Backup Gateway クイックスタートガイド（VMware vSphere）

リリース ***3.5***

Acronis International GmbH

2020 年 **07** 月 **31** 日

目次

第 1 章

このガイドについて

このガイドでは、VMware vSphere 6.5 以降で Acronis Cyber Infrastructure をデプロイして Backup Gateway を設定する方法を説明します。

以下の作業が必要です。

1. ネットワークを設定します。
2. Acronis Cyber Infrastructure の仮想マシンを作成します。
3. 仮想マシンに Acronis Cyber Infrastructure をデプロイします。

これらの手順について、この後のセクションで詳しく説明します。

Acronis Cyber Infrastructure をデプロイしたら、それぞれの用途に合わせた設定が必要です。Backup Gateway のセットアップ手順については、*Backup Gateway を経由した Acronis Backup ソフトウェアとストレージバックエンドの接続* (ページ 19) を参照してください。その他の手順の説明については、:doc:『管理者ガイド <admins_guide:index>』を参照してください。

1.1 要件

- Backup Gateway シナリオでは、Acronis Cyber Infrastructure を 1 つの仮想マシンにデプロイできます。一方、汎用配置環境の場合は、3 つから 5 つの仮想マシンを作成して、ロードバランシングと高可用性を有効にすることをお勧めします。
- vSphere データストアのストレージに十分な空き領域があることを確認してください。各仮想マシンが少なくとも 425 GB の領域を使用します（200 GB のストレージディスクが 2 つと、25 GB のシステムディスクが 1 つ）。Acronis Cyber Infrastructure のテンプレートも約 35 GB の領域を使用します。
- ホストに十分なメモリがあることを確認してください。1 ノードのセットアップでは、最低でも 4 GB の RAM が必要です。それ以外の場合は、管理ノードのために最低 8 GB の RAM、各セカンダリノードのために最低 4 GB の RAM が必要です。

- Backup Gateway クラスターごとに別々のオブジェクトコンテナを使用してください。

注釈: Backup Gateway シナリオの詳細なハードウェア要件については、Hardware Requirements を参照してください。

第 2 章

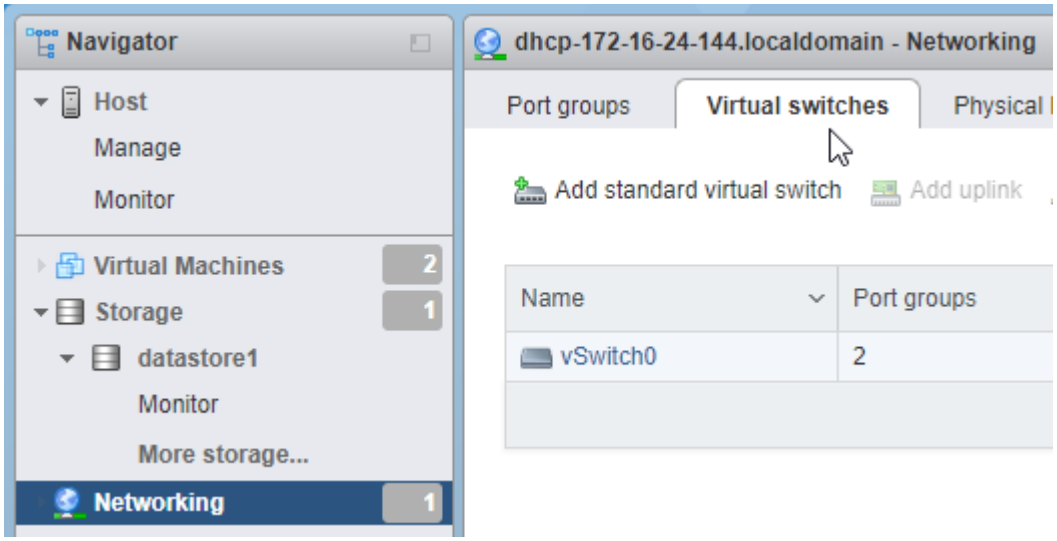
ネットワークの設定

Acronis Cyber Infrastructure では通常 2 つのネットワークが必要です。外部接続のためのパブリックネットワークと、仮想マシン同士の間のデータ交換のためのプライベートネットワークです。パブリックネットワークはすでにセットアップされている場合が多いですが、プライベートネットワークについては、すでに存在する場合でも専用のプライベートネットワークを作成することをお勧めします。プライベートネットワークを作成するには、カスタムセキュリティパラメータとポートグループを設定した仮想スイッチが必要です。

