Cyber Disaster Recovery Cloud

24.03

Guide de l’administrateur

RÉVISION :11/04/2024

Table des matières

À propos de Cyber Disaster Recovery Cloud **5**
Les fonctionnalités clés 5
Exigences logicielles **6**
Systèmes d'exploitation pris en charge 6
Plates-formes de virtualisation prises en charge 6
Limites 7
Version d'évaluation Cyber Disaster Recovery Cloud **9**
Limites d'utilisation du stockage géoredondant dans le cloud **10**
Compatibilité de la reprise d'activité après sinistre avec le logiciel de chiffrement **11**
Points de calcul **12**
Créer un plan de protection de reprise d'activité après sinistre **14**
Que faire ensuite 15
Modification des paramètres par défaut du serveur de restauration 15
Infrastructure du réseau Cloud 17
Configuration de la connectivité **18**
Concepts de réseau 18
Mode « sur Cloud uniquement » 19
Connexion OpenVPN de site à site 20
Connexion VPN IPsec multi-site 26
Accès VPN à distance de point à site 27
Suppression automatique des environnements clients non utilisés sur un site dans le Cloud 28
Configuration de la connectivité initiale 29
Configuration du mode « sur Cloud uniquement » 29
Configuration OpenVPN de site à site 29
Configuration d'un VPN IPsec multi-site 31
Recommandations pour la disponibilité des services de domaine Active Directory 37
Configuration de l'accès VPN à distance de point à site 37
Gestion du réseau 38
Gestion des réseaux 39
Gestion des paramètres de l'appliance VPN 42
Réinstallation de la passerelle VPN 43
Activation et désactivation de la connexion de site à site 43
Basculement du type de connexion de site à site 44
Réaffectation d'adresses IP 45
Configuration de serveurs DNS personnalisés 46

Suppression de serveurs DNS personnalisés ... 47
Téléchargement d'adresses MAC ... 47
Configuration du routage local ... 48
Autoriser le trafic DHCP via un VPN de couche 2 ... 48
Gestion des paramètres de la connexion de point à site ... 49
Connexions de point à site actives ... 50
Utilisation des journaux ... 50
Dépannage de la configuration VPN IPsec ... 53
Configuration des serveurs de restauration ... 57
Création d'un serveur de restauration ... 57
Fonctionnement du basculement ... 60
Basculement de la production ... 60
Tester le basculement ... 61
Basculement test automatisé ... 61
Réalisation d'un basculement test ... 61
Basculement test automatisé ... 64
Réalisation d'un basculement ... 66
Fonctionnement de la restauration automatique ... 68
Restauration automatique sur une machine virtuelle cible ... 69
Restauration automatique vers une machine physique cible ... 75
Restauration automatique en mode manuel ... 79
Travailler avec des sauvegardes chiffrées ... 81
Opérations réalisées avec les machines virtuelles Microsoft Azure ... 81
Configuration des serveurs primaires ... 83
Création d'un serveur primaire ... 83
Opérations sur un serveur primaire ... 85
Gestion des serveurs Cloud ... 86
Règles de pare-feu pour les serveurs Cloud ... 88
Définition de règles de pare-feu pour les serveurs Cloud ... 88
Vérification des activités de pare-feu dans le Cloud ... 91
Sauvegarde des serveurs Cloud ... 92
Orchestration (runbooks) ... 93
Pourquoi utiliser des runbooks ? ... 93
Création d'un runbook ... 93
Paramètres du runbook ... 96
Opérations avec les runbooks ... 97
Exécution d'un runbook ... 98

Arrêt de l'exécution d'un runbook 98
Affichage de l'historique d'exécution 98
OpenVPN de site à site – Informations complémentaires **100**
Glossaire **107**
Index **109**

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. 57).

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[1] (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

[1]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.

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 avec le logiciel de chiffrement, consultez le Guide de l'utilisateur de la cyberprotection.

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.

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. 45).

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. 57).
- Vous pouvez modifier la configuration de mise en réseau par défaut. Pour plus d'informations, voir "Configuration de la connectivité" (p. 18).
- 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. 15) et "Infrastructure du réseau Cloud" (p. 17).

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. 39).
- 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. 29). 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.

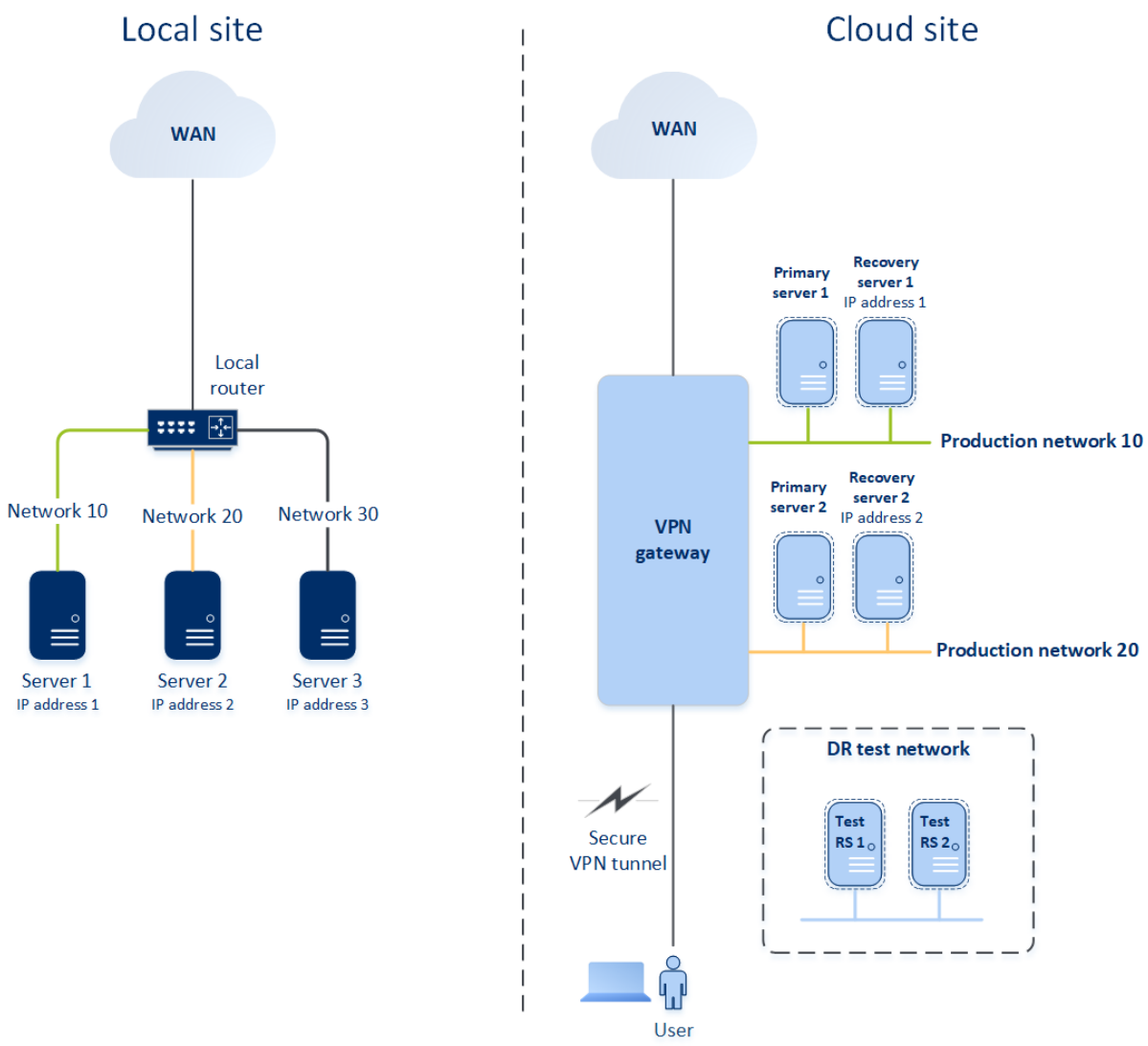
  Pour accéder à un site local, ce type de connexion requiert le déploiement d'un matériel VPN vers le site local.

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.



