Cyber Disaster Recovery Cloud

24.03

管理者ガイド

リビジョン:2024/04/10

目次

Cyber Disaster Recovery Cloudのバージョン情報

Cyber Disaster Recovery Cloud（DR）: Cyber Protectionの一部で、ディザスタリカバリをサービスとして提供します（DRaaS）。Cyber Disaster Recovery Cloudは、人為的災害や自然災害が発生した場合に、マシンをそのままコピーしたものをクラウドサイトに立ち上げ、元の破損したマシンからワークロードをリカバリサーバーに切り替える、高速で安定したソリューションを実現します。

次の方法で、ディザスタリカバリをセットアップして設定できます。

- ディザスタリカバリモジュールを含めた保護計画を作成し、デバイスに適用します。これによって、デフォルトのディザスタリカバリインフラが自動的にセットアップされます。「ディザスタリカバリ保護計画の作成」を参照してください。
- ディザスタリカバリクラウドインフラを手動でセットアップし、それぞれの手順を制御します。"復元サーバー設定"（55ページ）をご覧ください。

重要な機能

注意
適用されるライセンスモデルによっては、一部の機能で追加のライセンスが必要になる場合があります。

- Cyber Disaster Recovery Cloudサービスを単一のコンソールから管理
- セキュアなVPNトンネルを使用して最大23個のローカルネットワークをクラウドに拡張
- VPNアプライアンス[1]を配置せずに（クラウド限定モードで）クラウドサイトへの接続を確立
- ローカルおよびクラウドサイトへのポイントツーサイト接続を確立
- クラウドの復元サーバーを使用してマシンを保護
- クラウドのプライマリサーバーを使用してアプリケーションとアプライアンスを保護
- 暗号化済みバックアップへの自動ディザスタリカバリ操作を実行
- 隔離されたネットワークでテストフェールオーバーを実行
- ランブックを使用して、クラウドの本番環境をスピンアップ

[1]安全なVPNトンネルを介してローカルネットワークとクラウドサイト間の接続を可能にする特別な仮想マシン。VPNアプライアンスはローカルサイトに配置されています。

ソフトウェア要件

サポートされるオペレーティング システム

リカバリサーバーによる保護は、次のオペレーティングシステムで確認されています。

- 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: Nano Server以外のすべてのインストールオプション
- Windows Server 2019: Nano Server以外のすべてのインストールオプション
- Windows Server 2022: Nano Server以外のすべてのインストールオプション

このソフトウェアは他の Windows オペレーティングシステムや Linux ディストリビューションでも動作しますが、これは保証されていません。

注意
復元サーバーによる保護は、以下のオペレーティングシステムを搭載したMicrosoft Azure VMでテスト済みです。

- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016: Nano Server以外のすべてのインストールオプション
- Windows Server 2019: Nano Server以外のすべてのインストールオプション
- Windows Server 2022: Nano Server以外のすべてのインストールオプション
- Ubuntu Server 20.04 LTS - Gen2（Canonical）。復元サーバーコンソールへのアクセスの詳細については、https://kb.acronis.com/content/71616を参照してください。

サポートされる仮想環境プラットフォーム

リカバリサーバーによる仮想マシンの保護は、次の仮想環境プラットフォームで確認されています。

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
- Windows Server 2008 R2（Hyper-V 使用）
- Windows Server 2012/2012 R2（Hyper-V 使用）
- Windows Server 2016 with Hyper-V: Nano Server以外のすべてのインストールオプション
- Windows Server 2019 with Hyper-V: Nano Server以外のすべてのインストールオプション
- Windows Server 2022 with Hyper-V: Nano Server以外のすべてのインストールオプション
- Microsoft Hyper-V Server 2012/2012 R2

- Microsoft Hyper-V Server 2016
- カーネルベース仮想マシン（KVM） - 完全仮想化ゲスト（HVM）のみ。準仮想化ゲスト（PV）はサポート対象外です。
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2

VPN アプライアンスは、次の仮想環境プラットフォームで確認されています。

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2（Hyper-V 使用）
- Windows Server 2012/2012 R2（Hyper-V 使用）
- Windows Server 2016 with Hyper-V: Nano Server以外のすべてのインストールオプション
- Windows Server 2019 with Hyper-V: Nano Server以外のすべてのインストールオプション
- Windows Server 2022 with Hyper-V: Nano Server以外のすべてのインストールオプション
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

このソフトウェアは他の仮想環境プラットフォームやバージョンでも動作しますが、これは保証されていません。

制限事項

以下のプラットフォームと構成はCyber Disaster Recovery Cloudではサポート対象外です。

1. サポート外プラットフォーム:
   - Virtuozzoエージェント
   - macOS
   - Windowsデスクトップオペレーティングシステムは、Microsoftの製品利用規約により、サポートされません。
   - Windows Server Azure Edition

     Azure Editionは、Azure IaaS仮想マシン（VM）としてAzureで実行するか、Azure Stack HCIクラスター上のVMとして実行することに特化して構築されたWindows Serverの特別バージョンです。Standard Editionやデータセンターエディションとは異なり、Azure Editionは、ベアメタルハードウェア、WindowsクライアントHyper-V、Windows Server Hyper-V、サードパーティ製ハイパーバイザー、サードパーティ製クラウドでの実行はライセンスされていません。
2. サポート外構成:

   Microsoft Windows
   - ダイナミックディスクはサポート対象外です
   - Windowsデスクトップオペレーティングシステムは、（Microsoftの製品利用規約により）サポートされません
   - Active Directory service with FRSレプリケーションはサポート対象外です

- GPTまたはMBRフォーマットなしのリムーバブルメディア（いわゆる「スーパーフロッピー」）はサポート対象外です

Linux

- パーティションテーブルのないファイルシステム
- エージェントを使用してゲストOSからバックアップされた、以下の高度なLVM（論理ボリュームマネージャー）構成のボリュームを持つLinuxワークロード:ストライプボリューム、ミラーボリューム、RAID 0、RAID 4、RAID 5、RAID 6、RAID 10ボリューム。

注意
複数のオペレーティングシステムがインストールされたワークロードはサポートされていません。

3. サポートされていないバックアップの種類:
   - 継続的データ保護（CDP）復元ポイントに互換性がありません。

     重要
     CDP復元ポイントを有するバックアップからリカバリサーバーを作成する場合、フェールバックまたはリカバリサーバーの作成中に、CDP復元ポイントを含むデータが失われます。

   - フォレンジックバックアップは、リカバリサーバーの作成に利用できません。

リカバリサーバーには 1 つのネットワークインターフェースがあります。元のマシンに複数のネットワークインターフェースがある場合は、1 つだけがエミュレートされます。

クラウドサーバーは暗号化されていません。

Cyber Disaster Recovery Cloud試用版

Acronis Cyber Disaster Recovery Cloudの30日間の試用版をご利用いただけます。この場合パートナーテナントでは、ディザスタリカバリに次の制限があります。

- 復元サーバーおよびプライマリーサーバーはパブリックインターネットにアクセスできません。サーバーにパブリックIPアドレスを割り当てることはできません。
- IPsecマルチサイトVPNを利用できません。

地理的冗長性クラウドストレージ使用時の制限事項

地理的冗長性クラウドストレージは、バックアップデータのセカンダリロケーションを提供します。セカンダリロケーションは、プライマリのストレージロケーションとは地理的に異なる地域に存在します。地域を地理的に分離することで、万が一いずれかの地域に災害が発生し、バックアップデータが復旧不可能になっても、もう一方の地域は影響を受けず、処理を継続することができます。

重要

バックアップストレージのロケーションがプライマリロケーションから地理的に冗長化されたセカンダリロケーションに変更された場合、ディザスタリカバリサービスはサポートされません。

ディザスタリカバリと暗号化ソフトウェアの互換性

ディザスタリカバリには、以下のディスクレベルの暗号化ソフトウェアとの互換性があります。

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

注意

- ディスクレベルの暗号化を利用するワークロードの場合、ワークロードのゲストオペレーティングシステムにプロテクションエージェントをインストールし、エージェントベースのバックアップを実行することをお勧めします。
- 暗号化されたワークロードのエージェントレスバックアップでは、フェールオーバーとフェールバックはサポートされていません。

暗号化ソフトウェアの互換性の詳細については、『サイバープロテクションユーザーガイド』を参照してください。

コンピュートポイント

Disaster Recoveryでは、テストフェールオーバー時や本番フェールオーバー時のプライマリサーバーや復元サーバーに計算ポイントが使用されます。計算ポイントは、クラウド上のサーバー（仮想マシン）の実行に使用される計算リソースを反映します。

ディザスタリカバリ中の計算ポイントの消費は、サーバーのパラメータ、およびサーバーがフェールオーバー状態にある時間によって異なります。サーバーの処理能力が大きく、負荷がかかる時間が長いほど、より多くの計算ポイントが消費されます。より多くの計算ポイントが消費されるほど、請求金額が大きくなります。

Acronis Cloudで稼動しているすべてのサーバーは、状態（電源オンまたは電源オフ）に関係なく、設定されたフレーバーに応じて、計算ポイントに対して請求されます。

スタンバイ状態の復元サーバーは、計算ポイントを消費しないため、計算ポイントが請求されることはありません。

次の表では、異なるフレーバーを持つクラウド上の8台のサーバーと、それらが1時間あたりに消費する計算ポイントの例を示しています。サーバーのフレーバーは、**[詳細]** タブで変更できます。

種類	CPU	RAM	コンピュートポイント
F1	1 vCPU	2GB	1
F2	1 vCPU	4GB	2
F3	2 vCPU	8GB	4
F4	4 vCPU	16GB	8
F5	8 vCPU	32GB	16
F6	16 vCPU	64GB	32
F7	16 vCPU	128GB	64
F8	16 vCPU	256GB	128

表の情報を使用して、サーバー（仮想マシン）で消費される計算ポイント数を簡単に予測できます。

例えば、16GB RAMとvCPU*4基を備えた1台の仮想マシンと、8GBのRAMとvCPU 2基を備えた1台の仮想マシンをディザスタリカバリで保護する場合、最初の仮想マシンでは1時間あたり8個の計算ポイントが消費され、2番目の仮想マシンでは、1時間あたり4個の計算ポイントが消費されます。両方の仮想マシンがフェールオーバーされている状態では、合計消費量は1時間あたり12計算ポイント、つまり1日で288計算ポイントになります（12計算ポイントx24時間=288計算ポイント）。

*vCPUとは、仮想マシンに割り当てられる物理的な中央演算処理装置（CPU）のことであり、時間依存で存在します。

注意

計算ポイントクォータが制限値に達した場合、プライマリサーバーおよび復元サーバーはすべてシャットダウンされます。次の請求期間の開始まで、またはクォータを増やすまで、これらのサーバーを使用することはできません。デフォルトの請求期間は暦月です。

ディザスタリカバリ保護計画の作成

ディザスタリカバリモジュールを含めた保護計画を作成し、デバイスに適用します。

デフォルトでは、新しい保護計画の作成時にディザスタリカバリモジュールが無効になっています。ディザスタリカバリ機能を有効にしてサービスに計画を適用すると、クラウドネットワークインフラが作成されます。ここで作成されるインフラには、個別の保護対象のサービスに対応する復元サーバーが含まれています。復元サーバーは、選択されたデバイスをコピーしたクラウド内の仮想マシンです。選択されたそれぞれのデバイスに対して、デフォルト設定の復元サーバーがスタンバイ状態（仮想マシンが実行されていない）で作成されます。復元サーバーのサイズは、保護されているデバイスのCPUとRAMに応じて自動的に設定されます。次のようなデフォルトのクラウドネットワークインフラも自動的に作成されます。クラウドサイトのVPNゲートウェイとネットワーク。リカバリサーバーの接続先になります。

保護計画のディザスタリカバリモジュールを取り消したり、削除または無効化したりする場合でも、復元サーバーとクラウドネットワークが自動的に削除されることはありません。必要な場合は、ディザスタリカバリインフラを手動で削除できます。

注意

- ディザスタリカバリを構成すると、デバイスの復元サーバー作成後に生成された任意の復元ポイントから、テストまたは本番のフェールオーバーを実行できるようになります。デバイスがディザスタリカバリで保護される前（復元サーバーが作成される前）に生成された復元ポイントを使用してフェールオーバーを実行することはできません。
- デバイスのIPアドレスを検出できない場合、ディザスタリカバリ保護計画を有効にすることはできません。仮想マシンがエージェントレスでバックアップされ、IPアドレスが割り当てられていない場合などがこれに当たります。
- 保護計画を適用する際には、同じネットワークとIPアドレスがクラウドサイトで割り当てられます。IPsec VPN接続では、クラウドのネットワークセグメントとローカルサイトが重複しないことが求められます。マルチサイトIPsec VPN接続が構成され、1台または複数のデバイスに保護計画が後で適用される場合、追加でクラウドネットワークをアップデートしてクラウドサーバーのIPアドレスを再割り当てする必要があります。詳細については、"IPアドレスの再割り当て"（44ページ）を参照してください。

ディザスタリカバリ保護計画を作成するには

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. 保護するマシンを選択します。
3. **[保護]** をクリックしてから、**[計画の作成]** をクリックします。
   保護計画のデフォルト設定が開きます。
4. バックアップオプションを設定します。
   ディザスタリカバリの機能を使用する場合、この計画では、マシン全体、または起動と必須のサービスの提供に必要なディスクのみをクラウド ストレージにバックアップする必要があります。
5. モジュール名の横にあるスイッチをクリックして、ディザスタリカバリモジュールを有効にします。

6. **[作成]** をクリックします。
   計画が作成され、選択されたマシンに適用されます。

次に行うこと

- 復元サーバーのデフォルト設定は編集できます。詳細については、"復元サーバー設定"（55ページ）を参照してください。
- デフォルトのネットワーク設定は編集できます。詳細については、"接続設定"（18ページ）を参照してください。
- 復元サーバーのデフォルトパラメータとクラウドネットワークインフラについて、詳細が確認できます。詳細については、「"復元サーバーのデフォルトパラメータの編集"（15ページ）」と「"クラウドネットワークインフラストラクチャ"（16ページ）」を参照してください。

復元サーバーのデフォルトパラメータの編集

ディザスタリカバリ保護計画を作成して適用すると、デフォルトパラメータで復元サーバーが作成されます。これらのデフォルトパラメータは後で編集できます。

注意
リカバリサーバーは、存在していなかった場合のみ作成されます。既存の復元サーバーに変更や再作成は発生しません。

復元サーバーのデフォルトパラメータを編集するには

1. **[デバイス]** > **[すべてのデバイス]** に進みます。
2. デバイスを選択し、**[ディザスタリカバリ]** をクリックします。
3. 復元サーバーのデフォルトパラメータを編集します。
   復元サーバーのパラメータについては、次のテーブルで説明されています。

復元サーバーパラメータ	デフォルト数	説明
CPUとRAM	自動	リカバリサーバーの仮想CPUの数とRAMの容量。デフォルト設定は元のデバイスのCPUとRAMの設定に基づいて自動的に決定されます。
クラウドネットワーク	自動	サーバーが接続されるクラウドネットワーク。クラウドネットワークの設定内容の詳細については、「クラウドネットワークインフラストラクチャ」を参照してください。
本番ネットワークのIPアドレス	自動	稼働中のネットワークでサーバーに与えられるIPアドレス。デフォルトでは、元のマシンの IP アドレスが設定されています。
テストIPアドレス	無効化	テスト用のIPアドレスを使用することで、隔離され

		たテストネットワーク内でフェールオーバーをテストし、テストフェールオーバー中にRDPまたはSSH経由でリカバリサーバーに接続することが可能になります。テストフェールオーバーモードでは、VPNゲートウェイが、NATプロトコルを使用してテストIPアドレスを本番IPアドレスに置き換えます。テスト用のIPアドレスを指定しない場合、テストフェールオーバー中はコンソール以外でサーバーにアクセスできなくなります。
インターネットアクセス	有効化	リカバリサーバーが、実際のフェールオーバーまたはテストフェールオーバー中にインターネットにアクセスできるようにします。デフォルトでは、TCPポート25番の送信接続は拒否されます。
パブリックアドレスの使用	無効化	パブリック IP アドレスを使用すると、フェールオーバーまたはテストフェールオーバー中にインターネットからリカバリサーバーを使用できるようになります。パブリックIPアドレスを使用しない場合、サーバーは稼働中のネットワーク内部でのみ使用可能になります。パブリックIPアドレスを使用するには、インターネットアクセスを有効にする必要があります。パブリック IP アドレスは、設定が完了した後に表示されます。デフォルトでは、TCPポート443番は受信接続用に開いています。
RPO しきい値を設定	無効化	RPO しきい値は、最後の復元ポイントと現在時刻との間の最大許容時間間隔を定義します。数値は15～60分、1～24時間、1～14日間の範囲で設定できます。

クラウドネットワークインフラストラクチャ

クラウドネットワークインフラストラクチャは、クラウドサイトのVPNゲートウェイと復元サーバーが接続されるクラウドネットワークから構成されます。

注意
ディザスタリカバリ保護計画を適用すると、存在していない場合には復元クラウドネットワークインフラが作成されます。既存のクラウドネットワークの変更や再作成は発生しません。

システムによってデバイスのIPアドレスがチェックされ、IPアドレスに適した既存のクラウドネットワークが存在しない場合は、適切なクラウドネットワークが自動的に作成されます。リカバリサーバーのIPアドレスに適したクラウドネットワークが既に存在していれば、既存のクラウドネットワークの変更や作作成は発生しません。

- クラウドネットワークが存在しない場合や、初めてディザスタリカバリ設定を実施する場合、そのようなクラウドネットワークにはデバイスのIPアドレス範囲に基づいて、IANAがプライベートでの使用

に推奨している最大範囲（10.0.0.0/8、172.16.0.0/12、192.168.0.0/16）が設定されます。ネットワークマスクを編集すれば、ネットワーク範囲を狭くすることができます。

- 選択されたデバイスが複数のローカルネットワークに属している場合、クラウドサイトのネットワークはそれらのローカルネットワークのスーパーセットになる場合があります。ネットワークは **[接続]** セクションで再設定できます。"ネットワークの管理"（38ページ）をご覧ください。
- サイト間Open VPN接続をセットアップする必要がある場合は、VPNアプライアンスをダウンロードしてセットアップしてください。"サイト間Open VPNの構成"（29ページ）をご覧ください。クラウドネットワークの範囲が、VPNアプライアンスに接続されたローカルネットワークの範囲と一致しているのを確認します。
- デフォルトのネットワーク設定を変更するには、保護計画のディザスタリカバリモジュールにある **[接続に移動]** リンクをクリックするか、**[ディザスタリカバリ]** > **[接続]** へ移動します。

接続設定

このセクションでは、Cyber Disaster Recovery Cloudですべての機能がどのように動作するのかを理解するために必要なネットワークの概念について説明します。必要に応じてクラウドサイトへの異なる種類の接続をどのように設定するのかについて知ることができます。最終的には、クラウドでのネットワーク管理方法およびVPNアプライアンスとVPNゲートウェイの設定管理について知ることができます。

ネットワーク概念

注意
適用されるライセンスモデルによっては、一部の機能で追加のライセンスが必要になる場合があります。

Cyber Disaster Recovery Cloudでは、クラウドサイトへの次の接続タイプを定義できます。

- **クラウド限定モード**
  この種類の接続にはローカルサイトへのVPNアプライアンス配置が必要ありません。
  ローカルネットワークとクラウドネットワークは、独立したネットワークです。この種類の接続は、すべてのローカルサイトの保護されたサーバーのフェールオーバー、またはローカルサイトと通信する必要のない独立したサーバーの部分的なフェールオーバーのどちらか一方を意味します。
  クラウドサイト上のクラウドサーバーは、ポイントツーサイトVPN、およびパブリックIPアドレス（割り当てられている場合）を介してアクセスできます。
- **サイト間Open VPN接続**
  この種類の接続にはローカルサイトへのVPNアプライアンス配置が必要です。
  サイト間Open VPN接続により、IPアドレスを保持しながら、ネットワークをクラウドに拡張できます。
  セキュアなVPNトンネルによりローカルサイトがクラウドに接続されました。この種類の接続は、ローカルサイトにWebサーバーやデータベースサーバーなどの高依存度のサーバーがある場合に適しています。部分的なフェールオーバーの場合、これらのサーバーの多数がローカルサイトにとどまっている間に1つのサーバーがクラウドサイトで再作成されても、VPNトンネルを介して互いに通信できます。
  クラウドサイト上のクラウドサーバーは、ローカルネットワーク、ポイントツーサイトVPN、およびパブリックIPアドレス（割り当てられている場合）を介してアクセスできます。
- **マルチサイトIPsec VPN接続**
  このタイプの接続では、IPsec IKE v2をサポートするローカルVPNデバイスが必要となります。
  マルチサイトIPsec VPN接続の構成を開始すると、Cyber Disaster Recovery Cloudが自動的にパブリックIPアドレスによるクラウドVPNゲートウェイを作成します。
  マルチサイトIPsec VPNを使用すると、セキュアなIPsec VPNトンネルによりローカルサイトがクラウドに接続されます。
  このタイプの接続は、1つまたは複数のローカルサイトで重要なワークロードをホストしているか、サービスに緊密に依存している場合のディザスタリカバリシナリオに適しています。

サーバー群の1つが部分的にフェールオーバーする場合、そのサーバーがクラウドサイトで再作成される間も、他のサーバーはローカルサイトにとどまってIPsec VPNトンネルを介して引き続き互いに通信することが可能です。

ローカルサイトの1つが部分的にフェールオーバーする場合は、それ以外のローカルサイトは運用可能なままで、IPsec VPNトンネルを介して引き続き互いに通信できます。

- **ポイントツーサイトリモートVPNアクセス**

  エンドポイントデバイスを使用する外部からのクラウドおよびローカルワークロードに対するセキュアなポイントツーサイトリモートVPNアクセス。

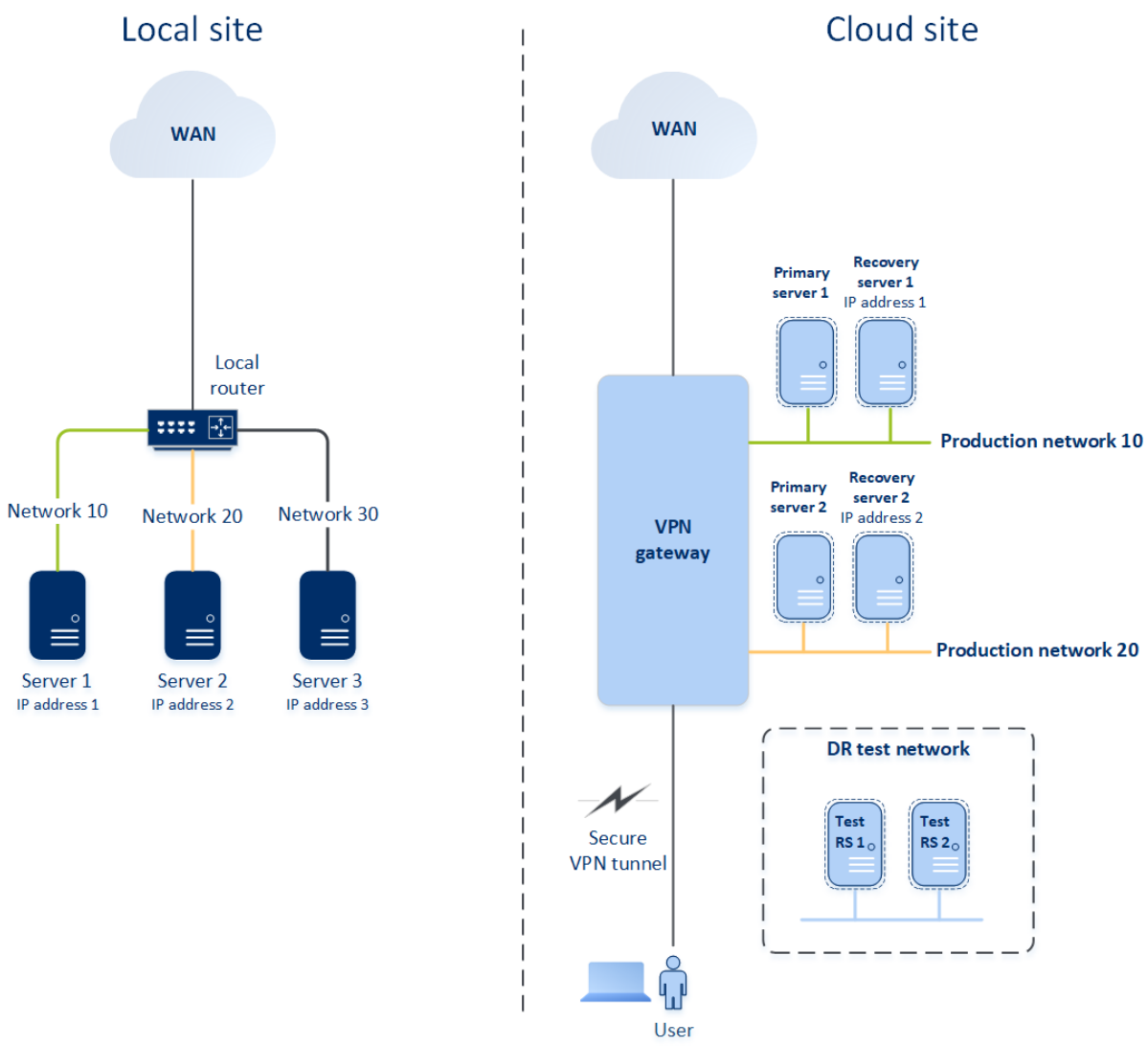
  ローカルサイトにアクセスする場合、この種類の接続にはローカルサイトへのVPNアプライアンス配置が必要です。

クラウド限定モード

クラウド限定モードでは、ローカルサイトへのVPNアプライアンス配置は必要ありません。これは、1つはローカルサイトに、もう1つはクラウドサイトにある、2つの独立したネットワークがあることを意味します。クラウドサイトのルータでルーティングが実行されます。