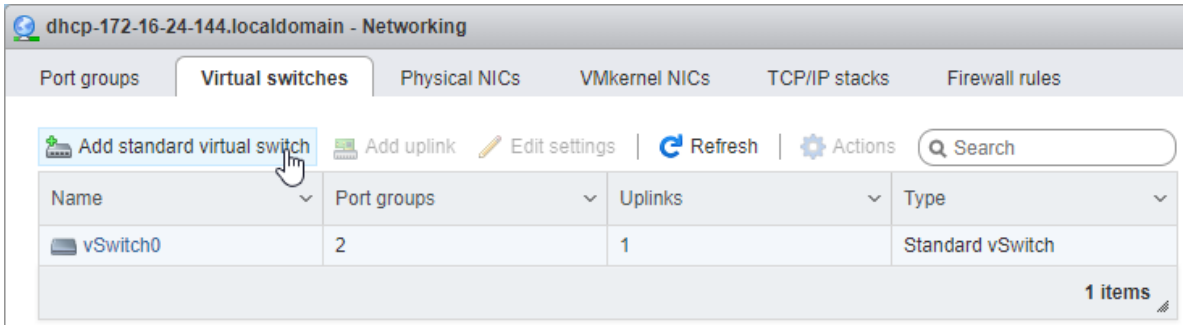
注釈: 詳細なネットワーク要件については、Planning Network を参照してください。

仮想スイッチを作成するには、以下の手順を実行します。

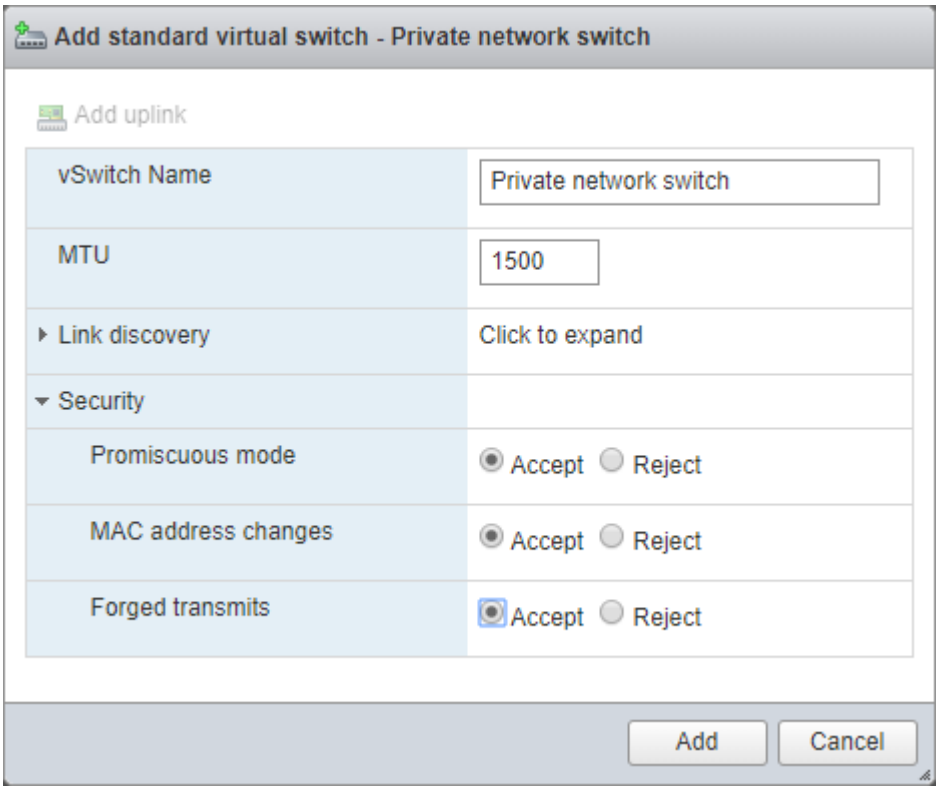
1. ホストクライアントの左のメニューで **[ネットワーク]** をクリックします。**[仮想スイッチ]** タブを開きます。



2. ツールバーで **[標準仮想スイッチを追加]** をクリックします。

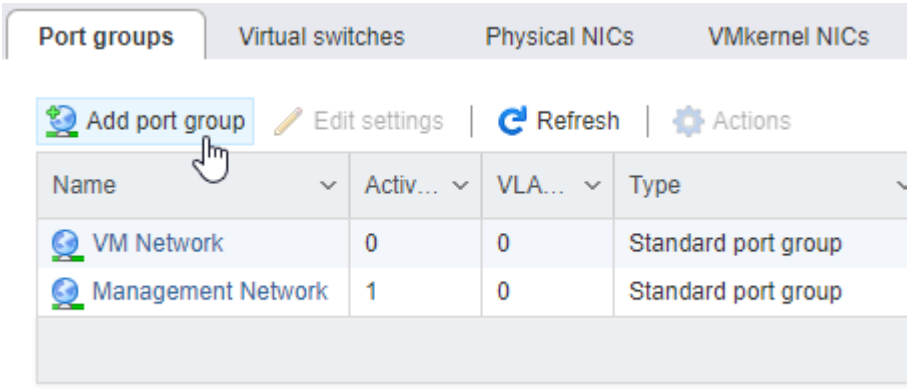


3. スイッチ名を入力して、**[セキュリティ]** を展開します。**[無作為モード]**、**[MAC アドレス変更]**、**[偽造送信]** で **[受け入れる]** を選択します。