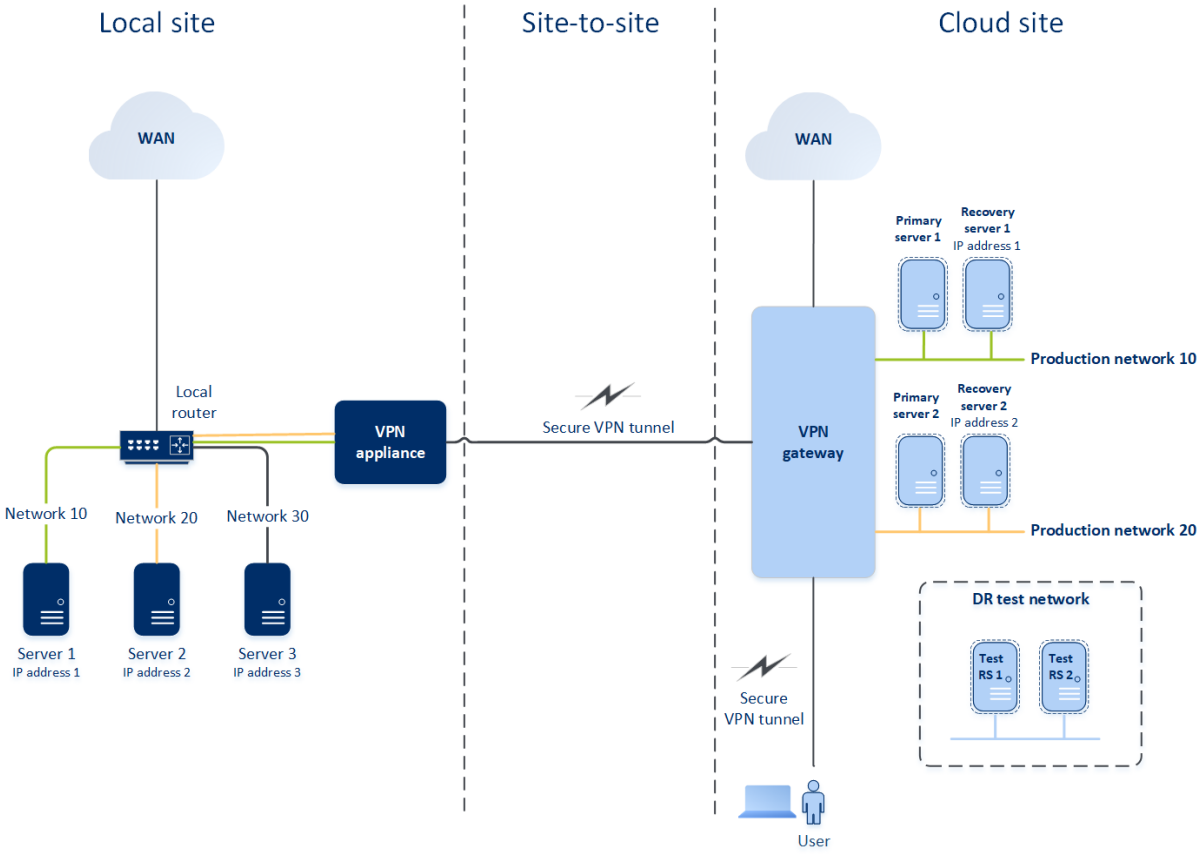
Connexion OpenVPN de site à site

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

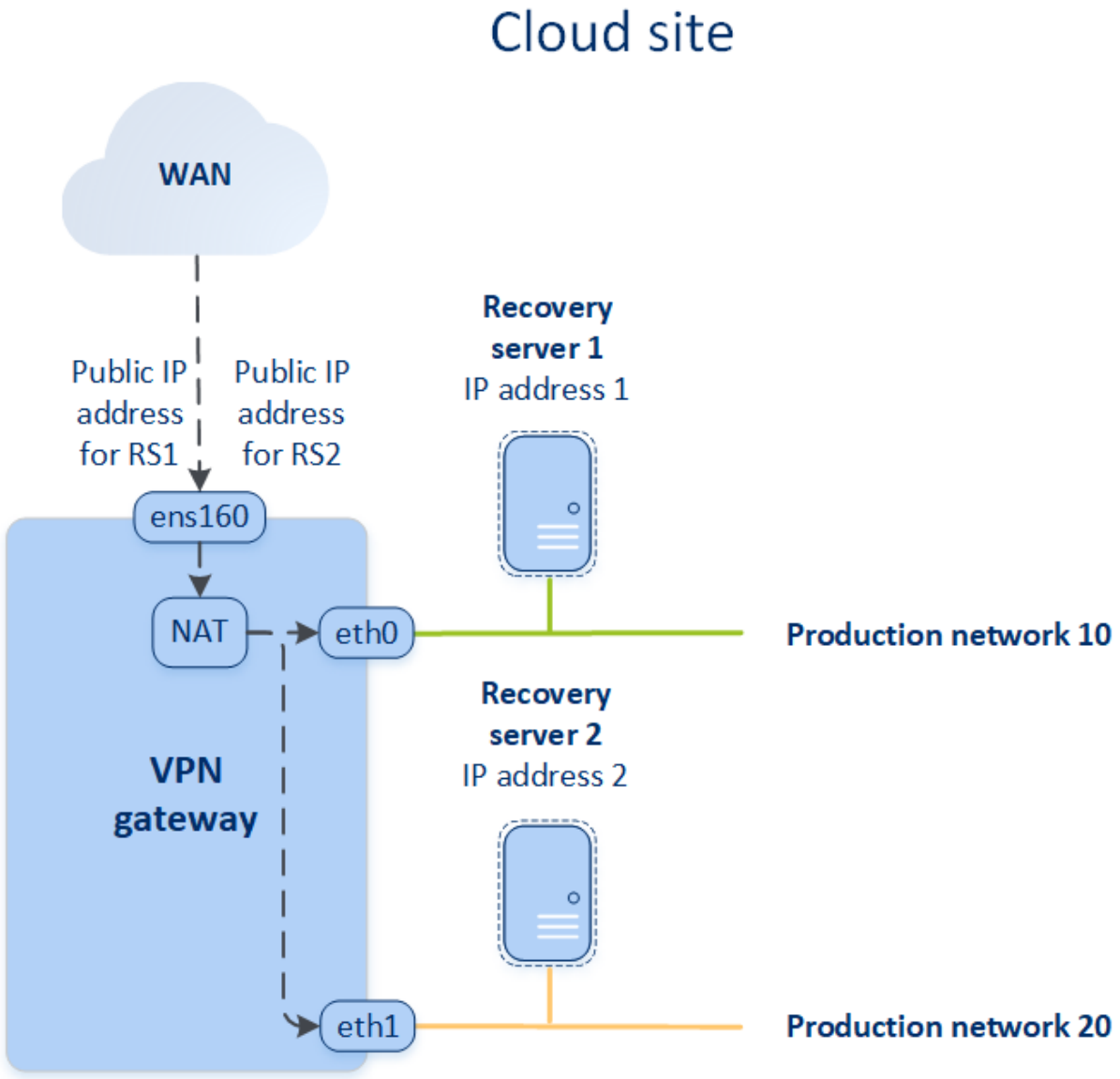
Un **serveur de restauration** : un réplica de la machine d'origine, basé sur les sauvegardes de serveur protégées stockées dans le Cloud. Les serveurs de restauration sont utilisés pour remplacer les ressources depuis les serveurs originaux en cas de sinistre.

Lorsque vous créez un serveur de restauration, vous devez préciser les paramètres de réseau suivants :

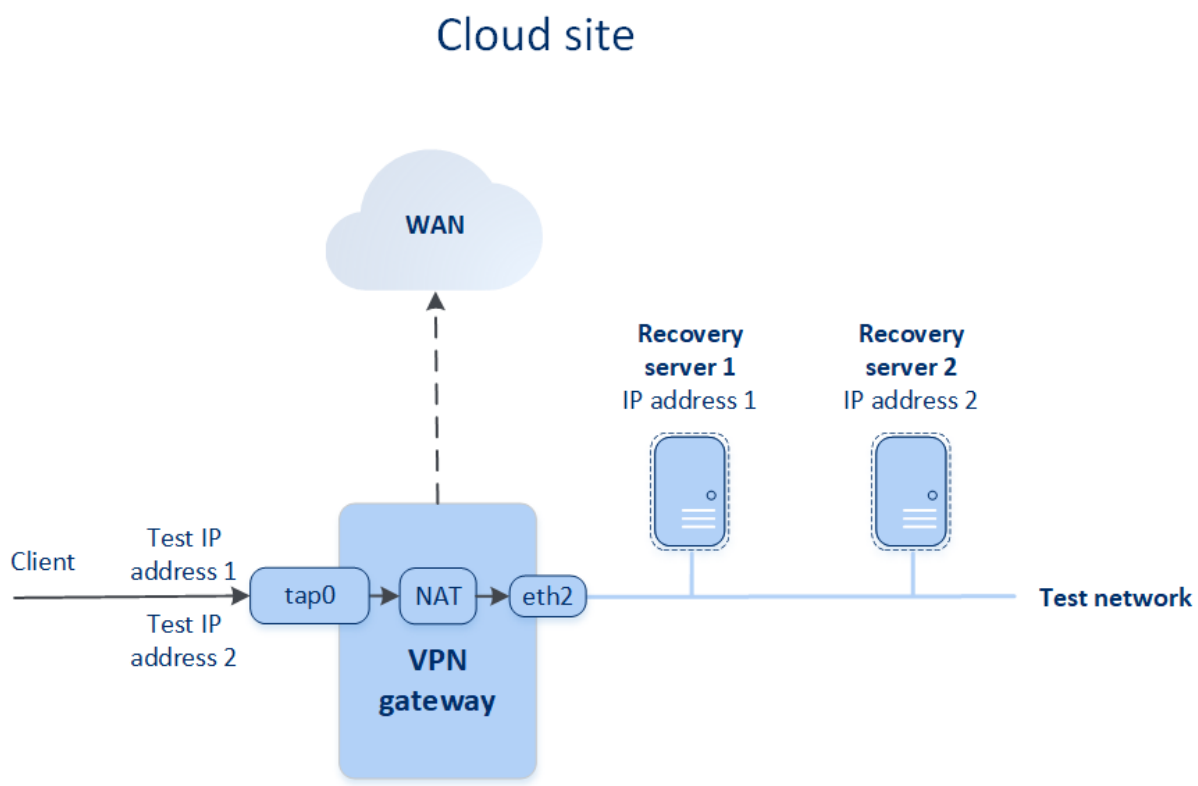
- **Réseau Cloud** (obligatoire) : un réseau Cloud auquel un serveur de restauration sera connecté.
- **Adresse IP dans le réseau de production** (obligatoire) : une adresse IP avec laquelle une machine virtuelle sera lancée pour un serveur de récupération. Cette adresse est utilisée dans les réseaux 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. 100).