ルーティングが動作する仕組み

クラウドオンリーモードが確立している場合、クラウドサイトのルーターによってルーティングが実行され、異なるクラウドネットワークに属するサーバー同士で通信できます。



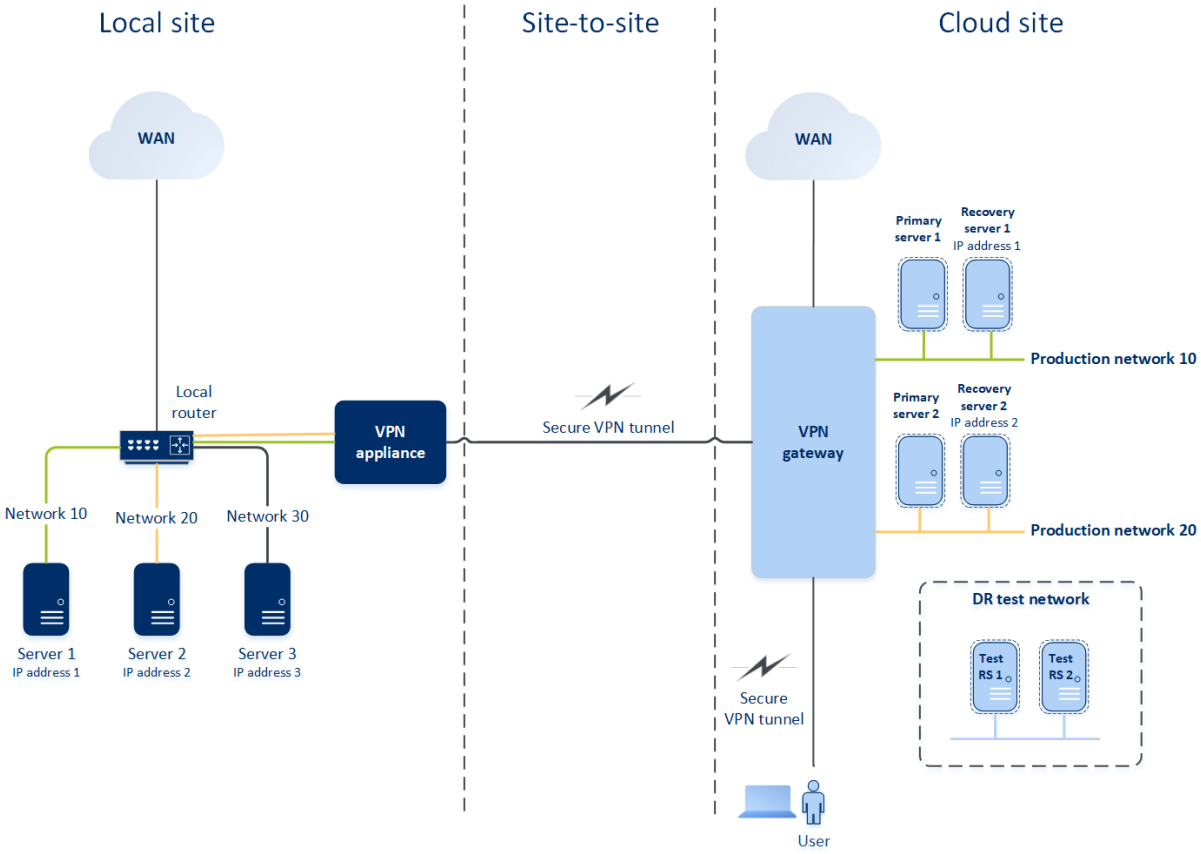
サイト間Open VPN接続

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

Cyber Disaster Recovery Cloudサービスでネットワークがどのように機能するかを理解するため、ローカルサイトの3つのネットワークに各々1つのマシンがある事例を検討します。ネットワーク10とネットワーク20の2つのネットワークについて、災害からの保護を設定します。

下の図では、マシンがホストされているローカルサイトと、災害発生時のためにクラウドサーバーが実行されているクラウドサイトが表示されています。

Cyber Disaster Recovery Cloudソリューションでは、ローカルサイトの破損したマシンからクラウド上のクラウドサーバーに対して、すべてのワークロードのフェールオーバーを行うことができます。
Cyber Disaster Recovery Cloudを使用して最大で23個のネットワークを保護できます。



ローカルサイトとクラウドサイト間のサイトツーサイトOpen VPN通信を確立するには、**VPNアプライアンス**と**VPNゲートウェイ**を使用します。Cyber Protectコンソールでサイトツーサイトopen VPN接続の設定を始める際、VPNゲートウェイは自動的にクラウドサイトに配置されます。それから、ローカルサイトへVPNアプライアンスを配置し、保護するネットワークを追加し、クラウドでアプライアンスを登録する必要があります。Cyber Disaster Recovery Cloudは、クラウドにローカルネットワークのレプリカを作成します。安全なVPNトンネルがVPNアプライアンスとVPNゲートウェイ間に確立されます。これにより、ローカルネットワーク拡張がクラウドに提供されます。クラウドの本番ネットワークがローカルネットワークにブリッジされます。ローカルサーバーとクラウドサーバーはこのVPNトンネルを介してあたかもそれらすべてが同じイーサネットセグメント内にあるかのように通信できます。ローカルのルーターによりルーティングが実行されます。

各ソースマシンを保護するために、クラウドサイトにリカバリサーバーを作成する必要があります。フェールオーバーイベントが生じるまで**スタンバイ**状態を保ちます。（**本番モード**で）災害が発生しフェールオーバープロセスを開始すると、保護されたマシンの厳密なコピーであるリカバリサーバーがクラウドで起動します。ソースマシンと同じIPアドレスを割り当て、同じイーサネットセグメントで起動することができます。顧客は、バックグラウンドでの変更に気付くことなくサーバーでの作業を続けることができます。

フェールオーバープロセスを**テストモード**で開始することもできます。これは、ソースマシンがまだ機能している時に、同時に同じIPアドレスを持つそれぞれの復元サーバーがクラウドで起動することを意味します。IPアドレスの競合を防ぐため、**テストネットワーク**という特別な仮想ネットワークがクラウドに作成されます。テストネットワークは、1つのイーサネットセグメント内でのソースマシンのIPアドレスの重複を防ぐために隔離されています。フェールオーバーのテストモードで復元サーバーにアクセ

スするには、復元サーバーの作成時に、**テストIPアドレス**を復元サーバーに割り当てる必要があります。指定できる復元サーバのパラメータは他にもあり、それらについては以下の各セクションで説明します。

ルーティングが動作する仕組み

サイト間接続が確立されている場合、ローカルのルーターによりクラウドネットワーク間のルーティングが実行されます。VPNサーバーは、異なるクラウドネットワークに配置されたクラウドサーバー間のルーティングを実行しません。いずれかのネットワークにあるクラウドサーバーと、別のクラウドネットワークにあるサーバーで通信が必要な場合、トラフィックはVPNトンネルを通じてローカルサイトのローカルルーターへ送られ、その後、ローカルルーターが、別のネットワークへのルーティングを実行します。そして、トラフィックはトンネル経由でクラウドサイトの目的のサーバーに戻ります。

VPN ゲートウェイ

ローカルサイトとクラウドサイト間の通信を可能にする主要なコンポーネントは**VPNゲートウェイ**です。これは、特別なソフトウェアがインストールされ、ネットワークが特異的に構成されているクラウド内の仮想マシンです。VPNゲートウェイには以下の機能があります。

- ローカルネットワークのイーサネットセグメントとクラウド内の稼働中のネットワークをL2モードで接続。
- iptablesとebtablesのルールを入力。
- テストネットワークと稼働しているネットワークのマシンのデフォルトルーターおよびNATとして動作。
- DHCPサーバーとして動作。本番ネットワークとテストネットワークのすべてのマシンはDHCPを介してネットワークの構成（IPアドレス、DNS設定）を取得します。クラウドサーバーは毎回、DHCPサーバーから同一のIPアドレスを取得します。カスタムDNS設定をセットアップする必要がある場合は、サポートチームに連絡する必要があります。
- キャッシングDNSとして動作。

VPNゲートウェイネットワークの構成

VPNゲートウェイには幾つかのネットワークインターフェースがあります。

- インターネットに接続されている外部インターフェース
- 本番ネットワークに接続されている本番インターフェース
- テストネットワークに接続されているテストインターフェース

加えて、2つの仮想インターフェースがポイントツーサイトおよびサイト間接続用に追加されています。

VPNゲートウェイが配置され初期化されると、ブリッジが作成されます。1つは外部インターフェース用、もう1つは顧客および本番インターフェース用です。クライアント本番環境のブリッジとテストインターフェースは同じIPアドレスを使用しますが、VPNゲートウェイは特定の技術を使用してパッケージを正しくルーティングできます。

VPNアプライアンス

VPNアプライアンスは、Linuxと特別なソフトウェアがインストールされ、ネットワークが特異的に構成されている、ローカルサイト上の仮想マシンです。ローカルサイトとクラウドサイト間の通信を可能にします。

リカバリサーバー

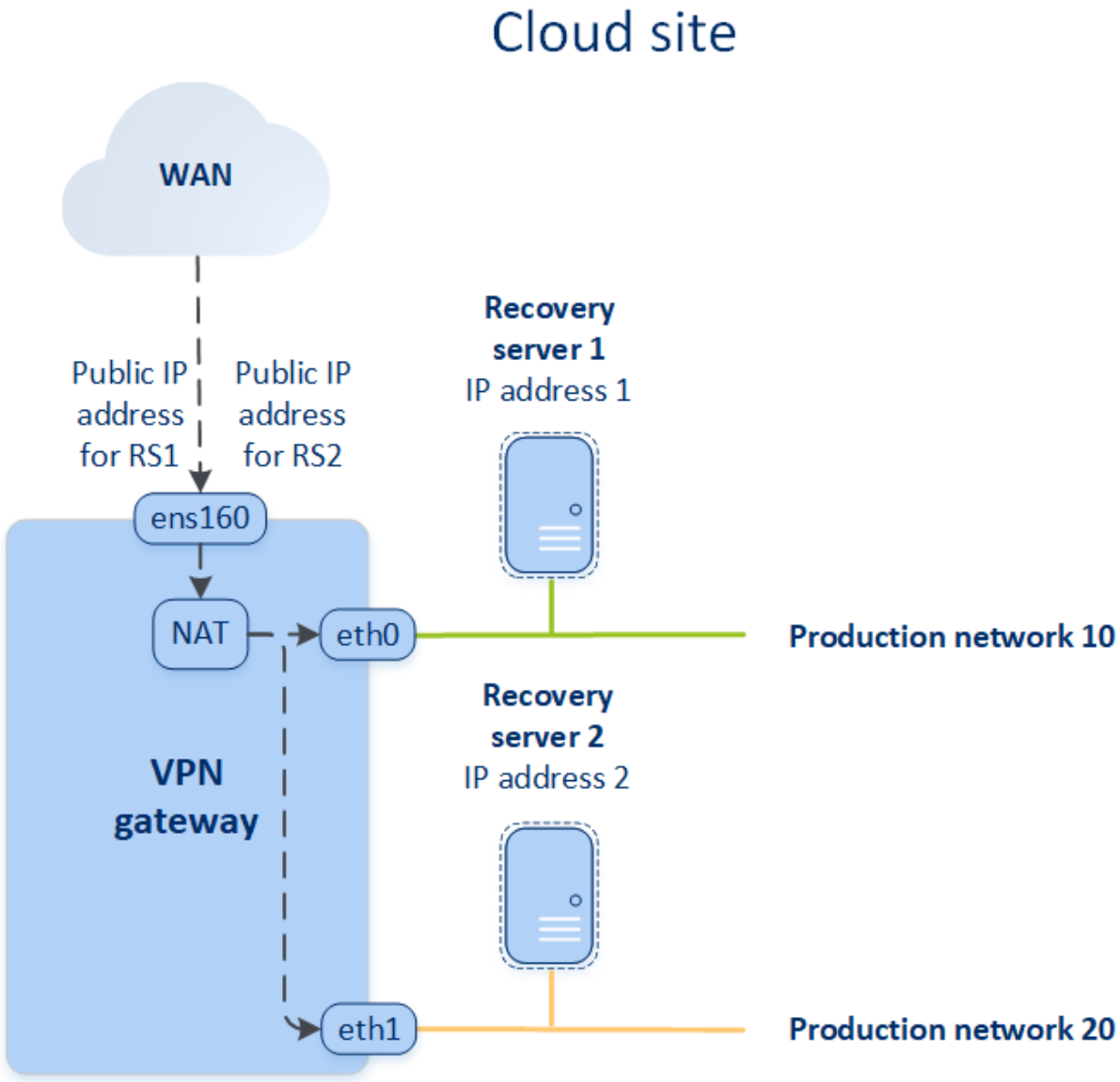
復元サーバーは、クラウドに保存されている保護されたサーバーのバックアップに基づく元のマシンのレプリカです。復元サーバーは、災害発生時にワークロードを元のサーバーから切り替えるのに使用されます。

復元サーバーを作成する際、以下のネットワークパラメータを指定する必要があります。

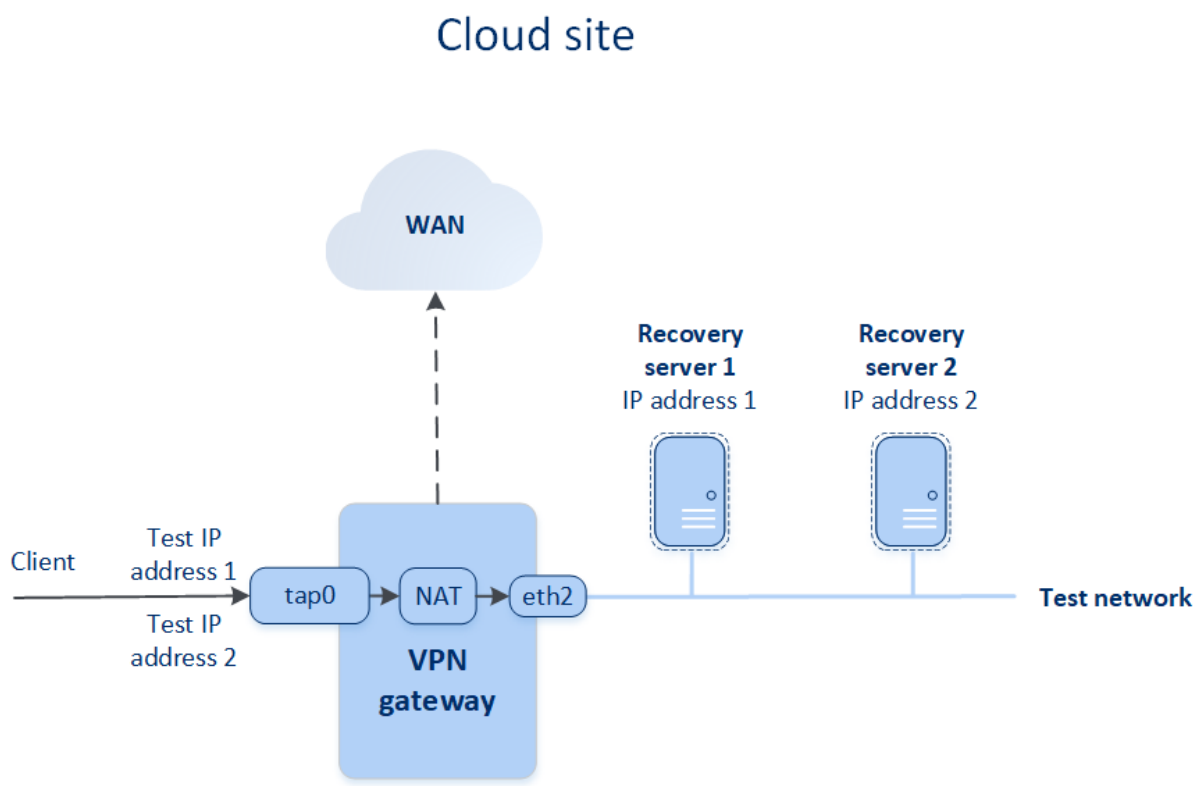
- **クラウドネットワーク**（必須）: 復元サーバーが接続されるクラウドネットワークです。
- **本番ネットワークにおける IP アドレス**（必須）:復元サーバー用の仮想マシンが起動する IP アドレス。このアドレスは本番ネットワークおよびテストネットワークの両方で使用されます。起動する前に、DHCPを介してIPアドレスを取得するよう仮想マシンを設定します。
- **テストIPアドレス**（オプション）:テストフェールオーバー中に顧客の稼働中ネットワークから復元サーバーにアクセスして、稼働中のIPアドレスが同じネットワーク内で重複しないようにするためのIPアドレス。このIPアドレスは本番ネットワークのIPアドレスとは異なります。ローカルサイトのサーバーは、テストIPアドレスを介してフェールオーバーのテスト中に復元サーバーに到達できますが、逆方向のアクセスは利用できません。復元サーバーの作成中に**インターネットアクセス**オプションが選択される場合、テストネットワークにおける復元サーバーからのインターネットアクセスが利用できます。
- **パブリックIPアドレス**（オプション）:インターネットから復元サーバーにアクセスするためのIPアドレス。サーバーにパブリックIPアドレスがない場合、ローカルネットワークからのみアクセスできます。
- **インターネットアクセス**（オプション）: 復元サーバがインターネットにアクセスすることを可能にします（本番およびテストのフェイルオーバーの両方）。

パブリックおよびテストIPアドレス

復元サーバー作成時にパブリックIPアドレスを割り当てた場合、復元サーバーはこのIPアドレスを介してインターネットから利用可能になります。ターゲットパブリックIPアドレスを持つパケットがインターネットから届くと、VPNゲートウェイはNATを使用してそれを適切な本番IPアドレスに再マッピングし、対応するリカバリサーバーに送信します。



復元サーバー作成時にテストIPアドレスを割り当てた場合、復元サーバーはこのIPアドレスを介してテストネットワークで利用可能になります。テストフェールオーバーを実行すると、元のマシンは実行されたままになり、同じIPアドレスを持つ復元サーバーがクラウドのテストネットワークで起動されます。テストネットワークが隔離されているので、IPアドレスの競合はありません。テストネットワーク内の復元サーバーは、NATを介して本番IPアドレスに再マッピングされる、それらのテストIPアドレスにより到達可能です。



サイト間Open VPNの詳細については、"サイトツーサイトOpen VPN - 追加情報"（94ページ）を参照してください。

プライマリサーバー

プライマリサーバーは、復元サーバーと比較すると、ローカルサイト上にリンクされたマシンがない仮想マシンです。プライマリサーバーは、レプリケーションによるアプリケーションの保護や、さまざまな補助サービスの実行などに使用されます（Webサーバーなど）。

通常、プライマリサーバーは、重要なアプリケーションを実行するサーバー間でのリアルタイムデータレプリケーションに使用されます。アプリケーションのネイティブツールを使用して、自分でレプリケーションをセットアップします。例えば、ローカルサーバーとプライマリサーバーの間でActive Directoryレプリケーションまたは SQLレプリケーションを構成できます。

または、プライマリサーバーを AlwaysOn 可用性グループ（AAG）またはデータベース可用性グループ（DAG）に含めることもできます。

どちらの方法でも、アプリケーションと管理者権限についての深い知識が必要です。プライマリサーバーは、コンピューティングリソースと高速ディザスタリカバリストレージの領域を絶えず消費します。それらはお客様側でメンテナンスが必要です。レプリケーションの監視、ソフトウェアアップデートのインストール、バックアップです。メリットは、サーバー全体をクラウドにバックアップする場合と比較して、本番環境への負荷を最小限に抑えた最小限の RPO と RTO です。

プライマリサーバーは本番ネットワーク上でのみ常に起動されており、以下のネットワークパラメータがあります。

- **クラウドネットワーク**（必須）: プライマリサーバーが接続されるクラウドネットワークです。
- **本番ネットワークにおける IP アドレス**（必須）:プライマリサーバーが本番ネットワークで持つ IP アドレス。デフォルトでは、本番ネットワークの最初の空き IP アドレスが設定されています。
- **パブリックIPアドレス**（オプション）:インターネットからプライマリサーバーにアクセスするためのIPアドレス。サーバーにパブリックIPアドレスがない場合、インターネット経由ではなくローカルネットワークからのみアクセスできます。
- **インターネットアクセス**（オプション）: プライマリサーバーがインターネットにアクセスすることを可能にします。

マルチサイトIPsec VPN接続

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

マルチサイトIPsec VPN接続を使用して、セキュアなL3 IPsec VPN接続を介した単一ローカルサイトの接続、または複数ローカルサイトのCyber Disaster Recovery Cloudへの接続が行えます。

この接続タイプは、ディザスタリカバリシナリオが次のユースケースに該当する場合に便利です。

- 重要なワークロードをホストする単一のローカルサイトがある。
- 重要なワークロードをホストする複数のローカルサイトがある（異なるロケーションにオフィスがあるなど）。
- サードパーティ製ソフトウェアのサイト、もしくはマネージドサービスプロバイダのサイトを使用しており、 それらがIPsec VPNトンネルを介して接続されている。

ローカルサイトとクラウドサイト間のマルチサイトIPsec VPN通信を確立するには、**VPNゲートウェイ**が使用されます。Cyber Protectコンソールでマルチサイトipsec VPN通信の設定を開始する場合には、VPNゲートウェイが自動的にクラウドサイトに配置されます。クラウドネットワークセグメントを設定し、ローカルネットワークセグメントと重複しないようにする必要があります。セキュアなVPNトンネルがローカルサイトとクラウドサイト間に確立されます。ローカルサーバーとクラウドサーバーはこのVPNトンネルを介してあたかもそれらすべてが同じイーサネットセグメント内にあるかのように通信できます。

各ソースマシンを保護するために、クラウドサイトにリカバリサーバーを作成する必要があります。フェールオーバーイベントが生じるまで**スタンバイ**状態を保ちます。（**本番モード**で）災害が発生しフェールオーバープロセスを開始すると、保護されたマシンの厳密なコピーであるリカバリサーバーがクラウドで起動します。顧客は、バックグラウンドでの変更に気付くことなくサーバーでの作業を続けることができます。

フェールオーバープロセスを**テストモード**で起動することもできます。これは、ソースマシンがまだ機能しているときに、同時にそれぞれの復元サーバーがクラウドで作成された特別な仮想ネットワーク（**テストネットワーク**）で起動することを意味します。テストネットワークは、他のクラウドネットワークセグメント内でのIPアドレスの重複を防ぐために隔離されています。

VPN ゲートウェイ

ローカルサイトとクラウドサイト間の通信を可能にする主要なコンポーネントは**VPNゲートウェイ**です。これは、特別なソフトウェアがインストールされ、ネットワークが特異的に構成されているクラウド内の仮想マシンです。VPNゲートウェイは以下の機能を提供します。

- ローカルネットワークのイーサネットセグメントとクラウド内の稼働中のネットワークをL3 IPsecモードで接続。
- テストネットワークと稼働しているネットワークのマシンのデフォルトルーターおよびNATとして動作。
- DHCPサーバーとして動作。本番ネットワークとテストネットワークのすべてのマシンはDHCPを介してネットワークの構成（IPアドレス、DNS設定）を取得します。クラウドサーバーは毎回、DHCPサーバーから同一のIPアドレスを取得します。

  必要に応じて、カスタムDNS構成を設定できます。詳細については、"カスタムDNSサーバーの構成"（45ページ）を参照してください。
- キャッシングDNSとして動作。

ルーティングが動作する仕組み

クラウドネットワーク間のルーティングはクラウドサイトのルーターで実行され、異なるクラウドネットワークに属するサーバー同士で通信できます。

ポイントツーサイトリモートVPNアクセス

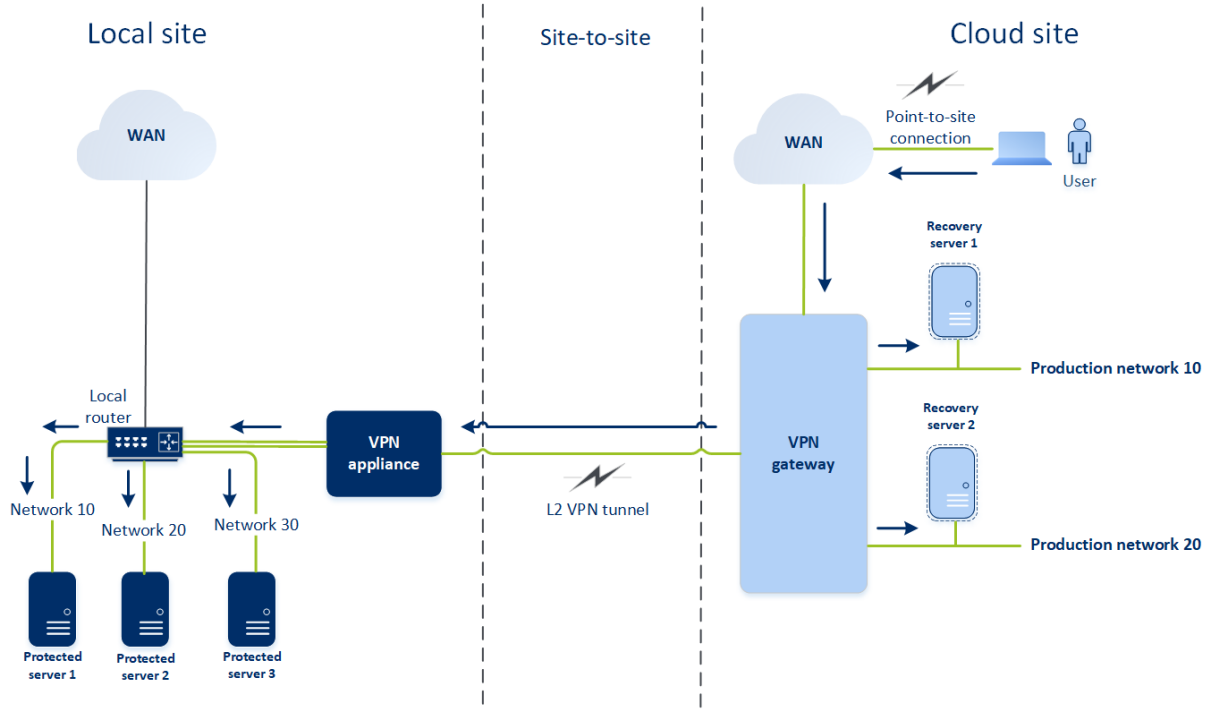
注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

ポイントツーサイト接続は、エンドポイントデバイス（コンピューターまたはノートPCなど）を使用して外部からクラウドサイトおよびローカルサイトにVPN経由で接続する安全な接続方法です。Cyber Disaster Recovery Cloudサイトへのサイト間Open VPN接続を確立した後に利用できます。このタイプの接続は次の場合に便利です。

- 多くの企業では、自社のサービスとWebリソースは、社内ネットワークに存在する場合のみ利用可能です。ポイントツーサイト接続を使用すると、ローカルサイトにセキュアに接続できます。
- 災害が発生し、ワークロードがクラウドサイトに切り替えられ、ローカルネットワークが停止した場合、クラウドサーバーに直接アクセスする必要があります。これは、クラウドサイトへのポイントツーサイト接続により可能となります。

ローカルサイトへのポイントツーサイト接続には、ローカルサイトにVPNアプライアンスをインストールしてからサイト間接続を設定し、その後ローカルサイトへのポイントツーサイト接続を設定する必要があります。これにより、リモートの従業員は、L2 VPNを介して社内ネットワークにアクセスできるようになります。

以下の図では、ローカルサイト、クラウドサイト、サーバー間通信が緑色で示されています。L2 VPNトンネルにより、ローカルサイトとクラウドサイトが接続されています。ユーザーがポイントツーサイト接続を確立すると、ローカルサイトへの通信がクラウドサイト経由で実行されます。



ポイントツーサイト構成では、証明書を使用してVPNクライアントを認証します。加えて、認証にはユーザー資格情報が使用されます。ローカルサイトへのポイントツーサイト接続については、次の点に注意してください。

- ユーザーはVPNクライアントでの認証にCyber Protect Cloudの資格情報を使用する必要があります。ユーザーには、「企業管理者」または「サイバープロテクション」ユーザーロールが必要です。
- OpenVPN設定を再生成した場合、クラウドサイトへのポイントツーサイト接続を使用しているすべてのユーザーにアップデートされた設定を提供する必要があります。

クラウドサイトで使用されていないカスタマー環境の自動削除

ディザスタリカバリサービスは、ディザスタリカバリ目的で作成されたカスタマー環境の使用状況をトラックします。カスタマー環境が使用されていない場合は、自動的に削除されます。

カスタマーテナントがアクティブかどうかを定義するために、次の条件が使用されます。

- 現在少なくとも1つのクラウドサーバーが存在するか、過去7日以内にクラウドサーバーが存在していた。
  または
- **[ローカルサイトへのVPNアクセス]** オプションが有効化されて、サイト間Open VPNトンネルが確立されるか、VPNアプライアンスから提供された過去7日のレポートデータが存在する。