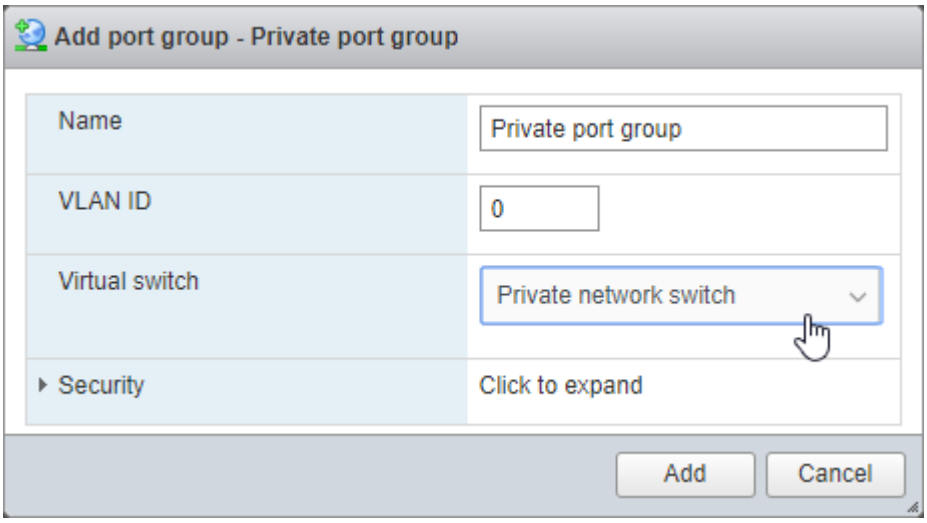


ポートグループを作成するには、以下の手順を実行します。

1. **[ポートグループ]** タブを開き、ツールバーで **[ポートグループを追加]** をクリックします。



2. ポートグループ名を入力します。先ほど作成した仮想スイッチを選択します。



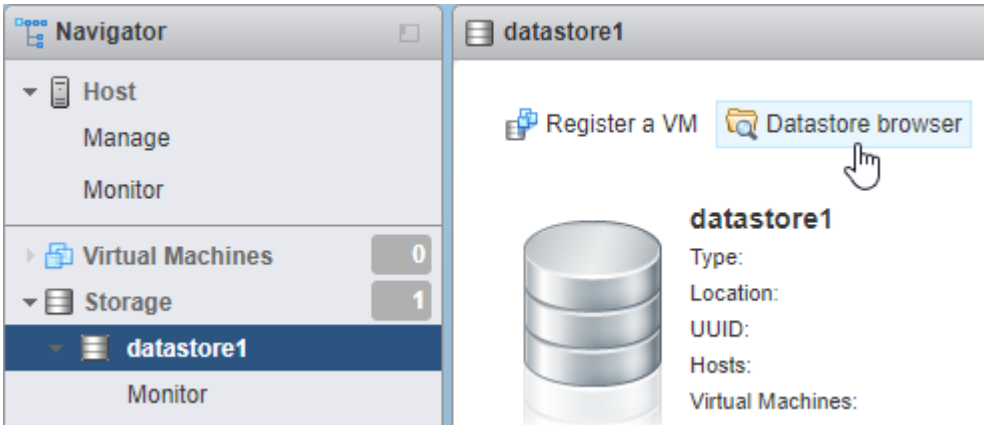
第 3 章

仮想マシンの作成

まず Acronis Cyber Infrastructure イメージ（2 つの VMDK ファイル）を入手します。そのためには、製品ページにアクセスして、要求を送信します。

次に、2 つの VMDK ファイルを VMware vSphere データストアにアップロードします。

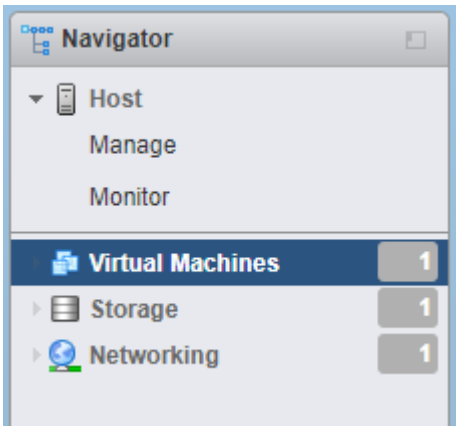
1. **[ナビゲーター]** パネルで、対象のデータストアをクリックします。ツールバーで **[データストアブラウザ]** をクリックします。
2. **[データストアブラウザ]** ウィンドウで、仮想マシンの名前にちなんだディレクトリを作成します。