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. 46).
- 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

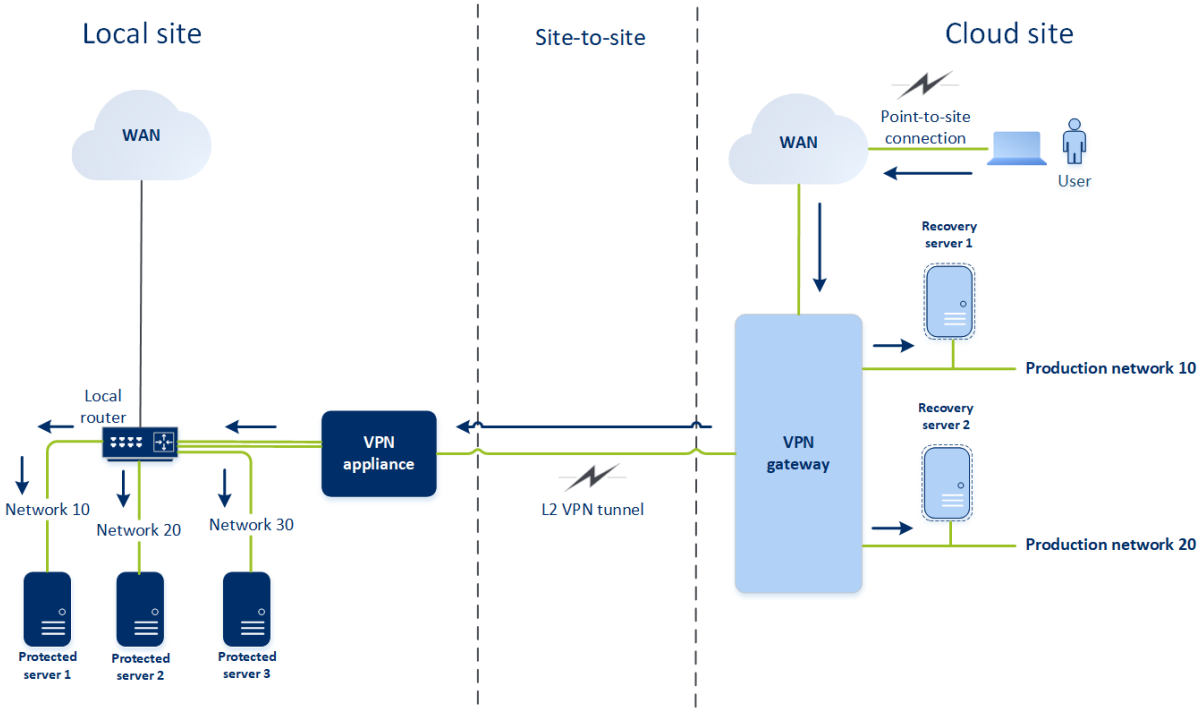
Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

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. 31).
- 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. 33).

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. 34).

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

Paramètre	Description
	long pour la clé. 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

Paramètre	Description
	uniquement lors de l'utilisation du back-end 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

Paramètre	Description
	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. 46).

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. 46).

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.

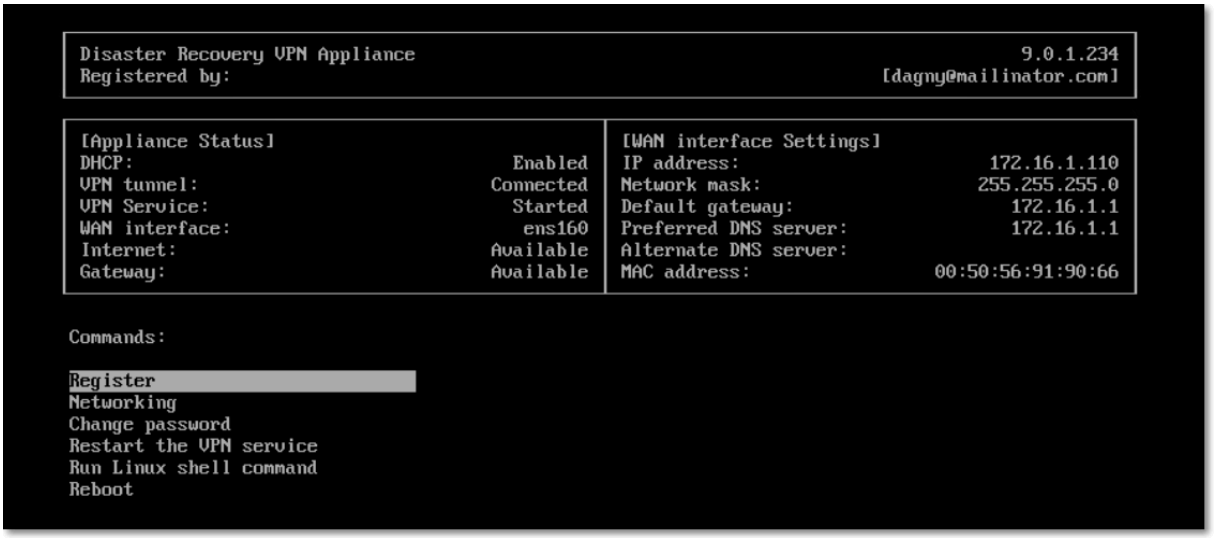
Gestion des réseaux

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.

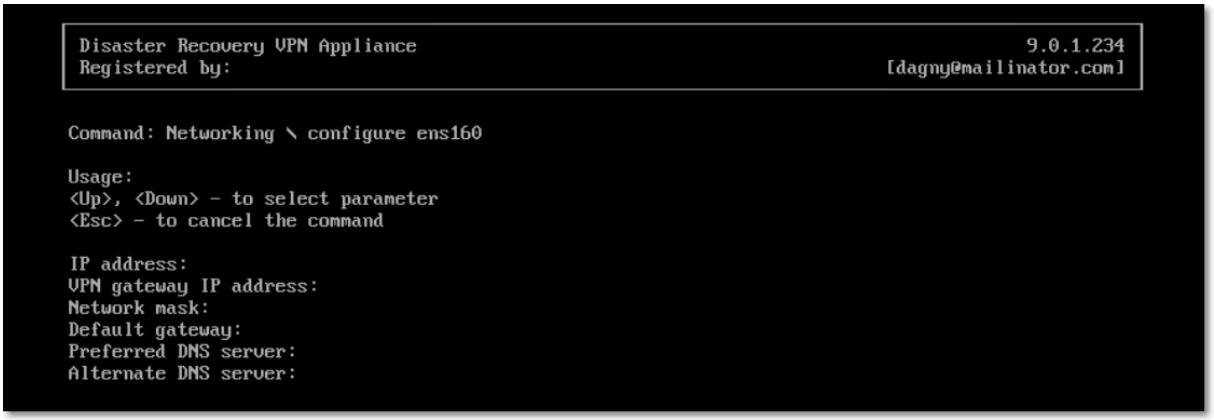
Pour supprimer un réseau étendu au Cloud

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

	Open VPN de site à site	VPN IPsec multi-site
		chevaucher
Prise en charge de l'accès point à site au site local	Oui	Non
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**.

Téléchargement d'adresses MAC

Vous pouvez télécharger une liste d'adresses MAC, puis les extraire et les importer dans la configuration de votre serveur DHCP personnalisé.

Pré-requis :

- Vous devez définir au moins un type de connectivité vers le site dans le Cloud.
- Au moins un serveur primaire ou serveur de restauration avec une adresse MAC doit être configuré.

