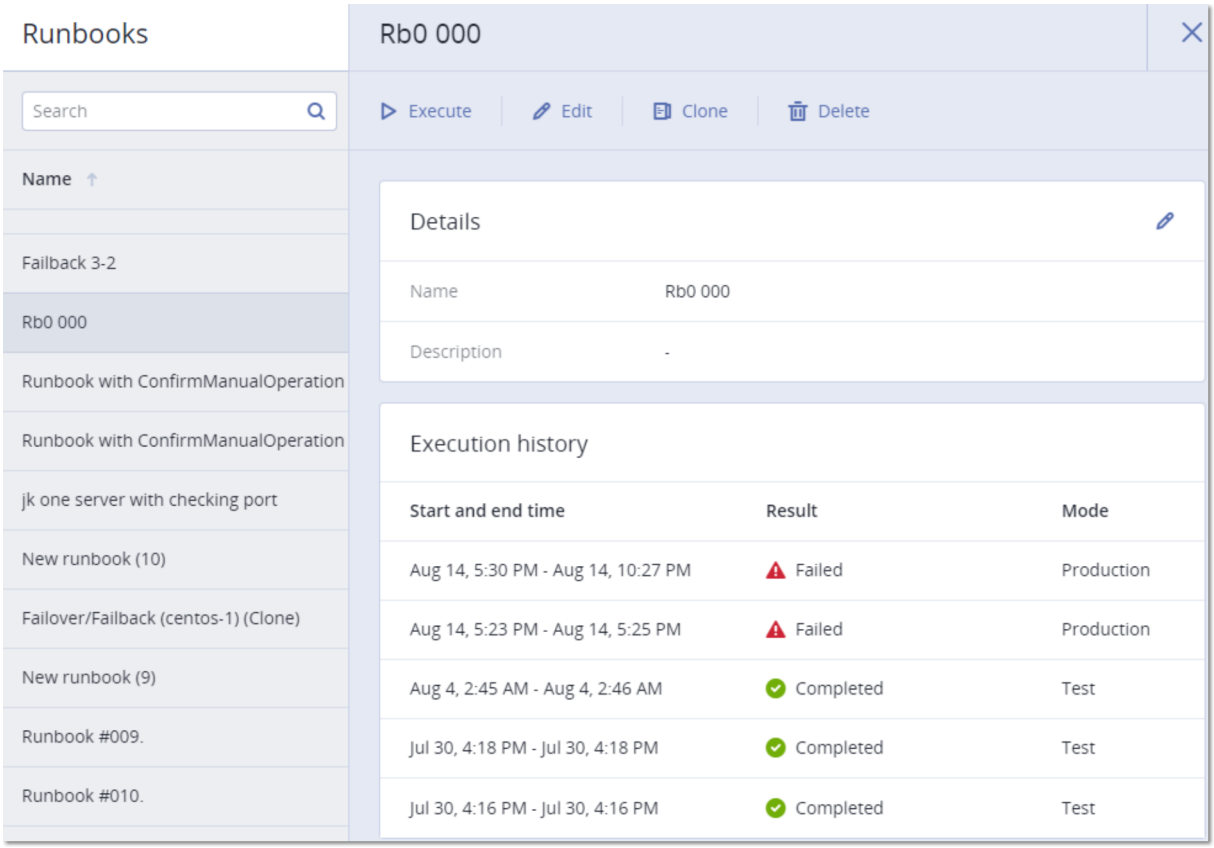
- **Mode basculement et restauration automatique**
  Choisissez si vous souhaitez réaliser un basculement test (par défaut) ou un basculement réel (production). Le mode de restauration automatique correspondra au mode de basculement choisi.
- **Point de récupération en mode basculement**
  Choisissez le point de récupération le plus récent (par défaut) ou sélectionnez un moment donné dans le passé. Dans le deuxième cas, les points de récupération situés le plus près avant la date et l'heure choisis seront sélectionnés pour chaque serveur.

Arrêt de l'exécution d'un runbook

Lors de l'exécution d'un runbook, vous pouvez sélectionner **Arrêter** dans la liste des opérations. Le logiciel terminera toutes les actions déjà démarrées, à l'exception de celles qui nécessitent une intervention de l'utilisateur.

Affichage de l'historique d'exécution

Lorsque vous sélectionnez un runbook dans l'onglet **Runbooks**, le logiciel affiche les détails du runbook et son historique d'exécution. Cliquez sur la ligne correspondant à une exécution spécifique pour afficher le journal d'exécution.



Configuration de la protection antivirus et antimalware

Remarque
Sur les ordinateurs Windows, la fonction de protection antimalware nécessite l'installation de l'agent pour la protection antimalware, et la fonction de filtrage d'URL nécessite l'installation de l'agent pour le filtrage d'URL. Ces agents sont installés automatiquement pour les ressources protégées si la **Protection antivirus et antimalware** et/ou les modules de **Filtrage d'URL** sont activés dans leurs plans de protection.

La protection contre les malwares dans Cyber Protection vous offre les avantages suivants :

- Protection optimale à toutes les étapes : proactive, active et réactive.
- Quatre technologies anti-malware intégrées pour vous offrir une protection de premier ordre à plusieurs niveaux.
- Gestion du service Microsoft Security Essentials et de l'antivirus Microsoft Defender.

  Remarque
  La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Important
Le fichier test EICAR est détecté uniquement lorsque l'option **Protection anti-malware Advanced** est activée dans le plan de protection. Cependant, les fonctionnalités antimalware de Cyber Protection ne sont pas affectées si le fichier test EICAR n'est pas détecté.

Plates-formes prises en charge

Les fonctionnalités de protection active antivirus et antimalware sont prises en charge sur les plates-formes suivantes.

Système d'exploitation	Version/Distribution
Windows	Windows 7 Service Pack 1 et versions ultérieures Windows Server 2008 R2 Service Pack 1 et versions ultérieures

Système d'exploitation	Version/Distribution
	Remarque Pour Windows 7, vous devez installer les mises à jour suivantes fournies par Microsoft avant d'installer l'agent de protection. • Mises à jour de sécurité étendues (ESU) pour Windows 7 • KB4474419 • KB4490628 Pour plus d'informations sur les mises à jour requises, reportez-vous à cet article de la base de connaissances.
Linux	Red Hat Linux 7.x, 8.x, 9.x CloudLinux 6.10, 7.x, 8.x CentOS 6.5 et dernières versions 6.x, 7.x, 8.x Ubuntu 16.04, 18.04, 20.04, 22.04, 22.10 Debian 8.x, 9.x, 10,x, 11.x Oracle Linux 7.x, 8.x, 9.x SUSE Enterprise Linux 15.x openSUSE Leap 15.x
macOS	macOS 10.13.x et versions ultérieures

Fonctionnalités prises en charge par plate-forme

Remarque
La protection antimalware pour Linux et macOS est disponible uniquement avec le pack antimalware Advanced.

Ensemble de fonctionnalités	Windows	Linux	macOS
Protection contre les virus et les malwares			
Fonctionnalité Active Protection totalement intégrée	Oui	Non	Non
Protection contre les malware en temps réel	Oui	Oui, avec le pack antimalware Advanced	Oui, avec le pack antimalware Advanced
Fonctionnalité avancée de protection contre les malwares en temps réel avec détection basée sur la signature locale	Oui	Oui	Oui

Ensemble de fonctionnalités	Windows	Linux	macOS
Protection contre les virus et les malwares			
Analyse statique pour les fichiers exécutables portables	Oui	Non	Oui*
Analyse anti-malware à la demande	Oui	Oui**	Oui
Protection du dossier réseau	Oui	Oui	Non
Protection côté serveur	Oui	Non	Non
Analyse des fichiers d'archive	Oui	Non	Oui
Analyse des lecteurs amovibles	Oui	Non	Oui
Analyse des fichiers nouveaux et modifiés uniquement	Oui	Non	Oui
Exclusions de fichier/dossier	Oui	Oui	Oui***
Exclusions des processus	Oui	Non	Oui
Moteur d'analyse du comportement	Oui	Non	Oui
Prévention des failles	Oui	Non	Non
Quarantaine	Oui	Oui	Oui
Nettoyage automatique de la zone de quarantaine	Oui	Oui	Oui
Filtrage d'URL (http/https)	Oui	Non	Non
Liste blanche à l'échelle de l'entreprise	Oui	Non	Oui
Gestion du pare-feu****	Oui	Non	Non
Gestion de l'antivirus Microsoft Defender*****	Oui	Non	Non
Gestion de Microsoft Security Essentials	Oui	Non	Non
Inscription et gestion de la protection contre les virus et les malwares via le centre de sécurité Windows	Oui	Non	Non
Pour plus d'informations sur les systèmes d'exploitation et leurs versions pris en charge, voir "Plates-formes prises en charge" (p. 860).			

***** L'analyse statique pour les fichiers exécutables portables est prise en charge uniquement pour les analyses planifiées sur macOS.

** Les conditions de démarrage ne sont pas prises en charge pour l'analyse à la demande sous Linux.

*** Les exclusions de fichier/dossier sont prises en charge uniquement lorsque vous spécifiez les fichiers et les dossiers qui ne seront pas analysés par la protection en temps réel ni par les analyses planifiées sur macOS.

**** La gestion du pare-feu est prise en charge sur Windows 8 et versions ultérieures.
Windows Server n'est pas compatible.

***** La gestion de l'antivirus Microsoft Defender est prise en charge sur Windows 8.1 et versions ultérieures.

Ensemble de fonctionnalités	Windows	Linux	macOS
Active Protection			
Détection d'un processus d'injection	Oui	Non	Non
Restauration automatique de fichiers affectés depuis le cache local	Oui	Oui	Oui
Auto-défense pour les fichiers de sauvegarde Acronis	Oui	Non	Non
Auto-défense pour le logiciel Acronis	Oui	Non	Oui (Uniquement les composants Active Protection et Antimalware)
Gestion des processus fiables/bloqués	Oui	Non	Oui
Exclusions des processus/dossiers	Oui	Oui	Oui
Détection des ransomware basée sur un comportement de processus (basé sur l'IA)	Oui	Oui	Oui
Détection du cryptominage basée sur un comportement de processus	Oui	Non	Non
Protection des lecteurs externes (HDD, lecteurs flash, cartes SD)	Oui	Non	Oui
Protection du dossier réseau	Oui	Oui	Oui
Protection côté serveur	Oui	Non	Non
Protection Zoom, Cisco Webex, Citrix Workspace et Microsoft Teams	Oui	Non	Non

Ensemble de fonctionnalités	Windows	Linux	macOS
Active Protection			
Pour plus d'informations sur les systèmes d'exploitation et leurs versions pris en charge, voir "Plates-formes prises en charge" (p. 860).			

Protection contre les virus et les malwares

Remarque
Certaines fonctionnalités peuvent nécessiter une licence supplémentaire, en fonction du modèle de gestion de licences appliqué.

Le module **Protection contre les virus et les malwares** protège vos ordinateurs Windows, Linux et macOS contre toutes les menaces de malwares récentes. Vous trouverez la liste complète des fonctionnalités antimalware prises en charge dans "Plates-formes prises en charge" (p. 860).

La protection contre les virus et les malwares est prise en charge et enregistrée dans le centre de sécurité Windows.

Fonctionnalités antimalware

- Détection des malwares dans les fichiers en mode temps réel et à la demande
- Détection des comportements malveillants dans les processus (Windows)
- Blocage de l'accès aux URL malveillantes (Windows)
- Placement des fichiers dangereux en quarantaine
- Ajout des applications d'entreprise de confiance à la liste d'autorisation

Types d'analyses

Vous pouvez configurer la protection contre les virus et les malwares pour qu'elle s'exécute en permanence en arrière-plan ou à la demande.

Protection en temps réel

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

La protection en temps réel vérifie tous les fichiers ouverts ou en cours d'exécution sur un ordinateur afin de prévenir les menaces liées à des malwares.

Pour éviter les éventuels problèmes de compatibilité et de performances, la protection en temps réel ne peut fonctionner en même temps que d'autres solutions antivirus qui proposent également des fonctionnalités de protection en temps réel. L'état des autres solutions antivirus installées est

déterminé via le centre de sécurité Windows. Si la machine Windows est déjà protégée par une autre solution antivirus, la protection en temps réel est automatiquement désactivée.

Pour activer la protection en temps réel, désactivez ou désinstallez l'autre solution antivirus. La protection en temps réel peut remplacer automatiquement la protection en temps réel de Microsoft Defender.

Remarque
Sur les machines fonctionnant sous Windows Server, Microsoft Defender ne sera pas désactivé automatiquement lors de l'activation de la protection en temps réel. Un administrateur doit désactiver manuellement Microsoft Defender pour éviter les problèmes de compatibilité potentiels.

Vous pouvez choisir l'un des modes d'analyse suivants :

- La détection **Mode sur accès intelligent** signifie que le programme anti-malware s'exécute en arrière-plan et analyse le système de votre ordinateur de manière active et constante, à la recherche de virus et d'autres menaces malveillantes, pendant tout le temps où votre système est sous tension. Les malware seront détectés dans les deux cas lorsqu'un fichier est en cours d'exécution et lors de diverses opérations impliquant le fichier, comme son ouverture en vue de sa lecture ou de sa modification.
- La détection **Lors de l'exécution** signifie que seuls les fichiers exécutables seront analysés lors de leur exécution, afin de garantir qu'ils sont inoffensifs et qu'ils n'endommageront pas votre machine ni vos données. La copie d'un fichier infecté ne sera pas détectée.

Analyse planifiée

L'analyse anti-malware est réalisée de façon planifiée.

Vous pouvez choisir l'un des modes d'analyse suivants.

- Mode **Analyse rapide** – Vérifie uniquement les fichiers système de la ressource.
- Mode **Analyse complète** – Vérifie tous les fichiers de votre ressource.
- Mode **Analyse personnalisée** – Vérifie les fichiers/dossiers ajoutés par l'administrateur au plan de protection.

Une fois les analyses antimalware effectuées, vous pouvez consulter les informations relatives aux ressources affectées par des menaces dans le widget **Surveillance** > **Vue d'ensemble** > Affectés récemment.

Paramètres de protection contre les virus et les malwares

Cette section décrit les fonctionnalités que vous pouvez configurer dans le module **Protection antivirus et antimalware** d'un plan de protection. Pour savoir comment créer un plan de protection, voir "Création d'un plan de protection" (p. 223).

Vous pouvez configurer les fonctionnalités suivantes d'un plan de protection dans le module Protection antivirus et antimalware :

- "Active Protection" (p. 866)
- "Protection anti-malware Advanced" (p. 867)
- "Protection du dossier réseau" (p. 867)
- "Protection côté serveur" (p. 868)
- "Autoprotection" (p. 869)
- "Détection d'un processus de cryptominage" (p. 870)
- "Quarantaine" (p. 871)
- "Moteur de comportement" (p. 871)
- "Prévention des failles" (p. 872)
- "Protection en temps réel" (p. 874)
- "Planifier l'analyse" (p. 875)
- "Exclusions de protection" (p. 878)

Remarque
Tous les systèmes d'exploitation ne prennent pas en charge les fonctions de protection Antivirus & Antimalware. Pour plus d'informations sur les fonctionnalités et systèmes d'exploitation pris en charge, voir "Plates-formes prises en charge" (p. 860). Certaines fonctionnalités nécessitent une certaine licence pour être disponibles dans votre plan de protection.

Active Protection

Active Protection protège votre système des logiciels malveillants connus sous le nom de ransomware, qui chiffrent les fichiers et exigent une rançon en échange de la clé de chiffrement.

Paramètre par défaut : **Activé**.

Remarque
Un agent de protection doit être installé sur la machine protégée. Pour plus d'informations sur les fonctionnalités et systèmes d'exploitation pris en charge, voir "Plates-formes prises en charge" (p. 860).

Pour configurer Active Protection

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Active Protection**.
3. Dans la section **Action lors de la détection**, sélectionnez l'une des options disponibles :

   Paramètre par défaut : **Revenir à l'utilisation du cache**

   - **Notifier uniquement** : le logiciel génère une alerte sur le processus suspecté d'activité de ransomware.

- **Arrêter le processus** : le logiciel génère une alerte et arrête le processus suspecté d'activité de ransomware.
- **Revenir à l'utilisation du cache** : le logiciel génère une alerte, arrête le processus et annule les modifications apportées aux fichiers, à l'aide du cache de service.

4. Cliquez sur **Terminé** pour appliquer les options sélectionnées à votre plan de protection.

Protection anti-malware Advanced

Ce moteur utilise une base de données améliorée de signatures de virus afin d'améliorer l'efficacité de la détection des malwares, aussi bien lors des analyses rapides que lors des analyses complètes.

Important
Cette fonctionnalité est disponible uniquement si le pack de protection Advanced Security est activé. Pour plus d'informations, voir https://www.acronis.com/fr-fr/products/cloud/cyber-protect/security/

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Pour configurer la protection antimalware avancée

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Dans la section **Protection anti-malware Advanced**, utilisez le bouton-bascule pour activer le moteur basé sur les signatures locales.

Remarque
La protection contre les virus et les malwares pour macOS et Linux nécessitent également le moteur basé sur la signature locale. Pour Windows, la protection contre les virus et les malwares est disponible avec ou sans ce moteur.

Protection du dossier réseau

La fonctionnalité **Protection du dossier réseau** définit si la protection antivirus et antimalware protège les dossiers réseau mappés en tant que lecteurs locaux. La protection s'applique aux dossiers partagés via les protocoles SMB ou NFS.

Pour configurer la protection du dossier réseau

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Protection du dossier réseau**.
3. Ajoutez les fichiers à l'endroit où vous souhaitez sauvegarder les dossiers réseau :
   - Par exemple, si votre ressource est une ressource Windows, saisissez dans le champ **Windows** le chemin d'accès au fichier Windows dans lequel vous souhaitez sauvegarder les

dossiers réseau. Valeur par défaut : C:\ProgramData\Acronis\Restored Network Files.

- Par exemple, si votre ressource est une ressource macOS, saisissez dans le champ **macOS** le chemin d'accès aux fichiers macOS dans lequel vous souhaitez sauvegarder les dossiers réseau. Valeur par défaut : /Library/Application Support/Acronis/Restored Network Files/.

Remarque
Saisissez le chemin d'un dossier local. Les dossiers réseau, y compris les dossiers sur les lecteurs mappés, ne sont pas pris en charge en tant que destinations de sauvegarde des dossiers réseau.

4. Cliquez sur **Terminé** pour appliquer les options sélectionnées à votre plan de protection.

Protection côté serveur

Cette fonctionnalité définit si la protection active protège les dossiers réseau que vous partagez des connexions extérieures entrantes en provenance d'autres serveurs du réseau, qui pourraient potentiellement apporter des menaces.

Paramètre par défaut : **Désactivé**.

Remarque
La protection côté serveur n'est pas prise en charge sous Linux.

Pour configurer des connexions fiables

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Protection côté serveur**.
3. Utilisez le bouton-bascule **Protection côté serveur** pour l'activer.
4. Sélectionnez l'onglet **Fiable**.
5. Dans le champ **Connexions fiables**, cliquez sur **Ajouter** pour définir les connexions qui seront autorisées à modifier les données.
6. Dans le champ **Nom d'ordinateur/Compte**, saisissez le nom de l'ordinateur et le compte de l'ordinateur sur lequel l'agent de protection est installé. Par exemple, `MyComputer\TestUser`.
7. Dans le champ **Nom de l'hôte**, saisissez le nom d'hôte de l'ordinateur autorisé à se connecter à l'ordinateur utilisant l'agent de protection.
8. Cliquez sur la coche à droite pour enregistrer la définition de connexion.
9. Cliquez sur **Valider**.

Pour configurer les connexions bloquées

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Protection côté serveur**.

3. Utilisez le bouton-bascule **Protection côté serveur** pour l'activer.
4. Sélectionnez l'onglet **Bloqué**.
5. Dans le champ **Connexions bloquées**, cliquez sur **Ajouter** pour définir les connexions qui ne seront pas autorisées à modifier les données.
6. Dans le champ **Nom d'ordinateur/Compte**, saisissez le nom de l'ordinateur et le compte de l'ordinateur sur lequel l'agent de protection est installé. Par exemple, `MyComputer\TestUser`.
7. Dans le champ **Nom de l'hôte**, saisissez le nom d'hôte de l'ordinateur autorisé à se connecter à l'ordinateur utilisant l'agent de protection.
8. Cochez la case à droite pour enregistrer la définition de connexion.
9. Cliquez sur **Valider**.

Autoprotection

L'autoprotection empêche les modifications non autorisées des propres processus du logiciel, de ses enregistrements du registre et de ses fichiers exécutables et de configuration, ainsi que des sauvegardes contenues dans vos dossiers locaux.

Les administrateurs peuvent activer l'**Autoprotection** sans activer **Active Protection**.

Paramètre par défaut : **Activé**.

Remarque
L'autoprotection n'est pas prise en charge sous Linux.

Pour activer l'autoprotection

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Autoprotection**.
3. Utilisez le bouton-bascule **Autoprotection** pour l'activer.

Activer la protection par mot de passe

1. Une fois la fonctionnalité **Autoprotection** activée, vous pouvez activer la fonctionnalité **Protection par mot de passe** à l'aide du bouton-bascule.
2. Cliquez sur **Générer un nouveau mot de passe** pour générer un mot de passe afin de modifier ou de supprimer des agents locaux.
3. Cliquez sur **Copier**, puis collez-le dans un emplacement sécurisé, car il sera demandé si vous souhaitez modifier la liste des composants localement.

Important
Le mot de passe ne sera pas disponible une fois que vous aurez fermé la fenêtre. Pour appliquer ce mot de passe aux terminaux, les paramètres du plan de protection doivent être enregistrés.

4. Cliquez sur **Fermer**.

La **protection par mot de passe** empêche les utilisateurs ou les logiciels non autorisés de désinstaller l'agent pour Windows ou de modifier ses composants. Ces actions sont possibles uniquement avec un mot de passe qu'un administrateur peut fournir.

Un mot de passe n'est jamais requis pour les actions suivantes :

- Mise à jour de l'installation en exécutant le programme d'installation au niveau local
- Mise à jour de l'installation à l'aide de la console Cyber Protect
- Réparation de l'installation

Paramètre par défaut : **Désactivé**

Pour plus d'informations sur l'activation de la **protection par mot de passe**, consultez la section Empêcher la désinstallation ou la modification non autorisée d'agents.

Détection d'un processus de cryptominage

Un malware de cryptominage réduit les performances des applications utiles, accroît la facture d'électricité, peut causer des plantages système et même endommager le matériel à cause d'un usage abusif. La fonctionnalité **Détection d'un processus de cryptominage** protège vos terminaux des malwares de cryptominage et évite toute utilisation non autorisée de ressources informatiques.

Les administrateurs peuvent activer la **Détection d'un processus de cryptominage** sans activer **Active Protection**. Paramètre par défaut : **Activé**.

Remarque
La détection de processus de cryptominage n'est pas prise en charge sous Linux.

Pour configurer la protection du dossier réseau

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Détection d'un processus de cryptominage**.
3. Utilisez le bouton-bascule **Détecter des processus de cryptominage** pour activer ou désactiver la fonctionnalité.
4. Sélectionnez l'opération à effectuer sur les processus suspectés d'activités de cryptominage :

   Paramètre par défaut : **Arrêter le processus**

   - **Notifier uniquement** : le logiciel génère une alerte.
   - **Arrêter le processus** : le logiciel génère une alerte et arrête le processus.
5. Cliquez sur **Terminé** pour appliquer les options sélectionnées à votre plan de protection.

Quarantaine

La quarantaine est un dossier utilisé pour isoler les fichiers suspects (probablement infectés) ou potentiellement dangereux.

Pour configurer la quarantaine

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Quarantaine**.
3. Dans le champ **Supprimer les fichiers mis en quarantaine après**, vous pouvez définir la période (en jours) après laquelle les fichiers en quarantaine seront supprimés.
   Paramètre par défaut : **30 jours**
4. Cliquez sur **Valider**.

Pour plus d'informations sur cette fonctionnalité, consultez la section Quarantaine.

Moteur de comportement

La fonctionnalité **Moteur de comportement** protège un système des malwares en adoptant une approche comportementale heuristique pour repérer les processus malveillants.

Paramètre par défaut : **Activé**.

Remarque
Le moteur de comportement n'est pas pris en charge sous Linux.

Pour configurer la protection du dossier réseau

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Moteur de comportement**.
3. Utilisez le bouton-bascule **Moteur de comportement** pour activer ou désactiver la fonctionnalité.
4. Dans la section **Action lors de la détection**, sélectionnez l'action que le logiciel exécutera lors de la détection d'une activité de malware :
   Paramètre par défaut : **Quarantaine**
   - **Notifier uniquement** : le logiciel génère une alerte au sujet du processus suspecté d'activité de malware.
   - **Arrêter le processus** : le logiciel génère une alerte et arrête le processus suspecté d'activité de malware.
   - **Quarantaine** : le logiciel génère une alerte, arrête le processus et place le fichier exécutable dans le dossier de quarantaine.
5. Cliquez sur **Terminé** pour appliquer les options sélectionnées à votre plan de protection.

Prévention des failles

Important
Cette fonctionnalité est disponible uniquement si le pack de protection Advanced Security est activé. Pour plus d'informations, voir https://www.acronis.com/fr-fr/products/cloud/cyber-protect/security/

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

La prévention des exploits détecte les processus infectés et les empêche de se diffuser et d'exploiter les vulnérabilités logicielles sur les systèmes. Lorsqu'une faille est détectée, le logiciel peut générer une alerte et arrêter le processus suspecté d'être à l'origine de la faille.

L'option Prévention des failles est disponible uniquement à partir des versions 12.5.23130 de l'agent (21.08, publiée en août 2020) ou versions ultérieures.

Paramètre par défaut : **Activé** pour les plans de protection nouvellement créés, et **Désactivé** pour les plans de protection existants, créés avec des versions antérieures de l'agent.

Remarque
La prévention des failles n'est pas prise en charge sous Linux.

Vous pouvez sélectionner l'action que le programme doit exécuter lors de la détection d'une faille et les méthodes de prévention des failles appliquées par le programme.

Pour configurer la prévention des exploits

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Prévention des failles**.
3. Dans la section **Action lors de la détection**, sélectionnez l'une des options disponibles :

   Paramètre par défaut : **Arrêter le processus**

   - **Notifier uniquement**
     Le logiciel générera une alerte au sujet du processus suspecté d'activités d'exploit.
   - **Arrêter le processus**
     Le logiciel générera une alerte et arrêtera le processus suspecté d'activités d'exploit.
4. Dans la section **Techniques de prévention des failles activées**, sélectionnez les options disponibles que vous souhaitez appliquer :

   Paramètre par défaut : **Toutes les méthodes sont activées**

   - **Protection de la mémoire**
     Détecte et stoppe les modifications suspectes des droits d'exécution des pages de mémoire. Des processus malveillants apportent de telles modifications aux propriétés de page pour

activer l'exécution de shellcodes depuis des zones de mémoire non exécutables telles que les piles et segments.

- **Protection contre la programmation orientée retour (ROP)**
  Détecte et stoppe les tentatives d'utilisation de la technique d'exploit ROP.
- **Protection contre la réaffectation de privilèges**
  Détecte et stoppe les tentatives de réaffectation de privilèges effectuées par un code ou une application non autorisés. La réaffectation de privilèges est utilisée par un code malveillant pour obtenir entièrement l'accès à la machine attaquée puis exécuter des tâches essentielles et sensibles. Un code non autorisé n'a pas le droit d'accéder à des ressources critiques du système ni de modifier les paramètres système.
- **Protection contre l'injection de code**
  Détecte et stoppe l'injection de code malveillant dans des processus distants. L'injection de code est utilisée pour masquer l'intention malveillante d'une application derrière des processus propres ou bénins, en vue d'éviter la détection par des solutions anti-malware.

5. Cliquez sur **Terminé** pour appliquer les options sélectionnées à votre plan de protection.

Remarque
Les processus identifiés comme fiables dans la liste d'exclusion ne seront pas analysés à la recherche de failles.

Autoriser les processus à modifier des sauvegardes

Le paramètre **Autoriser des processus particuliers à modifier des sauvegardes** est disponible uniquement lorsque l'option **Autoprotection** est activée.

Elle s'applique aux fichiers qui disposent d'une extension .tibx, .tib ou .tia et qui sont situés dans des dossiers locaux.

Ce paramètre vous permet de préciser les processus qui sont autorisés à modifier les fichiers de sauvegarde, même si ces fichiers sont protégés par l'autoprotection. Elle est très utile, par exemple, si vous supprimez des fichiers de sauvegarde ou les déplacez vers un emplacement différent à l'aide d'un script.

Si ce paramètre est désactivé, les fichiers de sauvegarde ne peuvent être modifiés que par les processus signés par le fournisseur du logiciel de sauvegarde. Cela permet au logiciel d'appliquer des règles de rétention et de supprimer des sauvegardes lorsqu'un utilisateur le demande depuis l'interface Web. Les autres processus, qu'ils soient suspects ou non, ne peuvent pas modifier les sauvegardes.

Si ce paramètre est activé, vous pouvez autoriser d'autres processus à modifier les sauvegardes. Spécifiez le chemin d'accès complet au processus exécutable, en commençant par la lettre du lecteur.

Paramètre par défaut : **Désactivé**.

Protection en temps réel

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

La **protection en temps réel** recherche en permanence des virus et d'autres menaces malveillantes dans votre système informatique pendant toute la durée d'activité du système, à moins qu'elle ne soit mise en pause par l'utilisateur de l'ordinateur.

Paramètre par défaut : **Activé**.

Important
Cette fonctionnalité est disponible uniquement si le pack de protection Advanced Security est activé. Pour plus d'informations, voir https://www.acronis.com/fr-fr/products/cloud/cyber-protect/security/

Pour configurer la protection en temps réel

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Protection en temps réel**.
3. Dans la liste déroulante **Action lors de la détection**, sélectionnez l'une des options disponibles :
   Paramètre par défaut : **Quarantaine**
   - **Notifier uniquement**

     Le logiciel génère une alerte concernant le processus suspecté d'activité de ransomware.
   - **Bloquer et notifier**

     Le logiciel bloque le processus et génère une alerte au sujet du processus suspecté d'activité de malware.
   - **Quarantaine**
4. Le logiciel génère une alerte, arrête le processus et place le fichier exécutable dans le dossier de quarantaine.
5. Dans la section **Mode d'analyse**, sélectionnez l'action que le logiciel exécutera lors de la détection d'un virus ou d'une autre menace malveillante :
   Paramètre par défaut : **Mode sur accès intelligent**
   - **Mode sur accès intelligent** : surveille toutes les activités du système et analyse automatiquement les fichiers lorsque quelqu'un y accède en lecture ou en écriture, ou à chaque lancement d'un programme.

- **Lors de l'exécution** : n'analyse automatiquement que les fichiers exécutables lors de leur lancement, afin de vérifier qu'ils sont inoffensifs et qu'ils n'endommageront pas votre ordinateur ni vos données.

6. Cliquez sur **Valider**.

Planifier l'analyse

L'analyse à la demande recherche des virus dans votre système informatique, en fonction du calendrier précisé. Une analyse complète vérifie tous les fichiers de votre machine, alors qu'une analyse rapide vérifie uniquement les fichiers système de la machine.

Pour configurer une analyse planifiée

Paramètres par défaut :

- L'**Analyse personnalisée** est désactivée.
- Des analyses **Rapides** et **Complètes** sont planifiées.

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Planifier l'analyse**.
3. Utilisez le bouton-bascule pour activer le type d'analyse que vous souhaitez appliquer à votre ordinateur.

Types d'analyse disponibles :

- **Complète** : elle est plus longue que l'analyse rapide, car chaque fichier est vérifié.
- **Rapide** : analyse uniquement les emplacements courants où se trouvent habituellement les malwares sur l'ordinateur.
- **Personnalisée** : analyse les fichiers/dossiers sélectionnés par l'administrateur du plan Protection.

> **Remarque**
> Vous pouvez planifier les trois analyses (**Rapide**, **Complète** et **Personnalisée**) dans un même plan de protection.

Pour configurer une analyse personnalisée

- Utilisez le bouton-bascule **Analyse personnalisée** pour activer ou désactiver ce type d'analyse.
- Dans la liste déroulante **Action lors de la détection**, sélectionnez l'une des options disponibles :

Paramètre par défaut : **Quarantaine**

Quarantaine

Le logiciel génère une alerte et place le fichier exécutable dans le dossier de quarantaine.

Notifier uniquement

Le logiciel génère une alerte au sujet du processus suspecté d'être un malware.

Champs	Description
Planifiez l'exécution de la tâche à l'aide des événements suivants	Ce paramètre définit le moment où la tâche sera exécutée. Les valeurs suivantes sont disponibles : • **Planifier selon l'horaire** : il s'agit du paramètre par défaut. La tâche sera exécutée selon l'horaire spécifié. • **Lorsque l'utilisateur se connecte au système** : par défaut, la connexion de n'importe quel utilisateur lancera la tâche. Vous pouvez modifier ce paramètre pour que seul un compte utilisateur spécifique déclenche la tâche. • **Lorsqu'un utilisateur se déconnecte du système** : par défaut, la déconnexion de n'importe quel utilisateur lancera la tâche. Vous pouvez modifier ce paramètre pour que seul un compte utilisateur spécifique déclenche la tâche. **Remarque** La tâche ne sera pas lancée lors d'un arrêt du système. Dans la configuration de planification, un arrêt est différent d'une déconnexion. • **Au démarrage du système** : la tâche sera exécutée au démarrage du système d'exploitation. • **À l'arrêt du système** : la tâche sera exécutée à l'arrêt du système d'exploitation.
Type de planification	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Mensuelle :** sélectionnez les mois et les semaines ou jours du mois pendant lesquels la tâche sera exécutée. • **Quotidienne** : il s'agit du paramètre par défaut. Sélectionnez les jours de la semaine au cours desquels la tâche sera exécutée. • **Horaire :** sélectionnez les jours de la semaine, le nombre de répétitions et l'intervalle d'exécution de la tâche.
Débuter à	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants** Sélectionnez l'heure exacte à laquelle la tâche sera exécutée.
Exécuter sur une plage de date	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**.

Champs	Description
	Configurez une plage pendant laquelle la planification configurée sera effective.
Précisez un compte utilisateur dont la connexion au système d'exploitation lancera une tâche	Ce champ apparaît si vous avez sélectionné l'option **Lorsque l'utilisateur se connecte au système** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Tout utilisateur** : utilisez cette option si vous souhaitez que la connexion de n'importe quel utilisateur déclenche la tâche. • **L'utilisateur suivant** : utilisez cette option si vous souhaitez que la connexion d'un compte utilisateur spécifique déclenche la tâche.
Précisez un compte utilisateur dont la déconnexion du système d'exploitation lancera une tâche	Ce champ apparaît si vous avez sélectionné l'option **Lorsqu'un utilisateur se déconnecte du système** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Tout utilisateur** : utilisez cette option si vous souhaitez que la déconnexion de n'importe quel utilisateur déclenche la tâche. • **L'utilisateur suivant** : utilisez cette option si vous souhaitez que la déconnexion d'un compte utilisateur spécifique déclenche la tâche.
Conditions de démarrage	Définit toutes les conditions qui doivent être remplies simultanément pour que la tâche soit exécutée. Les conditions de démarrage des analyses antimalware sont semblables aux conditions de démarrage du module **Sauvegarde** qui sont décrites dans la section Conditions de démarrage. Vous pouvez définir les conditions de démarrage suivantes : • **Répartir les heures de démarrage de tâche dans une fenêtre de temps :** cette option vous permet de définir le délai pour la tâche afin d'éviter les goulots d'étranglement au niveau du réseau. Vous pouvez indiquer le délai en heures ou minutes. Par exemple, si l'heure de démarrage par défaut est 10 h et que le délai est 60 minutes, la tâche démarrera entre 10 h et 11 h. • **Si la machine est arrêtée, exécutez les tâches ratées lors du démarrage de la machine** • **Empêcher l'activation du mode veille ou veille prolongée lors de l'exécution de la tâche** : cette option fonctionne uniquement pour les machines sous Windows. • **Si les conditions de démarrage ne sont pas remplies, exécutez quand même la tâche au bout de :** spécifiez la période après laquelle la tâche sera lancée, quelles que soient les autres conditions de démarrage.

Champs	Description
	Remarque Les conditions de démarrage ne sont pas prises en charge sous Linux.

- Cochez la case **Analyser uniquement les fichiers nouveaux ou modifiés** si vous souhaitez analyser uniquement les fichiers nouveaux ou modifiés.

Paramètre par défaut : **Activé**

- Deux options supplémentaires sont affichées pour l'**Analyse personnalisée** et l'**analyse complète** uniquement :

1. **Analyser les fichiers d'archive**

   Paramètre par défaut : **Activé**.

   Profondeur de réapparition maximum

   Paramètre par défaut : **16**

   Le nombre de niveaux d'archive incorporées qui peuvent être analysés. Par exemple, Document MIME > archive ZIP > archive Office > contenu du document.

   Taille maximale

   Paramètre par défaut : **100**

   Taille maximale d'un fichier d'archive à analyser.

2. **Analyser les lecteurs amovibles**

Paramètre par défaut : **Désactivé**

- **Lecteurs réseau mappés (à distance)**
- **Périphériques de stockage USB** (Par exemple, une clé USB ou des disques durs externes)
- **CD/DVD**

Remarque
L'analyse des lecteurs amovibles n'est pas prise en charge sous Linux.

Exclusions de protection

Les exclusions de protection vous permettent d'éliminer les faux positifs lorsqu'un programme fiable est considéré comme étant un ransomware ou un malware. Vous pouvez définir des éléments fiables et bloqués en les ajoutant à la liste des exclusions de la protection.

Dans la liste des éléments fiables, vous pouvez ajouter des fichiers, des processus et des dossiers afin qu'ils soient considérés dans le système comme étant sûrs et pour éviter toute détection ultérieure les concernant.

Dans la liste des éléments bloqués, vous pouvez ajouter des processus et des hachages. Cette option garantit que ces processus seront bloqués et que votre ressource sera sécurisée.

Élément exclu de la protection	Bloqué	Fiable
Hachage	Lorsqu'un hachage est ajouté à la liste des éléments bloqués, le système arrête le processus en fonction du hachage fourni. Par exemple, lorsque vous ajoutez ce hachage MD5, 938c2cc0dcc05f2b68c4287040cfcf71, le processus associé à ce hachage est bloqué.	Lorsqu'un hachage est ajouté à la liste des éléments fiables, le système connaît les processus que la surveillance doit ignorer en fonction du hachage fourni. Par exemple, lorsque vous ajoutez ce hachage MD5, 938c2cc0dcc05f2b68c4287040cfcf71, le processus associé à ce hachage est considéré comme fiable et est exclu de la surveillance.
Processus	Lorsqu'un processus est ajouté à la liste des éléments bloqués, le système sait que ces processus doivent être surveillés et ces derniers sont toujours bloqués. Par exemple, si vous ajoutez ce chemin C:\Users\user1\application\nppInstaller.exe à la liste des éléments bloqués, ce processus spécifique est bloqué et, lorsque vous essayez de l'ouvrir, son démarrage n'est pas autorisé.	Lorsqu'un processus est ajouté à la liste des éléments fiables, le système sait que ces processus doivent être exclus de la surveillance. **Remarque** Les processus signés par Microsoft sont toujours fiables. Par exemple, si vous ajoutez ce chemin C:\Users\user1\application\nppInstaller.exe, ce processus spécifique est exclu de la surveillance et l'antivirus n'interfère pas avec ce processus.
Fichier/dossier		Lorsqu'un fichier ou un dossier est ajouté à la liste des éléments fiables, le système sait que ces fichiers ou dossiers doivent toujours être considérés comme étant fiables, et qu'ils n'ont pas besoin d'être analysés/surveillés.

Pour indiquer les éléments toujours fiables

1. Ouvrez le plan de protection.
2. Développez le module **Protection contre les virus et les malwares**.

3. Sélectionnez l'option **Exclusions**.
   La fenêtre **Exclusions de protection** s'affiche.
4. Dans la section **Éléments fiables**, cliquez sur **Ajouter** pour sélectionner l'une des options disponibles :
   - Pour définir des fichiers, dossiers ou processus comme étant fiables, sélectionnez l'option **Fichier/dossier/processus**. La fenêtre **Ajouter un fichier/dossier/processus** s'ouvre.
     - Dans le champ **Fichier/dossier/processus**, saisissez le chemin d'accès de chaque processus, dossier ou fichier sur une nouvelle ligne. Dans la section **Description**, saisissez une brève description qui vous permettra de reconnaître votre modification dans la liste des éléments fiables.
     - Cochez la case **Ajouter en tant que fichier/dossier** pour définir le fichier/dossier comme étant fiable.
       Exemples de description de dossier : D:\dossier\, /home/Dossier/dossier2, F:\
     - Cochez la case **Ajouter en tant que processus** pour définir un processus comme étant fiable. Les processus sélectionnés seront exclus de la surveillance.

     Remarque
     Spécifiez le chemin d'accès complet au processus exécutable, en commençant par la lettre du lecteur. Par exemple, `C:\Windows\Temp\er76s7sdkh.exe`.

     Remarque
     Les chemins d'accès du réseau local sont pris en charge. Exemple : \\localhost\folderpath\file.exe
   - Sélectionnez l'option **Hachage** pour ajouter des hachages MD5 à la liste des éléments fiables. La fenêtre **Ajouter un hachage** s'ouvre.
     - Vous pouvez insérer ici des hachages MD5 sur des lignes séparées pour qu'ils soient inclus comme étant fiables dans la liste Exclusions de protection. Sur la base de ces hachages, Cyber Protection exclura les processus décrits par les hachages MD5 de la surveillance.

Paramètre par défaut : Aucune exclusion n'est définie par défaut.

Pour indiquer les éléments toujours bloqués

1. Ouvrez le plan de protection.
2. Développez le module **Protection contre les virus et les malwares**.
3. Sélectionnez l'option **Exclusions de protection**. La fenêtre **Exclusions de protection** s'affiche.

   Dans la section **Éléments bloqués**, cliquez sur **Ajouter** pour sélectionner l'une des options disponibles :
   - Pour bloquer des processus, sélectionnez l'option **Processus**. La fenêtre **Ajouter un processus** s'ouvre.
     - Dans le champ **Processus**, saisissez le chemin d'accès de chaque processus sur une nouvelle ligne. Dans le champ **Description**, saisissez une brève description qui vous permettra de reconnaître votre modification dans la liste des éléments bloqués.

Remarque
Ces processus ne pourront pas démarrer tant qu'Active Protection sera activé sur la machine.

- Pour bloquer des hachages, sélectionnez l'option **Hachage**. La fenêtre **Ajouter un hachage** s'ouvre.
  - Dans le champ **Hachage**, saisissez le hachage de chaque processus sur une nouvelle ligne. Dans le champ **Description**, saisissez une brève description qui vous permettra de reconnaître votre modification dans la liste des éléments bloqués.

Paramètre par défaut : Aucune exclusion n'est définie par défaut.

Caractères génériques

Pour spécifier des dossiers, vous pouvez utiliser les caractères génériques * et ?. L'astérisque (*) remplace zéro ou plusieurs caractères. Le point d'interrogation (?) remplace un seul caractère. Il n'est pas possible d'utiliser des variables d'environnement telles que `%AppData%`.

Vous pouvez utiliser un caractère générique (*) pour ajouter des éléments aux listes d'exclusion.

- Les caractères génériques peuvent être utilisés au milieu ou à la fin d'une description.

Exemple des caractères génériques acceptés dans des descriptions :

C:*.pdf

D:\dossiers\fichier.*

C:\Users*\AppData\Roaming

- Les caractères génériques ne peuvent pas être utilisés au début d'une description.

Exemple des caractères génériques non acceptés dans des descriptions :

*.docx

*:\dossier\

Variables

Vous pouvez utiliser des variables pour ajouter des éléments à la liste Exclusions de protection, avec les restrictions suivantes :

- Pour Windows, seules les variables SYSTEM sont prises en charge. Les variables propres à l'utilisateur, par exemple %USERNAME% ou %APPDATA% ne sont pas prises en charge. Les variables avec {username} ne sont pas prises en charge. Pour plus d'informations, voir https://ss64.com/nt/syntax-variables.html.
- Pour macOS, les variables d'environnement ne sont pas prises en charge.
- Pour Linux, les variables d'environnement ne sont pas prises en charge.

Exemples de formats pris en charge :

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

Description

Dans le champ **Description**, vous pouvez ajouter des notes concernant les exclusions que vous avez ajoutées à la liste Exclusions de protection. Voici quelques suggestions des notes que vous pouvez ajouter :

- Motifs et objectifs de l'exclusion.
- Nom réel du fichier de l'exclusion de hachage.
- Horodatage.

Si plusieurs éléments ont été ajoutés dans une seule entrée, il ne peut y avoir qu'un seul commentaire pour tous les éléments.

Active Protection dans l'édition Cyber Backup Standard

Dans Cyber Backup Standard Edition, Active Protection est un module distinct du plan de protection. Par conséquent, il peut être configuré différemment et appliqué à différents terminaux ou groupes de terminaux.

Dans toutes les autres éditions du service de cyberprotection, Active Protection fait partie du module **Antivirus et antimalware** du plan de protection.

Paramètre par défaut : **Activé**.

Remarque
Un agent de protection doit être installé sur la machine protégée. Pour plus d'informations sur les fonctionnalités et systèmes d'exploitation pris en charge, voir "Plates-formes prises en charge" (p. 860).

Fonctionnement

Active Protection surveille les processus en cours d'exécution sur la machine protégée. Lorsqu'un processus tiers essaye de chiffrer des fichiers ou de miner de la cryptomonnaie, Active Protection génère une alerte et exécute des actions supplémentaires précisées dans le plan de protection.

Par ailleurs, Active Protection empêche les modifications non autorisées des propres processus du logiciel de sauvegarde, de ses enregistrements du registre, et de ses fichiers exécutables et de configuration, ainsi que des sauvegardes contenues dans les dossiers locaux.

Pour identifier les processus malveillants, Active Protection utilise des heuristiques comportementales. Active Protection compare la chaîne d'actions réalisées par un processus avec la chaîne d'événements enregistrée dans la base de données des schémas de comportement

malveillants. Cette approche permet à Active Protection de détecter de nouveaux malware grâce à leur comportement typique.

Paramètres d'Active Protection dans Cyber Backup Standard

Dans l'édition Cyber Backup Standard, vous pouvez configurer les foncitonnalités Active Protection suivantes :

- Action lors de la détection
- Autoprotection
- Protection du dossier réseau
- Protection côté serveur
- Détection d'un processus de cryptominage
- Exclusions

Remarque
La fonctionnalité Active Protection pour Linux prend en charge les paramètres suivants : Action lors de la détection, Protection du dossier réseau et Exclusions. Le paramètre Protection du dossier réseau est toujours actif et n'est pas configurable.

Action lors de la détection

Dans la section **Action lors de la détection**, sélectionnez l'une des options disponibles :

- **Notifier uniquement**
  Le logiciel générera une alerte au sujet du processus suspecté d'activité de ransomware.
- **Arrêter le processus**
  Le logiciel générera une alerte et arrêtera le processus suspecté d'activité de ransomware.
- **Revenir à l'utilisation du cache**
  Le logiciel générera une alerte, arrêtera le processus et annulera les modifications apportées aux fichiers, à l'aide du cache de service.

Paramètre par défaut : **Revenir à l'utilisation du cache**.

L'autoprotection empêche les modifications non autorisées des propres processus du logiciel, de ses enregistrements du registre et de ses fichiers exécutables et de configuration, ainsi que des sauvegardes contenues dans vos dossiers locaux.

Les administrateurs peuvent activer l'**Autoprotection** sans activer **Active Protection**.

Paramètre par défaut : **Activé**.

Remarque
L'autoprotection n'est pas prise en charge sous Linux.

Pour activer l'autoprotection

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Autoprotection**.
3. Utilisez le bouton-bascule **Autoprotection** pour l'activer.

Activer la protection par mot de passe

1. Une fois la fonctionnalité **Autoprotection** activée, vous pouvez activer la fonctionnalité **Protection par mot de passe** à l'aide du bouton-bascule.
2. Cliquez sur **Générer un nouveau mot de passe** pour générer un mot de passe afin de modifier ou de supprimer des agents locaux.
3. Cliquez sur **Copier**, puis collez-le dans un emplacement sécurisé, car il sera demandé si vous souhaitez modifier la liste des composants localement.

   Important
   Le mot de passe ne sera pas disponible une fois que vous aurez fermé la fenêtre. Pour appliquer ce mot de passe aux terminaux, les paramètres du plan de protection doivent être enregistrés.

4. Cliquez sur **Fermer**.

La **protection par mot de passe** empêche les utilisateurs ou les logiciels non autorisés de désinstaller l'agent pour Windows ou de modifier ses composants. Ces actions sont possibles uniquement avec un mot de passe qu'un administrateur peut fournir.

Un mot de passe n'est jamais requis pour les actions suivantes :

- Mise à jour de l'installation en exécutant le programme d'installation au niveau local
- Mise à jour de l'installation à l'aide de la console Cyber Protect
- Réparation de l'installation

Paramètre par défaut : **Désactivé**

Pour plus d'informations sur l'activation de la **protection par mot de passe**, consultez la section Empêcher la désinstallation ou la modification non autorisée d'agents.

Protection du dossier réseau

Le paramètre **Protéger vos dossiers réseau mappés en tant que lecteurs locaux** définit si Active Protection protège les dossiers réseau qui sont mappés en tant que lecteurs locaux contre les processus malveillants locaux.

Ce paramètre s'applique aux fichiers partagés via les protocoles SMB ou NFS.

Si un fichier était situé à l'origine sur un lecteur mappé, il ne peut pas être sauvegardé dans l'emplacement d'origine lorsqu'il est extrait du cache à l'aide de l'action **Revenir à l'utilisation du cache**. Il sera en fait sauvegardé dans le dossier indiqué dans ce paramètre. Le dossier par défaut est `C:\ProgramData\Acronis\Restored Network Files` pour Windows, et

`Library/Application Support/Acronis/Restored Network Files/` pour macOS. Si ce dossier n'existe pas, il sera créé. Si vous souhaitez modifier ce chemin, choisissez un dossier local. Les dossiers réseau, y compris les dossiers sur les lecteurs mappés, ne sont pas pris en charge.

Paramètre par défaut : **Activé**.

Cette fonctionnalité définit si la protection active protège les dossiers réseau que vous partagez des connexions extérieures entrantes en provenance d'autres serveurs du réseau, qui pourraient potentiellement apporter des menaces.

Paramètre par défaut : **Désactivé**.

Remarque
La protection côté serveur n'est pas prise en charge sous Linux.

Pour configurer des connexions fiables

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Protection côté serveur**.
3. Utilisez le bouton-bascule **Protection côté serveur** pour l'activer.
4. Sélectionnez l'onglet **Fiable**.
5. Dans le champ **Connexions fiables**, cliquez sur **Ajouter** pour définir les connexions qui seront autorisées à modifier les données.
6. Dans le champ **Nom d'ordinateur/Compte**, saisissez le nom de l'ordinateur et le compte de l'ordinateur sur lequel l'agent de protection est installé. Par exemple, `MyComputer\TestUser`.
7. Dans le champ **Nom de l'hôte**, saisissez le nom d'hôte de l'ordinateur autorisé à se connecter à l'ordinateur utilisant l'agent de protection.
8. Cliquez sur la coche à droite pour enregistrer la définition de connexion.
9. Cliquez sur **Valider**.

Pour configurer les connexions bloquées

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Protection côté serveur**.
3. Utilisez le bouton-bascule **Protection côté serveur** pour l'activer.
4. Sélectionnez l'onglet **Bloqué**.
5. Dans le champ **Connexions bloquées**, cliquez sur **Ajouter** pour définir les connexions qui ne seront pas autorisées à modifier les données.
6. Dans le champ **Nom d'ordinateur/Compte**, saisissez le nom de l'ordinateur et le compte de l'ordinateur sur lequel l'agent de protection est installé. Par exemple, `MyComputer\TestUser`.

7. Dans le champ **Nom de l'hôte**, saisissez le nom d'hôte de l'ordinateur autorisé à se connecter à l'ordinateur utilisant l'agent de protection.
8. Cochez la case à droite pour enregistrer la définition de connexion.
9. Cliquez sur **Valider**.

Un malware de cryptominage réduit les performances des applications utiles, accroît la facture d'électricité, peut causer des plantages système et même endommager le matériel à cause d'un usage abusif. La fonctionnalité **Détection d'un processus de cryptominage** protège vos terminaux des malwares de cryptominage et évite toute utilisation non autorisée de ressources informatiques.

Les administrateurs peuvent activer la **Détection d'un processus de cryptominage** sans activer **Active Protection**. Paramètre par défaut : **Activé**.

Remarque
La détection de processus de cryptominage n'est pas prise en charge sous Linux.

Pour configurer la protection du dossier réseau

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Détection d'un processus de cryptominage**.
3. Utilisez le bouton-bascule **Détecter des processus de cryptominage** pour activer ou désactiver la fonctionnalité.
4. Sélectionnez l'opération à effectuer sur les processus suspectés d'activités de cryptominage :

   Paramètre par défaut : **Arrêter le processus**

   - **Notifier uniquement** : le logiciel génère une alerte.
   - **Arrêter le processus** : le logiciel génère une alerte et arrête le processus.
5. Cliquez sur **Terminé** pour appliquer les options sélectionnées à votre plan de protection.

Les exclusions de protection vous permettent d'éliminer les faux positifs lorsqu'un programme fiable est considéré comme étant un ransomware ou un malware. Vous pouvez définir des éléments fiables et bloqués en les ajoutant à la liste des exclusions de la protection.

Dans la liste des éléments fiables, vous pouvez ajouter des fichiers, des processus et des dossiers afin qu'ils soient considérés dans le système comme étant sûrs et pour éviter toute détection ultérieure les concernant.

Dans la liste des éléments bloqués, vous pouvez ajouter des processus et des hachages. Cette option garantit que ces processus seront bloqués et que votre ressource sera sécurisée.

Élément exclu de la protection	Bloqué	Fiable
Hachage	Lorsqu'un hachage est ajouté à la liste des éléments bloqués, le système arrête le processus en fonction du hachage fourni. Par exemple, lorsque vous ajoutez ce hachage MD5, 938c2cc0dcc05f2b68c4287040cfcf71, le processus associé à ce hachage est bloqué.	Lorsqu'un hachage est ajouté à la liste des éléments fiables, le système connaît les processus que la surveillance doit ignorer en fonction du hachage fourni. Par exemple, lorsque vous ajoutez ce hachage MD5, 938c2cc0dcc05f2b68c4287040cfcf71, le processus associé à ce hachage est considéré comme fiable et est exclu de la surveillance.
Processus	Lorsqu'un processus est ajouté à la liste des éléments bloqués, le système sait que ces processus doivent être surveillés et ces derniers sont toujours bloqués. Par exemple, si vous ajoutez ce chemin C:\Users\user1\application\nppInstaller.exe à la liste des éléments bloqués, ce processus spécifique est bloqué et, lorsque vous essayez de l'ouvrir, son démarrage n'est pas autorisé.	Lorsqu'un processus est ajouté à la liste des éléments fiables, le système sait que ces processus doivent être exclus de la surveillance. **Remarque** Les processus signés par Microsoft sont toujours fiables. Par exemple, si vous ajoutez ce chemin C:\Users\user1\application\nppInstaller.exe, ce processus spécifique est exclu de la surveillance et l'antivirus n'interfère pas avec ce processus.
Fichier/dossier		Lorsqu'un fichier ou un dossier est ajouté à la liste des éléments fiables, le système sait que ces fichiers ou dossiers doivent toujours être considérés comme étant fiables, et qu'ils n'ont pas besoin d'être analysés/surveillés.

Pour indiquer les éléments toujours fiables

1. Ouvrez le plan de protection.
2. Développez le module **Protection contre les virus et les malwares**.
3. Sélectionnez l'option **Exclusions**.
   La fenêtre **Exclusions de protection** s'affiche.

4. Dans la section **Éléments fiables**, cliquez sur **Ajouter** pour sélectionner l'une des options disponibles :
   - Pour définir des fichiers, dossiers ou processus comme étant fiables, sélectionnez l'option **Fichier/dossier/processus**. La fenêtre **Ajouter un fichier/dossier/processus** s'ouvre.
     - Dans le champ **Fichier/dossier/processus**, saisissez le chemin d'accès de chaque processus, dossier ou fichier sur une nouvelle ligne. Dans la section **Description**, saisissez une brève description qui vous permettra de reconnaître votre modification dans la liste des éléments fiables.
     - Cochez la case **Ajouter en tant que fichier/dossier** pour définir le fichier/dossier comme étant fiable.
       Exemples de description de dossier : D:\dossier\, /home/Dossier/dossier2, F:\
     - Cochez la case **Ajouter en tant que processus** pour définir un processus comme étant fiable. Les processus sélectionnés seront exclus de la surveillance.

       Remarque
       Spécifiez le chemin d'accès complet au processus exécutable, en commençant par la lettre du lecteur. Par exemple, `C:\Windows\Temp\er76s7sdkh.exe`.

       Remarque
       Les chemins d'accès du réseau local sont pris en charge. Exemple : \\localhost\folderpath\file.exe
   - Sélectionnez l'option **Hachage** pour ajouter des hachages MD5 à la liste des éléments fiables. La fenêtre **Ajouter un hachage** s'ouvre.
     - Vous pouvez insérer ici des hachages MD5 sur des lignes séparées pour qu'ils soient inclus comme étant fiables dans la liste Exclusions de protection. Sur la base de ces hachages, Cyber Protection exclura les processus décrits par les hachages MD5 de la surveillance.

Paramètre par défaut : Aucune exclusion n'est définie par défaut.

Pour indiquer les éléments toujours bloqués

1. Ouvrez le plan de protection.
2. Développez le module **Protection contre les virus et les malwares**.
3. Sélectionnez l'option **Exclusions de protection**. La fenêtre **Exclusions de protection** s'affiche.

   Dans la section **Éléments bloqués**, cliquez sur **Ajouter** pour sélectionner l'une des options disponibles :
   - Pour bloquer des processus, sélectionnez l'option **Processus**. La fenêtre **Ajouter un processus** s'ouvre.
     - Dans le champ **Processus**, saisissez le chemin d'accès de chaque processus sur une nouvelle ligne. Dans le champ **Description**, saisissez une brève description qui vous permettra de reconnaître votre modification dans la liste des éléments bloqués.

     Remarque
     Ces processus ne pourront pas démarrer tant qu'Active Protection sera activé sur la machine.

- Pour bloquer des hachages, sélectionnez l'option **Hachage**. La fenêtre **Ajouter un hachage** s'ouvre.
  - Dans le champ **Hachage**, saisissez le hachage de chaque processus sur une nouvelle ligne. Dans le champ **Description**, saisissez une brève description qui vous permettra de reconnaître votre modification dans la liste des éléments bloqués.

Paramètre par défaut : Aucune exclusion n'est définie par défaut.

Caractères génériques

Pour spécifier des dossiers, vous pouvez utiliser les caractères génériques * et ?. L'astérisque (*) remplace zéro ou plusieurs caractères. Le point d'interrogation (?) remplace un seul caractère. Il n'est pas possible d'utiliser des variables d'environnement telles que `%AppData%`.

Vous pouvez utiliser un caractère générique (*) pour ajouter des éléments aux listes d'exclusion.

- Les caractères génériques peuvent être utilisés au milieu ou à la fin d'une description.

Exemple des caractères génériques acceptés dans des descriptions :

C:*.pdf

D:\dossiers\fichier.*

C:\Users*\AppData\Roaming

- Les caractères génériques ne peuvent pas être utilisés au début d'une description.

Exemple des caractères génériques non acceptés dans des descriptions :

*.docx

*:\dossier\

Variables

Vous pouvez utiliser des variables pour ajouter des éléments à la liste Exclusions de protection, avec les restrictions suivantes :

- Pour Windows, seules les variables SYSTEM sont prises en charge. Les variables propres à l'utilisateur, par exemple %USERNAME% ou %APPDATA% ne sont pas prises en charge. Les variables avec {username} ne sont pas prises en charge. Pour plus d'informations, voir https://ss64.com/nt/syntax-variables.html.
- Pour macOS, les variables d'environnement ne sont pas prises en charge.
- Pour Linux, les variables d'environnement ne sont pas prises en charge.

Exemples de formats pris en charge :

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

Description

Dans le champ **Description**, vous pouvez ajouter des notes concernant les exclusions que vous avez ajoutées à la liste Exclusions de protection. Voici quelques suggestions des notes que vous pouvez ajouter :

- Motifs et objectifs de l'exclusion.
- Nom réel du fichier de l'exclusion de hachage.
- Horodatage.

Si plusieurs éléments ont été ajoutés dans une seule entrée, il ne peut y avoir qu'un seul commentaire pour tous les éléments.

Filtrage d'URL

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Les malwares sont souvent distribués par des sites malveillants ou infectés et font appel à une méthode d'infection appelée téléchargement furtif.

La fonctionnalité de filtrage d'URL vous permet de protéger les machines des menaces comme les malwares ou l'hameçonnage, en provenance d'Internet. Vous pouvez protéger votre organisation en bloquant l'accès de l'utilisateur aux sites Web dont le contenu est malveillant.

La fonctionnalité de filtrage d'URL vous permet aussi de contrôler l'utilisation d'Internet afin de respecter les réglementations externes et les règles internes de l'entreprise. Vous pouvez configurer l'accès aux sites Web en fonction de la catégorie à laquelle ils appartiennent. Le filtrage d'URL prend actuellement en charge 44 catégories de sites Web et permet de gérer leur accès.

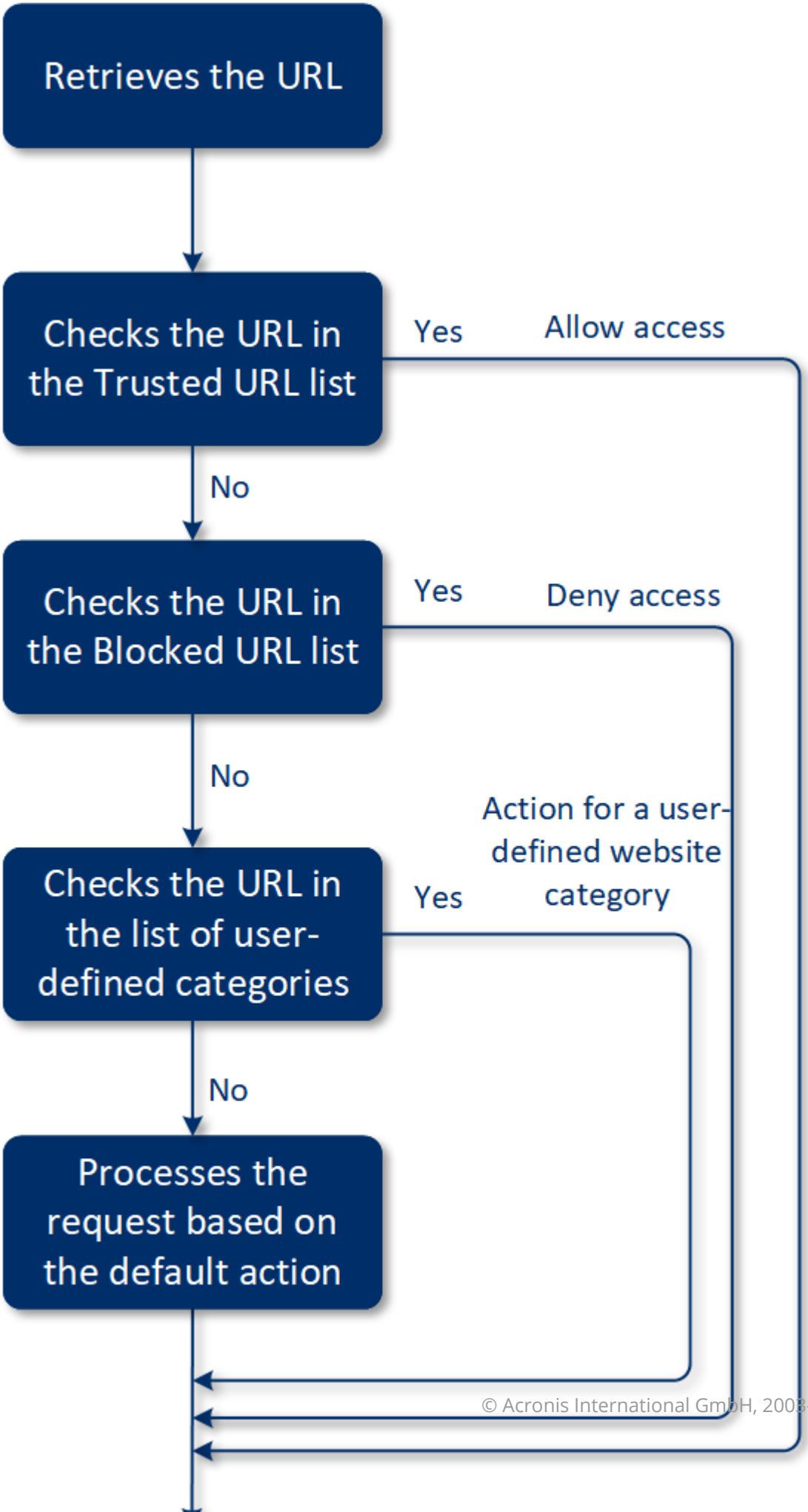
Pour le moment, les connexions HTTP/HTTPS sur les machines Windows sont vérifiées par l'agent de protection.

La fonctionnalité de filtrage des URL nécessite une connexion Internet.

Remarque
Afin d'éviter d'éventuels soucis de compatibilité avec les versions 15.0.26692 et précédentes de l'agent de protection (version C21.03 HF1), la fonctionnalité de filtrage d'URL sera automatiquement désactivée si une autre solution antivirus est détectée, ou si le service de Centre de sécurité Windows n'est pas présent dans le système.
Dans les agents de protection ultérieurs, les problèmes de compatibilité sont résolus de sorte que le filtrage d'URL est toujours activé selon la règle.

Fonctionnement

Un utilisateur saisit une URL dans un navigateur. L'intercepteur obtient le lien et l'envoie à l'agent de protection. L'agent reçoit l'URL, procède à son analyse syntaxique, et consulte les résultats. L'intercepteur redirige l'utilisateur vers la page comportant les messages avec les actions disponibles pour accéder manuellement à la page demandée.

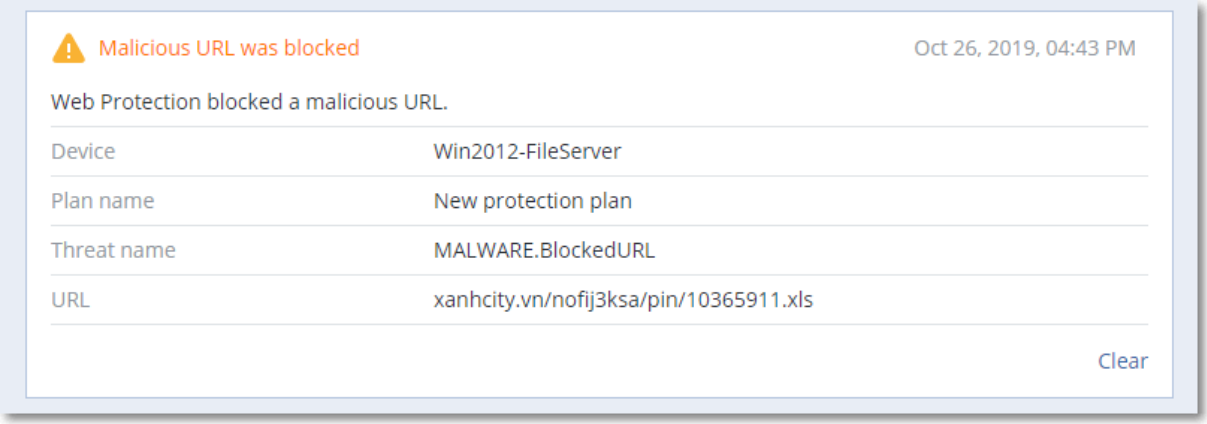


Procédure de configuration du filtrage d'URL

En général, la configuration du filtrage d'URL se compose des étapes suivantes :

1. Vous créez un plan de protection avec le module de **filtrage d'URL** activé.
2. Spécifiez les réglages du filtrage d'URL (voir ci-dessous).
3. Appliquez le plan de protection aux machines.

Pour consulter les URL qui ont été bloquées, accédez à **Surveillance** > **Alertes**.



Paramètres du filtrage d'URL

Vous pouvez définir les paramètres suivants pour le module de filtrage d'URL.

Accès à un site Web malveillant

Spécifiez l'action à exécuter lorsqu'un utilisateur ouvre un site Web malveillant :

- **Notifier uniquement** : le logiciel génère une alerte sur le processus suspecté d'activité de ransomware.
- **Bloquer** : bloque l'accès au site Web malveillant. L'utilisateur ne peut pas accéder au site Web et une alerte d'avertissement est générée.
- **Toujours demander à l'utilisateur** : demande à l'utilisateur s'il souhaite quand même accéder au site Web ou revenir en arrière.

Catégories à filtrer

Il existe 44 catégories de sites Web pour lesquelles vous pouvez configurer l'accès :

- **Autoriser** – autoriser l'accès aux sites Web appartenant à la catégorie sélectionnée.
- **Refuser** – refuser l'accès aux sites Web appartenant à la catégorie sélectionnée.

Par défaut, toutes les catégories sont autorisées.

Afficher toutes les notifications pour les URL bloquées par catégorie – si elles sont activées, vous recevrez toutes les notifications affichées dans la zone de notification pour les URL bloquées par catégorie. Si un site Web possède plusieurs sous-domaines, alors le système génère également des notifications pour eux ; il se peut donc que le nombre de notifications soit élevé.

Vous pouvez trouver les descriptions des catégories dans le tableau ci-dessous :

	Catégorie de site Web	Description
1	**Publicités**	Cette catégorie couvre les domaines dont le but principal est de proposer des publicités.
2	**Forums**	Cette catégorie couvre les forums et les sites Web de type question–réponse. Elle ne couvre pas les sections particulières des sites Web des entreprises, dans lesquelles les clients posent des questions.
3	**Sites Web personnels**	Cette catégorie couvre les sites Web personnels et tous les types de blog : individuels, collectifs et même ceux des entreprises. Un blog est un journal intime publié sur Internet. Il se compose d'entrées (« publications ») généralement affichées en ordre chronologique inversé, de façon à ce que la publication la plus récente apparaisse en premier.
4	**Sites Web professionnels/d'entreprise**	C'est une vaste catégorie qui couvre les sites Web professionnels qui n'appartiennent habituellement à aucune autre catégorie.
5	**Logiciel d'ordinateur**	Cette catégorie couvre les sites Web qui proposent des logiciels d'ordinateur, généralement soit des logiciels open source, soit des gratuiciels, soit des partagiciels. Elle peut également couvrir certaines boutiques en ligne.
6	**Médicaments**	Cette catégorie couvre les sites Web liés aux médicaments, à l'alcool ou aux cigares, qui contiennent des discussions sur l'utilisation ou la vente de médicaments ou d'équipement médical légaux, d'alcool ou de produits à base de tabac. Veuillez noter que les drogues illicites sont couvertes dans la catégorie Drogues.
7	**Enseignement**	Cette catégorie couvre les sites Web appartenant aux institutions pédagogiques officielles, dont ceux en dehors des domaines .edu. Elle comprend également des sites Web éducatifs, tels qu'une encyclopédie.
8	**Divertissement**	Cette catégorie couvre les sites Web qui apportent des informations liées aux activités artistiques et aux musées, ainsi que les sites qui évaluent ou notent du contenu tel que des films, de la musique ou de l'art.
9	**Partage de fichiers**	Cette catégorie couvre les sites Web de partage de fichiers, où

		un utilisateur peut transférer des fichiers et les partager avec d'autres. Elle couvre également les sites Web de partage BitTorrent et les traqueurs BitTorrent.
10	**Finance**	Cette catégorie couvre les sites Web appartenant à toutes les banques du monde qui proposent un accès en ligne. Certaines coopératives de crédit et autres institutions financières sont également prises en compte. Toutefois, certaines banques locales peuvent ne pas être prises en compte.
11	**Jeux d'argent**	Cette catégorie couvre les sites Web de jeux d'argent. Il s'agit des sites Web de type « casino en ligne » ou « loterie en ligne », qui nécessitent généralement un paiement avant qu'un utilisateur puisse parier de l'argent dans des jeux de roulette, poker, black jack ou similaires en ligne. Certains sont légitimes, ce qui signifie qu'il existe une chance de gagner ; d'autres sont frauduleux, ce qui signifie qu'il n'existe aucune chance de gagner. Les sites Web d'astuces et solutions pour les paris, qui décrivent les façons dont gagner de l'argent en pariant et sur les sites Web de loterie en ligne, sont également détectés.
12	**Jeux**	Cette catégorie couvre les sites Web qui proposent des jeux en ligne, généralement basés sur des applets Adobe Flash ou Java. La détection ne couvre pas le fait que le jeu soit gratuit ou nécessite un abonnement ; les sites Web de style casino sont toutefois détectés sous la catégorie Jeux d'argent. Cette catégorie ne prend pas en compte : • Les sites Web officiels des sociétés qui développent des jeux vidéos (à moins qu'ils ne produisent des jeux en ligne) • Les sites Web de discussion sur les jeux • Les sites Web sur lesquels vous pouvez télécharger des jeux qui ne sont pas des jeux en ligne (certains sont couverts dans la catégorie Activités illégales) • Les jeux qui nécessitent qu'un utilisateur télécharge et exécute un fichier exécutable, comme World of Warcraft ; ceux-ci peuvent être évités par divers moyens, comme un pare-feu
13	**Gouvernement**	Cette catégorie couvre les sites Web gouvernementaux, dont les sites des institutions et services gouvernementaux et des ambassades.
14	**Piratage**	Cette catégorie couvre les sites Web qui contiennent des outils de piratage, des articles sur le sujet, et des plates-formes de discussion pour pirates. Elle couvre également les exploitations d'offres de sites Web pour des plates-formes courantes, qui facilitent le piratage de compte Facebook ou Gmail.