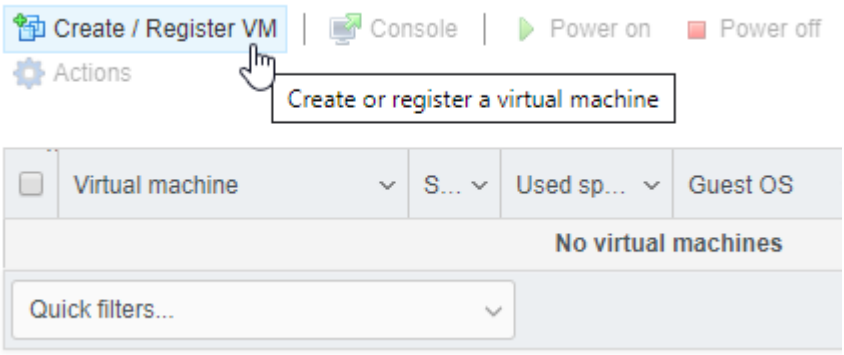
3. そのディレクトリに Acronis Cyber Infrastructure イメージ（2 つの VMDK ファイル）をアップロードします。

以下の手順を実行して、Acronis Cyber Infrastructure の仮想マシンを作成します。

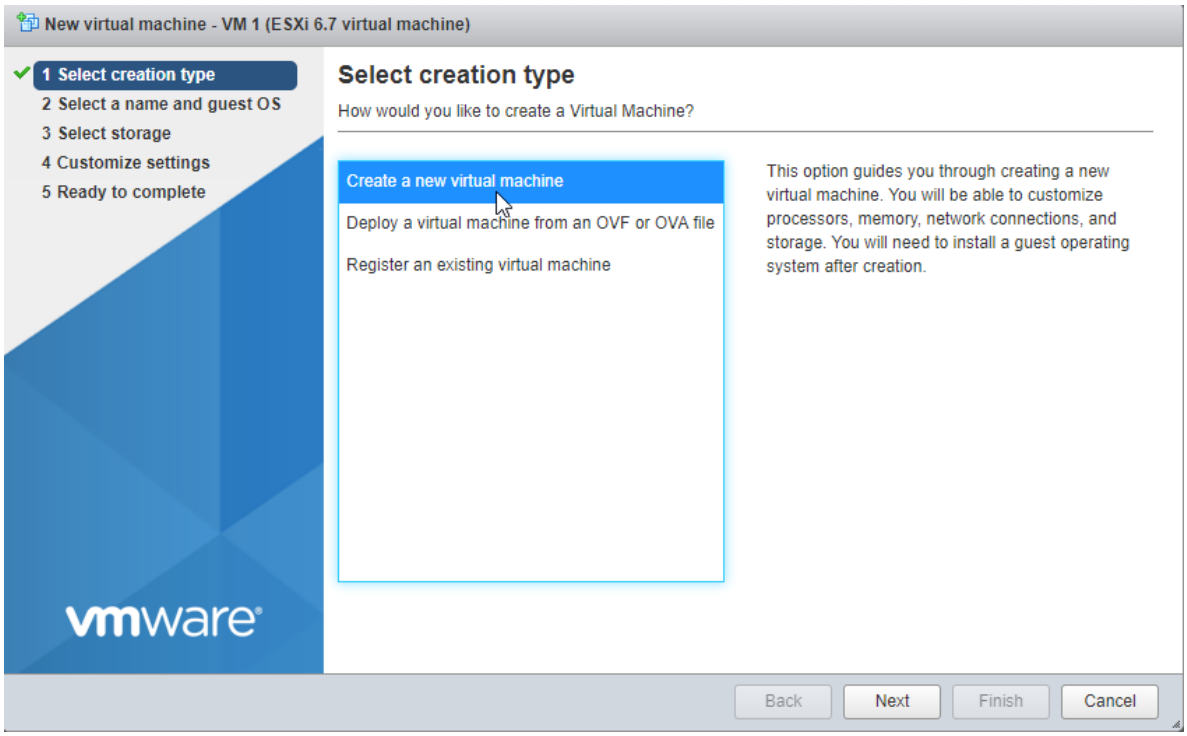
1. ホストクライアントの左のメニューで **[仮想マシン]** をクリックします。