Télécharger la liste des adresses MAC

1. Dans la console Cyber Protect, accédez à **Reprise d'activité après sinistre** > **Connectivité**.
2. Cliquez sur **Afficher les propriétés**.
3. Cliquez sur **Télécharger la liste des adresses MAC**, puis enregistrez le fichier CSV.

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.

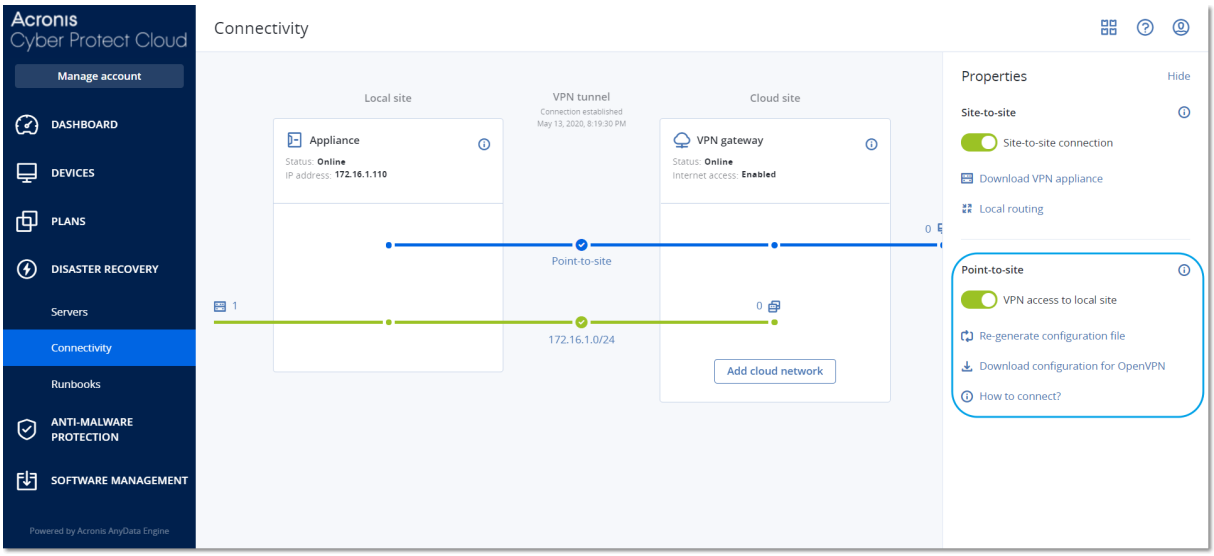
Pour autoriser le trafic DHCP à passer par la connexion VPN de couche 2

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 :

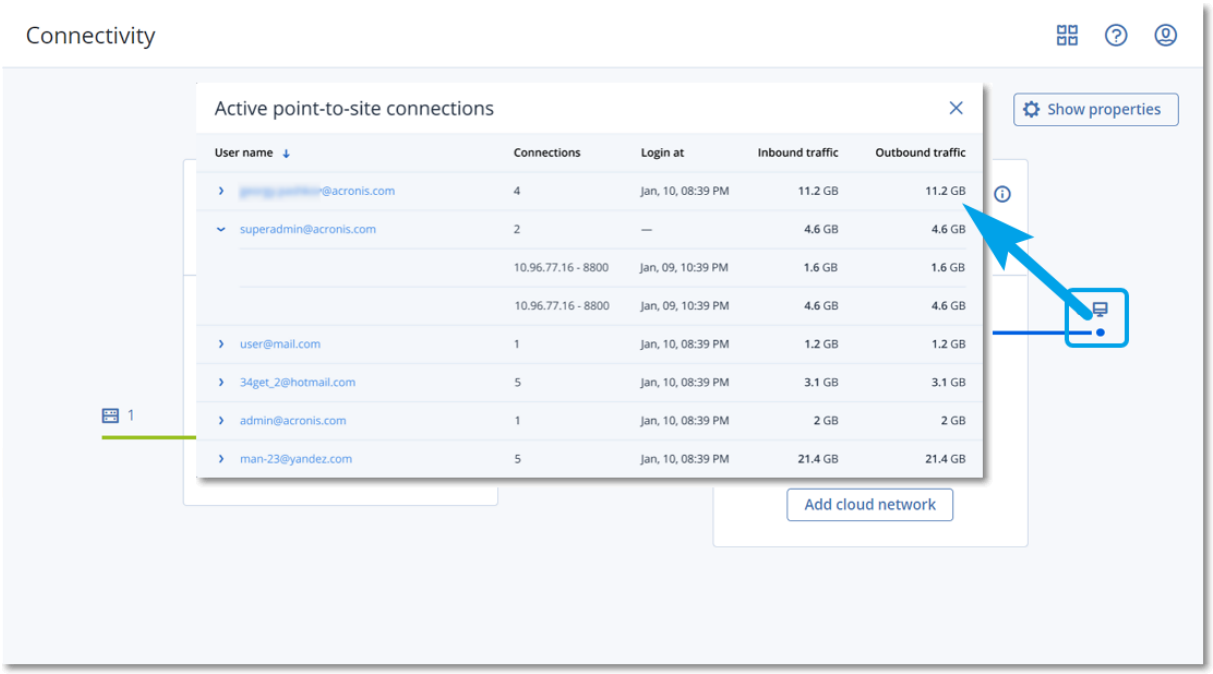
- Si vous pensez que le fichier de configuration est corrompu.
- L'authentification à deux facteurs a été activée pour votre compte.

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. 55).

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. 52).
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. 52).
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.

Problème	Solution possible
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.
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.

Problème	Solution possible
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. 12).

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.

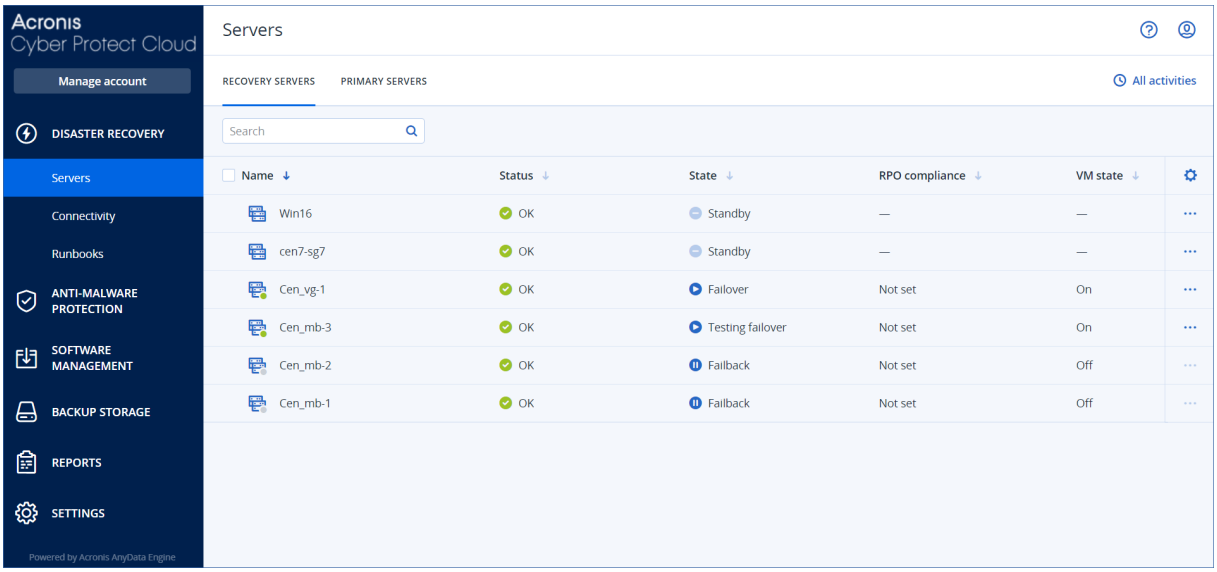
Remarque
Si vous désélectionnez la case **Utiliser une adresse IP publique** ou supprimez le serveur de restauration, son adresse IP publique n'est pas réservée.

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. 88).
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.