15	**Activités illégales**	Il s'agit d'une vaste catégorie liée au contenu haineux, violent ou raciste, qui a pour but de bloquer les catégories suivantes des sites Web : • Sites Web appartenant à des organisations terroristes • Sites Web au contenu raciste ou xénophobe • Sites Web traitant de sports agressifs, et/ou faisant la promotion de la violence
16	**Santé et forme physique**	Cette catégorie couvre les sites Web associés aux institutions médicales, ceux liés à la prévention et au traitement des maladies, et ceux qui apportent des informations sur la perte de poids, les régimes, les stéroïdes, les anabolisants ou les HCH, ainsi que les sites Web fournissant des informations concernant la chirurgie esthétique.
17	**Loisirs**	Cette catégorie couvre les sites Web qui présentent des ressources liées aux activités généralement réalisées pendant le temps libre d'un individu, comme les collections, les travaux manuels et le vélo.
18	**Hébergement Web**	Cette catégorie couvre les services gratuits et commerciaux d'hébergement de sites Web, qui permettent à des particuliers et à des organisations de créer et publier des pages Web.
19	**Téléchargements illégaux**	Cette catégorie couvre les sites Web liés au piratage de logiciels, y compris : • Les sites Web traqueurs pair à pair (BitTorrent, emule, DC++) connus pour aider à distribuer du contenu protégé sans le consentement du détenteur des droits d'auteur • Les sites Web et forums de discussion de warez (logiciel commercial piraté) • Les sites Web qui fournissent aux utilisateurs des cracks, des générateurs de clés et des numéros de série destinés à faciliterl'utilisation illégale d'un logiciel Il se peut également que certains de ces sites Websoient détectés dans la catégorie pornographie ou alcool/cigares, étant donné qu'ils utilisent souvent des publicités pornographiques ou pour l'alcool pour gagner de l'argent.
20	**Messagerie instantanée**	Cette catégorie couvre les sites Web de messagerie et de chat qui permettent aux utilisateurs de discuter en temps réel. Elle détectera également yahoo.com et gmail.com, étant donné que les deux comprennent un service de messagerie intégré.
21	**Emplois**	Cette catégorie couvre les sites Web qui présentent des tableaux d'offres d'emploi, des petites annonces d'emploi et des opportunités de carrière, ainsi que des agrégateurs de tels

		services. Elle ne couvre pas les agences de recrutement ou les pages d'offres d'emploi sur les sites Web habituels des entreprises.
22	**Contenu adulte**	Cette catégorie couvre le contenu étiqueté par un créateur de site Web comme destiné à un public adulte. Elle couvre une grande variété de sites Web, du Kama Sutra aux sites Web d'éducation sexuelle, en passant par la pornographie « dure ».
23	**Drogues**	Cette catégorie couvre les sites Web qui partagent des informations sur les drogues à usage récréatif et illégales. Elle couvre également les sites Web traitant des drogues en développement ou dont l'utilisation se répand.
24	**Actualités**	Cette catégorie couvre les sites Web d'actualités contenant du texte et des vidéos. Elle s'efforce de couvrir les sites Web d'actualités aussi bien mondiales que locales ; toutefois, il se peut que certains petits sites Web d'actualités locales ne soient pas couverts.
25	**Rencontres en ligne**	Cette catégorie couvre les sites Web de rencontres en ligne (gratuits et payants) où les utilisateurs peuvent rechercher des personnes à l'aide de certains critères. Ils peuvent également publier leur profil pour que d'autres puissent les trouver. Cette catégorie comprend les sites Web de rencontres en ligne aussi bien gratuits que payants. La plupart des réseaux sociaux populaires pouvant également être utilisés comme des sites Web de rencontres en ligne, certains sites Web populaires comme Facebook sont également détectés dans cette catégorie. Nous vous recommandons d'utiliser cette catégorie avec la catégorie Réseaux sociaux.
26	**Paiements en ligne**	Cette catégorie couvre les sites Web proposant des paiements ou des transferts d'argent. Elle détecte les sites Web de paiement populaires tels que PayPal ou Moneybookers. Elle détecte également de façon heuristique les pages Web des sites Web habituels demandant des informations de carte de crédit, ce qui permet de détecter des boutiques en ligne masquées, inconnues ou illégales.
27	**Partage de photos**	Cette catégorie couvre les sites Web de partage de photos dont le but principal est de permettre aux utilisateurs de transférer et partager des photos.
28	**Boutiques en ligne**	Cette catégorie couvre les boutiques en ligne connues. Un site Web est considéré comme étant une boutique en ligne s'il vend des biens ou des services en ligne.
29	**Pornographie**	Cette catégorie couvre les sites Web contenant du contenu

		érotique et de la pornographie. Elle comprend les sites Web gratuits aussi bien que payants. Elle couvre les sites Web qui fournissent des images, histoires et vidéos, et détecte également le contenu pornographique des sites Web à contenu mixte.
30	**Portails**	Cette catégorie couvre les sites Web qui agrègent les informations de multiples sources et domaines, et qui proposent généralement des fonctionnalités telles que des moteurs de recherche, un courrier électronique, des actualités et des informations de divertissement.
31	**Radio**	Cette catégorie couvre les sites Web qui offrent des services de streaming de musique sur Internet, allant des stations de Web radio aux sites proposant du contenu audio à la demande (gratuit ou payant).
32	**Religion**	Cette catégorie couvre les sites Web qui promeuvent une religion ou une secte. Elle couvre également les forums de discussion associés à une ou plusieurs religion(s).
33	**Moteurs de recherche**	Cette catégorie couvre les sites Web de moteurs de recherche tels que Google, Yahoo et Bing.
34	**Réseaux sociaux**	Cette catégorie couvre les sites Web de réseaux sociaux. Elle comprend MySpace.com, Facebook.com, Bebo.com, etc. Toutefois, les réseaux sociaux spécialisés, comme YouTube.com, seront répertoriés dans la catégorie Vidéo/Photo.
35	**Sport**	Cette catégorie couvre les sites Web qui proposent des informations, actualités et tutoriels liés au sport.
36	**Suicide**	Cette catégorie couvre les sites Web qui promeuvent, proposent ou défendent le suicide. Elle ne couvre pas les cliniques de prévention du suicide.
37	**Journaux à scandale**	Cette catégorie est principalement conçue pour la pornographie « douce » et les sites Web « people ». Il se peut que cette catégorie répertorie des sous-catégories de nombreux sites Web d'actualités de style journaux à scandale. La détection de cette catégorie se base également sur des heuristiques.
38	**Perte de temps**	Cette catégorie couvre les sites Web sur lesquels les individus ont tendance à passer beaucoup de temps. Cela peut comprendre des sites Web d'autres catégories telles que les réseaux sociaux ou le divertissement.
39	**Voyage**	Cette catégorie couvre les sites Web qui proposent des offres de voyage et d'équipement de voyage, ainsi que des critiques et notations de destinations de voyage.
40	**Vidéos**	Cette catégorie couvre les sites Web qui hébergent diverses

		photos ou vidéos, qu'elles soient transférées par les utilisateurs ou fournies par divers fournisseurs de contenu. Elle comprend des sites Web tels que YouTube, Metacafe, Google Video, et des sites Web de photo tels que Picasa ou Flickr. Elle détectera également des vidéos incorporées dans d'autres sites Web ou blogs.
41	**Dessins animés violents**	Cette catégorie couvre les sites Web qui partagent et proposent des dessins animés ou manga qui peuvent être inadaptés aux mineurs en raison de contenu violent ou sexuel, ou de langage explicite, ou qui permettent d'en discuter. Elle ne couvre pas les sites Web proposant des dessins animés traditionnels tels que « Tom et Jerry ».
42	**Armes**	Cette catégorie couvre les sites Web qui proposent la vente, l'échange, la fabrication ou l'utilisation d'armes. Elle couvre également le matériel de chasse et l'utilisation d'armes à air comprimé et à balles BB, ainsi que les armes de corps-à-corps.
43	**E-mail**	Cette catégorie couvre les sites Web qui fournissent des fonctionnalités d'e-mail en tant qu'application Web.
44	**Proxy Web**	Cette catégorie couvre les sites Web qui fournissent des services proxy. Il s'agit d'un site Web de type « navigateur dans un navigateur », lorsqu'un utilisateur ouvre une page Web, saisit l'URL demandée dans un formulaire, puis clique sur « Envoyer ». Le site de proxy Web télécharge la vraie page et l'affiche dans le navigateur de l'utilisateur. Ce type est détecté (et peut nécessiter d'être bloqué) pour les raisons suivantes : • Pour la navigation anonyme. Étant donné que les demandes vers le serveur Web de destination se font depuis le serveur de proxy Web, seule son adresse IP est visible, et si les administrateurs du serveur identifient l'utilisateur, la trace s'arrêtera au niveau du proxy Web, ce qui peut ou non conserver les journaux nécessaires pour localiser l'utilisateur d'origine. • Pour l'usurpation de l'emplacement. Les adresses IP des utilisateurs sont souvent utilisées pour établir le profil du service par emplacement de la source (il se peut que certains sites Web gouvernementaux nationaux soient disponibles uniquement depuis des adresses IP locales), et il se peut que l'utilisation de ces services aide l'utilisateur à masquer son véritable emplacement. • Pour accéder à du contenu interdit. Si un simple filtre d'URL est utilisé, il ne verra que les URL de proxy Web, et pas les véritables serveurs sur lesquels l'utilisateur se rend.

		• Pour éviter d'être surveillé par l'entreprise. Il se peut qu'une règle d'entreprise implique de surveiller l'utilisation Internet des employés. En accédant à tout via un proxy Web, il se peut qu'un utilisateur échappe à la surveillance, ce qui fournira des informations incorrectes. Étant donné que le SDK analyse la page HTML (si elle est fournie), et pas uniquement les URL, le SDK pourratoujours détecter le contenu de certaines catégories. Il est toutefois impossible d'éviter d'autres motifs simplement en utilisant le SDK.

Exclusions d'URL

Les URL considérées comme fiables peuvent être ajoutées à la liste des domaines de confiance. Les URL considérées comme une menace peuvent être ajoutées à la liste des domaines bloqués.

Pour indiquer les URL toujours fiables ou bloquées

1. Dans le module de filtrage d'URL d'un plan de protection, cliquez sur **Exclusions d'URL**.
   La fenêtre **Exclusions d'URL** s'ouvre.
   Les options suivantes sont affichées :

Éléments fiables : cliquez sur **Ajouter** pour sélectionner l'une des options disponibles :

- **Domaine** : si vous sélectionnez cette option, la fenêtre **Ajouter un domaine** s'affiche.
  - Dans le champ **Domaine**, saisissez chaque domaine sur une nouvelle ligne. Dans le champ **Description**, saisissez une brève description qui vous permettra de reconnaître votre modification dans la liste des éléments fiables.
- **Processus** : si vous sélectionnez cette option, la fenêtre **Ajouter un processus** s'affiche.
  - Dans le champ **Processus**, saisissez le chemin d'accès de chaque processus sur une nouvelle ligne. Dans la section **Description**, saisissez une brève description qui vous permettra de reconnaître votre modification dans la liste des éléments fiables.

Éléments bloqués : cliquez sur **Ajouter**. La fenêtre **Ajouter un domaine** s'affiche.

Dans le champ **Domaine**, saisissez chaque domaine sur une nouvelle ligne. Dans le champ **Description**, saisissez une brève description qui vous permettra de reconnaître votre modification dans la liste des éléments bloqués.

Remarque
Les chemins d'accès du réseau local sont pris en charge. Exemple : \\localhost\folderpath\file.exe.

Description

Dans le champ **Description**, vous pouvez saisir des notes concernant les exclusions que vous avez ajoutées à la liste d'exclusions des URL. Voici quelques suggestions de notes que vous pouvez

ajouter :

- Motifs et objectifs de l'exclusion.
- Horodatage.

Si plusieurs éléments ont été ajoutés dans une seule entrée, il ne peut y avoir qu'un seul commentaire pour tous les éléments.

Antivirus Microsoft Defender et Microsoft Security Essentials

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Antivirus Microsoft Defender

L'antivirus Microsoft Defender est un composant anti-malware intégré à Microsoft Windows, qui est fourni à partir de Windows 8.

Le module Antivirus Microsoft Defender vous permet de configurer la stratégie de sécurité de l'antivirus Microsoft Defender et de suivre son état via la console Cyber Protect.

Ce module s'applique aux ressources sur lesquelles l'antivirus Microsoft Defender est installé.

Microsoft Security Essentials

Microsoft Security Essentials est un composant anti-malware intégré à Microsoft Windows, qui est fourni avec les versions antérieures à Windows 8.

Le module Microsoft Security Essentials vous permet de configurer la stratégie de sécurité de Microsoft Security Essentials et de suivre son état via la console Cyber Protect.

Ce module s'applique aux ressources sur lesquelles Microsoft Security Essentials est installé.

Les paramètres pour Microsoft Security Essentials sont similaires à ceux pour l'antivirus Microsoft Defender, mais vous ne pouvez pas configurer la protection en temps réel et ne pouvez pas définir d'exclusions via la console Cyber Protect.

Planifier l'analyse

Spécifiez la planification pour l'analyse planifiée.

Mode d'analyse :

- **Complète** : une vérification complète de tous les fichiers et dossiers en plus des éléments analysés lors de l'analyse rapide. Son exécution requiert plus de ressources machine comparativement à l'exécution de l'analyse rapide.

- **Rapide** : une vérification rapide des processus et dossiers en mémoire, dans lesquels se trouvent généralement les malwares. Son exécution requiert moins de ressources machine.

Définissez l'heure et le jour de la semaine pour l'exécution de l'analyse.

Analyse quotidienne rapide : définit l'heure de l'analyse quotidienne rapide.

En fonction de vos besoins, vous pouvez définir les options suivantes :

Démarrer l'analyse planifiée lorsque la machine est allumée, mais pas en cours d'utilisation

Examinez les dernières définitions de virus et de logiciel espion avant d'exécuter une analyse planifiée

Limiter l'utilisation du CPU lors de l'analyse à

Pour en savoir plus sur les paramètres de l'antivirus Microsoft Defender, reportez-vous à l'article https://docs.microsoft.com/fr-fr/sccm/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settings.

Actions par défaut

Définissez les actions par défaut à exécuter pour les menaces détectées selon leur niveau de gravité :

- **Nettoyer** : nettoyer le malware détecté sur une ressource.
- **Quarantaine** : placer le malware détecté en quarantaine, mais ne pas le supprimer.
- **Supprimer** : supprimer le malware détecté sur une ressource.
- **Autoriser** : ne pas supprimer le malware détecté, ni le mettre en quarantaine.
- **Défini par l'utilisateur** : un utilisateur sera invité à spécifier l'action à effectuer avec le malware détecté.
- **Aucune action** : aucune action ne sera effectuée.
- **Bloquer** : bloquer le malware détecté.

Pour en savoir plus sur les paramètres des actions par défaut pour l'antivirus Microsoft Defender, reportez-vous à l'article https://docs.microsoft.com/fr-fr/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-settings.

Protection en temps réel

Activez la **protection en temps réel** pour détecter les malwares et les empêcher de s'installer ou de s'exécuter sur des ressources.

Analyser tous les téléchargements : si cette option est sélectionnée, l'analyse est effectuée sur tous les fichiers téléchargés et sur toutes les pièces jointes.

Activer surveillance des comportements : si cette option est sélectionnée, la surveillance des comportements sera activée.

Analyser les fichiers réseau : si cette option est sélectionnée, les fichiers réseau seront analysés.

Autoriser une analyse complète sur des lecteurs réseau mappés : si cette option est sélectionnée, les lecteurs réseau mappés seront entièrement analysés.

Autoriser l'analyse des e-mails : si l'option est activée, le moteur procèdera à l'analyse syntaxique de la boîte aux lettres et des fichiers de messagerie, en fonction de leur format spécifique, afin d'analyser le corps des e-mails et les pièces jointes.

Pour en savoir plus sur les paramètres de protection en temps réel pour l'antivirus Microsoft Defender, reportez-vous à l'article https://docs.microsoft.com/fr-fr/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settings.

Advanced

Spécifiez les paramètres d'analyse avancée :

- **Analyser les fichiers d'archive** : inclure les fichiers archivés, comme les fichiers .zip ou .rar, à l'analyse.
- **Analyser les lecteurs amovibles** : analyser les lecteurs amovibles lors d'une analyse complète.
- **Créer un point de restauration système** : dans certains cas, un fichier ou une entrée de registre important peut être supprimé alors qu'il s'agit d'un « faux positif ». Vous pourrez alors le ou la récupérer à partir d'un point de restauration.
- **Supprimer les fichiers mis en quarantaine après** : définir la période après laquelle les fichiers en quarantaine seront supprimés.
- **Envoyer automatiquement les échantillons de fichiers lorsqu'une analyse plus profonde est requise :**
  - **Toujours demander** : vous serez invité à confirmer avant l'envoi du fichier.
  - **Envoyer automatiquement tous les échantillons sécurisés** : la plupart des échantillons seront envoyés automatiquement, sauf les fichiers qui contiennent des informations personnelles. Ces fichiers nécessiteront une confirmation supplémentaire.
  - **Envoyer automatiquement tous les échantillons** : tous les échantillons seront automatiquement envoyés.
- **Désactiver l'interface utilisateur graphique de l'antivirus Windows Defender :** si cette option est sélectionnée, l'utilisateur de l'antivirus Windows Defender ne sera pas accessible à l'utilisateur. Vous pouvez gérer les règles relatives à l'antivirus Windows Defender via la console Cyber Protect.
- **MAPS (Microsoft Active Protection Service)** : communauté en ligne qui vous aide à choisir comment réagir face aux menaces potentielles.
  - **Je ne souhaite pas rejoindre MAPS** : aucune information ne sera envoyée à Microsoft au sujet des logiciels qui ont été détectés.
  - **Adhésion de base** : des informations de base seront envoyées à Microsoft au sujet des logiciels qui ont été détectés.
  - **Adhésion avancée** : des informations plus détaillées seront envoyées à Microsoft au sujet des logiciels qui ont été détectés.

Pour en savoir plus, reportez-vous à l'article https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise/ (en anglais).

Pour en savoir plus sur les paramètres avancés pour l'antivirus Microsoft Defender, reportez-vous à l'article https://docs.microsoft.com/fr-fr/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings.

Exclusions

Vous pouvez définir les fichiers et dossiers suivants afin de les exclure de l'analyse :

- **Processus :** n'importe quel fichier que le processus défini lit ou sur lequel il écrit sera exclu de l'analyse. Vous devez définir un chemin d'accès complet au fichier exécutable du processus.
- **Fichiers et dossiers :** les fichiers et dossiers spécifiés seront exclus de l'analyse. Vous devez définir un chemin d'accès complet au dossier ou au fichier, ou définir l'extension du fichier.

Pour en savoir plus sur les paramètres d'exclusion pour l'antivirus Microsoft Defender, reportez-vous à l'article https://docs.microsoft.com/fr-fr/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings.

Gestion du pare-feu

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

La gestion du pare-feu vous permet de configurer facilement les paramètres de pare-feu sur les ressources protégées.

Dans Cyber Protect, cette fonctionnalité est fournie via un composant de pare-feu Microsoft Defender intégré de Microsoft Windows. Le pare-feu Microsoft Defender bloque le trafic réseau non autorisé entrant ou sortant de vos ressources.

La gestion du pare-feu s'applique à toutes les ressources sur lesquelles le pare-feu Microsoft Defender est installé.

Systèmes d'exploitation Windows compatibles

Les systèmes d'exploitation Windows suivants sont compatibles avec la gestion du pare-feu :

Windows

- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Windows Server n'est pas compatible.

Activation et désactivation de la gestion du pare-feu

Vous pouvez activer la gestion du pare-feu lors de la création d'un plan de protection. Vous pouvez modifier un plan de protection existant afin d'activer ou de désactiver la gestion du pare-feu.

Activer ou désactiver la gestion du pare-feu

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Effectuez l'une des actions suivantes pour ouvrir le panneau du plan de protection :
   - Si vous souhaitez créer un plan de protection, sélectionnez un ordinateur à protéger, cliquez sur **Protection**, puis sur **Création d'un plan**.
   - Si vous souhaitez modifier un plan de protection existant, sélectionnez une machine protégée, cliquez sur **Protection**, sur les points de suspension (...) à côté du nom du plan de protection, puis sur **Modifier**.
3. Dans le panneau du plan de protection, accédez à la zone **Gestion du pare-feu**, et activez ou désactivez **Gestion du pare-feu**.
4. Effectuez l'une des actions suivantes pour appliquer vos modifications :
   - Si vous créez un plan de protection, cliquez sur **Créer**.
   - Si vous modifiez un plan de protection, cliquez sur **Enregistrer**.

Le **Statut du pare-feu Microsoft Defender** dans la zone **Gestion du pare-feu** du panneau du plan de protection s'affiche comme **Activé** ou **Désactivé**, selon que vous avez activé ou désactivé la gestion du pare-feu.

Vous pouvez également accéder au panneau du plan de protection depuis l'onglet Gestion. Toutefois, cette fonctionnalité n'est pas disponible dans toutes les éditions du service Cyber Protection.

Quarantaine

La zone de **quarantaine** est un dossier isolé spécial, présent sur le disque dur d'une machine, dans lequel sont placés les fichiers suspects détectés par la protection contre les virus et les malwares afin d'éviter de propager davantage les menaces.

La zone de quarantaine vous permet de consulter les fichiers suspects et potentiellement dangereux présents sur toutes les machines, et de décider s'ils doivent être supprimés ou restaurés. Les fichiers en quarantaine sont automatiquement supprimés si la machine est supprimée du système.

Comment les fichiers arrivent-ils dans le dossier de quarantaine ?

1. Vous configurez le plan de protection et indiquez que par défaut, les fichiers infectés doivent être mis en quarantaine.

2. Lors d'une analyse lors de l'accès ou lors d'une analyse planifiée, le système détecte des fichiers malveillants et les place dans le dossier sécurisé Quarantaine.
3. Le système met à jour la liste de quarantaine sur les machines.
4. Les fichiers sont automatiquement nettoyés du dossier de quarantaine après la période définie pour le paramètre **Supprimer les fichiers mis en quarantaine après** dans le plan de protection.

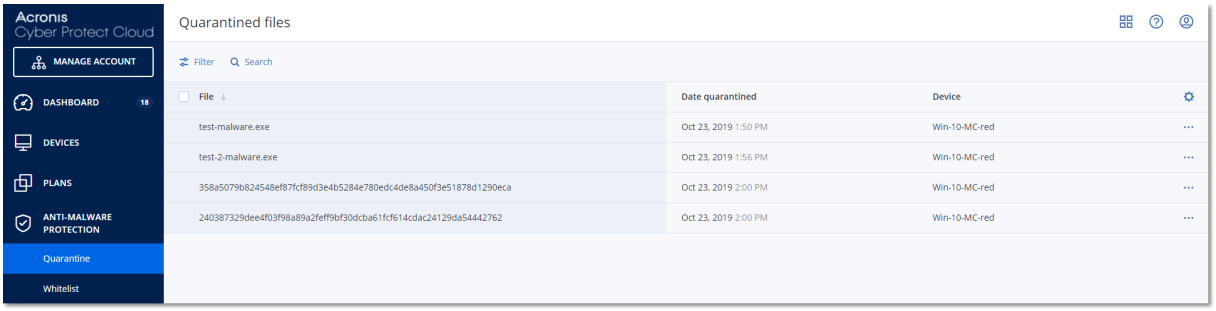
Gestion des fichiers mis en quarantaine

Pour gérer les fichiers mis en quarantaine, accédez à **Protection contre les malwares** > **Quarantaine**. Vous verrez la liste des fichiers mis en quarantaine sur toutes les machines.

Nom	Description
Fichier	Le nom du fichier.
Date de début de la mise en quarantaine	La date et l'heure auxquelles le fichier a été mis en quarantaine.
Terminal	Le terminal sur lequel le fichier infecté a été trouvé.
Nom de la menace	Le nom de la menace.
Plan de protection	Le plan de protection en vertu duquel le fichier suspect a été mis en quarantaine.

Pour les fichiers mis en quarantaine, deux actions sont possibles :

- **Supprimer :** supprimer définitivement un fichier mis en quarantaine de toutes les machines. Vous pouvez supprimer tous les fichiers avec le même hachage de fichier. Vous pouvez restaurer tous les fichiers avec le même hachage de fichier. Regroupez les fichiers par hachage, sélectionnez les fichiers nécessaires, puis supprimez-les.
- **Restaurer** : permet de restaurer un fichier mis en quarantaine à l'emplacement d'origine, sans aucune modification. Si un fichier de même nom se trouve à l'emplacement d'origine, il est remplacé par le fichier restauré. Notez que le fichier restauré est ajouté à la liste des autorisations et ignoré lors des analyses antimalware ultérieures.



Emplacement de quarantaine sur les machines

L'emplacement par défaut pour les fichiers mis en quarantaine est le suivant :

- Pour un ordinateur Windows : `%programdata%\Acronis\NGMP\quarantine`
- Pour un ordinateur Mac : `/Library/Application Support/Acronis/NGMP/quarantine`
- Pour un ordinateur Linux : `/var/lib/Acronis/NGMP/quarantine`

L'emplacement de quarantaine est sous l'autoprotection du fournisseur de services.

Dossier personnalisé en libre-service et à la demande

Vous pouvez sélectionner des dossiers personnalisés dans la ressource et les analyser directement depuis le menu contextuel.

Pour accéder à l'analyse avec l'option Cyber Protect dans le menu contextuel

Pour les ressources avec antivirus et antimalware activés dans le plan de protection, cliquez avec le bouton droit sur les fichiers/dossiers que vous voulez analyser.

Remarque
Cette option est disponible uniquement pour les administrateurs de la ressource.

Liste blanche d'entreprise

Une solution antivirus pourrait identifier des applications légitimes spécifiques à une entreprise comment étant suspectes. Afin d'éviter les faux positifs, les applications de confiance sont ajoutées manuellement à une liste blanche, ce qui est chronophage.

Remarque
La liste blanche d'entreprise n'affecte pas les analyses antimalware des sauvegardes.

Cyber Protection peut automatiser ce processus : les sauvegardes sont analysées par le module de protection Antivirus et Antimalware et les données examinées sont analysées, de sorte que ces applications sont déplacées vers la liste blanche et que les détections de faux positifs sont évitées. De plus, la liste blanche à l'échelle de l'entreprise améliore les performances de l'analyse antimalware.

La liste blanche est créée pour chaque client, et se base uniquement sur les données de ce client.

La liste blanche peut être activée et désactivée. Lorsqu'elle est désactivée, les fichiers qui y sont ajoutés sont temporairement masqués.

Remarque
Seuls les comptes ayant le rôle administrateur (par exemple, administrateur Cyber Protection ; administrateur de l'entreprise ; administrateur partenaire qui agit au nom d'un administrateur de l'entreprise ; administrateur de l'unité) peuvent configurer et gérer la liste blanche. Cette fonctionnalité n'est pas disponible pour un compte administrateur en lecture seule ou un compte utilisateur.

Ajout automatique à la liste blanche

1. Exécutez l'analyse Cloud des sauvegardes sur au moins deux ordinateurs. Pour cela, utilisez les plans d'analyse des sauvegardes.
2. Dans les paramètres de liste blanche, activez le commutateur **Génération automatique d'une liste blanche**.

Ajout manuel à la liste blanche

Même lorsque le commutateur **Génération automatique d'une liste blanche** est désactivé, vous pouvez ajouter des fichiers manuellement.

1. Dans la console Cyber Protect, accédez à **Protection Antimalware** > **Liste blanche**.
2. Cliquez sur **Ajouter un fichier**.
3. Indiquez le chemin d'accès au fichier, puis cliquez sur **Ajouter**.

Ajout de fichiers mis en quarantaine à la liste blanche

Vous pouvez ajouter des fichiers mis en quarantaine à la liste blanche.

1. Dans la console Cyber Protect, accédez à **Protection Antimalware** > **Quarantaine**.
2. Sélectionnez un fichier mis en quarantaine, puis cliquez sur **Ajouter à la liste blanche**.

Paramètres de liste blanche

Lorsque vous activez le commutateur **Génération automatique d'une liste blanche**, vous devez indiquer l'un des niveaux de protection heuristique suivants :

- **Basse** :
  les applications d'entreprise seront ajoutées à la liste blanche uniquement au terme d'un délai long et après un nombre important de vérifications. Ces applications sont plus fiables. Toutefois, cette approche augmente la possibilité de faux positifs. Les critères pour considérer qu'un fichier est propre et fiable sont stricts.
- **Défaut** :
  les applications d'entreprise seront ajoutées à la liste blanche en fonction du niveau de protection recommandé, afin de réduire la possibilité de faux positifs. Les critères pour considérer qu'un fichier est propre et fiable sont moyens.
- **Élevé** :
  les applications d'entreprise seront ajoutées à la liste blanche plus rapidement, afin de réduire la possibilité de faux positifs. Toutefois, cela ne garantit pas que le logiciel soit propre et il peut, par la suite, être identifié comme suspect ou malware. Les critères pour considérer qu'un fichier est propre et fiable sont faibles.

Afficher les détails à propos des éléments de la liste blanche

Vous pouvez cliquer sur un élément de la liste blanche pour afficher plus d'informations à son sujet et l'analyser en ligne.

Si vous avez des doutes concernant un élément que vous avez ajouté, vous pouvez le vérifier grâce à l'analyseur VirusTotal. Lorsque vous cliquez sur **Examiner sur VirusTotal**, le site analyse les URL et fichiers suspects, afin de détecter certains types de malwares en utilisant le hachage de fichier de l'élément que vous avez ajouté. Vous pouvez afficher le hachage dans la chaîne **Hachage du fichier (MD5)**.

Les valeurs **Machines** font référence au nombre de machines sur lesquelles ce hachage a été détecté lors de l'analyse de sauvegarde. Cette valeur n'est renseignée que si un élément a été retourné de l'analyse de sauvegarde ou de la quarantaine. Ce champ reste vide si le fichier est ajouté manuellement à la liste blanche.

Analyse anti-malware des sauvegardes

Grâce à l'analyse antimalware des sauvegardes, vous pouvez empêcher la reprise de fichiers infectés en vérifiant que vos sauvegardes ne comportent aucun malware. Les analyses antimalware sont effectuées par un agent Cloud qui réside dans le centre de données Cyber Protection et n'utilisent aucune ressource informatique.

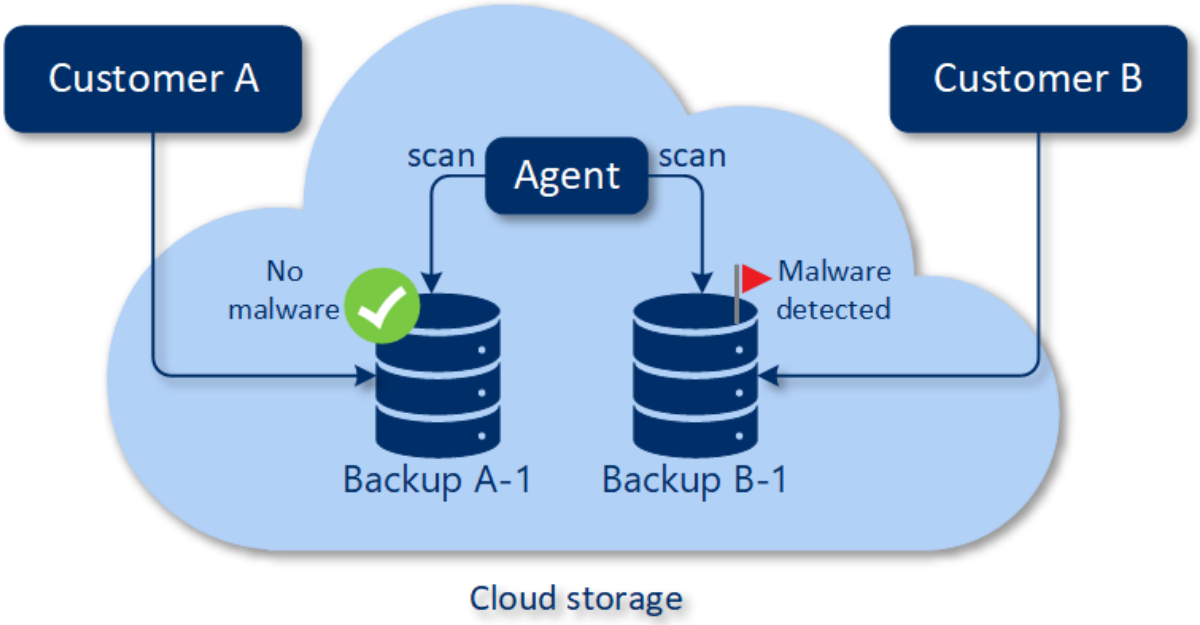
Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Pour exécuter une analyse antimalware, vous devez configurer un plan d'analyse de la sauvegarde. Pour en savoir plus sur la procédure à suivre, reportez-vous à "Plan d'analyse des sauvegardes" (p. 203).

Chaque plan d'analyse de la sauvegarde crée une tâche d'analyse pour l'agent Cloud et ajoute cette tâche à une file d'attente (une par centre de données). Les tâches d'analyse sont traitées en fonction de leur ordre dans la file d'attente. Par ailleurs, la durée de l'analyse dépend de la taille de la sauvegarde. C'est la raison pour laquelle il y a un décalage entre la création d'un plan d'analyse de la sauvegarde et l'exécution de l'analyse.

Les sauvegardes que vous avez sélectionnées pour l'analyse peuvent avoir l'un des états suivants :

- Non analysé
- Aucun malware
- Malware détecté



Vous pouvez consulter les résultats d'une analyse de la sauvegarde dans le widget **Détails de l'analyse de la sauvegarde (menaces)**. Vous les trouverez dans la console Cyber Protect > **Surveillance** > onglet **Vue d'ensemble**.

Limites

- L'analyse antimalware n'est prise en charge que pour les sauvegardes **Toute la machine** ou **Disques/volumes** des ressources suivantes :
  - Ordinateurs Windows sur lesquels un agent de protection est installé.
  - Machines virtuelles Windows sauvegardées au niveau de l'hyperviseur (sauvegarde sans agent) par l'agent pour Hyper-V et l'agent pour VMware (Windows).

  L'analyse antimalware n'est pas prise en charge pour les sauvegardes créées par des appliances virtuelles telles que l'agent pour VMware (appliance virtuelle), l'agent pour Virtuozzo et l'agent pour Scale Computing HC3.
- Seuls les volumes avec système de fichiers NTFS et partitionnement de table de partitions GUID et du secteur de démarrage principal sont analysés.
- Seul le stockage dans le Cloud par défaut est pris en charge comme emplacement de sauvegarde. Les stockages locaux et dans le cloud appartenant à un partenaire ne sont pas pris en charge.
- Lorsque vous sélectionnez des sauvegardes à analyser, vous pouvez sélectionner des ensembles de sauvegardes incluant une sauvegarde pour la protection continue des données. Toutefois, l'analyse ne concerne que les sauvegardes autres que les sauvegardes pour la protection continue des données figurant dans ces ensembles. Pour plus d'informations sur les sauvegardes pour la protection continue des données, consultez "Protection continue des données (CDP)" (p. 426).
- Lorsque vous exécutez la restauration sécurisée d'un ordinateur dans son intégralité, vous pouvez sélectionner un ensemble de sauvegardes qui comprend une sauvegarde pour la

protection continue des données. Toutefois, cette opération de récupération n'utilise pas les informations de la sauvegarde de protection continue des données. Pour restaurer les données de la protection continue des données, exécutez une autre opération de récupération de **Fichiers/dossiers**.

Utilisation des fonctionnalités de protection avancée

Par défaut, Cyber Protect inclut des fonctionnalités couvrant la plupart des menaces relatives à la cybersécurité. Vous pouvez utiliser ces fonctionnalités sans frais supplémentaires. Par ailleurs, vous pouvez activer des fonctionnalités avancées pour améliorer la protection de vos ressources.

- Si une fonctionnalité de protection avancée est disponible pour que vous puissiez l'utiliser, elle apparaît dans le plan de protection identifié par l'icône Fonctionnalité avancée  .
- Si une fonction de protection avancée n'est pas disponible pour vous, contactez l'administrateur pour activer le pack de protection avancée requis.
- Si l'administrateur vous a permis d'acheter d'autres packs de sécurité, vous pouvez choisir d'activer les fonctionnalités Advanced. Un message s'affiche pour vous informer que des frais supplémentaires s'appliquent.

Remarque
Si une fonctionnalité au moins est activée, vous devrez faire l'acquisition du pack de protection avancée correspondant.

Remarque
Si toutes les fonctionnalités avancées de votre plan de protection sont désactivées, le pack de protection avancée correspondant sera désactivé.

Pack de protection avancée	Fonctionnalités de protection avancée
Advanced Backup	Protège en permanence vos ressources et garantit que les modifications de dernière minute de votre travail ne seront pas perdues. Les fonctionnalités sont les suivantes : • Reprise en un seul clic • Protection continue des données • Prise en charge de la sauvegarde des clusters Microsoft SQL Server et Microsoft Exchange – Groupes de disponibilité AlwaysOn (AAG) et groupes de disponibilité de la base de données (DAG) • Prise en charge de la sauvegarde pour MariaDB, MySQL, Oracle DB et SAP HANA • Carte de protection des données et reporting de conformité • Traitement des données hors hôte • Fréquence de sauvegarde des ressources Microsoft 365 et Google Workspace • Opérations à distance avec un support de démarrage • Sauvegarde directe dans un stockage dans le cloud public Microsoft Azure

Advanced Security + EDR	Protège en permanence vos ressources contre toutes les menaces de logiciels malveillants. Les fonctionnalités sont les suivantes : • Gérer les incidents dans une page Incident centralisée • Visualiser la portée et l'impact des incidents • Recommandations et étapes de réparation • Consulter les attaques dévoilées publiquement sur vos ressources à l'aide de flux d'informations sur les menaces • Stocker les événements de sécurité pendant 180 jours • Protection en temps réel contre les virus et les malwares avec détection basée sur la signature locale (avec protection en temps réel) • Prévention des failles • Filtrage d'URL • Gestion du pare-feu des terminaux • Sauvegarde de données d'investigation, analyse des sauvegardes à la recherche de malwares, reprise sécurisée, liste d'autorisation de l'entreprise • Plans de protection intelligent (Intégration avec des alertes CPOC) • Analyse de sauvegarde centralisée à la recherche de malwares • Effacement à distance • Antivirus Microsoft Defender • Microsoft Security Essentials
Advanced Management	Permet de corriger les vulnérabilités des ressources protégées. Les fonctionnalités sont les suivantes : • Gestion des correctifs • État de santé du disque • Inventaire du logiciel • Application de correctifs sans échec • Création de cyber-scripts • Assistance à distance • Transfert et partage de fichiers • Sélection d'une session à laquelle se connecter • Observation de ressources en vue multiple • Modes de connexion : contrôle, affichage seul et rideau • Connexion via l'application Assistance rapide • Protocoles de connexion à distance : NEAR et Partage d'écran Apple • Enregistrement de session pour les connexions NEAR • Transmission de captures d'écran • Rapport d'historique des sessions • 24 moniteurs • Surveillance basée sur un seuil

	• Surveillance basée sur une anomalie
Advanced Data Loss Prevention	Empêche la fuite d'informations sensibles à partir des ressources protégées. Les fonctionnalités sont les suivantes : • Solution sensible au contenu pour la protection des ressources contre la perte de données via les périphériques et communications réseau • Détection automatique intégrée des informations personnelles identifiables (PII), des informations de santé protégées (PHI) et des données de l'industrie des cartes de paiement (PCI DSS), ainsi que des documents présents dans la catégorie « Marqué confidentiel » • Création automatique de règles de prévention de la perte de données avec assistance facultative pour l'utilisateur final • Application de la prévention de la perte de données avec ajustement des règles en fonction de l'apprentissage automatique • Centralisation des journaux d'audit, des alertes et des notifications à destination de l'utilisateur final dans le cloud

Advanced Data Loss Prevention

Le module Advanced Data Loss Prevention analyse le contenu et le contexte des transferts de données dans les ressources protégées, et empêche toute fuite de données sensibles par l'intermédiaire de périphériques ou de transferts réseau, à l'intérieur et à l'extérieur du réseau d'entreprise en fonction de la règle de flux de données.

Les fonctionnalités Advanced Data Loss Prevention peuvent être incluses dans n'importe quel plan de protection d'un tenant client si le service de protection et le pack Advanced Data Loss Prevention sont activés pour ce client.

Avant de commencer à utiliser le module Advanced Data Loss Prevention, veillez à lire et à comprendre les concepts de base et la logique de la gestion Advanced DLP qui sont décrits dans le guides des principes fondamentaux.

Vous souhaiterez peut-être consulter également le document Caractéristiques techniques.

Création des règles et des règles de flux de données

Le principe de prévention de la perte de données exige que les utilisateurs d'un système informatique d'entreprise soient autorisés à gérer les données sensibles uniquement dans la mesure nécessaire aux tâches qu'ils doivent effectuer. Tous les autres transferts de données sensibles qui ne sont pas pertinents pour les processus professionnels doivent être bloqués. Il est par conséquent essentiel de distinguer les transferts, ou flux de données professionnels et non autorisés.

La règle de flux de données contient des règles qui indiquent les flux de données autorisés et non autorisés, et par conséquent empêche les transferts non autorisés d'informations sensibles lorsque

le module de prévention de la perte de données est activé dans un plan de protection et s'exécute en mode Application.

Chaque catégorie de sensibilité de la règle contient une règle par défaut, marquée d'un astérisque (*), et une ou plusieurs règles explicites (autres que par défaut) qui définissent les flux de données d'utilisateurs ou de groupes spécifiques. Pour plus d'informations sur les types de règles, consultez le guides des principes fondamentaux.

La règle de flux de données est généralement créée automatiquement lorsque le module Advanced Data Loss Prevention s'exécute en mode d'observation. La durée nécessaire à la création d'une règle de flux de données représentative est d'environ un mois. Toutefois, elle peut différer en fonction des processus de votre organisation. La règle de flux de données peut également être créée, configurée ou modifiée manuellement par un administrateur d'entreprise ou d'unité.

Pour démarrer la création automatique de la règle de flux de données

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Gestion** > **Plans de protection**.
3. Cliquez sur **Création d'un plan**.
4. Développez la section **Prévention des pertes de données** et cliquez sur la ligne **Mode**.
5. Dans la boîte de dialogue Mode, Sélectionnez **Mode d'observation**, puis sélectionnez le mode de traitement des transferts de données :

Option	Description
Tout autoriser	Tous les transferts de données sensibles des ressources utilisateur sont traités comme étant nécessaires aux processus de l'entreprise et sécurisés. Une nouvelle règle est créée pour chaque flux de données détecté qui ne correspond pas à une règle déjà définie.
Justifier tout	Tous les transferts de données sensibles des ressources utilisateur sont traités comme étant nécessaires aux processus de l'entreprise, mais risqués. Par conséquent, pour chaque transfert intercepté de données sensibles vers une destination ou un destinataire à l'intérieur ou à l'extérieur de l'organisation qui ne correspond à aucune règle de flux de données créée, l'utilisateur doit saisir une justification commerciale unique. Lorsque la justification est soumise, une nouvelle règle de flux de données est créée dans la règle de flux de données.
Mixte	La logique Tout autoriser est appliquée à tous les flux de données sensibles internes et la logique Justifier tout est appliquée à tous les flux de données externes. **Remarque** Pour plus d'informations sur les données internes et externes, voir Détection automatique de la destination

6. Enregistrez le plan de protection et appliquez-le aux ressources à partir desquelles vous souhaitez collecter des données pour concevoir la règle.

Remarque
La fuite des données n'est pas évitée pendant le mode d'observation.

Pour configurer la règle de flux de données manuellement

1. Dans la console Cyber Protect, accédez à **Protection** > **Règle de flux de données**.
2. Cliquez sur **Nouvelle règle de flux de données**.
   Le panneau Nouvelle règle de flux de données se développe sur la droite.
3. Sélectionnez une catégorie de sensibilité, ajoutez un expéditeur et un destinataire, puis définissez l'autorisation de transferts de données pour la catégorie, l'expéditeur et le destinataires sélectionnés.

Option	Description
Autoriser	Autorise cet expéditeur à transférer des données de cette catégorie de sensibilité pour ce destinataire.
Exception	N'autorise pas cet expéditeur à transférer des données de cette catégorie de sensibilité pour ce destinataire, mais permet à l'expéditeur de soumettre une exception à la règle pour un transfert spécifique. Lorsque cet expéditeur essaie de transférer des données de cette catégorie de sensibilité à ce destinataire, bloque le transfert et demande à l'expéditeur de soumettre une exception pour autoriser le transfert. Lorsque l'exception est soumise, le transfert de données peut être effectué. **Important** Tous les autres transferts de données entre cet expéditeur et ce destinataire pour cette catégorie de sensibilité seront autorisés pendant cinq minutes après la soumission de l'exception.
Refuser	N'autorise pas cet expéditeur à transférer des données de cette catégorie de sensibilité pour ce destinataire et ne permet pas à l'expéditeur de demander une exception à la règle.

4. (Facultatif) Sélectionnez une action à exécuter lors du déclenchement de la règle.

Action	Description
Écrire dans un journal	Stocke un enregistrement d'événements dans le journal d'audit lors du déclenchement de la règle. Nous vous recommandons de sélectionner cette action pour les règles avec autorisation **Exception**.
Générer une alerte	Génère une alerte dans l'onglet **Alertes** Cyber Protect lors du déclenchement de la règle. Si les notifications sont activées pour l'administrateur, un e-mail de notification est également envoyé.
Notifier l'utilisateur final lorsqu'un transfert de données est refusé	Notifie l'utilisateur en temps réel par un avertissement à l'écran lors du déclenchement de la règle.

5. Cliquez sur **Enregistrer**.
6. Répétez les étapes 2 à 5 pour créer plusieurs règles de différentes catégories et options de sensibilité, puis vérifie que les règles qui en résultent correspondent aux options que vous avez sélectionnées.

Structure de la règle de flux de données

Dans la vue **Règle de flux de données**, les règles sont regroupées en fonction de la catégorie de données sensibles qu'elles contrôlent. L'identificateur de catégorie de sensibilité s'affiche immédiatement au-dessus du groupe de règles.

- Sensible
  - Informations de santé protégées (PHI)
  - Informations personnelles identifiables (PII)
  - Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS),
  - Marqué confidentiel
- Non sensible

Pour plus d'informations sur le concept et les fonctionnalités de règle de flux de données, voir le guides des principes fondamentaux.

Structure de règle

Chaque règle est constituée des éléments suivants.

- **Catégorie de sensibilité**
  - **Informations de santé protégées (PHI)**
  - **Informations personnelles identifiables (PII)**
  - **Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)**
  - **Marqué confidentiel**

    Voir "Définitions des données sensibles" (p. 929)
- **Expéditeur** - spécifie l'initiateur d'un transfert de données contrôlé par cette règle. Il peut s'agir d'un seul utilisateur, d'une liste d'utilisateurs ou d'un groupe d'utilisateurs.
  - **N'importe quel interne** - groupe d'utilisateurs qui comprend tous les utilisateurs internes de l'organisation.
  - **Contact/Organisation d'origine** – compte Windows dans l'organisation et reconnu par Advanced Data Loss Prevention, ainsi que tous les autres comptes (y compris ceux utilisés par des applications de communication tierces) qu'un compte Windows donné a utilisés précédemment.
  - **Contact/Identité personnalisée** - identificateur d'un utilisateur interne dans l'un des formats suivants : adresse e-mail, ID Skype, identificateur ICQ, identificateur IRC, adresse e-mail Jabber, adresse e-mail Mail.ru Agent, numéro de téléphone Viber, adresse e-mail Zoom.
    Les caractères génériques suivants peuvent être utilisés pour indiquer un groupe de contacts :

    - ***** - n'importe quel nombre de symboles
    - **?** - n'importe quel symbole unique
- **Destinataire** - spécifie la destination d'un transfert de données contrôlé par cette règle. Il peut s'agir d'un seul utilisateur, d'une liste d'utilisateurs ou d'un groupe d'utilisateurs, et également des autres types de destinations indiqués ci-dessous.
    - **Tout** - n'importe quel type de destinataire pris en charge par Advanced DLP.
    - **Contact/N'importe quel contact** - tout contact interne ou externe.
    - **Contact/N'importe quel contact interne** - tout contact d'un utilisateur interne (voir "Détection automatique de la destination" (p. 928)).
    - **Contact/N'importe quel contact externe** - tout contact d'une personne ou d'une entité externe.
    - **Contact/Organisation d'origine** - même principe que celui décrit dans le champ Expéditeur.
    - **Contact/Identité personnalisée** - même principe que celui décrit dans le champ Expéditeur.
    - **Services de partage de fichiers** - identificateur d'un service de partage de fichiers contrôlé.
    - **Réseau social** - identificateur d'un réseau social contrôlé.
    - **Hôte/N'importe quel hôte** - tout ordinateur reconnu par Advanced DLP comme interne ou externe.
    - **Hôte/N'importe quel hôte interne** - tout ordinateur reconnu par Advanced DLP comme interne.
    - **Hôte/N'importe quel hôte externe** - tout ordinateur reconnu par Advanced DLP comme externe.
    - **Hôte/Hôte spécifique** - identificateur d'ordinateur spécifié comme nom d'hôte (exemple : FQDN) ou adresse IP (IPv4 ou IPv6).
    - **Terminal/N'importe quel terminal** - tout périphérique connecté à la ressource.
    - **Terminal/Stockage externe** - stockage amovible ou lecteur mappé redirigé et connecté à la ressource.
    - **Terminal/Amovible chiffré** : un périphérique de stockage amovible chiffré avec BitLocker To Go.
    - **Terminal/Presse-papiers redirigé** - Presse-papiers redirigé et connecté à la ressource.
    - **Imprimantes** - imprimante locale ou réseau connectée à la ressource.
- **Autorisation** - contrôle préventif appliqué à un transfert de données contrôlé par cette règle. Décrite en détail dans la rubrique Autorisations dans les règles de flux de données.
- **Action** - action non préventive exécutée au déclenchement de cette règle. Par défaut, ce champ est défini sur Aucune action. Les options sont les suivantes :
    - **Écrire dans un journal** - stocke un enregistrement d'événements dans le journal d'audit lors du déclenchement de la règle.
    - **Notifier l'utilisateur final lorsqu'un transfert de données est refusé** - notifie l'utilisateur à l'aide d'un avertissement à l'écran en temps réel lors du déclenchement de la règle.
    - **Générer une alerte** - alerte l'administrateur lors du déclenchement de la règle.

Avertissement !
Lorsque l'option **Aucune action** est sélectionnée et que la règle est déclenchée :

- aucun enregistrement d'événement n'est ajouté au journal d'audit ;
- aucune alerte n'est envoyée à l'administrateur ;
- aucune notification n'est affichée sur l'écran de l'utilisateur final.

Qu'est-ce qui déclenche une règle ?

Un transfert de données correspond à une règle de flux de données si toutes les conditions suivantes sont vraies :

- Tous les expéditeurs de ce transfert de données sont répertoriés ou appartiennent à un groupe d'utilisateurs spécifié dans le champ **Expéditeur** de la règle.
- Tous les destinataires de ce transfert de données sont répertoriés ou appartiennent à un groupe d'utilisateurs spécifié dans le champ **Destinataire** de la règle.
- Les données transférées correspondent à la **catégorie de sensibilité** de la règle.

Ajustement des autorisations dans les règles de flux de données

Le module Advanced Data Loss Prevention prend en charge trois types d'autorisations dans les règles de flux de données. Les autorisations sont configurées individuellement dans chaque règle.

Autoriser (autorisation)	Les transferts de données autorisés sont ceux qui correspondent à la combinaison catégorie de sensibilité, expéditeur et destinataire définie dans la règle.
Exception (interdiction)	Les transferts de données non autorisés sont ceux qui correspondent à la combinaison catégorie de sensibilité, expéditeur et destinataire définie dans la règle. Toutefois, l'expéditeur peut soumettre une exception à la règle pour autoriser un transfert spécifique. **Important** Tous les autres transferts de données entre cet expéditeur et ce destinataire pour cette catégorie de sensibilité seront autorisés pendant cinq minutes après la soumission de l'exception.
Refuser (interdiction)	Les transferts de données non autorisés sont ceux qui correspondent à la combinaison catégorie de sensibilité, expéditeur et destinataire définie dans la règle. L'expéditeur n'a pas la possibilité de soumettre une exception.

Par ailleurs, un indicateur de priorité peut être affecté aux autorisations **Autoriser** et **Exception** afin d'améliorer la flexibilité de la gestion des règles. Grâce à ce paramètre, vous pouvez ignorer les autorisations définies pour des groupes spécifiques dans d'autres règles de flux de données. Vous pouvez l'utiliser pour n'appliquer une règle de flux de données de groupes qu'à certains de ses membres. Pour ce faire, vous devez créer une règle de flux de données pour des utilisateurs

spécifiques que vous souhaitez exclure des règles de groupe, puis donner la priorité à leurs autorisations par rapport aux restrictions de flux de données configurées dans les règles du groupe auquel ces utilisateurs appartiennent. Pour plus d'informations sur les priorités d'autorisation lors de la combinaison de règles, voir "Combinaison de règles de flux de données" (p. 920).

Important
Avant de faire passer une règle d'entreprise ou d'unité du mode d'observation au mode d'application, il est essentiel d'ajuster les règles par défaut de chaque catégorie de données sensibles en les faisant passer de l'état d'autorisation à l'état d'interdiction. Les règles par défaut sont marquées d'un (*) dans la vue **Règle de flux de données**. Pour plus d'informations sur les types de règles, consultez le guides des principes fondamentaux.

Pour modifier les autorisations dans les règles

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Protection** > **Règle de flux de données**.
3. Sélectionnez la règle à modifier, puis cliquez sur **Modifier** au-dessus de la liste de règles.
   La fenêtre **Modifier la règle de flux de données** s'ouvre.
4. Dans la section **Autorisation**, sélectionnez **Autoriser**, **Exception** ou **Refuser**.
5. (Facultatif) Pour donner la priorité à l'autorisation **Autoriser** ou **Exception** sur les autorisations des autres règles, cochez la case **Prioriser**.
   Vous n'avez pas besoin d'utiliser cette case à cocher pour donner la priorité à une règle de flux de données sur la règle par défaut Tout > Autre, car ce flux a par défaut la priorité la plus faible dans une règle.
   Pour plus d'informations sur les priorités d'autorisation lors de la combinaison de règles, voir "Combinaison de règles de flux de données" (p. 920).
6. (Facultatif) Sélectionnez une action à exécuter lors du déclenchement de la règle.
7. Enregistrez les modifications apportées à la règle.

Combinaison de règles de flux de données

Lorsqu'un transfert de données correspond à plusieurs règles, les autorisations et les actions configurées pour toutes les règles sont combinées et appliquées comme suit.

Autorisations

Si un transfert de données correspond à plusieurs règles dont les autorisations pour la même catégorie de données sont différentes, la règle prioritaire est celle dont l'autorisation a la priorité la plus élevée dans la liste des priorités des autorisations suivantes (dans l'ordre décroissant) :

1. Exception avec drapeau **Prioritaire**
2. Autoriser avec le drapeau **Prioritaire**
3. Refuser

4. Exception
5. Autoriser

Si un transfert de données correspond à plusieurs règles dont les autorisations pour différentes catégories de données sont différentes, la logique de remplacement suivante est appliquée :

1. L'autorisation de règle la plus restrictive est définie pour chacune des catégories de sensibilité correspondant au transfert de données.
2. Les autorisations de règles les plus restrictives et définies au point 1 sont appliquées.

Exemple

Un transfert de fichiers correspond à trois règles dans différentes catégories de sensibilité comme suit :

Catégorie de sensibilité	Autorisation
IPI	Autoriser - Prioritaire
IMP	Exception - Prioritaire
PCI	Refuser

L'autorisation qui sera appliquée est Refuser.

Actions

Si un transfert de données correspond à plusieurs règles dont les options configurées dans le champ **Action** sont différentes, toutes les actions configurées dans toutes les règles déclenchées sont effectuées.

Examen et gestion des règles

Avant d'être appliquée, la règle de flux de données de base créée automatiquement doit être examinée, validée et approuvée par le client, car c'est lui qui connaît toutes les spécificités de son activité et peut évaluer si elles sont interprétées de manière cohérente dans la règle de base. De la même manière, le client peut identifier les incohérences que peut alors résoudre l'administrateur partenaire.

Pendant l'examen de la règle, l'administrateur partenaire présente la règle de flux de données de base au client qui examine chaque flux et valide sa cohérence avec les processus professionnels. La validation n'exige aucune compétence technique, car la représentation des règles de la console Cyber Protect est très intuitive : chaque règle décrit qui est l'expéditeur et qui est le destinataire d'un flux de données sensibles.

En fonction des instructions du client, l'administrateur partenaire ajuste la règle de base manuellement en modifiant, en supprimant et en créant les règles de flux de données. Après l'approbation du client, la règle examinée est appliquée aux ressources protégées par le passage en mode Application du plan de protection appliqué à ces ressources.

Avant l'application d'une règle examinée, il est important de modifier l'autorisation **Autoriser** dans toutes les règles par défaut créées automatiquement pour les catégories de données sensibles sur l'état **Refuser** ou **Exception**. L'autorisation **Refuser** ne peut pas être remplacée par les utilisateurs tandis que l'autorisation **Exception** bloque un transfert correspondant à la règle, mais permet aux utilisateurs d'ignorer une situation d'urgence en soumettant une exception de nature commerciale.

Renouvellement de la règle de flux de données

Lorsque le processus professionnel de l'entreprise ou son unité est considérablement modifié, les règles DLP correspondantes doivent être renouvelées pour qu'elles soient cohérentes avec les modifications apportées aux flux de données sensibles du processus professionnel mis à jour. Un renouvellement de règle est également nécessaire si le rôle d'un employé est modifié. Dans ce cas, la partie de la règle d'unité utilisée pour protéger la ressource de l'employé doit également être renouvelée.

Le workflow de gestion des règles Advanced DLP permet aux administrateurs d'automatiser les renouvellements de règle pour l'intégralité de l'entreprise, une unité, un utilisateur ou une partie des utilisateurs d'une unité.

Renouvellement de la règle d'une société ou d'une unité

Toutes les options du mode d'observation peuvent être utilisées pour renouveler la règle de l'entreprise ou de l'unité, et également une règle d'unité pour un ou plusieurs utilisateurs de l'unité.

Pour renouveler la règle d'une société ou d'une unité

Le processus de renouvellement se compose des étapes suivantes qui doivent être effectuées par un administrateur de l'entreprise ou un partenaire qui gère les ressources de l'entreprise.

1. Supprimez toutes les règles qui ne sont pas par défaut dans la règle appliquée.
2. Pour démarrer le renouvellement, faites passer le plan de protection avec Advanced DLP appliqué à l'entreprise ou à l'unité à l'une des options de mode d'observation en utilisant l'option optimale pour cette entreprise ou cette unité, puis appliquez le plan à toutes les ressources de l'entreprise ou de l'unité.
3. À la fin de la période de renouvellement, examinez la nouvelle règle d'entreprise ou d'unité avec le client, effectuez les modifications nécessaires, puis obtenez l'approbation du client.
4. Faites passer le plan de protection appliqué aux ressources de l'entreprise ou de l'unité à une option de mode d'application approprié que le client considère comme étant optimale pour empêcher les fuites de données à partir des ressources de l'unité.

Renouvellement de la règle d'un ou plusieurs utilisateurs de la société ou de l'unité

Les règles de niveau utilisateur peuvent être renouvelées à l'aide de n'importe quelle option du mode d'observation et également du mode d'application adaptative.

Utilisation du mode d'observation pour le renouvellement d'une règle utilisateur

L'utilisation du mode d'observation pour le renouvellement de la règle d'un ou de plusieurs utilisateurs de l'entreprise (ou de l'unité) a les particularités suivantes : la règle de flux de données appliquée à l'intégralité de l'entreprise (ou de l'unité) n'est pas appliquée aux transferts de données des utilisateurs pendant la période de renouvellement. Par conséquent, les nouvelles règles de l'utilisateur créées pendant le renouvellement pourraient contredire les règles de groupe existantes (ou y correspondre) dans la règle appliquée pour l'entreprise (unité). Une fois le renouvellement terminé et la règle réappliquée aux transferts de données de l'utilisateur, ces nouvelles règles créées pour l'utilisateur sont appliquées ou non aux transferts de données de l'utilisateur selon les priorités sur d'autres règles auxquelles ces transferts de données doivent correspondre.

Pour renouveler la règle d'un utilisateur en mode d'observation

Le processus de renouvellement se compose des étapes suivantes qui doivent être effectuées par un administrateur de l'entreprise ou un partenaire qui gère les ressources de l'entreprise.

1. Supprimez toutes les règles qui ne sont pas par défaut et sont appliquées pour l'entreprise (ou l'unité) dont l'utilisateur est le seul expéditeur.
2. Supprimez l'utilisateur des listes d'expéditeurs de toutes les règles de flux de données qui ne sont pas par défaut dans la règle appliquée.
3. Créez un nouveau plan de protection avec Advanced DLP en mode d'observation et appliquez-le à la ressource de l'utilisateur pour démarrer la période de renouvellement (observation).
   La durée de la période de renouvellement dépend de la durée nécessaire à l'utilisateur pour effectuer toutes (ou 90 à 95 %) les activités régulières qui impliquent le transfert de données sensibles à partir de ses ressources.
4. À la fin de la période de renouvellement, examinez les nouvelles règles associées à cet utilisateur et qui ont été ajoutées à la règle appliquée, effectuez les modifications nécessaires, puis obtenez l'approbation du client.
5. Faites passer le plan de protection appliqué à la ressource de l'utilisateur au mode **Application stricte** ou **Application adaptative** selon l'option que le client considère comme étant optimale pour empêcher les fuites de données à partir de la ressource de l'utilisateur.
   Vous pouvez également réappliquer à la ressource de l'utilisateur le plan de protection appliqué à l'entreprise (ou à l'unité).

Utilisation du mode d'application adaptative pour le renouvellement d'une règle utilisateur

Le renouvellement de règle d'un ou de plusieurs utilisateurs de l'entreprise (ou de l'unité) peut être effectué à l'aide du mode d'application adaptative d'un plan de protection avec le module Advanced DLP appliqué à la ressource de l'utilisateur.

Remarque
Cette méthode de renouvellement de règle a les particularités suivantes : les règles d'entreprise (d'unité) appliquée aux groupes d'expéditeurs avec adhésion de l'utilisateur (par exemple, N'importe quel interne) sont également appliquées aux transferts de données de cet utilisateur pendant le renouvellement. Par conséquent, le renouvellement ne crée pas pour l'utilisateur de nouvelles règles qui contrediraient les règles existantes des groupes d'expéditeurs (ou y correspondraient). La méthode la plus efficace pour les renouvellements de règles utilisateur d'un client dépend des exigences spécifiques en matière de sécurité informatique.

Pour renouveler la règle d'un utilisateur en mode d'application adaptative

Le processus de renouvellement se compose des étapes suivantes qui doivent être effectuées par un administrateur de l'entreprise ou un partenaire qui gère les ressources de l'entreprise.

1. Supprimez toutes les règles qui ne sont pas par défaut et sont appliquées pour l'entreprise (ou l'unité) et dont l'utilisateur est le seul expéditeur.
2. Supprimez l'utilisateur des listes d'expéditeurs de toutes les règles de flux de données qui ne sont pas par défaut dans la règle appliquée.
3. Pour toutes les règles par défaut appliquées pour l'entreprise (ou l'unité), définissez leur autorisation sur **Exception**, puis sélectionnez l'action **Écrire dans un journal** dans le champ **Action**.
4. Si le plan de protection appliqué à la ressource de l'utilisateur est défini sur le mode **Application stricte**, créez un plan de protection avec Advanced DLP et appliquez-le à la ressource de l'utilisateur en mode **Application adaptative** pour démarrer la période de renouvellement.
   La durée de la période de renouvellement dépend de la durée nécessaire à l'utilisateur pour effectuer toutes (ou 90 à 95 %) les activités régulières qui impliquent le transfert de données sensibles à partir de ses ressources.
5. À la fin de la période de renouvellement, examinez les nouvelles règles associées à cet utilisateur et qui ont été ajoutées à la règle appliquée, effectuez les modifications nécessaires, puis obtenez l'approbation du client.
6. Faites passer le plan de protection appliqué à la ressource de l'utilisateur au mode **Application stricte** ou conservez le mode **Application adaptative** selon l'option que le client considère comme étant optimale pour empêcher les fuites de données à partir de la ressource de l'utilisateur.
   Vous pouvez également réappliquer à la ressource de l'utilisateur le plan de protection appliqué à l'entreprise (ou à l'unité).

Activation d'Advanced Data Loss Prevention dans les plans de protection

Les fonctionnalités Advanced Data Loss Prevention peuvent être incluses dans n'importe quel plan de protection d'un tenant client si le service de protection et le pack Advanced Data Loss Prevention sont activés pour ce client.

Advanced DLP est le module avancé regroupant les fonctionnalités de prévention des pertes de données. Les fonctionnalités Advanced DLP et le contrôle de terminal peuvent être utilisés ensemble ou indépendamment (dans un seul plan de protection ou dans deux plans protégeant la même ressource). Si elles sont utilisées ensemble, leurs capacités fonctionnelles sont coordonnées comme suit.

- Le contrôle de terminal cesse de contrôler l'accès de l'utilisateur à ces canaux locaux dans lesquels Advanced DLP inspecte le contenu des données transférées. En revanche, il conserve le contrôle sur les types de terminaux suivants s'ils sont configurés en accès en lecture seule ou si leur accès est refusé :
  - Amovible
  - Amovible chiffré
  - Lecteur mappé

  Par exemple, si le contrôle de terminal et Advanced DLP sont activés dans un seul plan de protection ou dans deux plans protégeant la même ressource, et que l'accès en lecture seule est configuré pour les périphériques USB dans le contrôle de terminal, l'accès en lecture seule est appliqué à tous les périphériques USB, à l'exception de ceux figurant dans la liste d'autorisation, indépendamment des paramètres d'accès du module Advanced DLP. Si l'accès est activé par défaut et configuré dans le contrôle de terminal, le paramètre d'accès d'Advanced DLP est appliqué.
- L'accès des utilisateurs aux canaux locaux et terminaux suivants de la liste d'autorisation est appliqué par le contrôle des terminaux :
  - Lecteurs optiques
  - Disquettes
  - Terminaux mobiles connectés par MTP
  - Adaptateurs Bluetooth
  - Presse-papiers Windows
  - Captures d'écran
  - Périphériques USB et types de périphériques (à l'exception du stockage amovible et des périphériques chiffrés)

Pour créer un plan de protection avec Advanced DLP

1. Accédez à **Gestion** > **Plans de protection**.
2. Cliquez sur **Création d'un plan**.
3. Développez la section **Prévention des pertes de données** et cliquez sur la ligne **Mode**.
   La boîte de dialogue **Mode** s'ouvre.
   - Pour démarrer la création ou le renouvellement de la règle de flux de données, sélectionnez **Mode d'observation**, puis le mode de traitement des transferts de données :

Option	Description
Tout autoriser	Tous les transferts de données sensibles des ressources utilisateur sont traités comme étant nécessaires aux processus de l'entreprise et sécurisés. Une nouvelle règle est créée pour chaque flux de données détecté qui ne correspond pas à une règle déjà définie.
Justifier tout	Tous les transferts de données sensibles des ressources utilisateur sont traités comme étant nécessaires aux processus de l'entreprise, mais risqués. Par conséquent, pour chaque transfert intercepté de données sensibles vers une destination ou un destinataire à l'intérieur ou à l'extérieur de l'organisation qui ne correspond à aucune règle de flux de données créée, l'utilisateur doit saisir une justification commerciale unique. Lorsque la justification est soumise, une nouvelle règle de flux de données est créée dans la règle de flux de données.
Mixte	La logique Tout autoriser est appliquée à tous les transferts internes de flux de données sensibles et la logique Justifier tout est appliquée à tous les transferts externes de flux de données sensibles. Pour la définition des destinations internes, voir "Détection automatique de la destination" (p. 928)

Avertissement !

- Sélectionnez **Mode d'observation** uniquement si vous n'avez aucune règle de flux de données créée ou si vous renouvelez la règle. Avant de commencer le renouvellement de règle, voir "Renouvellement de la règle de flux de données" (p. 922).
- La fuite des données n'est pas évitée en mode d'observation. Reportez-vous à Mode d'observation dans le guides des principes fondamentaux.

- Pour appliquer la règle de flux de données existante, sélectionnez **Mode d'application**, puis choisissez le mode d'application des règles de flux de données :

Option	Description
Application stricte	La règle de flux de données est appliquée en l'état et n'est pas étendue avec les nouvelles règles d'autorisation en cas de détection de flux de données sensibles non observés précédemment. Reportez-vous à Application stricte dans le guides des principes fondamentaux.
Application adaptative (application avec apprentissage)	La règle appliquée continue à s'adapter automatiquement aux opérations qui n'ont pas été effectuées pendant la période d'observation ou aux modifications apportées aux processus professionnels. Ce mode permet d'étendre la règle de flux de données appliquée en fonction des nouveaux flux de données appris et détectés dans les ressources. Reportez-vous à Application adaptative dans le guides des principes fondamentaux.

Important
Avant de faire passer une règle d'entreprise ou d'unité du mode d'observation au mode d'application, il est essentiel d'ajuster les règles par défaut de chaque catégorie de données sensibles en les faisant passer de l'état d'autorisation à l'état d'interdiction. Les règles par défaut sont marquées d'un (*) dans la vue **Règle de flux de données**. Pour plus d'informations sur les types de règles, consultez le guides des principes fondamentaux.

4. Cliquez sur **Terminé** pour fermer la boîte de dialogue Mode.
5. (Facultatif) Pour configurer la reconnaissance optique des caractères, les listes d'autorisation et d'autres options de protection, cliquez sur **Paramètres Avancés**.
   Pour plus d'informations sur les options disponibles, voir "Paramètres avancés" (p. 927).
6. Enregistrez le plan de protection et appliquez-le aux ressources que vous souhaitez protéger.

Paramètres avancés

Vous pouvez utiliser les paramètres avancés des plans de protection avec Advanced Data Loss Prevention afin d'augmenter la qualité de l'inspection du contenu de données dans les canaux contrôlés par Advanced Data Loss Prevention, et également pour exclure des contrôles préventifs les transferts de données vers les types de périphériques figurant dans la liste d'autorisation, les catégories de communications réseau, les hôtes de destination et les transferts de données initiés par les applications de la liste d'autorisation. Vous pouvez configurer les paramètres avancés suivants :

- **Reconnaissance optique des caractères**
  Ce paramètre active ou désactive la reconnaissance optique des caractères afin d'extraire des sections de texte dans 31 langues pour une inspection de contenu plus poussée à partir de fichiers graphiques et d'images qui se trouvent dans les documents, les messages, les analyses, les captures d'écran et d'autres objets.
- **Transfert des données protégées par mot de passe**
  Le contenu des archives et documents protégés par mot de passe ne peut pas être inspecté. Grâce à ce paramètre, Advanced DLP permet à l'administrateur de choisir si les transferts sortants de données protégées par mot de passe doivent être autorisés ou bloqués.
- **Empêcher le transfert de données en cas d'erreur**
  L'analyse de contenu envoyée peut parfois échouer ou une autre erreur de contrôle peut se produire dans les opérations de l'agent DLP. Si cette option est activée, le transfert est bloqué. Si l'option est désactivée, le transfert est autorisé malgré l'erreur.
- **Liste d'autorisation des types de terminal et des communications réseau**
  Les transferts de données vers des types de périphériques et dans les communications réseau sélectionnés dans cette liste sont autorisés, quelles que soient la sensibilité des données et la règle de flux des données appliquée.

Avertissement !
Cette option est utilisée si des problèmes liés à un type de terminal ou à un protocole spécifique se produisent. N'activez pas cette option, sauf si un représentant du support vous le conseille.

- **Liste d'autorisation des hôtes distants**
  Les transferts de données vers des hôtes de destination spécifiés dans cette liste sont autorisés, quelles que soient la sensibilité des données et la règle de flux des données appliquée.
- **Liste d'autorisation des applications**
  Les transferts de données réalisés par des applications spécifiées dans cette liste sont autorisés, quelles que soient la sensibilité des données et la règle de flux des données appliquée.

L'indicateur **Niveau de sécurité** des Paramètres avancés affichés dans les vues **Créer un plan de protection** et Détails d'un plan de protection comprend la logique suivante d'indication de niveau :

- **Basique** indique qu'aucun paramètre avancé n'est activé.
- **Modéré** indique qu'un ou que plusieurs paramètres sont activés, mais que la combinaison **Reconnaissance optique des caractères**, **Transfert des données protégées par mot de passe** et **Empêcher le transfert de données en cas d'erreur** n'est pas activée.
- **Strict** indique qu'au moins la combinaison **Reconnaissance optique des caractères**, **Transfert des données protégées par mot de passe** et **Empêcher le transfert de données en cas d'erreur** est activée.

Détection automatique de la destination

En mode d'observation mixte, le module Advanced Data Loss Prevention applique des règles différentes en fonction de la destination du transfert de données (interne ou externe) détecté. La logique de détermination d'une destination comme étant interne est décrite ci-dessous. Toutes les autres destinations sont considérées comme externes.

Pour chaque transfert de données intercepté, le module Advanced Data Loss Prevention détecte automatiquement si le serveur HTTP, FTP ou SMB destination est interne en effectuant une demande DNS et en comparant les noms FQDN du serveur distant et de l'ordinateur sur lequel s'exécute l'agent de prévention de la perte de données. Si la demande DNS échoue, le modèle vérifie également si la ressource protégée et le serveur distant se trouvent dans le même réseau. Les serveurs disposant du même nom de domaine (ou qui se trouvent dans le même sous-réseau) que l'ordinateur sur lequel s'exécute l'agent de prévention de la perte de données sont considérés comme étant internes.

Pour la communication par e-mail, le module Advanced Data Loss Prevention traite comme étant des transferts internes tous les e-mails envoyés à partir d'une adresse e-mail d'entreprise à l'aide du serveur de messagerie d'entreprise si l'adresse e-mail du destinataire se trouve sur le même domaine que l'adresse e-mail de l'expéditeur, et que le nom du serveur de messagerie du destinataire est le même.

Les e-mails autres que ceux de l'entreprise sont traités comme étant des communications externes, sauf si le compte du destinataire est connu. Les adresses e-mail connues sont mises à jour, car la prévention des pertes de données surveille l'activité des utilisateurs sur le réseau et met à jour la base de données du backend à l'aide des données des adresses associées à l'utilisateur.

Les communications par Messenger sont traitées comme étant des communications externes, sauf si le compte du destinataire est connu. Les comptes connus sont mis à jour, car la prévention de la perte de données surveille l'activité des utilisateurs sur le réseau et met à jour la base de données du backend à l'aide des données des comptes associés à l'utilisateur.

Définitions des données sensibles

Cette rubrique décrit la logique d'identification des données sensibles lors de l'analyse de contenu.

Pour réduire le nombre de faux positifs, les correspondances identiques sont comptabilisées comme une seule correspondance pour tous les groupes des expressions logiques décrites.

Important
Les expressions logiques utilisées pour l'identification de contenu sont fournies à titre d'information uniquement et ne décrivent pas la solution en détail.

Informations de santé protégées (PHI)

Langues prises en charge

- Anglais américain, anglais britannique, anglais international
- Finlandais
- Italien
- Français
- Polonais
- Russe
- Hongrois
- Norvégien
- Espagnol

Données considérées comme des informations de santé protégées

Les données suivantes sont considérées comme des informations de santé protégées.

- Prénoms et noms
- Adresse (rue, ville, comté, circonscription, code postal et leurs codes géographiques équivalents)
- Numéros de téléphone
- Adresses e-mail

- Numéros de sécurité sociale
- Numéros de bénéficiaires de la couverture santé
- Numéros de compte bancaire
- URL
- Numéros d'adresse IP
- Codes ICD-10-CM
- ICD-10-PCS-and-GEMs
- HIPAA
- Autre élément relatif aux soins de santé
- Numéros de carte de crédit

Expression logique utilisée pour la détection de contenu

L'expression logique se compose des chaînes suivantes rejointes par l'opérateur logique OR. L'opérateur OR est utilisé pour rejoindre différents groupes de données dans la liste ci-dessus si l'opérateur logique AND n'est pas spécifié explicitement. Les numéros entre parenthèses représentent le nombre d'instances détectées qui renverraient un résultat de détection positif.

- **Numéros de sécurité sociale** (5)
- (Prénoms et noms (3) OR Adresse (3) OR Numéros de téléphone (3) OR Adresse e-mail (3) OR Numéros de compte bancaire (3) OR Numéros de carte de crédit (3)) AND (Numéros de sécurité sociale (3) OR Numéros de bénéficiaires de la couverture santé (3) * OR Codes ICD-10-CM (3) OR ICD-10-PCS-and-GEMs (3) OR HIPAA (3) OR * Autre élément relatif aux soins de santé (3))

Informations personnelles identifiables (PII)

Langues prises en charge

- Anglais américain, anglais britannique, anglais international
- Bulgare
- Chinois
- Tchèque
- Danois
- Néerlandais
- Finlandais
- Français
- Allemand
- Hongrois
- Indonésien

- Italien
- Coréen
- Malais
- Norvégien
- Polonais
- Portugais (Brésil)
- Portugais (Portugal)
- Roumain
- Russe
- Serbe
- Singapour
- Espagnol
- Suédois
- Taïwan
- Turc
- Thaï
- Japonais

Données considérées comme informations personnelles identifiables (PII)

- Prénoms et noms
- Adresse (rue, ville, comté, code postal)
- Numéros de compte bancaire
- Numéros personnels et identifiants fiscaux
- Numéros de passeport
- Numéros de sécurité sociale
- Numéros de téléphone
- Numéros de plaque d'immatriculation
- Numéros de permis de conduire
- Identifiants et numéros de série
- Adresses IP
- Adresses e-mail
- Numéros de carte de crédit

Expression logique utilisée pour la détection de contenu

Expression logique pour toutes les langues prises en charge, à l'exception du japonais

L'expression logique se compose des chaînes suivantes rejointes par l'opérateur logique OR ou AND. Les numéros entre parenthèses représentent le nombre d'instances détectées qui renverraient un résultat de détection positif.