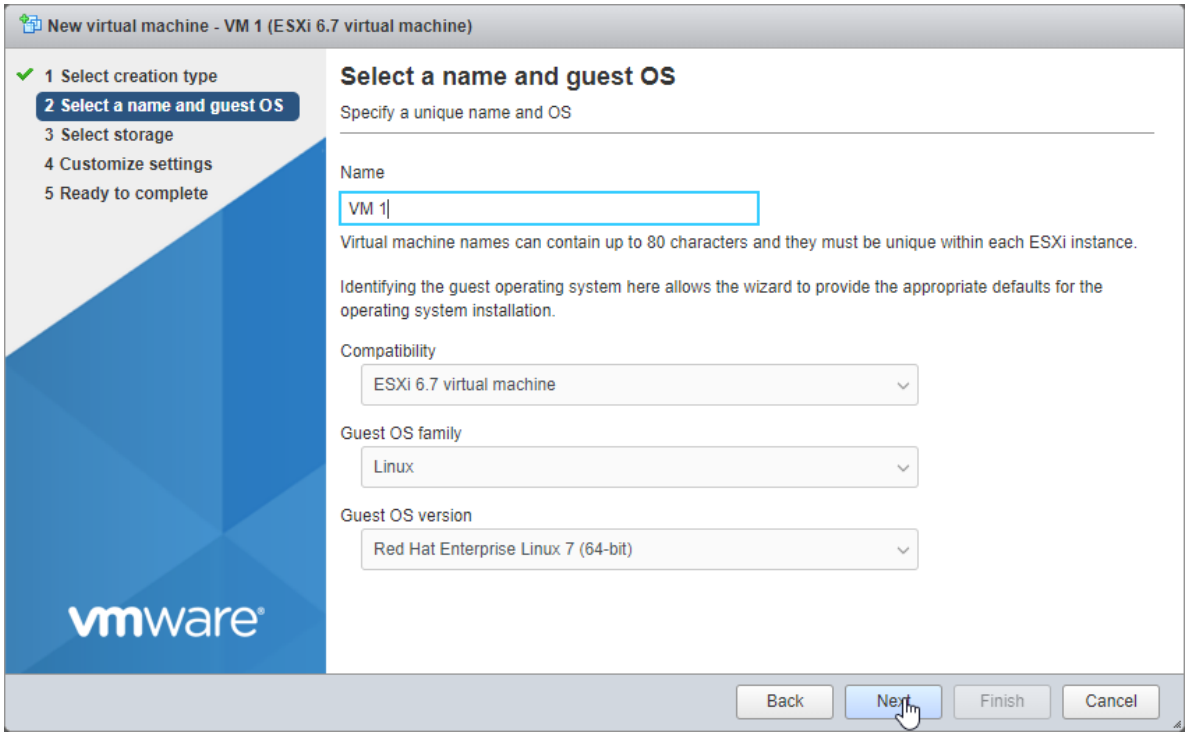
2. ツールバーで **[VM を作成/登録]** をクリックします。



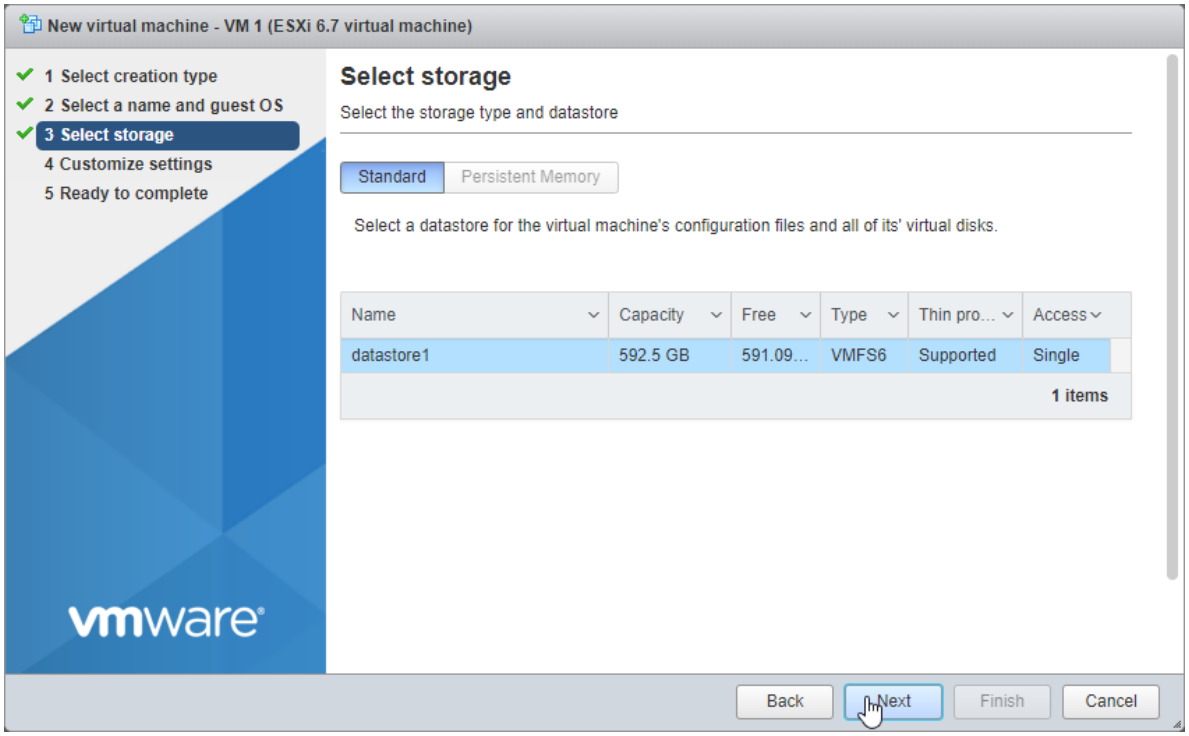
3. **[新しい仮想マシン]** ウィザードの手順 1 で、**[新しい仮想マシンを作成]** を選択します。**[次へ]** をクリックします。