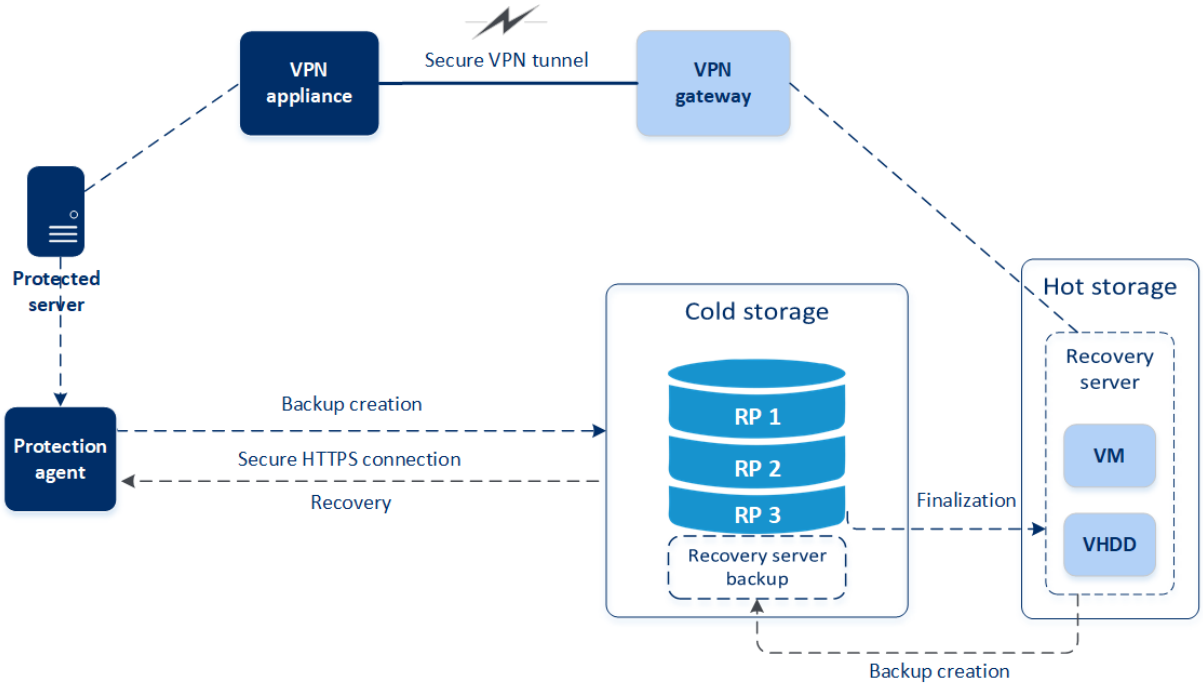
Lors du démarrage du processus de basculement, vous sélectionnez le point de restauration (sauvegarde) de l'ordinateur d'origine depuis lequel une machine virtuelle avec les paramètres prédéfinis sera créée. L'opération de basculement utilise la fonctionnalité « exécution d'une machine virtuelle à partir 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. 61).

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. 64) et "Configuration du basculement test automatisé" (p. 64).

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.

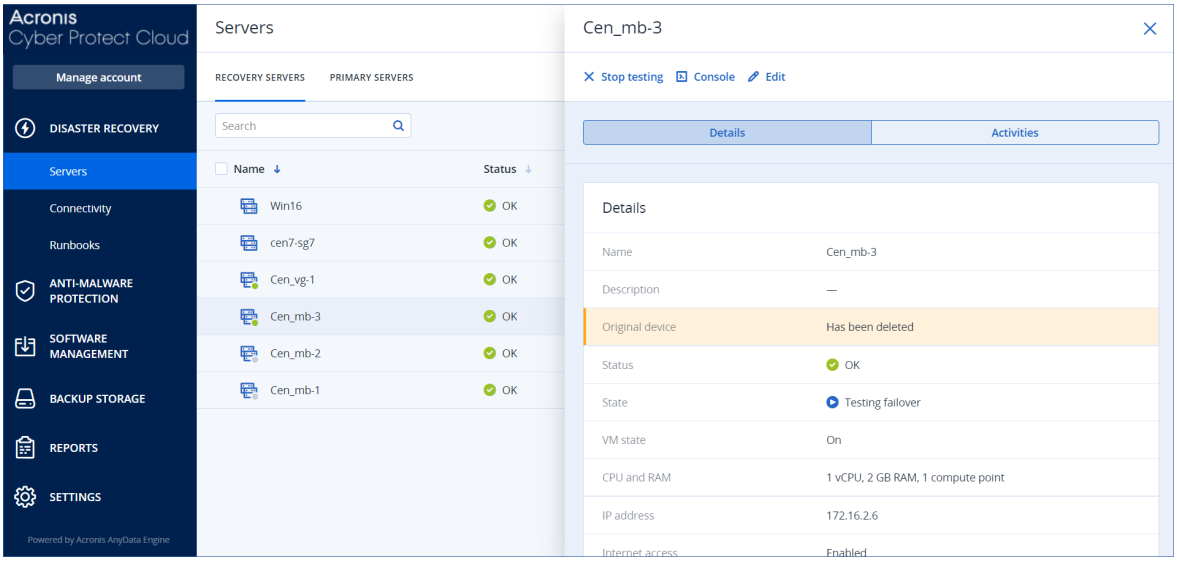
      Remarque
      Le mot de passe ne sera enregistré que temporairement et utilisé uniquement pour le basculement test en cours. Le mot de passe est supprimé automatiquement du magasin des identifiants si le basculement test est arrêté ou une fois que le basculement test est terminé.

   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. 64).

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. 57).

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**.

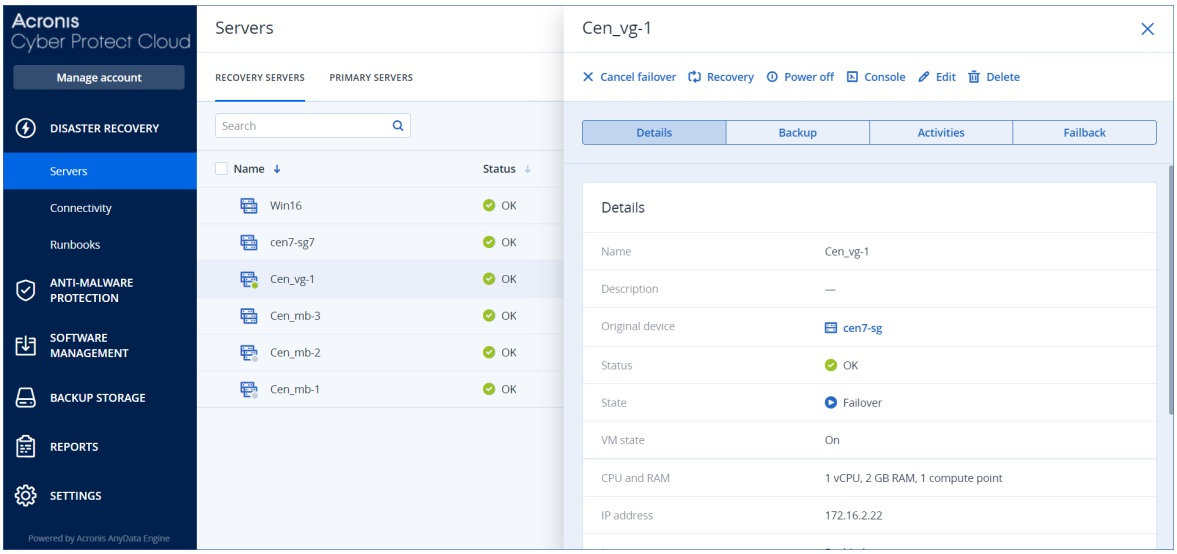
b. [Facultatif] Pour enregistrer le mot de passe de l'ensemble de sauvegardes et l'utiliser dans les opérations de basculement ultérieures, cochez la case **Stocker le mot de passe dans un magasin d'identifiants sécurisé** et saisissez un nom pour les identifiants dans le champ **Nom des identifiants**.

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. 60).



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. 69) et "Restauration automatique vers une machine physique cible" (p. 75).

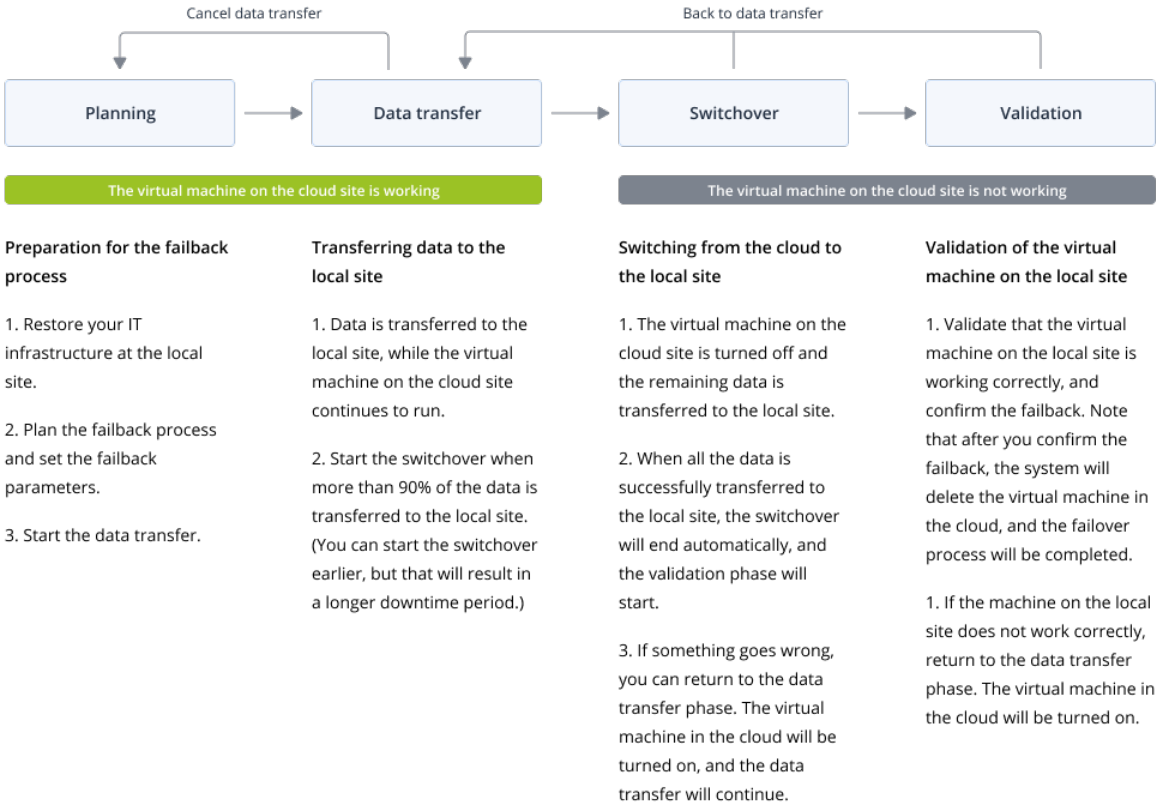
Dans des cas précis où vous ne pouvez pas utiliser la procédure de restauration automatique en mode automatisé, vous pouvez exécuter une restauration automatique en mode manuel. Pour plus d'informations, voir "Restauration automatique en mode manuel" (p. 79).