- Numéros personnels et identifiants fiscaux (5)
- Prénoms et noms (3) AND **(**Numéro de carte de crédit (3) OR Numéro de sécurité sociale (3) OR Numéro de compte bancaire (3) OR Numéros personnels et identifiants fiscaux (3) OR Numéros de permis de conduire (3) OR Numéros de passeport (3) OR Numéros de sécurité sociale (3) OR Adresses IP (3) OR Numéros de plaque d'immatriculation (3) OR Identifiants et numéros de série**)**
- Numéros de téléphone (3) AND **(**Numéro de carte de crédit (3) OR Numéro de sécurité sociale (3) OR Numéro de compte bancaire (3) OR Adresse (3) OR Numéros personnels et identifiants fiscaux (3) OR Numéros de permis de conduire (3) OR Numéros de passeport (3) OR Numéros de sécurité sociale (3) OR Numéros de plaque d'immatriculation (3) OR Identifiants et numéros de série (3)**)**
- **(**Prénoms et noms (30) OR Adresse (30)**)** AND **(**Adresses e-mail (30) OR Numéros de téléphone (30) OR Adresses IP (30)**)**
- Adresses e-mail (3) AND **(**Numéro de carte de crédit (3) OR Numéro de sécurité sociale (3) OR Numéro de compte bancaire (3) OR Numéros personnels et identifiants fiscaux (3) OR Numéros de permis de conduire (3) OR Numéros de passeport (3) OR Numéros de sécurité sociale (3) OR Numéros de plaque d'immatriculation (3) OR Identifiants et numéros de série (3)**)**
- Adresse e-mail (30) AND **(**Adresse (30) OR Numéros de téléphone (30)**)**
- Prénoms et noms (30) AND adresse (30)
- Numéros de téléphone (30) AND adresse (30)
- Prénoms et noms (3) AND Numéros de compte bancaire (3)
- Numéros de téléphone (3) AND **(**Numéro de carte de crédit (3) OR Numéro de compte bancaire (3) OR Numéros de sécurité sociale (3) OR Numéros personnels et identifiants fiscaux (3) OR Numéros de permis de conduire (3) OR Numéros de passeport (3)**)**

Expression logique pour le japonais

Remarque
La détection de contenu ne comptabilise que les correspondances uniques.

L'expression logique se compose des chaînes suivantes rejointes par l'opérateur logique OR. L'opérateur OR est utilisé pour rejoindre différents groupes si l'opérateur logique AND n'est pas spécifié explicitement.

- Numéros de sécurité sociale (5)
- Prénoms et noms (3) AND **(**Numéro de carte de crédit (3) OR Numéro de compte bancaire (3) OR Numéros de permis de conduire (3) OR Numéros de passeport (3) OR Numéros de sécurité sociale (3)**)**
- Prénoms et noms (30) AND **(**Adresses e-mail (30) OR Numéros de téléphone (30) OR Adresses IP (30) OR Adresse (30)**)**
- Adresse (3) AND **(**Numéro de carte de crédit (3) OR Numéro de compte bancaire (3) OR Numéros de permis de conduire (3) OR Numéros de passeport (3) OR Numéros de sécurité sociale (3)**)**
- Adresse e-mail (3) AND **(**Numéro de carte de crédit (3) OR Numéro de compte bancaire (3) OR Numéros de sécurité sociale (3) OR Numéros de permis de conduire (3)**)**
- Adresse (5) AND **(**Adresse e-mail (5) OR Prénoms et noms (5) OR Numéros de téléphone (5) OR Adresses e-mail (5)**)**
- Prénoms et noms (3) AND Numéros de compte bancaire (3)
- Numéros de téléphone (3) AND **(**Numéro de carte de crédit (3) OR Numéro de compte bancaire (3) OR Adresse (3) OR Numéros de sécurité sociale (3) OR Numéros de permis de conduire (3)**)**

Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)

Langues prises en charge

Ce groupe de sensibilité ne dépend pas de la langue. Les données PCI DSS sont en anglais dans tous les pays.

Données considérées comme données PCI DSS

- Données du détenteur de la carte
  - Numéro de compte principal (PAN)
  - Nom du détenteur de la carte
  - Date d'expiration
  - Code du service
- Données d'authentification sensibles
  - Données de piste complète (données d'une bande magnétique ou équivalent sur une puce)
  - CAV2/CVC2/CVV2/CID
  - Codes PIN/Blocs PIN

Expression logique utilisée pour la détection de contenu

L'expression logique se compose des chaînes suivantes rejointes par l'opérateur logique OR. Les numéros entre parenthèses représentent le nombre d'instances détectées qui renverraient un résultat de détection positif.

- Numéro de carte de crédit (5)
- Numéro de carte de crédit (3) AND (Nom américain (Ex) (3) OR Nom américain (3) OR Mots-clés DSS PCI (3) OR Date (mois/an) (3))
- Vidage de carte de crédit (5)

Marqué confidentiel

Des données marquées comme confidentielles sont détectées dans le groupe de mots-clés.

La condition de correspondance est pondérée et chaque mot a une pondération égale à 1. La détection de contenu est considérée comme positive lorsque la condition de correspondance est remplie si la pondération est supérieure à 3.

Langues prises en charge

- Anglais
- Bulgare
- Chinois simplifié
- Chinois traditionnel
- Tchèque
- Danois
- Néerlandais
- Finlandais
- Français
- Allemand
- Hongrois
- Indonésien
- Italien
- Japonais
- Coréen
- Malais
- Norvégien
- Polonais
- Portugais - Brésil
- Portugais - Portugal
- Russe
- Serbe
- Espagnol

- Suédois
- Turc

Groupes de mots-clés

Le groupe de mots-clés de chaque langue contient les équivalents propres au pays des mots-clés suivants qui sont utilisés pour la langue anglaise (non sensible à la casse).

- confidentiel
- distribution interne
- non destiné à la distribution
- ne pas distribuer
- non adapté au public
- non destiné à la distribution externe
- à usage interne uniquement
- documentation hautement qualifiée
- privé
- informations privilégiées
- à usage interne uniquement
- à usage officiel uniquement

Événements de prévention des pertes de données

La prévention des pertes de données génère des événements dans la vue des événements DLP comme suit.

- En mode d'observation, les événements sont générés pour tous les transferts de données justifiés.
- En mode d'application, les événements sont générés en fonction de l'action **Écrire dans un journal** configurée pour chaque règle déclenchée.

Pour afficher les événements d'une règle dans la règle de flux de données

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Protection** > **Règle de flux de données**.
3. Localisez la règle pour laquelle vous souhaitez visualiser les événements, puis cliquez sur le bouton représentant des points de suspension à la fin de la ligne de la règle.
4. Sélectionnez **Afficher les événements**.

Pour afficher les détails concernant un événement dans la vue des événements DLP

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Protection** > **Événements DLP**.
3. Cliquez dans la liste sur un événement pour en voir les détails.
   Le panneau détails de l'événement se développe vers la droite.
4. Faites défiler l'affichage du panneau détails de l'événement vers le haut ou vers le bas pour afficher les informations disponibles.
   Les détails affichés dépendent du type de règle et des paramètres de règle qui ont déclenché l'événement.

Pour filtrer les événements de la liste des événements DLP

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Protection** > **Événements DLP**.
3. En haut à gauche, cliquez sur **Filtrer**.
4. Sélectionnez dans les menus déroulants la catégorie de sensibilité, la ressource, le type d'action, l'utilisateur et le canal.
   Vous pouvez sélectionner plusieurs éléments dans les menus déroulants. Le filtrage applique l'opérateur logique OR entre les éléments du même menu. Quant à l'opérateur logique AND, il est utilisé entre des éléments de menus différents.
   Par exemple, si vous sélectionnez la catégorie de sensibilité **PHI** et **PII**, le résultat renvoie tous les événements contenant PHI ou PII, ou les deux. Si vous sélectionnez la catégorie de sensibilité **PHI** et l'action **Accès en écriture**, seuls les événements correspondant aux deux catégories apparaissent dans le résultat filtré.
5. Cliquez sur **Appliquer**.
6. Pour afficher de nouveau tous les événements, cliquez sur **Filtre**, **Réinitialiser au défaut** et **Appliquer**.

Pour rechercher des événements dans la liste des événements DLP

1. Répétez les étapes 1-2 de la procédure ci-dessus.
2. Dans la liste déroulante située à droite de Filtre, sélectionnez une catégorie dans laquelle vous souhaitez effectuer une recherche : **Expéditeur**, **Destination**, **Processus**, **Objet du message** ou **Motif**.
3. Dans la zone de texte, saisissez l'expression qui vous intéresse et confirmez en appuyant sur la touche Entrée du clavier.
   Seuls les événements correspondant à l'expression que vous avez saisie apparaît dans la liste.
4. Pour réinitialiser la liste des événements, cliquez sur le **X**, connectez-vous à la zone de texte de recherche, puis appuyez sur Entrée.

Pour afficher la liste des événements liés à des règles spécifiques de flux de données

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Protection** > **Règle de flux de données**.

3. Cochez la case figurant devant le nom de la règle qui vous intéresse.
   Vous pouvez sélectionner plusieurs règles si nécessaire.
4. Cliquez sur **Afficher les événements**.
   L'affichage passe à **Protection** > **Événements DLP** et la liste affiche les événements liés aux règles que vous avez sélectionnées.

Widgets Advanced Data Loss Prevention dans le tableau de bord Vue d'ensemble

Le tableau de bord **Vue d'ensemble** fournit un certain nombre de widgets personnalisables qui apporteront une vue d'ensemble des opérations liées au service Cyber Protection, y compris le module Advanced Data Loss Prevention. Vous trouverez les widgets Advanced Data Loss Prevention suivants dans le tableau de bord **Vue d'ensemble** dans **Surveillance**.

- **Transferts de données sensibles** - affiche le nombre total d'opérations de transfert de données sensibles aux destinataires internes et externes. Le graphique est divisé par le type d'autorisation : autorisées, justifiées ou bloquées. Vous pouvez personnaliser ce widget en sélectionnant la plage souhaitée (1 jour, 7 jours, 30 jours ou ce mois).
- **Catégories de données sensibles sortantes** - affiche le nombre total de transferts de données sensibles aux destinataires externes. Le graphique est divisé par les catégories sensibles : Informations de santé protégées (PHI), Informations personnelles identifiables (PII), PCI DSS et Marqué confidentiel (Confidentiel).
- **Principaux émetteurs de données sensibles sortantes** - affiche le nombre total de transferts de données sensibles depuis l'organisation vers des destinataires externes, ainsi que la liste des 5 utilisateurs ayant le plus de transferts (avec ces nombres). Cette statistique inclut les transferts autorisés et justifiés. Vous pouvez personnaliser ce widget en sélectionnant la plage souhaitée (1 jour, 7 jours, 30 jours ou ce mois).
- **Principaux émetteurs de transferts de données sensibles bloqués** - affiche le nombre total de transferts de données sensibles bloqués et la liste des 5 utilisateurs ayant le plus de tentatives de transferts (avec ces nombres). Vous pouvez personnaliser ce widget en sélectionnant la plage souhaitée (1 jour, 7 jours, 30 jours ou ce mois).
- **Événements DLP récents** - affiche les détails des événements récents de prévention de la perte de données sur la période donnée. Vous pouvez personnaliser ce widget à l'aide des options suivantes :
  - **Plage (date de publication)** (1 jour, 7 jours, 30 jours ou ce mois).
  - Nom de la **ressource**
  - **État de l'opération** (autorisée, justifiée ou bloquée)
  - **Sensibilité** (PHI, PII, Confidentiel, DSS PCI)
  - **Type de destination** (externe, interne)
  - **Regroupement** (ressource, utilisateur, canal, type de destination)

Les widgets sont mis à jour toutes les cinq minutes. Les widgets disposent d'éléments sur lesquels cliquer qui permettent de faire des recherches sur les problèmes et de les résoudre. Vous pouvez télécharger l'état actuel du tableau de bord ou bien l'envoyer par courrier électronique au format .pdf et/ou .xlsx.

Catégories personnalisées de sensibilité

Les catégories personnalisées de données sensibles peuvent aider une organisation à protéger sa propriété intellectuelle et ses données confidentielles en développant le catalogue intégré Advanced DLP des définitions de contenu relatif à la conformité réglementaire.

Pour créer une catégories personnalisée de sensibilité

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Protection** > **Prévention des pertes de données** > **Classifieurs de données**.
3. Sélectionnez **Catégorie de sensibilité**.
4. La liste qui s'affiche répertorie les sensibilités intégrées (Informations d'intégrité intégrées ou Informations personnelles identifiables) et personnalisées.
5. Cliquez sur **Créer une sensibilité** en haut à droite de la fenêtre.
6. Saisissez son nom dans la fenêtre suivante.
7. Les nouvelles sensibilités personnalisées sont toujours désactivées par défaut. Vous pouvez les activer après avoir configuré tous les paramètres.
8. Après avoir créé une nouvelle sensibilité, vous devez configurer ses détecteurs de contenu. Cliquez sur la flèche pour développer le contenu de votre nouvelle sensibilité, puis sélectionnez **Ajouter un détecteur de contenu**.
9. Dans la fenêtre suivante, vous pouvez utiliser l'un des détecteurs de contenu existants (en cochant la case située à côté de son nom, puis en cliquant sur **Ajouter** en bas à droite) ou en définir un nouveau.
10. Au lieu de créer une nouvelle sensibilité de toutes pièces, vous pouvez également réutiliser une sensibilité existante (intégrée ou personnalisée) en la clonant et en ajustant ses paramètres.
    - Pour cloner une sensibilité existante, cochez la case située à côté de son nom, puis sélectionnez **Cloner** dans le menu déroulant Action (indiqué par des points de suspension), en haut à gauche. Pour cloner plusieurs sensibilités, vous pouvez sélectionner plusieurs éléments simultanément.
    - Dans la fenêtre suivante, vous pouvez sélectionner les paramètres de la sensibilité existante que vous souhaitez conserver en cochant les cases situées à côté des différents paramètres.

    Remarque
    La copie d'une sensibilité intégrée dans un tenant crée une nouvelle sensibilité personnalisée composée des mêmes détecteurs

Pour créer un nouveau détecteur de contenu

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Protection** > **Prévention des pertes de données** > **Classifieurs de données**.
3. Sélectionnez **Détecteurs de contenu**.
4. La liste qui s'affiche répertorie les détecteurs de contenu intégrés et personnalisés.
5. Cliquez sur **Créer un détecteur de contenu** en haut à droite de la fenêtre.
6. Un menu déroulant s'affiche, dans lequel vous pouvez sélectionner le type de détecteur que vous souhaitez créer. Actuellement, seul le détecteur de contenu **Type de fichier** est disponible ; d'autres seront disponibles dans les prochaines mises à jour.
7. Vous pouvez configurer le détecteur de contenu dans la fenêtre suivante.

Type de détecteur de contenu	Description
Détecteur de contenu de type de fichier	a. Il existe deux listes : **Types de fichiers pris en charge** et **Types de fichiers sélectionnés**. En cliquant sur l'icône « plus » située à droite du type de fichier pris en charge, vous déplacez ce type vers la liste Types de fichiers sélectionnés. Vous pouvez également sélectionner plusieurs types de fichiers pris en charge en cochant les cases situées à côté de leur nom, puis en cliquant sur le bouton **Ajouter la sélection** en haut à droite. b. Pour supprimer un type de fichier de la liste Types de fichiers sélectionnés, cliquez sur l'icône de la corbeille à droite de son nom. Vous pouvez également supprimer plusieurs types de fichiers simultanément en cochant les cases correspondantes et en cliquant sur le bouton **Retirer la sélection**.
Détecteur de contenu de mots-clés	a. Lors de la création d'un nouveau détecteur de contenu de mots-clés, vous devez importer des mots-clés d'un fichier. Une fois l'importation effectuée, vous pouvez fusionner les nouveaux mots-clés et la liste des mots-clés existants, ou remplacer les mots-clés existants par les mots-clés importés. b. Vous devez également déterminer si vous souhaitez que le détecteur de contenu trouve une correspondance pour tous les mots-clés de la liste, pour n'importe quel mot-clé de cette liste ou pour un nombre de mots-clés personnalisé.

8. Au lieu de créer un nouveau détecteur de contenu de toutes pièces, vous pouvez également réutiliser un détecteur existant (intégré ou personnalisé) en le clonant et en ajustant ses paramètres.
   - Pour cloner un détecteur de contenu existant, cochez la case située à côté de son nom, puis sélectionnez **Cloner** dans le menu déroulant Action (indiqué par des points de suspension), en haut à gauche. Pour cloner plusieurs détecteurs de contenu, vous pouvez sélectionner plusieurs éléments simultanément.

Remarque
La copie d'un détecteur de contenu intégré crée un détecteur personnalisé.

Carte de l'organisation

Remarque
Cette fonctionnalité n'est accessible qu'aux administrateurs de l'entreprise.

La carte de l'organisation est une base de données qui contient les données des utilisateurs et de tous leurs comptes servant à transférer, via la messagerie instantanée, la messagerie électronique ou tout autre moyen, des données interceptées par Advanced DLP.

La carte de l'organisation permet de créer et de gérer des groupes d'utilisateurs dans Advanced DLP, ainsi que de gérer les utilisateurs et les comptes associés aux utilisateurs dans Advanced DLP. Les groupes d'utilisateurs peuvent ensuite être utilisés pour la gestion des règles DLP basées sur les groupes.

Pour localiser la carte de l'organisation

- Dans la console Cyber Protect Cloud, accédez à **Protection** > **Prévention des pertes de données** > **Carte de l'organisation**.

Comment cela fonctionne-t-il ?

Remarque
La carte de l'organisation est remplie lorsque le module Advanced DLP fonctionne en mode Observation.

Pour chaque transfert de données intercepté par l'agent DLP, les attributs suivants sont collectés en amont.

Attribut	Description	Étiquette dans l'interface utilisateur
Unité d'organisation	Groupe créé manuellement. L'unité d'organisation peut avoir une ou plusieurs unités d'organisation imbriquées.	Nom du groupe, tel que défini
ID de sécurité	Identificateur de sécurité unique.	Sur la page des détails de l'utilisateur > **SID**
	Nom affiché convivial dérivé des noms de comptes utilisateur. Ce nom n'est pas toujours disponible dans la carte de l'organisation.	**Nom**
PC\Nom de l'utilisateur	Nom de l'utilisateur du terminal (ressource). Un nom d'utilisateur ne peut être attribué qu'à une seule unité	**Nom de l'utilisateur**

Attribut	Description	Étiquette dans l'interface utilisateur
	d'organisation.	
Terminal (ressource)	Nom du terminal (ressource).	**Ressource**
Compte	Comptes utilisés par un utilisateur pour communiquer via la messagerie électronique et la messagerie instantanée, et qui ont été interceptés par l'agent DLP. Par exemple, si l'agent détecte que le nom d'utilisateur « PC\Jean » utilise jean@gmail.com pour envoyer un e-mail, ce compte est lié au nom d'utilisateur PC\Jean.	**Comptes**

Dans la carte de l'organisation, vous pouvez afficher et rechercher des comptes, des utilisateurs et des groupes, et créer, modifier et supprimer des groupes.

Pour rechercher des comptes spécifiques

Dans le cadre d'une enquête sur un incident, les administrateurs peuvent avoir besoin de trouver le propriétaire d'un compte spécifique impliqué dans une violation potentielle de données.

1. Dans la console Cyber Protect Cloud, accédez à **Protection** > **Prévention des pertes de données** > **Carte de l'organisation**.
2. Dans la zone de texte **Recherche** située au-dessus de la liste des utilisateurs, commencez à taper le nom du compte ou collez-le.
   La liste est filtrée au fur et à mesure de la saisie.

Pour rechercher un nom d'utilisateur spécifique

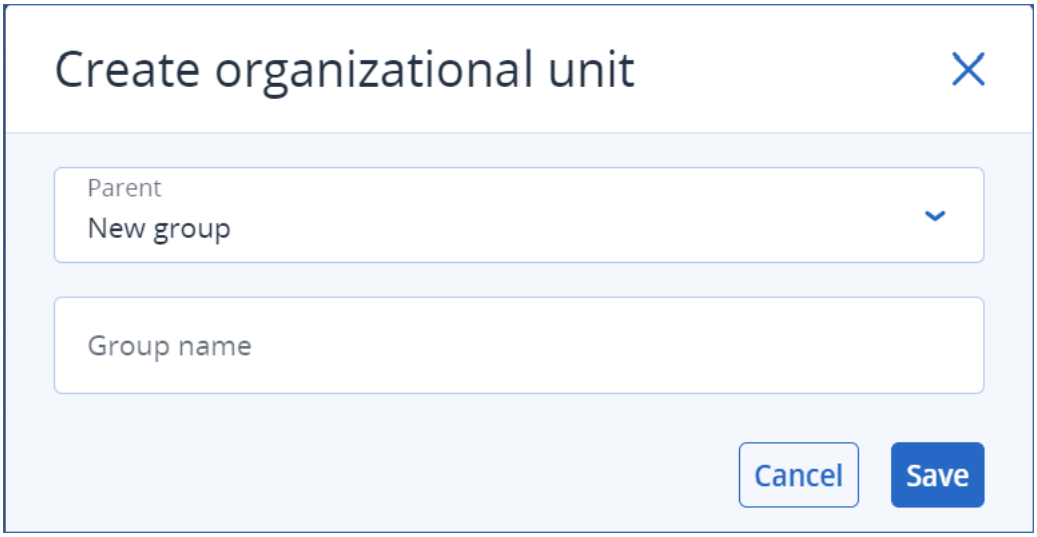
1. Dans la console Cyber Protect Cloud, accédez à **Protection** > **Prévention des pertes de données** > **Carte de l'organisation**.
2. Pour effectuer une recherche dans un groupe spécifique, cliquez sur le nom du groupe dans la liste.
3. Dans la zone de texte **Recherche** située au-dessus de la liste des utilisateurs, commencez à taper le nom du compte ou collez-le.
   La liste est filtrée au fur et à mesure de la saisie.

Pour afficher les comptes utilisés par un nom d'utilisateur particulier

1. Localisez l'utilisateur souhaité dans la liste.
2. Cliquez sur les trois points situés à l'extrémité de la ligne de l'utilisateur et sélectionnez **Afficher**.
3. Dans la boîte de dialogue des détails de l'utilisateur, localisez la section **Comptes associés**.
4. Vous pouvez ajouter des commentaires dans la zone de texte Description.

Pour créer un groupe d'utilisateurs

1. Dans la console Cyber Protect Cloud, accédez à **Protection** > **Prévention des pertes de données** > **Carte de l'organisation**.
2. Dans la partie inférieure gauche de la liste des groupes, cliquez sur **Créer un groupe**.
   La boîte de dialogue Créer une entité d'organisation s'ouvre.



3. Dans le menu déroulant Parent, sélectionnez le contexte du nouveau groupe.

   Remarque
   Vous ne pourrez pas modifier le parent ultérieurement. Le groupe restera imbriqué dans ce contexte.

4. Saisissez un nom de groupe et cliquez sur **Enregistrer**.

Pour ajouter un utilisateur à un groupe

1. Dans la console Cyber Protect Cloud, accédez à **Protection** > **Prévention des pertes de données** > **Carte de l'organisation**.
2. Dans la liste des utilisateurs, localisez l'utilisateur que vous souhaitez ajouter et cochez la case au début de sa ligne.
   Les boutons **Déplacer la sélection** et **Supprimer la sélection** apparaissent au-dessus de la liste des utilisateurs.

3. Cliquez sur **Déplacer la sélection**.
   La boîte de dialogue Déplacer l'utilisateur s'ouvre.
4. Sélectionnez un nouveau parent pour l'utilisateur sélectionné et cliquez sur **Enregistrer**.

Remarque
Un utilisateur ne peut appartenir qu'à un seul groupe.

Pour supprimer un compte associé à un utilisateur

1. Localisez l'utilisateur souhaité dans la liste.
2. Cliquez sur les trois points situés à l'extrémité de la ligne de l'utilisateur et sélectionnez **Afficher**.
3. Dans la boîte de dialogue des détails de l'utilisateur, localisez la section **Comptes associés**.
4. Localisez le compte que vous souhaitez supprimer et cliquez sur les trois points situés à côté.
5. Dans la liste déroulante, sélectionnez **Supprimer**.

Pour renommer un groupe d'utilisateurs

1. Dans la console Cyber Protect Cloud, accédez à **Protection** > **Prévention des pertes de données** > **Carte de l'organisation**.
2. Cliquez sur les trois points situés à côté du nom du groupe et cliquez sur **Renommer**.

Pour supprimer un groupe d'utilisateurs

1. Dans la console Cyber Protect Cloud, accédez à **Protection** > **Prévention des pertes de données** > **Carte de l'organisation**.
2. Cliquez sur les trois points situés à côté du nom du groupe et cliquez sur **Supprimer**.
   Tous les utilisateurs du groupe sont déplacés vers l'entité parent.

Problèmes connus et limites

- [DEVLOCK-4028] Aucun contrôle des chats de groupe dans l'agent Zoom pour ordinateur.
- [DEVLOCK-4016] Le nom convivial et l'identifiant d'expéditeur ne sont pas capturés pour GMX Web Mail et Web.de Mail en cas de création de brouillon.
- [DEVLOCK-4447] Aucune boîte de dialogue de justification pour WebMail naver.com en cas de création de brouillon.
- [DEVLOCK-1033] DeviceLockDriver : risque de bugcheck DRIVER_POWER_STATE_FAILURE provoqué par un blocage pendant le traitement IRP_MN_QUERY_DEVICE_RELATIONS.

Protection évolutive des points de terminaison (EDR)

Remarque
Cette fonctionnalité fait partie du pack Advanced Security + EDR, qui fait à son tour partie du service de cyberprotection. Notez que, lorsque vous ajoutez la fonctionnalité EDR à un plan de protection, vous êtes susceptible de devoir vous acquitter de frais supplémentaires.

La fonctionnalité EDR détecte toute activité suspecte sur une ressource, y compris les attaques qui n'ont pas été identifiées. Elle génère des incidents qui présentent en détail chaque attaque, ce qui vous permet de comprendre comment l'attaque s'est produite et comment éviter qu'elle se reproduise. Grâce aux interprétations faciles à comprendre de chaque phase de l'attaque, le temps consacré aux enquêtes sur les attaques peut être réduit à quelques minutes.

Utilité de la fonctionnalité EDR (Endpoint Detection and Response)

Aujourd'hui, les cybermenaces et les attaques malveillantes ne cessent de se développer, et la prévention n'est plus synonyme de protection complète. Malgré les différentes couches de prévention, certaines attaques parviennent toujours à se frayer un chemin et à pénétrer dans les réseaux. Les solutions classiques ne voient pas à quel moment l'intrusion se produit, ce qui laisse aux entités malveillantes la liberté de résider dans votre environnement pendant des jours, des semaines, voire des mois.

Les solutions EDR existantes, quant à elles, permettent d'empêcher ces « défaillances silencieuses », car elles recherchent les entités malveillantes et les suppriment dans les meilleurs délais. Toutefois, elles exigent généralement un niveau élevé d'expertise en matière de sécurité ou l'intervention coûteuse d'analystes du centre des opérations de sécurité. Par ailleurs, les analyses d'incident peuvent être extrêmement longues.

La fonctionnalité Acronis Advanced Security + EDR dépasse ces limites en détectant les attaques qui n'ont pas été identifiées. Vous pouvez ainsi comprendre comment une attaque s'est produite et comment éviter qu'elle se reproduise. Les enquêtes menées sur les attaques sont également plus rapides.

Voici en quoi la fonctionnalité EDR peut vous être utile :

- **Visibilité complète** : Vous comprenez l'événement qui s'est produit et comment il s'est produit, même pour les attaques qui n'ont pas été identifiées. L'évolution de chaque attaque est également représentée de manière visuelle, étape par étape (depuis le point d'entrée initial jusqu'à l'affichage des données ciblées et/ou exfiltrées), ce qui vous permet de mesurer rapidement la portée et l'impact d'un incident. Pour plus d'informations, voir "Comment enquêter sur des incidents dans la cyber kill chain" (p. 958).
- **Réduction de la durée de l'enquête** : La durée de l'enquête concernant les incidents passe de quelques heures à quelques minutes. L'option EDR détaille chaque étape de l'attaque de manière claire, dans une langue facile à comprendre, ce qui évite d'avoir à faire appel à des spécialistes coûteux ou à des effectifs supplémentaires. Pour plus d'informations, voir "Enquête sur les incidents" (p. 957).
- **Recherche de menaces connues dans les ressources** : Vous pouvez rechercher automatiquement dans les ressources des menaces issues de malware, des vulnérabilités, ainsi que d'autres types d'événements survenus dans le monde et qui peuvent avoir une incidence sur votre protection des données. Ces menaces, appelées incidents de compromission, sont basées sur les données concernant les menaces fournies par le centre opérationnel de cyberprotection (CPOC). Pour plus d'informations, voir "Rechercher des indicateurs de compromission dans des attaques connues publiquement et visant vos ressources" (p. 970).
- **Réponse rapide aux incidents** : Grâce à l'accès à toutes les activités ultérieures à la violation et au détail de chaque étape de la kill chain, vous pouvez effectuer un certain nombre d'opérations pour traiter chaque point d'attaque. Vous pouvez notamment effectuer une enquête à l'aide du contrôle à distance et de la sauvegarde riche en données d'investigation numérique (cette

fonctionnalité n'est pas disponible dans la version à accès anticipé), mettre des ressources en quarantaine et supprimer des processus de malware. Vous pouvez également reprendre l'activité à l'aide de Cyber Disaster Recovery Cloud. Pour plus d'informations, voir "Atténuation d'incidents" (p. 974).

- **Création de rapports fiables sur votre niveau de protection** : Grâce à l'option EDR, vous éliminez une grande part de l'insécurité et de la crainte liées à l'impact des cyberattaques sur votre activité. Par ailleurs, les informations relatives aux incidents sont stockées pendant 180 jours et peuvent être utilisées à des fins d'audit.

Fonctionnalités

La fonctionnalité EDR (Endpoint Detection and Response) comprend les fonctionnalités suivantes :

- Recevoir des notifications d'alerte en cas de violation
- Gèrer vos incidents dans la page Incident
- Visualisation facile à comprendre du scénario de l'attaque
- Recommandations et étapes de réparation
- Consulter les attaques dévoilées publiquement sur vos ressources à l'aide de flux d'informations sur les menaces
- Vue d'ensemble dans le tableau de bord
- Stocker les événements de sécurité pendant 180 jours

Recevoir des notifications d'alerte en cas de violation

La fonctionnalité EDR fournit des notifications d'alerte dès qu'un incident survient. Ces alertes sont mises en évidence dans le menu principal de la console Cyber Protect. Vous pouvez alors examiner une alerte en cliquant sur le bouton **Enquêter sur l'incident** qui vous redirige vers l'écran d'investigation sur l'incident (appelé également cyber kill chain).

Pour plus d'informations, voir "Examen des incidents" (p. 950).

Gérer vos incidents dans la page Incident

La fonctionnalité EDR vous permet de gérer tous vos incidents dans la page Incidents (accessible depuis le menu Protection de la console Cyber Protect). La page Incidents, qui peut être filtrée en fonction de vos besoins, vous permet de comprendre facilement et rapidement l'état actuel de vos incidents, y compris leur gravité, la ressource affectée et le niveau de positivité. Vous pouvez également accéder directement à la cyber kill chain pour visualiser le scénario de l'attaque, nœud par nœud.

Pour plus d'informations sur la page Incidents, reportez-vous à "Examen des incidents" (p. 950).

Visualisation facile à comprendre du scénario de l'attaque

La fonctionnalité EDR offre une représentation visuelle d'une attaque dans un format facile à lire. De cette manière, même le personnel non spécialisé dans la sécurité peut comprendre les objectifs et la gravité d'une attaque. Vous n'avez plus besoin des services d'un centre des opérations de sécurité ni d'embauche des spécialistes de la sécurité : la fonctionnalité EDR donne tous les détails concernant une attaque :

- Le mode de pénétration employé par l'entité malveillante
- Le mode employé par l'entité malveillante pour effacer sa trace
- Les dommages occasionnés
- Le mode de propagation de l'attaque

Pour plus d'informations, voir "Comment enquêter sur des incidents dans la cyber kill chain" (p. 958).

Recommandations et étapes de réparation

La fonctionnalité EDR offre des recommandations claires et faciles à implémenter pour la résolution d'attaques sur une ressource. Pour résoudre une attaque rapidement, cliquez sur le bouton **Atténuer tout l'incident** pour afficher et suivre les étapes recommandées pour atténuer l'incident. Ces recommandations vous permettent de reprendre rapidement les opérations affectées par une attaque. Toutefois, si vous souhaitez suivre des étapes d'atténuation plus granulaires, vous pouvez accéder à chaque nœud et l'atténuer à l'aide de la mesure pertinente.

Pour plus d'informations, voir "Atténuation d'incidents" (p. 974).

Consulter les attaques dévoilées publiquement sur vos ressources à l'aide de flux d'informations sur les menaces

La fonctionnalité EDR permet d'examiner les attaques connues et existant dans les flux d'informations sur les menaces visant vos ressources. Ces flux d'informations sur les menaces sont générés automatiquement en fonction des données de menaces reçues du Centre opérationnel de cyberprotection (CPOC). La fonctionnalité EDR vous permet de vérifier si une menace vise votre ressource, puis d'entreprendre les actions nécessaires pour la supprimer.

Pour plus d'informations, voir "Rechercher des indicateurs de compromission dans des attaques connues publiquement et visant vos ressources" (p. 970).

Vue d'ensemble dans le tableau de bord

La fonctionnalité EDR offre toute une série de statistiques dans le tableau de bord de la console Cyber Protect. Vous y trouverez :

- L'actuel état des menaces, y compris le nombre d'incidents qui doivent faire l'objet d'une enquête.

- L'évolution des attaques, classées par gravité, avec indication de campagnes d'attaques possibles.
- Le taux d'efficacité de clôture des incidents.
- Les tactiques les plus utilisées pour attaquer vos clients.
- Le statut réseau de la ressource, c'est-à-dire si elle est isolée ou connectée.

Stocker les événements de sécurité pendant 180 jours

La fonctionnalité EDR collecte des événements de ressource et d'application, et les stocke pendant 180 jours. Les événements qui précèdent la période de 180 jours sont supprimés (la suppression d'événement est basée sur l'ancienneté, pas sur l'espace de stockage). Notez que, même si la fonctionnalité EDR est désactivée, tous les événements collectés précédemment pour une ressource sont conservés, et restent disponibles pour toute enquête relative aux incidents.

Exigences logicielles

La fonctionnalité EDR (Endpoint Detection and Response) prend en charge les systèmes d'exploitation suivants :

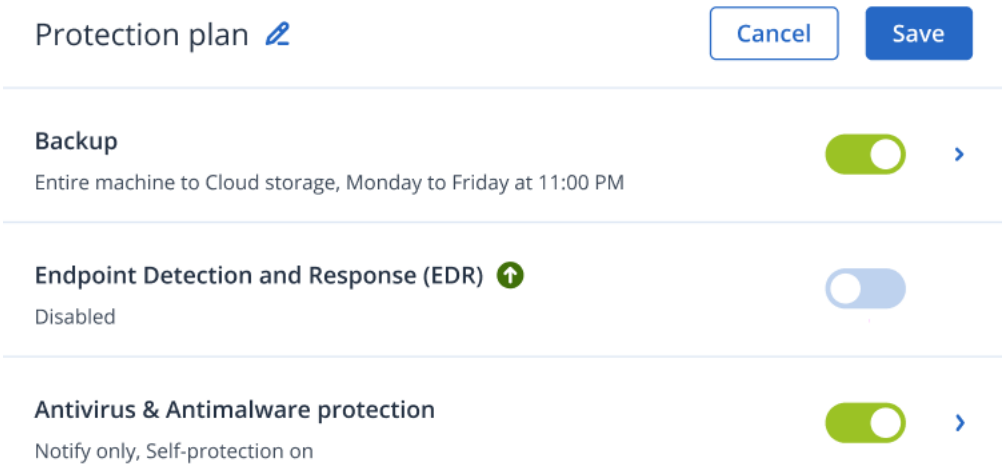
- Microsoft Windows 7 Service Pack 1 et versions ultérieures
- Microsoft Windows Server 2008 R2 et versions ultérieures

Activation de la fonctionnalité EDR (Endpoint Detection and Response)

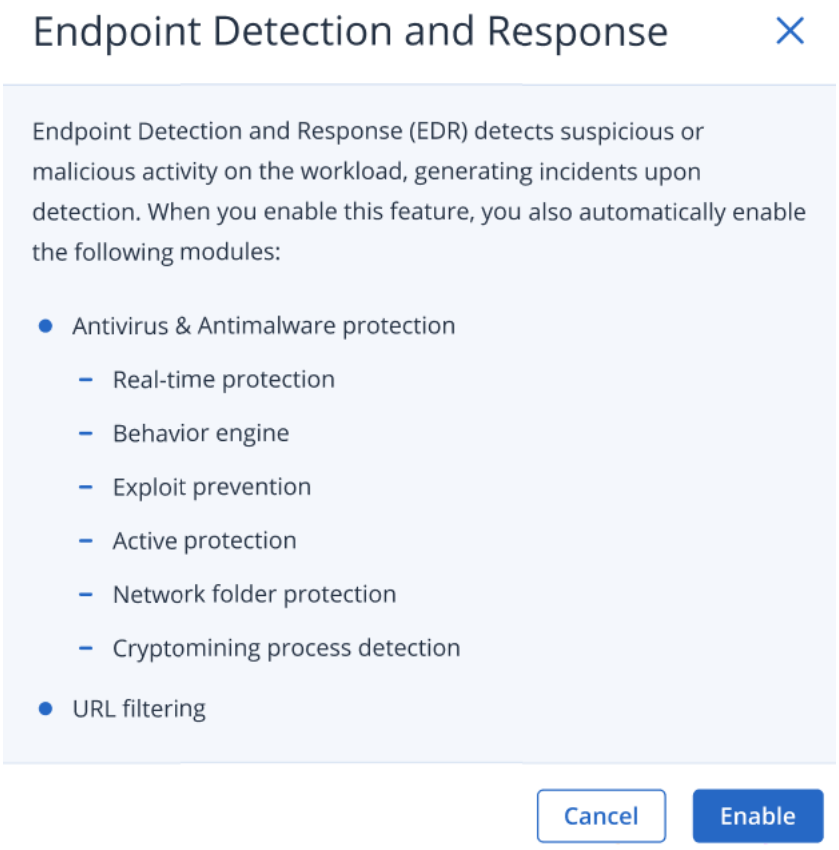
Vous pouvez activer la fonctionnalité EDR dans tous les plans de protection.

Pour activer la fonctionnalité EDR

1. Dans la console Cyber Protect, accédez à **Gestion > Plans de protection**.
2. Sélectionnez le plan de protection pertinent dans la liste affichée, puis cliquez sur **Modifier** dans l'encadré de droite.
   Vous pouvez également créer un nouveau plan de protection et passer à l'étape suivante. Pour plus d'informations sur l'utilisation des plans de protection, reportez-vous à "Plans et modules de protection" (p. 222).
3. Dans l'encadré du plan de protection, activez le module **EDR (Endpoint Detection and Response)** en cliquant sur le commutateur à côté du nom du module.



4. Dans la boîte de dialogue qui s'affiche, cliquez sur **Activer**. Notez que, lorsque le module EDR est activé, les autres modules de protection sont activés également, comme l'indique la boîte de dialogue affichée.



Remarque
Si l'un des modules **Protection active**, **Moteur de comportement**, **Prévention des failles** ou **Filtrage des URL** est **désactivé**, la fonctionnalité **EDR (Endpoint Detection and Response)** est également **désactivée**.

5. L'icône du pack **Advanced Security + EDR**, indiquée ci-dessous, est ajoutée à la liste des packs de protection nécessaires à l'implémentation du plan de protection, selon les packs supplémentaires que vous sélectionnez.

Méthode d'utilisation de la fonctionnalité EDR (Endpoint Detection and Response)

La fonctionnalité EDR vous permet de détecter des attaques qui n'ont pas été identifiées. Vous pouvez ainsi comprendre comment une attaque s'est produite et comment éviter qu'elle se reproduise. Grâce aux interprétations faciles à comprendre de chaque phase de l'attaque, le temps consacré aux enquêtes sur les attaques peut être réduit à quelques minutes.

Le tableau ci-dessous décrit le workflow général de l'utilisation de la fonctionnalité EDR. À l'origine, vous allez examiner les nouveaux incidents, leur donner un niveau de priorité, enquêter plus en détail dans la cyber kill chain, puis prendre les mesures d'intervention pertinentes.

Étape	Mode d'utilisation de la fonctionnalité EDR
ÉTAPE 1 : Examiner les incidents	Dans la liste EDR des incidents : • Comprendre la posture de sécurité d'une organisation : combien d'incidents doivent faire l'objet d'une investigation ? • Comprendre les incidents les plus critiques et définir une priorité d'investigation en fonction de leur gravité. • Comprendre si les incidents sont nouveaux ou continus.
ÉTAPE 2 : Enquêter sur les incidents	Dans la cyber kill chain EDR : • Comprendre les objectifs de l'entité malveillante et affichage des techniques d'attaque utilisées. • Vérifier le degré de probabilité qu'un incident soit une véritable attaque malveillante. • Vérifier si un flux d'informations sur les menaces a un impact sur votre ressource. • Consulter les mesures d'intervention déjà appliquées à un incident.
ÉTAPE 3 : Atténuer les incidents	Dans les sections EDR d'atténuation : • Atténuer rapidement et facilement l'intégralité d'un incident en appliquant des mesures d'intervention globales. • Atténuer les différents points d'attaque d'un incident. • Appliquer des mesures visant à empêcher l'attaque (ou les futures attaques) de se propager ou d'affecter les ressources ciblées par l'entité malveillante.

Examen des incidents

La fonctionnalité EDR (Endpoint Detection and Response) fournit une liste des incidents qui comprend des actions de prévention (ou malware) et des détections suspectes sur une ressource. La liste des incidents offre une vue d'ensemble des attaques ou menaces qui affectent vos ressources, y compris les menaces qui doivent encore être atténuées.

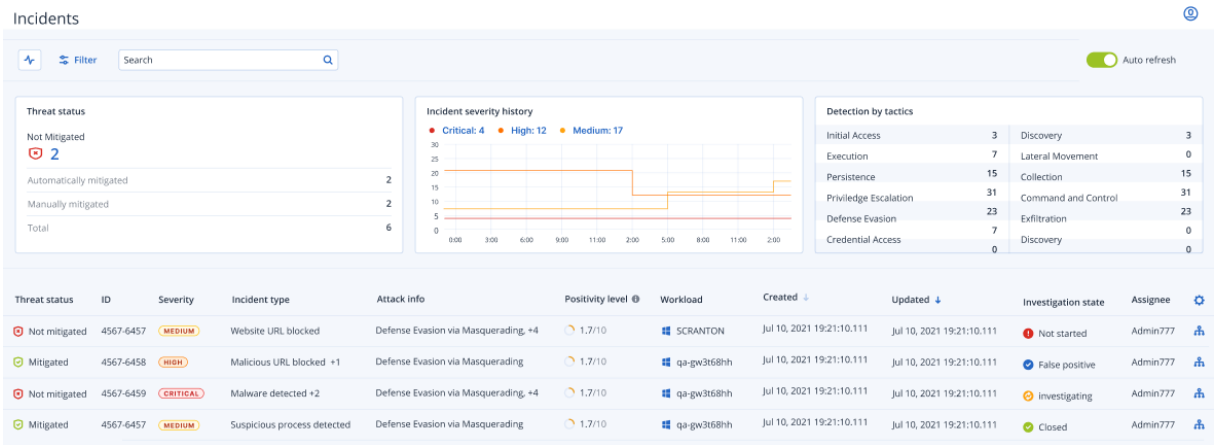
Depuis la liste des incidents, vous pouvez déterminer rapidement :

- La posture de sécurité d'une organisation : combien d'incidents doivent faire l'objet d'une investigation ?
- Quels sont les incidents les plus critiques et définir une priorité d'investigation en fonction de leur gravité.
- Si les incidents sont nouveaux ou continus.

Remarque
Lorsque vous êtes connecté en tant qu'administrateur partenaire, vous pouvez visualiser tous les incidents EDR dans un seul écran qui regroupe les incidents de tous vos clients, sans avoir besoin d'accéder à la vue des différents incidents de chaque client. Une colonne supplémentaire **Clients** est affichée ; elle comprend le nom du client auquel appartient chaque incident. En outre, les widgets affichés sur le tableau de bord de la **vue d'ensemble** affichent des mesures agrégées pour tous les clients.

La liste des incidents ci-dessous est accessible depuis le menu **Protection** de la console Cyber Protect. Pour plus d'informations sur l'examen des incidents figurant dans la liste, reportez-vous à "Affichage des incidents non atténués" (p. 953). Pour en savoir plus sur la date de création d'un incident, reportez-vous à la section Que sont les incidents exactement ?.

Remarque
Si les services gérés de détection et de neutralisation des menaces (MDR) sont activés sur vos ressources, une colonne supplémentaire **Ticket MDR** s'affiche. Elle indique le numéro de ticket fourni par le fournisseur MDR.



Remarque
La console Cyber Protect doit être ouverte pour que vous puissiez recevoir les notifications d'incident.

Que sont les incidents exactement ?

Les incidents, ou incidents de sécurité, peuvent être perçus comme des *conteneurs* comportant au moins un point de prévention ou de détection suspect (ou un mélange des deux) qui comprend tous les événements connexes et les détections d'une attaque. Ces incidents de sécurité peuvent également inclure d'autres événements bénins qui apportent un contexte supplémentaire.

De cette manière, vous pouvez visualiser les événements d'attaque d'un seul incident et comprendre les étapes logiques suivies par l'entité malveillante. Par ailleurs, la durée d'enquête sur une attaque est raccourcie.

Lorsque la fonctionnalité EDR est activée dans le plan de protection, les incidents de sécurité sont créés dans les cas suivants :

- **Une couche de prévention arrête quelque chose :** Ces incidents sont automatiquement fermés par le système, conformément aux paramètres du plan de protection. Toutefois, vous pouvez examiner précisément les opérations effectuées par le malware avant qu'il soit arrêté. Par exemple, le ransomware est arrêté lorsqu'il commence à chiffrer des fichiers, mais avant qu'il ait pu dérober des identifiants ou installé un service.
- **Une activité suspecte est détectée par la fonctionnalité EDR :** Il s'agit de détections qui devraient être examinées et traitées. En examinant la cyber kill chain visuelle améliorée (pour plus d'informations, reportez-vous à "Comment enquêter sur des incidents dans la cyber kill chain" (p. 958)), vous pouvez facilement appliquer les actions d'atténuation pertinentes.

Prioriser les incidents nécessitant une attention immédiate

La liste des incidents de la console Cyber Protect est accessible à tout moment depuis le menu **Protection** de la console Cyber Protect. La liste des incidents offre une vue d'ensemble des attaques ou menaces, ce qui vous permet de donner la priorité aux incidents nécessitant une attention particulière.

Important
Pour que les ressources restent sécurisées, analysez les incidents et donnez *toujours* la priorité à ceux qui sont en cours ou non atténués.

Comment analyser les incidents de sécurité nécessitant une attention immédiate

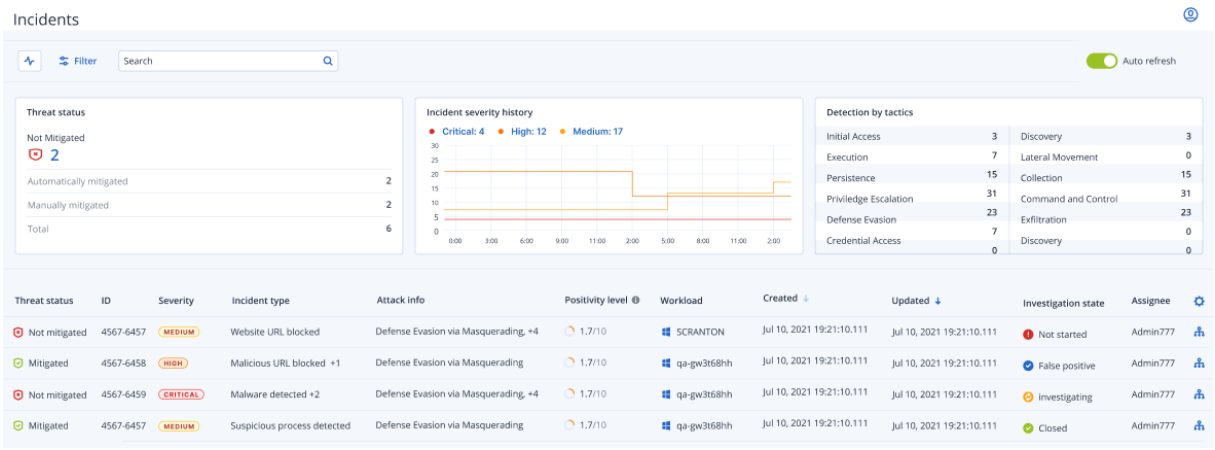
La liste des incidents vous permet d'analyser les incidents répertoriés et de donner la priorité à ceux nécessitant une attention particulière. Vous pouvez :

- Afficher les incidents non atténués : Vous pouvez rapidement comprendre, depuis la liste des incidents, si des attaques sont en cours. Les incidents non atténués (leur état est indiqué dans la

colonne **Statut de la menace**) doivent être examinés immédiatement. Par défaut, la liste des incidents est filtrée pour afficher ces incidents.

- Comprendre la portée et l'impact des incidents : En fonction du filtrage des attaques, nouvelles ou continues, vous pouvez comprendre la gravité des incidents filtrés, ainsi que leur impact sur votre activité.

Après avoir affiné la liste des incidents les plus importants, vous pouvez alors analyser les détails d'un incident afin de mieux comprendre cet incident, ainsi que les techniques utilisées par une entité malveillante pour atteindre son objectif. Pour plus d'informations, voir "Analyser les détails de l'incident" (p. 955).

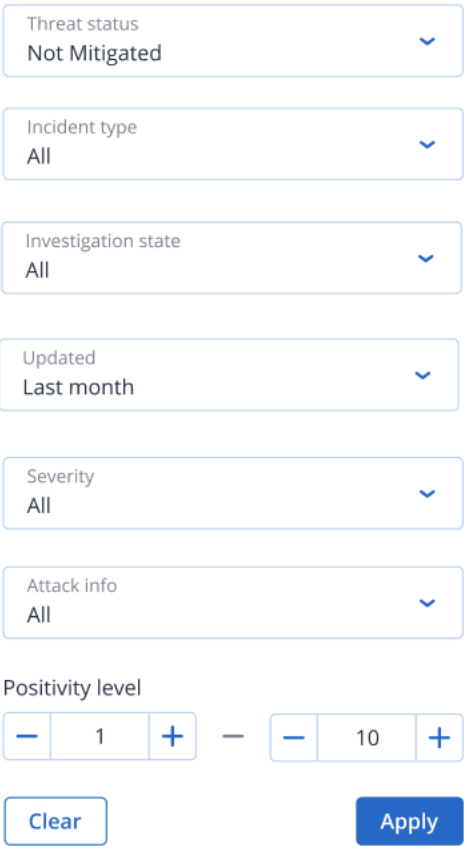


Remarque

Par défaut, la liste des incidents est triée en fonction de la colonne **Mis à jour**, qui indique la date et l'heure de la dernière mise à jour des incidents avec de nouvelles détections enregistrées dans l'incident. Notez que tout incident existant peut être mis à jour à tout moment, même s'il a été clôturé. Vous pouvez également filtrer la liste afin d'afficher les attaques nouvelles ou continues en fonction de vos besoins, en suivant la procédure ci-dessous.

Pour filtrer la liste des incidents

1. En haut de la liste des incidents, cliquez sur **Filtrer** pour la filtrer. Par exemple, si vous sélectionnez une date de début et une date de fin dans le champ **Créé**, la liste des incidents et les widgets affichent les incidents pertinents créés pendant la période définie.



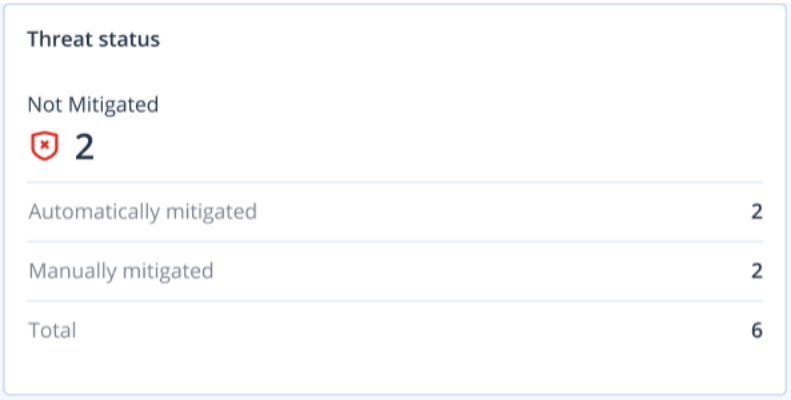
2. Lorsque vous avez terminé, cliquez sur **Appliquer**.

Affichage des incidents non atténués

Vous pouvez voir le statut d'une menace dans la colonne **Statut de la menace**, qui indique si l'incident est **Atténué** ou **Non atténué**. Le statut de la menace est défini automatiquement par la fonctionnalité EDR ; tout incident n'étant pas atténué doit faire l'objet d'une enquête dans les plus brefs délais.

Vous pouvez alors affiner encore la liste des incidents en appliquant des filtres. Par exemple, si vous souhaitez filtrer la liste en fonction du statut de la menace *et* d'un niveau de gravité spécifique, sélectionnez les options de filtre pertinentes. Après avoir filtré les incidents qui vous intéressent, vous pouvez alors effectuer une enquête, comme décrit dans "Enquête sur les incidents" (p. 957).

Vous pouvez également utiliser le widget **Statut de la menace**, comme indiqué ci-dessous, afin d'avoir une vue d'ensemble du statut de la menace. Notez que les données affichées dans ce widget reflètent les filtres que vous avez appliqués ; reportez-vous à "Pour filtrer la liste des incidents" (p. 952).



Compréhension de la portée et de l'impact des incidents

Vous pouvez comprendre rapidement la portée et l'impact des incidents en examinant les colonnes **Gravité**, **Informations concernant l'attaque** et **Niveau de positivité**. Comme indiqué ci-dessus, vous pouvez filtrer encore ces colonnes après avoir déterminé quels sont les incidents en cours. Pour ce faire, procédez comme suit :

- Examinez les incidents qui sont les plus critiques dans la colonne **Gravité**. L'état de gravité d'un incident peut être **Critique**, **Élevé** ou **Moyen**.
  - **Critique :** Il existe un fort risque de cyberactivité malveillante, avec un risque de compromission des hôtes critiques de votre environnement.
  - **Élevé :** Il existe un risque élevé de cyberactivité malveillante, avec un risque de dommages graves dans votre environnement.
  - **Moyen :** Il existe un risque accru de cyberactivité malveillante.

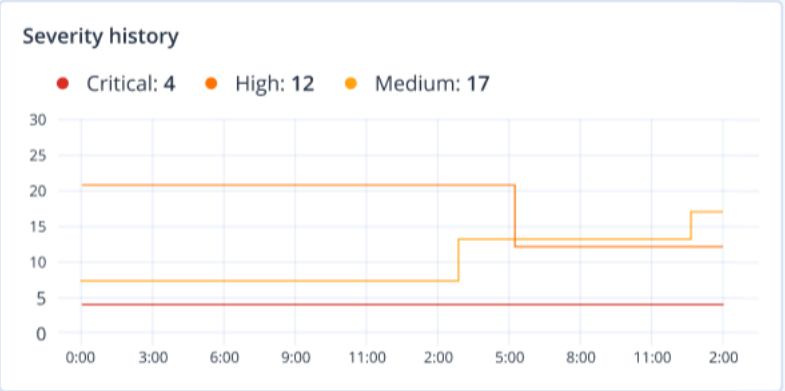
    Remarque
    Lors de la détermination de la gravité, l'algorithme EDR prend en compte le type de ressource, ainsi que la portée de chaque étape de l'attaque. Par exemple, un incident qui inclut des étapes relatives à l'usurpation d'identifiants est défini comme **Critique**.

- La colonne **Type d'incident** permet de comprendre pourquoi un incident a été créé. Le type d'incident peut comprendre un ou plusieurs des éléments suivants :
  - **Ransomware détecté**
  - **Malware détecté**
  - **Processus suspect détecté**
  - **Processus malveillant détecté**
  - **URL suspectes bloquées**
  - **URL malveillante bloquée**
- Déterminez les techniques d'attaque utilisées dans la colonne **Informations concernant l'attaque**, puis évaluez s'il existe un thème ou un modèle commun aux attaques.

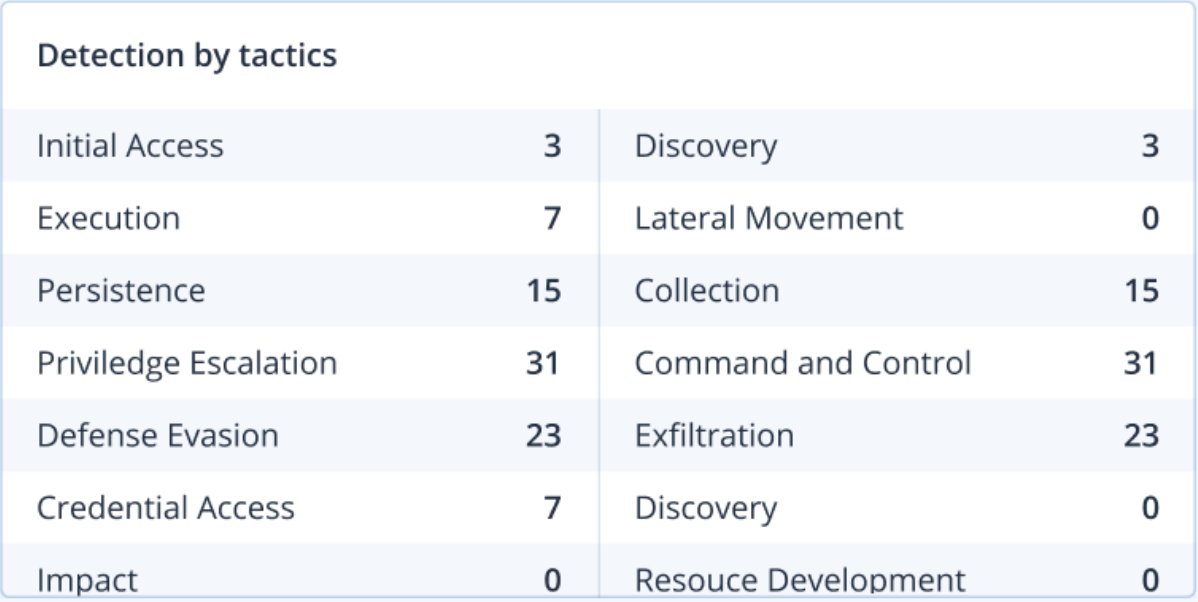
- Vérifiez si un incident est susceptible d'être une véritable attaque malveillante : la colonne **Niveau de positivité** indique une note comprise entre 1 et 10 (plus la note est élevée, plus l'attaque est susceptible d'être une véritable attaque malveillante).

Après avoir identifié les incidents qui nécessitent une attention immédiate, vous pouvez alors effectuer une enquête, comme décrit dans "Enquête sur les incidents" (p. 957).

Vous pouvez également utiliser les widgets **Historique de gravité de l'incident** et **Détection par tactique** afin d'avoir une vue d'ensemble de la gravité et des techniques d'attaque.



Le widget **Détection par tactique** affiche les différentes techniques d'attaque utilisées, avec des valeurs en vert ou en rouge qui indiquent l'augmentation ou la diminution par rapport à la période précédente spécifiée. Ce widget fournit une vue consolidée de tous les objectifs des incidents filtrés, ce qui permet d'avoir une vue rapide de l'impact sur vos clients.



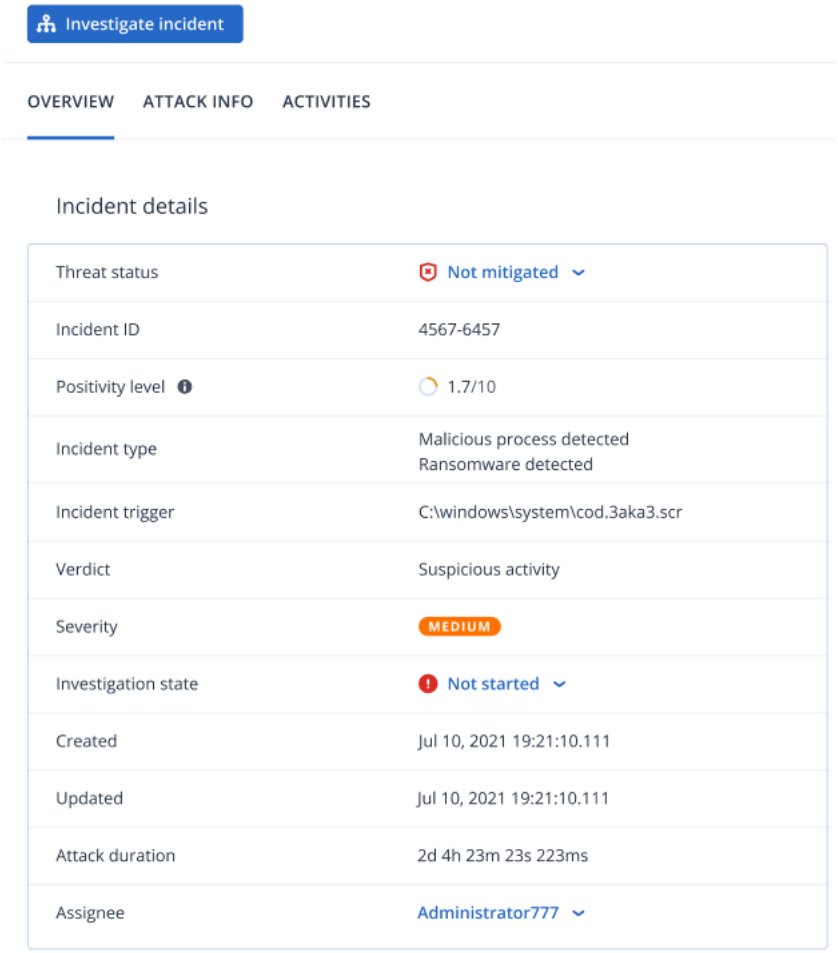
Analyser les détails de l'incident

Pendant la phase d'examen des incidents, vous pouvez également analyser les détails de chaque incident depuis la liste des incidents de la fonctionnalité EDR (Endpoint Detection and Response). Ces informations détaillées vous permettent d'examiner l'intégralité de l'incident et de comprendre

comment et à quel moment il est survenu. Par ailleurs, vous pouvez attribuer un incident à des utilisateurs spécifiques à des fins d'examen, et définir le statut d'enquête.

Pour analyser les détails de l'incident

1. Dans la console Cyber Protect, accédez à **Protection > Incidents**. La liste des incidents s'affiche.
2. Cliquez sur l'incident que vous souhaitez examiner. Les détails de l'incident sélectionné s'affichent.
3. Dans l'onglet **Vue d'ensemble**, vous pouvez examiner les détails de l'incident et de la ressource, y compris le statut et la gravité de la menace. Vous pouvez également définir l'**état de l'enquête** (vous avez le choix parmi **Enquête en cours**, **Non démarré** (état par défaut), **Faux positif** ou **Fermé**), puis sélectionnez l'utilisateur auquel vous souhaitez attribuer l'incident dans la liste déroulante **Cessionnaire**.



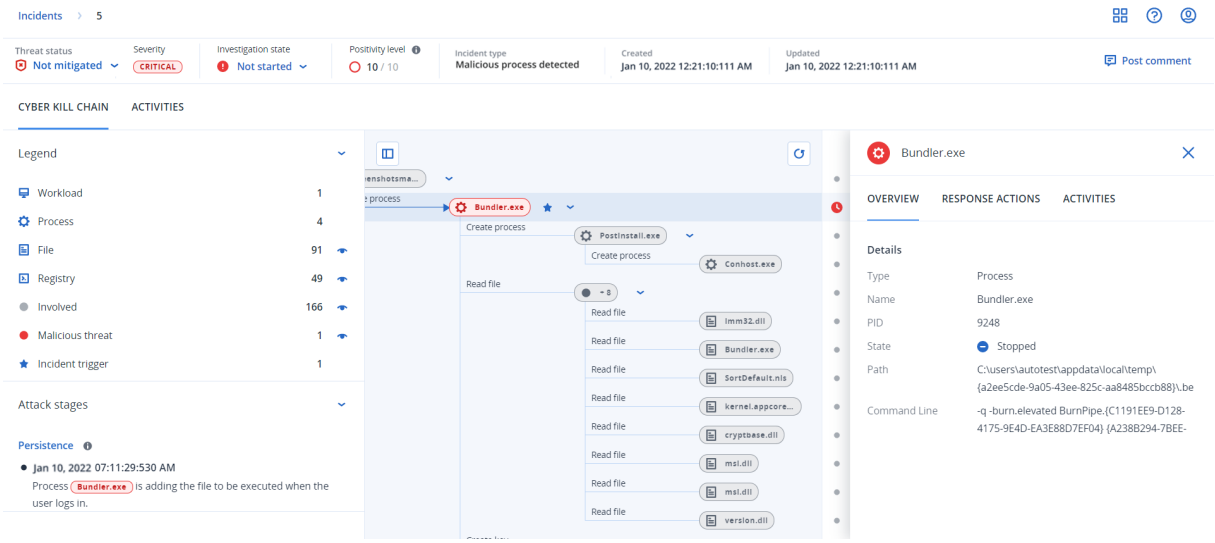
4. Cliquez sur l'onglet **Informations concernant l'attaque** pour examiner les détails de l'attaque et les techniques qu'elle utilise. Cliquez sur le lien situé en regard de la technique d'attaque répertoriée afin d'examiner plus en détail les informations sur la technique sur MITRE.org.
5. Cliquez sur l'onglet **Activités** pour examiner les actions entreprises dans la cyber kill chain afin d'atténuer l'incident. Pour plus d'informations, voir "Comment enquêter sur des incidents dans la cyber kill chain" (p. 958).

Par exemple, si un correctif a été installé sur la ressource, vous voyez qui l'a installé, la durée de son installation et toutes les erreurs qui sont survenues pendant son implémentation.

6. Cliquez sur **Enquêter sur l'incident** pour accéder à la cyber kill chain dans laquelle vous pouvez enquêter sur l'incident, nœud par nœud. Pour plus d'informations, voir "Comment enquêter sur des incidents dans la cyber kill chain" (p. 958).

Enquête sur les incidents

La fonctionnalité EDR (Endpoint Detection and Response) vous permet d'enquêter sur l'intégralité d'un incident, y compris toutes les phases et les objets de l'attaque (processus, valeurs de registre, tâches planifiées et domaines) impactés par une attaque. Ces objets sont représentés dans la cyber kill chain par des nœuds faciles à comprendre, comme indiqué ci-dessous. Utilisez la cyber kill chain pour comprendre rapidement ce qui s'est passé exactement, et le moment où l'incident s'est produit.



Chaque étape d'une attaque est visible dans la cyber kill chain et vous fournit une interprétation détaillée des circonstances de l'incident. La cyber kill chain utilise des phrases et des graphiques faciles à comprendre, qui expliquent chaque étape de l'attaque. La durée d'investigation est, par conséquent, réduite.

Vous pouvez rapidement comprendre la portée et l'impact d'un incident grâce à l'évolution de l'attaque mappée à la structure MITRE. De cette manière, vous pouvez analyser les événements qui sont survenus à chaque étape d'une attaque :

- Point d'entrée initial
- Mode d'exécution de l'attaque
- Toute élévation des privilèges
- Techniques d'évitement des détections
- Déplacements latéraux vers d'autres ressources

- Usurpation des informations d'identification
- Tentatives d'exfiltration

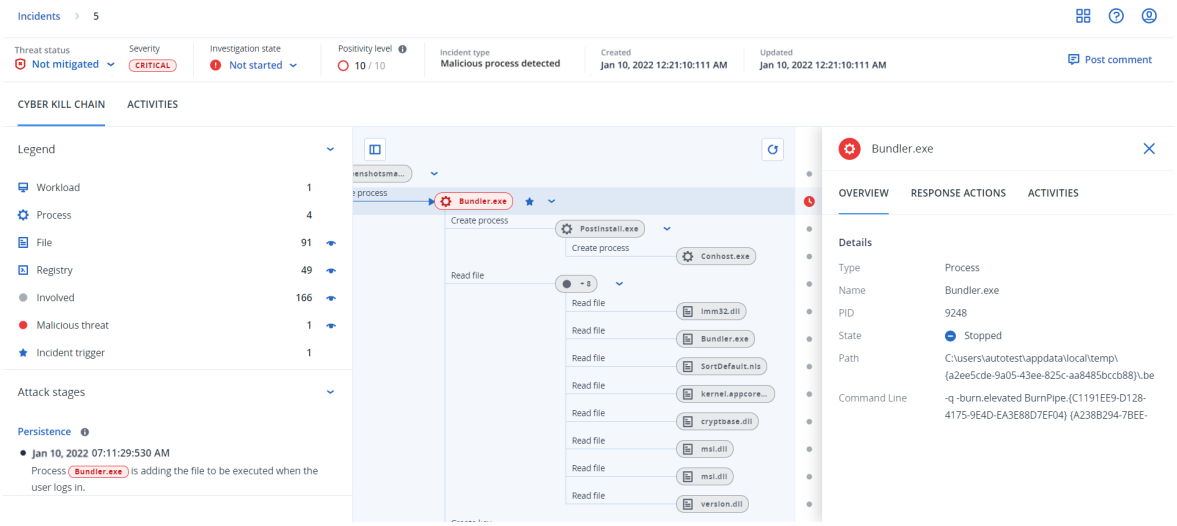
Remarque
Chaque objet impacté par l'attaque, qu'il s'agisse d'un processus, du registre, d'une tâche planifiée ou d'un domaine, est représenté par un nœud dans la cyber kill chain.

Comment enquêter sur des incidents dans la cyber kill chain

Vous pouvez enquêter à chaque étape d'une attaque dans la cyber kill chain. Suivez les phrases et les graphiques de la cyber kill chain ; ils sont faciles à interpréter et permettent de comprendre chaque étape de l'attaque, ce qui vous permet de réduire la durée de l'enquête.

Pour commencer une enquête dans la cyber kill chain

1. Dans la console Cyber Protect, accédez à **Protection > Incidents**.
2. Dans la liste des incidents affichée, cliquez sur dans la colonne à l'extrême droite de l'incident sur lequel vous souhaitez enquêter. La cyber kill chain de l'incident sélectionné est affichée.



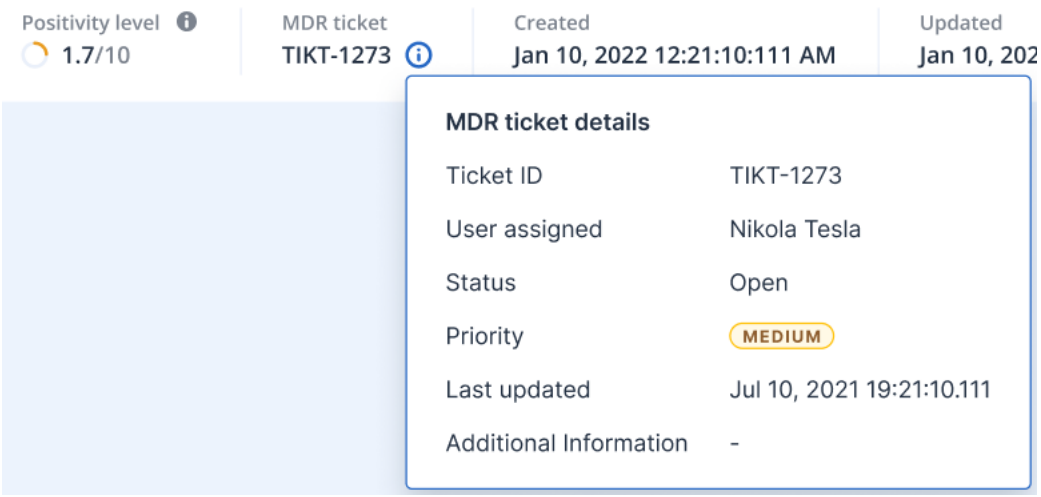
3. Affichez une synthèse de l'incident dans la barre d'état de la menace, en haut de la page. La barre d'état de la menace comprend les informations suivantes :
   - Statut actuel de la menace : Le statut de la menace est défini automatiquement par le système. Tout incident ayant le statut **Non atténué** doit faire l'objet d'une enquête dans les plus brefs délais.

Important
Un incident est défini comme étant **Atténué** lorsqu'une sauvegarde est restaurée avec succès ou que toutes les détections ont été traitées avec succès par un processus d'arrêt, une mise en quarantaine ou une restauration.

Un incident est défini comme étant **Non atténué** lorsqu'une restauration de sauvegarde n'a pas abouti ou qu'une détection au moins n'a pas été traitée par un processus d'arrêt, une mise en quarantaine ou une restauration.

Vous pouvez également définir manuellement le statut de la menace sur **Atténué** ou sur **Non atténué**. Lorsque vous sélectionnez l'un de ces statuts, vous êtes invité à saisir un commentaire. Ce commentaire est enregistré dans le cadre des activités d'investigation et est visible dans l'onglet **Activités**. Notez que la fonctionnalité EDR peut toujours rétablir le statut de la menace sur **Atténué** ou **Non atténué** si l'incident a été de nouveau détecté ou si des mesures d'intervention ont été exécutées avec succès.

- Gravité des incidents : **Critique**, **Élevée** ou **Moyenne**. Pour plus d'informations, voir "Examen des incidents" (p. 950).
- État actuel de l'enquête : L'un des états **Enquête en cours**, **Non démarré** (état par défaut), **Faux positif** ou **Fermé**. Lorsque vous démarrez une enquête sur un incident, vous devez changer le statut de cet incident afin que les autres collègues soient informés de toutes les modifications qui lui sont apportées.
- Niveau de positivité : Indique le degré de probabilité, noté entre 1 et 10, qu'un incident soit une véritable attaque malveillante. Pour plus d'informations, voir "Examen des incidents" (p. 950).
- Type d'incident : un ou plusieurs des éléments suivants : **Ransomware détecté**, **Malware détecté**, **Processus suspect détecté**, **Processus malveillant détecté**, **URL suspecte bloquée** et **URL malveillante bloquée**.
- Si les services gérés de détection et de neutralisation des menaces (MDR) sont activés sur la ressource, un champ **Ticket MDR** s'affiche. Vous pouvez consulter les détails du ticket MDR créé pour l'incident et l'analyste de sécurité MDR affecté à l'incident.



- Date de création et de mise à jour de l'incident : Date et heure de détection de l'incident ou de sa dernière mise à jour avec de nouvelles détections enregistrées dans l'incident.

4. Cliquez sur l'onglet **Légende** afin d'afficher les différents nœuds qui composent le graphique de la kill chain, puis définissez les nœuds à afficher. Pour plus d'informations, voir "Compréhension et personnalisation de la vue de la cyber kill chain" (p. 960).
5. Enquêtez et corrigez l'incident en effectuant les opérations suivantes. Notez qu'il s'agit du workflow type d'enquête et de correction d'un incident, mais qu'il peut varier en fonction de chaque incident et de vos propres exigences.
   a. Examinez chaque phase de l'attaque dans l'onglet **Phases de l'attaque**. Pour plus d'informations, voir "Comment parcourir les phases d'une attaque" (p. 963).
   b. Cliquez sur **Atténuer tout l'incident** pour appliquer les actions d'atténuation. Pour plus d'informations, voir "Atténuer l'intégralité d'un incident" (p. 975).

      Vous pouvez également traiter les différents nœuds de la cyber kill chain individuellement en suivant les indications de "Mesures d'intervention pour les différents nœuds de la cyber kill chain" (p. 980).
   c. Examinez les actions entreprises pour limiter l'incident dans l'onglet **Activités**. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 967).

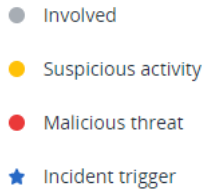
Compréhension et personnalisation de la vue de la cyber kill chain

Pour comprendre quels sont les nœuds impactés dans la cyber kill chain, accédez à la légende. La légende affiche tous les nœuds concernés par un incident, ce qui vous permet de comprendre comment ces différents nœuds ont été impactés par l'attaque de l'entité malveillante. Vous pouvez également définir les nœuds que vous souhaitez masquer ou afficher dans la cyber kill chain.

Pour accéder à la légende

1. Cliquez sur l'icône représentant une flèche à droite de la section Légende.
   La section Légende se développe, comme indiqué ci-dessous.

2. La légende utilise quatre couleurs principales qui vous permettent de comprendre rapidement les événements survenus dans chaque nœud de la cyber kill chain, comme indiqué ci-dessous. Ces nœuds à code couleur sont également inclus dans les phases de l'attaque, comme indiqué dans "Comment parcourir les phases d'une attaque" (p. 963).



Pour masquer ou afficher des nœuds dans la cyber kill chain

1. Dans la section Légende développée, vérifiez que s'affiche en regard des nœuds que vous souhaitez afficher dans la cyber kill chain. Si l'icône affichée est , cliquez dessus pour qu'elle devienne .
2. Pour masquer un nœud de la cyber kill chain, cliquez sur . L'icône change et devient , et le nœud n'est plus affiché dans la cyber kill chain.

Examiner les phases d'attaque d'un incident

Les phases d'attaque d'un incident permettent de comprendre les interprétations de chaque incident.