残りのすべてのテナントは、非アクティブのテナントと見なされます。このようなテナントについてはシステムで次の処理が実行されます。

- VPNゲートウェイとテナントに関連するすべてのクラウドリソースを削除。
- VPNアプライアンスの登録を解除。

非アクティブなテナントは、接続が設定される前の状態にロールバックされます。

初期接続設定

このセクションでは、接続設定シナリオについて説明します。

クラウド限定モードの構成

クラウド限定モードでの接続を構成するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. **[クラウド限定]** を選択し、**[設定]** をクリックします。
   その結果、VPNゲートウェイと、定義済みのアドレスおよびマスクを持つクラウドネットワークがクラウドサイトに配置されます。

クラウドでのネットワーク管理方法およびVPNゲートウェイの設定方法については、「クラウドネットワークの管理」を参照してください。

サイト間Open VPNの構成

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

VPNアプライアンスの要件

システム要件

- 1個のCPU
- 1GBのRAM
- 8GBのディスク容量

ポート

- TCP 443（送信）- VPN接続用
- TCP 80（送信）- アプライアンスの自動アップデート用

ファイアウォールおよびネットワークセキュリティのその他のコンポーネントで、これらのポートを通じて任意のIPアドレスに接続できることを確認します。

サイト間Open VPN接続の構成

VPNアプライアンスは、安全なVPNトンネルを経由してローカルネットワークをクラウドに拡張します。この種の接続は、しばしば「サイトツーサイト」（S2S）接続と呼ばれます。以下の手順を実行す

るか、ビデオチュートリアルを視聴できます。

VPNアプライアンスを介した接続を構成するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. **[サイト間Open VPN接続]** を選択し、**[構成]** をクリックします。
   システムはクラウドにVPNゲートウェイを展開し始めます。これには時間がかかります。一方、次のステップに進むことができます。

   注意
   VPNゲートウェイは追加料金なしで提供されます。ディザスタリカバリ機能が使用されていない場合、つまりプライマリサーバーまたは復元サーバーがクラウドに7日間存在しない場合、このファイルは削除されます。

3. **[VPNアプライアンス]** ブロックで、**[ダウンロードとデプロイ]** をクリックします。使用している仮想化プラットフォームに応じて、VMware vSphere または Microsoft Hyper-V 用の VPN アプライアンスをダウンロードします。
4. アプライアンスをデプロイし、本番ネットワークに接続します。
   vSphere では、**無差別モード**および**偽装転送**が有効になっており、VPN アプライアンスを本番ネットワークに接続するすべての仮想スイッチに対して**受け入れる**に設定されていることを確認します。これらの設定にアクセスするには、vSphere クライアントで [ホスト] > **[概要]** > **[ネットワーク]** > [スイッチを選択] > **[編集設定...]** > **[セキュリティ]** を選択します。
   Hyper-Vで、1024MBのメモリを搭載した**第1世代**の仮想マシンを作成します。マシンの**ダイナミックメモリ**を有効にすることを推奨します。マシンが作成されたら、**[設定]** > **[ハードウェア]** > **[ネットワークアダプタ]** > **[高度な機能]** に移動し、**[MACアドレスなりすまし有効]** チェックボックスをオンにします。
5. アプライアンスの電源を投入します。
6. アプライアンスコンソールを開き、「admin」/「admin」ユーザー名とパスワードでログインします。
7. （オプション）パスワードを変更します。
8. （オプション）必要であれば、ネットワーク設定を変更します。どのインターフェースが、インターネット接続のWANとして使用されるかを定義します。
9. 企業管理者の資格情報を使用して、Cyber Protectionサービスにアプライアンスを登録します。
   これらの資格情報は、証明書を取得するときに一度だけ使用されます。データセンターのURLは定義済みです。

   注意
   アカウントに二要素認証が設定されている場合、TOTPコードの入力も求められます。二要素認証が有効になっているもののアカウントに設定されていない場合、VPNアプライアンスを登録することはできません。まず、Cyber Protectコンソールのログインページへ移動し、アカウントのための二要素認証設定を完了する必要があります。二要素認証の詳細については、管理ポータル管理者ガイドをご覧ください。

設定が完了すると、アプライアンスは**オンライン**ステータスになります。アプライアンスはVPNゲートウェイに接続し、すべてのアクティブなインターフェースからCyber Disaster Recovery Cloudサービスへのネットワークについての情報のレポートを開始します。Cyber Protectコンソールは、VPNアプライアンスからの情報に基づいてインターフェイスを表示します。

マルチサイトIPsec VPNの構成

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

次の2つの方法で、マルチサイトIPsec VPN接続を構成できます。

- **[ディザスタリカバリ]** > **[接続]** タブから。
- 1台または複数のデバイスで保護計画を適用します。次に自動で作成されたサイト間Open VPN接続を手動でマルチサイトIPsec VPN接続に切り替え、マルチサイトIPsec VPN設定を構成してIPアドレスを再割り当てします。

[接続] タブからマルチサイトIPsec VPN接続を構成するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. **[マルチサイトVPN接続]** セクションで、**[設定]** をクリックします。
   VPNゲートウェイがクラウドサイトに配置されます。
3. マルチサイトIPsec VPN設定を構成する。

保護計画からマルチサイトIPsec VPN接続を構成するには

1. Cyber Protectコンソールで **[デバイス]** に進みます。
2. 一覧から1台または複数のデバイスに保護計画を適用します。
   復元サーバーとクラウドインフラ設定が自動的にサイト間Open VPN接続に設定されます。
3. **[Disaster Recovery]** > **[接続]** の順に移動します。
4. **[プロパティを表示]** をクリックします。
5. **[マルチサイトIPsec VPNへの切り替え]** をクリックします。
6. マルチサイトIPsec VPN設定を構成する。
7. クラウドネットワークとクラウドサーバーのIPアドレスを再割り当てする。

マルチサイトIPsec VPN設定の構成

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

マルチサイトIPsec VPNを構成後、**[ディザスタリカバリ]** > **[接続]** タブでクラウドサイトとローカルサイトの設定を行う必要があります。

前提条件

- マルチサイトIPsec VPN接続が設定されている。マルチサイトIPsec VPN接続の設定の詳細については、"マルチサイトIPsec VPNの構成"（31ページ）を参照してください。
- 各ローカルIPsec VPNゲートウェイにはパブリックIPアドレスがあります。
- （稼働中のネットワークの）保護されているマシンのコピーであるクラウドサーバー用のIPアドレスと、復元サーバー用のIPアドレス（必要に応じて、1つまたは2つのIPアドレス）が、クラウドネットワークで確保されます。
- （ローカルサイトとクラウドサイト間でファイアウォールを使用する場合）ローカルサイトで次のIPプロトコルとUDPポートに許可を付与します。IPプロトコルID 50（ESP）、UDPポート500（IKE）、UDPポート4500。
- ローカルサイトのNAT-T構成が無効になっています。

マルチサイトIPsec VPN接続を構成するには

1. クラウドサイトに1つ以上のネットワークを追加します。
   a. **[ネットワークを追加]** をクリックします。

   注意
   クラウドネットワークを追加すると、テストフェールオーバーを実行するために、対応するテストネットワークが、同じネットワークアドレスとマスクを使用して自動的に追加されます。テストネットワーク内のクラウドサーバーには、クラウドで稼働中のネットワークと同じIPアドレスが与えられます。テストフェールオーバー中に稼働中のネットワークからクラウドサーバーにアクセスする必要がある場合は、復元サーバーを作成する際に、2番目のテストIPアドレスを割り当てます。

   b. **[ネットワークアドレス]** フィールドで、ネットワークのIPアドレスを入力します。
   c. **[ネットワークマスク]** フィールドで、ネットワークのマスクを入力します。
   d. **[追加]** をクリックします。
2. ローカルサイトの推奨事項に沿って、クラウドサイトに接続する各ローカルサイトの設定を行います。これらの推奨事項の詳細については、「"ローカルサイト向けの一般的な推奨事項"（33ページ）」を参照してください。
   a. **[接続を追加]** をクリックします。
   b. ローカルVPNゲートウェイの名前を入力します。
   c. ローカルVPNゲートウェイの公開IPアドレスを入力します。
   d. （オプション） ローカルVPNゲートウェイの説明を入力します。
   e. **[次へ]** をクリックします。
   f. **[事前共有鍵]** フィールドで、事前共有鍵を入力するか、**[新しい事前共有鍵を生成]** をクリックして自動生成される値を使用します。

   注意
   ローカルおよびクラウドのVPNゲートウェイに同じ事前共有鍵を使用する必要があります。

g. **[IPsec/IKEセキュリティ設定]** をクリックして、設定を行います。構成可能な設定の詳細については、「"IPsec/IKEセキュリティ設定"（34ページ）」を参照してください。

注意
自動入力されるデフォルトの設定か、カスタム値を使用できます。IKEv2プロトコル接続のみがサポートされています。VPN確立時のデフォルトの **[起動アクション]** は **[追加]**（ローカルVPNゲートウェイから接続が開始される）ですが、**[開始]**（クラウドVPNゲートウェイから接続が開始される）か **[ルート]**（ルートオプションをサポートするファイアウォールに適しています）に変更できます。

h. **[ネットワークポリシー]** を構成します。
ネットワークポリシーでは、ネットワークが接続するIPsec VPNを指定します。CIDR形式を使用して、ネットワークのIPアドレスとマスクを入力します。ローカルネットワークとクラウドネットワークワークは、重複してはいけません。

i. **[保存]** をクリックします。

ローカルサイト向けの一般的な推奨事項

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

ローカルサイトにマルチサイトIPsec VPN接続を設定する場合、次の推奨事項を考慮してください。

- IKEフェーズごとに、クラウドサイトで次のパラメータの値を少なくとも1つ設定します。暗号化アルゴリズム、ハッシュアルゴリズム、ディフィーヘルマン群数。
- IKEフェーズ2については、クラウドサイトで設定されるディフィーヘルマン群数の値の少なくとも1つでPerfect Forward Secrecyを有効にします。
- IKEフェーズ1とIKEフェーズ2の **[ライフタイム]** をクラウドサイトと同様に設定します。
- NATトラバーサル（NAT-T）を使用した構成はサポートされていません。ローカルサイトでNAT-T構成を無効にしてください。それ以外の場合、追加のUDPカプセルとのネゴシエイトを実行できなくなる可能性があります。
- どちらの側から接続を開始するかは、**[起動アクション]** 設定で定義します。デフォルト値の **[追加]** を選択すると、ローカルサイトから接続が開始され、クラウドサイトは接続の開始を待機します。クラウドサイトから接続を開始する場合は、値を **[開始]** に変更します。また、両方の側から接続を開始できるようにする場合（ルートオプションをサポートするファイアウォールに適しています）は、値を **[ルート]** に変更します。

別のソリューションの詳細と設定例については、次を参照してください。

- この一連のナレッジベースの記事
- このビデオの例

IPsec/IKEセキュリティ設定

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

Psec/IKEセキュリティパラメータの詳細を次の表に示します。

パラメータ	説明
暗号化アルゴリズム	転送中のデータが見えないようにするために使用される暗号化アルゴリズムです。デフォルト設定では、すべてのアルゴリズムが選択されています。各IKEフェーズを対象とするローカルゲートウェイデバイスで、選択されたアルゴリズムのうち少なくとも1つを構成する必要があります。
ハッシュアルゴリズム	データのインテグリティと真正性を検証するために使用されるハッシュアルゴリズムです。デフォルト設定では、すべてのアルゴリズムが選択されています。各IKEフェーズを対象とするローカルゲートウェイデバイスで、選択されたアルゴリズムのうち少なくとも1つを構成する必要があります。
ディフィーヘルマン群数	ディフィーヘルマン群数により、インターネット鍵交換（IKE）プロセスで使用される鍵の強度を定義します。 群位数が高いほど安全ですが、鍵の算出に要する時間は長くなります。 デフォルト設定では、すべての群が選択されています。各IKEフェーズを対象とするローカルゲートウェイデバイスで、選択された群のうち少なくとも1つを構成する必要があります。
ライフタイム（秒）	ライフタイム値により、ネゴシエーションが成功してから有効期限が切れるまでの、ユーザーパケットの暗号化/認証鍵のセットを持つ接続インスタンスの持続時間を決定します。 フェーズ1の範囲:900-28800秒（デフォルトでは28800秒）。 フェーズ2の範囲:900-3600秒（デフォルトでは3600秒）。 フェーズ2のライフタイムは、フェーズ1のライフタイムより短くする必要があります。

パラメータ	説明
	接続は、期限が切れるまでにキー設定チャネルを通じて再ネゴシエートされます。「**キー再設定のマージン時間**」を参照してください。ローカルサイドとリモートサイドでライフタイムが一致しない場合、ライフタイムが長い方のサイドで優先されたコネクションのクラッタが発生します。「**キー再設定のマージン時間**」と「**キー再設定ファズ**」も参照してください。
キー再設定のマージン時間（秒）	VPN接続のローカル側で交換のネゴシエートを試行する際に、接続の有効期限またはキー設定チャネルの有効期限に設けられるマージン時間。キー再設定の正確な時間は、**キー再設定ファズ**の値に基づいてランダムに選択されます。これはローカルにのみ関係します。リモート側でこれに同意する必要はありません。範囲:900-3600秒。デフォルト値は3600です。
リプレイウィンドウサイズ（パケット）	この接続に対応するIPsecのリプレイウィンドウサイズです。 デフォルトの-1にすると、strongswan.confファイルのcharon.replay_windowで設定される値を使用します。 32より大きな値は、Netlinkバックエンドを使用する際にのみサポートされます。 値を0にすると、IPsecリプレイ保護が無効になります。
キー再設定ファズ（%）	マージンバイト、マージンパケット、マージン時間をランダムに増加させて、キー再設定の間隔をランダムにする最大パーセンテージです（接続数の多いホストでは重要）。 キー再設定ファズ値は、100%を超過する場合があります。ランダムで増加させた後に、marginTYPEの値がlifeTYPEの値を超えてはいけません。TYPEには、bytes、packets、timeのいずれかが入ります。 値を0%にすると、ランダム化が無効になります。これはローカルにのみ関係します。リモート側でこれに同意する必要はありません。
DPDタイムアウト（秒）	デッドピア検出（DPD）タイムアウトが発生した後の時間です。値は30より上で指定できます。デフォルト値は30です。
デッドピア検出（DPD）タイムアウトアク	デッドピア検出（DPD）タイムアウトが発生した後

パラメータ	説明
ション	に実行するアクションです。 **再起動**: DPDタイムアウトが発生したときに、セッションを再起動します。 **クリア**: DPDタイムアウトが発生したときに、セッションを終了します。 **指定しない**: DPDタイムアウトが発生したときのアクションを指定しません。
起動アクション	どちらの側から接続を開始してVPN接続のトンネルを確立するかを決定します。 **追加**: ローカルVPNゲートウェイから接続を開始します。 **開始**: クラウドVPNゲートウェイから接続を開始します。 **ルート**:ルートオプションをサポートするVPNゲートウェイに適しています。トンネルは、ローカルのVPNゲートウェイまたはクラウドのVPNゲートウェイのいずれかから開始されたトラフィックが存在する場合にのみ起動します。

Active Directoryドメインサービスのアベイラビリティーに関する推奨事項

保護済みワークロードがドメインコントローラーでの認証を必要する場合は、ディザスタリカバリサイトにActive Directoryドメインコントローラー（AD DC）インスタンスを用意することを推奨します。

L2 Open VPN接続用Active Directoryドメインコントローラー

L2 Open VPN接続を使用する場合、テストフェールオーバーまたは本番フェールオーバーの間、保護済みワークロードのIPアドレスはクラウドサイトで保持されます。そのため、テストフェールオーバーまたは本番フェールオーバーの間のAC DCのIPアドレスは、ローカルサイトのものと同じになります。

カスタムDNSを使用する場合は、すべてのクラウドサーバーに対して独自のカスタムDNSサーバーを設置できます。詳細については、"カスタムDNSサーバーの構成"（45ページ）を参照してください。

L3 IPsec VPN接続用Active Directoryドメインコントローラー

L3 IPsec VPN接続を使用する場合、保護済みワークロードのIPアドレスはクラウドサイトで保持されません。そのため、本番フェールオーバーを実行する前に、他の専用AD DCインスタンスをプライマリサーバーとしてクラウドサイトに用意することを推奨します。

専用AD DCインスタンスをプライマリサーバーとしてクラウドサイトで設定する場合の推奨事項は次の通りです。

- Windowsファイアウォールをオフにする。
- プライマリサーバーをActive Directoryサービスに接続する。
- プライマリサーバーがインターネットに接続できることを確認する。
- Active Directory機能を追加する。

カスタムDNSを使用する場合は、すべてのクラウドサーバーに対して独自のカスタムDNSサーバーを設置できます。詳細については、"カスタムDNSサーバーの構成"（45ページ）を参照してください。

ポイントツーサイトリモートVPNアクセスの構成

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

ローカルサイトにリモート接続する必要がある場合は、ローカルサイトへのポイントツーサイト接続を構成できます。以下の手順を実行するか、ビデオチュートリアルを視聴できます。

前提条件

- サイト間Open VPN接続が設定されている。
- VPNアプライアンスがローカルサイトにインストールされている。

ローカルサイトへのポイントツーサイト接続を構成するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. **[プロパティを表示]** をクリックします。
3. **[ローカルサイトへのVPNアクセス]** オプションを有効にします。
4. ローカルサイトへのポイントツーサイト接続を確立する必要があるユーザーが、
   - Cyber Protect Cloudにユーザーアカウントを所有していることを確認する。これらの資格情報は、VPNクライアントでの認証に使用されます。所有していない場合は、Cyber Protect Cloudにユーザーアカウントを作成します。
   - 「企業管理者」または「サイバープロテクション」ユーザーロール。
5. OpenVPNクライアントの構成
   a. OpenVPNクライアントバージョン2.4.0以降を、https://openvpn.net/community-downloads/からダウンロードします。
   b. ローカルサイトに接続するマシンにOpenVPNクライアントをインストールします。
   c. **[OpenVPN の設定のダウンロード]** をクリックします。構成ファイルは、組織の「企業管理者」または「サイバープロテクション」ユーザーロールを持つユーザーに対して有効です。
   d. OpenVPNにダウンロード済みの設定をインポートします。
   e. Cyber Protect Cloudユーザーの資格情報でOpenVPNクライアントにログインします（上記の手順4を参照）。
   f. （オプション）組織で二要素認証が有効になっている場合は、1回限りのTOTPコードを入力する必要があります。

重要
アカウントで二要素認証を有効化した場合は、構成ファイルを再生成して、既存のOpenVPNで構成ファイルを更新する必要があります。アカウントに二要素認証を設定するには、Cyber Protect Cloudに再度ログインする必要があります。

これによりユーザーはローカルサイト上のマシンに接続できるようになります。

ネットワーク管理

このセクションでは、ネットワーク管理シナリオについて説明します。

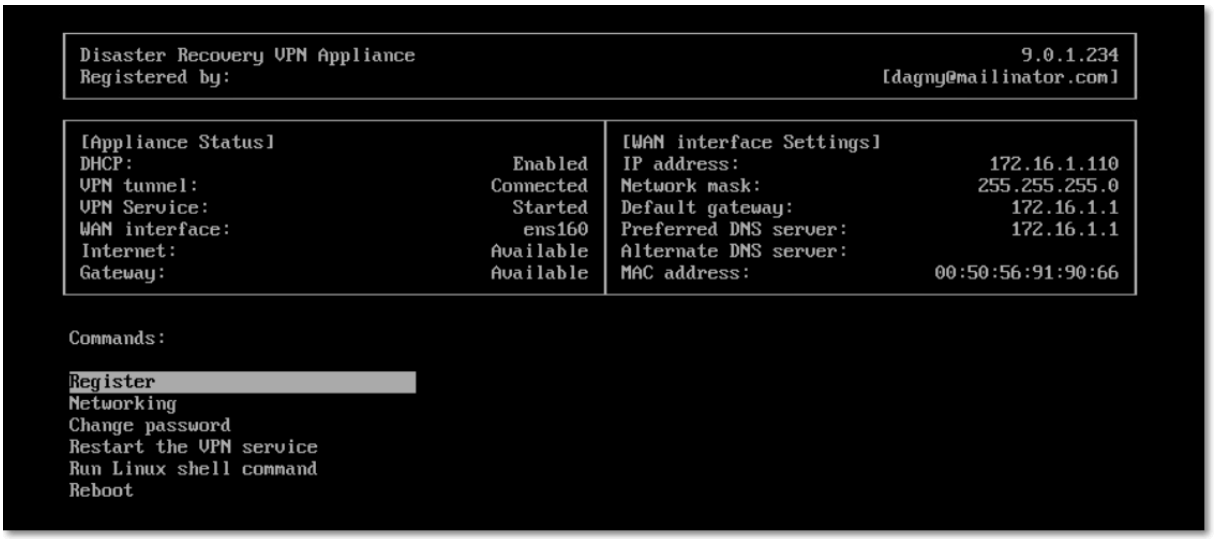
ネットワークの管理

注意
適用されるライセンスモデルによっては、一部の機能で追加のライセンスが必要になる場合があります。

サイト間Open VPN接続

ローカルサイトにネットワークを追加してクラウドに拡張するには

1. VPNアプライアンスで、クラウド内に拡張するローカルネットワークとの新しいネットワークインターフェースを設定します。
2. VPNアプライアンスコンソールにログインします。
3. **ネットワーク**セクションで、新しいインターフェースのためのネットワーク設定を行ないます。



VPNアプライアンスは、すべてのアクティブなインターフェイスからCyber Disaster Recovery Cloudへのネットワークについての情報のレポートを開始します。Cyber Protectコンソールは、VPNアプライアンスからの情報に基づいてインターフェイスを表示します。

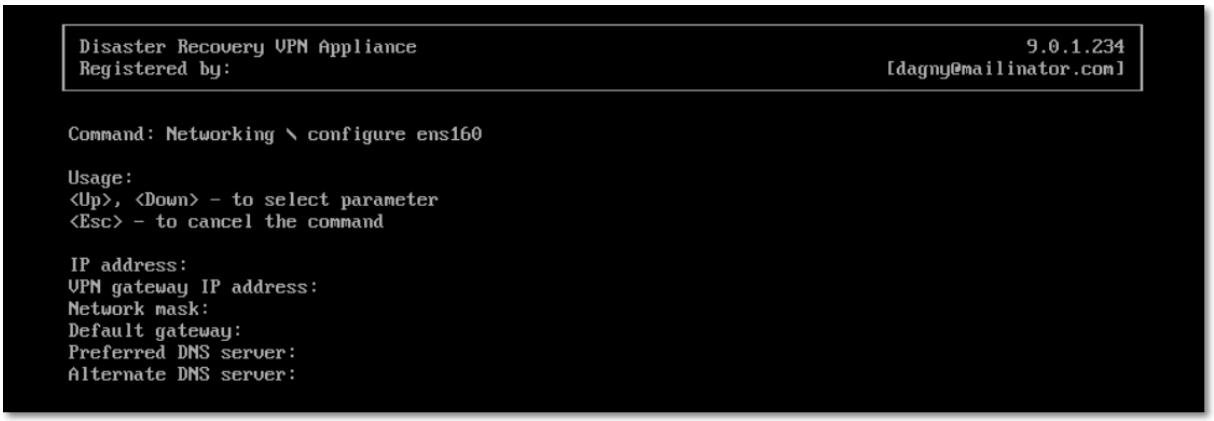
クラウドに拡張したネットワークを削除するには

1. VPNアプライアンスコンソールにログインします。
2. **ネットワーク**セクションで、削除するインターフェースを選択してから、**[ネットワーク設定の消去]** をクリックします。
3. 処理を確認します。

その結果、セキュアなVPNトンネル経由でのクラウドへのローカルネットワーク拡張が停止します。このネットワークは独立したクラウドセグメントとして稼働します。このインターフェースを使用してクラウドサイトから（へ）トラフィックを渡すと、クラウドサイトから（へ）のすべてのネットワーク接続が切断されます。

ネットワークパラメータを変更するには

1. VPNアプライアンスコンソールにログインします。
2. **ネットワーク**セクションで、編集するインターフェースを選択します。
3. **[ネットワーク設定の編集]** をクリックします。
4. 2つの可能なオプションのうちの1つを選択します。
   - DHCPを介した自動ネットワーク構成については、**[DHCPを使用]** をクリックします。処理を確認します。
   - 手動ネットワーク構成については、**[静的IPアドレスを設定]** をクリックします。次の設定を編集に使用できます。
     - **[IP アドレス]**: ローカルネットワークにおけるインターフェースの IP アドレスです。
     - **[VPNゲートウェイのIPアドレス]**: 適切なCyber Disaster Recovery Cloudサービス作業のためにネットワークのクラウドセグメント用に予約されている特別なIPアドレスです。
     - **[ネットワークマスク]**: ローカルネットワークのネットワークマスクです。
     - **[デフォルトゲートウェイ]**: ローカルサイト上のデフォルトゲートウェイです。
     - **[優先 DNS サーバー]**: ローカルサイト上のプライマリ DNS サーバーです。
     - **[代替 DNS サーバー]**: ローカルサイト上のセカンダリ DNS サーバーです。



- 必要な変更を実行し、[実行] をクリックして確認します。

クラウド限定モード

クラウドには最大で23個のネットワークを設定できます。

新しいクラウドネットワークを追加するには

1. **[Disaster Recovery]** > **[接続]** の順に移動します。
2. **[クラウドサイト]** で、**[クラウドネットワークを追加]** をクリックします。
3. ネットワークアドレスとマスクを含む、クラウドネットワークパラメータを定義します。準備ができたら、**[完了]** をクリックします。

その結果、定義済みのアドレスおよびマスクを持つ追加のクラウドネットワークがクラウドサイトに作成されます。

クラウドネットワークを削除するには

注意
1つ以上のクラウドサーバーが含まれているクラウドネットワークは、削除できません。まずクラウドサーバーを削除し、それからネットワークを削除します。

1. **[Disaster Recovery]** > **[接続]** の順に移動します。
2. **クラウドサイト**で、削除するネットワークアドレスをクリックします。
3. **[削除]** をクリックして、操作を確定します。

クラウドネットワークパラメータを変更するには

1. **[Disaster Recovery]** > **[接続]** の順に移動します。
2. **クラウドサイト**で、編集するネットワークアドレスをクリックします。
3. **[編集]** をクリックします。
4. ネットワークアドレスとマスクを定義し、**[完了]** をクリックします。

IPアドレスの再構成

適切なディザスタリカバリパフォーマンスのために、ローカルサーバとクラウドサーバに割り当てられているIPアドレスは一致している必要があります。IPアドレスに矛盾や不一致がある場合は、**[Disaster Recovery]** > **[接続]** の対応するネットワークの横に感嘆符が表示されます。

IPアドレスの不一致の、一般的に知られている理由の幾つかを以下に示します。

1. 復元サーバーが、あるネットワークから別のネットワークに移行された、またはクラウドネットワークのネットワークマスクが変更されました。その結果、クラウドサーバーに、接続されていないネットワークからのIPアドレスがあります。
2. 接続タイプが、サイト間接続なしからサイト間接続へと切り替えられました。その結果、ローカルサーバーは、クラウドサイト上の復元サーバーのために作成されたものとは異なるネットワークに配置されます。
3. 接続タイプが、サイト間Open VPNからマルチサイトIPsec VPN、またはマルチサイトIPsec VPNからサイト間Open VPNに切り替えられました。このシナリオの詳細については、「接続の切り替え」と「IPアドレスの再割り当て」を参照してください。
4. VPNアプライアンスサイトで以下のネットワークパラメータを編集します。
   - ネットワーク設定を介してインターフェースを追加
   - インターフェース設定を介してネットワークマスクを手動で編集
   - DHCPを介してネットワークマスクを編集