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 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

Paramètre	Description
	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. 66).

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 "Exécution d'une restauration automatique vers une machine physique" (p. 76).

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. 31).

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. 12).

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.

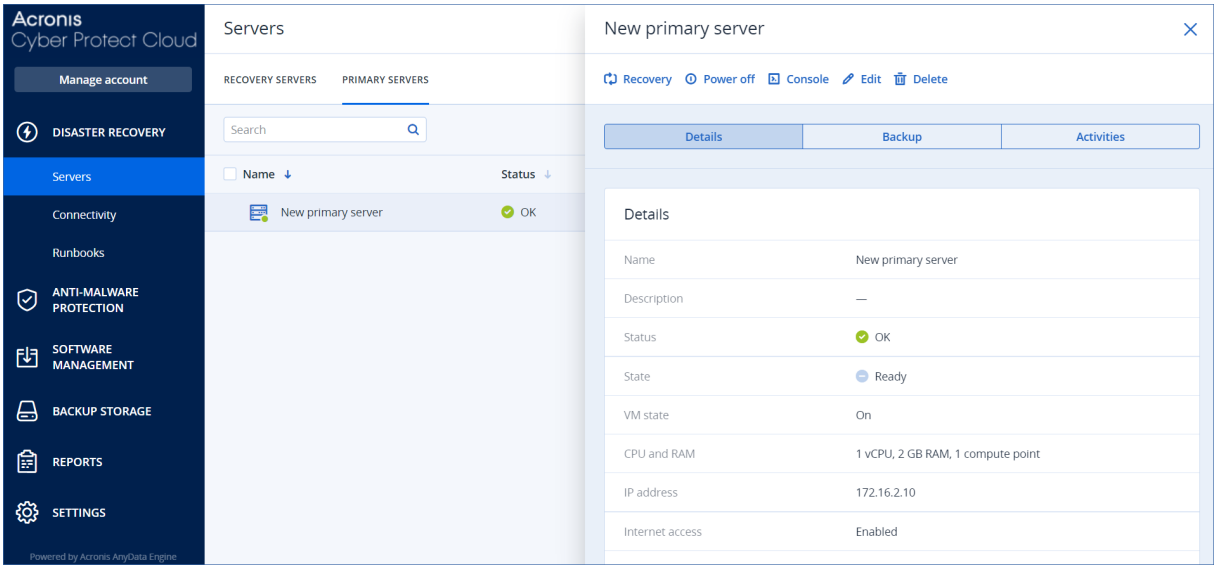
    L'adresse IP publique s'affichera une fois la configuration terminée. Par défaut, le port TCP 443 est ouvert pour les connexions entrantes vers des adresses IP publiques.

    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. 88).
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	Le temps passé depuis la création du dernier point de récupération

de récupération (RPO) réels	
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 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** • **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

Paramètre de pare-feu	Description
	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

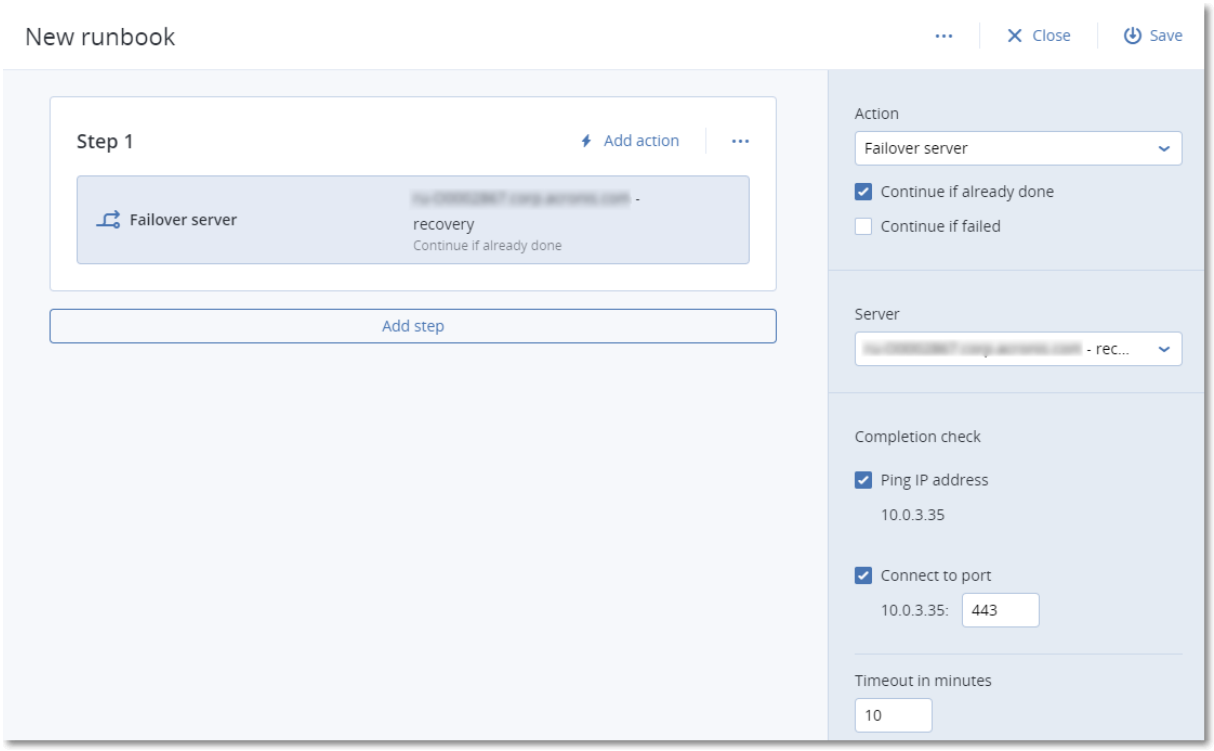
1. Dans la console Cyber Protection, accédez à **Reprise d'activité après sinistre** > **Runbooks**.
2. Cliquez sur **Créer un runbook**.
3. Cliquez sur **Ajouter une étape**.
4. Cliquez sur **Ajouter une action**, puis sélectionnez l'action que vous souhaitez ajouter à l'étape.

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. 96).

Action	Description
	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. 96). **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. 96). **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. 96). **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.

Action	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. 96).
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,

Paramètre de runbook	Catégorie	Disponible pour l'action	Description
			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 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.