Chaque phase d'attaque récapitule les événements qui se sont produits, ainsi que les objets (appelés *nœuds* de la cyber kill chain) qui étaient ciblés. Par exemple, si le nom d'un fichier

téléchargé a été modifié (masquerading), la phase de l'attaque l'indique et comprend des liens vers le nœud pertinent de la cyber kill chain que vous pouvez examiner, et vers la technique MITRE ATT&CK pertinente.

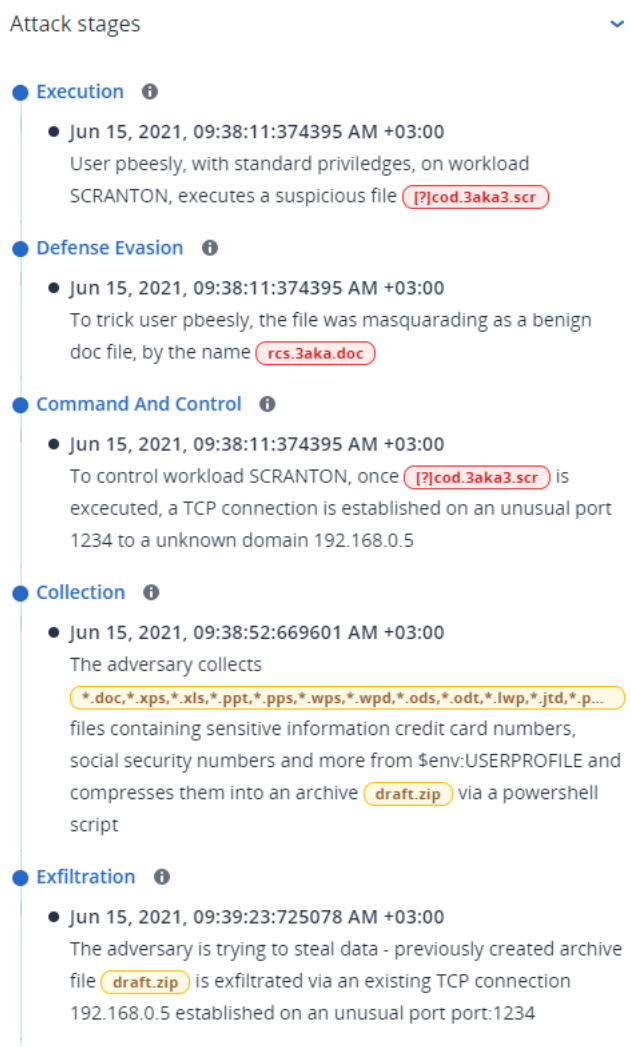
Chaque phase de l'attaque fournit les informations dont vous avez besoin pour répondre à ces questions essentielles :

- Quel était l'objectif de l'entité malveillante ?
- Dans quelle mesure l'entité malveillante a atteint cet objectif ?
- Quels nœuds étaient ciblés ?

Mais avant tout, l'interprétation permet de réduire considérablement le temps nécessaire à l'enquête sur l'incident, car vous n'avez plus à parcourir chaque événement de sécurité sur une chronologie ou un nœud graphique afin de tenter de créer une interprétation de l'attaque.

Les phases de l'attaque comprennent des informations sur les fichiers compromis contenant des informations sensibles telles que des informations de santé protégées (PHI), des numéros de carte de crédit et des numéros de sécurité sociale, comme indiqué dans la phase **Collecte** dans l'exemple ci-dessous.

Pour plus d'informations, voir "Quelles sont les informations incluses dans une phase d'attaque ?" (p. 963).



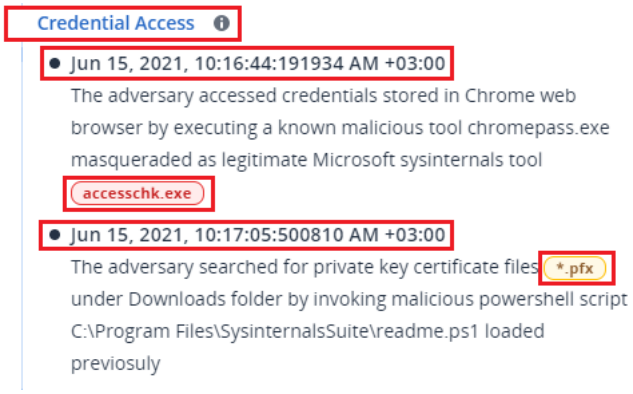
Comment parcourir les phases d'une attaque

Les phases d'une attaque sont répertoriées dans l'ordre chronologique. Faites défiler la liste complète des phases d'attaque de l'incident.

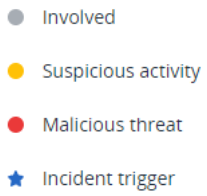
Pour examiner plus en détail une phase d'attaque spécifique, cliquez n'importe où dans la phase d'attaque pour accéder au nœud pertinent dans le graphique de la cyber kill chain. Pour plus d'informations sur la navigation dans le graphique de la cyber kill chain et des nœuds spécifiques, reportez-vous à "Examiner des nœuds de la cyber kill chain" (p. 965).

Quelles sont les informations incluses dans une phase d'attaque ?

Chaque phase d'attaque fournit une interprétation facile à comprendre de l'attaque, dans une langue facile à comprendre. Cette interprétation est composée d'un certain nombre d'éléments, comme indiqué ci-dessous et dans le tableau suivant.



Élément de phase d'attaque	Description
En-tête	Décrit l'opération que l'entité malveillante a essayé d'effectuer, ainsi que son objectif (dans l'exemple ci-dessus, **Accès par identifiants**), avec un lien vers une technique MITRE ATT&CK connue. Cliquez sur le lien pour plus d'informations sur le site Web MITRE ATT&CK. **Remarque** Si une phase d'attaque n'est pas une technique MITRE ATT&CK connue, le texte d'en-tête n'est pas lié. Ce système est pertinent pour les techniques génériques telles que des fichiers détectés dans un dossier aléatoire.
Horodatage	Heure à laquelle la phase d'attaque s'est produite.
Technique	Mode employé par l'entité malveillante pour atteindre son objectif et objets (entrées de registre, fichiers ou tâches planifiées) concernés. La description de la technique d'attaque inclut des liens à code couleur vers chaque nœud affecté de la cyber kill chain, comme indiqué dans l'exemple ci-dessus. Ces liens à code couleur vous permettent d'accéder rapidement au nœud affecté et d'enquête sur les événements exacts qui sont survenus. Les couleurs utilisées dans une phase d'attaque indiquent les éléments suivants :

Élément de phase d'attaque	Description
	 En observant la légende ci-dessus, nous voyons que la phase d'attaque exemple Accès par identifiants comporte un lien vers un nœud de malware accesschk.exe et un nœud de fichier suspect *.pfx (cliquez sur les liens pour accéder au nœud correspondant dans la cyber kill chain). Pour plus d'informations sur la navigation dans ces nœuds et sur les actions disponibles, voir "Examiner des nœuds de la cyber kill chain" (p. 965). Notez que les phases de l'attaque comprennent également des liens vers des nœuds de fichier comportant des informations sur les fichiers compromis contenant des informations sensibles : informations de santé protégées (PHI), numéros de carte de crédit et numéros de sécurité sociale.

Remarque
Chaque phase d'attaque est un événement de détection unique. Le contenu répertorié à chaque étape (en-tête, horodatage, technique) est généré en fonction de paramètres spécifiques dans l'événement de détection, qui sont basés sur les modèles de phase d'attaque stockés par EDR (Endpoint Detection and Response).

Examiner des nœuds de la cyber kill chain

Outre l'examen des phases d'attaque, vous pouvez également parcourir chacun des nœuds de l'attaque dans la cyber kill chain. De cette manière, vous pouvez accéder à des nœuds spécifiques de la cyber kill chain, et d'examiner et atténuer chaque nœud en fonction des besoins.

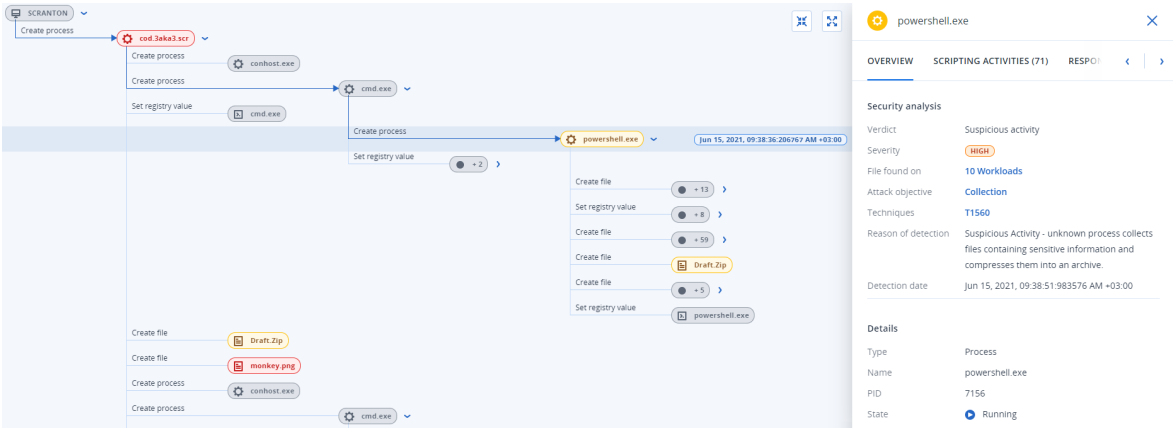
Par exemple, vous pouvez déterminer la probabilité avec laquelle un incident est une véritable attaque malveillante. En fonction de votre enquête, vous pouvez également appliquer un certain nombre de mesures d'intervention au nœud, y compris isoler une ressource ou mettre un fichier suspect en quarantaine.

Pour examiner des nœuds de la cyber kill chain

1. Dans la console Cyber Protect, accédez à **Protection > Incidents**.
2. Dans la liste des incidents affichée, cliquez sur dans la colonne à l'extrême droite de l'incident sur lequel vous souhaitez enquêter. La cyber kill chain de l'incident sélectionné est affichée.
3. Accédez au nœud pertinent, puis cliquez dessus pour afficher l'encadré correspondant.

   Remarque
   Cliquez sur le nœud pour le développer et afficher les nœuds associés.

   Par exemple, le fait de cliquer sur le nœud **powershell.exe** dans l'exemple ci-dessous ouvre l'encadré correspondant. Vous pouvez également cliquez sur l'icône en forme de flèche en regard du nœud pour afficher les nœuds associés, y compris les fichiers et les valeurs de registre, qui peuvent être affectés par le nœud **powershell.exe**. Vous pouvez ensuite cliquer sur ces nœuds associés afin d'approfondir votre enquête.



4. Examiner les informations incluses dans les onglets de l'encadré :
   - **Vue d'ensemble** : Comprend deux sections principales qui fournissent un résumé relatif à la sécurité du nœud attaqué.
     - **Analyse de la sécurité** : Fournit une analyse du nœud attaqué, y compris le verdict de la fonctionnalité EDR concernant la menace (activité suspecte, par exemple), l'objectif de l'attaque d'après les techniques d'attaque MITRE (cliquez sur le lien pour accéder au site Web MITRE), le motif de la détection, ainsi que le nombre de ressources qui peuvent être affectées par l'attaque (cliquez sur le lien **n ressources** pour afficher les ressources affectées).

       Remarque
       Le lien **n ressources** indique qu'un objet malveillant ou suspect a été *trouvé* sur d'autres ressources. Cela ne signifie pas que l'attaque se produit sur ces autres ressources, mais qu'il existe un indicateur de compromission les concernant. L'attaque s'est peut-être déjà produite (et a créé un autre incident) ou l'entité malveillante se prépare à attaquer ces autres ressources à l'aide de sa « boîte à outils ».

- **Détails** : Comprend des détails sur le nœud (son type, son nom et son état actuel), le chemin d'accès au nœud, ainsi que tous les hachages de fichier et les signatures numériques (numéros de série MD5 et de certificat).

- **Activités de script** : Comprend des détails sur les scripts appelés ou chargés dans l'attaque. Cliquez sur pour copier le script dans le Presse-papiers afin d'approfondir l'examen.

  Remarque
  L'onglet **Activités de script** n'est affiché que pour les nœuds de processus qui exécutent des commandes ou des scripts (par exemple, les commandes cmd ou PowerShell).

- **Mesures d'intervention** : Comprend un certain nombre de sections qui fournissent des actions supplémentaires d'examen, d'atténuation et de prévention, selon le type de nœud. Par exemple, pour les nœuds de ressource, vous pouvez définir un certain nombre de réponses qui comprennent une sauvegarde riche en données d'investigation numérique et une restauration à partir de la sauvegarde. En ce qui concerne les nœuds malveillants ou suspects, vous pouvez les arrêter ou les mettre en quarantaine, annuler les modifications apportées par l'attaque, et les ajouter à la liste d'autorisation ou à la liste de blocage d'un plan de protection.

  Pour plus d'informations sur l'application de mesures d'intervention à des nœuds spécifiques, reportez-vous à "Mesures d'intervention pour les différents nœuds de la cyber kill chain" (p. 980).
- **Activités** : Affiche les actions appliquées à l'incident dans l'ordre chronologique. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 967).

Comprendre les actions entreprises pour réduire un incident

Après avoir examiné un incident et enquêté sur le déroulement de l'attaque, vous appliquez généralement des mesures d'intervention. Une fois appliquées, ces mesures d'intervention sont visibles à différents endroits et vous permettent de mieux comprendre les actions entreprises pour réduire l'incident.

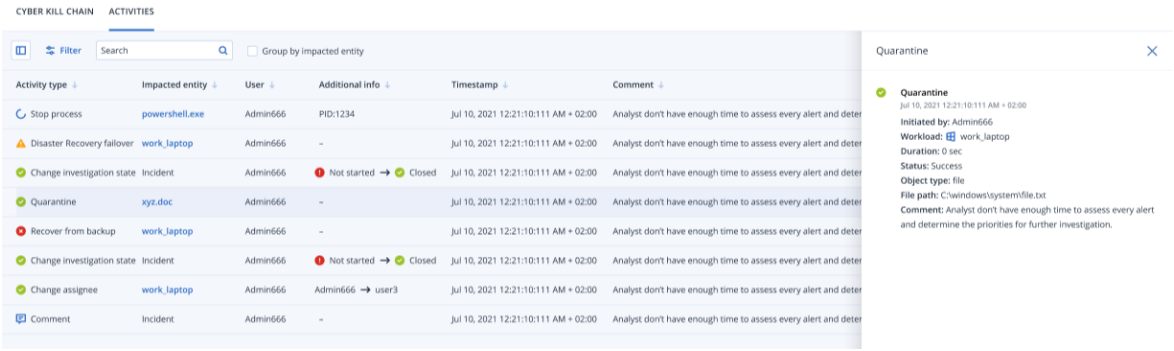
Remarque
Les incidents créés par les couches de prévention appliquent automatiquement les mesures configurées dans le plan de protection. Pour les points de détection, vous devez définir les mesures d'intervention pertinentes afin de limiter chaque scénario d'attaque.

Pour comprendre les mesures d'intervention qui ont été prises, vous pouvez afficher toutes les mesures appliquées à l'intégralité d'un incident ou à un nœud spécifique dans la cyber kill chain de l'incident.

Pour afficher toutes les mesures d'intervention appliquées à un incident

1. Dans la console Cyber Protect, accédez à **Protection > Incidents**.

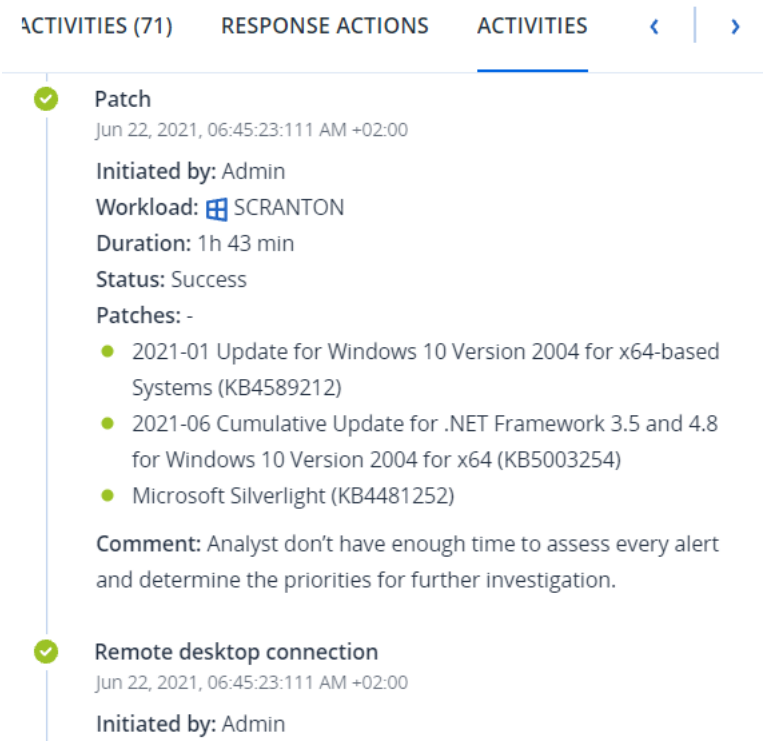
2. Dans la liste des incidents affichée, cliquez sur dans la colonne à l'extrême droite de l'incident sur lequel vous souhaitez enquêter. La cyber kill chain de l'incident sélectionné est affichée.
3. Cliquez sur l'onglet **Activités**.
   La liste des mesures d'intervention déjà appliquées à l'incident s'affiche.



4. Vous pouvez effectuer différentes opérations sur la liste affichée :
   - Cliquez sur une ligne de type d'activité pour afficher plus d'informations sur l'activité sélectionnée. Ces informations sont affichées dans un encadré, comme illustré à l'étape 3, et indiquent l'auteur et le statut de l'action, le chemin d'accès au fichier, ainsi que tout commentaire ajouté par l'auteur.
   - Pour rechercher une action spécifique, utilisez la case **Rechercher**.
   - Cliquez sur **Filtre** pour appliquer des filtres à la liste.
   - Cochez la case **Regrouper par entité impactée** afin de regrouper les actions pertinentes en fonction de l'entité.
   - Cliquez sur pour afficher/masquer la liste des actions entreprises.
     Vérifiez que s'affiche en regard des actions que vous souhaitez afficher. Si vous souhaitez masquer une action dans la liste, cliquez une nouvelle fois pour que l'icône change et devienne .

Pour afficher les mesures d'intervention appliquées à un nœud spécifique

1. Dans la cyber kill chain, cliquez sur un nœud pour afficher son encadré.
2. Cliquez sur l'onglet **Activités**.



3. Pour bien comprendre les mesures entreprises et les raisons de ce choix, vous devrez peut-être parcourir les mesures d'intervention appliquées au nœud. Par exemple, pour une connexion Bureau à distance, vous pouvez voir différentes informations : son auteur, son heure, sa durée et son statut global (si elle a abouti avec succès, a échoué ou a abouti avec des erreurs).

Rechercher des indicateurs de compromission dans des attaques connues publiquement et visant vos ressources

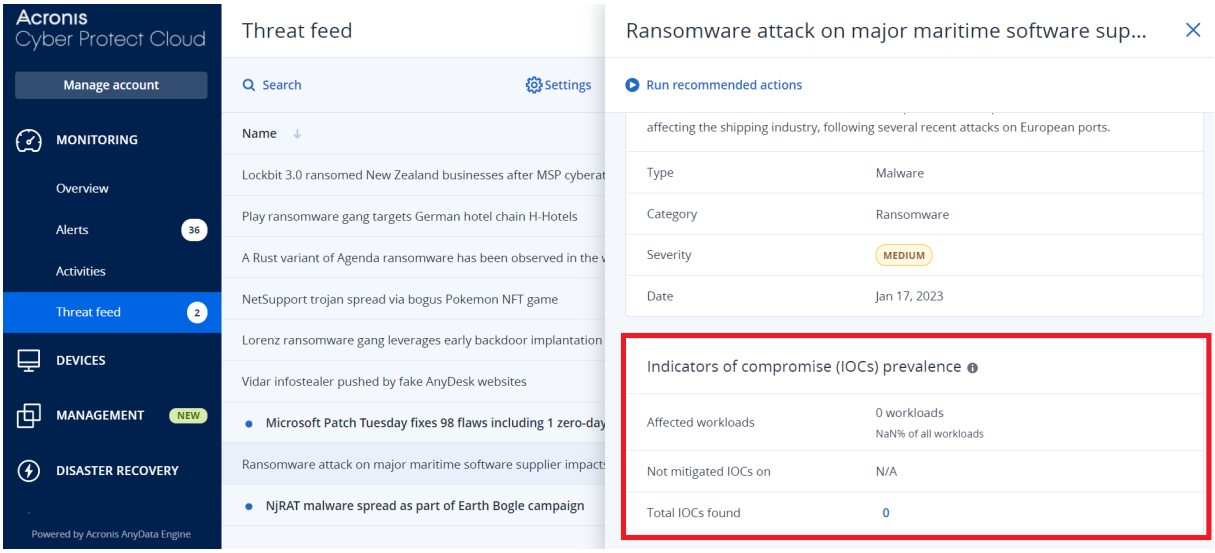
La fonctionnalité EDR (Endpoint Detection and Response) permet d'examiner les attaques connues et existant dans les flux d'informations sur les menaces visant vos ressources. Ces flux d'informations sur les menaces sont générés automatiquement en fonction des données de menaces reçues du Centre opérationnel de cyberprotection (CPOC). La fonctionnalité EDR vous permet de vérifier si une menace vise votre ressource, puis d'entreprendre les actions nécessaires pour la supprimer.

Vous pouvez accéder aux flux d'informations sur les menaces à partir du menu **Surveillance** dans la console Cyber Protect. Pour plus d'informations, voir "Flux de menaces" (p. 316).

Pour examiner une menace spécifique en détail et vérifier si elle impacte vos ressources, cliquez sur un flux d'informations sur les menaces. Vous y trouverez le nombre d'indicateurs de compromission détectés et de ressources affectées, et pourrez accéder aux ressources comportant des indicateurs de compromission non atténués.

Remarque

Si l'option EDR n'est pas activée dans le plan de protection, cette fonctionnalité supplémentaire de flux d'informations sur les menaces indiquée ci-dessous n'est pas affichée.



Définir les paramètres de flux d'informations sur les menaces

Vous pouvez définir un certain nombre de paramètres de flux d'informations sur les menaces afin de localiser et de limiter automatiquement les menaces connues.

Pour définir les paramètres de flux d'informations sur les menaces

1. Dans la console Cyber Protect, accédez à **Surveillance > Flux d'informations sur les menaces**.
2. Dans la page du flux d'informations sur les menaces qui s'affiche, cliquez sur **Paramètres**.

3. Dans la boîte de dialogue affichée, sélectionnez l'une des options suivantes :

Option	Description
Recherche d'indicateurs de compromission	Cliquez sur le commutateur pour activer la recherche automatique des indicateurs de compromission dans les ressources. Lorsque cette option est activée, les options **Action lors de la détection** et **Générer une alerte** sont également affichées.
Action lors de la détection	Dans la liste déroulante, sélectionnez l'action à entreprendre sur les fichiers concernés en cas de détection d'une menace sur une ressource : • **Aucune action** • **Quarantaine** • **Supprimer** • **Isoler les ressources**
Générer une alerte	Cochez la case pour générer une alerte si un indicateur de compromission est détecté dans une ressource. L'alerte s'affiche dans la page Alertes.

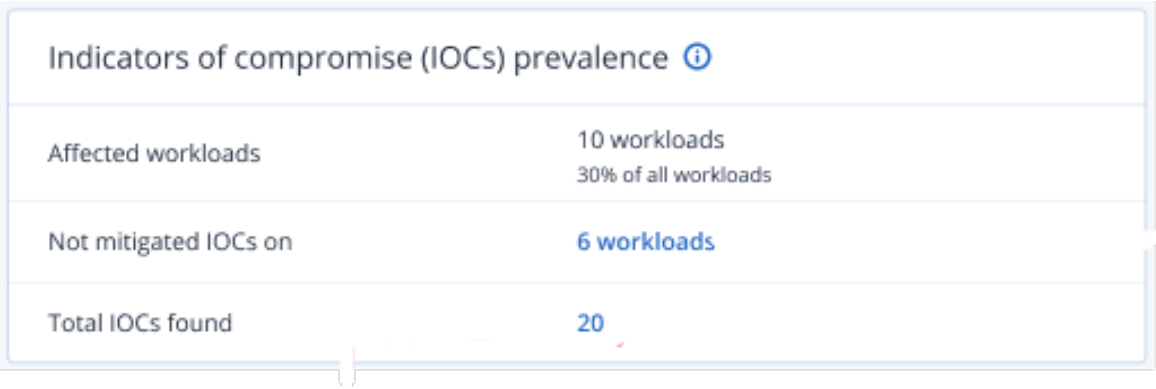
4. Cliquez sur **Appliquer**.

Examiner et atténuer les indicateurs de compromission sur les ressources affectées

Si la fonctionnalité EDR (Endpoint Detection and Response) est activée dans un plan de protection, vous pouvez visualiser toutes les menaces connues qui affectent des ressources dans le plan de protection. Vous pouvez également atténuer les autres indicateurs de compromission qui n'ont pas été atténués automatiquement. Pour plus d'informations sur l'atténuation automatique des indicateurs de compromission, reportez-vous à "Définir les paramètres de flux d'informations sur les menaces" (p. 971).

Pour examiner et atténuer les ressources affectées

1. Dans la console Cyber Protect, accédez à **Surveillance > Flux d'informations sur les menaces**.
2. Cliquez sur une menace pour afficher ses détails.
3. Dans la section **Prévalence des indicateurs de compromission**, cliquez sur le lien ***n* ressources** pour afficher les ressources présentant des indicateurs de compromission non atténués.



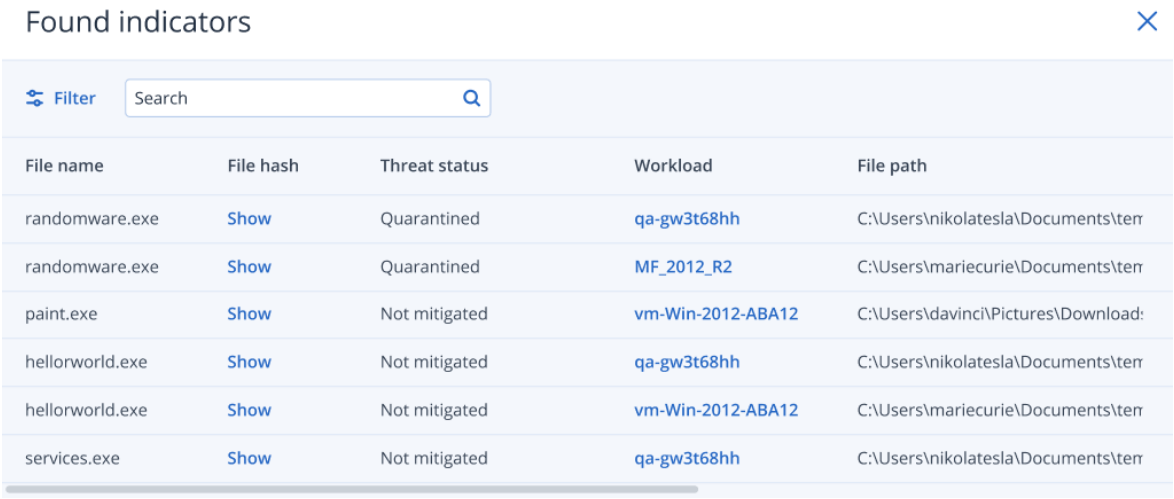
4. Dans la page Ressources, cliquez sur la ressource pertinente et examinez ses détails. Vous pouvez exécuter une fonctionnalité spécifique sur la ressource, en définissant également d'autres adresses URL à filtrer (voir "Filtrage d'URL" (p. 890)) et en bloquant les processus malveillants (reportez-vous à la section Exclusions dans "Paramètres de protection contre les virus et les malwares" (p. 865)).
   Par exemple, si un flux d'informations sur les menaces indique qu'une ressource a été affectée par un indicateur de compromission, commencez par localiser et analyser cet indicateur en suivant les indications de "Examiner et analyser les indicateurs de compromission découverts" (p. 973). Accédez ensuite au plan de protection de la ressource, puis définissez une protection supplémentaire telle que le blocage de hachages de fichiers ou de processus malveillants.

Examiner et analyser les indicateurs de compromission découverts

Outre l'examen des ressources affectées par des menaces connues, vous pouvez également examiner et analyser des indicateurs de compromission spécifiques. Vous pouvez ainsi visualiser les différentes ressources affectées par un indicateur de compromission et réduire cet indicateur.

Pour examiner et analyser des indicateurs de compromission

1. Dans la console Cyber Protect, accédez à **Surveillance > Flux d'informations sur les menaces**.
2. Cliquez sur une menace pour afficher ses détails.
3. Dans la section **Prévalence des indicateurs de compromission**, cliquez sur le lien **Nombre total d'indicateurs de compromission trouvés**.
   La page Indicateurs trouvés s'affiche.



4. (Facultatif) Utilisez l'option **Filtre** pour filtrer la liste des indicateurs de compromission en fonction de leur état. Vous pouvez également utiliser l'option **Recherche** pour rechercher des indicateurs de compromission spécifiques.
5. Pour afficher la ressource affectée par un indicateur de compromission, cliquez sur le lien figurant dans la colonne **Ressource**. Vous pouvez alors effectuer différentes opérations sur la ressource, notamment gérer les correctifs ou modifier un plan de protection.
6. (Facultatif) Dans la colonne **Hachage de fichier**, cliquez sur **Afficher** pour afficher les hachages de fichiers trouvés pour un indicateur de compromission spécifique. Dans la boîte de dialogue qui s'affiche, cliquez sur pour copier le hachage de fichier de l'indicateur de compromission dans un éditeur de texte.

Atténuation d'incidents

La fonctionnalité EDR (Endpoint Detection and Response) vous permet d'atténuer des incidents complets ou les différents points d'attaque d'un incident.

En atténuant l'intégralité d'un incident, vous pouvez choisir la ou les atténuations que vous souhaitez exécuter sur tout l'incident. Si vous devez gérer l'incident de manière plus granulaire, vous pouvez atténuer les différents points d'attaque en fonction de vos besoins. Par exemple, vous souhaiterez peut-être isoler le réseau d'une ressource afin d'arrêter le déplacement latéral ou les activités de commande et contrôle. De cette manière, même si la ressource est isolée, toutes les technologies Acronis Cyber Protect restent opérationnelles et une enquête peut être lancée.

La fonctionnalité EDR garantit une atténuation efficace par :

- Atténuation, afin de garantir que la menace est arrêtée.
- Restauration, afin de garantir que les services sont de nouveau en ligne immédiatement.
- Prévention, afin de garantir que les techniques utilisées dans une attaque ne seront plus détectées dans les futures attaques.

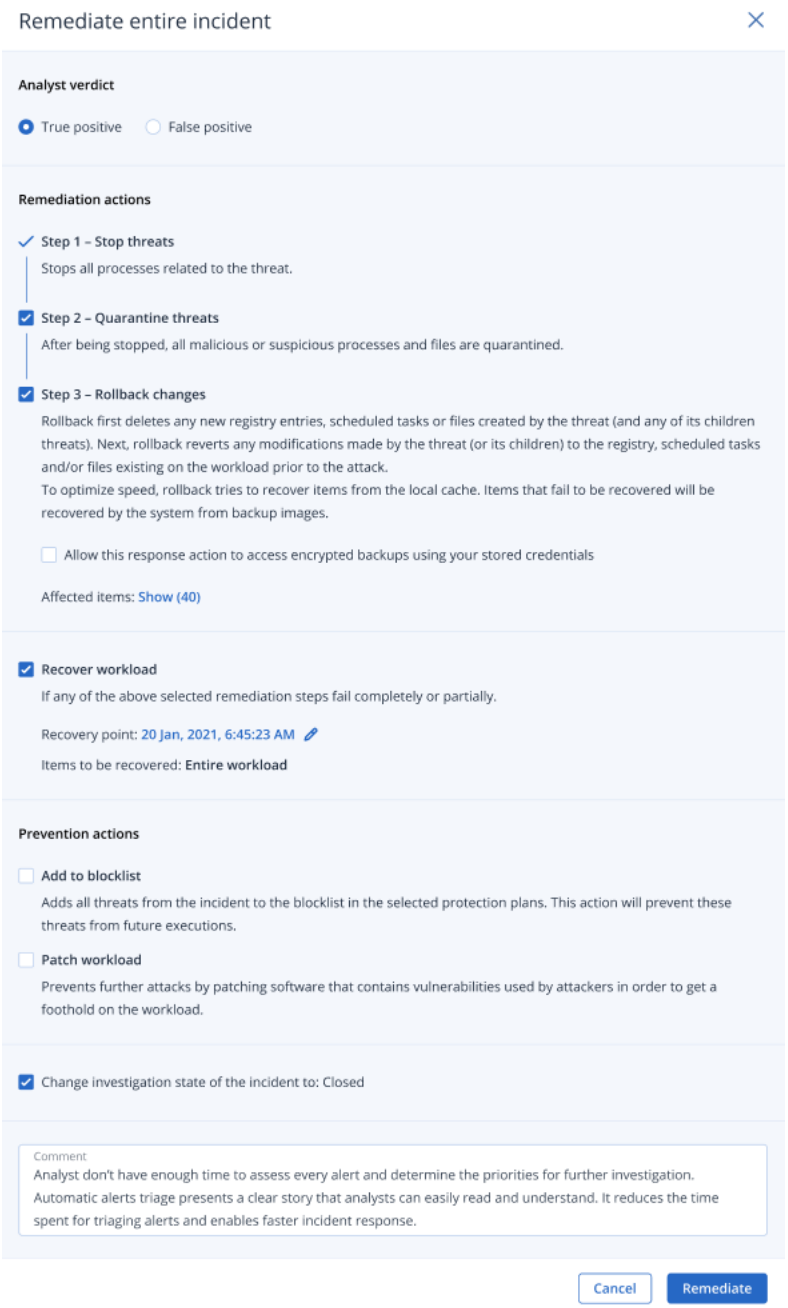
Atténuer l'intégralité d'un incident

En atténuant l'intégralité d'un incident, vous pouvez choisir rapidement et facilement la ou les atténuations que vous souhaitez exécuter sur tout l'incident. La fonctionnalité EDR (Endpoint Detection and Response) vous accompagne dans tout le processus d'atténuation, étape par étape.

Si vous devez gérer votre réseau et l'incident de manière plus granulaire, reportez-vous à "Mesures d'intervention pour les différents nœuds de la cyber kill chain" (p. 980).

Pour atténuer l'intégralité d'un incident

1. Dans la console Cyber Protect, accédez à **Protection > Incidents**.
2. Dans la liste des incidents affichée, cliquez sur  dans la colonne à l'extrême droite de l'incident sur lequel vous souhaitez enquêter. La cyber kill chain de l'incident sélectionné est affichée.
3. Cliquez sur **Atténuer tout l'incident**. La boîte de dialogue Atténuer tout l'incident s'affiche.



4. Dans la section **Verdict des analystes**, selon votre enquête sur l'incident, sélectionnez l'une des options suivantes :
   - **Vrai positif** : Sélectionnez cette option si vous avez la certitude que l'attaque est légitime. Une fois l'option sélectionnée, vous ajoutez les mesures d'atténuation et de prévention, comme le décrivent les étapes suivantes.
   - **Faux positif** : Sélectionnez cette option si vous avez la certitude que l'attaque n'est pas légitime. Dans ce mode, vous pouvez définir comment empêcher que ce classement se reproduise, par exemple en ajoutant l'incident à la liste d'autorisation d'un plan de protection.

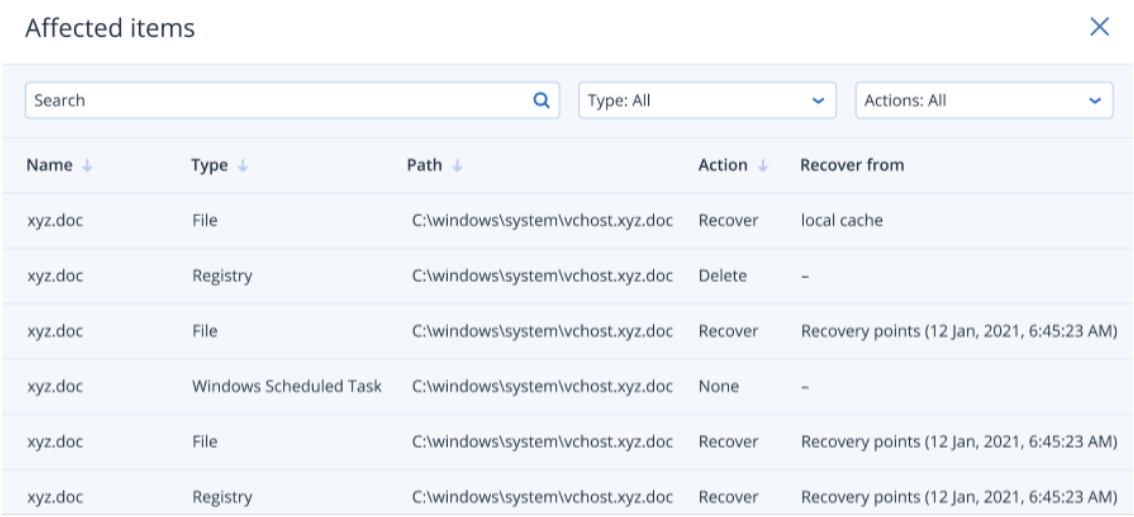
Remarque
Après avoir sélectionné **Faux positif**, vous ne pouvez définir que des actions de prévention. Pour plus d'informations, voir "Atténuer un incident faux positif" (p. 979).

5. Dans la section **Actions de réparation**, effectuez les opérations de réparation suivantes. Notez qu'elles doivent être effectuées de manière séquentielle. Par exemple, vous ne pouvez pas sélectionner l'étape 2 avant la fin de l'étape 1.
   a. **Étape 1 - Arrêter les menaces** : Cochez la case pour stopper tous les processus associés à la menace.
   b. **Étape 2 - Mettre les menaces en quarantaine** : Une fois que la menace est stoppée, cochez la case pour mettre en quarantaine tous les processus et fichiers malveillants et suspects.
   c. **Étape 3 - Annuler les modifications** : Une fois les menaces mises en quarantaine, cochez la case pour supprimer tout nouveau fichier, entrée de registre ou tâche planifiée créé par la menace (et toute menace enfant). Le processus d'annulation annule alors toute modification apportée par la menace (ou ses enfants) au registre, aux tâches planifiées et/ou aux fichiers existants sur la ressource avant l'attaque. Pour une rapidité optimale, le processus d'annulation tente de restaurer les éléments depuis le cache local. Les éléments non restaurés le seront par le système à partir d'images de sauvegarde.

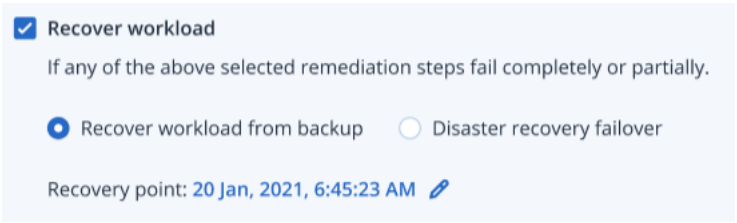
Remarque
Le processus de restauration ne concerne que les éléments stockés dans le cache local. La restauration à partir d'archives de sauvegarde sera disponible dans les prochaines versions.

Cochez la case **Autoriser cette mesure d'intervention à accéder aux sauvegardes chiffrées à l'aide des identifiants stockés** si l'accès aux sauvegardes pertinentes est chiffré. La fonctionnalité EDR accède aux identifiants utilisateur stockés pour déchiffrer les archives chiffrées et rechercher les fichiers pertinents.

Vous pouvez également cliquer sur **Éléments affectés** pour afficher tous les éléments (fichiers, registre ou tâches planifiées) affectés par l'annulation, les actions appliquées (**Supprimer**, **Restaurer** ou **Aucune**) et indiquer si les éléments sont restaurés depuis le cache local ou les images de sauvegarde.



d. **Restaurer la ressource** : Cochez cette case pour restaurer une ressource si l'une des étapes de réparation ci-dessus échoue totalement ou partiellement.



Sélectionnez l'une des options de reprise suivantes :

- **Restaurer la ressource depuis la sauvegarde** : Vous permet de restaurer une ressource à partir d'un point de reprise spécifique. Cliquez sur l'icône de modification du point de reprise pour sélectionner l'une des sauvegardes de reprise de la liste.
- **Basculement pour reprise d'activité après sinistre** : Vous permet d'exécuter une reprise d'activité après sinistre si cette fonctionnalité est activée dans votre plan de protection. Nous vous recommandons d'utiliser cette option pour les ressources critiques telles que les serveurs AD ou de bases de données. Pour plus d'informations, voir "Implémentation de la reprise d'activité après sinistre" (p. 772).

6. Dans la section **Actions de prévention**, sélectionnez les étapes d'atténuation pertinentes :
   - **Ajouter à la liste de blocage** : Cochez cette case et sélectionnez les plans de protection pertinents dans la liste des plans de protection affichée. Cette action préventive garantit que toutes les détections de l'incident ne seront plus exécutées pour les plans de protection sélectionnés.
   - **Correction de ressource** : Cochez la case pour corriger les logiciels vulnérables et empêcher les entités malveillantes d'accéder à la ressource. Vous pouvez alors sélectionner l'action à effectuer après l'installation du correctif (**Ne pas redémarrer**, **Redémarrer** ou **Redémarrer uniquement si nécessaire**), selon que l'utilisateur est connecté ou pas.
     Vous pouvez également cocher la case **Ne pas redémarrer si la sauvegarde est en cours d'exécution** afin que la ressource ne soit pas redémarrée pendant la sauvegarde.

7. Cochez la case **Modifier l'état de l'enquête sur l'incident en : Fermé**. Si cette option n'est pas sélectionnée, l'état antérieur de l'enquête est conservé.
8. Cliquez sur **Réparer**. Les actions d'atténuation que vous avez sélectionnées sont exécutées, étape par étape. La boîte de dialogue Atténuer tout l'incident indique la progression de chaque étape.
   Une fois que vous avez cliqué, le bouton indique **Aller à Activités**. Cliquez sur **Aller à Activités** pour examiner toutes les mesures d'intervention appliquées à l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 967).

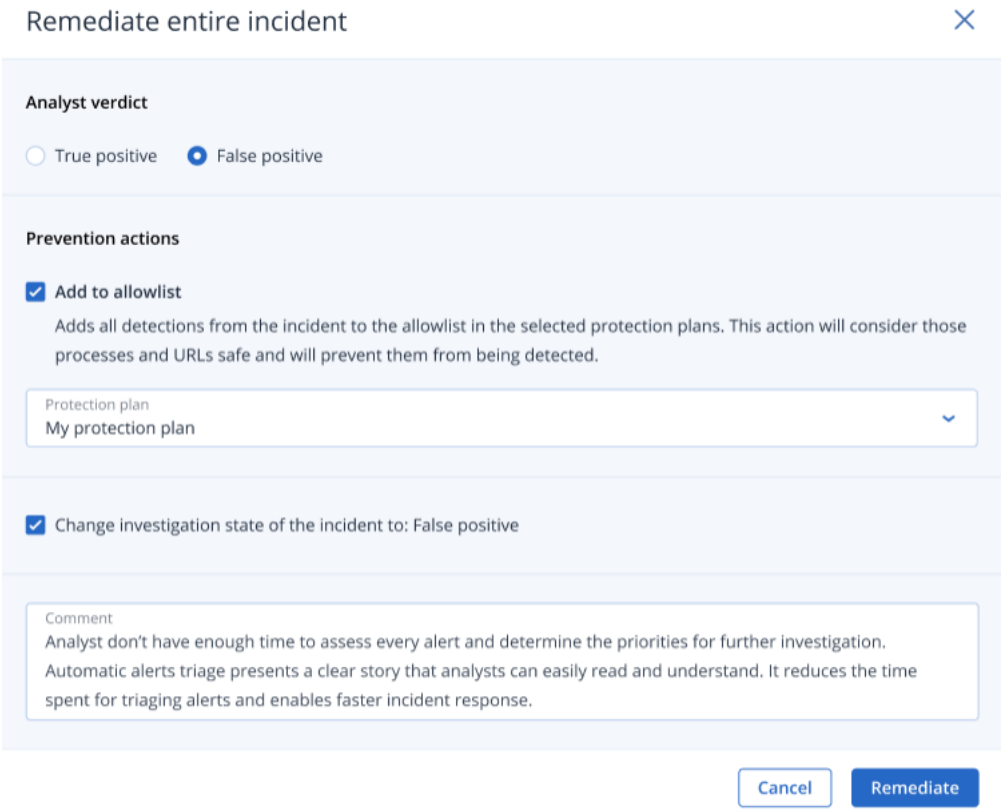
Atténuer un incident faux positif

Si vous avez la certitude qu'une attaque n'est pas une attaque authentique, en d'autres termes, si vous savez qu'il s'agit d'un faux positif, vous pouvez définir comment empêcher l'incident de survenir une nouvelle fois. Par exemple, vous pouvez ajouter l'incident à la liste d'autorisation d'un plan de protection.

Pour atténuer un incident faux positif

1. Dans la cyber kill chain de l'incident sélectionné, cliquez sur **Atténuer tout l'incident**. La boîte de dialogue Atténuer tout l'incident s'affiche.

2. Dans la section **Verdict des analystes**, sélectionnez **Faux positif**.



3. Dans la section **Actions de prévention**, cochez la case **Ajouter à la liste d'autorisation**. Dans la liste des plans de protection, sélectionnez les plans de protection pertinents.
   Cette action préventive garantit que toutes les détections de l'incident ne seront plus détectées pour les plans de protection sélectionnés.
4. Cochez la case **Modifier l'état de l'enquête sur l'incident en : Faux positif**.
5. Cliquez sur **Réparer**.
   Une fois que vous avez cliqué, le bouton indique **Aller à Activités**. Cliquez sur **Aller à Activités** pour examiner les mesures d'intervention appliquées à l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 967).

Mesures d'intervention pour les différents nœuds de la cyber kill chain

Si vous devez gérer l'incident de manière plus granulaire, vous pouvez appliquer des mesures d'intervention différentes à chacun des nœuds de la cyber kill chain. Ces mesures d'intervention vous permettent d'atténuer les nœuds rapidement et facilement.

Remarque
Pour appliquer des mesures d'intervention globales à l'intégralité d'un incident, reportez-vous à "Atténuer l'intégralité d'un incident" (p. 975).

Les mesures d'intervention sont divisées dans les catégories suivantes. Toutefois, les nœuds n'incluent pas tous la totalité des catégories suivantes :

- **Réparer** : Les actions de cette catégorie vous permettent d'appliquer une réponse immédiate à l'attaque. Elles incluent la gestion de l'isolation réseau d'une ressource, ainsi que la suppression et la mise en quarantaine de fichiers, de processus et de valeurs de registre.
- **Examiner** : Les actions de cette catégorie (applicables uniquement aux ressources) vous permettent d'exécuter une sauvegarde riche en données d'investigation numérique ou d'établir une connexion Bureau à distance afin d'effectuer une enquête plus approfondie.
- **Examiner** : Les actions de cette catégorie (applicables uniquement aux ressources) vous permettent d'établir une connexion Bureau à distance afin d'effectuer une enquête plus approfondie.
- **Restauration** : Les actions de cette catégorie (applicables uniquement aux ressources) vous permettent de répondre aux attaques intensives en exécutant une reprise à partir d'une sauvegarde ou un basculement de reprise d'activité après sinistre.
- **Prévenir** : Les actions de cette catégorie vous permettent de prévenir les futures menaces ou les faux positifs en les ajoutant à la liste d'autorisation ou la liste de blocage d'un plan de protection.

Remarque
Si un incident est clos, vous ne pouvez pas appliquer de mesure d'intervention à un nœud. En revanche, vous pouvez rouvrir un incident clos en modifiant son état d'investigation et en choisissant **Enquête en cours**. Une fois qu'il est rouvert, vous pouvez lui appliquer des mesures d'intervention.

Le tableau suivant décrit chacun des types de nœuds de la cyber kill chain, les catégories applicables pour chaque nœud et les mesures d'intervention disponibles.

Nœud	Catégorie	Mesures d'intervention
Ressource	Réparer	• Gérer l'isolation du réseau • Redémarrer la ressource
	Examiner	• Sauvegarde de données d'investigation • Connexion à distance au bureau
	Examiner	• Connexion à distance au bureau
	Restauration	• Restauration à partir d'une sauvegarde

Nœud	Catégorie	Mesures d'intervention
		• Basculement pour reprise d'activité après sinistre
	Prévenir	• Correctif
Processus	Réparer	• Stopper le processus • Quarantaine
	Prévenir	• Ajouter à la liste d'autorisation • Ajouter à la liste de blocage
Fichier	Réparer	• Supprimer • Quarantaine
	Prévenir	• Ajouter à la liste d'autorisation • Ajouter à la liste de blocage
Registre	Réparer	• Supprimer
Réseau	Prévenir	• Ajouter à la liste d'autorisation • Ajouter à la liste de blocage

Définir des mesures d'intervention pour une ressource affectée

Dans le cadre de votre réponse à une attaque, vous pouvez appliquer les actions suivantes aux ressources affectées :

- **Gérer l'isolation du réseau** : Vous permet de gérer l'isolation réseau d'une ressource afin d'arrêter le déplacement latéral ou les activités de commande et contrôle. Pour plus d'informations, voir "Gérer l'isolation réseau d'une ressource" (p. 983).
- **Correctif** : Vous permet d'installer un correctif sur une ressource afin d'éviter toute exploitation future des vulnérabilités lors de prochaines attaques potentielles. Pour plus d'informations, voir "Correction de ressource" (p. 987).

- **Redémarrer la ressource** : Vous permet de redémarrer une ressource immédiatement, ou de la redémarrer en fonction d'un délai d'expiration prédéfini. Pour plus d'informations, voir "Redémarrer une ressource" (p. 988).
- **Sauvegarde de données d'investigation** : Vous permet d'effectuer une sauvegarde riche en données d'investigation numérique à la demande à des fins d'audit ou d'investigation. Pour plus d'informations, voir "Exécuter une sauvegarde riche en données d'investigation numérique à la demande sur une ressource" (p. 990).
- **Connexion Bureau à distance** : Vous permet d'accéder à distance à la ressource faisant l'objet d'investigations. Pour plus d'informations, voir "Connexion à distance à une ressource" (p. 991).
- **Restauration à partir d'une sauvegarde** : Vous permet de restaurer à partir de la sauvegarde l'intégralité de votre ordinateur, ou des fichiers ou dossiers spécifiques. Pour plus d'informations, voir "Restauration à partir d'une sauvegarde" (p. 992).
- **Basculement pour reprise d'activité après sinistre** : Vous permet d'exécuter "Implémentation de la reprise d'activité après sinistre" (p. 772). Notez que votre ressource doit avoir un abonnement à Advanced Disaster Recovery. Pour plus d'informations, voir "Basculement pour reprise d'activité après sinistre" (p. 993).

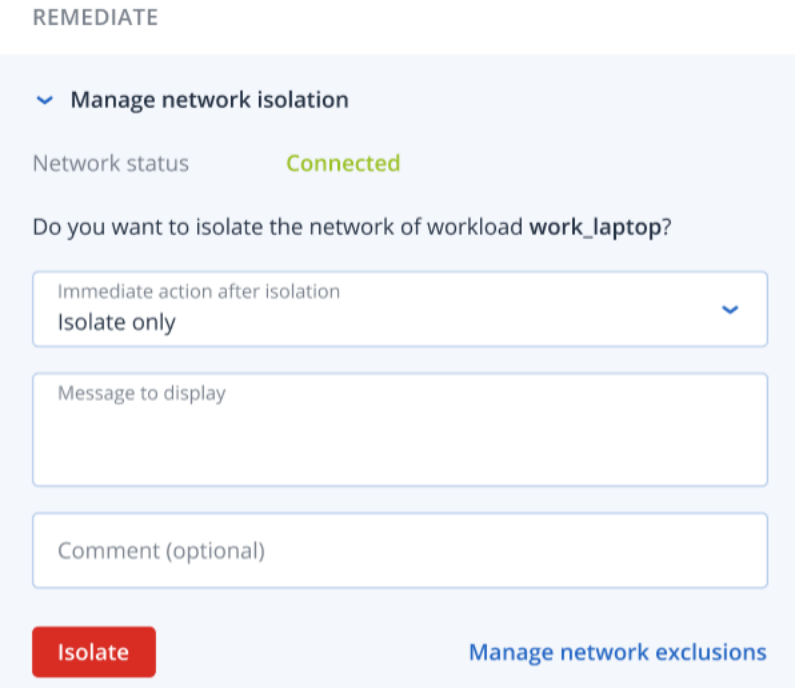
Gérer l'isolation réseau d'une ressource

La fonctionnalité EDR vous permet de gérer l'isolation réseau d'une ressource afin d'arrêter le déplacement latéral ou les activités de commande et contrôle. Selon vos exigences, vous avez le choix parmi différentes options d'isolation. Notez que toutes les technologies Acronis Cyber Protect sont fonctionnelles, même si une ressource est isolée, ce qui garantit le bon déroulement d'une enquête.

Pour isoler une ressource du réseau

1. Dans la cyber kill chain, cliquez sur le nœud de ressource que vous souhaitez traiter.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.

3. Dans la section **Réparer**, cliquez sur **Gérer l'isolation du réseau**.



Remarque
La valeur **État du réseau** indique si la ressource est connectée. Si la valeur indique **Isolé**, vous pouvez reconnecter la ressource isolée au réseau en suivant la procédure ci-dessous. Si la ressource est hors ligne, vous pouvez toujours l'isoler. Lorsqu'elle revient en ligne, elle passe automatiquement à l'état **Isolé**.

4. Dans la liste déroulante **Action immédiate après isolation**, sélectionnez l'une des options suivantes :
   - **Isoler uniquement**
   - **Isoler et sauvegarder la ressource**
   - **Isoler et sauvegarder la ressource avec des données d'investigation**
   - **Isoler la ressource et la mettre hors tension**

   Pour plus d'informations sur la définition de l'emplacement de sauvegarde de la ressource et des options de chiffrement, voir "Gestion de la sauvegarde et de la reprise des ressources et fichiers" (p. 414).
5. [Facultatif] Dans le champ **Message à afficher**, ajoutez un message qui sera visible par les utilisateurs finaux lorsqu'ils accéderont à la ressource isolée. Par exemple, vous pouvez informer les utilisateurs que la ressource est désormais isolée et que l'accès réseau (entrant et sortant) de la ressource n'est pas disponible pour l'instant. Notez que ce message s'affiche également sous la forme d'une notification dans la zone de notification et qu'il reste affiché jusqu'à ce que l'utilisateur le ferme.
6. [Facultatif] Dans le champ **Commentaire**, ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous

aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.

7. Cliquez sur **Gérer les exclusions du réseau** pour ajouter des ports, des adresses URL, des noms d'hôte et des adresses IP qui auront accès à la ressource pendant l'isolation. Pour plus d'informations, consultez la procédure de gestion des exclusions réseau.
8. Cliquez sur **Isoler**.
   La ressource est isolée. Cette action est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 967).

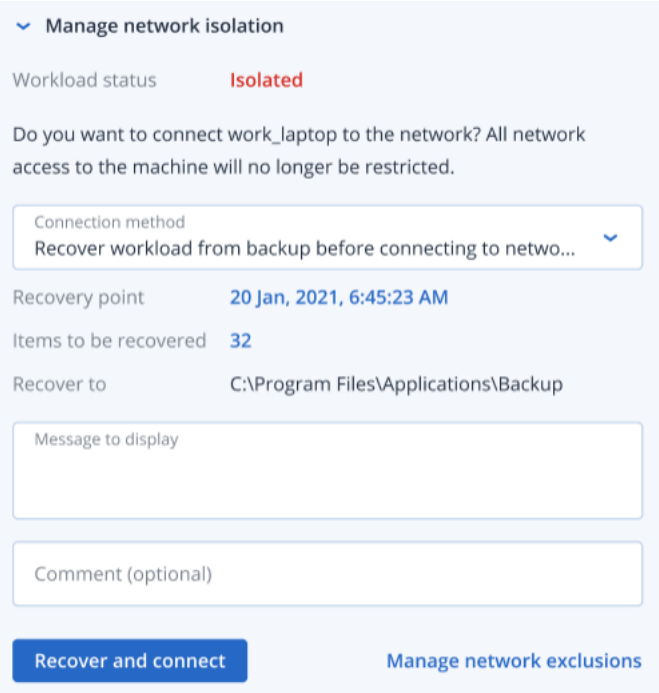
Remarque
La ressource est également affichée dans l'état **Isolé** dans le menu **Ressources** de la console Cyber Protect. Vous pouvez également isoler une ou plusieurs ressources à partir du menu **Ressources > Ressources avec agents** : sélectionnez la ou les ressources pertinentes, puis **Gérer l'isolation du réseau** dans l'encadré de droite. Dans la boîte de dialogue affichée, vous pouvez gérer les exclusions réseau, puis cliquer sur **Isoler** ou **Tout isoler** afin d'isoler les ressources sélectionnées.

Pour reconnecter une ressource isolée au réseau

1. Dans la cyber kill chain, cliquez sur le nœud de ressource que vous souhaitez reconnecter.

Remarque
Si la ressource isolée est hors ligne, vous pouvez toujours la reconnecter au réseau. Lorsqu'elle revient en ligne, elle prend automatiquement l'état **Connecté**.

2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Réparer**, cliquez sur **Gérer l'isolation du réseau**.
4. Sélectionnez l'une des options suivantes :
   - **Connecter immédiatement au réseau** : La ressource est reconnectée au réseau.
   - **Restaurer la ressource depuis la sauvegarde avant connexion au réseau** : Sélectionnez un point de reprise à partir duquel récupérer la ressource.
     a. Dans le champ **Point de récupération**, cliquez sur **Sélectionner**.
     b. Dans l'encadré affiché, sélectionnez le point de reprise pertinent.
     c. Cliquez sur **Restaurer > Intégralité de la ressource** pour restaurer tous les fichiers et dossiers de la ressource.
     Ou
     Cliquez sur **Restaurer > Fichiers/dossiers** pour restaurer des fichiers et dossiers spécifiques sur la ressource. Vous êtes alors invité à sélectionner les fichiers ou dossiers pertinents. Une fois la sélection effectuée, vous pouvez afficher la liste des éléments en cliquant sur la valeur pertinente dans le champ **Éléments à restaurer**.



Remarque
Si le point de reprise que vous sélectionnez est chiffré, vous êtes invité à fournir le mot de passe.

5. [Facultatif] Cochez la case **Redémarrer automatiquement la ressource, si nécessaire**. Cette option n'est pertinente que si vous avez sélectionné **Restaurer > Intégralité de la ressource** à l'étape 4.
6. [Facultatif] Dans le champ **Message à afficher**, ajoutez un message qui sera visible par les utilisateurs finaux lorsqu'ils accéderont à la ressource connectée. Par exemple, vous pouvez informer les utilisateurs qu'une sauvegarde a été restaurée sur la ressource et que l'accès réseau (entrant et sortant) de la ressource est de nouveau opérationnel.
7. [Facultatif] Dans le champ **Commentaire**, ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
8. Cliquez sur **Connexion** si vous avez sélectionné l'option **Connecter immédiatement au réseau** à l'étape 4.
   Ou
   Cliquez sur **Restaurer et connecter** si vous avez sélectionné l'option **Restaurer la ressource depuis la sauvegarde avant connexion au réseau** à l'étape 4.
   La ressource est reconnectée au réseau, et tout accès réseau à cette ressource n'est plus limité.

Remarque
Vous pouvez également connecter une ou plusieurs ressources à partir du menu **Ressources > Ressources avec agents** dans la console Cyber Protect : sélectionnez la ou les ressources pertinentes, puis **Gérer l'isolation du réseau** dans l'encadré de droite. Dans la boîte de dialogue qui s'affiche, cliquez sur **Connexion** ou **Connecter tout** pour reconnecter la ou les ressources sélectionnées au réseau.

Pour gérer les exclusions du réseau

Remarque
Même si toutes les technologies Acronis Cyber Protect sont opérationnelles lorsque la ressource est isolée, certains scénarios nécessitent l'établissement d'autres connexions réseau (par exemple, vous devrez peut-être transférer un fichier de la ressource vers un répertoire partagé). Dans ces scénarios, vous pouvez ajouter une exclusion du réseau ; toutefois, veillez au préalable à ce que toutes les menaces soient supprimées.

1. Dans la section **Réparer** de l'onglet **Mesures d'intervention**, cliquez sur **Gérer les exclusions du réseau**.
2. Dans l'encadré Exclusion du réseau, ajoutez les exclusions pertinentes. Pour chacune des options disponibles (Ports, Adresse URL et Nom d'hôte/Adresse IP), procédez comme suit :
   a. Cliquez sur **Ajouter**, puis saisissez le ou les ports, adresses URL ou nom d'hôte/adresses IP pertinents.
   b. Dans la liste déroulante **Direction du trafic**, sélectionnez l'une des **connexions entrantes et sortantes**, des **connexions entrantes uniquement** ou des **connexions sortantes uniquement**.
   c. Cliquez sur **Ajouter**.
3. Cliquez sur **Enregistrer**.

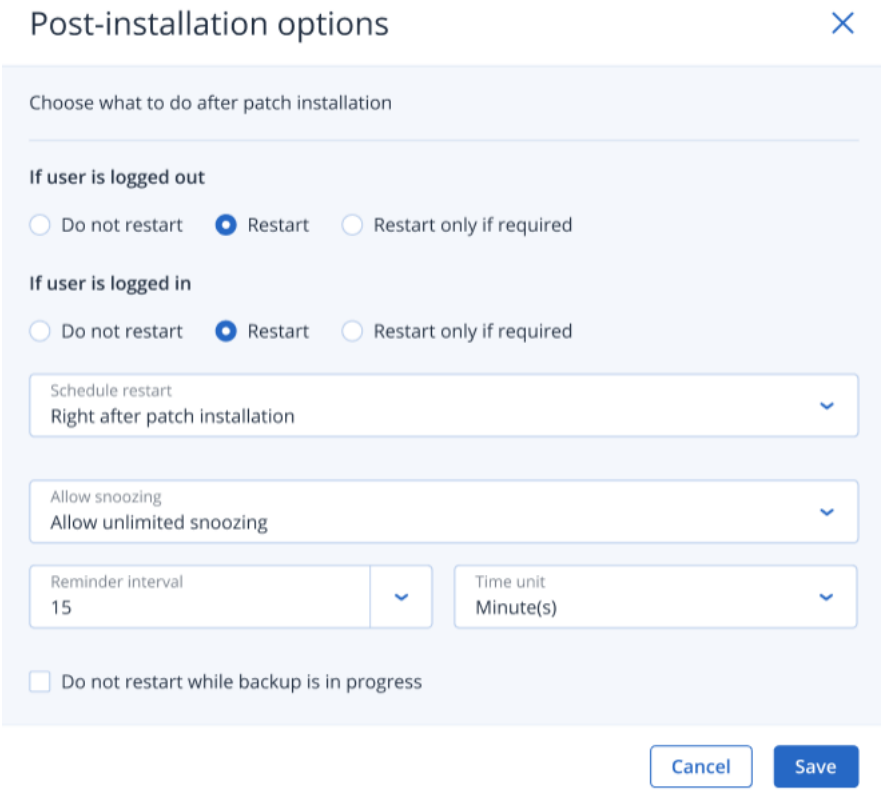
Correction de ressource

La fonctionnalité EDR détecte automatiquement si une ressource nécessite un correctif. Elle vous permet d'installer ce correctif afin d'éviter toute exploitation des vulnérabilités lors de prochaines attaques potentielles. Notez que cette fonctionnalité n'est disponible que si la ressource du partenaire comprend un abonnement pour Advanced Management.

Pour corriger une ressource

1. Dans la cyber kill chain, cliquez sur le nœud de ressource que vous souhaitez corriger.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Réparer**, cliquez sur **Correctif**.
4. Dans le champ **Correctifs à installer**, cliquez sur **Sélectionner**. Dans la boite de dialogue qui s'affiche, sélectionnez les correctifs pertinents, puis cliquez sur **Sélectionner**.

5. Dans le champ **Options de post-installation**, cliquez sur le lien affiché. La boîte de dialogue Options de post-installation s'affiche.



6. Sélectionnez l'action à effectuer après l'installation du correctif :
   - **Si l'utilisateur est déconnecté** : Sélectionnez l'une de ces options : **Ne pas redémarrer**, **Redémarrer** ou **Redémarrer uniquement si nécessaire**.
   - **Si l'utilisateur est connecté** : Sélectionnez l'une de ces options : **Ne pas redémarrer**, **Redémarrer** ou **Redémarrer uniquement si nécessaire**.
     Lorsque vous sélectionnez **Redémarrer**, vous pouvez également définir les options suivantes :
     - Planifier le redémarrage.
     - Permet d'interrompre le processus, ainsi que les intervalles entre chaque interruption.
7. [Facultatif] Cochez la case **Ne pas redémarrer si la sauvegarde est en cours d'exécution** afin que la ressource ne soit pas redémarrée si une sauvegarde est en cours.
8. Cliquez sur **Enregistrer**.
9. Dans l'onglet **Mesures d'intervention**, cliquez sur **Correctif**.
   Le correctif sélectionné est exécuté. Cette action est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 967).

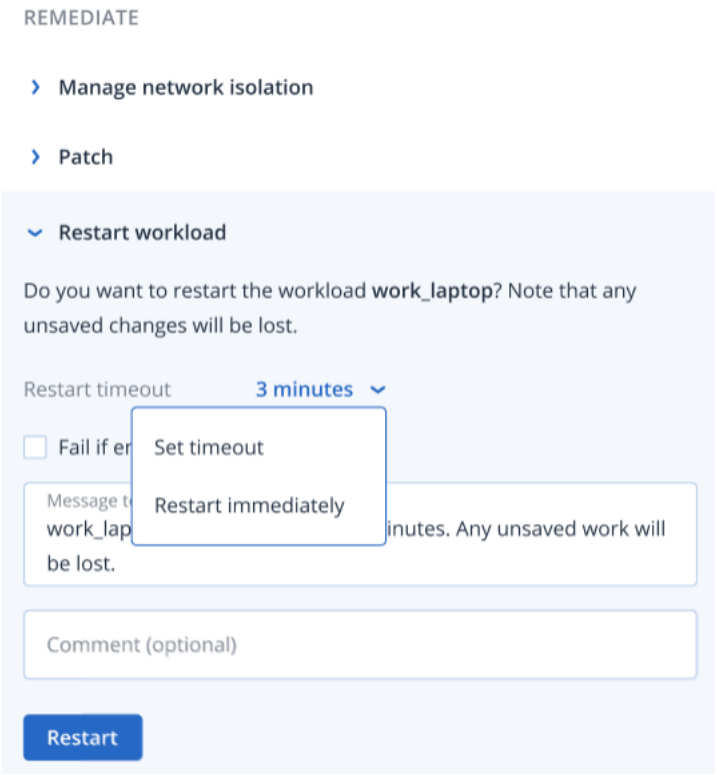
Redémarrer une ressource

Dans le cadre de votre réponse d'atténuation à une attaque, la fonctionnalité EDR vous permet de redémarrer une ressource immédiatement, ou de la redémarrer en fonction d'un délai d'expiration

prédéfini.

Pour redémarrer une ressource

1. Dans la cyber kill chain, cliquez sur le nœud de ressource pour lequel vous souhaitez planifier le redémarrage.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Réparer**, cliquez sur **Redémarrer la ressource**.



4. Dans le champ **Délai d'attente de redémarrage**, cliquez sur le lien affiché, puis sélectionnez l'une des options suivantes :
   - **Définir le délai d'attente** : Dans la boîte de dialogue Délai d'attente de redémarrage, définissez la période de redémarrage de la ressource, puis cliquez sur **Enregistrer**.
   - **Redémarrer immédiatement** : Sélectionnez cette option pour redémarrer la ressource immédiatement.
5. [Facultatif] Cochez la case **Échec si l'utilisateur final est connecté** afin que la ressource ne soit pas redémarrée si l'utilisateur est connecté.
6. Dans le champ **Message à afficher**, ajoutez un message qui sera visible par les utilisateurs lorsqu'ils accéderont à la ressource isolée.
7. [Facultatif] Dans le champ **Commentaire**, ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.

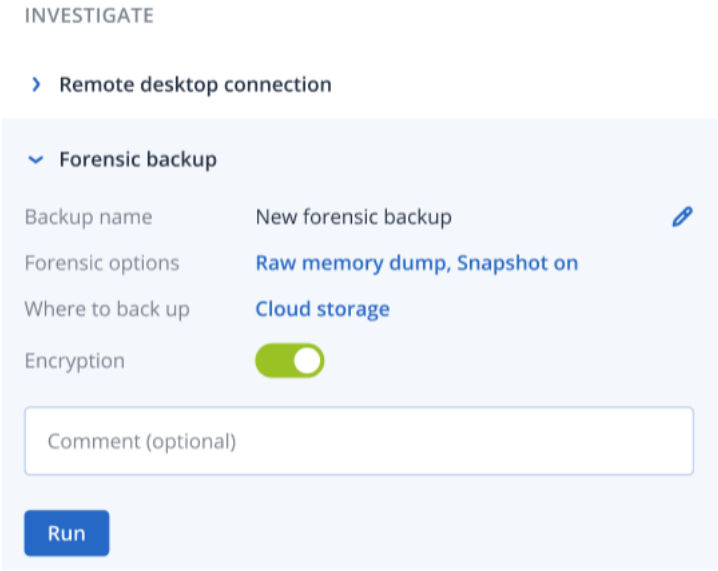
8. Cliquez sur **Redémarrer**.
   La ressource est configurée pour redémarrer en fonction de la planification définie. Cette action est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 967).

Exécuter une sauvegarde riche en données d'investigation numérique à la demande sur une ressource

Dans le cadre de votre enquête sur une attaque, la fonctionnalité EDR vous permet d'effectuer une sauvegarde riche en données d'investigation numérique à la demande à des fins d'audit ou d'investigation. Notez que cette fonctionnalité n'est disponible que si la ressource du partenaire comprend un abonnement pour Advanced Backup.

Pour exécuter une sauvegarde riche en données d'investigation numérique

1. Dans la cyber kill chain, cliquez sur le nœud de la ressource sur laquelle vous souhaitez exécuter une sauvegarde riche en données d'investigation numérique.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Examiner**, cliquez sur **Sauvegarde de données d'investigation**.



4. [Facultatif] Dans le champ **Nom de la sauvegarde**, cliquez sur l'icône de modification pour modifier le nom de la sauvegarde.
5. Dans le champ **Options d'investigation**, cliquez sur le lien affiché. Dans la boîte de dialogue Options d'investigation, sélectionnez l'une des options suivantes :
   - **Collecter le vidage mémoire brut**
   - **Collecter le vidage mémoire du noyau**

   Vous pouvez également cocher la case **Instantané des processus en cours d'exécution** pour ajouter des informations sur les processus en cours d'exécution au démarrage de la sauvegarde. Ces informations sont stockées dans une image de sauvegarde.
   Cliquez sur **Enregistrer** pour fermer la boîte de dialogue Options d'investigation.

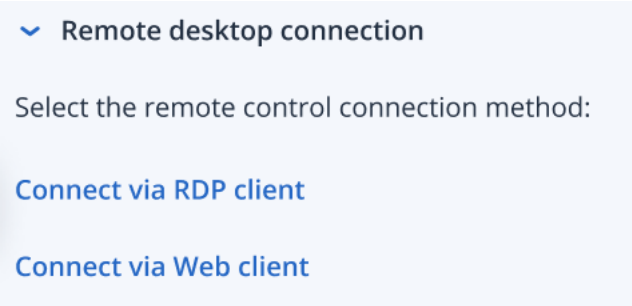
6. Dans le champ **Où sauvegarder**, cliquez sur le lien pour définir l'emplacement de la sauvegarde.
7. [Facultatif] Cliquez sur l'option **Chiffrement** pour activer le chiffrement. Dans la boîte de dialogue qui s'affiche, saisissez le mot de passe de la sauvegarde chiffrée et sélectionnez l'algorithme de chiffrement pertinent.
8. [Facultatif] Dans le champ **Commentaire**, ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
9. Cliquez sur **Exécuter**.
   La sauvegarde riche en données d'investigation numérique démarre. Cette action est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 967).

Connexion à distance à une ressource

Dans le cadre de votre enquête sur une attaque, la fonctionnalité EDR vous permet d'accéder à distance à la ressource faisant l'objet d'investigations.

Pour vous connecter à distance à une ressource

1. Dans la cyber kill chain, cliquez sur le nœud de la ressource à laquelle vous souhaitez vous connecter à distance.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Examiner**, cliquez sur **Connexion Bureau à distance**.



4. Sélectionnez l'une des méthodes de connexion à distance suivantes :
   - **Se connecter via un client RDP** : Cette méthode vous invite à télécharger et à installer le client Connexion Bureau à distance. Vous pouvez alors vous connecter à distance à une ressource à partir de la console Cyber Protect.
   - **Se connecter via le client Web** : Cette méthode ne nécessite l'installation d'aucun client RDP sur la ressource. Vous êtes redirigé vers l'écran de connexion dans lequel vous devez saisir vos identifiants de connexion à la machine distante.

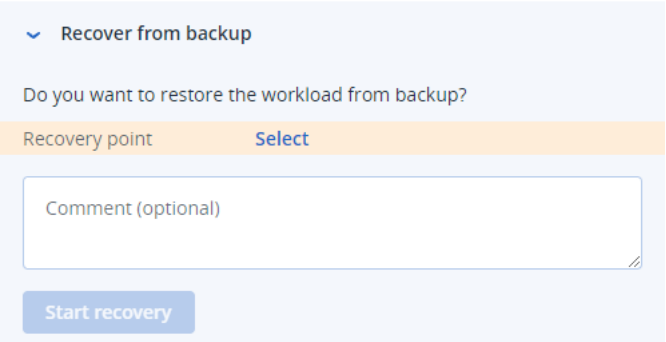
   Lorsque la connexion à distance est démarrée, cette action est visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 967).

Restauration à partir d'une sauvegarde

Dans le cadre de votre réponse de récupération à une attaque, la fonctionnalité EDR vous permet de restaurer à partir de la sauvegarde l'intégralité de votre ordinateur, ou des fichiers ou dossiers spécifiques.

Pour restaurer votre ressource depuis la sauvegarde

1. Dans la cyber kill chain, cliquez sur le nœud de ressource que vous souhaitez restaurer.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Reprise**, cliquez sur **Restauration à partir d'une sauvegarde**.



4. Dans le champ **Point de récupération**, cliquez sur **Sélectionner** et effectuez les opérations suivantes :
   a. Dans l'encadré affiché, sélectionnez le point de reprise pertinent.
   b. Cliquez sur **Restaurer > Intégralité de la ressource** pour restaurer tous les fichiers et dossiers de la ressource.
   Ou
   Cliquez sur **Restaurer > Fichiers/dossiers** pour restaurer des fichiers et dossiers spécifiques sur la ressource. Vous êtes alors invité à sélectionner les fichiers ou dossiers pertinents. Une fois la sélection effectuée, vous pouvez afficher les éléments sélectionnés pour la reprise en cliquant sur la valeur pertinente dans le champ **Éléments à restaurer**.

   Remarque
   Si le point de reprise que vous sélectionnez est chiffré, vous êtes invité à fournir le mot de passe.

5. [Facultatif] Cochez la case **Redémarrer automatiquement la ressource**. Cette option n'est pertinente que si vous avez sélectionné **Restaurer > Intégralité de la ressource** à l'étape 4.
6. [Facultatif] Dans le champ **Commentaire**, ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
7. Cliquez sur **Démarrer la récupération**.

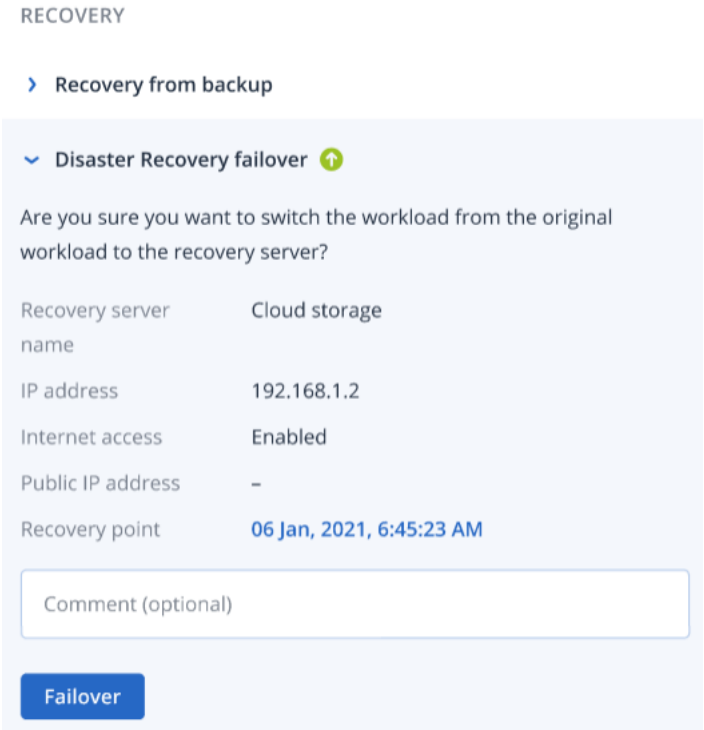
Le processus de récupération de la ressource démarre. La progression de cette action est visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 967).