- インターフェース設定を介してネットワークアドレスおよびマスクを手動で編集
- DHCPを介してネットワークマスクおよびアドレスを編集

上記のアクションの結果、クラウドサイト上のネットワークがローカルネットワークのサブセットまたはスーパーセットになるか、またはVPNアプライアンスインターフェースが、異なるインターフェイスに対して同じネットワーク設定をレポートすることがあります。

ネットワーク設定上の問題を解決するには

1. IPアドレスの再構成が必要なネットワークをクリックします。
   選択したネットワーク内のサーバーのリスト、それらのステータス、およびIPアドレスが表示されます。ネットワーク設定に矛盾があるサーバーは、感嘆符でマークされます。
2. サーバー用のネットワーク設定を変更するには、**[サーバーへ移動]** をクリックします。すべてのサーバー用のネットワーク設定を一括で変更するには、通知ブロックで、**[変更]** をクリックします。
3. **[新規IP]** および **[新規テストIP]** フィールドで定義することにより、必要に応じてIPアドレスを変更します。
4. 準備ができたら、**[確認]** をクリックします。

サーバーを適切なネットワークに移動する

ディザスタリカバリ保護計画を作成し、選択したデバイスに適用するとき、システムによってデバイスのIPアドレスがチェックされ、IPアドレスに適したクラウドネットワークが存在しない場合はクラウドネットワークが自動的に作成されます。デフォルトでは、そのようなクラウドネットワークにはIANAがプライベートでの使用に推奨している最大範囲（10.0.0.0/8、172.16.0.0/12、192.168.0.0/16）が設定されます。ネットワークマスクを編集すれば、ネットワーク範囲を狭くすることができます。

選択されたデバイスが複数のローカルネットワークに属している場合、クラウドサイトのネットワークはそれらのローカルネットワークのスーパーセットになります。この場合、クラウドネットワークを再設定するには次のようにします。

1. ネットワークサイズの再設定が必要なクラウドネットワークをクリックしてから、**[編集]** をクリックします。
2. ネットワークサイズを正しい値に再設定します。
3. その他の必要なネットワークを作成します。
4. ネットワークに接続されたデバイス数の横にある通知アイコンをクリックします。
5. **[適切なネットワークに移動する]** をクリックします。
6. 適切なネットワークに移動するサーバーを選択してから、**[移動]** をクリックします。

VPNアプライアンス設定の管理

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

Cyber Protectコンソール（**[ディザスタリカバリ]** > **[接続]**）では、次の操作を実行できます。

- ログファイルをダウンロードする。
- アプライアンスの登録を解除する（VPNアプライアンスの設定をリセットするか、クラウド限定モードに切り替える必要がある場合）。

これらの設定にアクセスするには、[**VPNアプライアンス**] ブロックの [**i**] アイコンをクリックします。

VPNアプライアンスコンソールでは、次の操作を実行できます。

- アプライアンスのパスワードを変更する。
- ネットワーク設定を表示/変更する。インターネット接続用のWANとして使用するインターフェースを定義する。
- （登録を繰り返すことにより）登録アカウントを登録/変更する。
- VPNサービスを再起動する。
- VPNアプライアンスを再起動する。
- Linux Shellコマンドを実行する（高度なトラブルシューティングの場合のみ）。

VPNゲートウェイの再インストール

VPNゲートウェイに解決できない問題が発生した場合は、VPNゲートウェイを再インストールすることをお勧めします。次のような問題が発生する可能性があります。

- VPNゲートウェイが、**エラー**ステータスである。
- VPNゲートウェイが、長時間**保留中**ステータスになる。
- VPNゲートウェイのステータスが、長時間確定されない。

VPNゲートウェイの再インストールでは、既存のVPNゲートウェイ仮想マシンを完全に削除し、テンプレートから新しい仮想マシンをインストールし、新しい仮想マシンに以前のVPNゲートウェイの設定を適用するという自動的な操作が実行されます。

前提条件:

クラウドサイトへの接続タイプの1つを設定する必要があります。

VPNゲートウェイを再インストールするには

1. Cyber Protectコンソールで、[**ディザスタリカバリ**] > [**接続**] の順に移動します。
2. VPNゲートウェイのギアアイコンをクリックし、[**VPNゲートウェイを再インストール**] を選択します。
3. [**VPNゲートウェイを再インストール**] ダイアログで、ログイン情報を入力します。
4. [**再インストール**] をクリックします。

サイト間接続の有効化または無効化

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

次のような場合にサイト間接続を有効にできます。

- ローカルサイトのサーバーと通信するためにクラウドサイトのクラウドサーバーが必要である場合。
- クラウドへのフェールオーバーの後、ローカルインフラストラクチャはリカバリされ、サーバーをローカルサイトにフェールバックできます。

サイト間接続を有効にするには

1. **[Disaster Recovery]** > **[接続]** の順に移動します。
2. **[プロパティを表示]** をクリックしてから、**[サイト間接続]** オプションを有効にします。

その結果、ローカルサイトとクラウドサイト間のサイト間VPN接続が有効になります。Cyber Disaster Recovery Cloudサービスは、VPNアプライアンスからネットワーク設定を取得し、ローカルネットワークをクラウドサイトに拡張します。

ローカルサイトのサーバーと通信するためにクラウドサイトのクラウドサーバーが必要ない場合は、サイト間接続を無効にできます。

サイト間接続を無効にするには

1. **[Disaster Recovery]** > **[接続]** の順に移動します。
2. **[プロパティを表示]** をクリックしてから、**[サイト間接続]** オプションを無効にします。

その結果、ローカルサイトがクラウドサイトから切断されます。

サイト間接続タイプの切り替え

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

サイト間Open VPN接続からマルチサイトIPsec VPN接続、およびマルチサイトIPsec VPN接続からサイト間Open VPN接続への切り替えを簡単に行うことができます。

接続タイプを切り替える際には、アクティブなVPN接続が削除されますが、クラウドサーバーとネットワーク構成は保持されます。ただし、引き続きクラウドネットワークとクラウドサーバーのIPアドレスを再割り当てする必要があります。

次の表では、サイト間Open VPN接続とマルチサイトIPsec VPN接続の基本的な特徴を比べています。

	サイト間Open VPN	マルチサイトIPsec VPN
ローカルサイトサポート	単一	単一、複数
VPNゲートウェイモード	L2 Open VPN	L3 IPsec VPN
ネットワークセグメント	ローカルネットワークをクラウドネットワークへ拡張	ローカルネットワークとクラウドネットワークワークのセグメントは、重複できない
ローカルサイトへのポイント	はい	いいえ

	サイト間Open VPN	マルチサイトIPsec VPN
ツーサイトアクセスをサポート		
クラウドサイトへのポイントツーサイトアクセスをサポート	はい	はい
パブリックIPの提供項目が必要	いいえ	はい

サイト間Open VPN接続からマルチサイトIPsec VPN接続へ切り替えるには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. **[プロパティを表示]** をクリックします。
3. **[マルチサイトIPsec VPNへの切り替え]** をクリックします。
4. **[再構成]** をクリックします。
5. クラウドネットワークとクラウドサーバーのIPアドレスを再割り当てする。
6. マルチサイトIPsec接続設定を構成する。

マルチサイトIPsec VPN接続からサイト間Open VPN接続へ切り替えるには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. **[プロパティを表示]** をクリックします。
3. **[サイト間Open VPNへの切り替え]** をクリックします。
4. **[再構成]** をクリックします。
5. クラウドネットワークとクラウドサーバーのIPアドレスを再割り当てする。
6. サイト間接続設定を行う。

IPアドレスの再割り当て

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

次の場合に設定を完了するには、クラウドネットワークとクラウドサーバーのIPアドレスを再割り当てする必要があります。

- サイト間Open VPNからマルチサイトIPsec VPNに切り替えた後、もしくはその逆。
- 保護計画を適用した後（マルチサイトIPsec VPN接続が構成される場合）。

クラウドネットワークのIPアドレスを再割り当てするには

1. **[接続]** タブで、クラウドネットワークのIPアドレスをクリックします。
2. **[ネットワーク]** ポップアップで、**[編集]** をクリックします。
3. 新しいネットワークアドレスとネットワークマスクを入力します。
4. **[完了]** をクリックします。

クラウドネットワークのIPアドレスを再割り当てしたら、再割り当てされたクラウドネットワークに属するクラウドサーバーの再割り当てを行う必要があります。

サーバーのIPアドレスを再割り当てするには

1. **[接続]** タブで、クラウドネットワークのサーバーのIPアドレスをクリックします。
2. **[サーバー]** ポップアップで、**[IPアドレスを変更する]** をクリックします。
3. **[IPアドレスを変更する]** ポップアップで、サーバーの新しいIPアドレスを入力するか、再割り当てされたクラウドネットワークに含まれる自動生成されたIPアドレスを使用します。

   注意
   Cyber Disaster Recovery Cloudにより、ネットワークIPアドレスの再割り当て前にクラウドネットワークに含まれていたすべてのクラウドサーバーに、クラウドネットワークのIPアドレスが割り当てられます。推奨されたIPアドレスをすべてのクラウドサーバーに対するIPアドレスの再割り当てにすぐに使用できます。

4. **[確認]** をクリックします。

カスタムDNSサーバーの構成

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

接続を構成するときには、Cyber Disaster Recovery Cloudがクラウドネットワークインフラストラクチャを作成します。クラウドDHCPサーバーにより、復元サーバーとプライマリサーバーに自動的にデフォルトのDNSサーバーが割り当てられます。ただし、デフォルト設定を変更してカスタムDNSサーバーを構成することが可能です。新しいDNS設定は、DHCPサーバーに対する次回のリクエスト時に適用されます。

前提条件:

クラウドサイトへの接続タイプの1つを設定する必要があります。

カスタムDNSサーバーを構成するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. **[プロパティを表示]** をクリックします。
3. **[デフォルト（クラウドサイトにより提供）]** をクリックします。
4. **[カスタムサーバー]** を選択します。
5. DNSサーバーのIPアドレスを入力します。
6. [オプション]別のDNSサーバーを追加する場合は、**[追加]** をクリックし、DNSサーバーのIPアドレスを入力します。

注意
カスタムDNSサーバーの追加後、デフォルトのDNSサーバーを追加することもできます。そのようにすることで、カスタムDNSサーバーが利用不能な場合に、Cyber Disaster Recovery Cloudがデフォルトの DNSサーバーを使用します。

7. **[完了]** をクリックします。

カスタムDNSサーバーの削除

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

カスタムDNSの一覧からDNSサーバーを削除できます。

前提条件:

カスタムDNSサーバーが構成されている。

カスタムDNSサーバーを削除するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. **[プロパティを表示]** をクリックします。
3. **[カスタムサーバー]** をクリックします。
4. DNSサーバーの横にある削除アイコンをクリックします。

注意
利用できるカスタムDNSサーバーが1台だけの場合、削除操作は無効です。カスタムDNSサーバーをすべて削除する場合は、**[デフォルト（クラウドサイトにより提供）]** を選択します。

5. **[完了]** をクリックします。

MACアドレスをダウンロードする

MACアドレスの一覧をダウンロードしてから展開し、カスタムDHCPサーバーの構成にインポートすることができます。

前提条件:

- クラウドサイトへの接続タイプの1つを設定する必要があります。
- 少なくとも、MACアドレスを持つプライマリサーバーまたは復元サーバーを1台構成する必要があります。

MACアドレスの一覧をダウンロードするには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. **[プロパティを表示]** をクリックします。
3. **[MACアドレスの一覧をダウンロード]** をクリックしてから、CSVファイルを保存します。

ローカルルーティングの設定

VPNアプライアンスを介してクラウドに拡張されているローカルネットワークに加えて、VPNアプライアンスに登録されていないもののその中のサーバーがクラウドサーバーと通信する必要がある他のローカルネットワークがあるかもしれません。そのようなローカルサーバーとクラウドサーバー間の接続を確立するため、ローカルルーティングを設定する必要があります。

ローカルルーティングを設定するには

1. **[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. **[プロパティを表示]** をクリックして、**[ローカルルーティング]** をクリックします。
3. CIDR表記でローカルネットワークを指定します。
4. **[保存]** をクリックします。

その結果、指定されたローカルネットワーク経由のサーバーがクラウドサーバーと通信できるようになります。

L2 VPNを介したDHCPトラフィックを許可

ローカルサイトのデバイスがDHCPサーバーからIPアドレスを取得する構成の場合、ディザスタリカバリによるDHCPサーバー保護を利用できます。つまり、DHCPサーバーをクラウドにフェールオーバーしている状態で、DHCPトラフィックをL2 VPN上で処理することが可能です。こうすれば、クラウド上で動作するDHCPサーバーから、ローカルデバイスへのIPアドレス割り当てを続行できます。

前提条件:

クラウドサイトへの接続タイプに、サイト間L2 VPN接続を設定する必要があります。

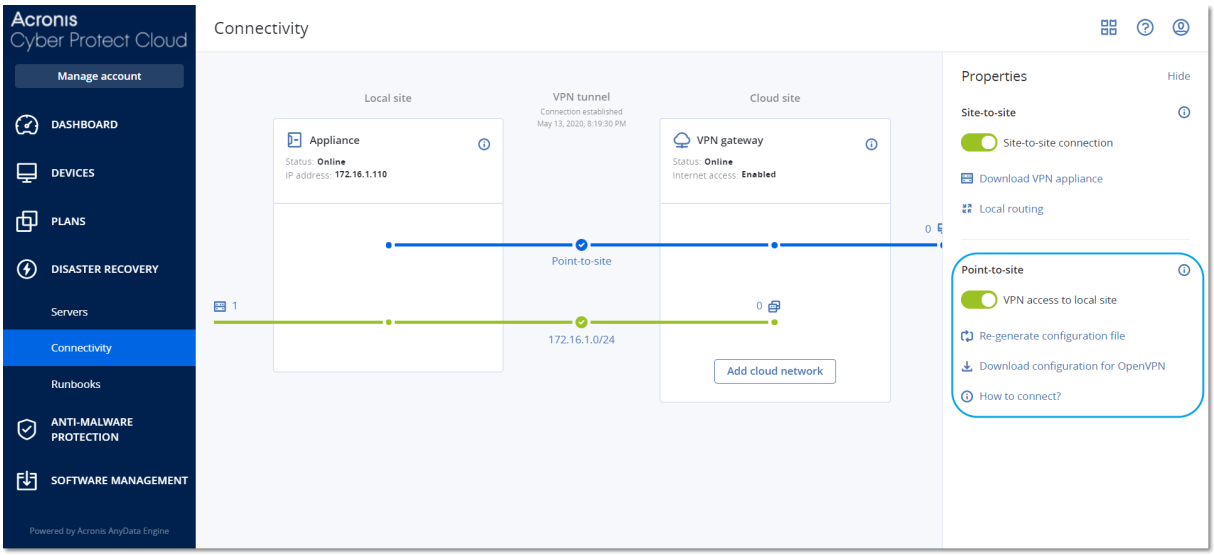
L2 VPN接続によるDHCPトラフィックを許可するには

1. **[ディザスタリカバリ]** > **[接続]** タブに移動します。
2. **[プロパティを表示]** をクリックします。
3. **[L2 VPNを介したDHCPトラフィックを許可]** スイッチを有効化します。

ポイントツーサイト接続設定の管理

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動し、右上隅の**[プロパティを表示]** をクリックします。



ローカルサイトへの VPN アクセス

このオプションは、ローカルサイトへのVPNアクセスの管理に使用します。デフォルト設定では、有効になっています。このオプションを無効にすると、ローカルサイトへのポイントツーサイトアクセスが許可されなくなります。

OpenVPNの設定をダウンロード

これは OpenVPN クライアントの設定ファイルをダウンロードします。このファイルは、クラウドサイトへのポイントツーサイト接続を確立するために必要です。

設定を再生成

OpenVPN クライアントの設定ファイルを再生成することができます。

これは、次の場合に必要です。

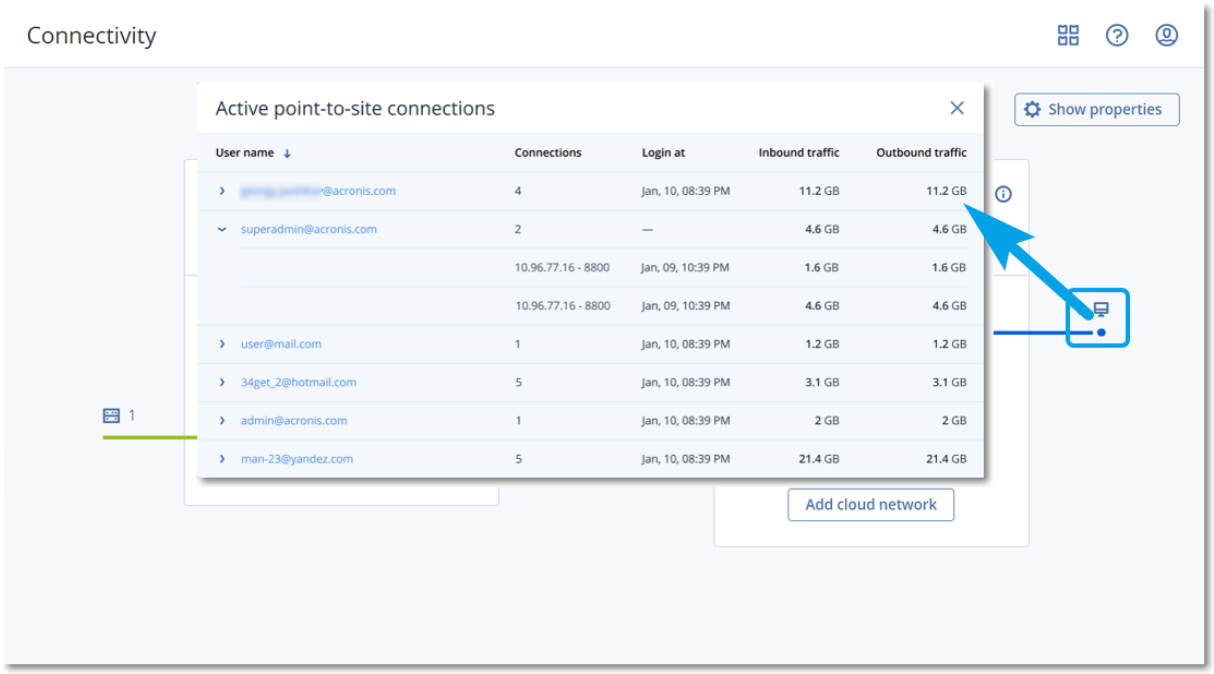
- 設定ファイルが侵害されていると思われる場合。
- 二要素認証がアカウントで有効になっていた場合。

設定ファイルが更新されるとすぐに、古い設定ファイルによる接続は不可能になります。ポイントツーサイト接続の使用を許可されているユーザーに新しいファイルを配布するようにしてください。

有効なポイントツーサイト接続

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

アクティブなポイントツーサイト接続は、**[ディザスタリカバリ]** > **[接続]** で確認できます。青の**ポイントツーサイト**ライン上のマシンアイコンをクリックすると、アクティブなポイントツーサイト接続に関する詳細な情報がユーザー名グループ別に表示されます。



ログを利用する

ディザスタリカバリでは、VPNアプライアンスとVPNゲートウェイのログが収集されます。ログは.txtファイルとして保存され、ZIPアーカイブに圧縮されます。アーカイブをダウンロードしてから展開し、トラブルシューティングや監視に利用できます。

次のリストでは、ZIPアーカイブの一部であるログファイルと、そこに含まれる情報について示します。

`dnsmasq.config.txt` - DNSとDHCPアドレスを提供するサービスの構成に関する情報が含まれているファイルです。

`dnsmasq.config.txt` - 現在のDHCPアドレスリースの情報が含まれているファイルです。

`dnsmasq_log.txt` - dnsmasqサービスのログが含まれているファイルです。

`ebtables.txt` - ファイアウォールテーブルに関する情報が含まれているファイルです。

`free.txt` - 空きメモリに関する情報が含まれているファイルです。

`ip.txt` - このファイルには、**ネットワークパケットのキャプチャ**の設定に使用できる名前を含む、ネットワークインターフェースの構成から得られたログが含まれています。

`NetworkManager_log.txt` - NetworkManagerサービスのログが含まれているファイルです。

`NetworkManager_status.txt` - NetworkManagerサービスのステータスに関する情報が含まれているファイルです。

`openvpn@p2s_log.txt` - OpenVPNサービスのログが含まれているファイルです。

`openvpn@p2s_status.txt` - VPNトンネルのステータスに関する情報が含まれているファイルです。

`ps.txt` - VPNゲートウェイまたはVPNアプライアンスで現在実行中のプロセスに関する情報が含まれているファイルです。

`resolf.conf.txt` - DNSサーバーの構成に関する情報が含まれているファイルです。

`routes.txt` - ネットワーキングのルートに関する情報が含まれているファイルです。

`uname.txt` - 現在稼働中のオペレーティングシステムのカーネルバージョンに関する情報が含まれているファイルです。

`uptime.txt` - オペレーティングシステムが再起動されなかった期間に関する情報が含まれているファイルです。

`vpnserver_log.txt` - VPNサービスのログが含まれているファイルです。

`vpnserver_status.txt` - VPNサーバーのステータスに関する情報が含まれているファイルです。

IPsec VPN接続に特化したログファイルについては、"マルチサイトIPsec VPNログファイル"（54ページ）を参照してください。

VPNアプライアンスログのダウンロード

VPNアプライアンスログを含むアーカイブをダウンロードしてから展開し、トラブルシューティングや監視に利用できます。

VPNアプライアンスログをダウンロードするには

1. **接続**ページで、VPNアプライアンスの横にあるギアアイコンをクリックします。
2. **[ログをダウンロード]** をクリックします。
3. （オプション）**[ネットワークパケットをキャプチャ]** を選択し、設定を構成します。詳細については、"ネットワークパケットのキャプチャ"（51ページ）を参照してください。
4. **[完了]** をクリックします。
5. ZIPアーカイブをダウンロードする準備が完了したら、**[ログをダウンロード]** をクリックして、ローカルに保存します。

VPNゲートウェイログのダウンロード

VPNゲートウェイログを含むアーカイブをダウンロードしてから展開し、トラブルシューティングや監視に利用できます。

VPNゲートウェイログをダウンロードするには

1. **接続**ページで、VPNゲートウェイの横にあるギアアイコンをクリックします。
2. **[ログをダウンロード]** をクリックします。
3. （オプション）**[ネットワークパケットをキャプチャ]** を選択してから、設定を構成します。詳細については、"ネットワークパケットのキャプチャ"（51ページ）を参照してください。
4. **[完了]** をクリックします。
5. ZIPアーカイブをダウンロードする準備が完了したら、**[ログをダウンロード]** をクリックして、ローカルに保存します。

ネットワークパケットのキャプチャ

ローカルの本番サイトとプライマリサーバーまたは復元サーバー間の通信をトラブルシュートおよび分析するには、VPNゲートウェイまたはVPNアプライアンスのネットワークパケットを収集します。

32000個のネットワークパケットが収集されるか、制限時間に到達すると、ネットワークパケットのキャプチャが停止し、結果が.libpcapファイルに書き込まれ、「logs」という名前のZIPアーカイブに追加されます。

構成可能な**ネットワークパケットのキャプチャ**設定の詳細を次の表に示します。

設定	説明
ネットワークインターフェース名	ネットワークパケットをキャプチャするネットワークインターフェース。すべてのネットワークインターフェースでネットワークパケットをキャプチャするには、**[すべて]** を選択します。
時間制限（秒）	ネットワークパケットキャプチャの時間制限。設定可能な最大値は1800です。
フィルタ処理	キャプチャ済みのネットワークパケットに適用される追加フィルタ。 プロトコル、ポート、方向、およびそれらの組み合わせを含む文字列を、スペースで区切って入力できます。例えば、「and」、「or」、「not」、「(」、「)」、「src」、「dst」、「net」、「host」、「port」、「ip」、「tcp」、「udp」、「icmp」、「arp」、「esp」などの文字列を使用できます。 括弧を使用する場合は、前後にスペースを挿入してください。また、IPアドレスやネットワークアドレスを入力することもできます（例:「icmp or arp」、「port 67 or 68」。）。 入力できる値の詳細については、Linuxのtcpdumpコマンドのヘルプを参照してください。

IPsec VPN設定のトラブルシューティング

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

IPsec VPN接続の設定時または使用時に、問題が発生することがあります。

発生した問題についてはIPsecログファイルで詳細を確認できます。また、IPsec VPN設定の問題箇所のトラブルシューティングを行い、発生する可能性がある一般的な問題に対するソリューションをチェックすることが可能です。

IPsec VPN設定の問題のトラブルシューティング

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

次の表では、 IPsec VPN設定について比較的よく起こる問題と、そのトラブルシュートの方法について説明します。

問題	考えられるソリューション
表示されるエラー:**IKEフェーズ1のネゴシエーションエラー。クラウド側とローカル側のIPsec IKEの設定を確認してください。**	**[再試行]** をクリックし、より具体的なエラーメッセージが表示されないか確認します。例えば、より具体的なエラーメッセージとしては、アルゴリズムの不一致や不正な事前共有鍵に関するエラーメッセージが挙げられます。 **注意** セキュリティ上の理由から、IPsec VPN接続には次のような制限事項が適用されます。 • IKEv1はRFC8247で非推奨とされています。これはセキュリティ上のリスクのためサポートされていません。IKEv2プロトコル接続のみがサポートされています。 • 次の暗号化アルゴリズムは安全ではないとみなされており、サポートされていません。DESおよび3DES。 • 次のハッシュアルゴリズムは安全ではないとみなされており、サポートされていません。SHA1およびMD5。 • ディフィーヘルマン群数2は安全ではないとみなされており、サポートされていません。
ローカルサイトとクラウドサイト間の接続ステータスが **[接続しています]** のままになる。	次の項目を確認します。 • UDPポート500が開いているか（ファイアウォールを使用する場合）。 • ローカルサイトとクラウドサイト間の接続。 • ローカルサイトのIPアドレスが正しいか。
ローカルサイトとクラウドサイト間の接続ステータスが **[接続を待機中]** のままになる。	クラウドサイトの **[起動アクション]** が **[追加]** に設定されている場合にこのステータスが表示されます。これは、クラウドサイトがローカルサイトからの接続が開始されるまで待機していることを意味します。 ローカルサイトから接続を開始します。