4. 手順 2 で、仮想マシンの名前を入力し、ゲスト OS を選択します。[次へ] をクリックします。

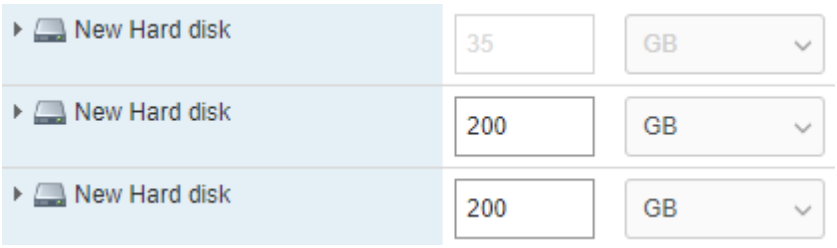


5. 手順 3 で、ストレージタイプとデータストアを選択します。データストアに十分な空き領域があることを確認してください。

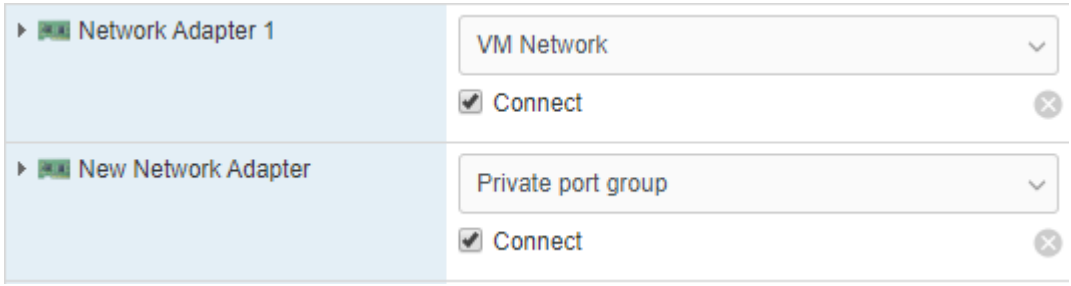


6. 手順 4 で、既存のハードディスクを削除し、ツールバーで **[ハードディスクを追加]** をクリックします。**[既存のハードディスク]** を選択し、先ほどデータストアにアップロードしたイメージを見付けて選択します。**[選択]** をクリックします。

7. ツールバーで **[ハードディスクを追加]** を再びクリックします。**[新しい標準ハードディスク]** を選択します。サイズを 200 GB に設定します。この手順を繰り返して、200 GB のハードディスクをもう 1 つ追加します。全部で 3 つのハードディスクになります。それぞれ、35 GB と 200 GB と 200 GB です。



8. **[設定をカスタマイズ]** ウィンドウのツールバーで **[ネットワークアダプタを追加]** をクリックします。1 つのアダプタがパブリックネットワークに接続し、もう 1 つのアダプタが作成したプライベートポートグループに接続していることを確認してください。



9. 手順 5 で、設定内容を確認し、**[完了]** をクリックします。
10. **[ナビゲーター]** メニューで仮想マシンを選択して起動します。

この手順を繰り返して、対象のシナリオで必要な数だけ仮想マシンを作成します（要件 (ページ 1) を参照）。

第 4 章

仮想マシンでの Acronis Cyber Infrastructure のデプロイ

仮想マシンが起動したら、次の手順を実行してください。

1. storage-user としてログインします。デフォルトのパスワード（password）を使用してください。パスワードを 1 度変更するよう求められます。例:

```
You are required to change your password immediately (root enforced)
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user storage-user.
Changing password for storage-user.
(current) UNIX password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

   （現在の）UNIX パスワードでは password を入力し、新しいパスワードとパスワードの再入力では新しいパスワードを入力します。storage-user とルートユーザーの両方でパスワードを変更できます。

2. 新しいパスワードを使って storage-user として再度ログインし、ルートユーザーに切り替えます。