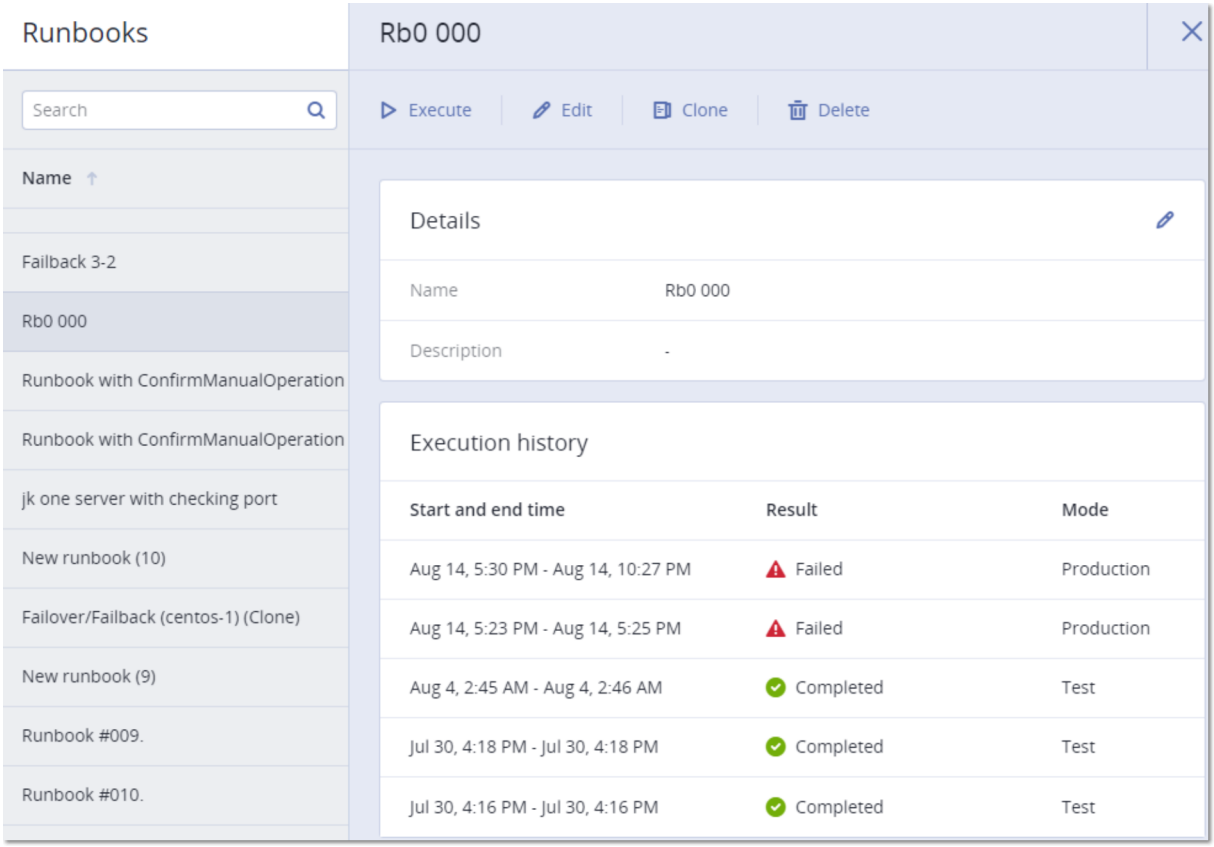
- **Mode basculement et restauration automatique**
  Choisissez si vous souhaitez réaliser un basculement test (par défaut) ou un basculement réel (production). Le mode de restauration automatique correspondra au mode de basculement choisi.
- **Point de récupération en mode basculement**
  Choisissez 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.


Runbooks
Search
Name
Failback 3-2
Rb0 000
Runbook with ConfirmManualOperation
Runbook with ConfirmManualOperation
jk one server with checking port
New runbook (10)
Failover/Failback (centos-1) (Clone)
New runbook (9)
Runbook #009.
Runbook #010.
Rb0 000
Execute
Edit
Clone
Delete
Details
Name
Rb0 000
Description
-
Execution history
Start and end time
Result
Mode
Aug 14, 5:30 PM - Aug 14, 10:27 PM
Failed
Production
Aug 14, 5:23 PM - Aug 14, 5:25 PM
Failed
Production
Aug 4, 2:45 AM - Aug 4, 2:46 AM
Completed
Test
Jul 30, 4:18 PM - Jul 30, 4:18 PM
Completed
Test
Jul 30, 4:16 PM - Jul 30, 4:16 PM
Completed
Test

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.

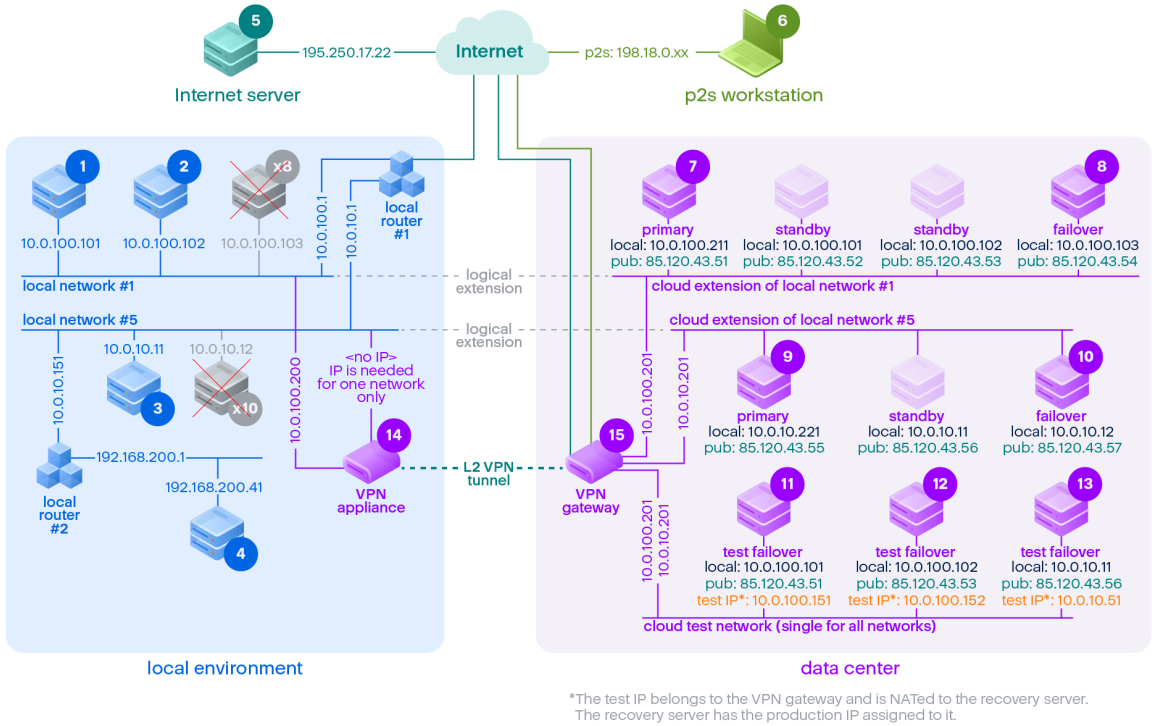
Pour accéder à un serveur de test depuis votre site local, vous devez utiliser l'**adresse IP de test**.

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 routeur local 1	via routeur local 2	via routeur local 1 et Internet	non	via tunnel : local via routeur local 1 et Internet : pub	via tunnel : local via routeur local 1 et Internet : pub	via tunnel : local via routeur local 1 et Internet : pub	via tunnel : local via routeur local 1 et Internet : pub	via tunnel : NAT (serveur VPN) via routeur local 1 et Internet : pub	via tunnel : NAT (serveur VPN) via routeur local 1 et Internet : pub	via local routeur 1 et tunnel : NAT (serveur VPN) via routeur local 1 et Internet : pub	direct	non
2	locale	direct		via routeur local 1	via routeur local 2	via routeur local 1 et Internet	non	via tunnel : local via routeur local 1 et Internet : pub	via tunnel : local via routeur local 1 et Internet : pub	via tunnel : local via routeur local 1 et Internet : pub	via tunnel : local via routeur local 1 et Internet : pub	via tunnel : NAT (serveur VPN) via routeur local 1 et Internet : pub	via tunnel : NAT (serveur VPN) via routeur local 1 et Internet : pub	via local routeur 1 et tunnel : NAT (serveur VPN) via routeur local 1 et Internet : pub	direct	non
3	locale	via routeur	via routeur		via routeur	via routeur local 1	non	via tunnel : local	via tunnel : local	via tunnel : local	via tunnel : local	via tunnel : NAT	via tunnel : NAT	via local routeur 1 et tunnel :	via routeur local	non

	À :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		local 1	local 1		local 2	et Internet		via router local 1 et Internet : pub	via router local 1 et Internet : pub	via router local 1 et Internet : pub	via router local 1 et Internet : pub	(serveur VPN) via router local 1 et Internet : pub	(serveur VPN) via router local 1 et Internet : pub	NAT (serveur VPN) via router local 1 et Internet : pub		
4	locale	via router local 2 et router 1	via router local 2 et router 1	via router local 2		via router local 2, router 1 et Internet	non	via router local 2 et tunnel : local via router local 2, router local 1 et Internet : pub	via router local 2 et tunnel : local via router local 2, router local 1 et Internet : pub	via router local 2 et tunnel : local via router local 2, router local 1 et Internet : pub	via router local 2 et tunnel : local via router local 2, router local 1 et Internet : pub	via tunnel : NAT (serveur VPN) via router local 2, router 1 et Internet : pub	via tunnel : NAT (serveur VPN) via router local 2, router 1 et Internet : pub	via tunnel : NAT (serveur VPN) via router local 2, router 1 et Internet : pub	via router 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		via	via VPN	via	via VPN	via VPN	via VPN	via VPN	non	non