問題	考えられるソリューション
ローカルサイトとクラウドサイト間の接続ステータスが [**トラフィックを待機中**] のままになる。	クラウドサイトの [**起動アクション**] が [**ルート**] に設定されている場合にこのステータスが表示されます。 ローカルサイトからの接続が見込まれる場合は、次の内容を実施します。 • ローカルサイトからクラウドサイトの仮想マシンに対してpingを試行します。これは、Cisco ASAなどのデバイスでトンネルを確立するために必要な標準動作です。（ルートモード） • ローカルサイトの [**起動アクション**] を [**開始**] に設定して、ローカルサイトでトンネルが確立されたか確認します。
ローカルサイトとクラウドサイト間の接続が確立されたが、1つ以上のネットワークポリシーのダウンが表示される。	この問題は、以下が原因である可能性があります。 • クラウドIPsecサイトのネットワークマッピングがローカルサイトのネットワーキングと異なっている。 ローカルサイトとクラウドサイトのネットワークマッピングとネットワークポリシーの順序が正確に一致しているか確認します。 • ローカルサイトとクラウドサイト、またはそれらのいずれかの [**起動アクション**] が [**ルート**] に設定されている場合（例えばCisco ASAデバイス上）、このステータスに問題はなく、その時点ではトラフィックが発生していません。pingを試行して、トンネルが確立されていることを確認できます。pingが動作しない場合は、ローカルサイトとクラウドサイトのネットワークマッピングをチェックします。
特定のIPsec接続を再起動する。	特定のIPsec接続を再起動するには: 1. [**ディザスタリカバリ**] > [**接続**] 画面で、IPsec接続をクリックします。 2. [**接続を無効化**] をクリックします。 3. IPsec接続を再度クリックします。 4. [**接続を有効化**] をクリックします。

IPsec VPNログファイルのダウンロード

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

IPsec接続に関するその他の情報は、VPNサーバーのログファイルで確認できます。ログファイルは.ZIPアーカイブで圧縮されており、ダウンロードして展開可能です。

前提条件

マルチサイトIPsec VPN接続が設定されている。

ログファイルの.ZIPアーカイブをダウンロードするには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. クラウドサイトのVPNゲートウェイの横にあるギアアイコンをクリックします。
3. **[ログをダウンロードする]** をクリックします。
4. **[完了]** をクリックします。
5. ZIPアーカイブをダウンロードする準備が完了したら、**[ログをダウンロード]** をクリックして、ローカルに保存します。

マルチサイトIPsec VPNログファイル

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

ZIPアーカイブの一部であるIPsec VPNログファイルと、そこに含まれる情報を次のリストに示します。

- `ip.txt`:このファイルにはネットワークインターフェースの構成ログが含まれます。パブリックIPアドレスとローカルIPアドレスの2つのIPアドレスが確認できるはずです。このログにこれらのIPアドレスが記載されていない場合は、何らかの問題があります。サポートチームにお問い合わせください。

  注意
  パブリックIPアドレスのマスクは32である必要があります。

- `swanctl-list-loaded-config.txt`: このファイルにはすべてのIPsecサイトに関する情報が含まれます。
  ファイルにサイトの情報がない場合は、IPsec構成が適用されていません。構成のアップデートを試して保存するか、サポートチームに問い合わせてください。
- `swanctl-list-active-sas.txt`: このファイルには、ステータスがアクティブか接続中の接続とポリシーが含まれます。

復元サーバー設定

このセクションでは、フェールオーバーとフェールバックの概念、復元サーバーの作成、およびディザスタリカバリ操作について説明します。

復元サーバーの作成

ワークロードのコピーとなる復元サーバーを作成するには、以下の手順を実行します。また、その手順を扱ったビデオチュートリアルを参照することもできます。

重要
フェールオーバーを実行する際は、復元サーバーの作成後に作成された復元ポイントのみを選択できます。

前提条件

- 保護する元のマシンに保護計画を適用する必要があります。この計画では、マシン全体、または起動と必須のサービスの提供に必要なディスクのみをクラウドストレージにバックアップする必要があります。
- クラウドサイトへの接続タイプの1つを設定する必要があります。

リカバリサーバーの作成

1. **[すべてのデバイス]** タブで、保護するマシンを選択します。
2. **[ディザスタリカバリ]** をクリックし、**[リカバリサーバーを作成]** をクリックします。
3. 仮想コアの数と RAM のサイズを選択します。

   注意
   すべてのオプションの計算ポイントを確認できます。コンピュートポイントの数は、リカバリサーバーを 1 時間当たり実行するコストを反映しています。詳細については、"コンピュートポイント"（12ページ）を参照してください。

4. サーバーが接続されるクラウドネットワークを指定します。
5. **[DHCP]** オプションを選択します。

DHCPオプション	説明
クラウドサイトにより提供	デフォルトの設定。サーバーのIPアドレスは、クラウド上に自動設定されたDHCPサーバーにより提供されます。
カスタム	サーバーのIPアドレスは、クラウド上で現在動作しているDHCPサーバーにより提供されます。

6. （オプション） **MACアドレス**を指定します。
   MACアドレスは、サーバーのネットワークアダプタに割り当てられる一意の識別子です。カスタムのDHCPを使用する場合、特定のMACアドレスに対して、常に特定のIPアドレスが割り当てられるよ

うに設定できます。これにより、復元サーバーが常に同じIPアドレスを取得できるようになります。MACアドレスで登録されたライセンスを有するアプリケーションを実行することができます。

7. 本番ネットワークでサーバーが持つ IP アドレスを指定します。デフォルトでは、元のマシンの IP アドレスが設定されています。

   注意
   DHCPサーバーを使用する場合は、IPアドレスの競合を回避するために、このIPアドレスをサーバーの除外一覧に追加します。
   カスタムのDHCPサーバーを使用する場合、**稼働中のネットワークのIPアドレス**には、DHCPサーバーの設定と同一のIPアドレスを指定する必要があります。そうしない場合、テストフェールオーバーが正しく動作せず、パブリックIPアドレス経由でサーバーに到達できなくなります。

8. （オプション）[**テストIPアドレス**] チェックボックスをオンにして、IP アドレスを指定します。
   これにより、隔離されたテストネットワーク内でフェールオーバーをテストする機能、およびテストフェールオーバー中にRDPまたはSSH経由で復元サーバーに接続する機能が提供されます。テストフェールオーバーモードでは、VPNゲートウェイが、NATプロトコルを使用してテストIPアドレスを本番IPアドレスに置き換えます。
   チェックボックスをオフのままにすると、コンソールがテストフェールオーバー中にサーバーにアクセスする唯一の方法になります。

   注意
   DHCPサーバーを使用する場合は、IPアドレスの競合を回避するために、このIPアドレスをサーバーの除外一覧に追加します。

   提案された IP アドレスのいずれかを選択するか、別の IP アドレスを入力することができます。

9. （オプション）[**インターネットアクセスの許可**] チェックボックスをオンにします。
   これにより、リカバリサーバーは、実際のフェールオーバーまたはテストフェールオーバー中にインターネットにアクセスできます。デフォルトでは、TCPポート25番はパブリックIPアドレスへの送信接続用に開いています。

10. （オプション）**RPOしきい値**を設定します。
    RPOしきい値は、フェールオーバーのための最後の適切な復元ポイントと現在時刻との間の許容される最大時間間隔を定義します。数値は15～60分、1～24時間、1～14日間の範囲で設定できます。

11. （オプション）[**パブリックIPアドレスを使用する**] チェックボックスをオンにします。
    パブリック IP アドレスを使用すると、フェールオーバーまたはテストフェールオーバー中にインターネットからリカバリサーバーを使用できるようになります。チェックボックスをオフのままにすると、サーバーは本番ネットワークでのみ使用可能になります。
    パブリックIPアドレスを使用するオプションでは、**インターネットアクセス**オプションを有効にする必要があります。
    パブリック IP アドレスは、設定が完了した後に表示されます。デフォルトでは、TCPポート443番はパブリックIPアドレスへの受信接続用に開いています。

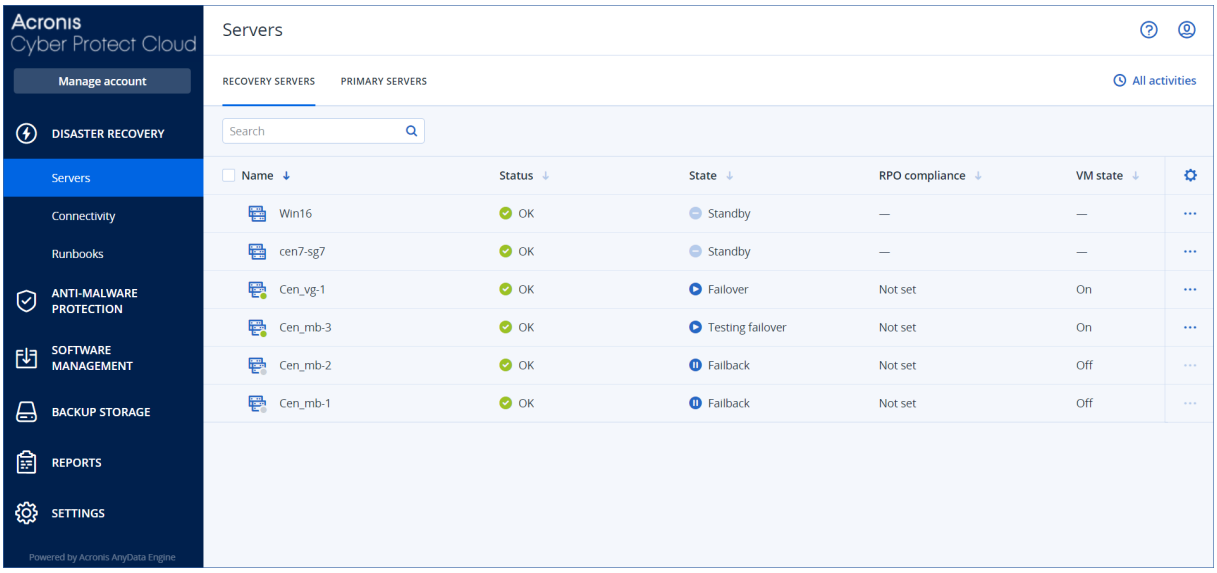
注意
[パブリックIPアドレスを使用する] チェックボックスをオフにするか、復元サーバーを削除すると、そのパブリックIPアドレスは予約されません。

12. （オプション）（選択したマシンのバックアップがマシンプロパティとしての暗号化を使用して暗号化されている場合）暗号化されたバックアップから復元サーバー用の仮想マシンを作成する際に自動的に使用されるパスワードを指定します。
    a. **[指定]** をクリックし、暗号化バックアップのパスワードを入力し、資格情報の名前を定義します。
       デフォルトでは、リスト内の最新のバックアップが表示されます。
    b. （オプション） すべてのバックアップを表示するには、**すべてのバックアップを表示**を選択します。
    c. **[完了]** をクリックします。

注意
指定したパスワードは安全な資格情報ストアに保存されますが、パスワードを保管する行為がコンプライアンス規定に抵触する場合があります。

13. （オプション）リカバリサーバー名を変更します。
14. （オプション）リカバリサーバーの説明を入力します。
15. （オプション）**[クラウドファイアウォールのルール]** タブをクリックして、デフォルトのファイアウォールルールを編集します。詳細については、"クラウドサーバーのファイアウォールルール設定"（83ページ）を参照してください。
16. **[作成]** をクリックします。

復元サーバーは、Cyber Protectコンソールの **[ディザスタリカバリ]** > **[サーバー]** > **[復元サーバー]** タブに表示されます。元のマシンを選択して **[ディザスタリカバリ]** をクリックしてその設定を表示することができます。



フェールオーバーが動作する仕組み

本番フェールオーバー

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

復元サーバーが作成されると、**スタンバイ**状態が維持されます。フェールオーバーが開始するまで、対応する仮想マシンは存在しない状態になります。フェールオーバープロセスを開始する前に、元のマシンの少なくとも1つのディスクイメージバックアップ（ブータブルボリュームを含む）を作成する必要があります。

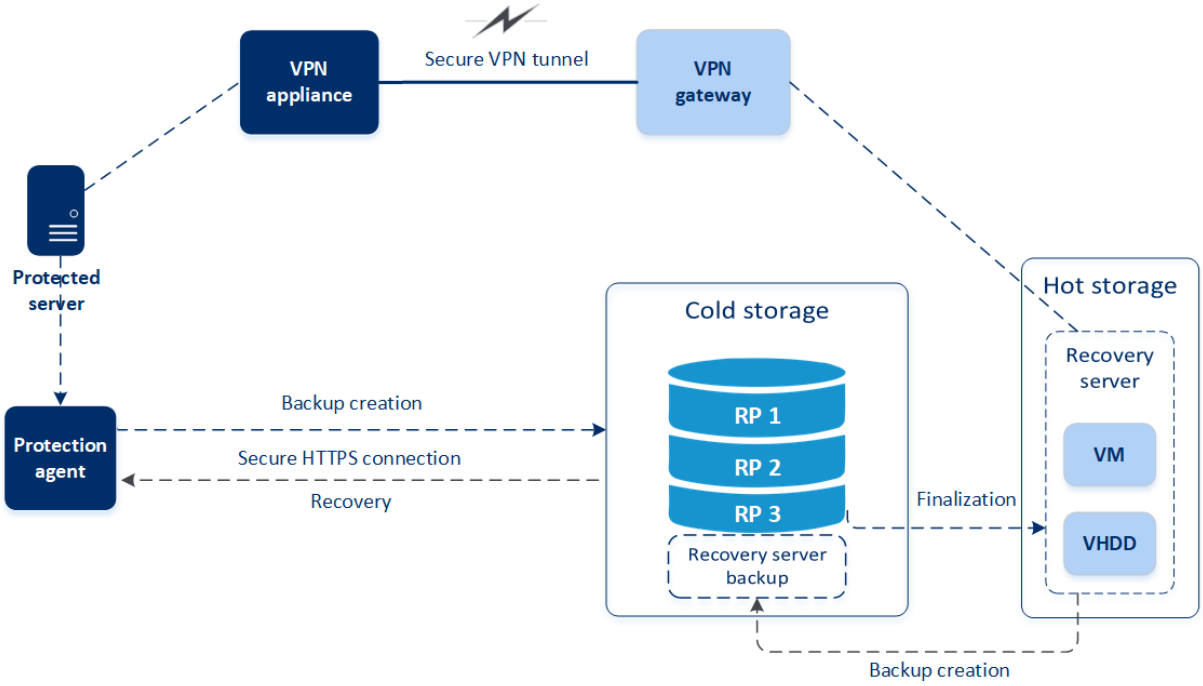
フェールオーバープロセスを開始した際、定義済みパラメータを有する仮想マシンの作成元である元のマシンの復元ポイント（バックアップ）を選択します。フェールオーバー操作では、「バックアップからVMを実行する」機能を使用します。復元サーバーはトランジション状態の**確定**を取得します。このプロセスは、サーバーの仮想ディスクをバックアップストレージ（「コールド」ストレージ）からディザスタリカバリストレージ（「ホット」ストレージ）に転送することを意味します。

注意
確定処理中は、パフォーマンスが通常より低くなりますが、サーバーはアクセスおよび操作可能です。サーバーコンソールを開くには、**コンソールの準備ができました**のリンクをクリックします。このリンクは、[**ディザスタリカバリ**] > [**サーバー**] 画面の [**VMステータス**] 列、およびサーバーの**詳細**ビューから利用可能です。

確定が完了すると、サーバーのパフォーマンスは通常の値に到達し、サーバーのステータスが、**フェールオーバー**に変わります。これで、ワークロードが元のマシンからクラウドサイトの復元サーバーに切り替わりました。

リカバリサーバーの内部に保護エージェントがある場合は、干渉（バックアップを開始したり古い状態をバックアップコンポーネントに報告したりする処理）を回避するために、エージェントサービスが停止します。

下の図では、フェールオーバーおよびフェールバック処理の両方について見ることができます。



テストフェールオーバー

テストフェールオーバー中、仮想マシンは最終化されません。これは、エージェントがバックアップから直接仮想ディスクのコンテンツを読み取る、つまり、バックアップのさまざまな部分へのランダムアクセスを実行するという意味です。これにより、パフォーマンスが通常の場合より低下する可能性があります。テストフェールオーバープロセスの詳細については、"テストフェールオーバーの実行"（59ページ）を参照してください。

自動テストフェールオーバー

自動テストフェールオーバーを構成すると、手動によるインタラクションなしにフェールオーバーが毎月実行されるようになります。詳細については、「"自動テストフェールオーバー"（61ページ）」と「"自動テストフェールオーバーの構成"（62ページ）」を参照してください。

テストフェールオーバーの実行

フェールオーバーのテストを実行することは、稼働中のネットワークから隔離されたテスト用VLAN内の復元サーバーを起動することを意味します。複数の復元サーバーを一度にテストして、インタラクションを確認できます。テストネットワークでは、サーバーは本番IPアドレスを使用して通信しますが、ローカルネットワーク内のワークロードへのTCPまたはUDP接続は開始できません。

テストフェールオーバー中、仮想マシン（復元サーバー）は最終化されません。エージェントでは、仮想ディスクの内容がバックアップから直接読み込まれ、バックアップの個別のパートにランダムアクセスされます。このため、ステータスがテストフェールオーバーになっている復元サーバーのパフォーマンスは、通常時のパフォーマンスと比べて低速になる場合があります。

フェールオーバーのテストの実行はオプションですが、コストと安全性の面で適切な頻度で定期的に実行することをお勧めします。クラウドの本番環境をスピンアップする方法を説明する一連の手順であるランブックを作成することをお勧めします。

重要
デバイスを災害から保護するために、事前に復元サーバーを作成する必要があります。

デバイスの復元サーバーが作成された後に作成された復元ポイントからのみ、フェールオーバーを実行できます。

復元サーバーへのフェールオーバーを実行する前に、少なくとも1つの復元ポイントを作成する必要があります。サポートされる復元ポイントの最大数は100件です。

テストフェールオーバーの実行

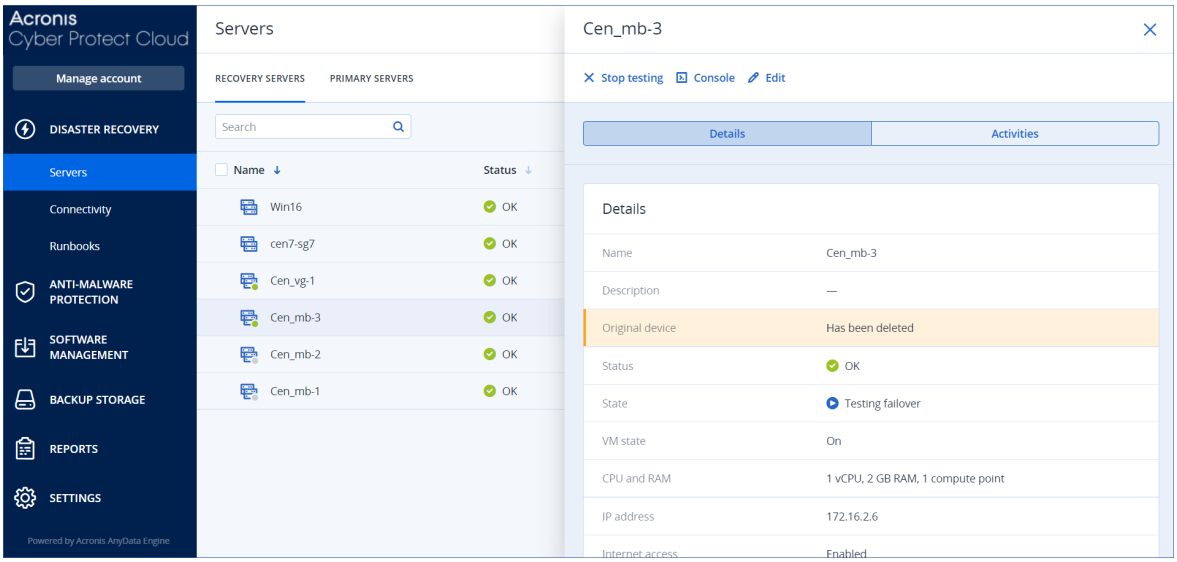
1. 元のマシンを選択するか、テストするリカバリサーバーを選択します。
2. [**ディザスタリカバリ**] をクリックします。
   リカバリサーバーの説明が開きます。
3. [**フェールオーバー**] をクリックします。
4. フェールオーバーの種類、[**テストフェールオーバー**] を選択します。
5. 復元ポイント（バックアップ）を選択して、[**開始**] をクリックします。
6. 選択したバックアップがマシンのプロパティとしての暗号化により暗号化されている場合:
   a. バックアップセットの暗号化パスワードを入力します。

      注意
      パスワードは一時的に保存され、現在のテストフェールオーバー処理にのみ使用されます。パスワードは、テストフェールオーバーが停止または完了すると、資格情報ストアから自動的に削除されます。

   b. （オプション） バックアップセットのパスワードを保存し、以降のフェールオーバー処理で使用するには、[**セキュアな資格情報ストアにパスワードを保存...**] チェックボックスを選択し、**資格情報名**フィールドに資格情報の名前を入力します。

      重要
      パスワードはセキュアな資格情報ストアに保存され、以降のフェールオーバー処理で自動的に適用されます。ただしパスワードを保管する行為が、コンプライアンス規定に抵触する場合があります。ご注意ください。

   c. [**完了**] をクリックします。
   リカバリサーバーが起動すると、状態は [**フェールオーバーテスト中**] に変わります。



7. 次のいずれかの方法を使用して、リカバリサーバーをテストします。
   - **[ディザスタリカバリ]** > **[サーバー]** でリカバリサーバーを選択して、**[コンソール]** をクリックします。
   - RD Pまたは SSH、およびリカバリサーバーの作成時に指定したテスト IP アドレスを使用して、リカバリサーバーに接続します。本番ネットワークの内部と外部の両方から接続を試してください（「ポイントツーサイト接続」に記載されています）。
   - リカバリサーバー内でスクリプトを実行します。

     スクリプトは、ログイン画面、アプリケーションの起動の有無、インターネット接続、および復元サーバーに接続する他のマシンの機能を確認できます。
   - 復元サーバーがインターネットとパブリックIPアドレスにアクセスできる場合は、TeamViewerを使用することができます。
8. テストが完了したら、**[テストの停止]** をクリックします。

   リカバリサーバーが停止します。テストフェールオーバー中に復元サーバーに加えられたすべての変更点は保存されません。

注意

ランブックの場合でも、手動でテストフェールオーバーを開始する場合でも、**サーバーを起動**および**サーバーを停止**アクションが、テストフェールオーバーの操作に適用されることはありません。これらのアクションを実行しようとすると、次のエラーメッセージが表示されて失敗します。

失敗:この操作は、現在のサーバーの状態には適用できません。

自動テストフェールオーバー

自動テストフェールオーバーでは、月に一度、自動的に復元サーバーのテストが行われます。手動のインタラクションは必要ありません。

自動テストフェールオーバーの処理は、以下のパートで構成されています。

1. 最新の復元ポイントから仮想マシンを作成する
2. 仮想マシンのスクリーンショットを取得する

3. 仮想マシンのオペレーティングシステムが正常に起動されたかどうかを分析する
4. テストフェールオーバーステータスに関して通知する

注意
自動テストフェールオーバーにより、コンピュートポイントが消費されます。

復元サーバーの設定で、自動テストフェールオーバーを設定できます。詳細については、"自動テストフェールオーバーの構成"（62ページ）を参照してください。

ごくまれに、自動テストのフェールオーバーがスキップされたり、スケジュールされた時刻に実行できなかったりする場合があります。ご注意ください。これは、本番環境でのフェールオーバーの優先度が自動テストでのフェールオーバーよりも高いため、自動テストでのフェールオーバーに割り当てられたハードウェアリソース（CPUとRAM）が一時的に制限されて、本番環境でのフェールオーバーを同時に行うためのリソースの確保が優先される可能性があるためです。

何らかの理由で自動テストのフェールオーバーがスキップされた場合、アラートが生成されます。

注意
オリジナルのマシンのバックアップがマシンプロパティとしての暗号化を使用して暗号化され、復元サーバーを作成する際に暗号化パスワードが指定されていない場合、自動テストフェールオーバーは失敗します。暗号化パスワードの指定の詳細については、"復元サーバーの作成"（55ページ）を参照してください。

自動テストフェールオーバーの構成

自動テストフェールオーバーを構成することで、手動で操作を行うことなく、毎月復元サーバーのテストを実行できます。

自動テストフェールオーバーを構成するには

1. コンソールで **[ディザスタリカバリ]** > **[サーバー]** > **[復元サーバー]** に移動し、復元サーバーを選択します。
2. **[編集]** をクリックします。
3. **[自動テストフェールオーバー]** セクションの **[スケジュール]** フィールドで、**[月単位]** を選択します。
4. （オプション）**[スクリーンショットのタイムアウト]** で、自動テストフェールオーバーの実行をシステムが試行する最大時間（分単位）のデフォルト値を変更します。
5. （オプション）**[スクリーンショットのタイムアウト]**の値をデフォルト値として保存し、他の復元サーバーの自動テストフェールオーバーを有効にするときの自動入力の値として使用するには、**[デフォルトタイムアウトとして設定]** を選択します。
6. **[保存]** をクリックします。

自動テストフェールオーバーのステータスを表示

自動テストフェールオーバーが完了すると、ステータス、開始時間、終了時間、期間、仮想マシンのスクリーンショットなどの詳細を表示できます。

復元サーバーの自動テストフェールオーバーステータスを表示するには

1. コンソールで **[ディザスタリカバリ]** > **[サーバー]** > **[復元サーバー]** に移動し、復元サーバーを選択します。
2. **[自動テストフェールオーバー]** セクションで、前回の自動テストフェールオーバーの詳細を確認します。
3. （オプション） **[スクリーンショットを表示]** をクリックすると、仮想マシンのスクリーンショットが表示されます。

自動テストフェールオーバーの無効化

リソースを節約したい場合や、特定の復元サーバーに対して自動テストフェールオーバーを実行する必要がない場合は、自動テストフェールオーバーを無効にすることができます。

自動テストフェールオーバーを無効化するには

1. コンソールで **[ディザスタリカバリ]** > **[サーバー]** > **[復元サーバー]** に移動し、復元サーバーを選択します。
2. **[編集]** をクリックします。
3. **[自動テストフェールオーバー]** セクションで、**[スケジュール]** フィールドで、**[なし]** を選択します。
4. **[保存]** をクリックします。

フェールオーバーの実行

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

フェールオーバーとは、構内からクラウドへワークロードを移動するプロセスおよびワークロードがクラウドに残っているときの状態です。

フェールオーバーを開始すると、復元サーバーが稼働中のネットワークで起動します。干渉や不要な問題が発生するのを回避するため、元のワークロードがオンラインでないこと、またVPN経由でアクセスできないことを確認してください。

同じクラウドアーカイブへのバックアップの干渉を避けるには、現在**フェールオーバー**ステータスになっているワークロードから保護計画を手動で取り消します。計画の取り消しの詳細については、「保護計画の取り消し」を参照してください。

重要
デバイスを災害から保護するために、事前に復元サーバーを作成する必要があります。

デバイスの復元サーバーが作成された後に作成された復元ポイントからのみ、フェールオーバーを実行できます。

復元サーバーへのフェールオーバーを実行する前に、少なくとも1つの復元ポイントを作成する必要があります。サポートされる復元ポイントの最大数は100件です。

以下の操作を実行するか、ビデオチュートリアルを視聴できます。

フェールオーバーの実行

1. 元のマシンがネットワーク上で使用できないことを確認します。
2. Cyber Protectコンソールで **[ディザスタリカバリ]** > **[サーバー]** > **[復元サーバー]** に移動し、復元サーバーを選択します。
3. **[フェールオーバー]** をクリックします。
4. フェールオーバーの種類、**本番フェールオーバー**を選択します。
5. 復元ポイント（バックアップ）を選択して、**[開始]** をクリックします。
6. （選択したバックアップがマシンのプロパティとしての暗号化により暗号化されている場合）
   a. バックアップセットの暗号化パスワードを入力します。