Basculement pour reprise d'activité après sinistre

Dans le cadre de votre réponse de récupération à une attaque, la fonctionnalité EDR vous permet d'exécuter "Implémentation de la reprise d'activité après sinistre" (p. 772) et de basculer la ressource vers le serveur de restauration. Notez que votre ressource doit avoir un abonnement à Advanced Disaster Recovery.

Pour effectuer un basculement pour reprise d'activité après sinistre

1. Dans la cyber kill chain, cliquez sur le nœud de ressource que vous souhaitez restaurer.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Reprise**, cliquez sur **Basculement pour reprise d'activité après sinistre**.



4. Dans le champ **Point de récupération**, effectuez les opérations suivantes :
   a. Cliquez sur la date du point de reprise actuel pour sélectionner un point de restauration.
   b. Dans l'encadré affiché, sélectionnez le point de reprise pertinent.

Remarque
Si vous avez un abonnement à Advanced Disaster Recovery, vous pouvez sélectionner le serveur de restauration pertinent (la machine virtuelle hors ligne) créée dans Reprise d'activité après sinistre. Si vous n'avez pas d'abonnement, vous êtes invité à configurer la reprise d'activité après sinistre.

5. [Facultatif] Dans le champ **Commentaire**, ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
6. Cliquez sur **Basculement**.
   La ressource est basculée vers le serveur de restauration. Cette action est visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 967).

Définir des mesures d'intervention pour un processus suspect

Dans le cadre de votre réponse de réparation à une attaque, vous pouvez appliquer les actions suivantes aux processus suspects :

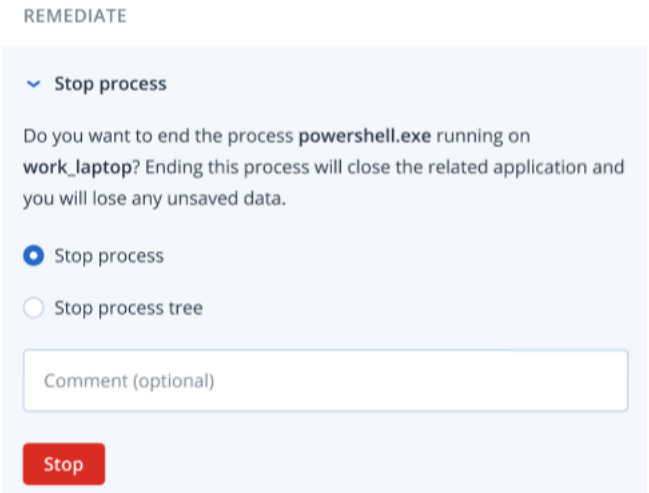
- Arrêter un processus (voir ci-dessous)
- Mettre un processus en quarantaine (voir ci-dessous)
- Annuler les modifications apportées par un processus (voir ci-dessous)
- Ajouter le processus à la liste d'autorisation ou à la liste de blocage d'un plan de protection (voir "Ajouter ou supprimer un processus, un fichier ou un réseau dans la liste de blocage ou la liste d'autorisation du plan de protection" (p. 999))

Pour arrêter un processus suspect

1. Dans la cyber kill chain, cliquez sur le nœud de processus que vous souhaitez traiter.

   Remarque
   Les processus Windows critiques ou les processus qui ne sont pas en cours d'exécution ne peuvent pas être arrêtés, et sont désactivés dans la cyber kill chain.

2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Réparer**, cliquez sur **Stopper le processus**.



4. Sélectionnez l'une des options suivantes :
   - **Stopper le processus** (arrête le processus spécifique)
   - **Stopper l'arborescence de processus** (arrête le processus spécifique et tous les processus enfants)
5. [Facultatif] Ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
6. Cliquez sur **Arrêter**. Le processus est arrêté.

Remarque
L'application associée est fermée et toutes les données non enregistrées sont perdues.

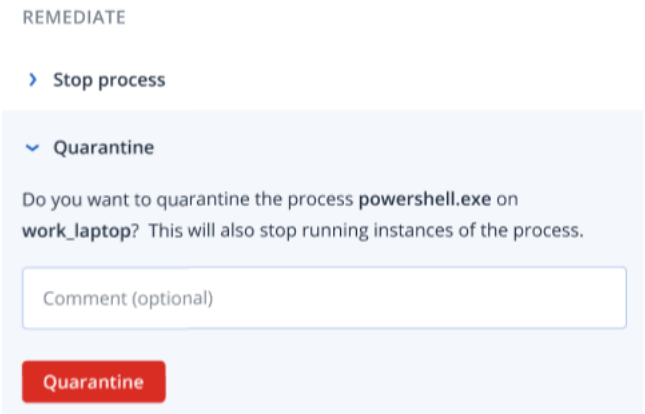
Cette action est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 967).

Pour mettre un processus suspect en quarantaine

1. Dans la cyber kill chain, cliquez sur le nœud de processus que vous souhaitez mettre en quarantaine.

Remarque
Les processus Windows critiques ne peuvent pas être mis en quarantaine et sont désactivés dans la cyber kill chain.

2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Réparer**, cliquez sur **Quarantaine**.



4. [Facultatif] Ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.

5. Cliquez sur **Quarantaine**. Le processus est arrêté, puis mis en quarantaine.

   Remarque
   Le processus est ajouté à la section de quarantaine disponible dans Protection antimalware, d'où il est géré.

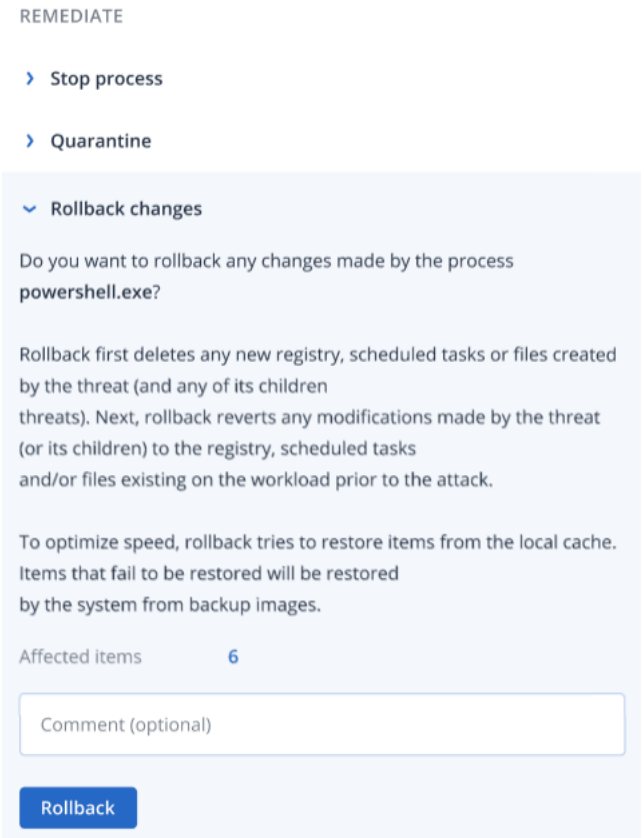
   Cette action est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 967).

Pour annuler les modifications

1. Dans la cyber kill chain, cliquez sur le nœud de processus dont vous souhaitez annuler les modifications.

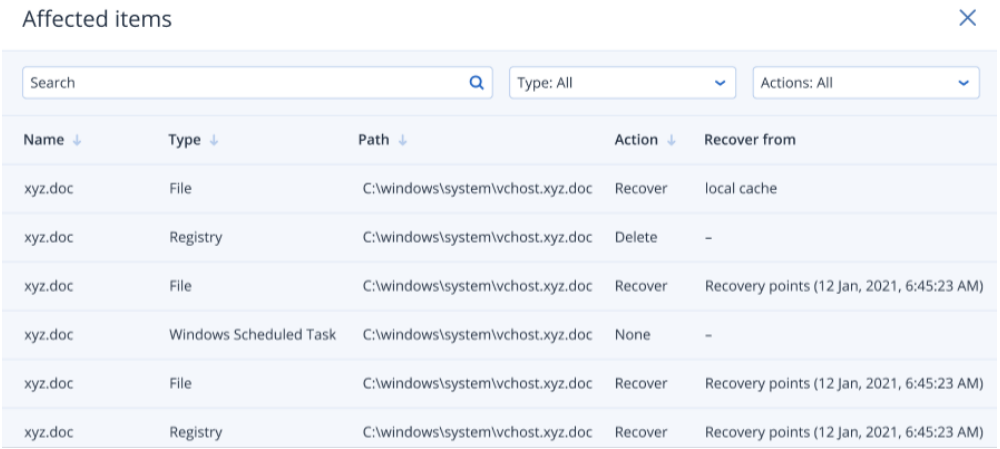
   Remarque
   Cette action est disponible uniquement pour les nœuds de détection (indiqués en rouge ou en jaune).

2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Réparer**, cliquez sur **Annuler les modifications**.



Remarque
Le processus de restauration ne concerne que les éléments stockés dans le cache local. La restauration à partir d'archives de sauvegarde sera disponible dans les prochaines versions.

4. Pour afficher les éléments affectés par l'annulation des modifications, cliquez sur le lien **Éléments affectés**. La boîte de dialogue qui s'affiche répertorie tous les éléments (fichiers, registre, tâches planifiées) que l'annulation rétablit, ainsi que l'action utilisée (**Supprimer**, **Restaurer** ou **Aucune**). Par ailleurs, vous voyez également si les éléments restaurés sont récupérés du cache local ou des points de reprise de sauvegarde.



5. [Facultatif] Ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
6. Cliquez sur **Annuler**. La fonctionnalité d'annulation rétablit les modifications apportées par le processus au registre, à un fichier ou à une tâche planifiée dans les étapes suivantes :
   a. Toutes les nouvelles entrées (registre, tâches planifiées ou fichiers) créées par la menace (et ses menaces enfants) sont supprimées.
   b. Toute modification apportée par la menace (et ses menaces enfants) au registre, aux tâches planifiées et/ou aux fichiers existants sur la ressource avant l'attaque est rétablie.
   c. L'annulation tente de restaurer les éléments depuis le cache local. Pour les éléments qui ne peuvent pas être restaurés, la fonctionnalité EDR les restaure automatiquement à partir d'images de sauvegarde intègres.

   L'action d'annulation est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 967).

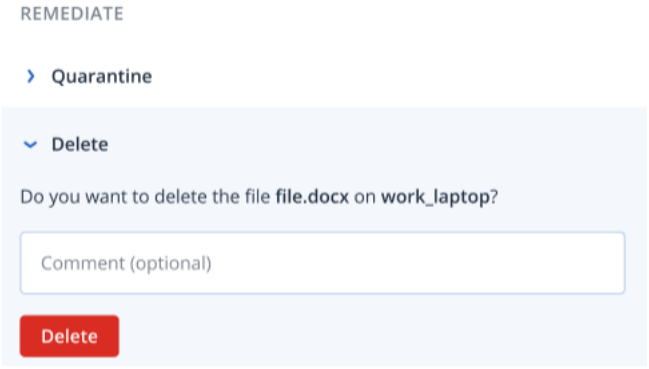
Définir des mesures d'intervention pour un fichier suspect

Dans le cadre de votre réponse de réparation à une attaque, vous pouvez appliquer les actions suivantes aux fichiers suspects :

- Supprimer un fichier (voir ci-dessous)
- Mettre un fichier en quarantaine (voir ci-dessous)
- Ajouter le fichier à la liste d'autorisation ou à la liste de blocage d'un plan de protection (voir "Ajouter ou supprimer un processus, un fichier ou un réseau dans la liste de blocage ou la liste d'autorisation du plan de protection" (p. 999))

Pour supprimer un fichier suspect

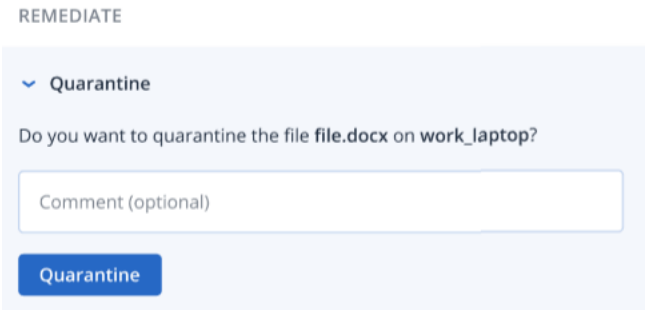
1. Dans la cyber kill chain, cliquez sur le nœud de fichier que vous souhaitez traiter.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Réparer**, cliquez sur **Supprimer**.



4. [Facultatif] Ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
5. Cliquez sur **Supprimer**.
   Le fichier est supprimé. Cette action est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 967).

Pour mettre un fichier suspect en quarantaine

1. Dans la cyber kill chain, cliquez sur le nœud de fichier que vous souhaitez traiter.
2. Dans l'encadré affiché, accédez à **Mesures d'intervention**.
3. Dans la section **Réparer**, cliquez sur **Quarantaine**.



4. [Facultatif] Ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
5. Cliquez sur **Quarantaine**.
   Le fichier est mis en quarantaine. Cette action est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 967).

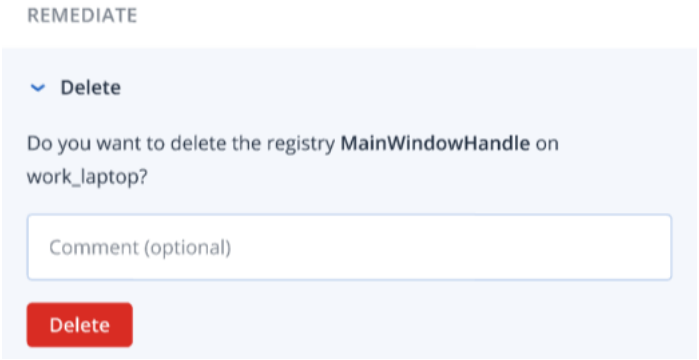
Définir des mesures d'intervention pour une entrée de registre suspecte

Dans le cadre de votre réponse de réparation à une attaque, vous pouvez supprimer les entrées de registre suspectes.

Cette option est disponible pour les nœuds de cyber kill chain du registre.

Pour supprimer une entrée de registre suspecte

1. Dans la cyber kill chain, cliquez sur le nœud que vous souhaitez traiter.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Réparer**, cliquez sur **Supprimer**.



4. [Facultatif] Ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
5. Cliquez sur **Supprimer**.
   L'entrée de registre est supprimée. Cette action est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 967).

Ajouter ou supprimer un processus, un fichier ou un réseau dans la liste de blocage ou la liste d'autorisation du plan de protection

Dans le cadre de votre réponse préventive à une attaque, vous pouvez ajouter un nœud à la liste d'autorisation ou à la liste de blocage de votre plan de protection.

Vous pouvez ajouter un nœud à une liste d'autorisation si vous considérez le nœud comme étant sécurisé et souhaitez éviter à l'avenir d'autres détections le concernant. Ajoutez un nœud à une liste de blocage pour que le nœud ne s'exécute plus à l'avenir.

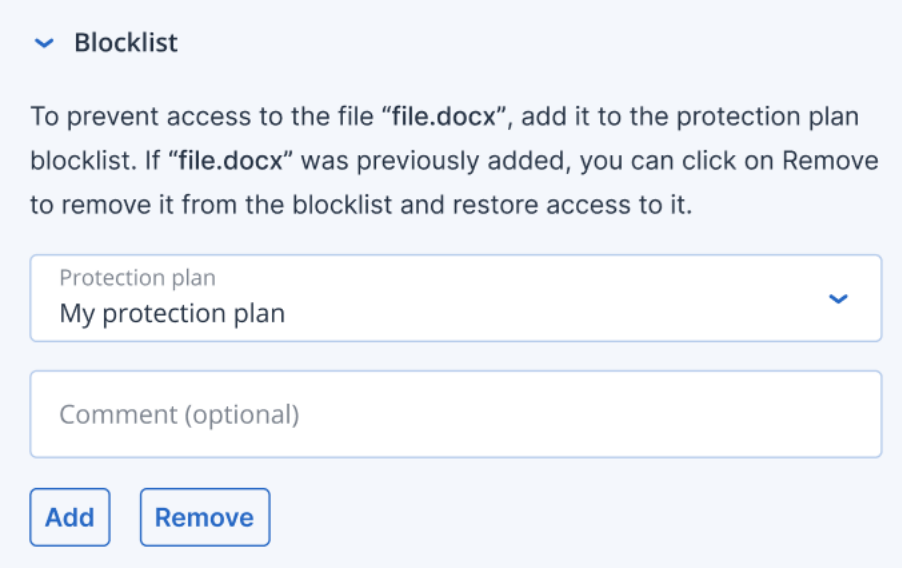
Vous pouvez également supprimer un nœud de la liste d'autorisation ou de la liste de blocage afin d'autoriser ou d'empêcher tout accès futur à ce nœud.

Cette option est disponible pour les nœuds de cyber kill chain suivants :

- Processus
- Fichier
- Réseau

Pour ajouter ou supprimer un processus, un fichier ou un réseau dans la liste de blocage du plan de protection

1. Dans la cyber kill chain, cliquez sur le processus, le fichier ou le nœud de réseau dont vous souhaitez résoudre les problèmes.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Prévention**, cliquez sur l'icône en forme de flèche située à côté de **Liste de blocage**.



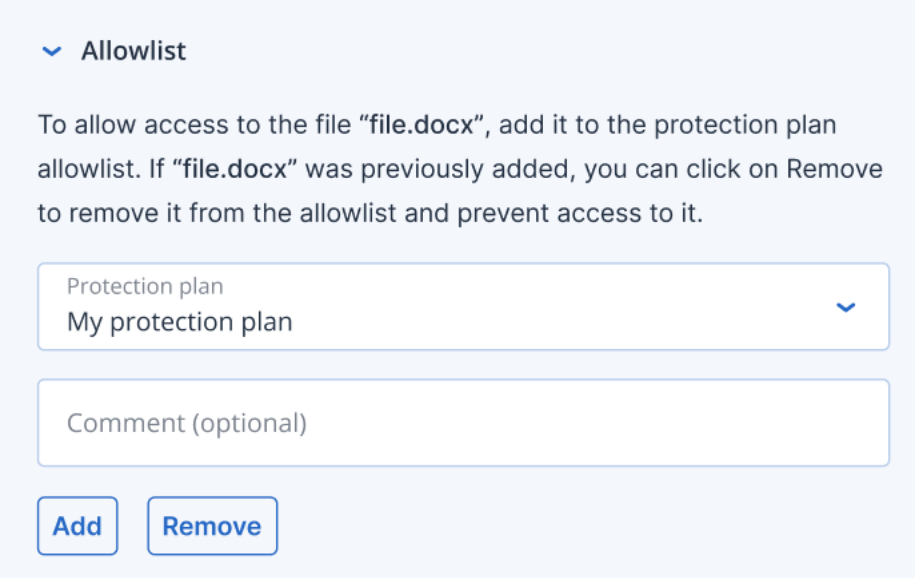
4. Sélectionnez le ou les plans de protection auxquels vous souhaitez appliquer cette mesure.
5. [Facultatif] Ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
6. Cliquez sur **Ajouter**.
   L'action est implémentée, et le processus, le fichier ou le réseau ne pourra plus être lancé.

Si le processus, le fichier ou le réseau a déjà été ajouté à la liste de blocage et que vous souhaitiez à présent le supprimer de cette liste, cliquez sur **Supprimer**. L'accès au nœud sera ainsi autorisé à l'avenir.

L'action d'ajout ou de suppression peut également être visualisée dans les onglets **Activités** de chaque nœud et de l'incident dans son intégralité. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 967).

Pour ajouter ou supprimer un processus, un fichier ou un réseau dans la liste des autorisations du plan de protection

1. Dans la cyber kill chain, cliquez sur le processus, le fichier ou le nœud de réseau dont vous souhaitez résoudre les problèmes.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Prévention**, cliquez sur l'icône en forme de flèche à côté de **Liste d'autorisation**.



4. Sélectionnez le ou les plans de protection auxquels vous souhaitez appliquer cette mesure.
5. [Facultatif] Ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
6. Cliquez sur **Ajouter**.
   L'action est implémentée, et le processus, le fichier ou le réseau ne pourra plus être détecté.
   Si le processus, le fichier ou le réseau a déjà été ajouté à la liste d'autorisations et que vous souhaitiez à présent le supprimer de cette liste, cliquez sur **Supprimer**. Cela empêchera tout accès futur au nœud.
   L'action d'ajout ou de suppression peut également être visualisée dans les onglets **Activités** de chaque nœud et de l'incident dans son intégralité. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 967).

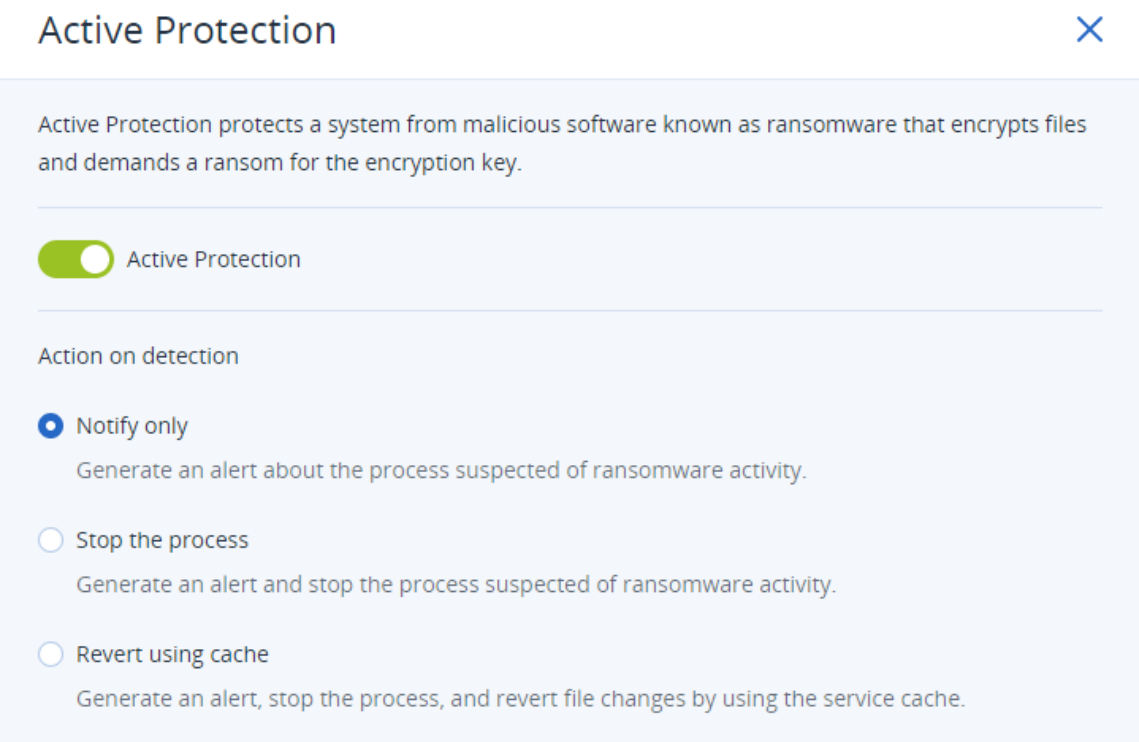
Activation du mode de surveillance pour EDR (Endpoint Detection and Response)

Le mode de surveillance dans Cyber Protection vous permet d'utiliser EDR dans un environnement de production. Cela vous permet de rechercher la présence de faux positifs et d'exclure les éléments nécessaires avant de déployer entièrement EDR.

En mode de surveillance, rien n'est bloqué ni arrêté. Des incidents sont créés, mais aucune réponse n'est initiée.

Pour activer le mode de surveillance pour EDR

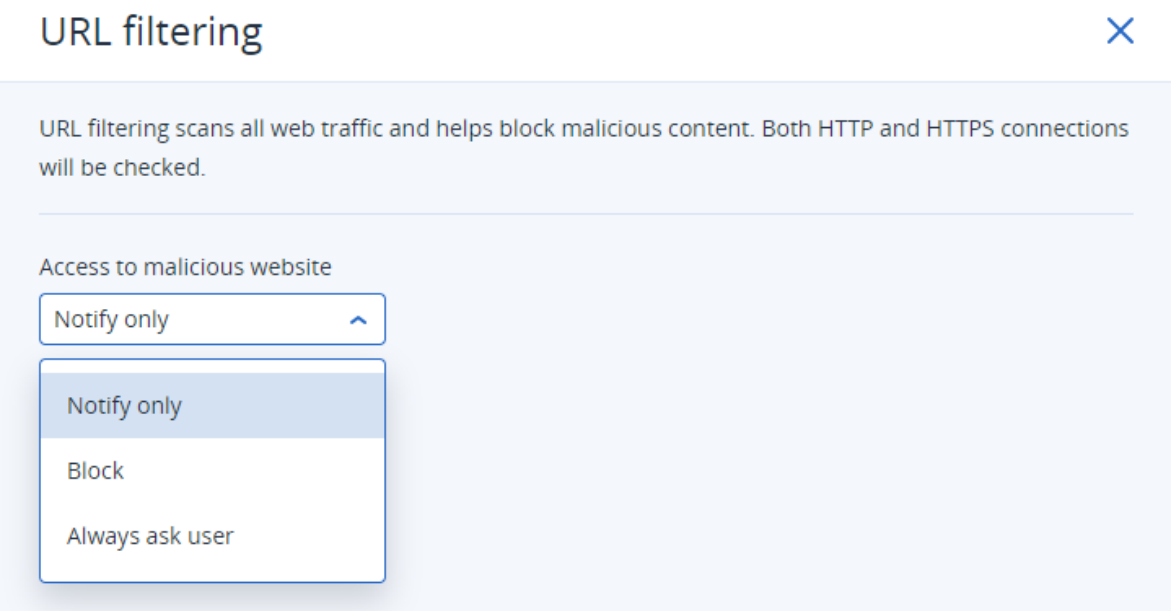
1. Dans le plan de protection pertinent, assurez-vous qu'EDR est activé. Pour plus d'informations, voir "Activation de la fonctionnalité EDR (Endpoint Detection and Response)" (p. 947).
2. Développez le module **Protection antivirus et antimalware**, puis définissez ce qui suit :
   - Cliquez sur **Active Protection**, puis dans la section **Action sur la détection**, sélectionnez **Notifier uniquement**. Cliquez ensuite sur **Terminé**. Pour plus d'informations, voir "Active Protection" (p. 866).



   - Cliquez sur **Moteur de comportement**, puis dans la section **Action lors de la détection**, sélectionnez **Notifier uniquement**. Cliquez ensuite sur **Terminé**. Pour plus d'informations, voir "Moteur de comportement" (p. 871).
   - Cliquez sur **Prévention des failles** et dans la section **Action sur la détection**, sélectionnez **Notifier uniquement**. Ensuite, cliquez sur **Terminé**. Pour plus d'informations, voir "Prévention des failles" (p. 872).

- Cliquez sur **Protection en temps réel**, et dans la section **Action sur la détection**, sélectionnez **Notifier uniquement**. Cliquez ensuite sur **Terminé**. Pour plus d'informations, voir "Protection en temps réel" (p. 874).
- Cliquez sur **Planifier l'analyse**, et dans la section **Action sur la détection**, sélectionnez **Notifier uniquement**. Cliquez ensuite sur **Terminé**. Pour plus d'informations, voir "Planifier l'analyse" (p. 875).

3. Développez le module **filtrage d'URL** et dans la liste déroulante **Accès à un site Web malveillant**, sélectionnez **Notifier uniquement**. Cliquez ensuite sur **Terminé**. Pour plus d'informations, voir "Filtrage d'URL" (p. 890).



Test du fonctionnement de la fonctionnalité EDR (Endpoint Detection and Response)

Pour vérifier si la fonctionnalité EDR est déployée et opérationnelle, vous pouvez exécuter un certain nombre de commandes qui déclenchent des détections EDR.

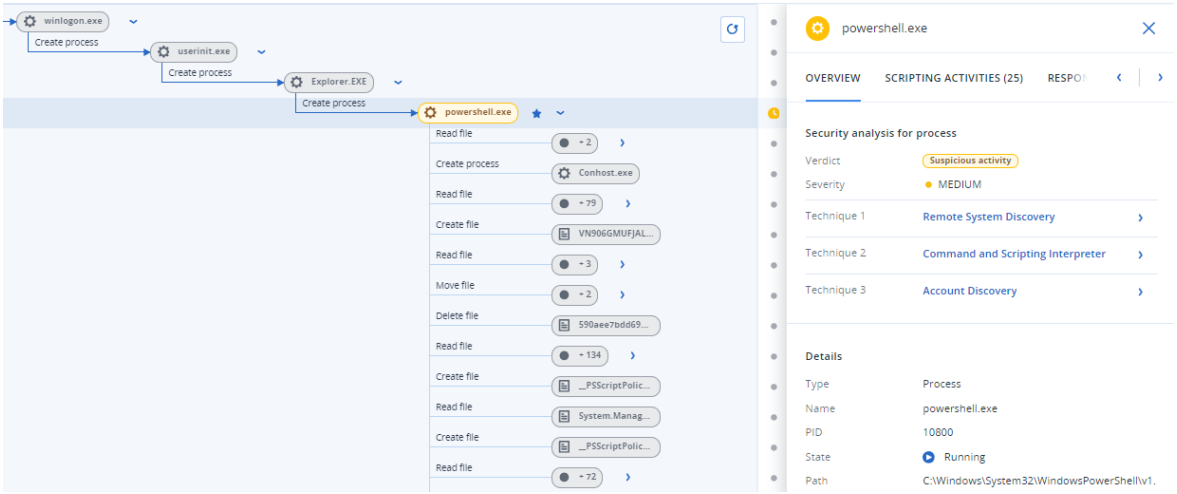
Remarque
Lorsque la fonctionnalité EDR est déployée, vous devriez constater des incidents immédiatement en cas d'activité suspecte. Les étapes ci-dessous vous permettent de vérifier si la fonctionnalité EDR est opérationnelle dans le cas où aucun nouvel incident n'a été déclenché pendant plusieurs jours.

Pour tester si la fonctionnalité EDR est déployée et fonctionne correctement

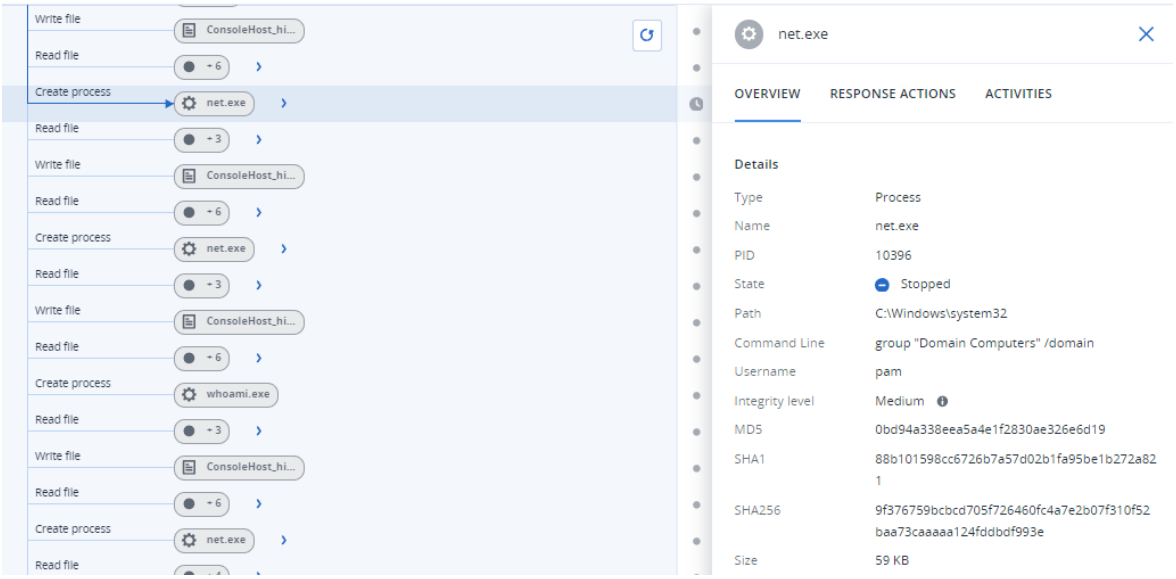
1. Connectez-vous au compte utilisateur Active Directory associé au domaine pertinent.
2. Exécutez les deux commandes suivantes dans Windows PowerShell :
   - `net group "Domain Computers" /domain`
   - `net user administrator /domain`

3. Dans la console Cyber Protect, accédez à **Protection > Incidents** pour voir l'incident généré.

   Vous pouvez également cliquer sur l'incident déclenché dont la gravité est de type **Moyen** afin de l'afficher dans la cyber kill chain EDR et vérifier les commandes PowerShell que vous avez exécutées à l'étape précédente, comme l'indique l'exemple ci-dessous.



4. Exécutez les commandes suivantes dans Windows PowerShell :
   - `c:\>whoami`
   - `c:\>net localgroup`
   - `c:\>net localgroup administrators`
   - `c:\>powershell -command start-process cmd -verb runas`
   - `c:\WINDOWS\system32>net user administrator /active:yes`
   - `c:\>powershell -command Get-Hotfix`
5. Dans la cyber kill chain EDR, cliquez sur les nœuds d'exécutables (par exemple, **net.exe** ou **whoami.exe**) pour afficher les commandes PowerShell exactes qui sont exécutées dans la ligne de commande. Ces commandes sont affichées dans la section **Détails** de l'onglet **Vue d'ensemble** dans l'exemple ci-dessous.



6. Après avoir vérifié qu'un incident EDR a été généré, définissez manuellement l'option **Statut de la menace** de l'incident sur **Atténué** et l'option **État de l'enquête** sur **Fermé**. Pour plus d'informations, voir "Comment enquêter sur des incidents dans la cyber kill chain" (p. 958). Vous pouvez également saisir un commentaire pour l'incident afin d'indiquer qu'il s'agissait d'un incident test.

Évaluation des vulnérabilités et gestion des correctifs

L'**évaluation des vulnérabilités** est un processus consistant à identifier, quantifier et classer par ordre de priorité les vulnérabilités identifiées dans le système. Dans le module d'évaluation des vulnérabilités, vous pouvez analyser vos ordinateurs à la recherche de vulnérabilités, et vérifier si les systèmes d'exploitation et les applications installées sont à jour et fonctionnent correctement.

L'analyse d'évaluation des vulnérabilités est prise en charge pour les machines exécutant les systèmes d'exploitation suivants :

- Windows. Pour plus d'informations, voir "Produits Microsoft et tiers pris en charge" (p. 1007).
- macOS. Pour plus d'informations, voir "Produits Apple et tiers pris en charge" (p. 1008).
- Ordinateurs Linux (CentOS 7/Virtuozzo/Acronis Cyber Infrastructure). Pour plus d'informations, voir "Produits Linux pris en charge" (p. 1009).

Utilisez la fonctionnalité **Gestion des correctifs** pour gérer les correctifs (mises à jour) des applications et systèmes d'exploitation installés sur vos ordinateurs, et tenir vos systèmes à jour. Dans le module Gestion des correctifs, vous pouvez approuver automatiquement ou manuellement l'installation de mises à jour sur vos ordinateurs.

La gestion des correctifs est prise en charge pour les machines exécutant les systèmes d'exploitation Windows. Pour plus d'informations, voir "Produits Microsoft et tiers pris en charge" (p. 1007).

Évaluation des vulnérabilités

Le processus d'évaluation des vulnérabilités se compose des étapes suivantes :

1. Vous créez un plan de protection avec le module d'évaluation des vulnérabilités activé, spécifiez les paramètres d'évaluation des vulnérabilités, et assignez le plan à des machines.
2. Le système, de façon planifiée ou à la demande, envoie une commande pour exécuter l'analyse d'évaluation des vulnérabilités aux agents de protection installés sur les machines.
3. Les agents reçoivent la commande, commencent à analyser les machines à la recherche de vulnérabilités, puis génèrent l'activité d'analyse.
4. Une fois l'analyse d'évaluation des vulnérabilités terminée, les agents génèrent les résultats et les envoient au service de surveillance.
5. Le service de surveillance traite les données reçues des agents et affiche les résultats dans les widgets d'évaluation des vulnérabilités et dans la liste des vulnérabilités trouvées.
6. Lorsque vous obteniez une liste des vulnérabilités trouvées, vous pouvez la traiter et décider des vulnérabilités trouvées à corriger.

Vous pouvez surveiller les résultats de l'analyse d'évaluation des vulnérabilités dans les widgets **Surveillance** > **Vue d'ensemble** > **Vulnérabilités/Vulnérabilités existantes**.

Produits Microsoft et tiers pris en charge

Les produits Microsoft et les produits tiers suivants pour les systèmes d'exploitation Windows sont pris en charge pour l'évaluation des vulnérabilités et la gestion des correctifs :

Produits Microsoft pris en charge

Système d'exploitation Windows

- Windows 7 (Entreprise, Professionnel, Intégrale)
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Système d'exploitation Windows Server

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Microsoft Office et composants connexes

- Microsoft Office 2019 (x64, x86)
- Microsoft Office 2016 (x64, x86)
- Microsoft Office 2013 (x64, x86)
- Microsoft Office 2010 (x64, x86)

Composants connexes au système d'exploitation Windows

- Internet Explorer
- Microsoft EDGE
- Windows Media Player
- .NET Framework
- Visual Studio et applications
- Composants du système d'exploitation

Applications serveur

- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019
- Microsoft SharePoint Server 2016
- Microsoft SharePoint Server 2019

Produits tiers pris en charge pour le système d'exploitation Windows

Le télétravail se répand de plus en plus à travers le monde, il devient donc important que les outils de collaboration et de communication ainsi que les clients VPN soient à jour, et qu'ils soient examinés pour détecter d'éventuelles vulnérabilités. Le service Cyber Protection prend en charge l'évaluation de la vulnérabilité et la gestion des correctifs pour ses applications.

Outils de collaboration et de communication, clients VPN

- Microsoft Teams
- Zoom
- Skype
- Slack
- Webex
- NordVPN
- TeamViewer

Pour plus d'informations sur les produits tiers pris en charge pour les systèmes d'exploitation Windows, reportez-vous à l'article List of third-party products supported by Patch Management (62853).

Produits Apple et tiers pris en charge

Les produits Apple suivants et les produits tiers pour macOS sont pris en charge pour l'évaluation des vulnérabilités :

Produits Apple pris en charge

macOS

- macOS 10.13.x et versions ultérieures

Applications macOS intégrées

- Safari, iTunes et autres.

Produits tiers pour macOS pris en charge

- Microsoft Office (Word, Excel, PowerPoint, Outlook, OneNote)
- Adobe Acrobat Reader
- Google Chrome
- Firefox
- Opera
- Zoom
- Skype
- Thunderbird
- VLC media player

Produits Linux pris en charge

Les distributions Linux suivantes sont prises en charge pour l'évaluation des vulnérabilités :

- Virtuozzo 7.x
- CentOS 7.x
- CentOS 8.x

Paramètres d'évaluation des vulnérabilités

Pour apprendre à créer un plan de protection avec le module d'évaluation des vulnérabilités, reportez-vous à la section Création d'un plan de protection. Vous pouvez effectuer une analyse d'évaluation des vulnérabilités de façon planifiée ou à la demande (à l'aide de l'action **Exécuter maintenant** d'un plan de protection).

Vous pouvez spécifier les paramètres suivants dans le module d'évaluation des vulnérabilités.

Éléments à analyser

Définir les produits logiciels que vous souhaitez analyser à la recherche de vulnérabilités :

- Ordinateurs Windows :
  - **Produits Microsoft**
  - **Produits Windows tiers** (pour plus d'informations sur les produits tiers pris en charge pour les systèmes d'exploitation Windows, reportez-vous à l'article List of third-party products supported by Patch Management (62853))

- Ordinateurs macOS :
  - **Produits Apple**
  - **Produits macOS tiers**
- Ordinateurs Linux :
  - **Analyser les packages Linux**

Planification

Définissez le planning selon lequel l'analyse d'évaluation des vulnérabilités sera effectuée sur les machines sélectionnées :

Champs	Description
Planifiez l'exécution de la tâche à l'aide des événements suivants	Ce paramètre définit le moment où la tâche sera exécutée. Les valeurs suivantes sont disponibles : • **Planifier selon l'horaire** : il s'agit du paramètre par défaut. La tâche sera exécutée selon l'horaire spécifié. • **Lorsque l'utilisateur se connecte au système** : par défaut, la connexion de n'importe quel utilisateur lancera la tâche. Vous pouvez modifier ce paramètre pour que seul un compte utilisateur spécifique déclenche la tâche. • **Lorsqu'un utilisateur se déconnecte du système** : par défaut, la déconnexion de n'importe quel utilisateur lancera la tâche. Vous pouvez modifier ce paramètre pour que seul un compte utilisateur spécifique déclenche la tâche. **Remarque** La tâche ne sera pas lancée lors d'un arrêt du système. Dans la configuration de planification, un arrêt est différent d'une déconnexion. • **Au démarrage du système** : la tâche sera exécutée au démarrage du système d'exploitation. • **À l'arrêt du système** : la tâche sera exécutée à l'arrêt du système d'exploitation.
Type de planification	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Mensuelle :** sélectionnez les mois et les semaines ou jours du mois pendant lesquels la tâche sera exécutée. • **Quotidienne** : il s'agit du paramètre par défaut. Sélectionnez les jours de la semaine au cours desquels la tâche sera exécutée.

Champs	Description
	• **Horaire :** sélectionnez les jours de la semaine, le nombre de répétitions et l'intervalle d'exécution de la tâche.
Débuter à	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants** Sélectionnez l'heure exacte à laquelle la tâche sera exécutée.
Exécuter sur une plage de date	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Configurez une plage pendant laquelle la planification configurée sera effective.
Précisez un compte utilisateur dont la connexion au système d'exploitation lancera une tâche	Ce champ apparaît si vous avez sélectionné l'option **Lorsque l'utilisateur se connecte au système** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Tout utilisateur** : utilisez cette option si vous souhaitez que la connexion de n'importe quel utilisateur déclenche la tâche. • **L'utilisateur suivant** : utilisez cette option si vous souhaitez que la connexion d'un compte utilisateur spécifique déclenche la tâche.
Précisez un compte utilisateur dont la déconnexion du système d'exploitation lancera une tâche	Ce champ apparaît si vous avez sélectionné l'option **Lorsqu'un utilisateur se déconnecte du système** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Tout utilisateur** : utilisez cette option si vous souhaitez que la déconnexion de n'importe quel utilisateur déclenche la tâche. • **L'utilisateur suivant** : utilisez cette option si vous souhaitez que la déconnexion d'un compte utilisateur spécifique déclenche la tâche.
Conditions de démarrage	Définit toutes les conditions qui doivent être remplies simultanément pour que la tâche soit exécutée. Les conditions de démarrage des analyses antimalware sont semblables aux conditions de démarrage du module **Sauvegarde** qui sont décrites dans la section Conditions de démarrage. Vous pouvez définir les conditions de démarrage suivantes : • **Répartir les heures de démarrage de tâche dans une fenêtre de temps :** cette option vous permet de définir le délai pour la tâche afin d'éviter les goulots d'étranglement au niveau du réseau. Vous pouvez indiquer le délai en heures ou minutes. Par exemple, si l'heure de démarrage par défaut est 10 h et que le délai est 60 minutes, la tâche

Champs	Description
	démarrera entre 10 h et 11 h. • **Si la machine est arrêtée, exécutez les tâches ratées lors du démarrage de la machine** • **Empêcher l'activation du mode veille ou veille prolongée lors de l'exécution de la tâche** : cette option fonctionne uniquement pour les machines sous Windows. • **Si les conditions de démarrage ne sont pas remplies, exécutez quand même la tâche au bout de :** spécifiez la période après laquelle la tâche sera lancée, quelles que soient les autres conditions de démarrage. **Remarque** Les conditions de démarrage ne sont pas prises en charge sous Linux.

Évaluation des vulnérabilités pour les machines Windows

Vous pouvez analyser les machines Windows et les produits tiers pour Windows à la recherche de vulnérabilités.

Pour configurer l'évaluation des vulnérabilités pour les machines Windows

1. Dans la console Cyber Protect, créez un plan de protection et activez le module **Évaluation des vulnérabilités**.
2. Spécifiez les paramètres d'évaluation des vulnérabilités :
   - **Éléments à analyser** : sélectionnez les **produits Microsoft**, les **produits Windows tiers**, ou les deux.
   - **Planification :** définir le calendrier de réalisation de l'évaluation des vulnérabilités.

   Pour en savoir plus sur les options de **Planification**, consultez "Paramètres d'évaluation des vulnérabilités" (p. 1009).
3. Assignez le plan aux ordinateurs Windows.

Après une analyse de l'évaluation de la vulnérabilité, vous pouvez consulter une liste des vulnérabilités trouvées. Vous pouvez traiter les informations et décider des vulnérabilités trouvées à corriger.

Pour surveiller les résultats de l'évaluation des vulnérabilités, consultez les widgets **Surveillance** > **Vue d'ensemble** > **Vulnérabilités/Vulnérabilités existantes**.

Évaluation des vulnérabilités pour les machines sous Linux

Vous pouvez analyser les machines sous Linux à la recherche de vulnérabilités au niveau des applications et des noyaux.

Pour configurer l'évaluation des vulnérabilités pour les machines sous Linux

1. Dans la console Cyber Protect, créez un plan de protection et activez le module **Évaluation des vulnérabilités**.
2. Spécifiez les paramètres d'évaluation des vulnérabilités :
   - **Éléments à analyser :** sélectionner **Analyser les packages Linux**.
   - **Planification :** définir le calendrier de réalisation de l'évaluation des vulnérabilités.

   Pour en savoir plus sur les options de **Planification**, consultez "Paramètres d'évaluation des vulnérabilités" (p. 1009).
3. Appliquez le plan aux machines Linux.

Après une analyse de l'évaluation de la vulnérabilité, vous pouvez consulter une liste des vulnérabilités trouvées. Vous pouvez traiter les informations et décider des vulnérabilités trouvées à corriger.

Pour surveiller les résultats de l'évaluation des vulnérabilités, consultez les widgets **Surveillance** > **Vue d'ensemble** > **Vulnérabilités/Vulnérabilités existantes**.

Évaluation des vulnérabilités pour les terminaux macOS

Vous pouvez analyser les terminaux macOS à la recherche de vulnérabilités au niveau du système d'exploitation et de l'application.

Pour configurer l'évaluation des vulnérabilités pour les terminaux macOS

1. Dans la console Cyber Protect, créez un plan de protection et activez le module **Évaluation des vulnérabilités**.
2. Spécifiez les paramètres d'évaluation des vulnérabilités :
   - **Éléments à analyser** : sélectionnez les **produits Apple**, les **produits macOS tiers**, ou les deux.
   - **Planification :** définir le calendrier de réalisation de l'évaluation des vulnérabilités.

   Pour en savoir plus sur les options de **Planification**, consultez "Paramètres d'évaluation des vulnérabilités" (p. 1009).
3. Appliquez le plan aux terminaux macOS.

Après une analyse de l'évaluation de la vulnérabilité, vous pouvez consulter une liste des vulnérabilités trouvées. Vous pouvez traiter les informations et décider des vulnérabilités trouvées à corriger.

Pour surveiller les résultats de l'évaluation des vulnérabilités, consultez les widgets **Surveillance** > **Vue d'ensemble** > **Vulnérabilités/Vulnérabilités existantes**.

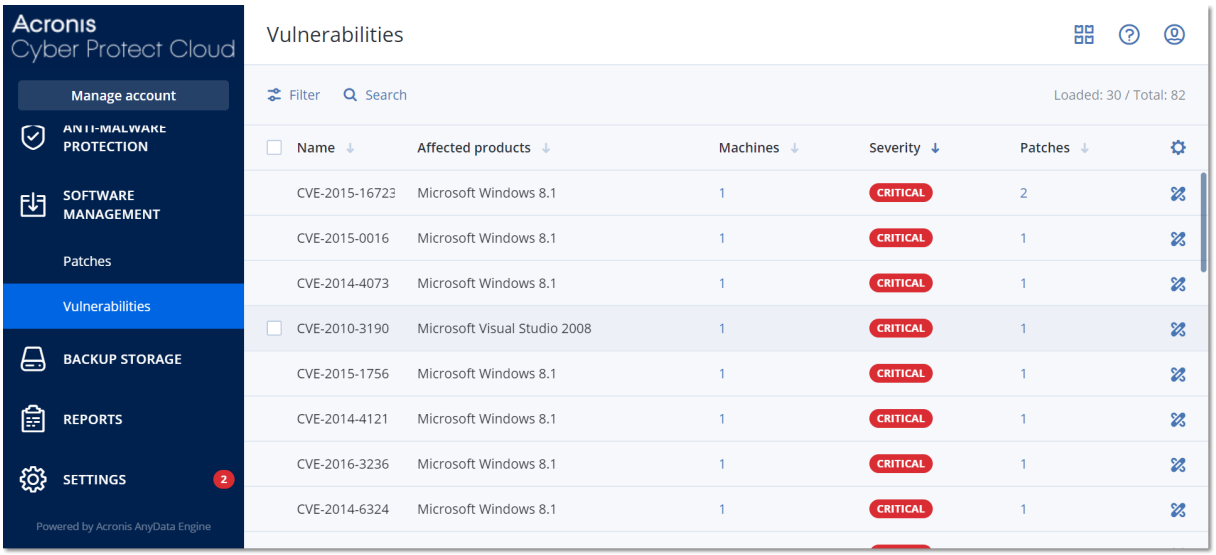
Gestion des vulnérabilités trouvées

Si l'évaluation des vulnérabilités a été effectuée au moins une fois et que des vulnérabilités ont été identifiées, vous pouvez les afficher dans **Gestion de logiciel** > **Vulnérabilités**. La liste des vulnérabilités affiche à la fois les vulnérabilités qui disposent de correctifs à installer et celles pour

lesquelles aucun correctif n'est suggéré. Vous pouvez vous servir du filtre pour afficher uniquement les vulnérabilités qui disposent d'un correctif.

Nom	Description
Nom	Le nom de la vulnérabilité.
Produits affectés	Produits logiciels pour lesquels les vulnérabilités ont été trouvées.
Machines	Le nombre de machines affectées.
La gravité	La gravité de la vulnérabilité trouvée. Les niveaux de gravité suivants peuvent être attribués, d'après le système d'évaluation des vulnérabilités (CVSS) : • **Critique** : 9 à 10 CVSS • **Élevé** : 7 à 9 CVSS • **Moyen** : 3 à 7 CVSS • **Basse** : 0 à 3 CVSS • **Aucun**
Correctifs	Le nombre de correctifs appropriés.
Publié	La date et l'heure auxquelles la vulnérabilité a été publiée dans Vulnérabilités et expositions courantes (CVE).
Détecté	La date à laquelle une vulnérabilité existante a été détectée pour la première fois sur des machines.

Vous pouvez afficher la description de la vulnérabilité trouvée en cliquant sur son nom dans la liste.



Démarrer le processus de réparation des vulnérabilités

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Vulnérabilités**.
2. Sélectionnez la vulnérabilité dans la liste, puis cliquez sur **Installer les correctifs**. L'assistant de réparation des vulnérabilités apparaît.
3. Sélectionnez les correctifs à installer sur les ordinateurs sélectionnés, puis cliquez sur **Suivant**.
4. Sélectionnez les ordinateurs sur lesquels vous souhaitez installer les correctifs.
5. Sélectionnez les options de redémarrage.
   a. Sélectionnez si vous souhaitez que l'ordinateur soit redémarré après l'installation des correctifs.

Option	Description
Non	Les ordinateurs ne seront pas redémarrés automatiquement après l'installation des correctifs.
Si nécessaire	Les ordinateurs seront redémarrés uniquement si cela est nécessaire à l'application des correctifs.
Oui	Les ordinateurs seront redémarrés automatiquement après l'installation des correctifs. Vous pouvez également spécifier un délai avant le redémarrage.

   b. [Facultatif] Si vous souhaitez retarder le redémarrage de l'ordinateur lorsqu'une sauvegarde de l'ordinateur est en cours, sélectionnez **Ne pas redémarrer avant la fin de la sauvegarde**.
6. Cliquez sur **Installer les correctifs**.

Les correctifs choisis sont alors installés sur les machines sélectionnées.

Gestion des correctifs

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Pour plus d'informations sur les produits tiers pris en charge pour les systèmes d'exploitation Windows, reportez-vous à l'article List of third-party products supported by Patch Management (62853).

Utilisez la fonctionnalité de gestion des correctifs pour :

- installer les mises à jour du système d'exploitation ou des applications
- approuver manuellement ou automatiquement les correctifs
- installer les correctifs à la demande ou de façon planifiée
- définir précisément quels correctifs installer selon différents critères : gravité, catégorie et statut d'approbation

- effectuer une sauvegarde pré mise à jour pour prévenir les éventuelles mises à jour ratées
- définir l'action de redémarrage après l'installation des correctifs

Remarque
Pour fonctionner avec les mises à jour Windows, la fonction de gestion des correctifs nécessite que les mises à jour Windows soient activées sur la ressource.

pour réduire le trafic sur la bande passante, Cyber Protection utilise une technologie de pair à pair. Vous pouvez choisir un ou plusieurs agents dédiés qui téléchargeront les mises à jour via Internet et les redistribueront à d'autres agents du réseau. Tous les agents partageront aussi leurs mises à jour avec les autres, en tant qu'agents de pair à pair.

Workflow Gestion des correctifs

Le workflow Gestion des correctifs comprend les étapes de configuration et d'application d'un plan de protection, l'exécution d'une analyse de l'évaluation des vulnérabilités, la configuration des paramètres de correctifs, l'approbation des correctifs et, enfin, l'installation de correctifs approuvés. Les étapes exactes du workflow sont les suivantes.

1. Configurez un plan de protection dont les modules **Évaluation des vulnérabilités** et **Gestion des correctifs** sont activés.
2. Configurez les paramètres d'évaluation des vulnérabilités. Pour plus d'informations sur ces paramètres, voir "Paramètres d'évaluation des vulnérabilités" (p. 1009).
3. Configurez les paramètres de gestion des correctifs. Pour plus d'informations sur ces paramètres, voir "Paramètres de gestion des correctifs dans le plan de protection" (p. 1017)
4. Appliquez le plan de protection à un ou plusieurs ordinateurs.
5. En attente de l'achèvement de l'analyse de l'évaluation des vulnérabilités. L'analyse démarre automatiquement en fonction de la planification configurée dans le plan de protection. Vous pouvez également démarrer l'analyse à la demande manuellement en cliquant sur l'icône **Exécuter maintenant** dans le module **Évaluation des vulnérabilités** dans le plan de protection.
6. Approuvez les correctifs. Vous pouvez définir les paramètres d'approbation automatique des correctifs, notamment l'installation automatique des correctifs sur les ordinateurs de test. Pour plus d'informations, voir "Approbation automatique des correctifs" (p. 1025). Vous pouvez également approuver les correctifs manuellement en définissant leur statut d'approbation sur **Approuvé**. Pour plus d'informations, voir "Approbation manuelle des correctifs" (p. 1030).
7. Installez les correctifs. Les correctifs approuvés peuvent être installés automatiquement en fonction de la planification configurée dans le plan de protection. Vous pouvez également installer les correctifs manuellement, à la demande. Pour plus d'informations, voir "Installation de correctifs à la demande" (p. 1030).

Vous pouvez surveiller les résultats de l'installation des correctifs dans le widget **Surveillance** > **Vue d'ensemble** > **Historique d'installation des correctifs**.

Paramètres de gestion des correctifs dans le plan de protection

Dans le module **Gestion des correctifs** du plan de protection, vous pouvez configurer les paramètres de gestion des correctifs suivants :

- Mises à jour à installer pour les produits Microsoft et tiers pour le système d'exploitation Windows.
- Moment d'exécution de l'installation automatique des correctifs.
- Exécution ou non d'une sauvegarde pré-mise à jour.

Pour plus d'informations sur la création d'un plan de protection et l'activation du module **Gestion des correctifs**, voir "Création d'un plan de protection" (p. 223).

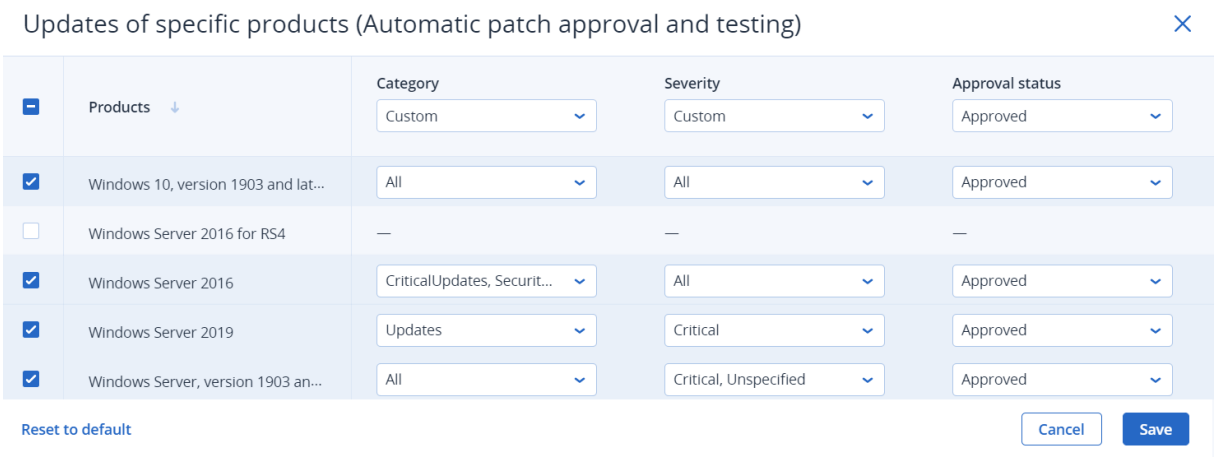
Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Produits Microsoft

Pour installer les mises à jour Microsoft sur les machines sélectionnées, activez l'option **Mettre les produits Microsoft à jour**.

Sélectionnez l'option d'installation :

Option	Description
Toutes les mises à jour	Utilisez cette option si vous souhaitez installer toutes les mises à jour approuvées.
Uniquement les mises à jour critiques et de sécurité	Utilisez cette option si vous souhaitez installer toutes les mises à jour de sécurité et critiques approuvées.
Mises à jour de produits spécifiques (approbation et test automatiques des correctifs)	Utilisez cette option si vous souhaitez définir des paramètres personnalisés pour différents produits. Si vous souhaitez mettre à jour des produits spécifiques, vous pouvez définir, pour chaque produit, les mises à jour à installer en fonction de la catégorie, de la sévérité ou du statut d'approbation. Si vous souhaitez configurer l'approbation du test automatique et le test des correctifs, sélectionnez cette option.



Pour les produits Microsoft, la distribution des correctifs utilise le service API Windows. Les correctifs et les mises à jour ne sont ni téléchargées ni stockées en interne ou sur des agents de distribution. Ils sont téléchargés depuis Microsoft CDN. Par conséquent, même si le rôle Responsable de la mise à jour lui est affecté, l'agent ne peut ni télécharger ni distribuer les correctifs.

Produits Windows tiers

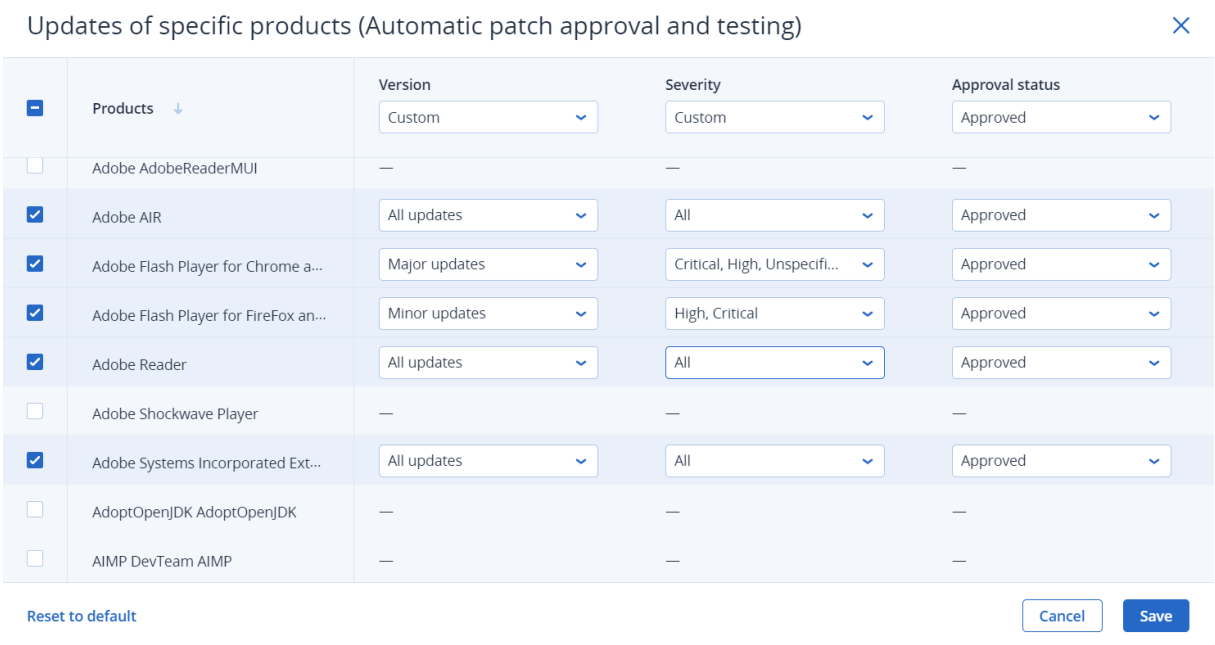
Pour installer les mises à jour tierces pour les systèmes d'exploitation Windows sur les machines sélectionnées, activez l'option **Produits Windows tiers**.

Sélectionnez les options d'installation :

Option	Description
Toutes les mises à jour	Utilisez cette option si vous souhaitez installer toutes les mises à jour approuvées. *
Mises à jour principales uniquement	Utilisez cette option si vous souhaitez installer toutes les mises à jour majeures approuvées.
Seulement des mises à jour mineures	Utilisez cette option si vous souhaitez installer des mises à jour mineures approuvées.
Mises à jour de produits spécifiques (approbation et test automatiques des correctifs)	Utilisez cette option si vous souhaitez définir des paramètres personnalisés pour différents produits. Si vous souhaitez mettre à jour des solutions spécifiques, vous pouvez définir, pour chaque solution, les mises à jour à installer en fonction de la catégorie, de la sévérité ou du statut d'approbation. Si vous souhaitez configurer l'approbation du test automatique et le test des correctifs, sélectionnez cette option.
N'installez les dernières	Cochez cette case si vous souhaitez installer les dernières

Option	Description
versions que pour les applications dont les vulnérabilités ont été détectées	mises à jour uniquement pour les applications qui ont détecté des vulnérabilités. *

* Cette option nécessite la version 23.11.36772 ou une version ultérieure de l'agent Cyber Protect.



Pour les produits tiers Windows, les correctifs sont distribués directement sur les ressources gérées depuis une base de données Acronis interne. Si le rôle Responsable de la mise à jour est affecté à un agent, ce dernier sera utilisé pour télécharger et distribuer les correctifs.

Planification

Définissez la planification selon laquelle les mises à jour seront installées sur les ordinateurs sélectionnés.

Champs	Description
Planifiez l'exécution de la tâche à l'aide des événements suivants	Ce paramètre définit le moment où la tâche sera exécutée. Les valeurs suivantes sont disponibles : • **Planifier selon l'horaire** : il s'agit du paramètre par défaut. La tâche sera exécutée selon l'horaire spécifié. • **Lorsque l'utilisateur se connecte au système** : par défaut, la connexion de n'importe quel utilisateur lancera la tâche. Vous pouvez modifier ce paramètre pour que seul un compte utilisateur spécifique déclenche la tâche. • **Lorsqu'un utilisateur se déconnecte du système** : par défaut, la

Champs	Description
	déconnexion de n'importe quel utilisateur lancera la tâche. Vous pouvez modifier ce paramètre pour que seul un compte utilisateur spécifique déclenche la tâche. **Remarque** La tâche ne sera pas lancée lors d'un arrêt du système. Dans la configuration de planification, un arrêt est différent d'une déconnexion. • **Au démarrage du système** : la tâche sera exécutée au démarrage du système d'exploitation. • **À l'arrêt du système** : la tâche sera exécutée à l'arrêt du système d'exploitation.
Type de planification	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Mensuelle :** sélectionnez les mois et les semaines ou jours du mois pendant lesquels la tâche sera exécutée. • **Quotidienne** : il s'agit du paramètre par défaut. Sélectionnez les jours de la semaine au cours desquels la tâche sera exécutée. • **Horaire :** sélectionnez les jours de la semaine, le nombre de répétitions et l'intervalle d'exécution de la tâche.
Débuter à	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants** Sélectionnez l'heure exacte à laquelle la tâche sera exécutée.
Configurer la fenêtre de maintenance des correctifs	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Sélectionnez ce paramètre si vous souhaitez que l'installation des correctifs ne s'exécute que pendant l'intervalle de temps que vous allez indiquer. Si le processus d'installation des correctifs n'est pas terminé à l'heure de fin définie par la fenêtre de maintenance des correctifs, il est arrêté automatiquement.
Exécuter sur une plage de date	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Configurez une plage pendant laquelle la planification configurée sera effective.

Champs	Description
Précisez un compte utilisateur dont la connexion au système d'exploitation lancera une tâche	Ce champ apparaît si vous avez sélectionné l'option **Lorsque l'utilisateur se connecte au système** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Tout utilisateur** : utilisez cette option si vous souhaitez que la connexion de n'importe quel utilisateur déclenche la tâche. • **L'utilisateur suivant** : utilisez cette option si vous souhaitez que la connexion d'un compte utilisateur spécifique déclenche la tâche.
Précisez un compte utilisateur dont la déconnexion du système d'exploitation lancera une tâche	Ce champ apparaît si vous avez sélectionné l'option **Lorsqu'un utilisateur se déconnecte du système** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Tout utilisateur** : utilisez cette option si vous souhaitez que la déconnexion de n'importe quel utilisateur déclenche la tâche. • **L'utilisateur suivant** : utilisez cette option si vous souhaitez que la déconnexion d'un compte utilisateur spécifique déclenche la tâche.
Conditions de démarrage	Définit toutes les conditions qui doivent être remplies simultanément pour que la tâche soit exécutée. Les conditions de démarrage des analyses antimalware sont semblables aux conditions de démarrage du module **Sauvegarde** qui sont décrites dans la section Conditions de démarrage. Vous pouvez définir les conditions de démarrage suivantes : • **Répartir les heures de démarrage de tâche dans une fenêtre de temps :** cette option vous permet de définir le délai pour la tâche afin d'éviter les goulots d'étranglement au niveau du réseau. Vous pouvez indiquer le délai en heures ou minutes. Par exemple, si l'heure de démarrage par défaut est 10 h et que le délai est 60 minutes, la tâche démarrera entre 10 h et 11 h. • **Si la machine est arrêtée, exécutez les tâches ratées lors du démarrage de la machine** • **Empêcher l'activation du mode veille ou veille prolongée lors de l'exécution de la tâche** : cette option fonctionne uniquement pour les machines sous Windows. • **Si les conditions de démarrage ne sont pas remplies, exécutez quand même la tâche au bout de :** spécifiez la période après laquelle la tâche sera lancée, quelles que soient les autres conditions de démarrage. **Remarque** Les conditions de démarrage ne sont pas prises en charge sous Linux.

Champs	Description
Redémarrage après la mise à jour	Définit si l'ordinateur doit être redémarré automatiquement après l'installation des mises à jour. Les valeurs suivantes sont disponibles : • **Jamais** : aucun redémarrage ne sera lancé après l'installation des mises à jour. • **Si nécessaire** : un redémarrage sera lancé uniquement si cela est nécessaire à l'application des mises à jour. • **Toujours** : un redémarrage sera toujours lancé après l'installation des mises à jour. Vous pouvez spécifier un délai avant le redémarrage.
Ne pas redémarrer avant la fin de la sauvegarde	Si vous sélectionnez cette option et qu'un processus de sauvegarde soit en cours d'exécution, le redémarrage de l'ordinateur sera retardé jusqu'à la fin de la sauvegarde.

Sauvegarde pré-mise à jour

Exécutez la sauvegarde avant d'installer les mises à jour du logiciel : le système créera une sauvegarde incrémentielle de la machine avant d'y installer des mises à jour. Si aucune sauvegarde n'avait été créée avant, une sauvegarde complète de la machine sera alors créée. Cela vous permet de prévenir les situations dans lesquelles l'installation des mises à jour a échoué et où vous devez revenir à un état précédent. Pour que l'option **Sauvegarde pré-mise à jour** fonctionne, le module de gestion des correctifs et le module de sauvegarde doivent tous les deux être activés sur les machines correspondantes au sein d'un plan de protection, et les éléments à sauvegarder doivent être la machine entière ou les volumes systèmes et les volumes de démarrage. Si vous sélectionnez des éléments inappropriés à sauvegarder, le système ne vous autorisera alors pas à activer l'option **Sauvegarde pré-mise à jour**.

Affichage de la liste des correctifs disponibles

Une fois l'analyse de l'évaluation des vulnérabilités effectuée, vous trouverez les informations sur les correctifs disponibles dans **Gestion de logiciel** > **Correctifs**.

Pour afficher les détails d'un correctif spécifique, cliquez dans la liste sur le correctif correspondant.

Le tableau suivant décrit les informations concernant le correctif affiché à l'écran.

Champs	Description
Statut d'approbation	Le statut d'approbation est principalement nécessaire pour les scénarios d'approbation automatique. Vous pouvez définir l'un des statuts suivants pour un correctif : • **Approuvé :** le correctif a été installé sur au moins une machine et a été validé. • **Refusé :** le correctif n'est pas sûr et peut corrompre le système d'une machine.

	• **En attente d'approbation** : le statut du correctif n'est pas clair et doit être validé
Contrat de licence	• Accepté • Refusé. Si vous refusez le contrat de licence, le statut du correctif devient **Refusé** et le correctif ne sera pas installé.
La gravité	La gravité du correctif : • **Critique** • **Élevée** • **Moyenne** • **Basse** • **Aucun**
Fournisseur	Le fournisseur du correctif.
Produit affecté	Le produit auquel s'applique le correctif.
Versions installées	Les versions du produit qui sont déjà installées.
Version	La version du correctif.
Catégorie	La catégorie à laquelle le correctif appartient : • **Mise à jour critique :** correctifs largement diffusés pour des problèmes spécifiques, afin de régler des problèmes critiques et non liés à la sécurité. • **Mise à jour de sécurité :** correctifs largement diffusés pour des produits spécifiques, pour régler des problèmes en lien avec la sécurité. • **Mise à jour de définition :** mise à jour des fichiers de définition de virus ou d'autres fichiers de définition. • **Mise à jour cumulative :** ensemble cumulatif de correctifs, de mises à jour de sécurité, de mises à jour critiques et de mises à jour, rassemblés pour un déploiement aisé. Une mise à jour cumulative cible généralement un domaine spécifique, comme la sécurité, ou un composant spécifique, comme Internet Information Services (IIS). • **Service pack** ensemble cumulatif de tous les correctifs et de toutes les mises à jour de sécurité, mises à jour critiques et mises à jour créées depuis la sortie du produit. Les Service Pack peuvent aussi contenir un nombre limité de fonctionnalités ou de changements de conception demandés par les clients. • **Outil :** utilitaires ou fonctionnalités aidant à accomplir une tâche ou un ensemble de tâches. • **Feature pack :** nouvelles fonctionnalités, généralement intégrées aux produits dans leur prochaine version. • **Mise à jour :** correctifs largement diffusés pour des produits spécifiques, pour régler des problèmes non critiques et non liés à la sécurité. • **Application** : correctifs pour une application.
Date de	La date à laquelle le correctif a été publié.

publication	
Date du dernier rapport	La date du dernier signalement du correctif
Date de la première installation	La date de la première installation réussie du correctif sur un ordinateur
Base de connaissances Microsoft	Si le correctif concerne un produit Microsoft, le champ indique l'identifiant de l'article de la base de connaissances
Machines	Le nombre de machines affectées.
Vulnérabilités	Le nombre de vulnérabilités. Si vous cliquez dessus, vous serez redirigé vers la liste des vulnérabilités.
Taille	La taille moyenne du correctif
Langue	La langue prise en charge par le correctif.
Site du fournisseur	Le site officiel du correctif.

Configuration de la durée de vie des correctifs dans la liste

Vous pouvez tenir à jour la liste des correctifs en configurant la durée de vie des correctifs dans la liste disponible dans l'écran **Correctifs**. Ce paramètre définit la durée pendant laquelle le correctif disponible détecté sera visible dans la liste des correctifs. Le correctif sera supprimé de la liste une fois qu'il sera correctement installé sur tous les ordinateurs sur lesquels il a été indiqué comme manquant ou une fois la durée de vie dans la liste écoulée.

Pour configurer la durée de vie des correctifs dans la liste

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Correctifs**.
2. Cliquez sur **Paramètres**.
3. Dans **Durée de vie dans la liste** sélectionnez l'option appropriée.

Option	Description
Toujours	Le correctif reste toujours dans la liste.
7 jours	Le correctif sera supprimé de la liste sept jours après sa première installation. Par exemple, considérons que vous disposez de deux ordinateurs sur lesquels des correctifs doivent être installés. L'un d'eux est en ligne, et l'autre est hors ligne. Le correctif a d'abord été installé sur la première machine. Après 7 jours, le correctif sera retiré de la liste des correctifs, même s'il n'a pas été installé sur le deuxième ordinateur (car il était hors ligne).
30 jours	Le correctif est supprimé de la liste 30 jours après sa première installation.

Approbation automatique des correctifs

L'approbation automatique des correctifs facilite le processus d'installation des mises à jour sur les ordinateurs. Grâce à l'approbation automatique des correctifs, l'installation des correctifs n'est pas retardée par le processus d'approbation manuelle des correctifs. Les mises à jour et correctifs importants sont installés plus rapidement, ce qui améliore la fiabilité de votre système.

Vous pouvez utiliser l'approbation automatique des correctifs dans les scénarios test pour l'installation automatique des correctifs. Si les correctifs sont installés avec succès sur les ordinateurs de test, les correctifs seront installés automatiquement sur les ordinateurs de production également. Pour plus d'informations sur ce scénario, voir "Cas d'utilisation de l'approbation et du test automatiques des correctifs" (p. 1026).

Vous pouvez également utiliser l'approbation automatique des correctifs dans les scénarios d'installation automatique de correctifs dans votre environnement de production, et ignorer la phase de test. Pour plus d'informations sur ce scénario, voir "Cas d'utilisation d'approbation automatique des correctifs sans test" (p. 1029).

Configuration de l'approbation automatique des correctifs

Vous pouvez configurer l'approbation automatique des correctifs et vous assurer que l'installation des correctifs n'est pas retardée par le processus d'approbation manuelle des correctifs.

Configurer l'approbation automatique des correctifs

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Correctifs**.
2. Cliquez sur **Paramètres**.
3. Activez **Approbation automatique des correctifs**.
4. Configurez les paramètres d'approbation automatique des correctifs.

a. Sélectionnez l'option Approbation automatique des correctifs.

Option	Description
Approbation et test automatiques des correctifs	Le statut d'approbation du correctif passera à **Approuvé** lorsque le nombre de jours sélectionnés sera écoulé après l'installation réussie du correctif. Nous vous recommandons d'utiliser ce paramètre si vous souhaitez tester les correctifs en les installant d'abord sur un ordinateur de test, de vérifier que tout fonctionne comme prévu, puis d'installer les correctifs dans votre environnement de production.
Approbation automatique des correctifs sans test	Le statut d'approbation du correctif passera à **Approuvé** lorsque le nombre de jours sélectionnés sera écoulé après la détection du correctif.

b. Sélectionnez le nombre de jours qui doivent s'écouler une fois que la condition de l'option Approbation automatique des correctifs est satisfaite. Après cette période, le statut d'approbation des correctifs passe automatiquement de **En attente d'approbation** à **Approuvé**.