	À :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						Internet		VPN p2s (serveur VPN) : local via Internet : pub	p2s (serveur VPN) : local via Internet : pub	VPN p2s (serveur VPN) : local via Internet : pub	p2s (serveur VPN) : local via Internet : pub	p2s – NAT (serveur VPN) via Internet : pub	p2s – NAT (serveur VPN) via Internet : pub	p2s – NAT (serveur VPN) via Internet : pub		
7	primaire	via tunnel	via tunnel	via tunnel et router local 1	via tunnel et router local 1 et 2	via Internet (via serveur VPN)	non		direct dans le Cloud : local	via tunnel et router local 1 : local	via tunnel et router local 1 : local	via serveur VPN : NAT	via serveur VPN : NAT	via tunnel et router local 1 : NAT	non	Protocoles DHCP et DNS seulement
8	basculement	via tunnel	via tunnel	via tunnel et router local 1	via tunnel et router local 1 et 2	via Internet (via serveur VPN)	non	direct dans le Cloud : local		via tunnel et router local 1 : local	via tunnel et router local 1 : local	via serveur VPN : NAT	via serveur VPN : NAT	via tunnel et router local 1 : NAT	non	Protocoles DHCP et DNS seulement
9	primaire	via tunn	via tunn	via tunnel	via tunnel	via Intern	non	via tunnel	via tunnel et router		direct dans le	via tunnel et router	via tunnel et router	via serveur VPN : NAT	non	Protocoles

	À :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		el et router local 1	el et router local 1			et (via serveur VPN)		et router local 1 : local	local 1 : local		Cloud : local	local 1 : NAT	local 1 : NAT			DHCP et DNS seulement
10	basculement	via tunnel et router local 1	via tunnel et router local 1	via tunnel	via tunnel	via Internet (via serveur VPN)	non	via tunnel et router local 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	Protocol

	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)			es DHCP et DNS seulement
14	application VPN	direct	direct	via routeur local 1	via routeur local 2	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	

Glossaire

A

Adresse IP publique

Une adresse IP nécessaire pour rendre les serveurs Cloud disponibles depuis Internet.

Adresse IP test

Une adresse IP nécessaire en cas de basculement test, pour éviter la duplication de l'adresse IP de production.

Application VPN

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

Faire passer la ressource ou l'application vers le site dans le Cloud en cas de catastrophe naturelle ou créée par l'homme sur le site local.

C

Connexion de point à site (P2S)

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)

Connexion qui étend le réseau local au Cloud via un tunnel VPN sécurisé.

F

Finalisation

L'état intermédiaire pour le processus de restauration ou de basculement en production du serveur Cloud. Ce processus implique le transfert des disques virtuels du serveur du stockage de sauvegarde (stockage « à froid ») vers le stockage pour reprise d'activité après sinistre (stockage « à chaud »). Lors de la finalisation, le serveur est accessible et opérationnel bien que ses performances soient inférieures à la normale.

O

Objectif de point de récupération (RPO)

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)

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.

R

Réseau de production

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

Réseau virtuel isolé, utilisé pour tester le processus de basculement.

Restauration automatique

Le processus de restauration des serveurs vers le site local après qu'ils sont passés vers le site dans le Cloud lors du basculement.

Runbook

Scénario planifié composé d'étapes configurables qui automatisent les actions de reprise d'activité après sinistre.

S

Serveur Cloud

Référence générale vers un serveur primaire ou de restauration.

Serveur de restauration

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

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).

Serveur protégé

Une machine physique ou virtuelle détenue par un client, et qui est protégée par le service.

Site dans le Cloud (ou site de RAS)

Site distant hébergé dans le Cloud et servant à exécuter l'infrastructure de restauration, en cas de sinistre.

Site local

L'infrastructure locale déployée sur les locaux de l'entreprise.

Index

A

À propos de Cyber Disaster Recovery Cloud 5

Accès VPN à distance de point à site 27

Accès VPN au site local 49

Activation et désactivation de la connexion de site à site 43

Adresse IP publique et de test 23

Affichage de l'historique d'exécution 98

Affichage du statut du basculement test automatisé 65

Application VPN 23

Arrêt de l'exécution d'un runbook 98

Autoriser le trafic DHCP via un VPN de couche 2 48

B

Basculement de la production 60

Basculement du type de connexion de site à site 44

Basculement test automatisé 61, 64

C

Capture des paquets réseau 52

Comment exécuter un basculement à l'aide d'un serveur DHCP 68

Comment exécuter un basculement des serveurs à l'aide d'un DNS local 68

Compatibilité de la reprise d'activité après sinistre avec le logiciel de chiffrement 11

Concepts de réseau 18

Configuration d'un VPN IPsec multi-site 31

Configuration d'une connexion OpenVPN de site à site 30

Configuration de l'accès VPN à distance de point à site 37

Configuration de la connectivité 18

Configuration de la connectivité initiale 29

Configuration de serveurs DNS personnalisés 46

Configuration des paramètres du VPN IPsec multi-site 32

Configuration des serveurs de restauration 57

Configuration des serveurs primaires 83

Configuration du basculement test automatisé 64

Configuration du mode « sur Cloud uniquement » 29

Configuration du routage local 48

Configuration OpenVPN de site à site 29

Configuration requise 29

Configuration réseau de la passerelle VPN 22

Connexion OpenVPN de site à site 20, 39

Connexion VPN IPsec multi-site 26

Connexions de point à site actives 50

Contrôleur de domaine Active Directory pour la connectivité OpenVPN de couche 2 37

Contrôleur de domaine Active Directory pour la connectivité VPN IPsec de couche 3 37

Création d'un runbook 93

Création d'un serveur de restauration 57

Création d'un serveur primaire 83

Créer un plan de protection de reprise d'activité après sinistre 14

D

Définition de règles de pare-feu pour les serveurs Cloud 88

Dépannage de la configuration VPN IPsec 53

Dépannage des problèmes de configuration VPN IPsec 53

Désactivation du basculement test automatisé 65

E

Exécution d'un runbook 98

Exécution d'une restauration automatique vers une machine physique 76

Exécution d'une restauration automatique vers une machine virtuelle 71

Exigences logicielles 6

Exigences relatives à l'appliance VPN 29

F

Fichiers journaux VPN IPsec multi-site 55

Fonctionnement de la restauration automatique 68

Fonctionnement du basculement 60

Fonctionnement du routage 19, 22, 27

G

Gestion des paramètres de l'appliance VPN 42

Gestion des paramètres de la connexion de point à site 49

Gestion des réseaux 39

Gestion des serveurs Cloud 86

Gestion du réseau 38

I

Infrastructure du réseau Cloud 17

L

Les fonctionnalités clés 5

Limites 7

Limites d'utilisation du stockage géoredondant dans le cloud 10

M

Mode « sur Cloud uniquement » 19, 40

Modification des paramètres par défaut du serveur de restauration 15

O

OpenVPN de site à site – Informations complémentaires 100

Opérations avec les runbooks 97

Opérations réalisées avec les machines virtuelles Microsoft Azure 81

Opérations sur un serveur primaire 85

Orchestration (runbooks) 93

P

Paramètres de sécurité IPsec/IKE 34

Paramètres du runbook 96

Passerelle VPN 22, 27

Plates-formes de virtualisation prises en charge 6

Points de calcul 12

Ports 29

Pourquoi utiliser des runbooks ? 93

Pré-requis 43, 46-48

Prérequis 32, 38, 55, 57, 71, 76, 83

Q

Que faire ensuite 15

R

Réaffectation d'adresses IP 45

Réalisation d'un basculement 66

Réalisation d'un basculement test 61

Réalisation d'une restauration automatique en mode manuel 79

Recommandations générales pour les sites locaux 33

Recommandations pour la disponibilité des services de domaine Active Directory 37

Reconfiguration d'une adresse IP 41

Régénération de la configuration 49

Règles de pare-feu pour les serveurs Cloud 88

Réinstallation de la passerelle VPN 43

Restauration automatique en mode manuel 79

Restauration automatique sur une machine virtuelle cible 69

Restauration automatique vers une machine physique cible 75

S

Sauvegarde des serveurs Cloud 92

Serveurs de restauration 23

Serveurs primaires 25

Suppression automatique des environnements clients non utilisés sur un site dans le Cloud 28

Suppression de serveurs DNS personnalisés 47

Systèmes d'exploitation pris en charge 6

T

Téléchargement d'adresses MAC 47

Téléchargement des fichiers journaux VPN IPsec 55

Téléchargement des journaux de l'appliance VPN 51

Téléchargement des journaux de la passerelle VPN 51

Téléchargez la configuration pour OpenVPN 49

Tester le basculement 61

Travailler avec des sauvegardes chiffrées 81

U

Utilisation des journaux 50

V

Vérification des activités de pare-feu dans le Cloud 91

Version d'évaluation Cyber Disaster Recovery Cloud 9