      注意
      パスワードは一時的に保存され、現在のフェールオーバー処理にのみ使用されます。フェールオーバー処理が完了し、サーバーが**スタンバイ**状態に戻ると、パスワードは資格情報ストアから自動的に削除されます。

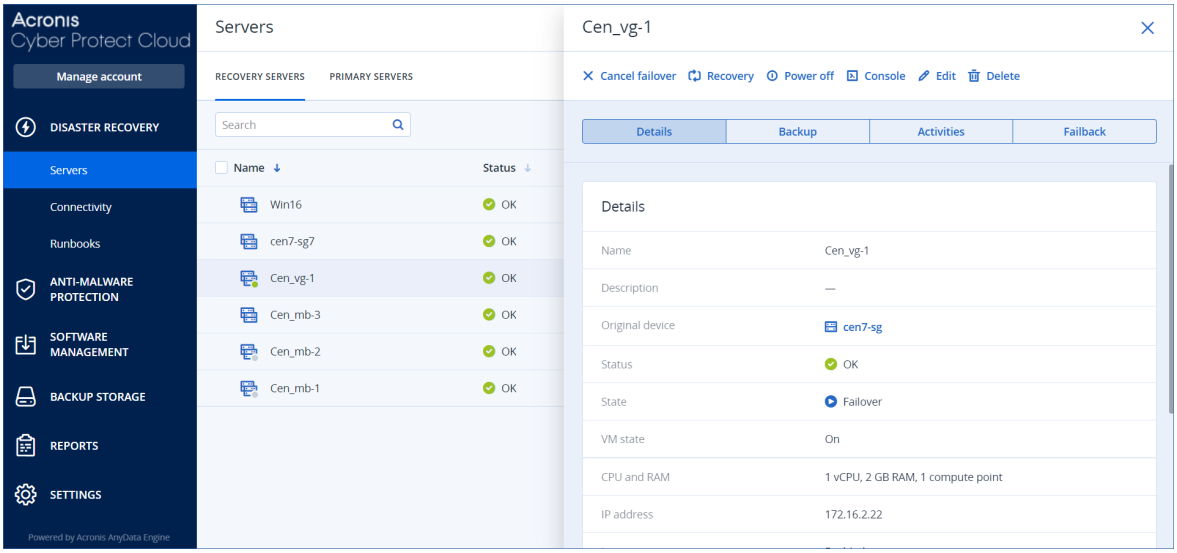
   b. （オプション） バックアップセットのパスワードを保存し、以降のフェールオーバー処理で使用するには、**[セキュアな資格情報ストアにパスワードを保存...]** チェックボックスを選択し、**資格情報名**フィールドに資格情報の名前を入力します。

      重要
      パスワードはセキュアな資格情報ストアに保存され、以降のフェールオーバー処理で自動的に適用されます。ただしパスワードを保管する行為が、コンプライアンス規定に抵触する場合があります。ご注意ください。

   c. **[完了]** をクリックします。

   リカバリサーバーが起動すると、状態は **[確定]** に変わり、しばらくしてから **[フェールオーバー]** になります。

重要
サーバーは、**確定**および**フェールオーバー**のいずれのステータスでも利用できることを理解しておく必要があります。**確定**ステータスの間に、サーバーコンソールを開くには、**コンソールの準備ができました**のリンクをクリックします。このリンクは、[**ディザスタリカバリ**] > [**サーバー**] 画面の [**VMステータス**] 列、およびサーバーの**詳細**ビューから利用可能です。詳細については、"フェールオーバーが動作する仕組み"（58ページ）を参照してください。



7. コンソールを表示して、リカバリサーバーが起動していることを確認します。[**ディザスタリカバリ**] > [**サーバー**] をクリックし、リカバリサーバーを選択して、[**コンソール**] をクリックします。
8. 復元サーバーの作成時に指定した本番IPアドレスを使用して、復元サーバーにアクセスできることを確認します。

リカバリサーバーが確定されると、新しい保護計画が自動的に作成され、適用されます。この保護計画は、リカバリサーバーの作成に使用された保護計画に基づいており、一定の制限があります。この計画では、スケジュールと保存ルールのみを変更できます。詳細については、「クラウドサーバーのバックアップ」を参照してください。

フェールオーバーをキャンセルする場合は復元サーバーを選択して [**フェールオーバーをキャンセル**] をクリックします。復元サーバーのバックアップを除き、フェールオーバー時点以降のすべての変更は失われます。リカバリサーバーは、**スタンバイ**状態に戻ります。

フェールバックを実行する場合、復元サーバーを選択して、[**フェールバック**] をクリックします。

ローカルDNSを使用してサーバーのフェールオーバーを実行する方法

ローカルサイトでDNSサーバーを使用してマシン名を解決する場合、フェールオーバー後、DNSに依存しているマシンに対応する復元サーバーは、クラウドで使用されているDNSサーバーが異なるため、通信に失敗します。デフォルトでは、クラウドサイトのDNSサーバーが、新しく作成されたクラウドサーバーに使用されます。カスタムDNS設定を適用する必要がある場合は、サポートチームに連絡してください。

DHCPサーバーのフェールオーバーを実行する方法

ローカルインフラストラクチャでは、WindowsまたはLinuxホストにDHCPサーバーが配置されている場合があります。そのようなホストがクラウドサイトにフェールオーバーされると、DHCPサーバーの複製の問題が生じます。これはクラウド内のVPNゲートウェイもDHCPの役割を果たしているためです。この問題を解決するには、次のいずれかを実行します。

- 残りのローカルサーバーがまだローカルサイトにある間にDHCPホストだけがクラウドにフェールオーバーされた場合、クラウド内のDHCPホストにログインして、その上にあるDHCPサーバーをオフにする必要があります。したがって、競合は発生せずに、VPNゲートウェイのみがDHCPサーバーとして機能します。
- クラウドサーバーがDHCPホストからすでにIPアドレスを取得している場合、クラウド内のDHCPホストにログインして、その上にあるDHCPサーバーをオフにする必要があります。さらに、正しいDHCPサーバー（VPNゲートウェイでホストされている）から割り当てられた新しいIPアドレスを割り当てるため、クラウドサーバーにログインし、DHCPリースを更新する必要があります。

注意
クラウドDHCPサーバーが **[カスタムDHCP]** オプションで構成されており、復元サーバーまたはプライマリサーバーのいずれかが、このDHCPサーバーからIPアドレスを取得している場合、この手順を使用することはできません。

フェールバックの動作について

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

フェールバックは、クラウドからローカルサイトの物理マシンまたは仮想マシンにワークロードを戻すプロセスです。**フェールオーバー**状態の復元サーバーでフェールバックを実行できます。またローカルサイトのサーバーを引き続き使用できます。

ローカルサイトの仮想または物理ターゲットマシンに対する自動フェールオーバーを実行できます。フェールバック中に、クラウド内の仮想マシンを引き続き実行しながら、バックアップデータをローカルサイトに転送できます。このテクノロジーにより、ダウンタイムを大幅に短縮できます。また予測される概算のダウンタイムがCyber Protectコンソールに表示されます。この情報を確認および使用してアクティビティを計画し、今後のダウンタイムに関して、必要に応じてクライアントに注意を喚起できます。

ターゲット仮想マシンとターゲット物理マシンに対するフェールバックプロセスは若干異なります。フェールバックプロセスのフェーズの詳細については、「"ターゲット仮想マシンへのフェールバック"（67ページ）」および「"ターゲット物理マシンへのフェールバック"（72ページ）」を参照してください。

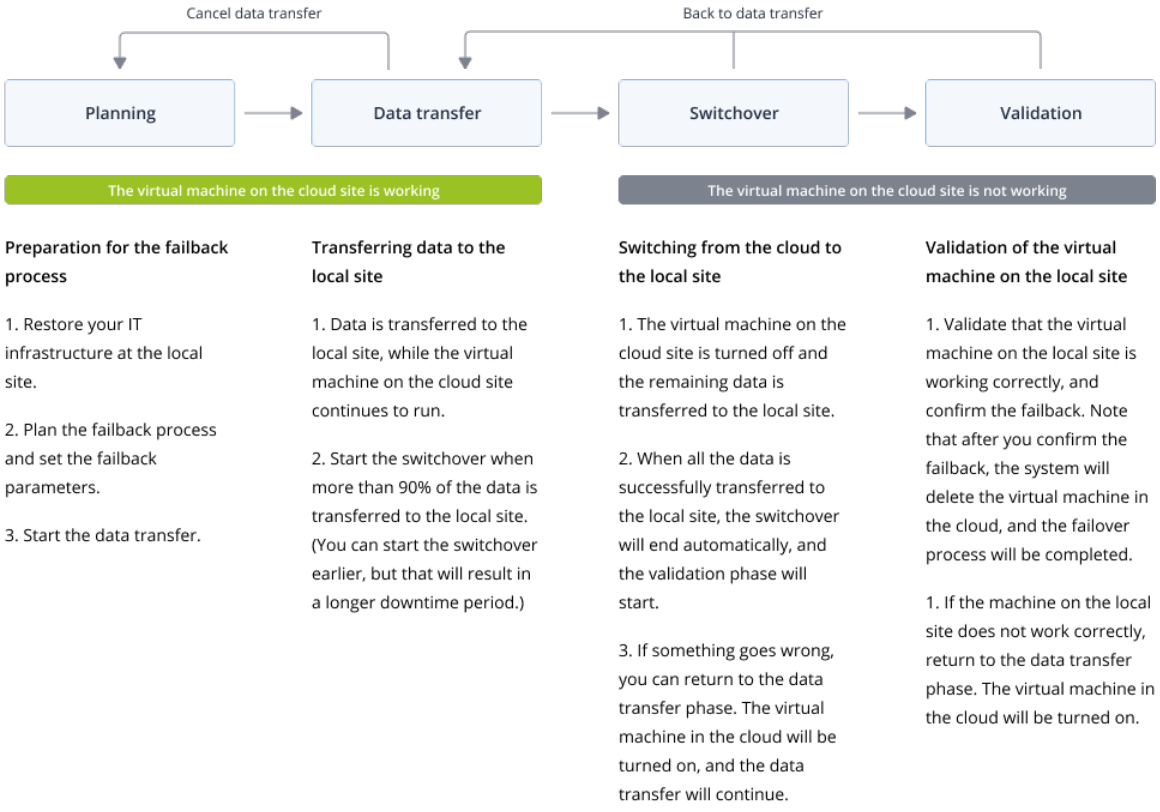
自動化されたフェールバック手順を使用できない特定のケースでは、手動でフェールバックを実行できます。詳細については、"手動フェールバック"（75ページ）を参照してください。

注意
ランブックの処理では、手動モードのフェールバックのみがサポートされます。これは、**フェールバックサーバー**手順を含むランブックを実行してフェールバックプロセスを開始した場合、その手順で手動によるインタラクションが必要となることを意味しています。つまり、マシンを手動でリカバリし、**[ディザスタリカバリ]** > **[サーバー]** タブからフェールバックプロセスを確認またはキャンセルする必要があります。

ターゲット仮想マシンへのフェールバック

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

ターゲット仮想マシンのフェールバックプロセスは次の4つのフェーズで構成されます。



1. **計画**:このフェーズでは、ホストやネットワーク構成などのローカルサイトのITインフラストラクチャを復元し、フェールバックパラメータを構成します。また、データ転送を開始するタイミングの計画を策定します。

注意
フェールバックプロセスの合計時間を最小限に抑えるために、ローカルサーバーをセットアップした直後にデータ転送フェーズを実行し、データ転送の間に、ネットワークと残りのローカルインフラストラクチャの構成を続行します。

2. **データ転送**:このフェーズでは、クラウド内の仮想マシンが引き続き実行されている間に、クラウドサイトからローカルサイトにデータが転送されます。データ転送の間は、任意のタイミングで次のフェーズであるスイッチオーバーを開始できます。ただし、次の関連要素を考慮する必要があります。

   データ転送フェーズの所要時間が長くなる
   - クラウドにおける仮想マシンの実行時間が長くなる。
   - 比較的多くのデータがローカルサイトに転送される
   - コストが高くなる（より多くのコンピュートポイントを消費する）
   - スイッチオーバーフェーズの間に発生するダウンタイムが短くなる。

   ダウンタイムを最小限に抑えたい場合は、データの90%以上がローカルサイトに転送された後にスイッチオーバーフェーズを開始します。

   より長いダウンタイムを許容する余裕があり、クラウドで仮想マシンを実行するために余分な計算ポイントを消費したくない場合は、より早いタイミングでスイッチオーバーフェーズを開始できます。

   データ転送フェーズ中にフェールバックプロセスをキャンセルした場合、転送されたデータはローカルサイトから削除されません。問題の発生をできるだけ回避するには、新しいフェールバックプロセスを開始する前に、転送されたデータを手動で削除します。以下のデータ転送プロセスは最初から開始されます。
3. **スイッチオーバー**:このフェーズでは、クラウド内の仮想マシンがオフになり、最新のバックアップ増分を含む残りのデータがローカルサイトに転送されます。復元サーバーにバックアップ計画が適用されていない場合、スイッチオーバーフェーズで自動的にバックアップが実行されるため、処理速度が遅くなります。

   このフェーズが終了するまでの推定時間（ダウンタイム期間）は、Cyber Protectコンソールで確認できます。すべてのデータがローカルサイトに転送された時点（データ損失がなく、ローカルサイトの仮想マシンがクラウド内の仮想マシンの正確なコピーになる）で、スイッチオーバーフェーズが完了します。ローカルサイトの仮想マシンがリカバリされ、検証フェーズが自動的に開始されます。
4. **検証**。このフェーズで、ローカルサイトの仮想マシンの準備が整い、自動的に起動しています。仮想マシンが正しく動作しているかどうかを確認できます。
   - すべてが意図したとおりに動作している場合は、フェールバックを確認します。フェールバック後、クラウドの仮想マシンが削除され、復元サーバーが**スタンバイ**状態に戻ります。これでフェールバックプロセスは終了です。
   - 何か問題がある場合は、スイッチオーバーをキャンセルしてデータ転送フェーズに戻ることができます。

仮想マシンへのフェールバックの実行

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

現在のローカルサイトのターゲット仮想マシンに対するフェールバックを実行できます。

前提条件

- フェールバックの実行に使用するエージェントはオンラインであり、現在、別のフェールバック操作には使用されていません。
- インターネット接続は安定しています。
- クラウド上に少なくとも1件の仮想マシンの完全バックアップが存在する。

仮想マシンのフェールバックを実行するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[サーバー]** の順に移動します。
2. **[フェールオーバー]** 状態のリカバリサーバーを選択します。
3. **[フェールバック]** タブをクリックします。
4. **[フェールバックパラメータ]** セクションで、**ターゲット**として **[仮想マシン]** を選択し、他のパラメータを構成します。

   デフォルトでは、一部の**フェールバックパラメータ**に対して推奨値が自動入力されますが、変更することができます。

   次の表に、**フェールバックパラメータ**の詳細を示します。

パラメータ	説明
バックアップ容量	フェールバック処理中にローカルサイトに転送されるデータの量です。 ターゲット仮想マシンへのフェールバック処理を開始すると、クラウド上の仮想マシンが継続して実行され、新しいデータが生成されるため、データ転送フェーズにおける**バックアップ容量**が大きくなります。 ターゲット仮想マシンへのフェールバック処理に伴うダウンタイムの目安を計算するには、**バックアップ容量**の10%に相当する値を算出（データの90%がローカルサイトに転送された後にスイッチオーバーフェーズを開始することを推奨しているため）して、その値をインターネットの転送速度で除算します。 **注意** 複数のフェールバック処理を同時に行うと、インターネット速度の値が低下します。
ターゲット	クラウドサーバーをリカバリするローカルサイトのワークロードのタイプ:**仮想マシン**または**物理マシン**。
ターゲット	フェールバックロケーション: VMware ESXiホストまたはMicrosoft Hyper-Vホスト。 サイバープロテクションサービスに登録されているエージェントが存在するすべての

パラメータ	説明
マシンロケーション	ホストから選択できます。
エージェント	フェールバック操作を実行するエージェント。 1つのエージェントを使用して、同時に1件のフェールバック操作を実行できます。 オンラインで、現在別のフェールバックプロセスに使用されておらず、フェールバック機能をサポートするバージョンがあり、バックアップにアクセスする権限が付与されているエージェントを選択できます。 VMware ESXiホストに複数のエージェントをインストールし、それぞれを使用して個別のフェールバックプロセスを開始できることに注意してください。これらのフェールバックプロセスは同時に実行できます。
ターゲットマシン設定	仮想マシンの設定: • **仮想プロセッサー**:仮想プロセッサーの数を選択します。 • **メモリ**:仮想マシンに搭載するメモリ容量を選択します。 • **単位**:メモリの単位を選択します。 • （オプション） **ネットワークアダプタ**:ネットワークアダプタを追加するには、**[追加]** をクリックして、**[ネットワーク]** フィールドでネットワークを選択します。 変更の準備ができたら、**[完了]** をクリックします。
パス	（Microsoft Hyper-Vホストの場合）マシンが保存されるホスト上のフォルダ。 ホストにマシン用の十分な空きメモリ容量があることを確認してください。
データストア	（VMware ESXiホストの場合）マシンが保存されるホスト上のデータストア。 ホストにマシン用の十分な空きメモリ容量があることを確認してください。
プロビジョニングモード	仮想ディスクの割り当て方法。 Microsoft Hyper-Vホストの場合: • **容量可変**（デフォルト値） • **固定サイズ** Microsoft Hyper-Vホストの場合: • **シン**（デフォルト値） • **シック**
ターゲットマシン名	ターゲットマシンの名前。デフォルトでは、ターゲットマシンの名前は復元サーバーの名前と同じです。 ターゲットマシン名は、選択した**ターゲットマシンロケーション**において一意である必要があります。

5. **[データ転送を開始]** をクリックして、確認ウィンドウでもう一度 **[開始]** をクリックします。

注意
クラウド上に仮想マシンのバックアップがない場合、システムはデータ転送フェーズの前に自動的にバックアップを実行します。

データ転送フェーズが開始します。コンソールには、次の情報が表示されます。

フィールド	説明
進行状況	このパラメータは、ローカルサイトにすでに転送されているデータの量と、転送する必要のあるデータの合計量を示します。 データの合計量には、データ転送フェーズが開始される前の最後のバックアップからのデータと、データ転送フェーズ中に仮想マシンが引き続き実行されることによって新しく生成される、データのバックアップ（バックアップの増分）が含まれます。このため、**進行状況**パラメータの2種類の値は時間とともに増加します。
ダウンタイムの推定	このパラメータは、スイッチオーバーフェーズを開始する場合、クラウドの仮想マシンが使用できなくなる期間を示します。この値は、**進行状況**パラメータの値に基づいて計算され、時間とともに減少します。

6. [**スイッチオーバー**] をクリックして、確認ウィンドウでもう一度 [**スイッチオーバー**] をクリックします。
   スイッチオーバーフェーズが開始します。コンソールには、次の情報が表示されます。

フィールド	説明
進行状況	このパラメータは、マシンのローカルサイトに対する復元の進行状況を示します。
完了までの推定所要時間	このパラメータは、スイッチオーバーフェーズが完了し、ローカルサイトでマシンを起動できるようになるまでの、おおよその時間を示します。

注意
クラウド上の仮想マシンにバックアップ計画が適用されていない場合、スイッチオーバーフェーズで自動的にバックアップが実行されるため、ダウンタイムが長くなります。

7. **スイッチオーバー**フェーズが完了し、ローカルサイトの仮想マシンが自動的に起動したら、正しく動作していることを検証します。
8. [**フェールバックの確認**] をクリックし、確認ウィンドウでもう一度 [**確認**] をクリックして、プロセスを最終化します。
   クラウドの仮想マシンが削除され、復元サーバーが**スタンバイ**状態に戻ります。

注意

フェールバック処理で、リカバリされたサーバーに保護計画が適用されることはありません。フェールバック処理が完了したら、リカバリされたサーバーに保護計画を適用して、保護が再開されるようにします。元のサーバーに適用されていたものと同じ保護計画、または**ディザスタリカバリ**モジュールが有効になっている新しい保護計画を適用できます。

ターゲット物理マシンへのフェールバック

注意

この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

ターゲット物理マシンへの自動フェールバックプロセスは、次のフェーズで構成されます。

1. **計画**:このフェーズでは、ホストやネットワーク構成などのローカルサイトのITインフラストラクチャを復元し、フェールバックパラメータを構成します。また、データ転送を開始するタイミングの計画を策定します。
2. **データ転送**:このフェーズでは、クラウド内の仮想マシンが引き続き実行されている間に、クラウドサイトからローカルサイトにデータが転送されます。データ転送の間は、任意のタイミングで次のフェーズであるスイッチオーバーを開始できます。ただし、次の関連要素を考慮する必要があります。

   データ転送フェーズの所要時間が長くなる

   - クラウドにおける仮想マシンの実行時間が長くなる。
   - 比較的多くのデータがローカルサイトに転送される
   - コストが高くなる（より多くのコンピュートポイントを消費する）
   - スイッチオーバーフェーズの間に発生するダウンタイムが短くなる。

   ダウンタイムを最小限に抑えたい場合は、データの90%以上がローカルサイトに転送された後にスイッチオーバーフェーズを開始します。

   より長いダウンタイムを許容する余裕があり、クラウドで仮想マシンを実行するために余分な計算ポイントを消費したくない場合は、より早いタイミングでスイッチオーバーフェーズを開始できます。

   注意

   データ転送プロセスでは、フラッシュバック技術が使用されます。このテクノロジーでは、ターゲットマシンで利用可能なデータとクラウド上の仮想マシンのデータが比較されます。データの一部がすでにターゲットマシンで利用可能な場合、そのデータは再度転送されません。このテクノロジーにより、データ転送フェーズが高速化されます。

   このため、サーバーをローカルサイトの元のマシンに復元することをお勧めします。

3. **スイッチオーバー**:このフェーズでは、クラウド内の仮想マシンがオフになり、最新のバックアップ増分を含む残りのデータがローカルサイトに転送されます。復元サーバーにバックアップ計画が適用されていない場合、スイッチオーバーフェーズで自動的にバックアップが実行されるため、処理速度が遅くなります。

4. **検証**:このフェーズで、ローカルサイトの物理マシンの準備が整い、Linuxベースのブータブルメディアを使って再起動できるようになります。仮想マシンが正しく動作しているかどうかを確認できます。
   - すべてが意図したとおりに動作している場合は、フェールバックを確認します。フェールバック後、クラウドの仮想マシンが削除され、復元サーバーが**スタンバイ**状態に戻ります。これでフェールバックプロセスは終了です。
   - 何か問題がある場合は、フェールオーバーをキャンセルして計画フェーズに戻ることができます。

   注意
   ブータブルメディアが再起動された後は、そのメディアを再度使用することはできません。検証フェーズで何らかの問題が見つかった場合は、新しいブータブルメディアを登録し、フェールバックプロセスを再度開始する必要があります。
   ただし、フラッシュバックテクノロジーが使用されるため、ローカルサイトにあるデータは再度転送されず、フェールバックプロセスはより高速になります。

物理マシンへのフェールバックの実行

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

現在のローカルサイトのターゲット物理マシンに対する自動フェールバックを実行できます。

注意
データ転送プロセスでは、フラッシュバック技術が使用されます。このテクノロジーでは、ターゲットマシンで利用可能なデータとクラウド上の仮想マシンのデータが比較されます。データの一部がすでにターゲットマシンで利用可能な場合、そのデータは再度転送されません。このテクノロジーにより、データ転送フェーズが高速化されます。

このため、サーバーをローカルサイトの元のマシンに復元することをお勧めします。

前提条件

- フェールバックの実行に使用するエージェントはオンラインであり、現在、別のフェールバック操作には使用されていません。
- インターネット接続は安定しています。
- 登録済みのブータブルメディアが利用可能である。詳細については、『Cyber Protectionユーザーガイド』の「ブータブルメディアを作成して、オペレーティングシステムをリカバリする」を参照してください。
- ターゲットの物理マシンがローカルサイトの元のマシンであるか、元のマシンと同じファームウェアを使用している。
- クラウド上に少なくとも1件の仮想マシンの完全バックアップが存在する。

物理マシンのフェールバックを実行するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[サーバー]** の順に移動します。
2. **[フェールオーバー]** 状態のリカバリサーバーを選択します。
3. **[フェールバック]** タブをクリックします。
4. **ターゲット**フィールドで、**[物理マシン]** を選択します。
5. **ターゲットブータブルメディア**フィールドで、**[指定]** をクリックし、ブータブルメディアを選択して **[完了]** をクリックします。

   注意
   ブータブルメディアはすでに構成されているため、事前構成済みのブータブルメディアを使用することをお勧めします。詳細については、『Cyber Protectionユーザーガイド』の「ブータブルメディアを作成して、オペレーティングシステムをリカバリする」を参照してください。

6. （オプション） デフォルトのディスクマッピングを変更するには、**ディスクマッピング**フィールドで **[指定]** をクリックし、バックアップのディスクをターゲットマシンのディスクにマッピングして、**[完了]** をクリックします。
7. **[データ転送を開始]** をクリックして、確認ウィンドウでもう一度 **[開始]** をクリックします。

   注意
   クラウド上に仮想マシンのバックアップがない場合、システムはデータ転送フェーズの前に自動的にバックアップを実行します。

   データ転送フェーズが開始します。コンソールには、次の情報が表示されます。

フィールド	説明
進行状況	このパラメータは、ローカルサイトにすでに転送されているデータの量と、転送する必要のあるデータの合計量を示します。 データの合計量には、データ転送フェーズが開始される前の最後のバックアップからのデータと、データ転送フェーズ中に仮想マシンが引き続き実行されることによって新しく生成される、データのバックアップ（バックアップの増分）が含まれます。このため、**進行状況**の値は時間とともに増加します。 システムによるデータ転送中はフラッシュバック技術が使用され、ターゲットマシン上ですでに利用可能なデータが転送されることはありません。それで、進行状況はコンソールで最初に計算された値よりも速く進む可能性があります。
ダウンタイムの推定	このパラメータは、スイッチオーバーフェーズを開始する場合、クラウドの仮想マシンが使用できなくなる期間を示します。この値は、**進行状況**パラメータの値に基づいて計算され、時間とともに減少します。 システムによるデータ転送中には、フラッシュバック技術が使用され、ターゲットマシン上ですでに利用可能なデータが転送されることはありません。それでダウンタイムはコンソールに最初に表示される値よりもはるかに短くなる可能性があります。

8. **[スイッチオーバー]** をクリックして、確認ウィンドウでもう一度 **[スイッチオーバー]** をクリックします。

スイッチオーバーフェーズが開始します。コンソールには、次の情報が表示されます。

フィールド	説明
進行状況	このパラメータは、マシンのローカルサイトに対する復元の進行状況を示します。
完了までの推定所要時間	このパラメータは、スイッチオーバーフェーズが完了し、ローカルサイトでマシンを起動できるようになるまでの、おおよその時間を示します。

注意
クラウド上の仮想マシンにバックアップ計画が適用されていない場合、スイッチオーバーフェーズで自動的にバックアップが実行されるため、ダウンタイムが長くなります。

9. **スイッチオーバー**フェーズが完了したら、ブータブルメディアを再起動し、ローカルサイトの物理マシンが想定した通りに動作していることを確認します。
   詳細については、『Cyber Protectionユーザーガイド』の「ブータブルメディアを使用したディスクのリカバリ」を参照してください。
10. **[フェールバックの確認]** をクリックし、確認ウィンドウでもう一度 **[確認]** をクリックして、プロセスを最終化します。
    クラウドの仮想マシンが削除され、復元サーバーが**スタンバイ**状態に戻ります。