5. Sélectionnez **Acceptez automatiquement les contrats de licence**.
6. Cliquez sur **Appliquer**.

Cas d'utilisation de l'approbation et du test automatiques des correctifs

Si vous souhaitez tester les derniers correctifs sur un ordinateur de test avant de les installer sur vos ordinateurs de production, vous pouvez configurer deux plans de protection : un plan pour l'installation de correctifs à des fins de test et un plan pour l'installation de correctifs testés sur les ordinateurs de production. Par conséquent, vous vous assurerez que les correctifs que vous installez dans votre environnement de production sont sécurisés et que vos ordinateurs de production fonctionnent correctement après l'installation de ces correctifs.

Le cas d'utilisation est constitué des étapes suivantes :

1. Configurez les paramètres d'approbation automatique des correctifs. Sélectionnez l'option **Approbation et test automatiques des correctifs**. Pour plus d'informations, voir "Configuration de l'approbation automatique des correctifs" (p. 1025).
2. Configurez un plan de protection à des fins de test (par exemple, Correctifs Test) avec le module **Gestion des correctifs** activé, puis appliquez-le aux ordinateurs dans l'environnement de test. Spécifiez la condition d'installation de correctif suivante : le statut d'approbation du correctif doit être **En attente d'approbation**. Cette étape est nécessaire pour valider les correctifs et vérifier si les machines fonctionnent correctement après l'installation des correctifs. Pour plus d'informations, voir "Configuration du plan de protection Correctifs Test" (p. 1027).
3. Configurez un plan de protection pour l'environnement de production (par exemple, Correctifs Production) avec le module **Gestion des correctifs** activé, puis appliquez-le aux ordinateurs dans l'environnement de production. Spécifiez la condition d'installation de correctif suivante : le

statut d'approbation du correctif doit être **Approuvé**. Pour plus d'informations, voir "Configuration du plan de protection Correctifs Production" (p. 1028).

4. Exécutez le plan « Correctifs Test » et vérifiez les résultats. Conservez le statut d'approbation **En attente d'approbation** des ordinateurs ne présentant aucun problème, mais modifier en **Refusé** celui des ordinateurs qui ne fonctionnent pas correctement. En fonction du nombre de jours défini dans le paramètre **Approbation automatique des correctifs**, le statut d'approbation des correctifs passe automatiquement de **En attente d'approbation** à **Approuvé**. Lorsque vous exécutez le plan Correctifs Production, seuls les correctifs ayant le statut **Approuvé** seront installés sur les ordinateurs de production. Pour plus d'informations, voir "Exécution du plan de protection Correctifs Test et refus des correctifs non sécurisés" (p. 1029).
5. Exécutez le plan Correctifs Production.

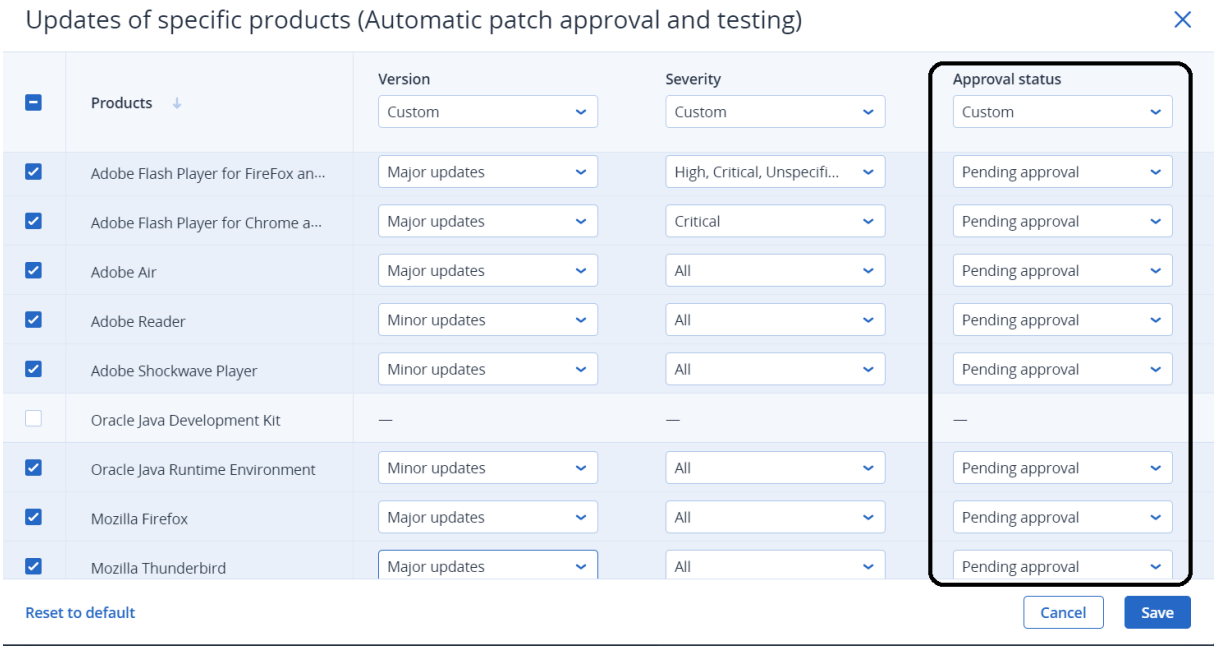
Configuration du plan de protection Correctifs Test

Vous pouvez configurer un plan de protection avec les paramètres d'installation des correctifs de vos ordinateurs dans l'environnement de test.

Pour configurer le plan de protection Correctifs Test

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Cliquez sur **Création d'un plan**.
3. Activez le module **Gestion des correctifs**.
4. Définissez les mises à jour à installer pour les produits Microsoft et tiers, le planning, et la sauvegarde pré mise à jour. Pour plus d'informations sur ces paramètres, voir "Paramètres de gestion des correctifs dans le plan de protection" (p. 1017).

Important
Pour tous les produits à mettre à jour, sélectionnez le statut d'approbation sur **En attente d'approbation**. Ainsi, l'agent installera uniquement les correctifs dont le statut est **En attente d'approbation** sur les ordinateurs sélectionnés dans l'environnement de test.



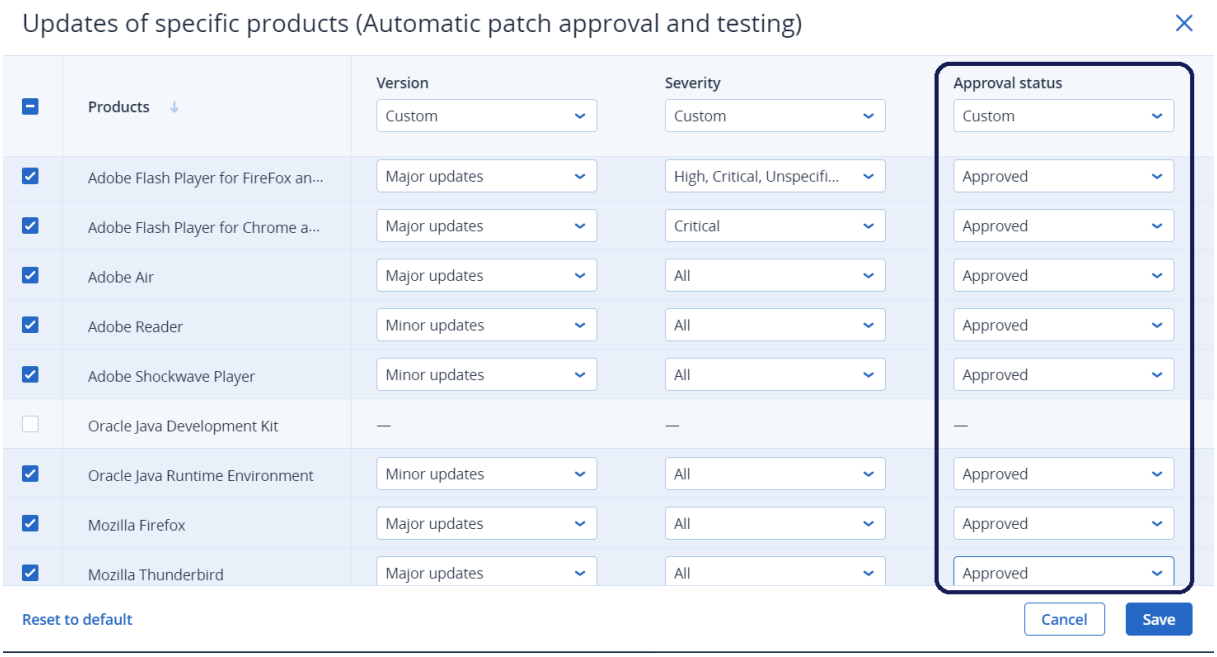
Configuration du plan de protection Correctifs Production

Vous pouvez configurer un plan de protection avec les paramètres d'installation des correctifs de votre ordinateur dans l'environnement de production.

Pour configurer le plan de protection Correctifs Production

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Cliquez sur **Création d'un plan**.
3. Activez le module **Gestion des correctifs**.
4. Définissez les mises à jour à installer pour les produits Microsoft et tiers, le planning, et la sauvegarde pré mise à jour. Pour plus d'informations sur ces paramètres, voir "Paramètres de gestion des correctifs dans le plan de protection" (p. 1017).

   Important
   Pour tous les produits à mettre à jour, définissez le **statut d'approbation** sur **Approuvé**. Ainsi, l'agent installera uniquement les correctifs dont le statut est **Approuvé** sur les ordinateurs sélectionnés dans l'environnement de production.



Exécution du plan de protection Correctifs Test et refus des correctifs non sécurisés

Après l'installation des correctifs sur les ordinateurs de votre environnement de test, vous pouvez vérifier si tout fonctionne correctement. Vous pouvez conserver le statut d'approbation **En attente d'approbation** des ordinateurs ne présentant aucun problème, mais modifier en **Refusé** celui des ordinateurs qui ne fonctionnent pas correctement.

Pour exécuter le plan de protection Correctifs Test et refuser les correctifs non sécurisés

1. Exécutez le plan de protection Correctifs Test (de façon planifiée ou manuellement).
2. Selon le résultat, déterminez les correctifs installés qui sont sûrs.
3. Accédez à **Gestion de logiciel** > **Correctifs** et définissez le **statut d'approbation** sur **Refusé** pour les correctifs qui ne sont pas sûrs.

Cas d'utilisation d'approbation automatique des correctifs sans test

Si vous souhaitez installer automatiquement de nouveaux correctifs sur vos ordinateurs de production dans les meilleurs délais, sans les installer d'abord sur les ordinateurs de test, vous pouvez configurer un seul plan de protection.

Le cas d'utilisation est constitué des étapes suivantes :

1. Configurez les paramètres d'approbation automatique des correctifs. Sélectionnez l'option **Approbation automatique des correctifs sans test**. Pour plus d'informations, voir "Configuration de l'approbation automatique des correctifs" (p. 1025).
2. Configurez un plan de protection pour l'environnement de production (par exemple, Correctifs Production) avec le module **Gestion des correctifs** activé, puis appliquez-le aux ordinateurs dans l'environnement de production. Spécifiez la condition d'installation de correctif suivante : le

statut d'approbation du correctif doit être **Approuvé**. Pour plus d'informations, voir "Configuration du plan de protection Correctifs Production" (p. 1028).

3. Exécutez le plan Correctifs Production.

Approbation manuelle des correctifs

Vous pouvez approuver un correctif manuellement et accélérer son installation en ignorant la phase de test.

Prérequis

- Un plan de protection dont le module **Gestion des correctifs** est activé est appliqué à un ordinateur Windows au moins.
- Des correctifs ne sont pas encore installés sur le ou les ordinateurs sur lesquels le plan de protection est appliqué.

Pour approuver manuellement des correctifs

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Correctifs**.
2. Sélectionnez les correctifs que vous souhaitez installer, puis acceptez les contrats de licence.
3. Définissez le **statut d'approbation** des correctifs sur **Approuvé**.
   Le statut d'approbation des correctifs est défini sur **Approuvé**. Les correctifs seront installés automatiquement sur les ordinateurs en fonction de la planification définie dans le plan de protection. Si vous souhaitez installer les correctifs immédiatement, suivez the procédure décrite dans "Installation de correctifs à la demande" (p. 1030).

Installation de correctifs à la demande

Vous pouvez installer les correctifs manuellement, à la demande, si vous ne souhaitez pas attendre l'heure d'installation planifiée.

Vous pouvez démarrer l'installation manuelle des correctifs à partir de trois écrans : **Correctifs**, **Vulnérabilités** et **Tous les terminaux**.

Pour installer manuellement un correctif

À partir de correctifs

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Correctifs**.
2. Acceptez le contrat de licence des correctifs que vous souhaitez installer.
3. Dans l'assistant **Installer les correctifs**, sélectionnez les correctifs que vous souhaitez installer, puis cliquez sur **Installer**.
4. Sélectionnez les ordinateurs sur lesquels vous souhaitez installer les correctifs.
5. Sélectionnez les options de redémarrage.
   a. Sélectionnez si vous souhaitez que l'ordinateur soit redémarré après l'installation des correctifs.

Option	Description
Non	Les ordinateurs ne seront pas redémarrés automatiquement après l'installation des correctifs.
Si nécessaire	Les ordinateurs seront redémarrés uniquement si cela est nécessaire à l'application des correctifs.
Oui	Les ordinateurs seront redémarrés automatiquement après l'installation des correctifs. Vous pouvez également spécifier un délai avant le redémarrage.

b. [Facultatif] Si vous souhaitez retarder le redémarrage de l'ordinateur lorsqu'une sauvegarde de l'ordinateur est en cours, sélectionnez **Ne pas redémarrer avant la fin de la sauvegarde**.

6. Cliquez sur **Installer les correctifs**.

À partir de vulnérabilités

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Vulnérabilités**.
2. Effectuez le processus de réparation tel que décrit dans "Gestion des vulnérabilités trouvées" (p. 1013).

À partir de tous les terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez l'ordinateur sur lequel vous souhaitez installer les correctifs.
3. Cliquez sur **Correctif**.
4. Sélectionnez les correctifs que vous souhaitez installer, puis cliquez sur **Suivant**.
5. Sélectionnez les options de redémarrage.
   a. Sélectionnez si vous souhaitez que l'ordinateur soit redémarré après l'installation des correctifs.

Option	Description
Non	Les ordinateurs ne seront pas redémarrés automatiquement après l'installation des correctifs.
Si nécessaire	Les ordinateurs seront redémarrés uniquement si cela est nécessaire à l'application des correctifs.
Oui	Les ordinateurs seront redémarrés automatiquement après l'installation des correctifs. Vous pouvez également spécifier un délai avant le redémarrage.

   b. [Facultatif] Si vous souhaitez retarder le redémarrage de l'ordinateur lorsqu'une sauvegarde de l'ordinateur est en cours, sélectionnez **Ne pas redémarrer avant la fin de la**

sauvegarde.

6. Cliquez sur **Installer les correctifs**.

Gestion de votre inventaire logiciel et matériel

Inventaire du logiciel

La fonctionnalité d'inventaire du logiciel est disponible pour les terminaux sur lesquels le pack Advanced est activé, ou qui possèdent l'(ancienne) licence Cyber Protect. Cette fonctionnalité vous permet d'afficher toutes les applications logicielles installées sur tous les terminaux Windows et macOS.

Pour obtenir les données d'inventaire du logiciel, vous pouvez exécuter des analyses automatiques ou manuelles sur les terminaux.

Vous pouvez utiliser les données d'inventaire du logiciel pour :

- rechercher et comparer les informations concernant toutes les applications installées sur les terminaux de l'entreprise ;
- déterminer si une application doit être mise à jour ;
- déterminer si une application inutilisée doit être supprimée ;
- vérifier que la version du logiciel est la même sur différents terminaux de l'entreprise ;
- surveiller les modifications du statut du logiciel entre des analyses consécutives.

Activation de l'analyse de l'inventaire du logiciel

Lorsque l'analyse de l'inventaire du logiciel est activée sur les terminaux, le système collecte automatiquement les données du logiciel toutes les 12 heures.

La fonctionnalité d'analyse de l'inventaire du logiciel est activée par défaut pour tous les terminaux qui possèdent la licence requise, mais vous pouvez modifier le paramètre si nécessaire.

Remarque
Les tenants du client peuvent activer ou désactiver l'analyse de l'inventaire du logiciel. Les tenants d'unités peuvent consulter les paramètres d'analyse de l'inventaire du logiciel, mais ils ne peuvent pas les modifier.

Pour activer l'analyse de l'inventaire du logiciel

1. Dans la console Cyber Protect, accédez à **Paramètres**.
2. Cliquez sur **Protection**.
3. Cliquez sur **Analyse de l'inventaire**.
4. Activez le module **Analyse de l'inventaire du logiciel** en cliquant sur le commutateur à côté du nom du module.

Pour désactiver l'analyse de l'inventaire du logiciel

1. Dans la console Cyber Protect, accédez à **Paramètres**.
2. Cliquez sur **Protection**.
3. Cliquez sur **Analyse de l'inventaire**.
4. Désactivez le module **Analyse de l'inventaire du logiciel** en cliquant sur le commutateur à côté du nom du module.

Exécution d'une analyse manuelle d'inventaire du logiciel

Vous pouvez exécuter manuellement une analyse d'inventaire du logiciel dans l'écran **Inventaire du logiciel** ou depuis l'onglet **Logiciel** de l'écran **Inventaire**.

Prérequis

- Le terminal utilise le système d'exploitation Windows ou macOS.
- Le terminal possède l'(ancienne) licence Cyber Protect requise ou a activé le pack Advanced Management.

Pour exécuter une analyse d'inventaire du logiciel dans l'écran Inventaire du logiciel

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel**.
2. Cliquez sur **Inventaire du logiciel**.
3. Dans le champ à liste déroulante **Regrouper par :**, sélectionnez **Terminaux**.
4. Recherchez le terminal que vous souhaitez analyser, puis cliquez sur **Analyser maintenant**.

Pour exécuter une analyse d'inventaire du logiciel dans l'onglet Logiciel de l'écran Inventaire

1. Dans la console Cyber Protect, accédez à **Terminaux**.
2. Cliquez sur le terminal que vous souhaitez analyser, puis sur **Inventaire**.
3. Dans l'onglet **Logiciel**, cliquez sur **Analyser maintenant**.

Navigation dans l'inventaire du logiciel

Vous pouvez afficher et rechercher les données de toutes les applications logicielles disponibles sur tous les terminaux de l'entreprise.

Prérequis

- Les terminaux utilisent le système d'exploitation Windows ou macOS.
- Les terminaux possèdent l'(ancienne) licence Cyber Protect requise ou ont activé le pack Advanced Management.
- L'analyse de l'inventaire du logiciel sur les terminaux s'est déroulée correctement.

Pour afficher toutes les applications logicielles disponibles sur tous les terminaux Windows et macOS de l'entreprise

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel**.
2. Cliquez sur **Inventaire du logiciel**.

   Par défaut, les données sont regroupées par terminal. Le tableau suivant décrit les données visibles dans l'écran **Inventaire du logiciel**.

Colonne	Description
Nom	Nom de l'application.
Version	Version de l'application.
Statut	Statut de l'application. • **Nouvelle**. • **Mise à jour**. • **Supprimée**. • **Aucun changement**.
Fournisseur	Fournisseur de l'application.
Date d'installation	Date et heure d'installation de l'application.
Dernière exécution	Réservé aux terminaux macOS. Date et heure de la dernière activité de l'application.
Emplacement	Répertoire d'installation de l'application.
Utilisateur	Utilisateur qui a installé l'application.
Type de système	Réservé aux terminaux Windows. Type binaire de l'application. • **X86** pour les applications 32 bits. • **X64** pour les applications 64 bits.

3. Pour regrouper les données par application, sélectionnez dans le champ à liste déroulante **Regrouper par :** l'option **Applications**.
4. Pour réduire la quantité d'informations affichées, utilisez un ou plusieurs filtres.
   a. Cliquez sur **Filtre**.
   b. Sélectionnez un ou plusieurs filtres.

      Le tableau suivant décrit les filtres de l'écran **Inventaire du logiciel**.

Filtre	Description
Nom du terminal	Nom du terminal. Il est possible de sélectionner plusieurs éléments. Utilisez ce filtre si vous souhaitez comparer le logiciel de terminaux spécifiques.
Application	Nom de l'application. Il est possible de sélectionner plusieurs éléments. Utilisez ce filtre si vous souhaitez comparer les données d'une application spécifique sur

Filtre	Description
	des terminaux spécifiques ou sur tous les terminaux.
Fournisseur	Fournisseur de l'application. Il est possible de sélectionner plusieurs éléments. Utilisez ce filtre si vous souhaitez afficher toutes les applications d'un fournisseur spécifique sur des terminaux spécifiques ou sur tous les terminaux.
Statut	Statut de l'application. Il est possible de sélectionner plusieurs éléments. Utilisez ce filtre si vous souhaitez afficher toutes les applications ayant le statut sélectionné sur des terminaux spécifiques ou sur tous les terminaux.
Date d'installation	Date d'installation de l'application. Utilisez ce filtre si vous souhaitez afficher toutes les applications installées à une date spécifique sur des terminaux spécifiques ou sur tous les terminaux.
Date de l'analyse	Date d'analyse de l'inventaire du logiciel. Utilisez ce filtre si vous souhaitez afficher les informations concernant le logiciel sur des terminaux spécifiques ou sur tous les terminaux analysés à cette date.

c. Cliquez sur **Appliquer**.

5. Pour parcourir toute la liste d'inventaire du logiciel, utilisez la pagination en bas à gauche de l'écran.

- Cliquez sur le numéro de la page à ouvrir.
- Dans le champ à liste déroulante, sélectionnez le numéro de la page à ouvrir.

Affichage de l'inventaire du logiciel d'un seul terminal

Vous pouvez afficher la liste de toutes les applications logicielles installées sur un seul terminal, ainsi que les informations détaillées concernant les applications, notamment le statut, la version, le fournisseur, la date d'installation, la dernière exécution et l'emplacement.

Prérequis

- Le terminal utilise le système d'exploitation Windows ou macOS.
- Le terminal possède l'(ancienne) licence Cyber Protect requise ou a activé le pack Advanced Management.
- L'analyse de l'inventaire du logiciel sur le terminal s'est déroulée correctement.

Pour afficher l'inventaire du logiciel d'un seul terminal depuis l'écran Inventaire du logiciel

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel**.
2. Cliquez sur **Inventaire du logiciel**.
3. Dans le champ à liste déroulante **Regrouper par :**, sélectionnez **Terminaux**.
4. Recherchez le terminal que vous souhaitez inspecter à l'aide de l'une des options suivantes.
   - Recherchez le terminal à l'aide de l'option **Filtre** :
     a. Cliquez sur **Filtre**.
     b. Dans le champ **Nom du terminal**, sélectionnez le nom du terminal à afficher.
     c. Cliquez sur **Appliquer**.
   - Recherchez le terminal à l'aide de l'option dynamique **Recherche** :
     a. Cliquez sur **Rechercher**.
     b. Saisissez une partie ou l'intégralité du nom du terminal.

Pour afficher l'inventaire du logiciel d'un seul terminal depuis l'écran Terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux**.
2. Cliquez sur le terminal que vous souhaitez afficher, puis sur **Inventaire**.
3. Cliquez sur l'onglet **Logiciel**.

Inventaire matériel

La fonctionnalité d'inventaire du matériel vous permet d'afficher tous les composants matériels disponibles sur :

- les terminaux Windows ou macOS physiques qui possèdent une licence prenant en charge la fonctionnalité « Inventaire du matériel ».
- les machines Windows et macOS fonctionnant sur les plates-formes de virtualisation suivantes : VMware, Hyper-V, Citrix, Parallels, Oracle, Nutanix, Virtuozzo et Virtuozzo Hybrid Infrastructure. Pour en savoir plus sur les versions des plates-formes de virtualisation prises en charge, consultez "Plates-formes de virtualisation prises en charge" (p. 32).

Remarque
La fonctionnalité « Inventaire du matériel » pour les machines virtuelles n'est pas prise en charge dans les anciennes éditions de Cyber Protect.

La fonctionnalité d'inventaire du matériel n'est prise en charge que pour les terminaux sur lesquels un agent de protection est installé.

Pour obtenir les données d'inventaire du matériel, vous pouvez exécuter des analyses automatiques ou manuelles sur le terminal.

Vous pouvez utiliser les données d'inventaire du matériel pour :

- découvrir toutes les ressources matérielles de l'organisation ;
- parcourir l'inventaire du matériel de tous les terminaux de votre organisation ;
- comparer les composants matériels sur plusieurs terminaux de l'entreprise ;
- afficher les informations détaillées concernant le composant matériel.

Activation de l'analyse de l'inventaire du matériel

Lorsque l'analyse de l'inventaire du matériel est activée sur les terminaux physiques et les machines virtuelles, le système collecte automatiquement les données du matériel toutes les 12 heures.

La fonctionnalité d'analyse de l'inventaire du matériel est activée par défaut, mais vous pouvez modifier le paramètre si nécessaire.

Remarque
Les tenants du client peuvent activer ou désactiver l'analyse de l'inventaire du matériel. Les tenants d'unités peuvent consulter les paramètres d'analyse de l'inventaire du matériel, mais ils ne peuvent pas les modifier.

Pour activer l'analyse de l'inventaire du matériel

1. Dans la console Cyber Protect, accédez à **Paramètres**.
2. Cliquez sur **Protection**.
3. Cliquez sur **Analyse de l'inventaire**.
4. Activez le module **Analyse de l'inventaire du matériel** en cliquant sur le commutateur à côté du nom du module.

Pour désactiver l'analyse de l'inventaire du matériel

1. Dans la console Cyber Protect, accédez à **Paramètres**.
2. Cliquez sur **Protection**.
3. Cliquez sur **Analyse de l'inventaire**.
4. Désactivez le module **Analyse de l'inventaire du matériel** en cliquant sur le commutateur à côté du nom du module.

Exécution d'une analyse manuelle d'inventaire du matériel

Vous pouvez exécuter manuellement une analyse de l'inventaire du matériel pour un seul terminal et afficher les données actuelles des composants matériels du terminal.

Remarque
L'analyse de l'inventaire du matériel des machines virtuelles n'est prise en charge que lorsque la date et l'heure actuelles de la machine virtuelle correspondent à la date et l'heure actuelle en UTC. Afin de vérifier que la machine virtuelle utilise les paramètres de date et d'heure corrects, désactivez l'option **Synchronisation date/heure** de la machine virtuelle, définissez la date, l'heure et le fuseau horaire actuels, puis redémarrez **Acronis Agent Core Service** et le **service de machine gérée Acronis**.

Prérequis

- (Pour tous les terminaux) Le terminal utilise un système d'exploitation Windows ou macOS.
- (Pour tous les terminaux) Les terminaux possèdent une licence qui prend en charge la fonctionnalité « Inventaire du matériel ». Notez que la fonctionnalité « Inventaire du matériel » pour les machines virtuelles n'est pas prise en charge dans les (anciennes) éditions de Cyber Protect.
- (Pour tous les terminaux) Un agent de protection est installé sur le terminal.
- (Pour les machines virtuelles) La machine utilise l'une des plates-formes de virtualisation prises en charge. Pour plus d'informations, voir "Inventaire matériel" (p. 1037).

Pour exécuter l'analyse de l'inventaire du matériel sur un seul terminal

1. Dans la console Cyber Protect, accédez à **Terminaux**.
2. Cliquez sur le terminal que vous souhaitez analyser, puis sur **Inventaire**.
3. Dans l'onglet **Matériel**, cliquez sur **Analyser maintenant**.

Navigation dans l'inventaire du matériel

Vous pouvez afficher et rechercher les données de tous les composants matériels disponibles sur tous les terminaux de l'entreprise.

Prérequis

- (Pour tous les terminaux) Les terminaux utilisent le système d'exploitation Windows ou macOS.
- (Pour tous les terminaux) Les terminaux possèdent une licence qui prend en charge la fonctionnalité « Inventaire du matériel ». Notez que la fonctionnalité « Inventaire du matériel » pour les machines virtuelles n'est pas prise en charge dans les anciennes éditions de Cyber Protect.
- (Pour tous les terminaux) Un agent de protection est installé sur le terminal.
- (Pour tous les terminaux) L'analyse de l'inventaire du matériel sur les terminaux s'est déroulée correctement.
- (Pour les machines virtuelles) La machine utilise l'une des plates-formes de virtualisation prises en charge. Pour plus d'informations, voir "Inventaire matériel" (p. 1037).

Pour afficher tous les composants matériels disponibles sur les terminaux Windows et macOS de l'entreprise

1. Dans la console Cyber Protect, accédez à **Terminaux**.
2. Dans le champ à liste déroulante **Affichage**, sélectionnez **Matériel**.

Remarque
La vue est un ensemble de colonnes qui détermine les données visibles à l'écran. Les vues prédéfinies sont **Standard** et **Matériel**. Vous pouvez créer et enregistrer des vues personnalisées qui incluent différents ensembles de colonnes plus adaptés à vos besoins.

Le tableau suivant décrit les données visibles dans la vue **Matériel**.

Colonne	Description
Nom	Nom du terminal.
État de l'analyse du matériel	Statut de l'analyse du matériel. • **Terminée**. • **Non démarrée**. • **Non prise en charge**. Ce statut concerne les ressources pour lesquelles la fonctionnalité d'inventaire du matériel n'est pas prise en charge. C'est le cas des machines virtuelles, des terminaux mobiles et des terminaux Linux. • **Mise à jour de l'agent**. S'affiche lorsque la version de l'agent installée sur le terminal est obsolète. Le fait de cliquer sur cette action permet d'accéder à la page Paramètres > Agents, où l'administrateur peut effectuer la mise à jour de l'agent. • **Mettre à niveau le quota**. Le fait de cliquer sur cette option ouvre une boîte de dialogue dans laquelle l'administrateur peut changer la licence actuelle et en sélectionner une autre disponible pour les tenants
Processeur	Modèles de tous les processeurs du terminal.
Cœurs de processeur	Nombre de cœurs de tous les processeurs du terminal.
Espace de stockage disque	Stockage utilisé et stockage total de tous les disques du terminal.
Mémoire	Capacité totale de la mémoire RAM du terminal.
Date de l'analyse	Date et heure de la dernière analyse de l'inventaire du matériel.

Colonne	Description
Carte mère	Carte mère du terminal.
Numéro de série de la carte mère	Numéro de série de la carte mère.
Version du BIOS	Version du BIOS du système.
Organisation	Organisation à laquelle appartient le terminal.
Propriétaire	Propriétaire du terminal.
Domaine	Domaine du terminal.
Système d'exploitation	Système d'exploitation du terminal.
Version du système d'exploitation	Version du système d'exploitation du terminal.

3. Pour ajouter des colonnes au tableau, cliquez sur l'icône des options de colonne, puis sélectionnez les colonnes qui doivent être visibles dans le tableau.
4. Pour réduire la quantité d'informations affichées, utilisez un ou plusieurs filtres.
   a. Cliquez sur **Rechercher**.
   b. Cliquez sur la flèche, puis sur **Matériel**.
   c. Sélectionnez un ou plusieurs filtres.
      Le tableau suivant décrit les filtres **Matériel**.

Filtre	Description
Modèle de processeur	Il est possible de sélectionner plusieurs éléments. Utilisez ce filtre si vous souhaitez afficher les données sur le matériel des terminaux disposant du modèle de processeur spécifié.
Cœurs de processeur	Utilisez ce filtre si vous souhaitez afficher les données sur le matériel des terminaux disposant du nombre de cœurs de processeur spécifié.
Taille totale du disque	Utilisez ce filtre si vous souhaitez afficher les données sur le matériel des terminaux disposant de la taille totale de stockage spécifiée.
Capacité mémoire	Utilisez ce filtre si vous souhaitez afficher les données sur le matériel des terminaux disposant de la capacité de mémoire RAM spécifiée.

   d. Cliquez sur **Appliquer**.
5. Pour trier les données dans l'ordre croissant, cliquez sur un nom de colonne.

Affichage du matériel d'un seul terminal

Vous pouvez afficher des informations détaillées sur la carte mère, les processeurs, la mémoire, la carte graphique, les lecteurs de stockage, le réseau et le système d'un terminal spécifique.

Prérequis

- (Pour tous les terminaux) Le terminal utilise un système d'exploitation Windows ou macOS.
- (Pour tous les terminaux) Les terminaux possèdent une licence qui prend en charge la fonctionnalité « Inventaire du matériel ». Notez que la fonctionnalité « Inventaire du matériel » pour les machines virtuelles n'est pas prise en charge dans les anciennes éditions de Cyber Protect.
- (Pour tous les terminaux) Un agent de protection est installé sur le terminal.
- (Pour tous les terminaux) L'analyse de l'inventaire du matériel sur le terminal s'est déroulée correctement.
- (Pour les machines virtuelles) La machine utilise l'une des plates-formes de virtualisation prises en charge. Pour plus d'informations, voir "Inventaire matériel" (p. 1037).

Pour afficher les informations détaillées sur le matériel d'un terminal spécifique

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Dans le champ à liste déroulante **Affichage**, sélectionnez **Matériel**.
3. Recherchez le terminal que vous souhaitez inspecter à l'aide de l'une des méthodes décrites ci-dessous.
   - Recherchez le terminal à l'aide de l'option **Filtre** :
     a. Cliquez sur **Filtre**.
     b. Sélectionnez un ou plusieurs des paramètres de filtre pour rechercher le terminal.
     c. Cliquez sur **Appliquer**.
   - Recherchez le terminal à l'aide de l'option **Recherche** :
     a. Cliquez sur **Rechercher**.
     b. Saisissez une partie ou l'intégralité du nom du terminal, puis appuyez sur la touche **Entrée**.
4. Cliquez sur la ligne qui indique le terminal, puis cliquez sur **Inventaire**.
5. Cliquez sur l'onglet **Matériel**.
   Les données suivantes sur le matériel sont disponibles.

Composant matériel	Informations affichées
Carte mère	Nom, fabricant, modèle et numéro de série de la carte mère du terminal.
Processeurs	Fabricant, modèle, vitesse maximale de l'horloge et nombre de cœurs de chaque processeur du terminal.
Mémoire	Capacité, fabricant et numéro de série de la mémoire du terminal.

Composant matériel	Informations affichées
Graphiques	Fabricant et modèle des processeurs graphiques du terminal.
Lecteurs de stockage	Modèle, type de support, espace disponible et taille des lecteurs de stockage du terminal.
Réseau	Adresse MAC, adresse IP et type des cartes réseau du terminal.
Système	Identifiant de produit, date d'installation d'origine, heure de démarrage, fabricant et modèle du système, version du BIOS, périphérique de démarrage, langue et fuseau horaire du système.

Connexion à des ressources de type Bureau ou assistance à distance

La fonctionnalité de bureau et d'assistance à distance est un moyen pratique de se connecter aux ressources de votre organisation à des fins de contrôle ou d'assistance à distance. Depuis décembre 2022, la fonctionnalité prend en charge les protocoles NEAR, RDP et Partage d'écran Apple. Pour plus d'informations, voir "Protocoles de connexion à distance" (p. 1050).

Vous pouvez utiliser la fonctionnalité Bureau à distance pour effectuer les tâches suivantes.

- Connectez-vous à des ressources Windows, macOS et Linux distantes en utilisant NEAR en mode affichage seul.
- Vous connecter à des ressources Windows à l'aide du protocole RDP.
- Connectez-vous à des ressources macOS distantes en utilisant le partage d'écran Apple en mode affichage seul ou en mode rideau.
- Vous connecter à des ressources gérées et les contrôler à distance à l'aide de connexions à distance dans le cloud.
- Vous connecter à des ressources non gérées et les contrôler à distance à l'aide de connexions à distance directes.
- Vous connecter à des ressources distantes non gérées à l'aide de Acronis Assistance rapide.
- Vous connecter à des ressources distantes à l'aide de différentes méthodes d'authentification : avec identifiants de la ressource distante, en demandant l'autorisation d'observation ou de contrôle, ou avec un code d'accès (pour Assistance rapide).
- Observer simultanément plusieurs écrans dans la vue multiple.
- Enregistrer des sessions distantes (lors de la connexion via NEAR).
- Visualiser le rapport d'historique des sessions.

Pour plus d'informations sur les fonctionnalités intégrées dans les packs Standard et Advanced Management, voir "Fonctionnalités prises en charge de bureau et assistance à distance" (p. 1046).

Vous pouvez utiliser la fonctionnalité d'assistance à distance pour effectuer les tâches suivantes.

- Vous connecter à des ressources Windows, macOS et Linux distantes à l'aide du protocole NEAR en mode de contrôle.
- Connectez-vous à des ressources macOS distantes en utilisant le partage d'écran Apple en mode contrôle.
- Fournir une assistance à distance à des ressources à l'aide de connexions à distance dans le cloud.
- Transférer des fichiers entre les ressources locales et distantes.
- Effectuer des actions de gestion de base sur la ressource distance : redémarrer, arrêter, veille,

vider la corbeille et déconnecter l'utilisateur distant.

- Surveiller la ressource distante en effectuant régulièrement des captures d'écran de son bureau.

Pour plus d'informations sur les fonctionnalités intégrées dans Protection Standard et Advanced Management, voir "Fonctionnalités prises en charge de bureau et assistance à distance" (p. 1046).

Important

Pour activer la fonctionnalité complète de bureau et assistance à distance pour une ressource gérée, vous devez configurer et appliquer un plan de gestion à distance à la ressource. Vous ne pouvez appliquer qu'un seul plan de gestion à distance par ressource, mais selon vos besoins, vous pouvez configurer différents plans de gestion à distance et les appliquer à différentes ressources.

Par exemple, vous pouvez créer un plan de gestion à distance ayant uniquement le protocole RDP activé et l'appliquer à certaines ressources. De cette manière, vous pourrez vous connecter à distance à ces ressources sans activer la licence Advanced Management par ressource et sans avoir à payer de frais supplémentaires.

D'autre part, vous pouvez créer un autre plan de gestion à distance avec les protocoles NEAR et Partage d'écran Apple activés. Dans ce cas, la licence Advanced Management par ressource sera activée et vous serez facturé pour chaque ressource à laquelle ce plan de gestion à distance est appliqué.

Pour plus d'informations sur les plans de gestion à distance et sur leur utilisation, voir "Plans de gestion à distance" (p. 1053).

Remarque

La fonctionnalité de bureau et assistance à distance nécessite les éléments suivants :

- une installation unique de Client Connect sur la ressource de gestion (hôte). Le système vous suggère de télécharger le client lorsque vous essayez d'effectuer pour la première fois une opération à distance (contrôle ou assistance) sur une ressource cible. Vous pouvez également télécharger Client Connect depuis la fenêtre **Téléchargements** dans la console Protection. Pour plus d'informations sur les paramètres que vous pouvez configurer, reportez-vous à "Configuration des paramètres Client Connect" (p. 1085).
- une installation de Agent Connect sur les ressources gérées. Agent Connect est un module faisant partie de l'agent Protection à partir de la version 15.0.31266.
- Pour les ressources distantes macOS, les autorisations système requises doivent être accordées à Agent Connect. Pour plus d'informations, voir "Installation des agents de protection sous macOS" (p. 85).
- l'exécution de l'application Acronis Assistance rapide sur les ressources non gérées. Vous pouvez télécharger Acronis Assistance rapide à partir du site Web.

Pour plus d'informations sur les plates-formes prises en charge par chaque composant de bureau et assistance à distance, reportez-vous à "Plates-formes prises en charge" (p. 1049).

Fonctionnalités prises en charge de bureau et assistance à distance

Le tableau suivant fournit des informations supplémentaires sur les modifications apportées aux fonctionnalités de bureau et assistance à distance prises en charge et ajoutées en décembre 2022.

Fonctionnalité	Protection standard avant décembre 2022	Advanced Management avant décembre 2022	Protection standard après décembre 2022	Advanced Management après décembre 2022
Assistance à distance via RDP pour Windows	Oui	Non	Non	Non
Partager une connexion à distance avec les utilisateurs	Non	Oui	Non	Non
Connexions à distance				
Actions à distance	Non	Non	Oui	Oui
Sélection d'une session pour Windows/macOS/Linux à laquelle se connecter	Non	Non	Non	Oui
Connexion directe via RDP et Partage d'écran Apple	Non	Non	Non	Oui
Contrôle multifenêtre	Non	Non	Non	Oui
Modes de connexion : Contrôle/Affichage seul/Rideau	Non	Non	Non	Oui
Prise en charge d'identifiants communs pour les connexions à distance	Non	Non	Oui	Oui

Fonctionnalité	Protection standard avant décembre 2022	Advanced Management avant décembre 2022	Protection standard après décembre 2022	Advanced Management après décembre 2022
Connexions simultanées par technicien				
via RDP	Oui	Oui	Oui	Oui
via NEAR	Non	Non	Non	Oui
Transfert et partage de fichiers				
depuis Windows vers Windows/macOS/Linux	Non	Non	Non	Oui
depuis macOS vers Windows/macOS/Linux	Non	Non	Non	Oui
depuis Linux vers Windows/macOS/Linux	Non	Non	Non	Oui
Connexion via l'application Assistance rapide				
depuis Windows vers Windows/macOS/Linux	Non	Non	Non	Oui
depuis macOS vers Windows/macOS/Linux	Non	Non	Non	Oui
depuis Linux vers Windows/macOS/Linux	Non	Non	Non	Oui
Connexions à distance via des protocoles				
Connexion à distance via NEAR				
depuis Windows vers Windows/macOS/Linux	Non	Non	Non	Oui

Fonctionnalité	Protection standard avant décembre 2022	Advanced Management avant décembre 2022	Protection standard après décembre 2022	Advanced Management après décembre 2022
depuis macOS vers Windows/macOS/Linux	Non	Non	Non	Oui
depuis Linux vers Windows/macOS/Linux	Non	Non	Non	Oui
Connexion à distance via RDP (client du bureau à distance)				
depuis Windows vers Windows	Oui	Oui	Oui	Oui
depuis macOS vers Windows	Oui	Oui	Oui	Oui
depuis Linux vers Windows	Non	Non	Oui	Oui
Connexion à distance via RDP (client Web)				
depuis Windows vers Windows	Oui	Oui	Oui	Oui
depuis macOS vers Windows	Oui	Oui	Oui	Oui
depuis Linux vers Windows	Non	Non	Oui	Oui
Connexion à distance via Partage d'écran Apple				
depuis Windows/macOS/Linux vers macOS	Non	Non	Non	Oui
Gestion de session				
Enregistrement de session	Non	Non	Non	Oui
Reporting et surveillance				
Historique des sessions et	Non	Non	Non	Oui

Fonctionnalité	Protection standard avant décembre 2022	Advanced Management avant décembre 2022	Protection standard après décembre 2022	Advanced Management après décembre 2022
recherche				
Transmission de captures d'écran	Non	Non	Non	Oui

Plates-formes prises en charge

Le tableau suivant répertorie les systèmes d'exploitation pris en charge par chaque composant de la fonctionnalité de bureau et assistance à distance.

Composant Bureau à distance	Plates-formes prises en charge
Client Connect	• Windows 7 ou version ultérieure • macOS 10.13 ou version ultérieure • Linux : openSUSE 8 Debian 9, 10 Ubuntu 18.0-20.10 Red Hat Enterprise Linux 8 CentOS 8 Fedora 31-33 SUSE Linux Enterprise Server 15 SP2 Linux Mint 20 Manjaro 20
Agent Connect	• Windows 7 ou version ultérieure • Windows Server 2008 R2 ou version ultérieure • macOS 10.13 ou version ultérieure • Linux : Red Hat Enterprise Linux 8, 8.1 Fedora 30 Ubuntu 18.4 LTS (Bionic Beaver) - 19.04 (Disco Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1
Acronis Assistance rapide	• Windows 7 ou version ultérieure • Windows Server 2008 R2 ou version ultérieure • macOS 10.13 ou version ultérieure

Composant Bureau à distance	Plates-formes prises en charge
	• Linux : Red Hat Enterprise Linux 8, 8.1 Fedora 30 Ubuntu 18.4 LTS (Bionic Beaver) - 19.04 (Disco Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1

Protocoles de connexion à distance

La fonctionnalité Bureau à distance utilise les protocoles suivants pour les connexions à distance.

NEAR

Le protocole NEAR est un protocole hautement sécurisé développé par Acronis et ayant les caractéristiques suivantes.

- ### H.264

  Le protocole NEAR implémente trois modes de qualité : **Lisse**, **Équilibré** et **Net**. En mode **Lisse**, le protocole NEAR utilise le codage matériel H.264 sous macOS et Windows afin de coder l'image du bureau. Par ailleurs, le basculement vers le codeur logiciel si le codeur matériel n'est pas disponible. La taille de l'image est actuellement limitée à la résolution Full HD (1 920 x 1 080).

- ### Codec adaptatif

  En modes de qualité **Équilibré** et **Net**, le protocole NEAR utilise le codec adaptatif, ce qui fournit la meilleure qualité d'image en 32 bits par rapport au mode vidéo utilisé par le protocole H.264.
  En mode **Équilibré**, la qualité de l'image est ajustée automatiquement en fonction de vos conditions réseau et la fréquence d'images actuelle est conservée.
  En mode **Net**, la qualité d'image est la meilleure. Toutefois, le nombre d'images par seconde peut être réduit si votre réseau, votre processeur ou votre carte vidéo sont surchargés.
  Le codec adaptatif utilise OpenCL sous Windows et macOS lorsqu'il est disponible dans les pilotes graphiques.

- ### Transfert audio

  Le protocole NEAR peut capturer le son de l'ordinateur distant et le transférer à l'hôte. Pour plus d'informations sur l'activation de la redirection du son à distance sous Windows, macOS et Linux, voir "Redirection du son à distance" (p. 1051).

- ### Différentes options de connexion

  Vous pouvez utiliser les méthodes suivantes pour vous connecter à la ressource distante.

  Code d'accès : l'utilisateur qui est connecté à la ressource distante exécute Assistance rapide et vous indique le code d'accès. Grâce à cette méthode, vous vous connectez toujours à la session de l'utilisateur connecté.

  Identifiants de la ressource : connectez-vous à la ressource distante à l'aide des identifiants d'administrateur qui sont enregistrés dans la ressource.

  Demander l'autorisation d'observation ou de contrôle : le système demandera à l'utilisateur connecté à la ressource distante d'autoriser ou de refuser la connexion.

- ### Sécurité

  Vos données sont toujours chiffrées dans les deux sens avec le chiffrement AES dans NEAR.

RDP

Le protocole RDP (Remote Desktop Protocol) est un protocole propriétaire développé par Microsoft qui permet d'établir une connexion réseau à un ordinateur Windows distant.

Partage d'écran Apple

Le partage d'écran Apple est un client VNC d'Apple inclus dans macOS depuis la version 10.5.

Redirection du son à distance

Client Connect prend en charge la diffusion du son via le protocole de connexion NEAR. Pour plus d'informations sur NEAR, reportez-vous à "Protocoles de connexion à distance" (p. 1050).

Redirection du son d'une ressource distante Windows

Pour les ressources Windows, le son distant devrait être transmis automatiquement. Assurez-vous que des terminaux de sortie audio (haut-parleurs ou casque) sont connectés à la ressource distante.

Redirection du son d'une ressource distante macOS

Pour activer la redirection du son depuis une ressource macOS, vérifiez les points suivants :

- L'agent Protection est installé sur la ressource.
- La ressource dispose d'un pilote de capture audio.
- La ressource utilise le protocole NEAR pour les connexions à distance.

Remarque
Pour macOS 10.15 Catalina, l'autorisation d'accès au microphone doit être accordée à Agent Connect. Pour plus d'informations sur l'autorisation d'accès à Agent Connect, reportez-vous à "Attribution des autorisations système requises à Agent Connect" (p. 86).

L'agent utilise les pilotes de capture audio suivants : Soundflower ou Blackhole.

Le processus d'installation sur les dernières versions est décrit sur la page wiki de Blackhole : https://github.com/ExistentialAudio/BlackHole/wiki/Installation.

Remarque
Client Connect ne prend actuellement en charge que la version à 2 canaux de Blackhole.

Si Homebrew est installé sur la ressource, vous pouvez installer Blackhole en exécutant la commande suivante :

```
brew install --cask blackhole-2ch
```

Remarque
Si le son d'une ressource macOS distante est redirigé, l'utilisateur qui est connecté à la ressource distante n'entendra pas le son.

Redirection du son d'une ressource distante Linux

La redirection du son à distance devrait s'effectuer automatiquement sur la plupart des distributions Linux. Si la redirection du son à distance ne fonctionne pas par défaut, installez le pilote PulseAudio en exécutant la commande suivante :

```
sudo apt-get install pulseaudio
```

Connexions à des ressources distantes de type bureau ou assistance à distance

La fonctionnalité de bureau et assistance à distance propose différentes méthodes permettant d'établir des connexions à distance directes ou dans le cloud à vos ressources.

Les connexions directes sont établies par TCP/IP sur un réseau local entre Client Connect et la ressource distante sur laquelle aucun agent n'est installé. Elles ne nécessitent aucun accès Internet.

Les connexions dans le cloud sont établies entre Client Connect et l'agent ou Assistance rapide sur la ressource via Acronis Cloud.

Le tableau suivant fournit des informations complémentaires sur les options de connexion dans le cloud.

Connexion dans le cloud	Option Connexion dans le cloud	Mode d'affichage	Action à distance prise en charge	Disponible pour
via NEAR	de Client Connect à Agent Connect de Client Connect à Assistance rapide	Contrôle Affichage seul	Bureau à distance Assistance à distance	ressources gérées
via RDP	de Client Connect à Agent Connect depuis le client Web vers Agent Connect	Contrôle	Bureau à distance	ressources gérées
via Partage d'écran Apple	de Client Connect à Agent Connect	Contrôle Affichage seul Rideau	Bureau à distance Assistance à distance	ressources gérées

Le tableau suivant fournit des informations complémentaires sur les options de connexion directe.

Connexion directe	Option Connexion directe	Action à distance prise en charge	Disponible pour
via RDP	depuis Client Connect vers un serveur RDP	Bureau à distance	ressources non gérées
via Partage d'écran Apple	de Client Connect vers le serveur Partage d'écran Apple	Bureau à distance Assistance à distance	ressources non gérées

Plans de gestion à distance

Les plans de gestion à distance sont des plans que vous appliquez à l'agent Protection afin d'activer et de configurer la fonctionnalité de bureau et assistance à distance sur vos ressources gérées.

Si aucun plan de gestion à distance n'est appliqué à une ressource, la fonctionnalité de bureau et assistance à distance est limitée aux actions à distance (redémarrage, arrêt, mise en veille, vidage de la corbeille et déconnexion de l'utilisateur distant).

Remarque
La disponibilité des paramètres que vous pouvez configurer dans le plan de gestion à distance dépend du Service Pack appliqué au tenant. Pour accéder à tous les paramètres, activez le pack Advanced Management. Pour plus d'informations sur les fonctionnalités intégrées dans les packs Standard et Advanced Management, voir "Fonctionnalités prises en charge de bureau et assistance à distance" (p. 1046).

Création d'un plan de gestion à distance

Vous pouvez créer un plan de gestion à distance, puis l'affecter à une ressource afin de configurer la fonctionnalité de bureau et assistance à distance sur la ressource gérée.

Remarque
La disponibilité des paramètres du plan de gestion à distance dépend du quota de service affecté au tenant. Si vous utilisez la fonctionnalité standard, vous ne pouvez configurer que les connexions via RDP.

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour créer un plan de gestion à distance

Depuis les plans de gestion à distance

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de gestion à distance**.
2. Créez un plan de gestion à distance en utilisant l'une des deux options.
   - Si la liste ne comprend aucun plan de gestion à distance, cliquez sur **Créer**.
   - Si la liste comprend des plans de gestion à distance, cliquez sur **Création d'un plan**.
3. [Facultatif] Pour modifier le nom par défaut du plan, cliquez sur l'icône en forme de crayon, saisissez le nom du plan, puis cliquez sur **Continuer**.
4. Cliquez sur **Protocoles de connexion** et activez les protocoles que vous souhaitez voir disponibles dans ce plan de gestion à distance pour les connexions à distance - NEAR, RDP ou Partage d'écran Apple.
5. [Facultatif] Pour le protocole NEAR, dans la section **Paramètres de sécurité**, cochez ou désélectionnez les cases afin d'activer ou de désactiver le paramètre correspondant, puis cliquez sur **Terminé**.

Paramètre	Description	Disponible pour
Verrouiller la ressource lorsque l'utilisateur se déconnecte d'une session de console	Si vous sélectionnez ce paramètre, la ressource distante sera verrouillée lorsque vous vous déconnecterez de la session de console.	Windows, macOS
Autoriser un seul utilisateur à la fois à se connecter via NEAR ou à transférer des fichiers	Si vous sélectionnez ce paramètre, les connexions à l'aide du protocole NEAR et les transferts de fichiers ne seront pas possibles pendant	Windows, macOS, Linux

Paramètre	Description	Disponible pour
	qu'une connexion à distance à la ressource est active.	
Autoriser l'administrateur de la ressource à se connecter à toute session d'utilisateur non-administrateur	Si vous sélectionnez ce paramètre, l'administrateur est autorisé à se connecter à une session utilisateur standard sur la ressource. Si les options **Autoriser l'administrateur de la ressource à se connecter à toute session d'utilisateur non-administrateur** et **Autoriser la création d'une session système** sont toutes deux désélectionnées, vous ne pourrez vous connecter qu'aux sessions administrateur actives sur les ressources macOS distantes.	Windows, macOS
Autoriser la création d'une session système	Si vous sélectionnez ce paramètre, lors de l'établissement de connexions à distance, l'administrateur se connectera à une nouvelle session au lieu d'utiliser l'une des sessions actives.	macOS
Autoriser la synchronisation du Presse-papiers	Si vous sélectionnez ce paramètre, vous pourrez transférer des données entre votre Presse-papiers et celui de la ressource distante. Par exemple, vous pourrez copier du texte d'un fichier sur la ressource distante, puis le coller dans un fichier sur votre ressource, et inversement.	Windows, macOS, Linux

6. Cliquez sur **Paramètres de sécurité**, cochez ou désélectionnez les cases afin d'activer ou de désactiver le paramètre correspondant, puis cliquez sur **Terminé**.

Paramètre	Description
Afficher si la ressource est contrôlée à distance	Si vous sélectionnez ce paramètre, une notification s'affichera sur le bureau de la ressource distante s'il existe une connexion Bureau à distance active à la ressource.
Demander l'autorisation de l'utilisateur à effectuer des captures d'écran de la ressource	Si vous sélectionnez ce paramètre, l'utilisateur de la ressource distante sera informé lorsque l'administrateur demande la transmission d'une capture d'écran depuis cette ressource.

7. Cliquez sur **Gestion des ressources**, sélectionnez les fonctionnalités que vous souhaitez mettre à la disposition des ressources distantes, puis cliquez sur **Terminé**.

Paramètre	Description	Disponible sur
Transfert de fichiers	Permet les transferts de fichiers entre les ressources locales et distantes.	Windows, macOS, Linux
Transmission de captures d'écran	Permet la transmission des captures d'écran du bureau de la ressource distante à la console Cyber Protect.	Windows, macOS, Linux

8. Cliquez sur **Paramètres d'affichage**, cochez ou désélectionnez les cases afin d'activer ou de désactiver le paramètre correspondant, puis cliquez sur **Terminé**.

Remarque
Les **Paramètres d'affichage** sont uniquement disponibles pour les connexions via NEAR.

Paramètre	Description	Disponible sur
Utiliser la déduplication de bureau pour effectuer la capture d'un bureau	La duplication de bureau est l'une des méthodes de capture d'écran de Windows. Dans certains environnements, l'opération peut être instable. Si vous n'utilisez pas la déduplication de bureau, vous utiliserez plutôt la méthode de base (BitBlt) qui est plus lente, mais plus stable.	Windows
Utiliser l'accélération	L'accélération OpenCL peut	Linux

Paramètre	Description	Disponible sur
OpenCL	accélérer le codec adaptatif qui est responsable du mode de qualité **Équilibré** en exécutant des calculs sur le processeur graphique. Cette option nécessite l'installation d'un pilote OpenCL sur la ressource Linux distante. Le codec adaptatif utilise OpenCL sous macOS et Windows s'il est disponible dans vos pilotes graphiques.	
Utiliser le codage matériel H.264	Le protocole NEAR prend en charge trois modes de qualité : **Lisse**, **Équilibré** et **Net**. Le mode **Lisse** utilise le codage matériel H.264 pour coder l'image du bureau. Le mode **Équilibré** utilise le codec adaptatif, ce qui fournit la meilleure qualité d'image en 32 bits par rapport au mode vidéo utilisé par le protocole H.264. La qualité de l'image est ajustée automatiquement en fonction de vos conditions réseau et la fréquence d'images actuelle est conservée. Le mode **Net** utilise le codec adaptatif, ce qui fournit la meilleure qualité d'image en 32 bits par rapport au mode vidéo utilisé par le protocole H.264. La qualité d'image est toujours la meilleure. Toutefois, le nombre d'images par seconde peut être réduit si votre réseau ou processeur/carte vidéo sont surchargés.	Windows, macOS

9. Si vous souhaitez que les informations concernant les derniers utilisateurs qui se sont connectés aux ressources soient visibles dans les détails de ces ressources, cliquez sur **Boîte à outils**, sélectionnez **Afficher les derniers utilisateurs connectés**, puis cliquez sur **Terminé**.

   Pour plus d'informations sur les derniers utilisateurs connectés, voir "Rechercher le dernier utilisateur connecté" (p. 413).
10. [Facultatif] Pour ajouter des ressources au plan :
    a. Cliquez sur **Ajouter des ressources**.
    b. Sélectionnez les ressources, puis cliquez sur **Ajouter**.
    c. Si vous avez des problèmes de compatibilité à résoudre, suivez la procédure décrite dans "Résolution des problèmes de compatibilité avec les plans de gestion à distance" (p. 1066).
11. Cliquez sur **Créer**.

À partir de tous les terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur la ressource à laquelle vous souhaitez appliquer un plan de gestion à distance.
3. Cliquez sur **Protection**, puis sur **Ajouter un plan**.
4. Cliquez sur **Création d'un plan**, puis sélectionnez **Gestion à distance**.
5. [Facultatif] Pour modifier le nom par défaut du plan, cliquez sur l'icône en forme de crayon, saisissez le nom du plan, puis cliquez sur **Continuer**.
6. Cliquez sur **Protocoles de connexion** et activez les protocoles que vous souhaitez voir disponibles dans ce plan de gestion à distance pour les connexions à distance - NEAR, RDP ou Partage d'écran Apple.
7. [Facultatif] Pour le protocole NEAR, dans la section **Paramètres de sécurité**, cochez ou désélectionnez les cases afin d'activer ou de désactiver le paramètre correspondant, puis cliquez sur **Terminé**.

Paramètre	Description	Disponible pour
Verrouiller la ressource lorsque l'utilisateur se déconnecte d'une session de console	Si vous sélectionnez ce paramètre, la ressource distante sera verrouillée lorsque vous vous déconnecterez de la session de console.	Windows, macOS
Autoriser un seul utilisateur à la fois à se connecter via NEAR ou à transférer des fichiers	Si vous sélectionnez ce paramètre, les connexions à l'aide du protocole NEAR et les transferts de fichiers ne seront pas possibles pendant qu'une connexion à distance à la ressource est active.	Windows, macOS, Linux

Paramètre	Description	Disponible pour
Autoriser l'administrateur de la ressource à se connecter à toute session d'utilisateur non-administrateur	Si vous sélectionnez ce paramètre, l'administrateur est autorisé à se connecter à une session utilisateur standard sur la ressource. Si les options **Autoriser l'administrateur de la ressource à se connecter à toute session d'utilisateur non-administrateur** et **Autoriser la création d'une session système** sont toutes deux désélectionnées, vous ne pourrez vous connecter qu'aux sessions administrateur actives sur les ressources macOS distantes.	Windows, macOS
Autoriser la création d'une session système	Si vous sélectionnez ce paramètre, lors de l'établissement de connexions à distance, l'administrateur se connectera à une nouvelle session au lieu d'utiliser l'une des sessions actives.	macOS
Autoriser la synchronisation du Presse-papiers	Si vous sélectionnez ce paramètre, vous pourrez transférer des données entre votre Presse-papiers et celui de la ressource distante. Par exemple, vous pourrez copier du texte d'un fichier sur la ressource distante, puis le coller dans un fichier sur votre ressource, et inversement.	Windows, macOS, Linux

8. Cliquez sur **Paramètres de sécurité**, cochez ou désélectionnez les cases afin d'activer ou de désactiver le paramètre correspondant, puis cliquez sur **Terminé**.

Paramètre	Description
Afficher si la ressource est contrôlée à distance	Si vous sélectionnez ce paramètre, une notification s'affichera sur le bureau de la

Paramètre	Description
	ressource distante s'il existe une connexion Bureau à distance active à la ressource.
Demander l'autorisation de l'utilisateur à effectuer des captures d'écran de la ressource	Si vous sélectionnez ce paramètre, l'utilisateur de la ressource distante sera informé lorsque l'administrateur demande la transmission d'une capture d'écran depuis cette ressource.

9. Cliquez sur **Gestion des ressources**, sélectionnez les fonctionnalités que vous souhaitez mettre à la disposition des ressources distantes, puis cliquez sur **Terminé**.

Paramètre	Description	Disponible sur
Transfert de fichiers	Permet les transferts de fichiers entre les ressources locales et distantes.	Windows, macOS, Linux
Transmission de captures d'écran	Permet la transmission des captures d'écran du bureau de la ressource distante à la console Cyber Protect.	Windows, macOS, Linux

10. Cliquez sur **Paramètres d'affichage**, cochez ou désélectionnez les cases afin d'activer ou de désactiver le paramètre correspondant, puis cliquez sur **Terminé**.

Remarque
Les **Paramètres d'affichage** sont uniquement disponibles pour les connexions via NEAR.

Paramètre	Description	Disponible sur
Utiliser la déduplication de bureau pour effectuer la capture d'un bureau	La duplication de bureau est l'une des méthodes de capture d'écran de Windows. Dans certains environnements, l'opération peut être instable. Si vous n'utilisez pas la déduplication de bureau, vous utiliserez plutôt la méthode de base (BitBlt) qui est plus lente, mais plus stable.	Windows
Utiliser l'accélération OpenCL	L'accélération OpenCL peut accélérer le codec adaptatif qui est responsable du mode	Linux

Paramètre	Description	Disponible sur
	de qualité **Équilibré** en exécutant des calculs sur le processeur graphique. Cette option nécessite l'installation d'un pilote OpenCL sur la ressource Linux distante. Le codec adaptatif utilise OpenCL sous macOS et Windows s'il est disponible dans vos pilotes graphiques.	
Utiliser le codage matériel H.264	Le protocole NEAR prend en charge trois modes de qualité : **Lisse**, **Équilibré** et **Net**. Le mode **Lisse** utilise le codage matériel H.264 pour coder l'image du bureau. Le mode **Équilibré** utilise le codec adaptatif, ce qui fournit la meilleure qualité d'image en 32 bits par rapport au mode vidéo utilisé par le protocole H.264. La qualité de l'image est ajustée automatiquement en fonction de vos conditions réseau et la fréquence d'images actuelle est conservée. Le mode **Net** utilise le codec adaptatif, ce qui fournit la meilleure qualité d'image en 32 bits par rapport au mode vidéo utilisé par le protocole H.264. La qualité d'image est toujours la meilleure. Toutefois, le nombre d'images par seconde peut être réduit si votre réseau ou processeur/carte vidéo sont surchargés.	Windows, macOS

11. Si vous souhaitez que les informations concernant les derniers utilisateurs qui se sont connectés aux ressources soient visibles dans les détails de ces ressources, cliquez sur **Boîte à outils**,

sélectionnez **Afficher les derniers utilisateurs connectés**, puis cliquez sur **Terminé**.

Pour plus d'informations sur les derniers utilisateurs connectés, voir "Rechercher le dernier utilisateur connecté" (p. 413).

12. Cliquez sur **Créer**.

Ajout d'une ressource à un plan de gestion à distance

En fonction de vos besoins, vous pouvez ajouter des ressources à un plan de gestion à distance après sa création.

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour ajouter une ressource à un plan de gestion à distance

Depuis les plans de gestion à distance

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de gestion à distance**.
2. Cliquez sur le plan de gestion à distance.
3. Selon que le plan est déjà appliqué ou pas à une ressource, effectuez l'une des opérations suivantes :
   - Cliquez sur **Ajouter des ressources**, si le plan n'a encore été appliqué à aucune ressource.
   - Cliquez sur **Gérer les ressources** si le plan n'a été appliqué à aucune ressource.
4. Sélectionnez une ressource dans la liste, puis cliquez sur **Ajouter**.
5. Cliquez sur **Enregistrer**.
6. Cliquez sur **Confirmer** pour appliquer le quota de service requis à la ressource.

À partir de tous les terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur la ressource à laquelle vous souhaitez appliquer un plan de gestion à distance.
3. Cliquez sur **Protection**, puis sur **Ajouter un plan**.
4. Dans **Sélectionnez un plan dans la liste ci-dessous**, sélectionnez **Gestion à distance** pour n'afficher que les plans de gestion à distance.
5. Cliquez sur **Appliquer**.
6. Cliquez sur **Confirmer** pour appliquer le quota de service requis à la ressource.

Suppression de ressources d'un plan de gestion à distance

En fonction de vos besoins, vous pouvez supprimer des ressources d'un plan de gestion à distance.

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour supprimer des ressources d'un plan de gestion à distance

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de gestion à distance**.
2. Cliquez sur le plan de gestion à distance.
3. Cliquez sur **Gérer les ressources**.
4. Sélectionnez une ou plusieurs ressources que vous souhaitez supprimer du plan de gestion à distance, puis cliquez sur **Supprimer**.
5. Cliquez sur **Valider**.
6. Cliquez sur **Enregistrer**.

Autres opérations effectuées avec des plans de gestion à distance existants

Dans l'écran **Plans de gestion à distance**, vous pouvez effectuer les opérations supplémentaires suivantes avec les plans de gestion à distance : afficher les détails, afficher et modifier les activités, afficher les alertes, renommer, activer, désactiver, cloner, exporter et supprimer les alertes.

Afficher les détails

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour afficher les détails d'un plan de gestion à distance

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Plus d'actions** du plan de gestion à distance.
2. Cliquez sur **Afficher les détails**.

Modifier

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour modifier un plan

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Plus d'actions** du plan de gestion à distance.
2. Cliquez sur **Modifier**.

Activités

Pour afficher les activités relatives à un plan de gestion à distance

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Plus d'actions** du plan de gestion à distance.

2. Cliquez sur **Activités**.
3. Cliquez sur une activité pour visualiser plus de détails la concernant.

Alertes

Pour afficher les alertes

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Plus d'actions** du plan de gestion à distance.
2. Cliquez sur **Alertes**.

Renommer

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Renommer un plan de gestion à distance

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Plus d'actions** du plan de gestion à distance.
2. Cliquez sur **Renommer**.
3. Saisissez le nouveau nom du plan, puis cliquez sur **Continuer**.

Activer

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Activer un plan de gestion à distance

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Plus d'actions** du plan de gestion à distance.
2. Cliquez sur **Activer**.

Désactiver

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Désactiver un plan de gestion à distance

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Plus d'actions** du plan de gestion à distance.
2. Cliquez sur **Désactiver**.

Cloner

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour cloner un plan de gestion à distance

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Plus d'actions** du plan de gestion à distance.
2. Cliquez sur **Cloner**.
3. Cliquez sur **Créer**.

Exporter

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour exporter un plan de gestion à distance

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Plus d'actions** du plan de gestion à distance.
2. Cliquez sur **Exporter**.
   La configuration du plan est exportée au format JSON vers la machine locale.

Supprimer

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Supprimer un plan de gestion à distance

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Plus d'actions** du plan de gestion à distance.
2. Cliquez sur **Supprimer**.
3. Sélectionnez **Je confirme**, puis cliquez sur **Supprimer**.

Problèmes de compatibilité avec les plans de gestion à distance

Dans certains cas, l'application d'un plan de gestion à distance sur une ressource peut provoquer des problèmes de compatibilité. Vous pouvez observer les problèmes de compatibilité suivants :

- Plans en conflit : ce problème survient lorsqu'un autre plan de gestion à distance est déjà appliqué à la ressource (il n'est possible d'appliquer qu'un seul plan de gestion à distance à une ressource).
- Système d'exploitation incompatible : ce problème survient lorsque le système d'exploitation de la ressource n'est pas pris en charge.

- Agent non pris en charge : ce problème survient lorsque la version de l'agent de protection sur la ressource est obsolète et ne prend pas en charge la fonctionnalité Bureau à distance.
- Quota insuffisant : ce problème survient lorsque le quota de service dans le tenant est insuffisant pour l'affectation aux ressources sélectionnées.

Si le plan de gestion à distance est appliqué au maximum à 150 ressources sélectionnées individuellement, vous serez invité à résoudre les conflits existants avant d'enregistrer le plan. Pour résoudre un conflit, supprimez sa cause racine ou les ressources concernées du plan. Pour plus d'informations, voir "Résolution des problèmes de compatibilité avec les plans de gestion à distance" (p. 1066). Si vous enregistrez le plan sans résoudre les conflits, le plan sera désactivé automatiquement pour les ressources non prises en charge, et des alertes s'afficheront.

Si le plan de gestion à distance est appliqué à plus de 150 ressources ou à des groupes de terminaux, il sera d'abord enregistré, puis sa compatibilité sera vérifiée. Le plan sera automatiquement désactivé pour les ressources incompatibles, et des alertes apparaîtront.

Résolution des problèmes de compatibilité avec les plans de gestion à distance

Selon la cause des problèmes de compatibilité, vous pouvez effectuer différentes actions afin de résoudre ces problèmes dans le cadre du processus de création d'un nouveau plan de gestion à distance.

Remarque
Lors de la résolution d'un problème de compatibilité par suppression de ressources d'un plan, vous ne pouvez pas supprimer les ressources faisant partie d'un groupe de terminaux.

Pour résoudre les problèmes de compatibilité

1. Cliquez sur **Examiner les problèmes**.
2. [Pour résoudre les problèmes de compatibilité avec des plans de gestion à distance existants par suppression de ressources du nouveau plan]
   a. Dans l'onglet **Plans en conflit**, sélectionnez les ressources que vous souhaitez supprimer.
   b. Cliquez sur **Supprimer les ressources du plan**.
   c. Cliquez sur **Supprimer**, puis sur **Fermer**.
3. [Pour résoudre les problèmes de compatibilité avec des plans de gestion à distance par désactivation des plans déjà appliqués aux ressources]
   a. Cliquez sur **Désactiver les plans appliqués**.
   b. Cliquez sur **Désactiver**, puis sur **Fermer**.
4. [Pour résoudre les problèmes de compatibilité avec des systèmes d'exploitation incompatibles]
   a. Dans l'onglet **Système d'exploitation incompatible**, sélectionnez les ressources que vous souhaitez supprimer.

b. Cliquez sur **Supprimer les ressources du plan**.

c. Cliquez sur **Supprimer**, puis sur **Fermer**.

5. [Pour résoudre les problèmes de compatibilité avec des agents non pris en charge par suppression de ressources du plan]
   a. Dans l'onglet **Agents non pris en charge**, sélectionnez les ressources que vous souhaitez supprimer.
   b. Cliquez sur **Supprimer les ressources du plan**.
   c. Cliquez sur **Supprimer**, puis sur **Fermer**.
6. [Pour résoudre les problèmes de compatibilité avec des agents non pris en charge grâce à la mise à jour de la version de l'agent] Cliquez sur **Accéder à la liste des agents**.

   Remarque
   Cette option est disponible uniquement pour les administrateurs clients.

7. [Pour résoudre les problèmes de compatibilité liés à un quota insuffisant par suppression de ressources du plan]
   a. Dans l'onglet **Quota insuffisant**, sélectionnez les ressources que vous souhaitez supprimer.
   b. Cliquez sur **Supprimer les ressources du plan**.
   c. Cliquez sur **Supprimer**, puis sur **Fermer**.
8. [Pour résoudre les problèmes de compatibilité liés à un quota insuffisant par augmentation du quota du tenant]

   Remarque
   Cette option est disponible uniquement pour les administrateurs partenaires.

   a. Dans l'onglet **Quota insuffisant**, cliquez sur **Accéder au portail de gestion**.
   b. Augmentez le quota de service du client.

Identifiants de la ressource

Vous pouvez ajouter les identifiants de l'administrateur ou d'un autre type d'utilisateur des ressources distantes (nom d'utilisateur et mot de passe, ou mot de passe VNC), les enregistrer dans le magasin d'identifiants dans le cloud, puis les utiliser pour l'authentification automatique lors de la connexion aux ressources que vous gérez. De cette manière, au lieu de saisir ces identifiants manuellement à l'étape d'authentification de chaque connexion, vous pouvez ajouter ces identifiants au magasin d'identifiants une fois. Client Connect utilisera alors ces identifiants chaque fois que vous souhaiterez vous connecter aux ressources à distance.

Remarque
Les identifiants conservés dans le magasin d'identifiants ne sont pas partagés entre les différents niveaux de tenants. Ils ne sont partagés que sur le même niveau de tenant, pour le même tenant client ou tenant partenaire.

Cela signifie que si un tenant client comporte plusieurs administrateurs, ces derniers voient et partagent les identifiants dans le magasin d'identifiants, tandis que les autres administrateurs de partenaires ou les administrateurs clients d'autres tenants ne pourront ni visualiser ni utiliser ces identifiants.

Ajout d'identifiants

Vous pouvez ajouter des identifiants et les utiliser pour les connexions à distance à plusieurs ressources.

Pour ajouter les identifiants à une ressource et les enregistrer dans le magasin d'identifiants

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur la ressource à laquelle vous souhaitez ajouter des identifiants.
3. Accédez au menu **Paramètres** de l'une des manières suivantes :
   - Cliquez sur **Bureau à distance**, puis sur **Paramètres**.
   - Cliquez sur **Gérer**, puis sur **Paramètres**.
4. Cliquez sur **Ajouter les identifiants**.
5. Dans le **magasin d'identifiants**, cliquez sur **Ajouter les identifiants**.
6. Saisissez les identifiants.

Champs	Description
Nom des identifiants	Identificateur des identifiants qui sera visible dans le magasin d'identifiants.
Nom d'utilisateur	Nom d'utilisateur qui sera utilisé pour les connexions à distance à la ressource cible.
Mot de passe	Mot de passe qui sera utilisé pour les connexions à distance à la ressource cible.
Mot de passe VNC	Ce champ n'est disponible que pour le partage d'écran Apple.

7. Cliquez sur **Enregistrer**.

Affectation d'identifiants à une ressource

Après avoir ajouté des identifiants, vous pouvez les utiliser pour vous authentifier automatiquement lorsque vous vous connectez à une ressource que vous gérez.

Pour affecter des identifiants enregistrés pour l'authentification automatique sur une ressource

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Accédez au menu **Paramètres** de l'une des manières suivantes :
   - Cliquez sur **Bureau à distance**, puis sur **Paramètres**.
   - Cliquez sur **Gérer**, puis sur **Paramètres**.
3. Dans l'onglet du protocole supporté (NEAR, RDP ou Partage d'écran Apple) cliquez sur **Ajouter des identifiants**.
4. Dans le **magasin d'identifiants**, sélectionnez les identifiants dans la liste, puis cliquez sur **Sélectionner les identifiants**.

Suppression d'identifiants

Vous pouvez supprimer les identifiants qui ne sont plus utiles.

Pour supprimer des identifiants du magasin d'identifiants

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Accédez au menu **Paramètres** de l'une des manières suivantes :
   - Cliquez sur **Bureau à distance**, puis sur **Paramètres**.
   - Cliquez sur **Gérer**, puis sur **Paramètres**.
3. Dans l'onglet du protocole pris en charge (NEAR, RDP ou Partage d'écran Apple), cliquez sur **Supprimer**.
4. Dans la fenêtre de confirmation, cliquez sur **Supprimer**.

Annulation de l'affectation d'identifiants d'une ressource

Vous pouvez annuler l'affectation d'identifiants d'une ressource, mais les conserver dans le magasin d'identifiants.

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Accédez au menu **Paramètres** de l'une des manières suivantes :
   - Cliquez sur **Bureau à distance**, puis sur **Paramètres**.
   - Cliquez sur **Gérer**, puis sur **Paramètres**.
3. Dans l'onglet du protocole pris en charge (NEAR, RDP ou Partage d'écran Apple cliquez sur **Annuler l'affectation**.
4. Dans la fenêtre de confirmation, cliquez sur **Annuler l'affectation**.

Utilisation des ressources gérées

Les ressources gérées sont des ressources sur lesquelles l'agent Protection est installé.