```
$ sudo su
```

3. [eth1] ネットワークインターフェースを設定して有効にします。

```
# cat > /etc/sysconfig/network-scripts/ifcfg-eth1 << EOF
ARPCHECK="no"
BOOTPROTO="static"
IPADDR=192.168.1.<node>
NETMASK=255.255.255.0
DEVICE="eth1"
```

(次のページに続く)

(前のページからの続き)

```
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
NAME="eth1"
ONBOOT="yes"
EOF
# ifup eth1
```

<node>はノード番号です。2 は管理ノード、3 は最初のセカンダリノードといった具合になります。

4. IP アドレスが割り当てられていて、インターフェースが稼働していること（`ip -4 a show eth1` のようになっていること）を確認してください。

その他の設定は、ノードのロールによって異なります。1 つの管理ノードをデプロイする必要がありますし、2 つから 4 つのセカンダリノードをデプロイすることも可能です。

4.1 管理ノードのデプロイ

1. 管理ノードを登録し、管理者パネルを初期化するには、root ユーザーとして以下のように実行します。

```
# echo '<passwd>' | /usr/libexec/vstorage-ui-backend/bin/configure-backend.sh \
-i <int_net> -x <ext_net>
# systemctl start vstorage-ui-backend
# systemctl start vstorage-ui-agent
# /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <mn_IP>
```

<passwd>は対象の管理者パスワード、<int_net>は内部（プライベート）ネットワークインターフェース、<ext_net>は外部（パブリック）ネットワークインターフェース、<mn_IP>は管理ノードの IP アドレスです。

2. 仮想マシンを再起動します。管理者パネルの IP アドレスが端末の [ようこそ] 画面に表示されます。ポート 8888 で管理者パネルにログインできます。admin ユーザー名と、前の手順で指定した管理ノードの root パスワードを使用します。

   デプロイしたノードが、管理者パネルの **[インフラストラクチャ] > [ノード]** 画面の **[割り当て解除]** リストに表示されます。

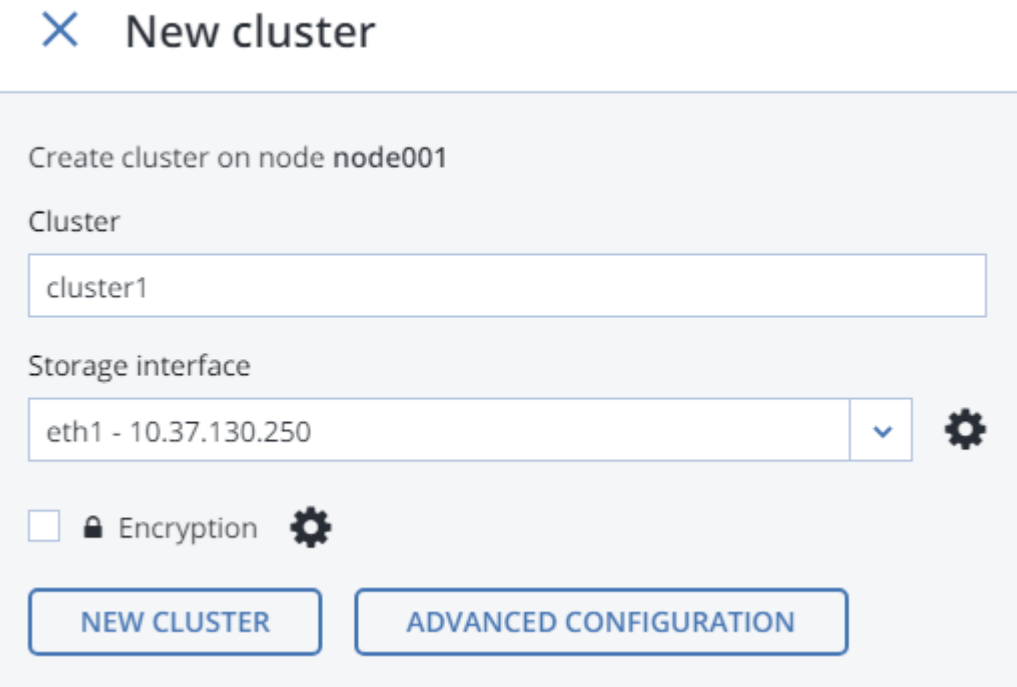
3. **[インフラストラクチャ] > [ネットワーク]** 画面で **[編集]** をクリックします。**[API を計算]** トラフィックタイプをパブリックネットワークで使用できるようにして、**[保存]** をクリックします。

次に、ストレージクラスターを作成する必要があります。以下の手順を実行します。

1. **[インフラストラクチャ] > [ノード]** 画面を開いて、**[割り当て解除]** リストでノードをクリックします。

2. ノードの概要画面で **[クラスターを作成]** をクリックします。

3. **[クラスター]** フィールドにクラスターの名前を入力します。名前に使用できるのは、英字（a-z、A-Z）、数字（0-9）、下線（_）、ハイフン（-）だけです。



4. **[新しいクラスター]** をクリックします。

ストレージクラスターの準備ができました。対象のシナリオでセカンダリノードのデプロイが必要な場合は、その作業に進みます。Backup Gateway で必要なノードが 1 つだけの場合は、*Backup Gateway* を経由した *Acronis Backup* ソフトウェアとストレージバックエンドの接続 (ページ 19) に進みます。

4.2 セカンダリノードのデプロイ

仮想マシンでセカンダリノードをデプロイするには、以下の手順を実行します。

1. 管理者パネルで管理ノードの IP アドレスとトークンを取得します。**[インフラストラクチャ]** > **[ノード]** を開きます。**[ノードを追加]** をクリックし、管理ノードの IP アドレスとトークンの画面を呼び出します。

2. 仮想マシンの端末を開き、以下のようにしてセカンダリノードを管理者パネルに登録します。