注意
フェールバック処理で、リカバリされたサーバーに保護計画が適用されることはありません。
フェールバック処理が完了したら、リカバリされたサーバーに保護計画を適用して、保護が再開されるようにします。元のサーバーに適用されていたものと同じ保護計画、または**ディザスタリカバリ**モジュールが有効になっている新しい保護計画を適用できます。

手動フェールバック

注意
サポートチームからアドバイスを受けた場合に限り、手動モードの使用によるフェールバックプロセスの実行をお勧めします。

手動モードでフェールバックプロセスを開始することもできます。この場合、クラウド上のバックアップからローカルサイトへのデータ転送は自動的には行われません。クラウド上の仮想マシンの電源が遮断された後に手動で行う必要があります。このため、手動モードでのフェールバック処理は非常に遅くなり、ダウンタイムの期間が長くなることが想定されます。

手動モードでのフェールバックプロセスは、以下のフェーズで構成されます:

1. **計画**:このフェーズでは、ホストやネットワーク構成などのローカルサイトのITインフラストラクチャを復元し、フェールバックパラメータを構成します。また、データ転送を開始するタイミングの計画を策定します。

2. **スイッチオーバー**:このフェーズでは、クラウド内の仮想マシンがオフになり、新しく生成されたデータがバックアップされます。復元サーバーにバックアップ計画が適用されていない場合、スイッチオーバーフェーズで自動的にバックアップが実行されるため、処理速度が遅くなります。バックアップが完了したら、ローカルサイトにマシンを手動でリカバリします。ブータブルメディアを使用してディスクをリカバリするか、クラウドバックアップストレージからマシン全体をリカバリすることができます。
3. **検証**:このフェーズでは、ローカルサイトの物理マシンまたは仮想マシンが正しく動作していることを検証し、フェールバックを確認します。確認後、クラウドサイトの仮想マシンが削除され、復元サーバーが**スタンバイ**状態に戻ります。

手動フェールバックを実行する

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

現在のローカルサイトのターゲット物理マシンまたは仮想マシンに対する手動フェールバックを実行できます。

手動フェールバックを実行するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[サーバー]** の順に移動します。
2. **[フェールオーバー]** 状態のリカバリサーバーを選択します。
3. **[フェールバック]** タブをクリックします。
4. **ターゲット**フィールドで、**[物理マシン]** を選択します。
5. ギアアイコンをクリックし、**[マニュアルモードを使用する]** スイッチを有効にします。
6. （オプション）**バックアップサイズ**の値をインターネットの転送速度で除算することで、ターゲット物理マシンへのフェールバック処理に伴うダウンタイムの目安を計算できます。

   注意
   複数のフェールバック処理を同時に行うと、インターネット速度の値が低下します。

7. **[スイッチオーバー]** をクリックして、確認ウィンドウでもう一度 **[スイッチオーバー]** をクリックします。
   クラウドサイトの仮想マシンがオフになっています。

   注意
   クラウド上の仮想マシンにバックアップ計画が適用されていない場合、スイッチオーバーフェーズで自動的にバックアップが実行されるため、ダウンタイムが長くなります。

8. 現在のローカルサイトの物理マシンまたは仮想マシンに対して、クラウドバックアップからサーバーをリカバリします。詳細については、『Cyber Protectionユーザーガイド』の「マシンをリカバリする」を参照してください。

9. リカバリが完了し、リカバリしたマシンが正常に動作することを確認してから、**[マシンが復元されました]** をクリックします。
10. 意図したとおりに動作が完了している場合、**[フェールバックの確認]** をクリックして、確認ウィンドウでもう一度 **[確認]** をクリックします。
    復元サーバーと復元ポイントは、次のフェールオーバーのために準備完了となります。新しい復元ポイントを作成するには、新しいローカルサーバーに保護計画を適用します。

注意
フェールバック処理で、リカバリされたサーバーに保護計画が適用されることはありません。フェールバック処理が完了したら、リカバリされたサーバーに保護計画を適用して、保護が再開されるようにします。元のサーバーに適用されていたものと同じ保護計画、または**ディザスタリカバリ**モジュールが有効になっている新しい保護計画を適用できます。

暗号化されたバックアップでの作業

暗号化されたバックアップから復元サーバーを作成できます。便宜を図るため、復元サーバーへのフェールオーバー中に、暗号化されたバックアップに対して自動パスワードアプリケーションを設定できます。

復元サーバーを作成する際、自動ディザスタリカバリ操作に使用するパスワードを指定できます。これは、資格情報の安全な保管場所である資格情報ストアに保存されます。資格情報ストアは、**[設定]** > **[資格情報]** セクションにあります。

1つの資格情報を幾つかのバックアップにリンクさせることができます。

資格情報ストアで保存したパスワードを管理するには

1. **[設定]** > **[資格情報]** へ進みます。
2. 特定の資格情報を管理するには、最後の列のアイコンをクリックします。この資格情報にリンクされたアイテムを確認できます。
   - 選択した資格情報からバックアップをリンク解除するには、バックアップの近くにあるゴミ箱アイコンをクリックします。その結果、復元サーバーへのフェールオーバー中、パスワードを手動で指定する必要が生じます。
   - 資格情報を編集するには、**[編集]** をクリックし、名前またはパスワードを指定します。
   - 資格情報を削除するには、**[削除]** をクリックします。復元サーバーへのフェールオーバー中、パスワードを手動で指定する必要があることに留意してください。

Microsoft Azure仮想マシンを使った処理

注意
適用されるライセンスモデルによっては、一部の機能で追加のライセンスが必要になる場合があります。

Microsoft Azure仮想マシンのフェールオーバーを Acronis Cyber Protect Cloudで実行できます。詳細については、"フェールオーバーの実行"（63ページ）を参照してください。

その後、Acronis Cyber Protect CloudからAzure仮想マシンへのフェールバックを実行できます。このフェールバックプロセスは、物理マシンへのフェールバックプロセスと同様です。詳細については、"物理マシンへのフェールバックの実行"（73ページ）を参照してください。

注意
フェールバック用のAzure仮想マシンを新規に登録するには、Azureで利用可能なAcronis Backup VM拡張機能を使用できます。

Acronis Cyber Protect CloudとAzure VPNゲートウェイ間のマルチサイトIPsec VPN接続を構成できます。詳細については、"マルチサイトIPsec VPNの構成"（31ページ）を参照してください。

プライマリサーバー設定

このセクションでは、プライマリサーバーの作成および管理の方法について説明します。

プライマリサーバーの作成

前提条件

- クラウドサイトへの接続タイプの1つを設定する必要があります。

プライマリサーバーを作成します

1. **[ディザスタリカバリ]** > **[サーバー]** > **[プライマリサーバー]** タブの順に移動します。
2. **[作成]** をクリックします。
3. 新しい仮想マシンのテンプレートを選択します。
4. 構成のフレーバー（仮想コアの数とRAMのサイズ）を選択します。次の表は、各フレーバーのディスク容量合計の最大値（GB）を示しています。

種類	vCPU	RAM（GB）	ディスク容量合計の最大値（GB）
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

注意
すべてのオプションの計算ポイントを確認できます。コンピュートポイントの数は、プライマリサーバーを 1 時間当たり実行するコストを反映しています。詳細については、"コンピュートポイント"（12ページ）を参照してください。

5. （オプション）仮想ディスクサイズの変更複数のハードディスクが必要な場合は、**[ディスクを追加]** をクリックし、新しいディスクサイズを指定します。現在、プライマリサーバーにはディスクを9台まで追加できます。
6. プライマリサーバーが含まれるクラウドネットワークを指定します。
7. **[DHCP]** オプションを選択します。

DHCPオプション	説明
クラウドサイトにより提供	デフォルトの設定。サーバーのIPアドレスは、クラウド上に自動設定されたDHCPサーバーにより提供されます。
カスタム	サーバーのIPアドレスは、クラウド上で現在動作しているDHCPサーバーにより提供されます。

8. （オプション） **MACアドレス**を指定します。
   MACアドレスは、サーバーのネットワークアダプタに割り当てられる一意の識別子です。カスタムのDHCPを使用する場合、特定のMACアドレスに対して、常に特定のIPアドレスが割り当てられるように設定できます。これにより、プライマリサーバーが常に同じIPアドレスを取得できるようになります。MACアドレスで登録されたライセンスを有するアプリケーションを実行することができます。
9. 本番ネットワークでサーバーが持つ IP アドレスを指定します。デフォルトでは、本番ネットワークの最初の空き IP アドレスが設定されています。

   注意
   DHCPサーバーを使用する場合は、IPアドレスの競合を回避するために、このIPアドレスをサーバーの除外一覧に追加します。
   カスタムのDHCPサーバーを使用する場合、**稼働中のネットワークのIPアドレス**には、DHCPサーバーの設定と同一のIPアドレスを指定する必要があります。そうしない場合、テストフェールオーバーが正しく動作せず、パブリックIPアドレス経由でサーバーに到達できなくなります。

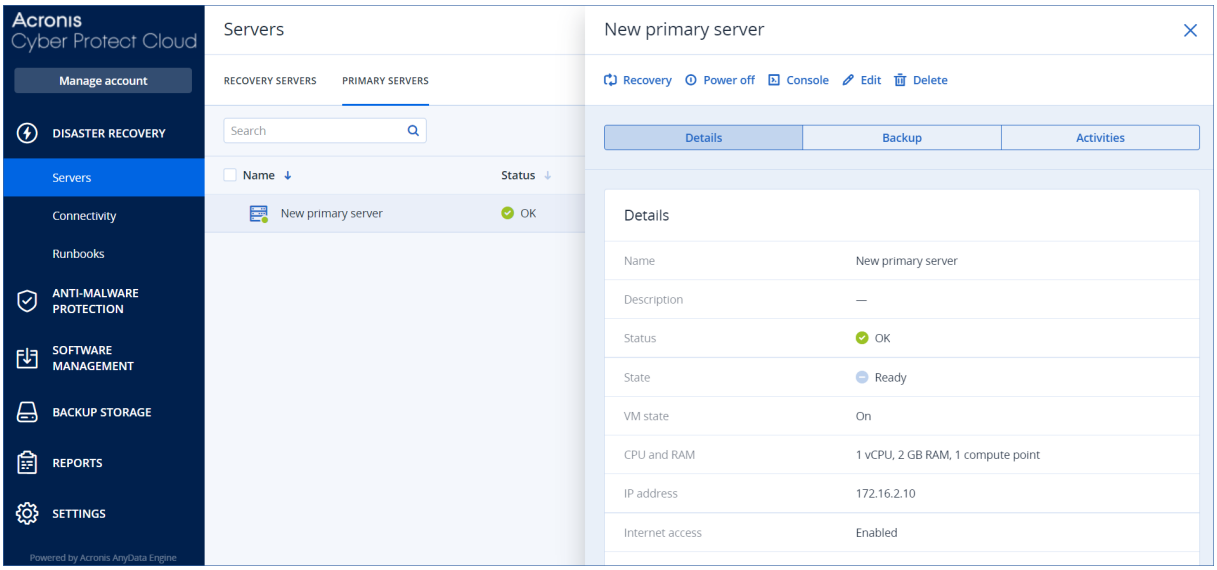
10. （オプション）**[インターネットアクセスの許可]** チェックボックスをオンにします。
    これにより、プライマリサーバーはインターネットにアクセスできます。デフォルトでは、TCPポート25番はパブリックIPアドレスへの送信接続用に開いています。
11. （オプション）**[パブリックIPアドレスを使用する]** チェックボックスをオンにします。
    パブリック IP アドレスを持つことで、プライマリサーバーがインターネットから利用可能になります。チェックボックスをオフのままにすると、サーバーは本番ネットワークでのみ使用可能になります。
    パブリック IP アドレスは、設定が完了した後に表示されます。デフォルトでは、TCPポート443番はパブリックIPアドレスへの受信接続用に開いています。

    注意
    [パブリックIPアドレスを使用する] チェックボックスをオフにするか、復元サーバーを削除すると、そのパブリックIPアドレスは予約されません。

12. （オプション）**RPO しきい値を設定**を選択します。
    RPO しきい値は、最後の復元ポイントと現在時刻との間の最大許容時間間隔を定義します。数値は15～60分、1～24時間、1～14日間の範囲で設定できます。
13. プライマリサーバー名を定義します。
14. （オプション）プライマリサーバーの説明を指定します。

15. （オプション）**[クラウドファイアウォールのルール]** タブをクリックして、デフォルトのファイアウォールルールを編集します。詳細については、"クラウドサーバーのファイアウォールルール設定"（83ページ）を参照してください。
16. **[作成]** をクリックします。

プライマリサーバーが本番ネットワークで使用できるようになります。コンソール、RDP、SSH、または TeamViewer を使用してサーバーを管理できます。



プライマリサーバーでの操作

プライマリサーバーは、コンソールの **[ディザスタリカバリ]** > **[サーバー]** > **[プライマリサーバー]** タブに表示されます。

サーバーを起動または停止するには、プライマリサーバーパネルの **[電源オン]** または **[電源オフ]** をクリックします。

プライマリサーバーの設定を編集するには、サーバーを停止し、**[編集]** をクリックします。

プライマリサーバーに保護計画を適用するには、該当の保護計画を選択し、**[計画]** タブで **[作成]** をクリックします。スケジュールと保持ルールのみを変更できる事前定義済みの保護計画が表示されます。詳細については、「クラウドサーバーのバックアップ」を参照してください。

クラウドサーバーの管理

クラウドサーバーを管理するには、[**Disaster Recovery**] > [**サーバー**] の順に移動します。2種類のタブがあります。[**リカバリサーバー**] と [**プライマリサーバー**] です。表内のすべてのオプション列を表示するには、ギアアイコンをクリックします。

タブをクリックすると、各クラウドサーバーについて以下の情報を見つけることができます。

列名	説明
名前	定義したクラウドサーバー名
ステータス	クラウドサーバーに関係する最も深刻な問題を反映しているステータス（アクティブアラートに基づく）
状態	クラウドサーバーの状態
VMの状態	クラウドサーバーに関連付けられた仮想マシンの電源の状態
アクティブなロケーション	サーバーがホストされるロケーションです。たとえば、**クラウド**のようになります。
RPOしきい値	フェールオーバーのための最後の適切な復元ポイントと現在時刻との間の許容される最大時間間隔。数値は15〜60分、1〜24時間、1〜14日間の範囲で設定できます。
RPOコンプライアンス	RPOコンプライアンスは、実際のRPOとRPOしきい値との比率です。RPOしきい値が定義されるとRPOコンプライアンスが表示されます。 それは以下のように計算されます。 **RPOコンプライアンス=実際のRPO/RPOしきい値** ここで、 **実際のRPO=現在時刻–直近の復元ポイント** **RPOコンプライアンス状態** 実際のRPOとRPOしきい値との比率の値に応じて、以下の状態が使用されます。 • **準拠**。RPOコンプライアンス<1x。サーバーがRPOしきい値を満たしています。 • **超過**。RPOコンプライアンス<=2x。サーバーがRPOしきい値に違反しています。 • **大幅に超過**。RPOコンプライアンス<=4x。サーバーがRPOしきい値に2倍以上違反しています。 • **危機的な超過**。RPOコンプライアンス>4x。サーバーがRPOしきい値に4倍以上違反しています。 • **保留中（バックアップなし）**。サーバーは保護計画により保護されていますが、バックアップは作成中で、まだ完了していません。
実際のRPO	最後の復元ポイント作成から経過した時間
前回の復元ポイント	前回復元ポイントが作成された日時

クラウドサーバーのファイアウォールルール

ファイアウォールルールを構成して、クラウドサイトのプライマリサーバーと復元サーバーの受信トラフィックと送信トラフィックを制御できます。

クラウドサーバーのパブリックIPアドレスをプロビジョニングした後、受信ルールを構成できます。デフォルトでは、TCPポート443番が許可され、他のすべての受信接続は拒否されます。デフォルトのファイアウォールルールを変更したり、受信例外を追加または削除したりできます。パブリックIPがプロビジョニングされていない場合、受信ルールは表示のみが可能であり、構成することはできません。

クラウドサーバーにインターネットアクセスをプロビジョニングした後、送信ルールを構成できます。デフォルトでは、TCPポート25番は拒否され、他のすべての送信接続は許可されます。デフォルトのファイアウォールルールを変更したり、送信例外を追加または削除したりできます。インターネットアクセスがプロビジョニングされていない場合、送信ルールは表示のみが可能であり、構成することはできません。

注意
セキュリティ上の理由から変更できない、事前定義のファイアウォールルールがあります。

受信および送信接続の場合:

- pingを許可する:ICMPエコー要求（タイプ8、コード0）およびICMPエコー応答（タイプ0、コード0）
- ICMP need-to-fragを許可（タイプ3、コード4）
- TTL超過を許可（タイプ11、コード0）

受信接続のみの場合:

- 構成できない部分:すべて拒否

送信接続のみの場合:

- 構成できない部分:すべて拒否

クラウドサーバーのファイアウォールルール設定

クラウド内のプライマリサーバーと復元サーバーにおけるデフォルトのファイアウォールルールを編集できます。

クラウドサイト上のサーバーのファイアウォールルールを編集するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[サーバー]** の順に移動します。
2. 復元サーバーのファイアウォールルールを編集する場合は、**[復元サーバー]** タブをクリックします。また、プライマリサーバーのファイアウォールルールを編集する場合は、**[プライマリサーバー]** タブをクリックします。
3. サーバーをクリックしてから、 **[編集]** をクリックします。
4. **[クラウドファイアウォールのルール]** タブをクリックします。
5. 受信接続のデフォルトアクションを変更する場合:

a. **[受信]** ドロップダウンフィールドで、デフォルトのアクションを選択します。

アクション	説明
すべて拒否	すべての受信トラフィックを拒否 例外を追加して、特定のIPアドレス、プロトコル、およびポートからのトラフィックを許可できます。
すべて許可	すべての受信TCPおよびUDPトラフィックを許可します。 例外を追加して、特定のIPアドレス、プロトコル、およびポートからのトラフィックを拒否できます。

注意
デフォルトのアクションを変更すると、既存の受信ルールの構成が無効になり、削除されます。

b. （オプション） 既存の例外を保存する場合は、確認ウィンドウで **[記述済みの例外を保存する]** を選択します。

c. **[確認]** をクリックします。

6. 例外を追加する場合:

a. **[例外の追加]** をクリックします。

b. ファイアウォールのパラメータを指定します。

ファイアウォールパラメータ	説明
プロトコル	接続のプロトコルを選択します。次のオプションがサポートされています。 • **TCP** • **UDP** • **TCP+UDP**
サーバーポート	ルールを適用するポートを選択します。次の項目を指定できます。 • 特定のポート番号（`2298`など） • ポート番号の範囲（`6000-6700`など） • 任意のポート番号。ルールを任意のポート番号に適用する場合、`*`を使用します。
クライアントIPアドレス	ルールを適用するIPアドレスを選択します。次の項目を指定できます。 • 特定のIPアドレス（`192.168.0.0`など） • CIDR表記を使用したIPアドレスの範囲（`192.168.0.0/24`など）。 • 任意のIPアドレス。ルールを任意のIPアドレスに適用する場合、`*`を使用します。

7. 既存の受信例外を削除する場合は、その横にあるごみ箱アイコンをクリックします。

8. 送信接続のデフォルトアクションを変更する場合:
   a. **[送信]** ドロップダウンフィールドで、デフォルトのアクションを選択します。

アクション	説明
すべて拒否	すべての送信トラフィックを拒否します。 例外を追加して、特定のIPアドレス、プロトコル、およびポートへのトラフィックを許可できます。
すべて許可	すべての送信トラフィックを許可します。 例外を追加して、特定のIPアドレス、プロトコル、およびポートからのトラフィックを拒否できます。

注意
デフォルトのアクションを変更すると、既存の送信ルールの構成が無効になり、削除されます。

   b. （オプション） 既存の例外を保存する場合は、確認ウィンドウで **[記述済みの例外を保存する]** を選択します。
   c. **[確認]** をクリックします。
9. 例外を追加する場合:
   a. **[例外の追加]** をクリックします。
   b. ファイアウォールのパラメータを指定します。

ファイアウォールパラメータ	説明
プロトコル	接続のプロトコルを選択します。次のオプションがサポートされています。 • **TCP** • **UDP** • **TCP+UDP**
サーバーポート	ルールを適用するポートを選択します。次の項目を指定できます。 • 特定のポート番号（`2298`など） • ポート番号の範囲（`6000-6700`など） • 任意のポート番号。ルールを任意のポート番号に適用する場合、*を使用します。
クライアントIPアドレス	ルールを適用するIPアドレスを選択します。次の項目を指定できます。 • 特定のIPアドレス（`192.168.0.0`など） • CIDR表記を使用したIPアドレスの範囲（`192.168.0.0/24`など）。 • 任意のIPアドレス。ルールを任意のIPアドレスに適用する場合、*を使用します。

10. 既存の送信例外を削除する場合は、その横にあるごみ箱アイコンをクリックします。
11. **[保存]** をクリックします。

クラウドファイアウォールのアクティビティを確認する

クラウドサーバーのファイアウォールルールの構成をアップデートすると、アップデートアクティビティのログがCyber Protectコンソールで利用できるようになります。ログを表示して、次の情報を確認できます。

- 構成をアップデートしたユーザーのユーザー名
- アップデートの日時
- 受信および送信接続のファイアウォール設定
- 受信および送信接続のデフォルトアクション
- 受信接続と送信接続の例外のプロトコル、ポート、およびIPアドレス

クラウドファイアウォールルールの構成変更に関する詳細を表示するには

1. Cyber Protectコンソールで、**[監視]** > **[アクティビティ]** をクリックします。
2. 対応するアクティビティをクリックしてから、**[すべてのプロパティ]** をクリックします。
   アクティビティの説明を、**クラウドサーバー構成の更新**にする必要があります。
3. **[コンテキスト]** フィールドで、興味のある情報を調べます。

クラウドサーバーのバックアップ

プライマリサーバーと復元サーバーは、クラウドサイトにてエージェントレスでバックアップされます。これらのバックアップには以下の制限があります。

- 唯一可能なバックアップロケーションはクラウドストレージです。プライマリサーバーのバックアップ先は、**プライマリサーバーのバックアップ**ストレージです。

  注意
  Microsoft Azureのバックアップロケーションはサポートされていません。

- 複数のサーバーにバックアップ計画を適用することはできません。すべてのバックアップ計画に同じ設定が適用されていても、各サーバーには独自のバックアップ計画が必要です。
- サーバーに適用できるバックアップ計画は 1 つのみです。
- アプリケーションアウェアバックアップはサポートされていません。
- 暗号化は使用できません。
- バックアップオプションを使用できません

プライマリサーバーを削除すると、そのバックアップも削除されます。

リカバリサーバーは、フェールオーバー状態でのみバックアップされます。そのバックアップは、元のサーバーのバックアップシーケンスを続行します。フェールバックが実行されると、元のサーバーはこのバックアップシーケンスを続行できます。したがって、リカバリサーバーのバックアップは、手動で、または保持ルールを適用した結果としてのみ削除できます。リカバリサーバーが削除されると、そのバックアップは常に保持されます。

注意
クラウドサーバーのバックアップ計画はUTC時間に従って実行されます。

オーケストレーション（ランブック）

注意
適用されるライセンスモデルによっては、一部の機能で追加のライセンスが必要になる場合があります。

ランブックは、クラウドで製品環境を立ち上げる方法を説明する指示のセットです。ランブックは、Cyber Protectコンソールから作成できます。**[ランブック]** 画面にアクセスするには、**[ディザスタリカバリ]** > **[ランブック]** を選択します。

ランブックを使用する理由

ランブックを使用して以下の操作を実行できます。

- 1台以上のサーバーのフェールオーバーを自動化する
- サーバーIPアドレスにpingを実行し、指定するポートとの接続を確認して、フェールオーバーの結果を自動的に確認する
- 分散アプリケーションを実行しているサーバーの操作の順序を設定する
- ワークフローに手動操作を含める
- ランブックをテストモードで実行して、ディザスタリカバリソリューションのインテグリティを検証します。

ランブックの作成

ランブックは、連続して実行される手順で構成されています。手順は、同時に開始される操作で構成されています。

以下の操作を実行するか、ビデオチュートリアルを視聴できます。

ランブックを作成するには

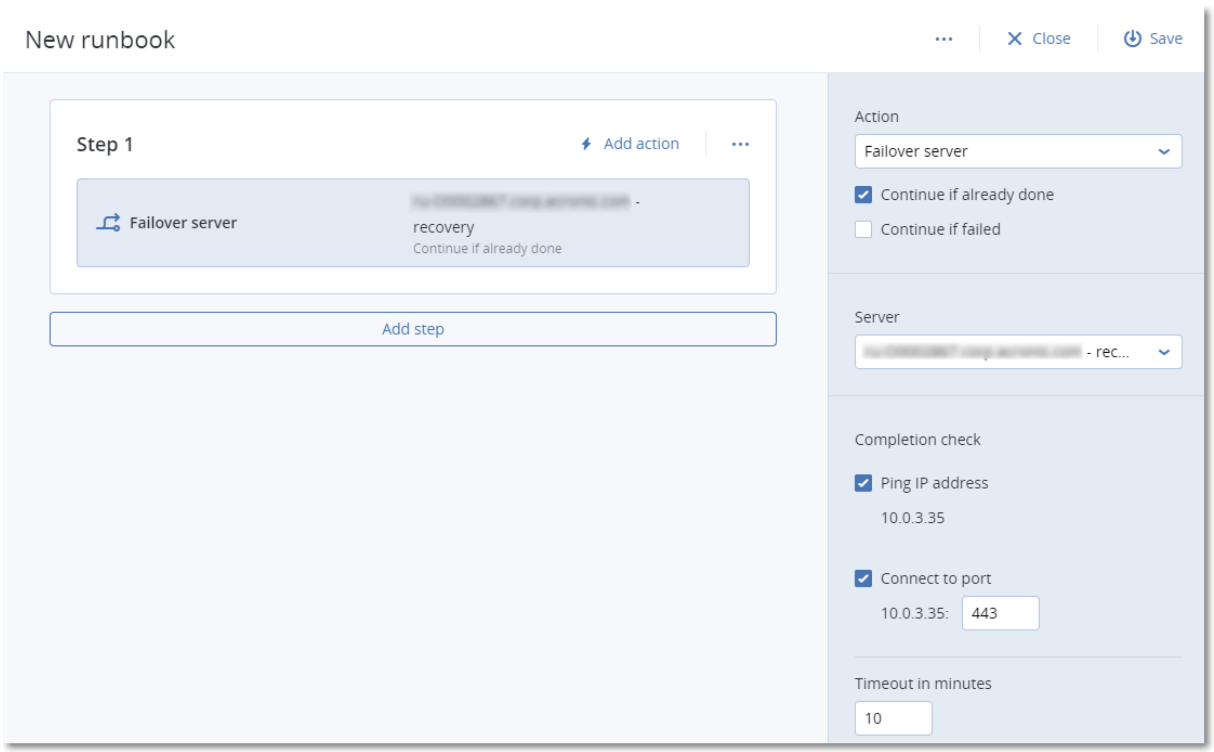
1. Cyber Protectionコンソールで、**[ディザスタリカバリ]** > **[ランブック]** に移動します。
2. **[ランブックを作成]** をクリックします。
3. **[手順を追加]** をクリックします。
4. **[操作を追加]** をクリックし、手順に追加したい操作を選択します。