Vous pouvez effectuer les opérations suivantes sur les ressources distantes gérées :

- se connecter pour l'assistance à distance ou le bureau à distance en utilisant NEAR en mode contrôle ou affichage seul
- Effectuer une connexion de type Bureau à distance via RDP en mode de contrôle
- se connecter pour l'assistance à distance ou le bureau à distance en utilisant le Partage d'écran Apple en mode contrôle, affichage seul ou mode rideau
- Effectuer une connexion de type Bureau à distance via un client Web
- Redémarrer un ordinateur, l'arrêter, le mettre en veille, vider la corbeille et déconnecter l'utilisateur distant des ressources distantes
- Transférer des fichiers entre votre ressource et les ressources distantes
- Surveiller les ressources en effectuant des captures d'écran

Remarque
Les connexions Bureau à distance aux ressources gérées nécessitent l'installation d'un agent Protection et l'application d'un plan de gestion à distance sur la ressource.

Configuration des paramètres RDP

Vous pouvez configurer les paramètres qui seront appliqués automatiquement aux connexions RDP à distance de type contrôle à la ressource gérée.

Pour configurer les paramètres RDP d'une ressource

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Accédez au menu **Paramètres** de l'une des manières suivantes :
   - Cliquez sur **Bureau à distance**, puis sur **Paramètres**.
   - Cliquez sur **Gérer**, puis sur **Paramètres**.

3. Dans l'onglet **RDP**, configurez les paramètres.

Paramètre	Description
Lecture audio	Ce paramètre active ou désactive la redirection du son de la ressource distante sur votre ressource locale.
Enregistrement audio	Ce paramètre détermine si l'enregistrement audio (effectué à l'aide du microphone) sera transféré à la ressource distante.
Rediriger les imprimantes	Si vous sélectionnez ce paramètre, les imprimantes de votre ressource seront disponibles sur la ressource distante.
Rediriger les fichiers	Ce paramètre définit si les fichiers de votre ressource locale seront partagés sur la ressource distante.
Intensité de couleur	Ce paramètre détermine le nombre de couleurs dans l'image qui sera transférée par RDP. Plus la valeur est élevée, plus la bande passante nécessaire est importante. **32 768 couleurs** : 16 bits **Couleurs vraies** : • 24 bits pour les connexions RDP via le client Web • 32 bits pour les connexions RDP via Client Connect

4. Cliquez sur le bouton Fermer.

Connexion à des ressources gérées de type bureau ou assistance à distance

Remarque
La disponibilité des protocoles de connexion que vous pouvez utiliser pour les connexions à distance dépend de la configuration du plan de gestion à distance et du système d'exploitation de la ressource distante.

Prérequis

- Un plan de gestion à distance sur lequel le protocole de connexion correspondant est activé est appliqué à la ressource gérée.
- Le quota de service nécessaire est affecté à la ressource. (Le quota de service est acquis automatiquement lorsque vous appliquez un plan de gestion à distance à la ressource.)
- [Pour les connexions en partage d'écran Apple] Partage d'écran Apple est activé sur la ressource macOS.
- L'authentification à deux facteurs est activée pour votre compte utilisateur dans Acronis Cyber Protect Cloud.

Pour établir une connexion de type bureau ou assistance à distance à une ressource gérée

1. Dans la Cyber Protect console, allez sur **Terminaux** > **Ordinateurs avec agents**.
2. Cliquez sur la ressource à laquelle vous souhaitez vous connecter.
3. Cliquez sur **Bureau à distance**.
   Par défaut, le protocole de connexion sélectionné est le protocole NEAR.
4. [Facultatif] Dans la liste déroulante **Protocole de connexion**, sélectionnez le protocole de connexion que vous souhaitez utiliser.
5. Cliquez sur le mode d'affichage que vous souhaitez utiliser.

Protocole	Connexions à distance à	Mode d'affichage	Action à distance prise en charge
NEAR	Windows Linux macOS	**Contrôle** : dans ce mode, vous pourrez observer la ressource distante et y effectuer des opérations. **Affichage seul** - Dans ce mode, vous ne pourrez qu'observer la ressource distante.	Bureau à distance Assistance à distance
RDP	Windows	**Contrôle** : dans ce mode, vous pourrez visualiser la ressource distante et y effectuer des opérations. **Remarque** Si RDP est désactivé dans les paramètres du système d'exploitation de la ressource, une fenêtre pop-up s'affiche. Utilisez cette fenêtre pour activer RDP pour la ressource, pour la session en cours ou en général : • Si vous souhaitez activer RDP pour cette ressource uniquement pour la session en cours, sélectionnez **Désactiver après la fin de la session**, puis cliquez sur **Autoriser**. • Si vous souhaitez activer RDP pour cette ressource, cliquez sur **Autoriser**.	Bureau à distance
Partage d'écran Apple	macOS	**Contrôle** : dans ce mode, vous pourrez observer la ressource distante et y effectuer des opérations. **Affichage seul** - Dans ce mode, vous ne pourrez qu'observer la ressource distante. **Rideau** : disponible uniquement pour les ressources macOS. Si vous vous connectez à la ressource distante en mode rideau, l'affichage de la ressource distante est	Bureau à distance Assistance à distance

Protocole	Connexions à distance à	Mode d'affichage	Action à distance prise en charge
		assombri et l'utilisateur distant ne pourra pas voir vos actions sur la ressource.	

6. Selon que Client Connect est installé ou pas sur votre ressource, effectuez l'une des opérations suivantes :
   - Si Client Connect n'est pas installé, téléchargez-le, installez-le, puis sélectionnez **Autoriser** dans la fenêtre de confirmation qui s'affiche.
   - Si Client Connect est déjà installé, cliquez sur **Ouvrir le client Connect** dans la fenêtre de confirmation qui s'affiche.
7. Dans la fenêtre **Authentification**, sélectionnez une option d'authentification, puis indiquez les identifiants nécessaires.

Remarque
Si vous avez affecté des identifiants à la ressource, l'authentification est automatique et cette étape est ignorée. Pour plus d'informations, voir "Affectation d'identifiants à une ressource" (p. 1068).

Option d'authentification	Description
Avec identifiants de la ressource distante	Vous serez autorisé à établir la connexion à distance après avoir indiqué le nom d'utilisateur et le mot de passe d'un utilisateur administrateur de la ressource distante. Cette option est disponible pour NEAR, RDP et Partage d'écran Apple. Vous pouvez utiliser cette option pour vous authentifier lors d'une connexion Bureau ou assistance à distance.
Demander l'autorisation d'observation	Vous pourrez établir la connexion à distance en mode d'observation lorsque l'utilisateur connecté sur la ressource distante l'aura autorisée. Cette option est disponible pour NEAR et Partage d'écran Apple. Vous pouvez utiliser cette option pour vous authentifier lors d'une connexion de type assistance à distance.
Demander l'autorisation de contrôle	Vous pourrez établir la connexion à distance en mode de contrôle lorsque l'utilisateur connecté sur la ressource distante l'aura autorisée. Cette option est disponible pour NEAR et Partage d'écran Apple. Vous pouvez utiliser cette option pour vous authentifier lors d'une connexion de type assistance à distance.

8. Cliquez sur **Connexion**, puis sur la session à afficher (dans le cas où plusieurs sessions utilisateur sont disponibles sur la ressource).
   Client Connect ouvre une nouvelle fenêtre de visionneuse dans laquelle vous pouvez voir le bureau de la ressource distante. La visionneuse dispose d'une barre d'outils comportant d'autres actions que vous pouvez effectuer sur la ressource distante une fois la connexion à distance établie. Pour plus d'informations, voir "Utilisation de la barre d'outils dans la fenêtre de la visionneuse" (p. 1082).

Connexion à une ressource gérée via un client Web

Vous pouvez établir une connexion Bureau à distance à une ressource gérée via un client Web.

Prérequis

- Un quota de service standard est affecté à la ressource.
- Un plan de gestion à distance avec RDP activé est appliqué à la ressource gérée.
- Le protocole RDP est activé sur la ressource gérée.
- Votre navigateur prend en charge HTML5.
- L'authentification à deux facteurs est activée pour votre compte utilisateur dans Acronis Cyber Protect Cloud.

Pour vous connecter à distance à une ressource via un client Web

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur la ressource à laquelle vous souhaitez vous connecter à distance, puis cliquez sur **Bureau à distance** > **Connecter via le client web**.
3. Saisissez l'identifiant et le mot de passe pour accéder à la ressource, puis cliquez sur **Connexion**.

Remarque
Si vous avez affecté des identifiants à la ressource, l'authentification est automatique et cette étape est ignorée. Pour plus d'informations, voir "Affectation d'identifiants à une ressource" (p. 1068).

Transfert de fichiers

Vous pouvez transférer facilement des fichiers entre la ressource locale et une ressource gérée.

Prérequis

- Un plan de gestion à distance disposant du protocole NEAR et sur lequel la fonctionnalité de transfert de fichiers est activée est appliqué à la ressource.
- Le quota Advanced Management est appliqué à la ressource.
- L'authentification à deux facteurs est activée pour votre compte utilisateur dans Acronis Cyber Protect Cloud.

Pour transférer à distance des fichiers entre votre ressource et une ressource gérée

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Cliquez sur la ressource dont vous souhaitez transférer des fichiers.
3. Cliquez sur **Gérer**, puis sur **Transférer des fichiers**.
4. Selon que Client Connect est installé ou pas sur votre ressource, effectuez l'une des opérations suivantes :
   - Si Client Connect n'est pas installé, téléchargez-le, installez-le, puis cliquez sur **Autoriser** dans la fenêtre de confirmation qui s'affiche.
   - Si Client Connect est déjà installé, cliquez sur **Ouvrir le client Connect** dans la fenêtre de confirmation qui s'affiche.
5. Dans la fenêtre **Authentification**, sélectionnez une option d'authentification, puis indiquez les identifiants nécessaires.

Option d'authentification	Description
Avec identifiants de la ressource distante	Vous serez autorisé à établir la connexion à distance après avoir indiqué le nom d'utilisateur et le mot de passe d'un utilisateur administrateur de la ressource distante.
Demander l'autorisation de transfert de fichiers	Vous pourrez transférer des fichiers lorsque l'utilisateur connecté sur la ressource distante l'aura autorisé.

6. Dans la fenêtre **Transfert de fichiers**, parcourez les fichiers et faites-les glisser pour les déposer dans la destination souhaitée.

   Remarque
   Les fichiers de la ressource locale sont répertoriés dans le panneau de gauche et ceux de la ressource distante figurent dans le panneau de droit.
   Lorsqu'un transfert de fichiers commence, il est répertorié dans le panneau **Tâches**.

7. [Facultatif] Si vous souhaitez supprimer les tâches terminées du panneau **Tâches**, cliquez sur **Effacement terminé**.
8. Lorsque tous les transferts sont terminés, fermez la fenêtre.

Réalisation d'actions de contrôle sur les ressources gérées

Vous pouvez gérer une ressource distante en y effectuant des actions de contrôle de base : vider la corbeille, veille, redémarrer, arrêter et déconnecter l'utilisateur distant.

Prérequis

- Un quota de service standard est appliqué à la ressource.
- L'authentification à deux facteurs est activée pour votre compte utilisateur dans Acronis Cyber Protect Cloud.

Vider la corbeille

Pour vider la corbeille sur la ressource distante

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Cliquez sur la ressource sur laquelle vous souhaitez effectuer cette opération.
3. Cliquez sur **Gérer**, puis sur **Vider la corbeille**.
4. Sélectionnez la session utilisateur pour laquelle vous souhaitez effectuer cette action, puis cliquez sur **Vider la corbeille**.

Veille

Pour mettre la ressource distante en veille

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Cliquez sur la ressource sur laquelle vous souhaitez effectuer cette opération.
3. Cliquez sur **Gérer**, puis sur **Veille**.

Redémarrer

Pour redémarrer une ressource distante

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Cliquez sur la ressource sur laquelle vous souhaitez effectuer cette opération.
3. Cliquez sur **Gérer**, puis sur **Redémarrer**.
   - Pour les ressources Windows, sélectionnez si vous souhaitez autoriser l'utilisateur actuellement connecté localement à la ressource à enregistrer les modifications avant le redémarrage de la ressource, sélectionnez l'utilisateur, puis cliquez sur **Redémarrer** à nouveau.
   - Pour les ressources macOS, sélectionnez si vous souhaitez autoriser l'utilisateur actuellement connecté localement à la ressource à enregistrer les modifications avant le redémarrage de la ressource, puis cliquez sur **Redémarrer** à nouveau.
   - Pour les ressources Linux, cliquez sur **Redémarrer**.

Arrêt du système

Pour arrêter une ressource distante

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Cliquez sur la ressource sur laquelle vous souhaitez effectuer cette opération.
3. Cliquez sur **Gérer**, puis sur **Arrêt du système**.
   - Pour les ressources Windows, sélectionnez si vous souhaitez autoriser l'utilisateur actuellement connecté localement à la ressource à enregistrer les modifications avant l'arrêt de la ressource, sélectionnez l'utilisateur, puis cliquez sur **Arrêter** à nouveau.

- Pour les ressources macOS, sélectionnez si vous souhaitez autoriser l'utilisateur actuellement connecté localement à la ressource à enregistrer les modifications avant l'arrêt de la ressource, puis cliquez sur **Arrêter** à nouveau.
- Pour les ressources Linux, cliquez sur **Arrêt du système**.

Déconnecter l'utilisateur distant

Pour déconnecter l'utilisateur d'une ressource distante

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Cliquez sur la ressource sur laquelle vous souhaitez effectuer cette opération.
3. Cliquez sur **Gérer**, puis sur **Déconnecter l'utilisateur distant**.
4. Sélectionnez l'utilisateur que vous souhaitez déconnecter, puis cliquez sur **Déconnexion**.

Surveillance des ressources par transmission de captures d'écran

Vous pouvez surveiller le statut d'une ressource à l'aide de la fonctionnalité de transmission de captures d'écran.

Prérequis

- Un plan de gestion à distance sur lequel la fonctionnalité de transmission de capture d'écran est activée est appliqué à la ressource.
- La version de l'agent de protection est à jour et prend en charge la fonction de transmission des captures d'écran.
- Un quota de service Advanced Management est appliqué à la ressource.
- La ressource est en ligne.
- L'authentification à deux facteurs est activée pour votre compte utilisateur dans Acronis Cyber Protect Cloud.

Surveillance d'une ressource par transmission de captures d'écran

Pour surveiller une ressource par transmission de captures d'écran

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Transmission de captures d'écran**.
2. Cliquez sur la ressource que vous souhaitez ajouter.
3. Sélectionnez la session utilisateur.
4. Sélectionnez l'affichage.
5. Sélectionnez le taux d'actualisation auquel une nouvelle capture d'écran du bureau est prise.
6. Sélectionnez la qualité d'image.
7. Pour télécharger la capture d'écran, cliquez sur l'icône de téléchargement.

Création d'une capture d'écran d'une ressource

Pour effectuer une capture d'écran d'une ressource gérée

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Cliquez sur la ressource dont vous souhaitez effectuer une capture d'écran.
3. Cliquez sur **Gérer**, puis sur **Prendre un instantané du bureau**.
   L'écran **Transmission de captures d'écran** s'ouvre ; la ressource y est présélectionnée. Selon les paramètres du plan de gestion à distance qui est appliqué à la ressource, vous verrez la capture d'écran immédiatement ou une fois que l'utilisateur de la ressource distance aura approuvé la demande.

Observation simultanée de plusieurs ressources gérées

Vous pouvez observer simultanément les bureaux de plusieurs ressources distantes dans une même fenêtre.

Remarque
Le nombre de bureaux que vous pouvez visualiser simultanément dans la fenêtre dépend de la taille de l'écran.

Prérequis

- Le protocole NEAR/Partage d'écran est activé dans les plans de gestion à distance qui sont appliqués aux ressources.
- Un quota de service Advanced Management est appliqué à la ressource.
- L'authentification à deux facteurs est activée pour votre compte utilisateur dans Acronis Cyber Protect Cloud.

Pour observer simultanément plusieurs ressources

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez les ressources que vous souhaitez observer.
3. Cliquez sur **Vue multiple**.
4. Selon que Client Connect est installé ou pas sur votre ressource, effectuez l'une des opérations suivantes :
   - Si Client Connect n'est pas installé, téléchargez-le, installez-le, puis sélectionnez **Autoriser** dans la fenêtre de confirmation qui s'affiche.
   - Si Client Connect est déjà installé, cliquez sur **Ouvrir le client Connect** dans la fenêtre de confirmation qui s'affiche.
5. Dans la fenêtre **Authentification**, sélectionnez une option d'authentification, puis indiquez les identifiants nécessaires.

Option d'authentification	Description
Avec identifiants de la ressource	Vous serez autorisé à établir la connexion à distance après avoir indiqué le nom d'utilisateur et le mot de passe d'un utilisateur

Option d'authentification	Description
distante	administrateur sur la ressource distante.
Demander l'autorisation d'observation	Vous pourrez établir la connexion à distance en mode d'observation lorsque l'utilisateur connecté sur la ressource distante l'aura autorisée.

6. Si vous souhaitez utiliser la même méthode d'authentification et les mêmes identifiants lors de la connexion à toutes les ressources distantes que vous avez sélectionnées à l'étape 2, sélectionnez **Utiliser sur les autres ordinateurs**.
7. Cliquez sur **Connexion**.

   Dans la barre d'outils de la fenêtre Vue multiple, vous pouvez sélectionner un mode d'affichage pour la connexion à une ressource. Cette action ouvre une autre fenêtre de visionneuse pour cette ressource.

Remarque
Si l'une des ressources sélectionnées est hors ligne ou si la version de l'agent qui y est installée est obsolète, cette ressource n'est pas affichée dans la fenêtre Vue multiple.
Toutes les connexions en vue multiple à des ressources distantes sont en mode **Affichage seul**.

Utilisation des ressources non gérées

Les ressources non gérées sont des ressources sur lesquelles l'agent Protection n'est pas installé.

Vous pouvez effectuer les opérations suivantes sur les ressources distantes non gérées :

- Effectuer une connexion de type assistance à distance à l'aide de Acronis Assistance rapide
- Effectuer une connexion de type assistance ou Bureau à distance à l'aide d'une adresse IP
- Transférer des fichiers entre votre ressource et la ressource distante à l'aide de Assistance rapide

Remarque
Pour vous connecter à distance à des ressources non gérées à l'aide de Assistance rapide, vérifiez les éléments suivants :

- Le pack Advanced Management est activé pour votre tenant client.
- L'application Assistance rapide s'exécute sur la ressource distante à laquelle vous souhaitez vous connecter.

Connexion à des ressources non gérées via Acronis Assistance rapide

Vous pouvez utiliser la fonctionnalité Assistance rapide pour vous connecter à distance et à la demande à des ressources non gérées, et fournir une aide ponctuelle.

Prérequis

- Le pack Advanced Management est affecté à votre tenant client.
- L'authentification à deux facteurs est activée pour votre compte utilisateur dans Acronis Cyber Protect Cloud.
- L'utilisateur distant a fourni l'identifiant de ressource et le code d'accès à partir de Assistance rapide.
- L'utilisateur distant a téléchargé et exécuté Acronis Assistance rapide.

Pour établir une connexion de type assistance à distance à une ressource à l'aide de Assistance rapide

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur **Assistance rapide**.
3. Dans la fenêtre **Assistance rapide**, saisissez l'identifiant de ressource que l'utilisateur final vous a donné, puis sélectionnez **Connexion**.
4. Cliquez sur **Connexion**.
5. Selon que Client Connect est installé ou pas sur votre ressource, effectuez l'une des opérations suivantes :
   - Si Client Connect n'est pas installé, téléchargez-le, installez-le, puis sélectionnez **Autoriser** dans la fenêtre de confirmation qui s'affiche.
   - Si Client Connect est déjà installé, cliquez sur **Ouvrir le client Connect** dans la fenêtre de confirmation qui s'affiche.
6. Dans la fenêtre **Authentification**, saisissez le code d'accès.
7. Client Connect ouvre une nouvelle fenêtre de visionneuse dans laquelle vous pouvez voir le bureau de la ressource distante. La visionneuse dispose d'une barre d'outils comportant d'autres actions que vous pouvez effectuer sur la ressource distante une fois la connexion à distance établie. Pour plus d'informations, voir "Utilisation de la barre d'outils dans la fenêtre de la visionneuse" (p. 1082).

Connexion à des ressources non gérées via une adresse IP

Si une ressource non gérée se trouve sur votre réseau local, vous pouvez vous y connecter pour un contrôle ou une assistance à distance à l'aide de son adresse IP. Cette connexion ne nécessite aucun accès Internet.

Prérequis

- Le pack Advanced Management est affecté à votre tenant client.
- L'authentification à deux facteurs est activée pour votre compte utilisateur dans Acronis Cyber Protect Cloud.

Pour établir une connexion de type bureau ou assistance à distance à une ressource à l'aide de son adresse IP

1. Dans la console Cyber Protect, accédez à **Tous les terminaux**.
2. Cliquez sur **Assistance rapide**.
3. Cliquez sur l'onglet **Par adresse IP**.
4. Saisissez l'adresse IP et le port de la ressource.
5. Sélectionnez un protocole de connexion - RDP (ressources Windows) ou Partage d'écran Apple (pour les ressources macOS), en fonction du système d'exploitation de la ressource distante.

   Remarque
   Les connexions via RDP prennent en charge l'action de bureau à distance, et les connexions via Partage d'écran Apple prennent en charge les actions de bureau à distance et d'assistance à distance.

6. Cliquez sur **Connexion**.
7. Dans la fenêtre **Authentification**, indiquez les identifiants nécessaires.

Pour les connexions Partage d'écran Apple, Client Connect ouvrira une nouvelle fenêtre de visualisation dans laquelle vous pourrez voir le bureau de la ressource distante. La visionneuse comporte une barre d'outils avec des actions supplémentaires que vous pouvez effectuer sur la ressource distante après l'établissement de la connexion à distance. Pour plus d'informations, voir "Utilisation de la barre d'outils dans la fenêtre de la visionneuse" (p. 1082).

Transfert de fichiers via Acronis Assistance rapide

Vous pouvez utiliser la fonctionnalité Assistance rapide pour transférer des fichiers entre votre ressource et des ressources non gérées.

Prérequis

- Le pack Advanced Management est affecté à votre tenant client.
- L'authentification à deux facteurs est activée pour votre compte utilisateur dans Acronis Cyber Protect Cloud.
- L'utilisateur distant a téléchargé et exécuté Acronis Assistance rapide.
- L'utilisateur distant a fourni l'identifiant d'ordinateur et le code d'accès à partir de Assistance rapide.

Pour transférer des fichiers à une ressource à l'aide de Assistance rapide

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur **Assistance rapide**.
3. Dans la fenêtre **Assistance rapide**, saisissez l'identifiant de ressource que l'utilisateur final vous a attribué, puis sélectionnez **Transfert de fichiers**.

4. Cliquez sur **Connexion**.
5. Selon que Client Connect est installé ou pas sur votre ressource, effectuez l'une des opérations suivantes :
   - Si Client Connect n'est pas installé, téléchargez-le, installez-le, puis sélectionnez **Autoriser** dans la fenêtre de confirmation qui s'affiche.
   - Si Client Connect est déjà installé, cliquez sur **Ouvrir le client Connect** dans la fenêtre de confirmation qui s'affiche.
6. Dans la fenêtre **Authentification**, saisissez le code d'accès.
7. Dans la fenêtre **Transfert de fichiers**, parcourez les fichiers et faites-les glisser pour les déposer dans la destination souhaitée.

   Remarque
   Les fichiers de la ressource locale sont répertoriés dans le panneau de gauche et ceux de la ressource distante figurent dans le panneau de droit.
   Lorsqu'un transfert de fichiers commence, il est répertorié dans le panneau **Tâches**.

8. [Facultatif] Si vous souhaitez supprimer les tâches terminées du panneau **Tâches**, cliquez sur **Effacement terminé**.
9. Lorsque tous les transferts sont terminés, fermez la fenêtre.

Utilisation de la barre d'outils dans la fenêtre de la visionneuse

Une fois que vous êtes connecté à une ressource distante, vous pouvez utiliser la barre d'outils de la fenêtre de la visionneuse pour effectuer rapidement les différentes actions.

Icône	Description
	**Taille réelle** Adapte le bureau de la ressource distante afin qu'un pixel du bureau distant corresponde à un pixel dans la fenêtre de la visionneuse.
	**Zoom pour ajuster** Adapte le bureau de la ressource distante à la fenêtre de la visionneuse.
	**Verrouiller** et **Déverrouiller l'écran** Affiche un espace réservé sur l'écran de la ressource distante afin que l'utilisateur distant ne voie pas vos actions.
	**Prendre un instantané** Enregistre l'image du bureau du serveur distant dans un fichier local.

Icône	Description
	**Sélectionner l'affichage** Sélectionne l'écran de la ressource distante que vous souhaitez afficher, ainsi que la résolution souhaitée. Disponible pour les connexions de Partage d'écran Apple sur macOS et les connexions NEAR sur n'importe quel système d'exploitation.
	**Qualité d'image** Ajuste la qualité de l'image de l'écran distant du noir et blanc à la plus haute qualité possible sur les connexions de Partage d'écran Apple.
	**Qualité d'image NEAR** Ajuste le ratio qualité/performance sur les connexions NEAR. La partie gauche du curseur (Lisse) donne la priorité aux performances sur la qualité d'image et la partie droite (Net) correspond à la meilleure qualité de l'écran du bureau distant, mais probablement aux pires performances.
	**Envoyer Ctrl+Alt+Suppr** Envoie une séquence Ctrl+Alt+Suppr à la ressource distante. Disponibles pour les ressources Windows et Linux.
	**Transfert de fichiers** Ouvre la fenêtre du Gestionnaire de fichiers afin d'échanger des fichiers entre la ressource distante et la ressource locale. Disponible pour les connexions NEAR.
	**Épingler la barre d'outils** Désactive le masquage automatique de la barre d'outils de la visionneuse. Disponible pour les ressources Windows.
	**Plein écran** Passe en plein écran et adapte la ressource distante afin qu'elle remplisse complètement l'écran local. Disponible pour les ressources Windows.
	**Fermer** Ferme la fenêtre de la visionneuse et met fin à la session de contrôle à distance. Disponible pour les ressources Windows.

Selon le type de connexion, d'autres options peuvent être disponibles lorsque vous cliquez sur l'icône **Autre**.

Option	Description
Commencer l'enregistrement/Arrêter l'enregistrement	Enregistre la session actuelle Bureau à distance. Les enregistrements des sessions sont sauvegardés sous forme de fichiers .crec sur la ressource locale. Vous pouvez ouvrir les fichiers .crec à l'aide de Acronis Client Connect. Disponible pour les connexions NEAR
Synchroniser automatiquement le Presse-papiers	Lorsque cette option est activée, le client synchronise automatiquement votre Presse-papiers local et le Presse-papiers de l'ordinateur distant. Disponible pour les connexions NEAR et Partage d'écran Apple.
Envoyer le Presse-papiers **Obtenir le Presse-papiers**	L'option **Envoyer le Presse-papiers** remplace le contenu du Presse-papiers de l'ordinateur distant par le contenu du Presse-papiers local. L'option **Obtenir le Presse-papiers** transfère le contenu du Presse-papiers de l'ordinateur distant au Presse-papiers local.
Clavier intelligent/Touches brutes/Touches brutes avec tous les raccourcis	Change le mode de saisie du clavier de la connexion en cours. **Clavier intelligent** : le client transmet les codes Unicode des symboles saisis localement à l'ordinateur distant **Touches brutes** : le client utilise les codes bruts des touches du clavier sur lesquelles vous appuyez. **Touches brutes avec tous les raccourcis** : le client désactive les raccourcis du système local afin qu'ils soient également transmis au système d'exploitation distant.
Activation de clavier lors du survol de la souris	Lorsque cette option est activée, le client ne capture la saisie au clavier que lorsque le curseur de la souris locale est placé sur la fenêtre de la visionneuse. Lorsque cette option est désactivée, le client capture la saisie au clavier dès que sa fenêtre est active.
Afficher les infos de connexion/Masquer les infos de connexion	Lorsque l'option **Afficher les infos de connexion** est sélectionnée, un petit panneau d'informations apparaît sur l'écran du bureau distant et affiche les données les plus essentielles concernant la connexion en cours.
Son distant	Permet au client de rediriger le son depuis l'ordinateur distant vers l'ordinateur local. Disponible pour les connexions NEAR

Option	Description
Préférences	Configurez les paramètres de Client Connect. Pour plus d'informations, voir "Configuration des paramètres Client Connect" (p. 1085).

Enregistrement et lecture de sessions à distance

Vous pouvez enregistrer une session à distance via NEAR sur Acronis Client Connect.

Pour enregistrer une session à distance

1. Dans la barre d'outils de la visionneuse dans Client Connect, cliquez sur **Autre** et sélectionnez **Démarrer l'enregistrement**.
2. Sélectionnez un nom et un emplacement pour l'enregistrement.

   Par défaut, le fichier est nommé avec la date et l'heure en cours ; il se trouve dans le dossier **Documents** du répertoire personnel de l'utilisateur actuel. Lorsque l'enregistrement est actif, la barre d'outils de la **visionneuse** affiche un cercle rouge clignotant dans l'angle supérieur droit de l'écran distant, ainsi que la minuterie d'enregistrement.
3. Pour arrêter l'enregistrement, cliquez sur **Autre**, puis sur **Arrêter l'enregistrement**. Sur un Mac, vous pouvez également cliquer sur **Arrêter** dans la barre d'outils.

   Tous les fichiers .crec créés par Acronis Client Connect seront ouverts par défaut avec Acronis Client Connect.

Pour écouter un enregistrement

1. Localisez le fichier d'enregistrement.
2. Ouvrez-le.

   Le lecteur d'enregistrement de Acronis Client Connect s'ouvre. Notez qu'il n'est pas possible de naviguer dans l'enregistrement. Pour trouver un moment précis dans l'enregistrement, attendez que le lecteur l'atteigne.
3. [Facultatif] Pour régler la vitesse de lecture, utilisez les icônes **<<** et **>>** dans la section des commandes de lecture.

   L'enregistrement est stocké sous la forme d'une séquence d'événements transmis vers et depuis le serveur distant au cours d'une connexion. Cela garantit la meilleure qualité d'enregistrement pour une taille de fichier minimale. Toutefois, cela signifie également qu'il n'est pas possible de naviguer dans l'enregistrement. Pour l'instant, il n'est pas non plus possible de convertir les enregistrements dans un format vidéo.

Configuration des paramètres Client Connect

Après avoir installé Client Connect sur votre ressource, vous pouvez configurer ses paramètres en fonction de vos préférences.

Pour configurer les paramètres de Client Connect

1. Dans le menu Démarrer, recherchez **Client Connect**, puis démarrez-le.
2. Configurez les paramètres dans l'onglet **Général**.

Option	Description
Écrire des journaux détaillés	Sélectionnez cette option pour autoriser Client Connect à écrire des journaux détaillés. Si cette option est désactivée, le client n'écrira que des informations générales dans le fichier journal.
Paramètres proxy	Sélectionnez si vous souhaitez utiliser le proxy système par défaut ou configurer un proxy SOCKSS personnalisé.

3. Configurez les paramètres dans l'onglet **Visionneuse**.

Option	Description
Demander confirmation lors de la fermeture d'une visionneuse	Sélectionnez cette option si vous souhaitez que Client Connect affiche un message de confirmation lorsque vous essayez de fermer la fenêtre de la visionneuse afin d'éviter toute fermeture accidentelle.
Lors de la réduction en icône	Indiquez si vous souhaitez interrompre l'activité de la visionneuse lorsqu'elle est réduite en icône afin de diminuer la charge du processeur.
Lors de l'agrandissement	Indiquez si vous souhaitez activer le mode plein écran lors de l'agrandissement.
Transfert de Presse-papiers	Active l'affichage de l'indicateur de transfert du Presse-papiers dans la fenêtre de la visionneuse lorsque vous copiez ou collez du texte et des images.
Mode clavier	Active l'affichage de l'indicateur du mode de saisie dans le titre de la fenêtre de la visionneuse lorsque des événements à la souris ou au clavier sont envoyés à la machine distante.
Presse-papiers	Sélectionnez **Synchroniser le Presse-papiers automatiquement** afin d'activer la synchronisation automatique du Presse-papiers lorsqu'elle est disponible.
Envoyer les événements de clavier	Choisissez d'utiliser votre saisie au clavier local dès que la fenêtre Client Connect est active ou uniquement lorsque le pointeur de la souris locale la survole.
Couleur d'arrière-plan de la visionneuse	Change la couleur d'arrière-plan de la fenêtre de la visionneuse.
Se reconnecter automatiquement	Sélectionnez **Activer pour automatiser la reconnexion** si vous souhaitez que Client Connect rétablisse automatiquement la connexion si elle a été interrompue.

Option	Description
H.264	Vous pouvez désactiver les décodeurs matériels.
Fermer en veille	Sélectionnez l'intervalle de temps avant la mise en veille une fois la fenêtre de la visionneuse fermée.

4. Configurez les paramètres dans l'onglet **Clavier**.

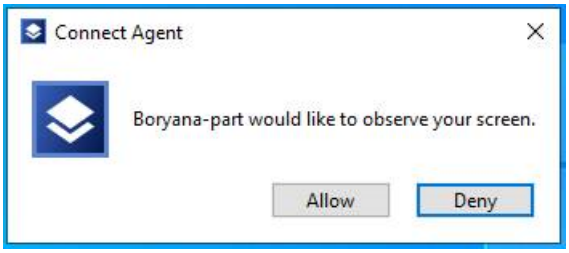
Option	Description
Mappages de modificateurs	Change le comportement des clés de modificateurs à l'aide d'un menu contextuel. Ces paramètres sont enregistrés séparément pour les connexions NEAR, Partage d'écran Apple et RDP.
Mode d'entrée	Pour chaque type de connexion (sélectionné dans l'en-tête du panneau), sélectionnez le mode par défaut de saisie au clavier.

5. Cliquez sur **OK**.

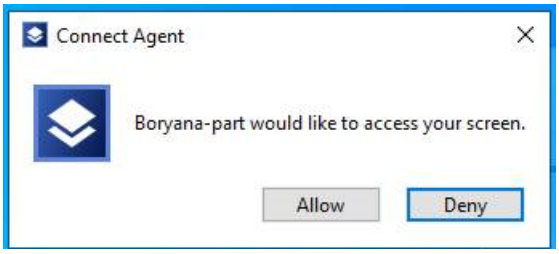
Notificateurs de Bureau à distance

Agent Connect affiche des boîtes de dialogue d'action (notificateurs) sur le bureau de la ressource distante dans les cas suivants :

- lorsque vous essayez de vous connecter à la ressource distante en demandant l'autorisation d'observer. L'utilisateur qui est connecté à la ressource distante localement peut autoriser ou refuser la demande.

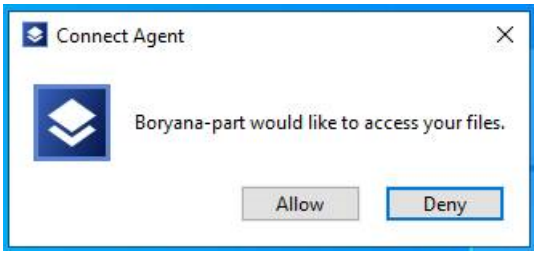


- lorsque vous essayez de vous connecter à la ressource distante en demandant l'autorisation de contrôler. L'utilisateur qui est connecté à la ressource distante localement peut autoriser ou refuser la demande.



- lorsque vous essayez d'échanger des fichiers entre votre ressource et la ressource distante en demandant l'autorisation de transférer des fichiers. L'utilisateur qui est connecté à la ressource

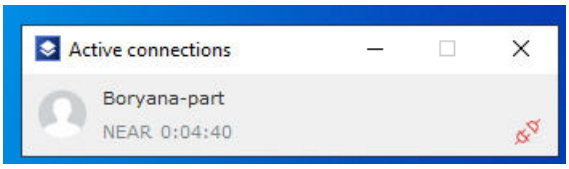
distante localement peut autoriser ou refuser la demande.



Lorsque vous établissez une connexion Bureau à distance à une ressource, l'utilisateur qui est connecté à la ressource recevra une notification de connexion différente contenant les informations suivantes :

- le nom d'utilisateur qui est connecté à distance
- le protocole de connexion qui est utilisé pour établir la connexion à distance
- la durée de la connexion à distance

L'utilisateur qui est connecté à la ressource distante localement peut mettre fin à la connexion à tout moment en cliquant sur l'icône **Déconnecter** ou **Fermer**.



Surveillance de l'intégrité et des performances de la ressource

Vous pouvez surveiller les paramètres système et l'intégrité des ressources de votre organisation. Si un paramètre est hors norme, vous en êtes informé immédiatement et pouvez résoudre le problème rapidement. Vous pouvez également configurer des alertes personnalisées et des mesures d'intervention automatiques. Il s'agit de mesures qui seront réalisées automatiquement pour résoudre les anomalies de comportement de la ressource.

Remarque
La fonctionnalité de surveillance nécessite l'installation de l'agent Protection version 15.0.35324 ou ultérieure sur les ressources.

Plans de surveillance

Pour commencer la surveillance des performances, du matériel, du logiciel, du système et des paramètres de sécurité de vos ressources gérées, appliquez-leur un plan de surveillance. Les plans de surveillance se composent de différents moniteurs que vous pouvez activer et configurer. Certains moniteurs prennent en charge le type de surveillance basé sur une anomalie. Pour plus d'informations sur les plans de surveillance, voir "Plans de surveillance" (p. 1124). Pour plus d'informations sur les moniteurs disponibles que vous pouvez configurer dans les plans de surveillance, reportez-vous à "Moniteurs configurables" (p. 1090).

Si, pour une raison quelconque, l'agent ne peut pas collecter de données d'une ressource, le système génère une alerte.

Types de surveillance

Vous devez configurer le type de surveillance pour chaque moniteur que vous activez dans le plan. Le type de surveillance détermine l'algorithme qu'utilisera le moniteur pour estimer le comportement normal et l'écart de la ressource. Il existe deux types de surveillance : la surveillance basée sur un seuil et celle basée sur une anomalie. Certains moniteurs ne prennent en charge que le type de surveillance basé sur un seuil.

La surveillance basée sur un seuil vérifie si les valeurs des paramètres se trouvent au-dessus ou en dessous d'une valeur de seuil que vous configurez. Grâce à ce type de surveillance, vous avez la charge de définir les valeurs de seuil correctes pour les ressources. Le système détermine le comportement normal en fonction de ces valeurs de seuil statiques, sans prendre en compte d'autres conditions spécifiques qui pourraient provoquer ce comportement. C'est la raison pour laquelle la surveillance basée sur un seuil peut être moins précise que la surveillance basée sur une anomalie.

La surveillance basée sur une anomalie utilise l'apprentissage automatique pour créer les modèles de comportement normal d'une ressource et détecter un comportement anormal. Pour plus d'informations, voir "Surveillance basée sur une anomalie" (p. 1090).

Surveillance basée sur une anomalie

La surveillance basée sur une anomalie utilise les modèles d'apprentissage automatique afin de créer les modèles de comportement normal d'une ressource et de détecter les anomalies (crêtes inattendues dans les données temporelles) dans le comportement de la ressource. Lorsque vous activez ce type de surveillance, le système crée un modèle et démarre son autoformation, puis ajuste le modèle de la ressource spécifique en fonction des données collectées sur la ressource. Cela signifie que, au début de la période de formation, les données risquent de ne pas être totalement pertinentes. La création d'un modèle fiable nécessite au moins trois semaines de formation du modèle. À mesure que le système collecte des données et analyse les ensembles de données historiques, il affine le modèle petit à petit et crée les seuils supérieur et inférieur dynamiques de chaque mesure de la ressource. Ce type de surveillance est plus souple que la surveillance basée sur des seuils, car le système surveille les valeurs des paramètres et leur contexte. Par exemple, il peut être normal qu'une ressource spécifique ait une charge élevée à certaines heures de la journée. Le type de surveillance basée sur les seuils interpréterait par erreur ce comportement comme étant anormal et déclencherait une alerte.

Vous pouvez réinitialiser les modèles d'apprentissage automatique d'une ressource. Dans ce cas, le système supprime toutes les données et tous les modèles des moniteurs appliqués à la ressource. Pour plus d'informations, voir "Réinitialisation des modèles d'apprentissage automatique" (p. 1134).

Plates-formes prises en charge pour la surveillance

La fonctionnalité de surveillance est prise en charge pour les systèmes d'exploitation suivants.

Versions de Windows prises en charge	Versions de macOS prises en charge
• Windows 7 SP1 • Windows 8, 8.1 • Windows 10 • Windows 11 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022	• macOS 10.14 (Mojave) • macOS 10.15 (Catalina) • macOS 11.x (Big Sur) • macOS 12.x (Monterey) • macOS 13.x (Ventura)

Moniteurs configurables

La fonctionnalité de surveillance prend en charge les contrôles suivants, divisés en six catégories : Matériel, Performance, Logiciel, Système, Sécurité et Personnalisé.

Moniteur	Description	Systèmes d'exploitation pris en charge	Fréquence de collecte des données	Prise en charge de la surveillance basée sur une anomalie	Disponibilité dans la protection standard ou dans Advanced Management
Matériel					
Espace disque	Surveille l'espace libre sur un lecteur spécifique de la ressource.	Windows macOS	1 minute	Oui	Protection standard
Température du processeur	Surveille la température du processeur.	Windows macOS	30 s	Oui	Advanced Management
Température du processeur graphique	Surveille la température du processeur graphique.	Windows macOS	30 s	Oui	Advanced Management
Modifications apportées au matériel	Surveille les modifications du matériel (ajout, suppression ou remplacement de matériel) sur une ressource.	Windows macOS	24 heures	Non	Protection standard
Performance					
Utilisation du processeur	Surveille l'utilisation globale du processeur (par tous les processeurs de la ressource).	Windows macOS	30 s	Oui	Advanced Management

Moniteur	Description	Systèmes d'exploitation pris en charge	Fréquence de collecte des données	Prise en charge de la surveillance basée sur une anomalie	Disponibilité dans la protection standard ou dans Advanced Management
Utilisation de la mémoire	Surveille l'utilisation globale de la mémoire (par tous les logements mémoire sur la ressource).	Windows macOS	30 s	Oui	Advanced Management
Vitesse de transfert du disque	Surveille la vitesse de lecture et d'écriture de chaque disque physique sur la ressource.	Windows macOS	30 s	Oui	Advanced Management
Utilisation du réseau	Surveille les trafics entrant et sortant pour chaque carte réseau de la ressource.	Windows macOS	30 s	Oui	Advanced Management
Utilisation du processeur par processus	Surveille l'utilisation du processeur par certains processus.	Windows macOS	30 s	Non	Advanced Management
Utilisation de la mémoire par processus	Surveille l'utilisation de la mémoire par le processus sélectionné.	Windows macOS	30 s	Non	Advanced Management
Vitesse de transfert du	Surveille la vitesse de	Windows macOS	30 s	Non	Advanced Management

Moniteur	Description	Systèmes d'exploitation pris en charge	Fréquence de collecte des données	Prise en charge de la surveillance basée sur une anomalie	Disponibilité dans la protection standard ou dans Advanced Management
disque par processus	lecture et d'écriture du processus sélectionné.				
Utilisation du réseau par processus	Surveille le trafic entrant et sortant du processus sélectionné.	Windows macOS	30 s	Non	Advanced Management
Logiciel					
État du service Windows	Surveille l'état du service Windows sélectionné (en cours d'exécution ou arrêté).	Windows	30 s	Non	Advanced Management
État du processus	Surveille l'état du processus sélectionné (en cours d'exécution ou arrêté).	Windows macOS	30 s	Non	Advanced Management
Logiciel installé	Surveille l'installation, la mise à jour ou la suppression des applications logicielles.	Windows macOS	24 heures	Non	Advanced Management
Système					
Dernier redémarrage du système	Surveille le moment de redémarrage	Windows macOS	1 heure	Non	Protection standard

Moniteur	Description	Systèmes d'exploitation pris en charge	Fréquence de collecte des données	Prise en charge de la surveillance basée sur une anomalie	Disponibilité dans la protection standard ou dans Advanced Management
	de la ressource.				
Journal des événements Windows	Surveille des événements essentiels spécifiques dans les journaux d'événements Windows.	Windows	10 min	Non	Advanced Management
Taille des fichiers et dossiers	Surveille la taille totale des fichiers ou dossiers sélectionnés.	Windows macOS	10 min	Non	Protection standard
Sécurité					
État de Windows Update	Surveille l'état de Windows Update de la ressource et indique si les dernières mises à jour sont installées.	Windows	15 min	Non	Advanced Management
État du pare-feu	Surveille l'état du pare-feu intégré ou tiers qui est installé sur la ressource.	Windows macOS	5 min	Non	Advanced Management
État du logiciel antimalware	Surveille l'état du logiciel antimalware	Windows macOS	5 min	Non	Advanced Management

Moniteur	Description	Systèmes d'exploitation pris en charge	Fréquence de collecte des données	Prise en charge de la surveillance basée sur une anomalie	Disponibilité dans la protection standard ou dans Advanced Management
	intégré ou tiers qui est installé sur la ressource.				
Échecs de connexion	Surveille les tentatives de connexion infructueuses sur la ressource.	Windows	1 heure	Non	Advanced Management
État de l'exécution automatique	Surveille si la fonctionnalité d'exécution automatique pour le support de stockage amovible est activée.	Windows	1 heure	Non	Advanced Management
Personnalisé					
Personnalisé	Surveille les objets personnalisés par l''exécution de scripts.	Windows macOS	personnalisé	Non	Advanced Management

Paramètres du moniteur Espace disque

Le moniteur **Espace disque** surveille l'espace libre sur un lecteur spécifique de la ressource.

Remarque
Lors du calcul de l'espace, le moniteur utilise des octets binaires (1 024 octets par Ko, 1 024 Ko par Mo et 1 024 Mo par Go) pour les ressources Windows et macOS.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Surveillance basée sur un seuil	
Lecteur	Lecteur que vous souhaitez surveiller. Les valeurs suivantes sont disponibles. • **Lecteur système** —Il s'agit de la valeur par défaut. • **N'importe quel lecteur**
Opérateur	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Inférieur à** —Il s'agit de la valeur par défaut. • **Inférieur ou égal à**
Seuil d'espace libre sur le disque	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier dans la plage comprise entre 1 et 100 (%). La valeur par défaut est 20.
Inclure les lecteurs amovibles	Ce paramètre est disponible si la valeur **Lecteur** est **N'importe quel lecteur**. Sélectionnez ce paramètre si vous souhaitez ajouter des lecteurs amovibles tels que des lecteurs flash USB à surveiller. Ce paramètre est désactivé par défaut.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 30.
Surveillance basée sur une anomalie	
Lecteur	Lecteur que vous souhaitez surveiller. Les valeurs suivantes sont disponibles. • **Lecteur système** —Il s'agit de la valeur par défaut. • **N'importe quel lecteur**
Période d'entraînement du modèle	Période pendant laquelle le système formera les modèles d'apprentissage automatique à partir des données collectées auprès des agents, puis créera le modèle de comportement normal de la ressource. Plus l'entraînement du modèle est long, plus le modèle de comportement créé par le système est précis à long terme. Nous vous recommandons de définir un entraînement du modèle d'au moins vingt-et-un jours.

Paramètre	Description
	Saisissez une valeur d'entier (jours). La valeur par défaut est 21.
Recevoir des alertes d'anomalie pendant la période de formation	Si vous sélectionnez ce paramètre, vous recevrez des alertes en cas d'anomalie pendant l'entraînement du modèle. Ces alertes peuvent être erronées, car l'entraînement des modèles est encore en cours et peut manquer de précision. Ce paramètre est sélectionné par défaut.
Niveau de sensibilité	Le niveau de sensibilité agit comme un filtre préliminaire sur les anomalies si leurs valeurs sont comprises dans une plage spécifique. Ce filtre fonctionne indépendamment de l'algorithme de détection des anomalies. Il vise à arrêter le traitement des anomalies comprises dans la plage spécifiée par l'algorithme de détection des anomalies. Pendant la période de formation : 1. L'algorithme est formé à l'aide des données collectées pendant la formation. 2. L'algorithme détecte les anomalies dans les données de formation. 3. Un filtrage basé sur la moyenne et l'écart type est appliqué. 4. Toutes les anomalies détectées dans l'intervalle spécifié sont filtrées. 5. Dans les points de données anormaux restants, l'anomalie avec le niveau le plus faible est sélectionnée. Ce niveau (numéro flottant compris entre 0 et 1) est enregistré dans le modèle. Pendant la prévision : 1. L'algorithme prévoit les anomalies dans les données d'inférence. 2. Les anomalies prévues sont filtrées en fonction de la moyenne et de l'écart type, conformément au niveau de sensibilité. 3. Les anomalies restantes sont filtrées encore en fonction du principe suivant : les valeurs au-dessus du niveau de seuil sont considérées comme des anomalies et celles en dessous du niveau de seuil sont considérées comme ayant un comportement normal. Les valeurs suivantes sont disponibles. • **Bas** : le niveau bas est égal à la valeur de la moyenne et à la valeur de l'écart type. • **Normal** : il s'agit de la valeur par défaut. Le niveau normal est égal à la valeur de la moyenne et à deux fois la valeur de l'écart type. • **Élevé** : le niveau élevé est égal à la valeur de la moyenne et à trois fois la valeur de l'écart type.
Durée de l'anomalie	Le système ne générera une alerte pour une anomalie détectée que si le comportement anormal persiste pendant la période spécifiée. La valeur par défaut est 30 minutes.

Paramètres du moniteur Température du processeur

Le moniteur **Température du processeur** surveille la température du processeur de la ressource.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Surveillance basée sur un seuil	
La température du processeur a dépassé (C°)	Valeur minimale de la mesure surveillée. Si la valeur est dépassée, le système génère une alerte. Saisissez une valeur d'entier (C). La valeur par défaut est 80.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Surveillance basée sur une anomalie	
Période d'entraînement du modèle	Période pendant laquelle le système formera les modèles d'apprentissage automatique à partir des données collectées auprès des agents, puis créera le modèle de comportement normal de la ressource. Plus l'entraînement du modèle est long, plus le modèle de comportement créé par le système est précis à long terme. Nous vous recommandons de définir un entraînement du modèle d'au moins vingt-et-un jours. Saisissez une valeur d'entier (jours). La valeur par défaut est 21.
Niveau de sensibilité	Le niveau de sensibilité agit comme un filtre préliminaire sur les anomalies si leurs valeurs sont comprises dans une plage spécifique. Ce filtre fonctionne indépendamment de l'algorithme de détection des anomalies. Il vise à arrêter le traitement des anomalies comprises dans la plage spécifiée par l'algorithme de détection des anomalies. Pendant la période de formation : 1. L'algorithme est formé à l'aide des données collectées pendant la formation. 2. L'algorithme détecte les anomalies dans les données de formation. 3. Un filtrage basé sur la moyenne et l'écart type est appliqué. 4. Toutes les anomalies détectées dans l'intervalle spécifié sont filtrées. 5. Dans les points de données anormaux restants, l'anomalie

Paramètre	Description
	avec le niveau le plus faible est sélectionnée. Ce niveau (numéro flottant compris entre 0 et 1) est enregistré dans le modèle. Pendant la prévision : 1. L'algorithme prévoit les anomalies dans les données d'inférence. 2. Les anomalies prévues sont filtrées en fonction de la moyenne et de l'écart type, conformément au niveau de sensibilité. 3. Les anomalies restantes sont filtrées encore en fonction du principe suivant : les valeurs au-dessus du niveau de seuil sont considérées comme des anomalies et celles en dessous du niveau de seuil sont considérées comme ayant un comportement normal. Les valeurs suivantes sont disponibles. • **Bas** : le niveau bas est égal à la valeur de la moyenne et à la valeur de l'écart type. • **Normal** : il s'agit de la valeur par défaut. Le niveau normal est égal à la valeur de la moyenne et à deux fois la valeur de l'écart type. • **Élevé** : le niveau élevé est égal à la valeur de la moyenne et à trois fois la valeur de l'écart type.
Durée de l'anomalie	Le système ne générera une alerte pour une anomalie détectée que si le comportement anormal persiste pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 15.

Paramètres du moniteur Température du processeur graphique

Le moniteur **Température du processeur graphique** surveille la température du processeur graphique de la ressource.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Surveillance basée sur un seuil	
La température du processeur graphique a dépassé	Valeur minimale de la mesure surveillée. Si la valeur est dépassée, le système détecte une anomalie. Saisissez une valeur d'entier (C). La valeur par défaut est 80.

Paramètre	Description
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Surveillance basée sur une anomalie	
Période d'entraînement du modèle	Période pendant laquelle le système formera les modèles d'apprentissage automatique à partir des données collectées auprès des agents, puis créera le modèle de comportement normal de la ressource. Plus l'entraînement du modèle est long, plus le modèle de comportement créé par le système est précis à long terme. Nous vous recommandons de définir un entraînement du modèle d'au moins vingt-et-un jours. Saisissez une valeur d'entier (jours). La valeur par défaut est 21.
Niveau de sensibilité	Le niveau de sensibilité agit comme un filtre préliminaire sur les anomalies si leurs valeurs sont comprises dans une plage spécifique. Ce filtre fonctionne indépendamment de l'algorithme de détection des anomalies. Il vise à arrêter le traitement des anomalies comprises dans la plage spécifiée par l'algorithme de détection des anomalies. Pendant la période de formation : 1. L'algorithme est formé à l'aide des données collectées pendant la formation. 2. L'algorithme détecte les anomalies dans les données de formation. 3. Un filtrage basé sur la moyenne et l'écart type est appliqué. 4. Toutes les anomalies détectées dans l'intervalle spécifié sont filtrées. 5. Dans les points de données anormaux restants, l'anomalie avec le niveau le plus faible est sélectionnée. Ce niveau (numéro flottant compris entre 0 et 1) est enregistré dans le modèle. Pendant la prévision : 1. L'algorithme prévoit les anomalies dans les données d'inférence. 2. Les anomalies prévues sont filtrées en fonction de la moyenne et de l'écart type, conformément au niveau de sensibilité. 3. Les anomalies restantes sont filtrées encore en fonction du principe suivant : les valeurs au-dessus du niveau de seuil sont considérées comme des anomalies et celles en dessous du niveau de seuil sont considérées comme ayant un comportement normal. Les valeurs suivantes sont disponibles. • **Bas** : le niveau bas est égal à la valeur de la moyenne et à la valeur de l'écart type. • **Normal** : il s'agit de la valeur par défaut. Le niveau normal est égal à la valeur de la moyenne et à deux fois la valeur de l'écart type.

Paramètre	Description
	• **Élevé** : le niveau élevé est égal à la valeur de la moyenne et à trois fois la valeur de l'écart type.
Durée de l'anomalie	Le système ne générera une alerte pour une anomalie détectée que si le comportement anormal persiste pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 15.

Paramètres du moniteur Modifications apportées au matériel

Le moniteur **Modifications apportées au matériel** surveille les modifications du matériel (ajout, suppression ou remplacement de matériel) sur une ressource.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Composants matériels	Sélectionnez un ou plusieurs composants matériels dont vous souhaitez surveiller les modifications. Les valeurs suivantes sont disponibles. • **Tout** — Il s'agit de la valeur par défaut. • **Carte mère** • **Processeur** • **RAM** • **Disque** • **Processeur graphique** • **Adaptateur réseau**
Que surveiller ?	Spécifiez les modifications pour lesquelles vous souhaitez surveiller les composants matériels sélectionnés. Vous pouvez sélectionner plusieurs éléments dans la liste. Les valeurs suivantes sont disponibles. • **Toute modification** —Il s'agit de la valeur par défaut. • **Nouveaux composants ajoutés** • **Composants remplacés** • **Composants supprimés**

Paramètres du moniteur Utilisation du processeur

Le moniteur **Utilisation du processeur** surveille l'utilisation totale du processeur de la ressource. Si la ressource comprend plusieurs processeurs, l'utilisation totale du processeur correspond à la somme des utilisations de tous les processeurs.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Surveillance basée sur un seuil	
Opérateur	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil d'utilisation du processeur	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier dans la plage comprise entre 1 et 100 (%). La valeur par défaut est 90.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Surveillance basée sur une anomalie	
Période d'entraînement du modèle	Période pendant laquelle le système formera les modèles d'apprentissage automatique à partir des données collectées auprès des agents, puis créera le modèle de comportement normal de la ressource. Plus l'entraînement du modèle est long, plus le modèle de comportement créé par le système est précis à long terme. Nous vous recommandons de définir un entraînement du modèle d'au moins vingt-et-un jours. Saisissez une valeur d'entier (jours). La valeur par défaut est 21.
Recevoir des alertes d'anomalie pendant la période de formation	Si vous sélectionnez ce paramètre, vous recevrez des alertes en cas d'anomalie pendant l'entraînement du modèle. Ces alertes peuvent être erronées, car l'entraînement des modèles est encore en cours et peut manquer de précision. Ce paramètre est sélectionné par défaut.
Niveau de sensibilité	Le niveau de sensibilité agit comme un filtre préliminaire sur les anomalies si leurs valeurs sont comprises dans une plage spécifique. Ce filtre fonctionne indépendamment de l'algorithme de détection des anomalies. Il vise à arrêter le traitement des anomalies comprises dans la plage spécifiée par l'algorithme de détection des anomalies. Pendant la période de formation :

Paramètre	Description
	1. L'algorithme est formé à l'aide des données collectées pendant la formation. 2. L'algorithme détecte les anomalies dans les données de formation. 3. Un filtrage basé sur la moyenne et l'écart type est appliqué. 4. Toutes les anomalies détectées dans l'intervalle spécifié sont filtrées. 5. Dans les points de données anormaux restants, l'anomalie avec le niveau le plus faible est sélectionnée. Ce niveau (numéro flottant compris entre 0 et 1) est enregistré dans le modèle. Pendant la prévision : 1. L'algorithme prévoit les anomalies dans les données d'inférence. 2. Les anomalies prévues sont filtrées en fonction de la moyenne et de l'écart type, conformément au niveau de sensibilité. 3. Les anomalies restantes sont filtrées encore en fonction du principe suivant : les valeurs au-dessus du niveau de seuil sont considérées comme des anomalies et celles en dessous du niveau de seuil sont considérées comme ayant un comportement normal. Les valeurs suivantes sont disponibles. • **Bas** : le niveau bas est égal à la valeur de la moyenne et à la valeur de l'écart type. • **Normal** : il s'agit de la valeur par défaut. Le niveau normal est égal à la valeur de la moyenne et à deux fois la valeur de l'écart type. • **Élevé** : le niveau élevé est égal à la valeur de la moyenne et à trois fois la valeur de l'écart type.
Durée de l'anomalie	Le système ne générera une alerte pour une anomalie détectée que si le comportement anormal persiste pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 15.

Paramètres du moniteur Utilisation de la mémoire

Le moniteur **Utilisation de la mémoire** surveille l'utilisation totale de la mémoire par tous les modules de mémoire de la ressource.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Surveillance basée sur un seuil	
Opérateur	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles.

Paramètre	Description
	• **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil d'utilisation de la mémoire	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier dans la plage comprise entre 1 et 100 (%). La valeur par défaut est 90.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Surveillance basée sur une anomalie	
Période d'entraînement du modèle	Période pendant laquelle le système formera les modèles d'apprentissage automatique à partir des données collectées auprès des agents, puis créera le modèle de comportement normal de la ressource. Plus l'entraînement du modèle est long, plus le modèle de comportement créé par le système est précis à long terme. Nous vous recommandons de définir un entraînement du modèle d'au moins vingt-et-un jours. Saisissez une valeur d'entier (jours). La valeur par défaut est 21.
Recevoir des alertes d'anomalie pendant la période de formation	Si vous sélectionnez ce paramètre, vous recevrez des alertes en cas d'anomalie pendant l'entraînement du modèle. Ces alertes peuvent être erronées, car l'entraînement des modèles est encore en cours et peut manquer de précision. Ce paramètre est sélectionné par défaut.
Niveau de sensibilité	Le niveau de sensibilité agit comme un filtre préliminaire sur les anomalies si leurs valeurs sont comprises dans une plage spécifique. Ce filtre fonctionne indépendamment de l'algorithme de détection des anomalies. Il vise à arrêter le traitement des anomalies comprises dans la plage spécifiée par l'algorithme de détection des anomalies. Pendant la période de formation : 1. L'algorithme est formé à l'aide des données collectées pendant la formation. 2. L'algorithme détecte les anomalies dans les données de formation. 3. Un filtrage basé sur la moyenne et l'écart type est appliqué. 4. Toutes les anomalies détectées dans l'intervalle spécifié sont filtrées.

Paramètre	Description
	5. Dans les points de données anormaux restants, l'anomalie avec le niveau le plus faible est sélectionnée. Ce niveau (numéro flottant compris entre 0 et 1) est enregistré dans le modèle. Pendant la prévision : 1. L'algorithme prévoit les anomalies dans les données d'inférence. 2. Les anomalies prévues sont filtrées en fonction de la moyenne et de l'écart type, conformément au niveau de sensibilité. 3. Les anomalies restantes sont filtrées encore en fonction du principe suivant : les valeurs au-dessus du niveau de seuil sont considérées comme des anomalies et celles en dessous du niveau de seuil sont considérées comme ayant un comportement normal. Les valeurs suivantes sont disponibles. • **Bas** : le niveau bas est égal à la valeur de la moyenne et à la valeur de l'écart type. • **Normal** : il s'agit de la valeur par défaut. Le niveau normal est égal à la valeur de la moyenne et à deux fois la valeur de l'écart type. • **Élevé** : le niveau élevé est égal à la valeur de la moyenne et à trois fois la valeur de l'écart type.
Durée de l'anomalie	Le système ne générera une alerte pour une anomalie détectée que si le comportement anormal persiste pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 30 minutes.

Paramètres du moniteur Vitesse de transfert du disque

Le moniteur **Vitesse de transfert du disque** surveille la vitesse de lecture et d'écriture de chaque disque physique sur la ressource.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Surveillance basée sur un seuil	
Que surveiller ?	Sélectionnez la vitesse que vous souhaitez surveiller. Les valeurs suivantes sont disponibles. • **Vitesse de lecture et d'écriture**. Il s'agit de la valeur par défaut. • **Vitesse de lecture** • **Vitesse d'écriture**
Opérateur de la vitesse de lecture	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur.

Paramètre	Description
	Les valeurs suivantes sont disponibles. • **Supérieur à**. Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil de la vitesse de lecture	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Ko/s). La valeur par défaut est 0 Ko/s.
Période de la vitesse de lecture	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Opérateur de la vitesse d'écriture	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil de la vitesse d'écriture	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Ko/s). La valeur par défaut est 0 Ko/s.
Période de la vitesse d'écriture	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Surveillance basée sur une anomalie	
Période d'entraînement du modèle	Période pendant laquelle le système formera les modèles d'apprentissage automatique à partir des données collectées auprès des agents, puis créera le modèle de comportement normal de la ressource. Plus l'entraînement du modèle est long, plus le modèle de comportement créé par le système est précis à long terme. Nous vous recommandons de définir un entraînement du modèle d'au moins vingt-et-un jours. Saisissez une valeur d'entier (jours). La valeur par défaut est 21.

Paramètre	Description
Recevoir des alertes d'anomalie pendant la période de formation	Si vous sélectionnez ce paramètre, vous recevrez des alertes en cas d'anomalie pendant l'entraînement du modèle. Ces alertes peuvent être erronées, car l'entraînement des modèles est encore en cours et peut manquer de précision. Ce paramètre est sélectionné par défaut.
Que surveiller ?	Sélectionnez la vitesse que vous souhaitez surveiller. Les valeurs suivantes sont disponibles. • **Vitesse de lecture et d'écriture**. Il s'agit de la valeur par défaut. • **Vitesse de lecture** • **Vitesse d'écriture**
Niveau de sensibilité	Le niveau de sensibilité agit comme un filtre préliminaire sur les anomalies si leurs valeurs sont comprises dans une plage spécifique. Ce filtre fonctionne indépendamment de l'algorithme de détection des anomalies. Il vise à arrêter le traitement des anomalies comprises dans la plage spécifiée par l'algorithme de détection des anomalies. Pendant la période de formation : 1. L'algorithme est formé à l'aide des données collectées pendant la formation. 2. L'algorithme détecte les anomalies dans les données de formation. 3. Un filtrage basé sur la moyenne et l'écart type est appliqué. 4. Toutes les anomalies détectées dans l'intervalle spécifié sont filtrées. 5. Dans les points de données anormaux restants, l'anomalie avec le niveau le plus faible est sélectionnée. Ce niveau (numéro flottant compris entre 0 et 1) est enregistré dans le modèle. Pendant la prévision : 1. L'algorithme prévoit les anomalies dans les données d'inférence. 2. Les anomalies prévues sont filtrées en fonction de la moyenne et de l'écart type, conformément au niveau de sensibilité. 3. Les anomalies restantes sont filtrées encore en fonction du principe suivant : les valeurs au-dessus du niveau de seuil sont considérées comme des anomalies et celles en dessous du niveau de seuil sont considérées comme ayant un comportement normal. Les valeurs suivantes sont disponibles. • **Bas** : le niveau bas est égal à la valeur de la moyenne et à la valeur de l'écart type. • **Normal** : il s'agit de la valeur par défaut. Le niveau normal est égal à la valeur de la moyenne et à deux fois la valeur de l'écart type. • **Élevé** : le niveau élevé est égal à la valeur de la moyenne et à trois fois

Paramètre	Description
	la valeur de l'écart type.
Durée de l'anomalie (Vitesse de lecture)	Le système ne générera une alerte pour une anomalie détectée que si le comportement anormal persiste pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 25.
Durée de l'anomalie (Vitesse d'écriture)	Le système ne générera une alerte pour une anomalie détectée que si le comportement anormal persiste pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 25.

Paramètres du moniteur Utilisation du réseau

Le moniteur **Utilisation du réseau** surveille les trafics entrant et sortant pour chaque carte réseau de la ressource.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Surveillance basée sur un seuil	
Direction du trafic	Direction du trafic que vous souhaitez surveiller. Les valeurs suivantes sont disponibles. • **Trafics entrant et sortant**. Il s'agit de la valeur par défaut. • **Trafic entrant** • **Trafic sortant**
Opérateur du trafic entrant	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil du trafic entrant	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Ko/s). La valeur par défaut est 0 Ko/s.
Période du trafic	Le système ne générera une alerte pour un problème détecté que si la

Paramètre	Description
entrant	valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Opérateur du trafic sortant	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil du trafic sortant	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Ko/s). La valeur par défaut est 0 Ko/s.
Période du trafic sortant	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Surveillance basée sur une anomalie	
Période d'entraînement du modèle	Période pendant laquelle le système formera les modèles d'apprentissage automatique à partir des données collectées auprès des agents, puis créera le modèle de comportement normal de la ressource. Plus l'entraînement du modèle est long, plus le modèle de comportement créé par le système est précis à long terme. Nous vous recommandons de définir un entraînement du modèle d'au moins vingt-et-un jours. Saisissez une valeur d'entier (jours). La valeur par défaut est 21.
Recevoir des alertes d'anomalie pendant la période de formation	Si vous sélectionnez ce paramètre, vous recevrez des alertes en cas d'anomalie pendant l'entraînement du modèle. Ces alertes peuvent être erronées, car l'entraînement des modèles est encore en cours et peut manquer de précision. Ce paramètre est sélectionné par défaut.
Direction du trafic	• **Trafics entrant et sortant**. Il s'agit de la valeur par défaut. • **Trafic entrant** • **Trafic sortant**
Niveau de	Le niveau de sensibilité agit comme un filtre préliminaire sur les

Paramètre	Description
sensibilité	anomalies si leurs valeurs sont comprises dans une plage spécifique. Ce filtre fonctionne indépendamment de l'algorithme de détection des anomalies. Il vise à arrêter le traitement des anomalies comprises dans la plage spécifiée par l'algorithme de détection des anomalies. Pendant la période de formation : 1. L'algorithme est formé à l'aide des données collectées pendant la formation. 2. L'algorithme détecte les anomalies dans les données de formation. 3. Un filtrage basé sur la moyenne et l'écart type est appliqué. 4. Toutes les anomalies détectées dans l'intervalle spécifié sont filtrées. 5. Dans les points de données anormaux restants, l'anomalie avec le niveau le plus faible est sélectionnée. Ce niveau (numéro flottant compris entre 0 et 1) est enregistré dans le modèle. Pendant la prévision : 1. L'algorithme prévoit les anomalies dans les données d'inférence. 2. Les anomalies prévues sont filtrées en fonction de la moyenne et de l'écart type, conformément au niveau de sensibilité. 3. Les anomalies restantes sont filtrées encore en fonction du principe suivant : les valeurs au-dessus du niveau de seuil sont considérées comme des anomalies et celles en dessous du niveau de seuil sont considérées comme ayant un comportement normal. Les valeurs suivantes sont disponibles. • **Bas** : le niveau bas est égal à la valeur de la moyenne et à la valeur de l'écart type. • **Normal** : il s'agit de la valeur par défaut. Le niveau normal est égal à la valeur de la moyenne et à deux fois la valeur de l'écart type. • **Élevé** : le niveau élevé est égal à la valeur de la moyenne et à trois fois la valeur de l'écart type.
Durée de l'anomalie (entrante)	Le système ne générera une alerte pour une anomalie détectée que si le comportement anormal persiste pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 25.
Durée de l'anomalie (sortante)	Le système ne générera une alerte pour une anomalie détectée que si le comportement anormal persiste pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 25.

Paramètres du moniteur Utilisation du processeur par processus

Le moniteur **Utilisation du processeur par processus** surveille l'utilisation du processeur par le processus sélectionné. Si plusieurs instances d'un même processus sont présentes, le système surveille l'utilisation totale par toutes ces instances et génère une alerte lorsque les conditions sont remplies.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Nom du processus	Nom du processus que vous souhaitez surveiller. Saisissez le nom du processus, sans l'extension.
Opérateur	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier dans la plage comprise entre 1 et 100 (%). La valeur par défaut est 90.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.

Paramètres du moniteur Utilisation de la mémoire par processus

Le moniteur **Utilisation de la mémoire par processus** surveille l'utilisation de la mémoire par le processus sélectionné. Si plusieurs instances d'un même processus sont présentes, le système surveille l'utilisation totale par toutes ces instances et génère une alerte lorsque les conditions sont remplies.

Remarque
Les agents utilisent l'ensemble de travail total des processus (privés et partagés) pour estimer la taille de la mémoire utilisée par processus. C'est la raison pour laquelle les informations affichées dans le widget peuvent indiquer une taille de mémoire utilisée différente de celle affichée dans le Gestionnaire des tâches Windows (ensemble de travail privé).

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Nom du processus	Nom du processus que vous souhaitez surveiller. Saisissez le nom du processus, sans l'extension.
Opérateur	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Ko). La valeur par défaut est 1.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.

Paramètres du moniteur Vitesse de transfert du disque par processus

Le moniteur **Vitesse de transfert du disque par processus** surveille la vitesse de lecture et d'écriture du processus sélectionné. Si plusieurs instances d'un même processus sont présentes, le système surveille l'utilisation totale par toutes ces instances et génère une alerte lorsque les conditions sont remplies.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Nom du processus	Nom du processus que vous souhaitez surveiller. Saisissez le nom du processus, sans l'extension.
Que surveiller ?	Vitesse que vous souhaitez surveiller. Les valeurs suivantes sont disponibles. • **Vitesse de lecture et d'écriture**. Il s'agit de la valeur par défaut. • **Vitesse de lecture** • **Vitesse d'écriture**

Paramètre	Description
Opérateur de la vitesse de lecture	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil de la vitesse de lecture	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Ko/s). La valeur par défaut est 0 Ko/s.
Période de la vitesse de lecture	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Opérateur de la vitesse d'écriture	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil de la vitesse d'écriture	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Ko/s). La valeur par défaut est 0 Ko/s.
Période de la vitesse d'écriture	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.

Paramètres du moniteur Utilisation du réseau par processus

Le moniteur **Utilisation du réseau par processus** surveille les trafics entrant et sortant du processus sélectionné. Si plusieurs instances d'un même processus sont présentes, le système surveille l'utilisation totale par toutes ces instances et génère une alerte lorsque les conditions sont remplies pour toutes les instances.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Nom du processus	Nom du processus que vous souhaitez surveiller. Saisissez le nom du processus, sans l'extension.
Direction du trafic	Direction du trafic que vous souhaitez surveiller. Les valeurs suivantes sont disponibles. • **Trafics entrant et sortant**. Il s'agit de la valeur par défaut. • **Trafic entrant** • **Trafic sortant**
Opérateur du trafic entrant	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil du trafic entrant	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Ko/s). La valeur par défaut est 0 Ko/s.
Période du trafic entrant	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Opérateur du trafic sortant	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil du trafic sortant	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Ko/s). La valeur par défaut est 0 Ko/s.
Période du	Le système ne générera une alerte pour un problème détecté que si la valeur

Paramètre	Description
trafic sortant	de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.

Paramètres du moniteur de statut du service Windows

Le **statut du service Windows** surveille si le service Windows sélectionné est en cours d'exécution ou est arrêté.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Nom du service	Nom du service Windows que vous souhaitez surveiller. Vous pouvez sélectionner un nom de service dans la liste des services Windows. La liste répertorie tous les agents du tenant après l'analyse réussie de l'inventaire logiciel sur les ressources. Vous pouvez également ajouter un nom de service non répertorié. Il s'agit de la seule option disponible si l'analyse de l'inventaire logiciel n'a pas été effectuée sur les ressources.
État du service	Si le service est dans l'état sélectionné, le système génère un événement. Les valeurs suivantes sont disponibles. • **En cours d'exécution** • **Arrêté**—Il s'agit de la valeur par défaut.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 1.

Paramètres du moniteur État du processus

Le moniteur **État du processus** surveille si le processus sélectionné est en cours d'exécution ou est arrêté. Si plusieurs instances d'un même processus sont présentes, le système surveille chaque instance du processus et génère une alerte lorsque les conditions sont remplies pour toutes les instances du processus.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Nom du processus	Nom du processus que vous souhaitez surveiller. Saisissez le nom du fichier exécutable, sans l'extension.
État du	Si le processus est dans l'état sélectionné, le système génère un événement.

Paramètre	Description
processus	Les valeurs suivantes sont disponibles. • **En cours d'exécution** • **Arrêté**—Il s'agit de la valeur par défaut.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 1.

Paramètres du moniteur Logiciel installé

Le moniteur **Logiciel installé** surveille l'installation, les mises à jour ou la suppression des applications logicielles sur la ressource.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Quel logiciel surveiller ?	Spécifiez le logiciel que vous souhaitez surveiller. Les valeurs suivantes sont disponibles. • **N'importe quel logiciel** —Il s'agit de la valeur par défaut. • **Logiciel spécifique**
Noms de logiciel	Ce paramètre devient disponible si vous sélectionnez la valeur **Logiciel spécifique** pour **Quel logiciel surveiller**. Saisissez le nom d'une ou de plusieurs applications logicielles. Vous pouvez sélectionner un nom d'application logicielle dans la liste des services Windows. La liste répertorie tous les agents du tenant après l'analyse réussie de l'inventaire logiciel sur les ressources. Vous pouvez également ajouter un nom d'application logiciel non répertorié. Il s'agit de la seule option disponible si l'analyse de l'inventaire logiciel n'a pas été effectuée sur les ressources.
Statut d'installation	Spécifiez si vous souhaitez surveiller les logiciels installés, non installés ou mis à jour. Les valeurs suivantes sont disponibles. • **Installé** - Il s'agit de la valeur par défaut. Si vous sélectionnez cette valeur, le moniteur génère une alerte lorsqu'une nouvelle application logicielle est installée sur la ressource. • **Mis à jour** : si vous sélectionnez cette valeur, le moniteur génère une alerte lors de la mise à jour d'une application logicielle. • **Non installé** : si vous sélectionnez cette valeur, le moniteur génère une alerte lorsqu'une application logicielle est désinstallée ou non disponible

Paramètre	Description
	sur la ressource.

Paramètres du moniteur Dernier redémarrage du système

Dernier redémarrage du système lors du dernier redémarrage de la ressource.

Vous pouvez configurer le paramètre suivant du moniteur.

Paramètre	Description
La ressource n'a pas été redémarrée pour	Période (en nombre de jours) depuis le dernier redémarrage de la ressource. Si la ressource n'a pas été redémarrée pendant une période plus longue que celle que vous spécifiez, le système génère une alerte. Saisissez une valeur d'entier dans la plage comprise entre 1 et 180 (jours). La valeur par défaut est 30.