アクション	説明
サーバーをフェールオーバー	クラウドサーバーのフェールオーバーを実行します。この操作を定義するには、クラウドサーバーを選択し、この操作で利用可能なランブックのパラメータを設定する必要があります。これらのパラメータについての詳細は、"ランブックパラメータ"（91ページ）を参照してください。

アクション	説明
	注意 選択したサーバーのバックアップがマシンプロパティとしての暗号化を使用して暗号化されている場合、**サーバーをフェールオーバー**の操作は一時停止され、自動的に**インタラクションが必要**に変更されます。ランブックの実行を続けるためには、暗号化されたバックアップのパスワードを指定する必要があります。
サーバーをフェールバック	クラウドサーバーのフェールバックを実行します。この操作を定義するには、クラウドサーバーを選択し、この操作に利用可能なランブックのパラメータを設定する必要があります。これらの設定の詳細については、"ランブックパラメータ"（91ページ）を参照してください。 **注意** ランブックの処理では、手動モードのフェールバックのみがサポートされます。これは、**サーバーをフェールバック**手順を含むランブックを実行してフェールバックプロセスを開始した場合、その手順で手動によるインタラクションが必要となることを意味しています。つまり、マシンを手動でリカバリし、**[ディザスタリカバリ]** > **[サーバー]** タブからフェールバックプロセスを確認またはキャンセルする必要があります。
サーバーを起動	クラウドサーバーを起動します。この操作を定義するには、クラウドサーバーを選択し、この操作で利用可能なランブックのパラメータを設定する必要があります。これらの設定の詳細については、"ランブックパラメータ"（91ページ）を参照してください。 **注意** **サーバーを起動**操作は、ランブック内のテストフェールオーバー操作には適用できません。この操作を実行しようとすると、次のエラーメッセージにより失敗します。 失敗: この操作は現在のサーバーステータスには適用できません。
サーバーを停止	クラウドサーバーを停止します。この操作を定義するには、クラウドサーバーを選択し、この操作で利用可能なランブックのパラメータを設定する必要があります。これらの設定の詳細については、"ランブックパラメータ"（91ページ）を参照してください。 **注意** **サーバーを停止**操作は、ランブック内のテストフェールオーバー操作には適用できません。この操作を実行しようとすると、次のエラーメッセージにより失敗します。 失敗: この操作は現在のサーバーステータスには適用できません。
手動処理	手動処理はユーザーからのインタラクションを必要とします。この操作を定義するには、説明を入力する必要があります。 ランブックのシーケンスが手動処理に到達すると、ランブックは一時停止し、ユーザーが確認ボタンをクリックするなどの必要な手動処理が実行されるまで、続行されません。

アクション	説明
ランブックを実行する	別のランブックを実行します。この操作を定義するには、ランブックを選択する必要があります。 ランブックは、任意のランブックの1つの実行のみを含めることができます。たとえば、アクション"ランブックAを実行"を追加した場合、アクション"ランブックBを実行"は追加できますが、別のアクション"ランブックAを実行"を含めることはできません。

5. 操作のランブックパラメータを定義します。これらのパラメータの詳細については、"ランブックパラメータ"（91ページ）を参照してください。
6. （オプション） 手順の説明を追加するには:
   a. アイコンの省略記号をクリックしてから、**[説明]** をクリックします。
   b. 手順の説明を入力します。
   c. **[完了]** をクリックします。
7. 必要な手順と操作のシーケンスが作成できるまで、手順3から6を繰り返します。
8. （オプション） ランブックのデフォルト名を変更するには:
   a. 省略記号アイコンをクリックします。
   b. ランブックの名前を入力します。
   c. ランブックの説明を入力します。
   d. **[完了]** をクリックします。
9. **[保存]** をクリックします。
10. **[閉じる]** をクリックします。



ランブックパラメータ

ランブックのパラメータは、ランブックの操作を定義するために構成しなければならない特定の設定です。ランブックのパラメータには、操作パラメータと完全性チェックパラメータの2種類のカテゴリがあります。

操作パラメータは、操作の初期化状態または結果によってランブックの動作を定義します。

完全性チェックパラメータは、サーバーが利用可能で必要なサービスが提供されていることを確認します。完全性チェックが失敗すると、その操作は失敗とみなされます。

各操作に対して構成可能なランブックのパラメータを次の表に示します。

ランブックパラメータ	カテゴリ	操作に対して利用可能	説明
実行済みの場合は続行	操作パラメータ	• **サーバーをフェールオーバー** • **サーバーを起動** • **サーバーを停止** • **サーバーをフェールバック**	このパラメータでは、必要な操作がすでに完了している場合（例えば、フェールオーバーがすでに実行されているか、サーバーがすでに稼働している場合など）のランブックの動作を定義します。有効にすると、ランブックで警告が発生したあとも、処理が続行されます。無効にした場合、操作が失敗したあとは、ランブックは実行されません。 デフォルトでは、このパラメータは有効化されています。
失敗の場合は続行	操作パラメータ	• **サーバーをフェールオーバー** • **サーバーを起動** • **サーバーを停止** • **サーバーをフェールバック**	このパラメータでは、必要な操作が失敗したときのランブックの動作を定義します。有効にすると、ランブックで警告が発生したあとも、処理が続行されます。無効にした場合、操作が失敗したあとは、ランブックは実行されません。 デフォルトでは、このパラメータは無効化されています。
IPアドレスにpingを実行	完了の確認	• **サーバーを起動**	ソフトウェアは、サーバーが応答するかタイムアウトするか、いずれか早い方まで、クラウドサーバーの本番IPアドレスにpingを実行します。
[ポートに接続]（デフォルトでは443）	完了の確認	• **サーバーをフェールオーバー** • **サーバーを起動**	ソフトウェアは、接続が確立するかタイムアウトするか、いずれか早い方まで、クラウドサーバーの本番IPアドレスと指定するポートを使用して、クラウドサーバーに接続しようとします。この方法で、指定したポートで待機するアプリケーションが動作しているかどうかを確認できます。
タイムアウト（分）	完了の確認	• **サーバーをフェールオー**	デフォルトのタイムアウトは10分間です。

ランブックパラメータ	カテゴリ	操作に対して利用可能	説明
		バー • サーバーを起動	

ランブックの操作

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

操作の一覧にアクセスするには、ランブックにマウスポインタを重ね、省略記号アイコンをクリックします。ランブックが実行中ではない場合は、以下の操作が利用できます。

- **実行**
- **編集**
- **クローンを作成**
- **削除**

ランブックの実行

[実行] をクリックするたびに、実行パラメータを求められます。これらのパラメータは、ランブックに含まれるすべてのフェールオーバーとフェールバックに適用されます。**[ランブックを実行]** 操作で指定されるランブックは、メインのランブックからこれらのパラメータを継承します。

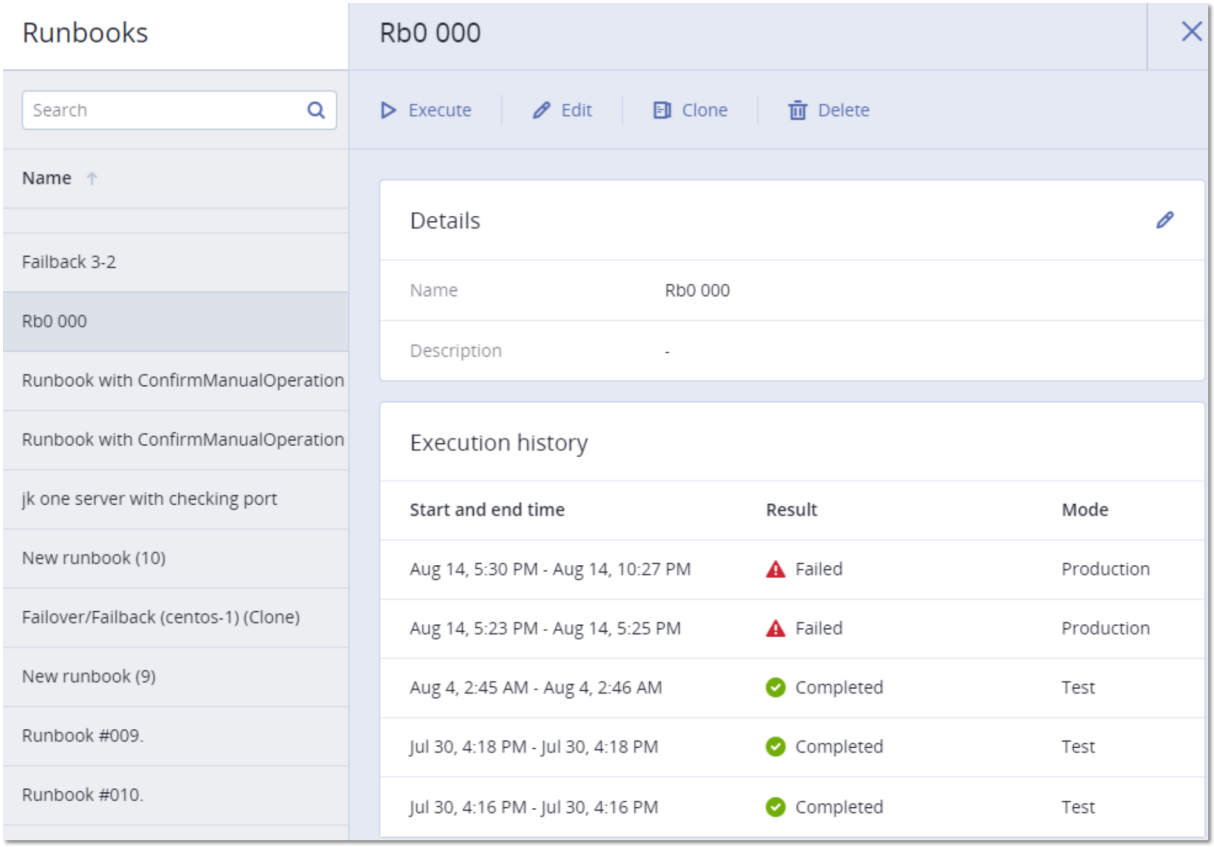
- **フェールオーバーおよびフェールバックモード**
  テストフェールオーバー（デフォルト）を実行するか本番フェールオーバーを実行するかを選択します。フェールバックモードは、選択されたフェールオーバーモードに対応します。
- **フェールオーバー復元ポイント**
  最新の復元ポイントを選択する（デフォルト）か、過去の時点を選択します。後者の場合、各サーバーについて、指定した日時の前で最も近い復元ポイントが選択されます。

ランブックの実行の停止

ランブックの実行中、操作の一覧で **[停止]** を選択できます。ユーザーの干渉を必要とするものを除き、ソフトウェアは、開始済みのすべてのアクションを完了します。

実行履歴の表示

[ランブック] タブでランブックを選択したとき、ソフトウェアによりランブックの詳細と実行履歴が表示されます。実行ログを表示するには、特定の実行に対応する行をクリックします。


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

サイトツーサイトOpen VPN - 追加情報

復元サーバーを作成する場合、サーバーで**稼働中のネットワークのIPアドレス**を構成し、**テストIPアドレス**を行います。

フェールオーバーを実行し（仮想マシンをクラウドで稼働させ）、仮想マシンにログインしてサーバーのIPアドレスを確認します。**稼働中のネットワークのIPアドレス**が表示されているはずです。

テストフェールオーバーを実行する場合、テストサーバーへのアクセスには、**テストIPアドレス**を使用する必要があります。このIPアドレスは、復元サーバーの構成でのみ表示されます。

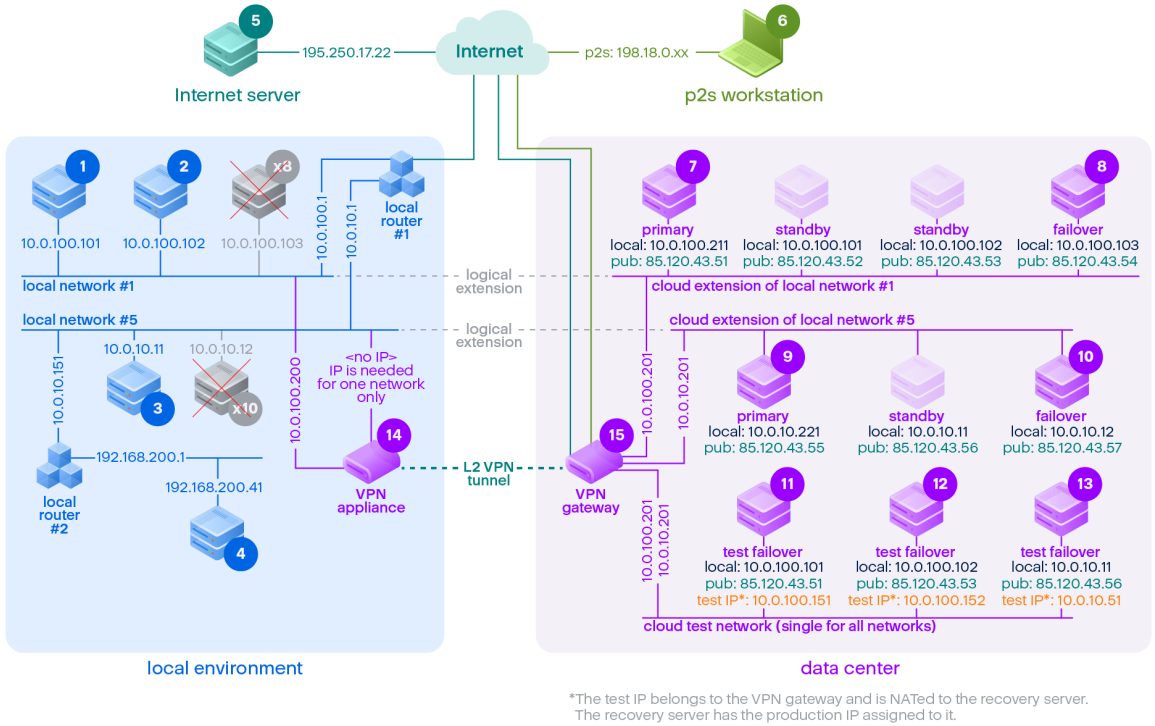
ローカルサイトからテストサーバーにアクセスするには、**テストIPアドレス**を使用する必要があります。

注意
サーバーのネットワーク構成には、常に**稼働中のネットワークのIPアドレス**が表示されます（テストサーバーは、稼働中のサーバーの状態をミラーリングするため）。これは、テスト用IPアドレスがテストサーバーではなく、VPNゲートウェイに属していて、NATにより稼働中のIPアドレスに変換されるためです。

次の図は、サイト間Open VPN構成の例を示しています。ローカル環境の一部のサーバーは、フェールオーバーを使用してクラウドにリカバリされます（ネットワークインフラストラクチャへの影響はありません）。

1. カスタマーが以下の方法によりディザスタリカバリを有効化しました:
   a. VPNアプライアンス（14）を構成し、それを専用のクラウドVPNサーバー（15）に接続する
   b. 一部のローカルサーバーをディザスタリカバリで保護する（1、2、3、x8、x10）
      ローカルサイトの一部のサーバー（4など）は、VPNアプライアンスへの接続がないネットワークに接続されています。このようなサーバーは、ディザスタリカバリで保護されていません。
2. 一部のサーバー（異なるネットワークに接続）は、ローカルサイトで動作しています:（1、2、3、4）
3. 保護済みのサーバー（1、2、3）は、テストフェールオーバーでテストされています（11、12、13）
4. ローカルサイトの一部のサーバーは、利用できません（x8、x10）。これらは、フェールオーバーの実行後、クラウドで利用可能になります（8および10）。
5. クラウド環境では、異なるネットワークに接続されたいくつかのプライマリサーバー（7、9）が利用できます

6. （5）は、パブリックIPアドレスを持つインターネット上のサーバーです
7. （6）はポイントツーサイトVPN接続（p2s）でクラウドに接続されているワークステーションです



この例では、**From:**列のサーバーから**To:**列のサーバーに対して、以下のような接続設定が利用できます（たとえば、「ping」）。

	［終了日:］	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
［開始時		ローカル	ローカル	ローカル	ローカル	インター	p2s	プライマリ	フェールオーバー	プライマリ	フェールオーバー	テストフェール	テストフェール	テストフェール	VPN	VPNサー

	[終了日:]	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
刻:]						ネット						オーバー	オーバー	オーバー	アプライアンス	バー
1	ローカル		ダイレクト	ローカルルーター1経由	ローカルルーター2経由	ローカルルーター1およびインターネット経由	いいえ	トンネル: local経由 ローカルルーター1およびインターネット: pub経由	トンネル: local経由 ローカルルーター1およびインターネット: pub経由	トンネル: local経由 ローカルルーター1およびインターネット: pub経由	トンネル: local経由 ローカルルーター1およびインターネット: pub経由	トンネル経由:NAT（VPNサーバー） ローカルルーター1およびインターネット: pub経由	トンネル経由:NAT（VPNサーバー） ローカルルーター1およびインターネット: pub経由	ローカルルーター1およびトンネル経由:NAT（VPNサーバー） ローカルルーター1およびインターネット: pub経由	ダイレクト	いいえ
2	ローカル	ダイレクト		ローカルルーター1経由	ローカルルーター2経由	ローカルルーター1およびインターネット	いいえ	トンネル: local経由 ローカルルーター1および	トンネル: local経由 ローカルルーター1および	トンネル: local経由 ローカルルーター1および	トンネル: local経由 ローカルルーター1および	トンネル経由:NAT（VPNサーバー）	トンネル経由:NAT（VPNサーバー）	ローカルルーター1およびトンネル経由:NAT	ダイレクト	いいえ

	[終了日:]	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						経由		インターネット: pub経由	インターネット: pub経由	インターネット: pub経由	インターネット: pub経由	ローカルルーター1およびインターネット: pub経由	ローカルルーター1およびインターネット: pub経由	（VPNサーバー） ローカルルーター1およびインターネット: pub経由		
3	ローカル	ローカルルーター1経由	ローカルルーター1経由		ローカルルーター2経由	ローカルルーター1およびインターネット経由	いいえ	トンネル: local経由 ローカルルーター1およびインターネット: pub経由	トンネル: local経由 ローカルルーター1およびインターネット: pub経由	トンネル: local経由 ローカルルーター1およびインターネット: pub経由	トンネル: local経由 ローカルルーター1およびインターネット: pub経由	トンネル経由:NAT（VPNサーバー） ローカルルーター1およびインターネット: pub経由	トンネル経由:NAT（VPNサーバー） ローカルルーター1およびインターネット: pub経由	ローカルルーター1およびトンネル経由:NAT（VPNサーバー） ローカルルーター1およびインターネット: pub経由	ローカルルーター経由	いいえ

	[終了日:]	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
4	ローカル	ローカルルーター2およびルーター1経由	ローカルルーター2およびルーター1経由	ローカルルーター2経由		ローカルルーター2、およびルーター1、およびインターネット経由	いいえ	ローカルルーター2およびトンネル経由:ローカル ローカルルーター2、およびローカルルーター1、およびインターネット:pub経由	ローカルルーター2およびトンネル経由:ローカル ローカルルーター2、およびローカルルーター1、およびインターネット:pub経由	ローカルルーター2およびトンネル経由:ローカル ローカルルーター2、およびローカルルーター1、およびインターネット:pub経由	ローカルルーター2およびトンネル経由:ローカル ローカルルーター2、およびローカルルーター1、およびインターネット:pub経由	トンネル経由:NAT（VPNサーバー） ローカルルーター2、およびルーター1、およびインターネット:pub経由	トンネル経由:NAT（VPNサーバー） ローカルルーター2、およびルーター1、およびインターネット:pub経由	トンネル経由:NAT（VPNサーバー） ローカルルーター2、およびルーター1、およびインターネット:pub経由	ローカルルーター2経由	いいえ
5	インターネット	いいえ	いいえ	いいえ	いいえ		使用不可	インターネット:pub経由	インターネット:pub経由	インターネット:pub経由	インターネット:pub経由	インターネット:pub経由	インターネット:pub経由	インターネット:pub経由	いいえ	いいえ
6	p2s	いいえ	いいえ	いいえ	いいえ	インターネット経由		p2s VPN（VPNサーバー）:local経由	p2s VPN（VPNサーバー）:local経由	p2s VPN（VPNサーバー）:local経由	p2s VPN（VPNサーバー）:local経由	p2s VPN経由 - NAT（VPNサーバー）	p2s VPN経由 - NAT（VPNサーバー）	p2s VPN経由 - NAT（VPNサーバー）	いいえ	いいえ

	[終了日:]	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								インターネット: pub経由	インターネット: pub経由	インターネット: pub経由	インターネット: pub経由	インターネット: pub経由	インターネット: pub経由	インターネット: pub経由		
7	プライマリ	トンネル経由	トンネル経由	トンネルおよびローカルルーター1経由	トンネルおよびローカルルーター1/2経由	インターネット経由（VPNサーバー経由）	いいえ		クラウドダイレクト: local	トンネルおよびローカルルーター1: local経由	トンネルおよびローカルルーター1: local経由	VPNサーバー経由:NAT	VPNサーバー経由:NAT	トンネルおよびローカルルーター1経由:NAT	いいえ	DHCPおよびDNSプロトコルのみ
8	フェールオーバー	トンネル経由	トンネル経由	トンネルおよびローカルルーター1経由	トンネルおよびローカルルーター1/2経由	インターネット経由（VPNサーバー経由）	いいえ	クラウドダイレクト: local		トンネルおよびローカルルーター1: local経由	トンネルおよびローカルルーター1: local経由	VPNサーバー経由:NAT	VPNサーバー経由:NAT	トンネルおよびローカルルーター1経由:NAT	いいえ	DHCPおよびDNSプロトコルのみ
9	プライマリ	トンネル	トンネル	トンネル	トンネル	インター	いいえ	トンネルおよび	トンネルおよび		クラウドダイレク	トンネルおよび	トンネルおよび	VPNサーバー経	いいえ	DHCPおよび

	[終了日:]	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		および ローカル ルーター1 経由	および ローカル ルーター1 経由	経由	経由	ネット 経由 （VPN サーバー経由）		ローカル ルーター 1: local 経由	ローカル ルーター 1: local 経由		ト: local	ローカル ルーター 1経由:NAT	ローカル ルーター 1経由:NAT	由:NAT		DNSプロトコルのみ
10	フェールオーバー	トンネルおよび ローカル ルーター1 経由	トンネルおよび ローカル ルーター1 経由	トンネル 経由	トンネル 経由	インターネット 経由 （VPN サーバー経由）	いいえ	トンネルおよび ローカル ルーター 1: local 経由	トンネルおよび ローカル ルーター 1: local 経由	クラウドダイレクト: local		トンネルおよび ローカル ルーター 1経由:NAT	トンネルおよび ローカル ルーター 1経由:NAT	VPNサーバー経由:NAT	いいえ	DHCPおよびDNSプロトコルのみ
11	テストフェールオーバー	いいえ	いいえ	いいえ	いいえ	インターネット 経由 （VPN サーバー経由）	いいえ	いいえ	いいえ	いいえ	いいえ		クラウドダイレクト: local	VPNサーバー: local経由（ルーティング）	いいえ	DHCPおよびDNSプロトコルのみ
12	テスト	いい	いい	いい	いい	イン	いい	いいえ	いいえ	いいえ	いいえ	クラウド		VPNサー	いい	DHCP

	[終了日:]	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	フェールオーバー	え	え	え	え	ターネット経由（VPNサーバー経由）	え					ダイレクト: local		バー: local経由（ルーティング）	え	およびDNSプロトコルのみ
13	テストフェールオーバー	いいえ	いいえ	いいえ	いいえ	インターネット経由（VPNサーバー経由）	いいえ	いいえ	いいえ	いいえ	いいえ	VPNサーバー: local経由（ルーティング）	VPNサーバー: local経由（ルーティング）		いいえ	DHCPおよびDNSプロトコルのみ
14	VPNアプライアンス	ダイレクト	ダイレクト	ローカルルーター1経由	ローカルルーター2経由	インターネット経由（ローカルルーター1）	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ		いいえ
15	VPNサーバー	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	

用語集

V

VPNアプライアンス

安全なVPNトンネルを介してローカルネットワークとクラウドサイト間の接続を可能にする特別な仮想マシン。VPNアプライアンスはローカルサイトに配置されています。

VPNゲートウェイ（旧称VPNサーバーまたは接続ゲートウェイ）

安全なVPNトンネルを介してローカルサイトとクラウドサイトのネットワーク間の接続を提供する特別な仮想マシン。VPNゲートウェイはクラウドサイトに配置されます。

く

クラウドサーバー

復元またはプライマリサーバーへの一般的な参照。

クラウドサイト（またはDRサイト）

リモートサイトはクラウドでホストされ、災害時に復元インフラストラクチャを実行するために使用されます。

さ

サイト間（S2S）接続

セキュアなVPNトンネル経由でローカルネットワークをクラウドに拡張する接続。

て

テストIPアドレス

本番用IPアドレスの重複を防ぐために、フェイルオーバーのテストの際に必要なIPアドレス。

テストネットワーク

フェールオーバープロセスをテストするために使用される、隔離された仮想ネットワーク。

は

パブリックIPアドレス

インターネットからクラウドサーバーを利用可能にするために必要なIPアドレス。

ふ

フェールオーバー

ローカルサイトで自然災害または人為的災害が生じた場合、ワークロードまたはアプリケーションをクラウドサイトへ切り替えます。

フェールバック

フェールオーバー中にサーバーをクラウドサイトに移動した後に、サーバーをローカルサイトに復元するプロセス。

プライマリサーバー

ローカルサイト上にリンクされたマシンがない仮想マシン（復元サーバーなど）。プライマリサーバーは、アプリケーションの保護や、さまざまな補助サービスの実行などに使用されます（Webサーバーなど）。

ほ

ポイントツーサイト（P2S）接続

エンドポイントデバイス（コンピューターまたはラップトップなど）を使用して、外部からクラウドおよびローカルサイトに接続する安全なVPN接続です。

ら

ランブック

ディザスタリカバリアクションを自動化する設定可能なステップからなる計画シナリオ。

ろ

ローカルサイト

会社の構内に配置されたローカルインフラストラクチャ。

漢字

確定

クラウドサーバーの本番フェイルオーバーまたは復元プロセスの中間状態。このプロセスは、サーバーの仮想ディスクをバックアップストレージ（「コールド」ストレージ）からディザスタリカバリストレージ（「ホット」ストレージ）に転送することを意味します。最終処理中は、パフォーマンスが通常より低くなりますが、サーバーはアクセスおよび操作可能です。

復元サーバー

クラウドに保存されている保護されたサーバーバックアップによる、元のマシンのVMレプリカ。災害発生時に、復元サーバーを使用して元のサーバーからワークロードを切り替えます。

復元ポイント目標（RPO）

停止によって失われたデータの量であり、計画された停止または災害イベントからの時間として測定されます。 RPOしきい値は、フェールオーバーのための最後の適切な復元ポイントと現在時刻との間の許容される最大時間間隔を定義します。

保護されたサーバー

カスタマーが所有し、サービスで保護されている物理または仮想マシン。

本番ネットワーク

VPNトンネルによって拡張され、ローカルおよびクラウドサイトの両方をカバーする内部ネットワーク。ローカルサーバーとクラウドサーバーは本番ネットワーク上で互いに通信できます。

索引