Paramètres du moniteur du journal des événements Windows

Le **Journal des événements Windows** surveille des événements critiques spécifiques dans les journaux des événements Windows.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Nom du journal des événements	Sélectionnez un journal des événements dans la liste des journaux des événements Windows disponibles dans l'Observateur d'événements Windows. Les valeurs suivantes sont disponibles. • **N'importe lequel** —Il s'agit de la valeur par défaut. • **Application** • **Sécurité** • **Système**
Source d'événement	Nom de la source d'événement Vous pouvez sélectionner la valeur dans la liste des sources d'événements collectées dans tous les agents du tenant ou saisissez le nom d'une nouvelle source manuellement. Si l'analyse Inventaire du logiciel est désactivée pour le tenant, la liste des sources d'événements est vide.
Mode de correspondance	Vous pouvez spécifier dans ce champ si les paramètres **Identifiants d'événement**, **Type d'événement** et **Description d'événement** doivent être connectés à l'aide de l'opérateur **N'importe lequel** ou **Tout**.

Paramètre	Description
	Les valeurs suivantes sont disponibles. • **N'importe lequel** —Il s'agit de la valeur par défaut. Une alerte est générée uniquement si l'un des critères sélectionnés correspond. • **Tout** — Une alerte est générée uniquement si tous les critères sélectionnés correspondent.
Identifiants d'événement	Saisissez un ou plusieurs identifiants d'événement en les séparant par une virgule. Si le système trouve dans le journal des événements l'un des codes d'événement que vous avez saisis dans ce champ, il génère une alerte.
Type d'événement	Sélectionnez un ou plusieurs types d'événements à surveiller. Les valeurs suivantes sont disponibles. • **N'importe lequel** —Il s'agit de la valeur par défaut. • **Erreur** • **Avertissement** • **Informations** • **Audit de succès** • **Audit d'échec**
Description d'événement	Mots-clés ou expressions spécifiques figurant dans la description d'événement que vous recherchez. Chaque mot-clé ou expression que vous saisissez doit être mis entre guillemets et ils doivent tous être séparés par une virgule. Si le système trouve l'un des mots-clés ou expressions que vous avez saisis, il génère une alerte.
Nombre d'occurrences	Nombre minimal d'occurrences d'un événement dans le journal pendant la période pour que le système génère une alerte. Saisissez une valeur d'entier dans la plage comprise entre 1 et 1 000.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier, puis sélectionnez l'unité : minutes ou heures. La valeur par défaut est 60 minutes.

Paramètres du moniteur Taille des fichiers et dossiers

Le moniteur **Taille des fichiers et dossiers** surveille la taille totale des fichiers ou dossiers sélectionnés.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Fichiers ou dossiers à surveiller	Chemin d'accès aux fichiers ou dossiers que vous souhaitez surveiller. Vous pouvez également spécifier les fichiers ou dossiers que vous souhaitez exclure de la surveillance. Vous pouvez utiliser les caractères génériques suivants. • * — Pour zéro ou plusieurs caractères dans un nom de fichier ou de dossier • ? — Pour exactement un caractère dans un nom de fichier ou de dossier Pour les ressources Windows : • Le chemin d'accès complet doit commencer par la lettre de lecteur, suivie du séparateur :\. • Vous pouvez utiliser une barre oblique ou une barre oblique inverse comme caractère de séparation des chemins d'accès. • Le nom du fichier ou du dossier ne doit pas se terminer par un espace ou un point. Pour les ressources macOS : • Le chemin d'accès complet doit commencer par le répertoire racine. • Vous pouvez utiliser une barre oblique comme caractère de séparation des chemins d'accès. • Le nom du fichier ou du dossier ne doit pas se terminer par un espace ou un point. La spécification d'un emplacement spécifique n'est pas obligatoire pour les filtres d'exclusion. Les fichiers saisis sans emplacement spécifique seront exclus des dossiers surveillés.
Opérateur	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Inférieur à**
Valeur de seuil	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Mo).
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 10 et 60 (min). La valeur par défaut est 10.

Paramètres du moniteur de statut de Windows Update

Le **statut de Windows Update** surveille l'état de Windows Update de la ressource et indique si les dernières mises à jour sont installées.

Si vous activez ce moniteur, le système génère une alerte dans les cas suivants.

- Windows Update est désactivé sur la ressource.
- Windows Update est activé sur la ressource, mais les dernières mises à jour n'ont pas été installées.

Paramètres du moniteur État du pare-feu

Le moniteur **État du pare-feu** surveille l'état du pare-feu intégré ou tiers qui est installé sur la ressource.

Si vous activez ce moniteur, le système génère une alerte dans les cas suivants.

- Le pare-feu intégré du système d'exploitation (Pare-feu Windows Defender ou pare-feu macOS) est désactivé et aucun pare-feu tiers n'est en cours d'exécution.
- Le pare-feu Windows Defender est désactivé pour les réseaux publics.
- Le pare-feu Windows Defender est désactivé pour les réseaux privés.
- Le pare-feu Windows Defender est désactivé pour les réseaux de domaine.

Paramètres du moniteur Échecs de connexion

Le moniteur **Échecs de connexion** surveille les tentatives de connexion infructueuses sur la ressource.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Seuil de tentatives de connexion infructueuses	La valeur de seuil détermine les limites de performances normales de la mesure surveillée. Lorsque la valeur de seuil est dépassée, la valeur est hors norme. Saisissez une valeur d'entier. La valeur par défaut est 60.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 24, puis sélectionnez une unité : heures ou jours. La valeur par défaut est 12.

Paramètres du moniteur État du logiciel antimalware

Le moniteur **État du logiciel antimalware** surveille l'état du logiciel antimalware intégré ou tiers qui est installé sur la ressource.

Si vous activez ce moniteur, le système génère une alerte lorsqu'il identifie l'une des conditions suivantes.

- Le logiciel antimalware n'est pas installé sur la ressource.
- Le logiciel antimalware est installé, mais n'est pas en cours d'exécution.
- Le logiciel antimalware est installé et est en cours d'exécution, mais les définitions de malware ne sont pas à jour.

Remarque
Cette condition est vérifiée pour les systèmes d'exploitation Windows et Windows Server.

Système d'exploitation	Logiciel antimalware pris en charge
Windows	• Acronis Cyber Protect • Windows Defender • Symantec Endpoint Security • Norton 360 • Norton Antivirus • SentinelOne • Trend Micro Endpoint Security with Apex One • Trend Micro Worry-Free Business • McAfee Endpoint Security • McAfee Endpoint Protection for SMB • FireEye Endpoint Security • F-Secure SAFE • F-Secure Client Security • CrowdStrike Falcon • Kaspersky Endpoint Security Cloud • BitDefender Antivirus • Sophos Intercept X Endpoint • Avast Business Antivirus • AVG Antivirus Business Edition • AVG Internet Security Business Edition • Panda Endpoint Protection • Tencent PC Manager • Webroot Business Endpoint Protection • ESET Endpoint Security

Système d'exploitation	Logiciel antimalware pris en charge
	• Avira Antivirus • Comodo Internet Security • Comodo Business Antivirus • K7 Business Security • K7 Total Security • Vipre Endpoint Protection • Total AV
Windows Server	• Acronis Cyber Protect • Windows Defender • ESET Endpoint Security **Remarque** Le moniteur peut fonctionner avec d'autres plateformes antimalware, mais cela n'est pas garanti.
macOS	• Acronis Cyber Protect • F-Secure Safe • BitDefender Anti-virus for Mac • Sophos Home • Sophos Endpoint Protection • Avast Security for Mac • AVG AntiVirus for Mac • Webroot SecureAnywhere • ESET Cybersecurity • Avira Antivirus for Mac • Comodo Antivirus for Mac • K7 Antivirus for Mac • Vipre Advanced Security • Total AV for Mac **Remarque** Le moniteur peut fonctionner avec d'autres plateformes antimalware, mais cela n'est pas garanti.

Paramètres du moniteur État de la fonctionnalité d'exécution automatique

Le moniteur **État de la fonctionnalité d'exécution automatique** surveille si la fonctionnalité d'exécution automatique pour le support amovible est activée.

Pour des raisons de sécurité, nous vous recommandons de désactiver sur la ressource la fonctionnalité d'exécution automatique pour le support amovible. Si la fonctionnalité est activée, le système génère une alerte.

Paramètres du moniteur personnalisé

Le moniteur **Personnalisé** surveille les objets personnalisés par l'exécution d'un script.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Script à exécuter	Liste des scripts prédéfinis dans le référentiel de scripts.
Planification	Heure d'exécution du script et (facultatif) conditions supplémentaires devant être remplies pour que le script s'exécute. Les valeurs suivantes sont disponibles. • **Planifier selon l'horaire** — Le script s'exécute à l'heure exacte, les jours, les semaines ou les mois que vous indiquez. Il s'agit de la valeur par défaut. **Type de planification** — **Par heure**, **Par jour** ou **Par mois** **Exécuter sur une plage de dates** — Plage d'exécution du script. • **Lorsque l'utilisateur se connecte au système** — Le script s'exécute lorsqu'un utilisateur se connecte à la ressource. • **Lorsque l'utilisateur se connecte au système** — Le script s'exécute lorsqu'un utilisateur se déconnecte de la ressource. • **Au démarrage du système** — Le script s'exécute au démarrage du système d'exploitation de la ressource. • **Lorsque le système est arrêté** — Le script s'exécute à l'arrêt de la ressource. • **Lorsque le système est en ligne** — Le script s'exécute lorsque la ressource devient disponible en ligne. **Conditions de démarrage** — La tâche est effectuée à un moment ou à un événement spécifié uniquement si la condition est remplie. Si plusieurs conditions sont sélectionnées, toutes doivent être remplies simultanément pour permettre le démarrage de la tâche. Par défaut, la condition **Empêcher l'activation du mode veille ou veille prolongée pour démarrer une tâche planifiée** est sélectionnée. **Si les conditions de démarrage ne sont pas remplies, exécutez quand même la tâche par la suite** — Par défaut, cette condition est activée. La valeur par défaut est 1 heure.
Compte pour l'exécution du script	Compte sur lequel s'exécutera le script. Les valeurs suivantes sont disponibles.

Paramètre	Description
	• **Compte système** — Il s'agit de la valeur par défaut. • **Compte actuellement connecté**
Durée maximale	Période maximale pendant laquelle le script peut s'exécuter sur la ressource. Si le script ne se termine pas pendant cette période, l'opération échoue. Saisissez une valeur d'entier dans la plage comprise entre 1 et 1 440 (minutes). La valeur par défaut est 3 minutes.
Stratégie d'exécution PowerShell	Stratégie d'exécution PowerShell. Les valeurs suivantes sont disponibles. • **Undefined** • **AllSigned** • **Bypass** — Il s'agit de la valeur par défaut. • **RemoteSigned** • **Restricted** • **Unrestricted** Pour plus d'informations sur ces valeurs, reportez-vous à la documentation Microsoft.

Plans de surveillance

Les plans de surveillance sont des plans que vous appliquez aux ressources que vous gérez afin d'activer et de configurer la fonctionnalité de surveillance.

Si aucun plan de surveillance n'est appliqué à une ressource, les fonctionnalités de surveillance ne seront pas disponibles pour la ressource.

Remarque
La disponibilité des paramètres que vous pouvez configurer dans le plan de surveillance dépend du pack de service appliqué au tenant. Pour accéder à tous les paramètres, activez le pack Advanced Management.

Création d'un plan de surveillance

Vous pouvez créer un plan de surveillance, puis ajouter des ressources afin de configurer la fonctionnalité de surveillance sur les ressources gérées.

Prérequis

La version de l'agent installée sur la ressource prend en charge la fonctionnalité de surveillance.

Pour créer un plan de surveillance

À partir de Plans de surveillance

1. Dans la console Protection, accédez à **Gestion** > **Plans de surveillance**.
2. Créez un plan de surveillance en utilisant l'une des deux options.
   - Si la liste ne comprend aucun plan de surveillance, cliquez sur **Créer**.
   - Si la liste comprend des plans de surveillance, cliquez sur **Création d'un plan**.
3. Dans la fenêtre **Créer un plan de surveillance**, effectuez l'une des opérations suivantes, selon que le pack Advanced Management est activé, ou pas, pour votre tenant :
   - Si le tenant utilise la protection standard, les quatre moniteurs suivants sont ajoutés automatiquement au plan de surveillance : Espace disque, Modifications apportées au matériel, Dernier redémarrage du système et Taille des fichiers et dossiers.
   - Si le pack Advanced Management est activé pour votre tenant, sélectionnez l'une des options de modèle, puis cliquez sur **Suivant**.

Option	Description
Recommandé	Sélectionnez cette option pour créer un plan de surveillance avec la configuration de surveillance par défaut.
Personnalisé	Utilisez cette option pour créer un plan de surveillance de toutes pièces.

4. [Facultatif] Pour modifier le nom par défaut du plan, cliquez sur l'icône en forme de crayon, saisissez le nom du plan, puis cliquez sur **OK**.
5. [Facultatif] Pour ajouter un moniteur au plan, cliquez d'abord sur **Ajouter un moniteur**, puis sur le moniteur dans la liste et enfin sur **Ajouter**.

   Remarque
   Les paramètres du moniteur sont renseignés automatiquement avec les valeurs par défaut. Vous pouvez ajouter à un plan de surveillance jusqu'à trois moniteurs du même type et jusqu'à 30 moniteurs au total.

6. [Facultatif] Dans l'écran Paramètres de moniteur, modifiez les paramètres par défaut du moniteur et des alertes, puis cliquez sur **Terminé**.

   Remarque
   Vous pouvez configurer différents paramètres pour chaque moniteur. Pour plus d'informations, voir "Moniteurs configurables" (p. 1090) et "Configuration des alertes de surveillance" (p. 1135).

7. [Facultatif] Pour supprimer un moniteur, cliquez sur l'icône de la corbeille, puis cliquez sur **Supprimer**.
8. [Facultatif] Pour ajouter des ressources au plan :
   a. Cliquez sur **Ajouter des ressources**.
   b. Sélectionnez les ressources, puis cliquez sur **Ajouter**.
   c. Si vous avez des problèmes de compatibilité à résoudre, suivez la procédure décrite dans "Résolution des problèmes de compatibilité avec les plans de surveillance" (p. 1133).

9. Cliquez sur **Créer**.

À partir de tous les terminaux

1. Dans la console Protection, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur la ressource à laquelle vous souhaitez appliquer un plan de surveillance.
3. Cliquez sur **Protection**.
4. Selon qu'un plan de surveillance est appliqué, ou pas, à la ressource, effectuez l'une des opérations suivantes :
   - Si un plan de surveillance est déjà appliqué à la ressource, cliquez sur **Création d'un plan**, puis sélectionnez **Surveillance**.
   - Si aucun plan de surveillance n'est appliqué à la ressource, cliquez sur **Ajouter un plan**, puis sur **Création d'un plan**, puis sélectionnez **Surveillance**.
5. Dans la fenêtre **Créer un plan de surveillance**, sélectionnez l'une des options de modèle, puis cliquez sur **Suivant**.

Option	Description
Recommandé	Sélectionnez cette option pour créer un plan de surveillance avec la configuration de surveillance par défaut.
Personnalisé	Utilisez cette option pour créer un plan de surveillance de toutes pièces.

6. [Facultatif] Pour modifier le nom par défaut du plan, cliquez sur l'icône en forme de crayon, saisissez le nom du plan, puis cliquez sur **OK**.
7. [Facultatif] Si vous souhaitez modifier les paramètres par défaut du moniteur et des alertes, configurez les nouvelles valeurs, puis cliquez sur **Terminé**.

   Remarque
   Vous pouvez ajouter à un plan de surveillance jusqu'à trois moniteurs du même type et jusqu'à 30 moniteurs au total.

8. [Facultatif] Dans l'écran Paramètres de moniteur, modifiez les paramètres par défaut du moniteur et des alertes, puis cliquez sur **Terminé**.

   Remarque
   Vous pouvez configurer différents paramètres pour chaque moniteur. Pour plus d'informations, voir "Moniteurs configurables" (p. 1090) et "Configuration des alertes de surveillance" (p. 1135).

9. [Facultatif] Pour supprimer un moniteur, cliquez sur l'icône de la corbeille, puis cliquez sur **Supprimer**.
10. Cliquez sur **Créer**.

Ajout de ressources à des plans de surveillance

En fonction de vos besoins, vous pouvez ajouter des ressources à un plan de surveillance après sa création.

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- La version de l'agent installée sur la ressource prend en charge la fonctionnalité de surveillance.
- Un plan de surveillance au moins est disponible.

Pour ajouter une ressource à un plan de surveillance

À partir de Plans de surveillance

1. Dans la console Protection, accédez à **Gestion** > **Plans de surveillance**.
2. Cliquez sur le plan de surveillance.
3. Selon que le plan est déjà appliqué, ou pas, à une ressource, effectuez l'une des opérations suivantes :
   - Cliquez sur **Ajouter des ressources**, si le plan n'a encore été appliqué à aucune ressource.
   - Cliquez sur **Gérer les ressources** si le plan n'a été appliqué à aucune ressource.
4. Sélectionnez une ressource dans la liste, puis cliquez sur **Ajouter**.
5. Cliquez sur **Enregistrer**.
6. Si nécessaire, cliquez sur **Confirmer** pour appliquer le quota de service requis à la ressource.

À partir de Tous les terminaux

1. Dans la console Protection, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur la ressource à laquelle vous souhaitez appliquer un plan de surveillance.
3. Cliquez sur **Protection**.
4. Recherchez le plan de surveillance auquel vous souhaitez ajouter la ressource, puis cliquez sur **Appliquer**.
5. Si nécessaire, cliquez sur **Confirmer** pour appliquer le quota de service requis à la ressource.

Révocation de plans de surveillance

Vous pouvez révoquer un plan de surveillance d'une ressource à laquelle le plan a été appliqué.

Prérequis

Un plan de surveillance au moins est appliqué à la ressource.

Pour révoquer un plan de surveillance

1. Dans la console Protection, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur la ressource, puis sur **Protection**.
3. Cliquez sur l'icône **Plus d'actions** du plan de surveillance que vous souhaitez révoquer, puis sur **Révoquer**.

Configuration des mesures d'intervention automatiques

Les mesures d'intervention automatiques sur les événements indiqués dans les alertes sont des actions ou des mesures prédéfinies qui sont déclenchées automatiquement en réponse à des événements ou des incidents détectés. Ces actions sont conçues pour limiter les menaces potentielles et réduire des dommages.

Vous pouvez configurer une ou plusieurs mesures d'intervention automatiques sur les événements indiqués dans les alertes. Le nombre maximal de mesures d'intervention automatiques par moniteur est de 20.

Pour configurer des mesures d'intervention automatiques

1. Dans la console Protection, accédez à **Gestion** > **Plans de surveillance**.
2. Sélectionnez le plan de surveillance pour lequel vous souhaitez configurer des mesures d'intervention automatiques.
3. Sélectionnez le moniteur dans lequel vous souhaitez configurer des mesures d'intervention automatique ou, si vous n'avez pas encore ajouté de moniteurs, cliquez sur **Ajouter un moniteur**, sélectionnez le moniteur souhaité dans la liste, cliquez sur **Ajouter**, puis sélectionnez le moniteur.
4. Cliquez sur le lien situé à côté de **Mesures d'intervention automatiques**.
5. Dans la fenêtre **Mesures d'intervention automatiques**, ajoutez une ou plusieurs mesures d'intervention qui devront s'exécuter automatiquement lors du déclenchement d'une alerte.
6. Configurez chaque mesure d'intervention automatique. Par exemple, si vous avez ajouté la mesure d'intervention automatique **Démarrer un service Windows**, procédez comme suit :
   a. À côté de **Service Windows**, cliquez sur **Spécifier**.
   b. Dans le champ **Service**, sélectionnez un service pour démarrer une mesure d'intervention.
   c. Cliquez sur **Valider**.
7. Dans la liste de toutes les mesures d'intervention ajoutées, utilisez les flèches Haut et Bas ou la fonctionnalité de glisser-déposer pour configurer la séquence des mesures d'intervention.
8. Configurez comment gérer des mesures d'intervention successives si la mesure précédente a échoué. Sélectionnez l'une des options suivantes :
   a. **Passer à la mesure d'intervention suivante**.
   b. **Ne pas passer à la mesure d'intervention suivante**.
9. Cliquez sur **Valider**.

Le nombre de mesures configurées figure à côté du paramètre **Mesures d'intervention automatiques** de votre plan de surveillance. Vous pouvez modifier ou supprimer ces mesures, et en ajouter d'autres ultérieurement.

Le tableau suivant répertorie et décrit toutes les mesures d'intervention automatiques disponibles dans les paramètres de moniteur.

Mesure d'intervention automatique	Description	Système d'exploitation pris en charge
Exécuter un script	Si vous ajoutez cette action, vous pouvez effectuer les opérations suivantes : 1. Sélectionnez un script à exécuter sur la ressource. 2. Spécifiez le compte sous lequel vous souhaitez exécuter le script. 3. Spécifiez la durée maximale de l'opération. 4. Spécifiez la stratégie d'exécution PowerShell. 5. Exécutez un script. Pour exécuter cette action, vous avez besoin d'une licence pour le pack Advanced Management pour la ressource (si elle n'est pas encore affectée). Lorsque les conditions sont réunies, le système exécute le script distant sélectionné avec les paramètres spécifiés.	Windows, macOS
Redémarrer la ressource	Lorsque les conditions sont réunies et que vous ajoutez cette action, le système redémarre la ressource à distance.	Windows, macOS
Arrêter le processus	Si vous ajoutez cette action, vous pouvez indiquer le processus à arrêter par l'intermédiaire de la saisie manuelle du nom du processus. Lorsque les conditions sont réunies, le système arrête le processus.	Windows, macOS
Démarrer le service Windows	Si vous ajoutez cette action, vous pouvez sélectionner le service Windows à démarrer depuis la liste dynamique des services que remplissent les agents. Lorsque les conditions sont réunies, le	Windows

Mesure d'intervention automatique	Description	Système d'exploitation pris en charge
	système redémarre le service.	
Arrêter le service Windows	Si vous ajoutez cette action, vous pouvez sélectionner le service Windows à arrêter depuis la liste dynamique des services que remplissent les agents. Lorsque les conditions sont réunies, le système arrête le service.	Windows
Activer Windows Update	Lorsque les conditions sont réunies et que vous ajoutez cette action, le système redémarre la ressource à distance. Cette action n'est disponible que pour le moniteur de statut Windows Update.	Windows
Désactiver l'exécution automatique sur les lecteurs amovibles	Lorsque les conditions sont réunies et que vous ajoutez cette action, le système désactive la fonctionnalité d'exécution automatique sur le support de stockage amovible de la ressource. Cette action n'est disponible que pour le moniteur de statut de l'exécution automatique.	Windows

Autres opérations réalisables avec les plans de surveillance

Dans l'écran **Plans de surveillance**, vous pouvez effectuer les opérations supplémentaires suivantes avec les plans de surveillance : afficher les détails, modifier et afficher les activités, afficher, renommer, activer, désactiver, cloner, exporter et supprimer les alertes.

Afficher les détails

Pour afficher les détails d'un plan de surveillance

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Plus d'actions** du plan de surveillance.
2. Cliquez sur **Afficher les détails**.
3. [Facultatif] Si vous souhaitez afficher les détails d'un moniteur activé dans le plan, cliquez sur le nom du moniteur.

Modifier

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour modifier un plan

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Plus d'actions** du plan de surveillance.
2. Cliquez sur **Modifier**.
3. [Facultatif] Pour supprimer un moniteur du plan, cliquez sur l'icône de la corbeille, à droite du nom du moniteur.
4. [Facultatif] Pour activer ou désactiver un moniteur dans le plan, utilisez le bouton bascule à côté du nom du moniteur.
5. [Facultatif] Pour modifier les paramètres de moniteur, procédez comme suit.
   a. Cliquez sur le nom du moniteur.
   b. Cliquez sur la vue d'ensemble des paramètres de moniteur.
   c. Dans l'écran **Paramètres de moniteur**, configurez les paramètres, puis cliquez sur **Terminé**.

      Remarque
      Vous pouvez configurer différents paramètres pour chaque moniteur. Pour plus d'informations, voir "Moniteurs configurables" (p. 1090) et "Configuration des alertes de surveillance" (p. 1135).

   d. Fermez l'écran et confirmez les modifications.
6. [Facultatif] Pour ajouter un moniteur, cliquez sur **Ajouter un moniteur**, puis, si nécessaire, modifiez les paramètres en suivant les explications de l'étape précédente.
7. Cliquez sur **Enregistrer**.

Activités

Pour afficher les activités relatives à un plan de surveillance

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Plus d'actions** du plan de surveillance.
2. Cliquez sur **Activités**.
3. Cliquez sur une activité pour visualiser plus de détails la concernant.

Alertes

Pour afficher les alertes

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Plus d'actions** du plan de surveillance.
2. Cliquez sur **Alertes**.

Renommer

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour renommer un plan de surveillance

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Plus d'actions** du plan de surveillance.
2. Cliquez sur **Renommer**.

3. Saisissez le nouveau nom du plan, puis cliquez sur **OK**.

Activer

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Le plan de surveillance est appliqué à au moins une ressource.

Pour activer un plan de surveillance

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Plus d'actions** du plan de surveillance.
2. Cliquez sur **Activer**.

Désactiver

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour désactiver un plan de surveillance

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Plus d'actions** du plan de surveillance.
2. Cliquez sur **Désactiver**.

Cloner

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour cloner un plan de surveillance

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Plus d'actions** du plan de surveillance.
2. Cliquez sur **Cloner**.
3. Cliquez sur **Créer**.

Exporter

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour exporter un plan de surveillance

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Plus d'actions** du plan de surveillance.
2. Cliquez sur **Exporter**.
   La configuration du plan est exportée au format JSON vers la machine locale.

Supprimer

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour supprimer un plan de surveillance

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Plus d'actions** du plan de surveillance.
2. Cliquez sur **Supprimer**.
3. Sélectionnez **Je confirme**, puis cliquez sur **Supprimer**.

Problèmes de compatibilité avec les plans de surveillance

Dans certains cas, l'application d'un plan de surveillance sur une ressource peut provoquer des problèmes de compatibilité. Vous pouvez observer les problèmes de compatibilité suivants :

- Système d'exploitation incompatible : ce problème survient lorsque le système d'exploitation de la ressource n'est pas pris en charge.
- Agent non pris en charge : ce problème survient lorsque la version de l'agent de protection sur la ressource est obsolète et ne prend pas en charge la fonctionnalité de surveillance.
- Quota insuffisant : ce problème survient lorsque le quota de service dans le tenant est insuffisant pour l'affectation aux ressources sélectionnées.

Si le plan de surveillance est appliqué au maximum à 150 ressources sélectionnées individuellement, vous serez invité à résoudre les conflits existants avant d'enregistrer le plan. Pour résoudre un conflit, supprimez sa cause racine ou les ressources concernées du plan. Pour plus d'informations, voir "Résolution des problèmes de compatibilité avec les plans de surveillance" (p. 1133). Si vous enregistrez le plan sans résoudre les conflits, le plan sera désactivé automatiquement pour les ressources non prises en charge, et des alertes s'afficheront.

Si le plan de surveillance est appliqué à plus de 150 ressources ou à des groupes de terminaux, il sera d'abord enregistré, puis sa compatibilité sera vérifiée. Le plan sera automatiquement désactivé pour les ressources incompatibles, et des alertes apparaîtront.

Résolution des problèmes de compatibilité avec les plans de surveillance

Selon la cause des problèmes de compatibilité, vous pouvez effectuer différentes actions afin de résoudre ces problèmes dans le cadre du processus de création d'un nouveau plan de surveillance.

Pour résoudre les problèmes de compatibilité

1. Cliquez sur **Examiner les problèmes**.
2. [Facultatif] Pour résoudre les problèmes de compatibilité liés à des systèmes d'exploitation incompatibles par suppression de ressources du plan :
   a. Dans l'onglet **Système d'exploitation incompatible**, sélectionnez les ressources que vous souhaitez supprimer.

b. Cliquez sur **Supprimer les ressources du plan**.

c. Cliquez sur **Supprimer**, puis sur **Fermer**.

3. [Facultatif] Pour résoudre les problèmes de compatibilité liés à des systèmes d'exploitation incompatibles par désactivation d'un moniteur dans le plan :
   a. Dans l'onglet **Système d'exploitation incompatible**, sélectionnez les moniteurs que vous souhaitez supprimer.
   b. Cliquez sur **Désactiver le moniteur**.
   c. Cliquez sur **Désactiver**, puis sur **Fermer**.
4. [Facultatif] Pour résoudre les problèmes de compatibilité d'agents non pris en charge par suppression de ressources du plan :
   a. Dans l'onglet **Agents non pris en charge**, sélectionnez les ressources que vous souhaitez supprimer.
   b. Cliquez sur **Supprimer les ressources du plan**.
   c. Cliquez sur **Supprimer**, puis sur **Fermer**.
5. [Facultatif] Pour résoudre les problèmes de compatibilité d'agents non pris en charge grâce à la mise à jour de la version de l'agent, cliquez sur **Accéder à la liste des agents**.

   Remarque
   Cette option est disponible uniquement pour les administrateurs clients.

6. [Facultatif] Pour résoudre les problèmes de compatibilité liés à un quota insuffisant par suppression de ressources du plan :
   a. Dans l'onglet **Quota insuffisant**, sélectionnez les ressources que vous souhaitez supprimer.
   b. Cliquez sur **Supprimer les ressources du plan**.
   c. Cliquez sur **Supprimer**, puis sur **Fermer**.
7. [Facultatif] Pour résoudre les problèmes de compatibilité liés à un quota insuffisant par augmentation du quota du tenant :
   a. Dans l'onglet **Quota insuffisant**, cliquez sur **Accéder au portail de gestion**.
   b. Augmentez le quota de service du client.

      Remarque
      Cette option est disponible uniquement pour les administrateurs partenaires.

Réinitialisation des modèles d'apprentissage automatique

Vous pouvez réinitialiser les modèles d'une ressource lorsqu'ils deviennent obsolètes ou invalides. Cette action supprime les modèles créés et les données collectées pour la ressource par les surveillance basée sur une anomalie, puis démarre de toutes pièces la formation des modèles d'apprentissage automatique pour la ressource.

Pour réinitialiser les modèles d'apprentissage automatique pour une ressource

1. Dans la console Protection, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur une ressource dans la liste, puis sur l'onglet **Détails**.
3. Dans la section **Réinitialiser les modèles d'apprentissage automatique**, cliquez sur **Réinitialiser**.
4. Dans la fenêtre de confirmation, cliquez de nouveau sur **Réinitialiser**.

Alertes de surveillance

Les alertes de surveillance sont affichées dans la console Protection et sont envoyées par e-mail lorsque le comportement surveillé des ressources est hors norme. Les alertes garantissent que les parties prenantes sont informées dans les meilleurs délais en cas de problème dans l'environnement informatique de l'organisation.

Remarque
Pour activer les alertes de surveillance via e-mail, vous devez configurer au moins une stratégie de notification par e-mail pour le type d'alerte correspondant. Pour plus d'informations, voir "Configuration des stratégies de notification par e-mail" (p. 1143).

Configuration des alertes de surveillance

Vous pouvez configurer les paramètres d'alerte du moniteur lorsque vous ajoutez un moniteur à un plan de surveillance ou que vous modifiez un moniteur déjà disponible dans un plan de surveillance.

Pour configurer des alertes de surveillance

1. Dans la fenêtre **Paramètres de moniteur**, accédez à la section **Générer des alertes**.
2. Dans **Gravité de l'alerte**, sélectionnez la gravité correspondant à la priorité de l'alerte.

Option	Description
Critique	Ces alertes ont la priorité la plus élevée et concernent des problèmes critiques qui ont un impact sur le fonctionnement de la ressource. Résolvez ces problèmes dès que possible.
Erreur	Une alerte d'erreur est moins grave et indique que quelque chose ne marche pas ou ne se comporte pas normalement. Résolvez les problèmes à temps pour éviter qu'ils provoquent des difficultés plus graves.
Avertissement	Une alerte d'avertissement indique qu'il existe une condition que vous devez connaître, mais qui ne devrait pas créer de problème pour l'instant. Résolvez ces problèmes après avoir réglé ce qui provoque des alertes critiques ou d'erreur. Il s'agit de la valeur par défaut.

Option	Description
Infomations	Ces alertes ont la priorité la plus faible. La gravité Informations n'indique pas de problème. Ces alertes fournissent des informations sur les actions associées à un objet surveillé.

3. Dans **Fréquence des alertes**, sélectionnez le mode de génération d'une alerte lorsque la condition est remplie.

Option	Description
Une seule fois jusqu'à la réussite de la vérification	Le système génère une alerte une fois la vérification terminée avec succès. Il s'agit de la valeur par défaut.
Après X échecs consécutifs	Le système génère une alerte après X tentatives consécutives infructueuses, X étant une valeur d'entier.

4. Dans **Message d'alerte**, cliquez sur l'icône représentant un crayon pour modifier le message par défaut qui sera utilisé par le système lors de la génération de l'alerte. Vous pouvez spécifier un message d'alerte personnalisé qui contient des variables. Pour plus d'informations sur les variables que vous pouvez utiliser, reportez-vous à "Variables des alertes de surveillance" (p. 1136).

   Remarque
   Vous pouvez configurer plusieurs messages d'alerte pour certains des moniteurs.

5. Activez **Résolution automatique des alertes** si vous souhaitez que le système résolve automatiquement l'alerte lorsque la mesure surveillée revient à l'état normal et que le comportement est à nouveau normal. Ce paramètre est activé par défaut.

Variables des alertes de surveillance

Vous pouvez configurer différentes variables d'alerte pour les différents moniteurs. Pour utiliser une variable, vous devez la mettre entre {{}}.

Le tableau suivant fournit plus d'informations sur les variables disponibles.

Variable	Description	Disponible pour le moniteur
plan_name	Nom de la stratégie	Tous les moniteurs
monitor_name	Nom de la sous-stratégie du plan de surveillance	Tous les moniteurs
workload_ name	Nom de la ressource	Tous les moniteurs
threshold_	Conditions spécifiques de surveillance ou seuils	Tous les moniteurs

Variable	Description	Disponible pour le moniteur
value	de génération d'une alerte	prenant en charge la surveillance basée sur un seuil.
threshold_unit	Unité associée à la valeur de seuil. Par exemple, %, Mo ou Mo/s.	Tous les moniteurs prenant en charge la surveillance basée sur un seuil.
time_period	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée.	Tous les moniteurs prenant en charge la surveillance basée sur un seuil.
time_unit	Unité qui sera associée à la période (s/min/heures/jour).	Tous les moniteurs prenant en charge la surveillance basée sur un seuil.
anomaly_value	Valeur d'anomalie	Tous les moniteurs prenant en charge la surveillance basée sur une anomalie.
anomaly_unit	Unité qui sera associée à la valeur d'anomalie	Tous les moniteurs prenant en charge la surveillance basée sur une anomalie.
deviation_value	Valeur d'écart	Tous les moniteurs prenant en charge la surveillance basée sur une anomalie.
deviation_unit	Unité qui sera associée à la valeur d'écart	Tous les moniteurs prenant en charge la surveillance basée sur une anomalie.
drive_name	Lecteur pour Windows ou partition pour macOS	Espace disque,
CPU_model	Modèle du processeur surveillé	Température du processeur
GPU_model	Modèle du processeur graphique surveillé	Température du processeur graphique
hardware_	Modèle du composant surveillé	Modifications apportées

Variable	Description	Disponible pour le moniteur
model		au matériel
hardware_component	Type du matériel surveillé	Modifications apportées au matériel
hardware_model_old	Modèle du composant surveillé qui a été remplacé	Modifications apportées au matériel
hardware_model_new	Modèle du nouveau composant surveillé qui a été ajouté	Modifications apportées au matériel
disk_model	Modèle du disque	Vitesse de transfert du disque
network_adapter_model	Modèle de la carte réseau	Utilisation du réseau
process_name	Nom du processus	Utilisation du processeur par processus Utilisation de la mémoire par processus Vitesse de transfert du disque par processus Utilisation du réseau par processus État du processus
service_name	Nom du service	État du service Windows
software_name	Nom de l'application logicielle	Logiciel installé
software_version	Version de l'application logicielle	Logiciel installé
software_version_old	Version de l'application logicielle avant la mise à jour	Logiciel installé
software_version_new	Version de la nouvelle application logicielle ou de l'application mise à jour	Logiciel installé
number_of_occurrences	Nombre d'occurrences d'un événement dans le journal	Journal des événements Windows
event_types	Type de l'événement	Journal des événements Windows

Variable	Description	Disponible pour le moniteur
event_source	Source de l'événement	Journal des événements Windows
event_log_ name	Nom de l'événement	Journal des événements Windows
firewall_ software_name	Nom du logiciel du pare-feu	État du pare-feu
antimalware_ software_name	Nom du logiciel antimalware	État du logiciel antimalware
user_name	Nom de l'utilisateur	État de la fonctionnalité d'exécution automatique
script_name	Nom du script	Personnalisé

Mesures d'intervention manuelles

Lorsque vous voyez une alerte, vous pouvez sélectionner une mesure d'intervention que vous souhaitez prendre sur les événements figurant dans les alertes.

Pour réaliser une mesure d'intervention manuelle

1. Dans la console Protection, accédez à **Alertes**.
2. Ouvrez l'alerte que vous souhaitez afficher.
3. Cliquez sur **Mesure d'intervention**, puis sélectionnez une mesure d'intervention dans la liste déroulante.

La liste des mesures d'intervention disponibles pour une alerte particulière dépend du type d'alerte, de la disponibilité des fonctionnalités pour un tenant particulier et du système d'exploitation de la ressource.

Pour information, le tableau suivant répertorie et décrit toutes les mesures d'intervention manuelles.

Mesure d'intervention manuelle	Description	Système d'exploitation pris en charge
Parcourir la tendance d'utilisation de l'espace disque	Ouvre une fenêtre comportant le graphique **Utilisation de l'espace disque** dans laquelle vous pouvez effectuer les opérations suivantes : • Consulter l'évolution dans le temps de l'utilisation de l'espace disque (pendant	Windows, macOS

Mesure d'intervention manuelle	Description	Système d'exploitation pris en charge
	le dernier jour/les 7 derniers jours/le dernier mois). • Consulter la différence d'utilisation de l'espace disque en valeur relative (%) pendant la période sélectionnée.	
Parcourir la tendance d'augmentation de la taille des fichiers	Ouvre une fenêtre comportant le graphique **Augmentation de la taille des fichiers** dans laquelle vous pouvez effectuer les opérations suivantes : • Consulter l'évolution dans le temps de la taille totale des fichiers et dossiers surveillés (pendant le dernier jour/les 7 derniers jours/le dernier mois). • Consulter la différence de la taille totale des fichiers en valeur relative (%) pendant la période sélectionnée.	Windows, macOS
Exécuter un script	Ouvre une fenêtre dans laquelle vous pouvez effectuer les opérations suivantes : 1. Sélectionnez un script à exécuter sur la ressource. 2. Spécifiez le compte sous lequel vous souhaitez exécuter le script. 3. Spécifiez la durée maximale de l'opération. 4. Spécifiez la stratégie d'exécution PowerShell. 5. Exécutez un script. Pour exécuter cette action, vous avez besoin d'une licence pour le pack Advanced Management pour la ressource (si elle n'est pas encore affectée).	Windows, macOS
Connecter via NEAR	Acronis Client Connect établit une connexion à distance.	Windows, macOS
Connecter via RDP	Acronis Client Connect établit une connexion à distance.	Windows
Ouvrir l'inventaire matériel	Vous êtes redirigé vers l'onglet **Inventaire du matériel** de la ressource actuelle.	Windows, macOS

Mesure d'intervention manuelle	Description	Système d'exploitation pris en charge
Parcourir les 10 principaux processus qui ont chargé le processeur	Ouvre une fenêtre avec les 10 principaux processus qui ont chargé le processeur et ont peut-être provoqué sa surchauffe (instantané du système au moment de la génération de l'alerte).	Windows, macOS
Parcourir les 10 principaux processus qui ont chargé le processeur graphique	Ouvre une fenêtre avec les 10 principaux processus qui ont chargé le processeur graphique et ont peut-être provoqué sa surchauffe (instantané du système au moment de la génération de l'alerte).	Windows, macOS
Parcourir les 10 principaux processus qui ont chargé la mémoire	Ouvre une fenêtre avec les 10 principaux processus qui ont chargé la mémoire (instantané du système au moment de la génération de l'alerte).	Windows, macOS
Parcourir les 10 principaux processus qui ont chargé le disque	Ouvre une fenêtre avec les 10 principaux processus qui ont chargé le disque (instantané du système au moment de la génération de l'alerte).	Windows, macOS
Parcourir les 10 principaux processus qui ont chargé le réseau	Ouvre une fenêtre avec les 10 principaux processus qui ont chargé l'adaptateur de l'interface réseau (instantané du système au moment de la génération de l'alerte).	Windows, macOS
Parcourir l'utilisation des ressources par processus	Ouvre une fenêtre comprenant des informations détaillées sur l'utilisation des ressources matérielles par le processus concerné : Utilisation du processeur, utilisation de la mémoire, E/S disque, utilisation du réseau.	Windows, macOS
Redémarrer la ressource	Ouvre une fenêtre de confirmation. Démarre la ressource après la confirmation.	Windows, macOS
Démarrer le service Windows	Ouvre une fenêtre de confirmation. Démarre le service Windows après la confirmation.	Windows
Arrêter le service Windows	Ouvre une fenêtre de confirmation. Arrête le service Windows après la confirmation.	Windows
Stopper le processus	Ouvre une fenêtre de confirmation. Arrête	Windows, macOS

Mesure d'intervention manuelle	Description	Système d'exploitation pris en charge
	le processus auquel l'alerte fait référence après la confirmation.	
Activer Windows Update	Ouvre une fenêtre de confirmation. Active Windows Update après la confirmation.	Windows
Désactiver la fonctionnalité d'exécution automatique sur les lecteurs amovibles	Ouvre une fenêtre de confirmation. Désactive la fonctionnalité d'exécution automatique au niveau du système de la ressource après la confirmation.	Windows

Important
Pour des raisons de sécurité, l'authentification à deux facteurs est nécessaire à la réalisation des mesures d'intervention manuelles suivantes :

- Exécuter un script
- Connecter via NEAR
- Connecter via RDP
- Redémarrer la ressource
- Démarrer le service Windows
- Arrêter le service Windows
- Stopper le processus
- Activer Windows Update
- Désactiver la fonctionnalité d'exécution automatique sur les lecteurs amovibles

Visualisation des alertes de surveillance pour une ressource

Dans l'onglet **Alertes**, vous pouvez voir les alertes de surveillance d'une ressource spécifique et effectuer différentes actions.

Pour voir les alertes de surveillance d'une ressource

1. Dans la console Protection, accédez à **Tous les terminaux**.
2. Cliquez sur une ressource, puis sélectionnez l'onglet **Alertes**.
3. [Facultatif] Dans le volet d'alerte de surveillance, effectuez l'une des actions suivantes :
   - Pour effacer l'alerte, cliquez sur **Effacer**.
   - Pour prendre une mesure d'intervention, cliquez sur **Mesure d'intervention**, puis sur

l'action.

- Pour contacter l'équipe de support, cliquez sur **Obtenir du support**.

4. [Facultatif] Pour effacer toutes les alertes de surveillance concernant la ressource, cliquez sur **Tout effacer**.

Affichage du journal des alertes de surveillance

Vous pouvez voir tous les événements associés à une alerte de surveillance, classés dans l'ordre chronologique : les mesures d'interventions (automatiques ou manuelles) réalisées, ainsi que les notifications par e-mail envoyées.

Pour afficher le journal d'audit d'une alerte de surveillance

1. Dans la console Protection, accédez à **Alertes**.
2. Ouvrez l'**affichage tableau**.
3. Dans la liste des alertes, clique sur l'alerte de surveillance que vous souhaitez afficher.
4. Cliquez sur **Détails**, puis sur **Journal des alertes**.

Configuration des stratégies de notification par e-mail

Les stratégies de notification par e-mail spécifient les utilisateurs qui recevront des notifications par e-mail envoyées par les différents moniteurs.

Dans l'écran **Notifications par e-mail**, vous pouvez effectuer les actions suivantes avec les stratégies de notification par e-mail : ajout, modification, activation, désactivation et suppression.

Ajouter

Pour ajouter une nouvelle stratégie de notification

1. Dans la console Protection, accédez à **Paramètres** > **Notifications par courrier électronique**.
2. Cliquez sur **Ajouter une stratégie**.
3. Cliquez sur **Sélectionner les destinataires**.
4. Dans l'écran **Sélectionner les destinataires**, sélectionnez les utilisateurs devant recevoir des alertes par e-mail, puis cliquez sur **Sélectionner**.
5. Dans **Types d'alerte**, sélectionnez les moniteurs pour lesquels vous souhaitez que le système envoie des alertes par e-mail.
6. Cliquez sur **Ajouter**.

Modifier

Pour modifier une stratégie de notification par e-mail

1. Dans la console Protection, accédez à **Paramètres** > **Notifications par courrier électronique**.
2. Cliquez sur l'icône représentant des points de suspension de la stratégie de notification, puis cliquez sur **Modifier**.

3. [Facultatif] Pour changer les destinataires, cliquez sur **Modifier les destinataires**, ajoutez ou supprimez des utilisateurs de la liste, puis cliquez sur **Sélectionner**.
4. [Facultatif] Dans **Types d'alerte**, sélectionnez les types d'alertes de surveillance que vous souhaitez envoyer aux destinataires sélectionnés.
5. Cliquez sur **Enregistrer**.

Activer

Pour activer une stratégie de notification par e-mail

1. Dans la console Protection, accédez à **Paramètres** > **Notifications par courrier électronique**.
2. Dans l'écran **Notifications par e-mail**, cliquez sur l'icône représentant des points de suspension **...** de la stratégie de notification par e-mail.
3. Cliquez sur **Activer**.

Désactiver

Pour désactiver une stratégie de notification par e-mail

1. Dans la console Protection, accédez à **Paramètres** > **Notifications par courrier électronique**.
2. Dans l'écran **Notifications par e-mail**, cliquez sur l'icône représentant des points de suspension **...** de la stratégie de notification par e-mail.
3. Cliquez sur **Désactiver**.

Supprimer

Pour supprimer une stratégie de notification par e-mail

1. Dans la console Protection, accédez à **Paramètres** > **Notifications par courrier électronique**.
2. Dans l'écran **Notifications par e-mail**, cliquez sur l'icône représentant des points de suspension **...** de la stratégie de notification par e-mail.
3. Cliquez sur **Supprimer**, puis sur **Confirmer**.

Visualisation des données des moniteurs

Pour chaque ressource, vous pouvez voir la liste des moniteurs appliqués, l'état actuel des moniteurs et les détails historiques des performances dans une vue graphique. Vous pouvez utiliser ces informations pour analyser l'état de la ressource et l'évolution dans le temps de son état.

Prérequis

- Un plan de surveillance est appliqué à la ressource.
- La ressource est en ligne et comprend des données pour le moniteur correspondant.
- La version de l'agent installée sur la ressource prend en charge les plans de surveillance.

Pour afficher les moniteurs appliqués à une ressource et les données de moniteur

1. Dans la console Protection, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur une ressource, puis sur l'onglet **Surveillance**.

   L'onglet **Surveillance** affiche un widget pour chaque moniteur activé pour la ressource. Chaque widget affiche les informations suivantes.

Informations affichées	Description
Nom du moniteur	Nom du moniteur
Dernier résultat	Valeur la plus récente de la mesure surveillée ou dernier état de l'événement
Dernière vérification	Date et heure de collecte des dernières données par le moniteur
Alertes	Nombre d'alertes générées par le moniteur et restant non résolues. Si le moniteur a généré au moins une alerte qui n'est pas résolue, le fait de cliquer sur le nombre ouvre l'onglet **Alertes**. Les alertes sont filtrées, et seules les alertes de ce moniteur sont répertoriées.

   Remarque
   Les widgets deviennent visibles dans l'onglet 15 minutes (ou à la fréquence minimale définie pour un moniteur) après l'application d'un plan de surveillance à la ressource.

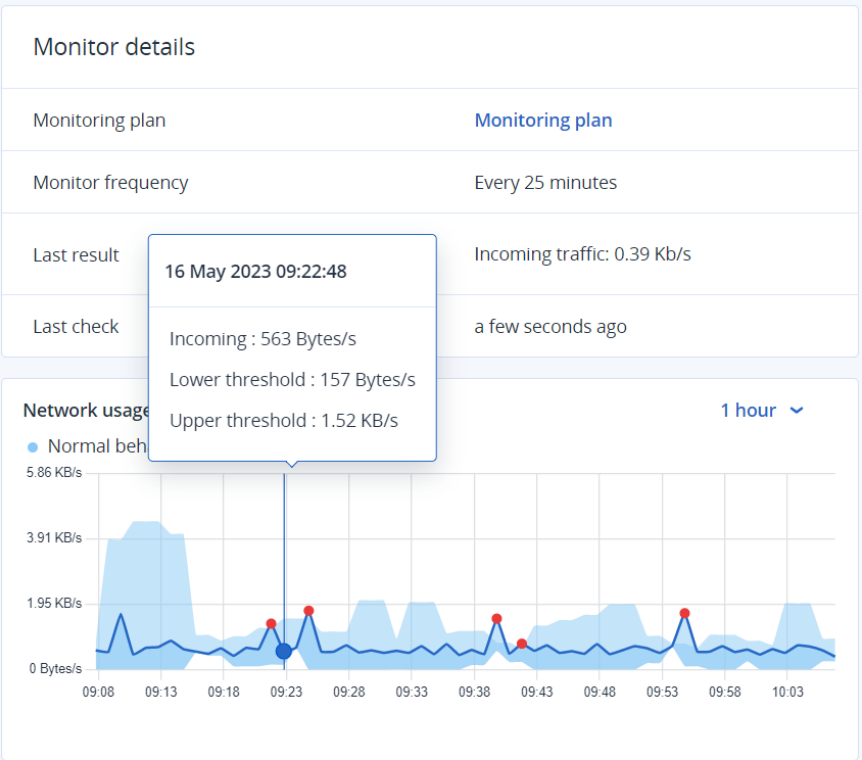
3. [Facultatif] Pour afficher d'autres détails sur le moniteur et, le cas échéant, les données historiques collectées pour la mesure surveillée, cliquez dans le widget du moniteur sur l'icône représentant des points de suspension, puis sur **Détails**.

   Pour plus d'informations sur les paramètres de moniteur que vous pouvez voir dans les widgets, reportez-vous à "Widgets de moniteurs" (p. 1145).

Widgets de moniteurs

Dans le widget de moniteur, vous pouvez consulter les détails suivants concernant le moniteur.

Détail	Description
Plan de surveillance	Nom du plan de surveillance contenant le moniteur. Le nom du plan de surveillance est un lien qui ouvre le plan de surveillance en mode d'affichage.
Fréquence de surveillance	Intervalle de collecte par le moniteur des données de la ressource
Dernier résultat	Valeur la plus récente de la mesure surveillée ou dernier état de l'événement
Dernière vérification	Date et heure de collecte des dernières données par le moniteur

Détail	Description
Dernière alerte	Date et heure de génération de la dernière alerte Le champ ne s'affiche que si une alerte au moins est générée pour le moniteur.
Graphique historique	Pour les moniteurs qui collectent des données de série temporelle, le widget affiche les données historiques d'une période sélectionnée (1 heure, 6 heures, 12 heures, 1 jour, 1 semaine ou 1 mois) dans une vue graphique. Le graphique affiche les valeurs réelles des indicateurs pendant la période que vous sélectionnez. Si, pour une raison quelconque, l'agent n'a pas envoyé les données collectées au cloud, les valeurs manquantes sont affichées sous forme de ligne en pointillé qui relie les points de données aux valeurs réelles qui précèdent et suivent la valeur manquante. Pour les moniteurs qui utilisent la surveillance **basée sur les anomalies**, le graphique affiche la zone des valeurs de référence, c'est-à-dire une ligne qui indique les valeurs réelles de l'indicateur, ainsi que les anomalies. Les anomalies correspondent aux pics ou aux valeurs en dehors des valeurs de référence, et elles sont affichées sur le graphique sous la forme de points rouges. Si vous survolez le graphique, vous voyez la valeur réelle et les valeurs de seuil d'une durée spécifique.  **Remarque** Les données affichées sur les graphiques sont affichées dans le fuseau horaire du système local. Il s'agit du fuseau horaire du navigateur de la ressource à partir de laquelle vous accédez à la console Protection.

Autres outils Cyber Protection

Mode de conformité

Le mode Conformité est conçu pour les clients ayant des exigences de sécurité élevées. Ce mode exige un chiffrement obligatoire pour toutes les sauvegardes et n'autorise que les mots de passe de chiffrement définis localement.

Avec le mode Conformité, toutes les sauvegardes créées dans un tenant client et dans ses unités sont chiffrées automatiquement avec l'algorithme AES et une clé de chiffrement 256 bits. Les utilisateurs peuvent définir leur mot de passe de chiffrement uniquement sur les terminaux protégés et ne peuvent pas les définir dans les plans de protection.

Important
Vous ne pouvez pas désactiver le mode Conformité.

Limites

- Le mode Conformité n'est compatible qu'avec les agents de la version 15.0.26390 ou supérieure.
- Le mode Conformité n'est pas disponible pour les terminaux exécutant Red Hat Enterprise Linux 4.x ou 5.x et leurs dérivés.
- Les services cloud ne peuvent pas accéder aux mots de passe de chiffrement. En raison de cette limitation, certaines fonctionnalités ne sont pas disponibles pour les tenants en mode Conformité.

Fonctionnalités non prises en charge

Les fonctionnalités suivantes ne sont pas disponibles pour les tenants en mode Conformité :

- Restauration depuis la console Cyber Protect
- Navigation de niveau fichier dans les sauvegardes depuis la console Cyber Protect
- Sauvegarde de Cloud à Cloud
- Sauvegarde des sites Web
- Sauvegarde d'applications
- Sauvegarde des terminaux mobiles
- Analyse anti-malware des sauvegardes
- Restauration sûre
- Création automatique de listes blanches d'entreprise
- Carte de la protection des données
- Reprise d'activité après sinistre
- Rapports et tableaux de bord liés aux fonctionnalités non disponibles

Définition du mot de passe de chiffrement

Vous devez définir le mot de passe de chiffrement localement sur le terminal protégé. Vous ne pouvez pas définir le mot de passe de chiffrement dans le plan de protection. Sans mot de passe, la création de sauvegardes échouera.

Avertissement !
Il est impossible de restaurer les sauvegardes chiffrées si vous perdez ou oubliez le mot de passe.

Vous pouvez définir le mot de passe de chiffrement de l'une des manières suivantes :

1. Lors de l'installation de l'agent de protection (pour Windows, macOS et Linux).
2. À l'aide de la ligne de commande (pour Windows et Linux).
   C'est la seule façon de définir un mot de passe de chiffrement sur une appliance virtuelle.
   Pour en savoir plus sur la définition d'un mot de passe de chiffrement avec l'outil **Acropsh**, reportez-vous à "Chiffrement" (p. 462).
3. Dans l'application Moniteur Cyber Protect (pour Windows and macOS).

Pour définir le mot de passe de chiffrement dans Moniteur Cyber Protect

1. Sur le terminal protégé, connectez-vous en tant qu'administrateur.
2. Cliquez sur l'icône du Moniteur Cyber Protect dans la zone de notification (sous Windows) ou dans la barre des menus (sous macOS).
3. Cliquez sur l’icône en forme d’engrenage.
4. Cliquez sur **Chiffrement**.
5. Définissez le mot de passe de chiffrement.
6. Cliquez sur **OK**.

Modification du mot de passe de chiffrement

Vous pouvez modifier le mot de passe de chiffrement avant qu'un plan de protection ne crée la moindre sauvegarde.

Nous vous recommandons de ne pas modifier le mot de passe de chiffrement après la création des sauvegardes, car les sauvegardes ultérieures échoueront. Pour continuer à protéger le même ordinateur, vous devez lui créer un nouveau plan de protection. La modification du mot de passe de chiffrement et du plan de protection permettra la création de sauvegardes chiffrées avec le mot de passe modifié. Les sauvegardes qui ont été créées avant ces modifications ne seront pas affectées.

Si vous préférez, vous pouvez aussi conserver le plan de protection appliqué et modifier uniquement le nom du fichier de sauvegarde qu'il contient. Cela permettra aussi la création de sauvegardes chiffrées avec le mot de passe modifié.Pour en savoir plus sur le nom du fichier de sauvegarde, reportez-vous à "Nom de fichier de sauvegarde" (p. 471).

Vous pouvez modifier le mot de passe de chiffrement de l'une des manières suivantes :

1. Dans l'application Moniteur Cyber Protect (pour Windows and macOS).
2. À l'aide de la ligne de commande (pour Windows et Linux).
   Pour en savoir plus sur la définition d'un mot de passe de chiffrement avec l'outil **Acropsh**, reportez-vous à "Chiffrement" (p. 462).

Restauration de sauvegardes pour les tenants en mode Conformité

En mode Conformité, vous ne pouvez pas restaurer les sauvegardes dans la console Cyber Protect.

Les options suivantes sont disponibles :

- Restauration d'un ordinateur entier, de ses disques ou de ses fichiers à l'aide d'un support de démarrage.
- Extraction de fichiers à partir de sauvegardes locales d'ordinateurs Windows avec l'agent installé, à l'aide de l'Explorateur de fichiers Windows.

Stockage immuable

Grâce au stockage immuable, vous pouvez accéder à des sauvegardes supprimées pendant une période de rétention spécifiée. Vous pouvez restaurer du contenu depuis ces sauvegardes, mais vous ne pouvez ni les modifier, ni les déplacer, ni les supprimer. À la fin de la période de rétention, les sauvegardes supprimées sont définitivement supprimées.

Le stockage immuable contient les sauvegardes suivantes :

- Sauvegardes supprimées manuellement.
- Sauvegardes supprimées automatiquement, conformément aux paramètres de la section **Durée de conservation** d'un plan de protection ou de la section **Règles de rétention** d'un plan de nettoyage.

Les sauvegardes supprimées du stockage immuable utilisent toujours de l'espace de stockage et sont facturées en conséquence.

Les tenants supprimés ne sont facturés pour aucun stockage, pas même le stockage immuable.

Modes de stockage immuable

Pour les tenants de clients, le stockage immuable est disponible dans les modes suivants :

Le stockage immuable est disponible dans les modes suivants :

- **Mode de gouvernance**
  Vous pouvez désactiver et réactiver le stockage immuable. Vous pouvez modifier la période de rétention ou passer en mode de conformité.
- **Mode de conformité**

Avertissement !
La sélection du mode de conformité est irréversible.

Vous ne pouvez pas désactiver le stockage immuable. Vous ne pouvez pas modifier la période de rétention ni revenir au mode de gouvernance.

Stockages et agents pris en charge

- Le stockage immuable n'est pris en charge que pour le stockage dans le cloud.

  Le stockage immuable est disponible pour les stockages dans le cloud hébergés par Acronis et ses partenaires qui utilisent Acronis Cyber Infrastructure version 4.7.1 ou ultérieure.

  Tous les systèmes de stockage pouvant être utilisés avec Acronis Cyber Infrastructure Backup Gateway sont pris en charge. Par exemple, le stockage Acronis Cyber Infrastructure, les stockages Amazon S3 et EC2, et le stockage Microsoft Azure.

  Le stockage immuable nécessite que le port TCP 40440 soit ouvert pour le service Backup Gateway dans Acronis Cyber Infrastructure. Dans les versions 4.7.1 et ultérieure, le port TCP 40440 est automatiquement ouvert avec le type de trafic **public Backup (ABGW)**. Pour plus d'informations sur les types de trafic, consultez la documentation d'Acronis Cyber Infrastructure.
- Le stockage immuable nécessite un agent de protection version 21.12 (15.0.28532) ou ultérieure.
- Seules les sauvegardes TIBX (version 12) sont prises en charge.

Activation du stockage immuable

Vous pouvez configurer les paramètres de stockage immuable dans la console Cyber Protect ou dans le portail de gestion. Les deux permettent d'accéder aux mêmes paramètres. La procédure ci-dessous utilise la console Cyber Protect. Pour savoir comment configurer les paramètres du stockage immuable dans le portail de gestion, voir Configuration du stockage immuable dans le guide de l'administrateur.

La configuration des paramètres de stockage immuable exige l'authentification à deux facteurs dans le tenant à qui le compte administrateur appartient.

Pour activer le stockage immuable

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Réglages** > **Paramètres du système**.
3. Faites défiler la liste des options de sauvegarde par défaut, puis cliquez sur **Stockage immuable**.
4. Activez le commutateur **Stockage immuable**.
5. Spécifiez une période de rétention comprise entre 14 et 3 650 jours.

   Par défaut, la période de rétention est de 14 jours. Une période de rétention plus longue augmentera l'utilisation du stockage.
6. Sélectionnez le mode de stockage immuable, puis confirmez votre choix si vous y êtes invité.

   En mode gouvernance, vous pouvez activer ou désactiver le stockage immuable et modifier la période de rétention. Vous pouvez passer du mode gouvernance au mode conformité.

Avertissement !
Le passage en mode conformité est irréversible. Une fois que vous avez sélectionné le mode conformité, vous ne pouvez plus désactiver le stockage immuable, ni modifier son mode ni sa période de rétention.

7. Cliquez sur **Enregistrer**.
8. Pour qu'une archive existante prenne en charge le stockage immuable, créez une nouvelle sauvegarde dans cette archive.

   Pour créer une nouvelle sauvegarde, exécutez le plan de protection manuellement ou selon une planification.

Avertissement !
Si vous supprimez une sauvegarde avant de configurer l'archive pour qu'elle prenne en charge le stockage immuable, la sauvegarde sera supprimée définitivement.

Désactivation du stockage immuable

Remarque
Vous ne pouvez désactiver le stockage immuable qu'en mode de gouvernance.

Pour désactiver le stockage immuable

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Dans le menu de navigation, cliquez sur **Paramètres** > **Paramètres système**.
3. Faites défiler la liste des options de sauvegarde par défaut, puis cliquez sur **Stockage immuable**.
4. Désactivez le commutateur **Stockage immuable**.
5. Confirmez votre choix en cliquant sur **Désactiver**.

Avertissement !
La désactivation du stockage immuable n'entre pas en vigueur immédiatement. Pendant une période de grâce de 14 jours, le stockage immuable reste actif et vous pouvez accéder aux sauvegardes supprimées pendant leur période de rétention d'origine. À la fin de la période de grâce, toutes les sauvegardes stockées dans le stockage immuable sont définitivement supprimées.

Accès aux sauvegardes supprimées dans le stockage immuable

Pendant la période de rétention, vous pouvez accéder aux sauvegardes supprimées et restaurer des données qu'elles contiennent.

Remarque
Pour permettre l'accès aux sauvegardes supprimées, le port 40440 sur le stockage des sauvegardes doit être activé pour les connexions entrantes.

Pour accéder à une sauvegarde supprimée

1. Dans l'onglet **Stockage de sauvegarde**, sélectionnez le stockage dans le cloud qui contient la sauvegarde supprimée.
2. [Uniquement pour les archives supprimées] Pour voir les archives supprimées, cliquez sur **Afficher les éléments supprimés**.
3. Sélectionnez l'archive qui contient la sauvegarde que vous souhaitez restaurer.
4. Cliquez sur **Afficher les sauvegardes**, puis sur **Afficher les éléments supprimés**.
5. Sélectionnez la sauvegarde que vous voulez restaurer.
6. Effectuez l'opération de récupération décrite dans "Restauration" (p. 518).

Stockage géoredondant

Le stockage géoredondant garantit la durabilité des données en les copiant de manière asynchrone dans un emplacement secondaire, distant géographiquement de l'emplacement principal. Grâce à la géoredondance, vos données restent accessibles, même si l'emplacement principal n'est pas disponible.

Important
Les données répliquées occupent le même espace de stockage que les données d'origine.

Activation et désactivation du stockage géoredondant

Prérequis

- Le stockage géoredondant devient disponible dans la console Cyber Protect uniquement après qu'un administrateur partenaire l'a activé dans le portail de gestion ou via l'API.
- Seuls les administrateurs peuvent activer ou désactiver le stockage géoredondant dans la console Cyber Protect. Vérifiez que vous disposez des droits d'administrateur.

Pour activer le stockage géoredondant

1. [Uniquement si le stockage géoredondant a été activé via l'API] Dans l'alerte figurant au-dessus de « La géoredondance est disponible pour toutes vos données dans le cloud. », cliquez sur **Activer Geo-redundant Cloud Storage**.
2. Dans la console Cyber Protect, accédez à **Paramètres** > **Paramètres système**.
3. Faites défiler la liste des options de sauvegarde par défaut, puis cliquez sur **Geo-redundant Cloud Storage**.
4. Activez le commutateur **Geo-redundant Cloud Storage**.

5. Cliquez sur **Enregistrer**.

   Désormais, vos données seront répliquées dans un emplacement secondaire et resteront disponibles, même en cas de défaillance de l'emplacement principal.

Pour désactiver le stockage géoredondant

Avertissement !
Les données répliquées sont supprimées un jour après la désactivation de la géoredondance.

1. Dans la console Cyber Protect, accédez à **Paramètres** > **Paramètres système**.
2. Faites défiler la liste des options de sauvegarde, puis cliquez sur **Geo-redundant Cloud Storage**.
3. Désactivez le commutateur **Geo-redundant Cloud Storage**.
4. Confirmez votre choix en saisissant **Désactiver**, puis cliquez sur **Désactiver**.

Statut de géo-réplication

La géoredondance implique que les données soient répliquées dans un emplacement secondaire. Le statut de géo-réplication indique les phases de ce processus. Les statuts suivants sont possibles :

- **Synchronisé** : les données ont été répliquées dans l'emplacement secondaire.
- **Synchronisation** : les données sont en cours de réplication dans l'emplacement secondaire. La durée de cette opération dépend du volume des données.
- **En attente** : la réplication des données est suspendue temporairement.
- **Désactivé** : la réplication des données est désactivée.

Pour vérifier le statut de réplication dans la console Cyber Protect

1. Sur la console Cyber Protect, accédez à **Stockage de sauvegarde**.
2. Sélectionnez l'emplacement et l'ensemble de sauvegardes.
3. Cliquez sur **Détails**, puis cliquez sur le statut dans **Statut de géo-réplication**.

Limites

- Actuellement, les emplacements secondaires pour les données répliquées ne sont disponibles qu'aux États-Unis et au Canada.
- Pour plus d'informations sur les limites du service Reprise d'activité après sinistre lors de l'utilisation de la géoredondance, consultez la documentation sur la reprise d'activité après sinistre.

Glossaire

A

Adresse IP publique

[Disaster Recovery] Une adresse IP nécessaire pour rendre les serveurs Cloud disponibles depuis Internet.

Adresse IP test

[Disaster Recovery] Une adresse IP nécessaire en cas de basculement test, pour éviter la duplication de l'adresse IP de production.

Agent de prévention des pertes de données

Un composant client du système de prévention des pertes de données qui protège son ordinateur hôte contre l'utilisation, la transmission et le stockage non autorisés de données confidentielles, protégées ou sensibles en appliquant une combinaison de techniques d'analyse de contexte et de contenu et en mettant en œuvre des politiques de prévention des pertes de données gérées de manière centralisée. Cyber Protection propose un agent de prévention des pertes de données complet. Toutefois, la fonctionnalité de l'agent sur un ordinateur protégé est limitée à l'ensemble de fonctionnalités de prévention des pertes de données disponibles sous licence dans Cyber Protection, et dépend du plan de protection appliqué à cet ordinateur.

Agent de protection

Un agent de protection est l'agent à installer sur les machines à des fins de protection des données.

Application VPN

[Disaster Recovery] Une machine virtuelle spéciale qui connecte le réseau local et le site dans le Cloud via un tunnel VPN sécurisé. Le matériel VPN est déployé sur le site local.

B

Basculement

Rebasculement d'une ressource d'un serveur de production vers un serveur de secours (tel qu'un réplica de machine virtuelle ou un serveur de restauration s'exécutant dans le Cloud).

Base de données des périphériques USB

[Contrôle des terminaux] Le module de contrôle des terminaux tient à jour une base de données des périphériques USB depuis laquelle ils peuvent être ajoutés à la liste des exclusions du contrôle d'accès aux terminaux. La base de données enregistre les périphériques USB par identifiants de périphérique, qui peuvent être entrés manuellement ou sélectionnés à partir des terminaux connus dans la console Cyber Protect.

C

Connexion de point à site (P2S)

[Disaster Recovery] Une connexion VPN sécurisée extérieure en utilisant vos terminaux (comme un ordinateur de bureau ou un ordinateur portable) vers le site local et dans le Cloud.

Connexion de site à site (S2S)

[Disaster Recovery] Connexion qui étend le réseau local au Cloud via un tunnel VPN sécurisé.

F

Finalisation

L'opération qui consiste à faire d'une machine virtuelle temporaire s'exécutant depuis une sauvegarde une machine virtuelle permanente. Physiquement, cela signifie restaurer l'ensemble des disques de la machine virtuelle, y compris les modifications effectuées lors de l'exécution de la machine, dans le magasin de données stockant ces modifications.

Format de sauvegarde sous forme d'un fichier unique

Format de sauvegarde, pour lequel les sauvegardes complètes et incrémentielles suivantes sont enregistrées sous forme d'un fichier .tibx unique. Ce format accélère la vitesse de la méthode de sauvegarde incrémentielle, tout en évitant ses principaux inconvénients et la suppression complexe de sauvegardes ayant expiré. Le logiciel définit les blocs de sauvegarde utilisés par des sauvegardes ayant expiré comme étant « libres » et y inscrit les nouvelles sauvegardes. Ce procédé permet un nettoyage extrêmement rapide et une consommation minimale des ressources. Le format de sauvegarde sous forme de fichier unique n'est pas disponible lorsque la sauvegarde est effectuée sur des emplacements qui ne prennent pas en charge les lectures et écritures en accès aléatoire.

J

Jeu de sauvegardes

Il s'agit d'un groupe de sauvegardes auquel il est possible d'appliquer une règle individuelle de rétention. Pour le modèle de sauvegarde Personnalisé, les jeux de sauvegardes correspondent aux méthodes de sauvegarde (Complète, Différentielle et Incrémentielle). Dans tous les autres cas de figure, les jeux correspondent à une sauvegarde : Mensuelle, Quotidienne, Hebdomadaire et Par heure. Une sauvegarde mensuelle correspond à la première sauvegarde créée dès qu'un mois commence. Une sauvegarde hebdomadaire correspond à la première sauvegarde créée le jour de la semaine sélectionné dans l'option Sauvegarde hebdomadaire (cliquez sur l'icône en forme d'engrenage, puis sur Options de sauvegarde > Sauvegarde hebdomadaire). Si une sauvegarde hebdomadaire correspond à la première sauvegarde créée dès qu'un mois commence, cette sauvegarde est considérée comme étant mensuelle. Dans ce cas, une sauvegarde hebdomadaire sera créée lors du jour de la semaine sélectionné. Une sauvegarde quotidienne correspond à la première sauvegarde créée dès qu'un jour commence, sauf si elle répond à la définition d'une sauvegarde mensuelle ou hebdomadaire. Une sauvegarde par heure correspond à la première sauvegarde créée dès qu'une heure commence, sauf si elle répond à la définition d'une sauvegarde mensuelle, hebdomadaire ou quotidienne.

M

Machine physique

Une machine sauvegardée par un agent installé sur le système d'exploitation.

Machine virtuelle

Une machine virtuelle sauvegardée au niveau de l'hyperviseur par un agent externe tel que l'agent pour VMware ou l'agent pour Hyper-V. Une machine virtuelle avec un agent interne est traitée comme une machine physique au niveau de la sauvegarde.

Module

Un module est un élément du plan de protection, fournissant une fonctionnalité de protection particulière, par exemple le module de sauvegarde, le module de protection contre les virus et les malwares, etc.

Module de contrôle des terminaux

Dans le cadre d'un plan de protection, le module de contrôle des terminaux tire parti d'un sous-ensemble fonctionnel de l'agent de prévention des pertes de données sur chaque ordinateur protégé afin de détecter et de prévenir la consultation et la transmission non autorisées de données via les canaux de l'ordinateur local. Cela comprend l'accès de l'utilisateur aux ports et périphériques, l'impression de documents, les opérations de copier-coller, le formatage des supports et les opérations d'éjection, ainsi que les synchronisations aux terminaux mobiles connectés localement. Le module de contrôle des terminaux offre un contrôle granulaire et contextuel sur les types de terminaux et de ports auxquels les utilisateurs peuvent accéder sur l'ordinateur protégé, ainsi que les actions que ces utilisateurs peuvent réaliser sur ces terminaux.

O

Objectif de point de récupération (RPO)

[Reprise d'activité après sinistre] Quantité de données perdues à cause d'une panne, mesurée en termes de temps à partir d'une panne ou d'un sinistre programmés. Le seuil des objectifs de point de reprise définit l'intervalle de temps maximum autorisé entre le dernier point de récupération pour un basculement et l'heure actuelle.

P

Passerelle VPN (anciennement serveur VPN ou passerelle de connectivité)

[Disaster Recovery] Une machine virtuelle spéciale qui connecte les réseaux du site local et du site dans le Cloud via un tunnel VPN sécurisé. La passerelle VPN est déployée dans le site dans le Cloud.

Plan de protection

Un plan de protection est un plan qui combine des modules de protection des données, notamment les modules suivants : sauvegarde, protection contre les virus et les malwares, filtrage d'URL, Windows Defender Antivirus, Microsoft Security Essentials, évaluation des vulnérabilités, gestion des correctifs, carte de protection de données, contrôle des terminaux.

Prévention des pertes de données (anciennement, prévention des fuites de données)

Un système de technologies intégrées et de mesures organisationnelles destinées à détecter et à prévenir la divulgation/consultation accidentelle ou intentionnelle de données confidentielles,

protégées ou sensibles par des entités non autorisées, au sein ou en dehors de l'organisation, ou le transfert de telles données vers des environnements non dignes de confiance.

R

Réseau de production

[Disaster Recovery] Le réseau interne étendu au moyen d'une transmission tunnel VPN, et qui couvre aussi bien les sites locaux et dans le Cloud. Les serveurs locaux et les serveurs dans le Cloud peuvent communiquer entre eux dans le réseau de production.

Réseau de test

[Disaster Recovery] Réseau virtuel isolé, utilisé pour tester le processus de basculement.

Restauration automatique

Rebasculement d'une ressource d'un serveur de secours (tel qu'un réplica de machine virtuelle ou un serveur de restauration s'exécutant dans le Cloud) vers un serveur de production.

Runbook

[Disaster Recovery] Scénario planifié composé d'étapes configurables qui automatisent les actions de reprise d'activité après sinistre.

S

Sauvegarde complète

Sauvegarde autonome contenant toutes les données choisies pour la sauvegarde. Vous n'avez pas besoin d'accéder à une autre sauvegarde pour récupérer les données à partir d'une sauvegarde complète.

Sauvegarde différentielle

Une sauvegarde différentielle stocke les modifications apportées à des données par rapport à la dernière sauvegarde complète. Vous devez avoir accès à la sauvegarde complète correspondante pour récupérer les données à partir d'une sauvegarde différentielle.

Sauvegarde incrémentielle

Sauvegarde qui stocke les modifications apportées aux données par rapport à la dernière sauvegarde. Vous avez besoin d'accéder à d'autres sauvegardes pour récupérer les données à partir d'une sauvegarde incrémentielle.

Sauvegarde orpheline

Une sauvegarde orpheline est une sauvegarde qui n'est plus associée à un plan de protection.

Serveur Cloud

[Disaster Recovery] Référence générale vers un serveur primaire ou de restauration.

Serveur de restauration

[Disaster Recovery] Un réplica en MV de la machine d'origine, basé sur les sauvegardes de serveur protégées stockées dans le Cloud. Les serveurs de restauration sont utilisés pour remplacer les ressources depuis les serveurs originaux en cas de sinistre.

Serveur primaire

[Disaster Recovery] Une machine virtuelle qui ne possède pas de machine associée sur le site local (tel qu'un serveur de restauration). Les serveurs primaires servent à protéger une

application ou à exécuter divers services auxiliaires (tels qu'un service Web).

Site dans le Cloud (ou site de RAS)

[Disaster Recovery] Site distant hébergé dans le Cloud et servant à exécuter l'infrastructure de restauration, en cas de sinistre.

Site local

[Disaster Recovery] L'infrastructure locale déployée sur les locaux de l'entreprise.

V

Validation

Opération qui vérifie la possibilité de récupération de données à partir d'une sauvegarde. La validation d'une sauvegarde de fichiers imite la restauration de tous les fichiers à partir de la sauvegarde vers une destination factice. La validation d'une sauvegarde de disque calcule une somme de contrôle pour chaque bloc de données enregistré dans la sauvegarde. Les deux procédures nécessitent beaucoup de ressources. Même si une validation réussie signifie qu'il existe une forte probabilité de réussite de la restauration, elle ne vérifie pas tous les facteurs ayant une incidence sur le processus de restauration.

Index

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W