```
# /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <mn_addr> -t
↪<token>
```

   <mn_addr>は管理ノードの IP アドレス、<token>は管理者パネルで取得したトークンです。

   新しく登録したセカンダリノードが、管理者パネルの **[インフラストラクチャ]** > **[ノード]** 画面の **[割り当て解除]** リストに表示されます。

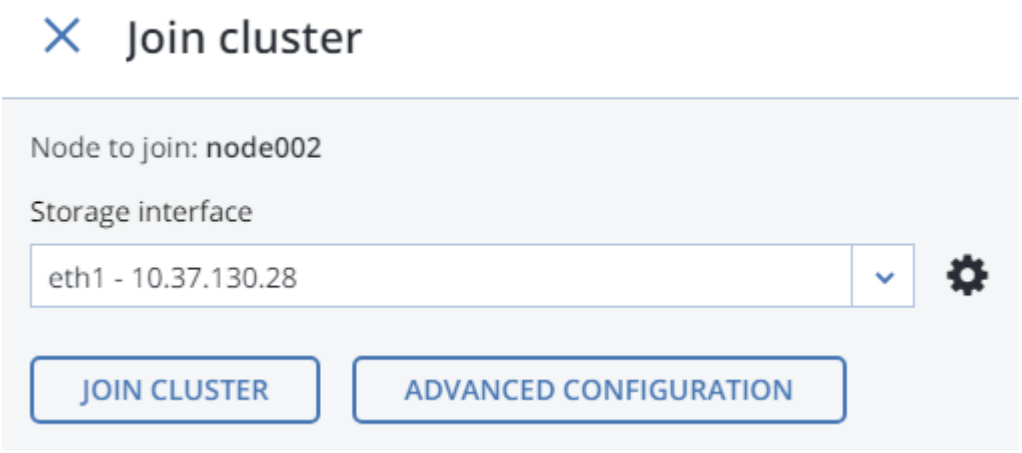
3. セカンダリノードをストレージクラスターに追加します。

   （a）**[インフラストラクチャ] > [ノード]** 画面で、まだ割り当てられていないノードをクリックします。

   （b）ノードの概要画面で **[クラスターを接続]** をクリックします。

   （c）トラフィックタイプ **[ストレージ]** でネットワークに接続しているネットワークインターフェースが **[ストレージインターフェース]** ドロップダウンリストで選択されていることを確認します。

   ノードのネットワークインターフェースが設定されていない場合は、歯車のアイコンをクリックし、トラフィックタイプ **[ストレージ]** のネットワークをノードのネットワークインターフェースに割り当てます。



   （d）**[クラスターを接続]** をクリックすると、Acronis Cyber Infrastructure によってディスクにロールが自動的に割り当てられ、現在のクラスターにノードが追加されます。**[詳細構成]** をクリックして、各ドライブに手動でロールを割り当てることも可能です。

各セカンダリノードでこの手順を繰り返します。ストレージクラスターにすべてがそろったら、**[設定] > [管理ノード] > [高可用性を管理]** 画面で、管理ノードの高可用性を有効にできます。

対象のシナリオに合わせた Acronis Cyber Infrastructure のセットアップに進みます。各種の設定タスクを実行する方法については、:doc:『管理者ガイド <admins_guide:index>』を参照してください。

第 5 章

Acronis Cyber Infrastructure に領域を追加しています

新しいディスクを作成する前に、以下の推奨サイズを検討してください。

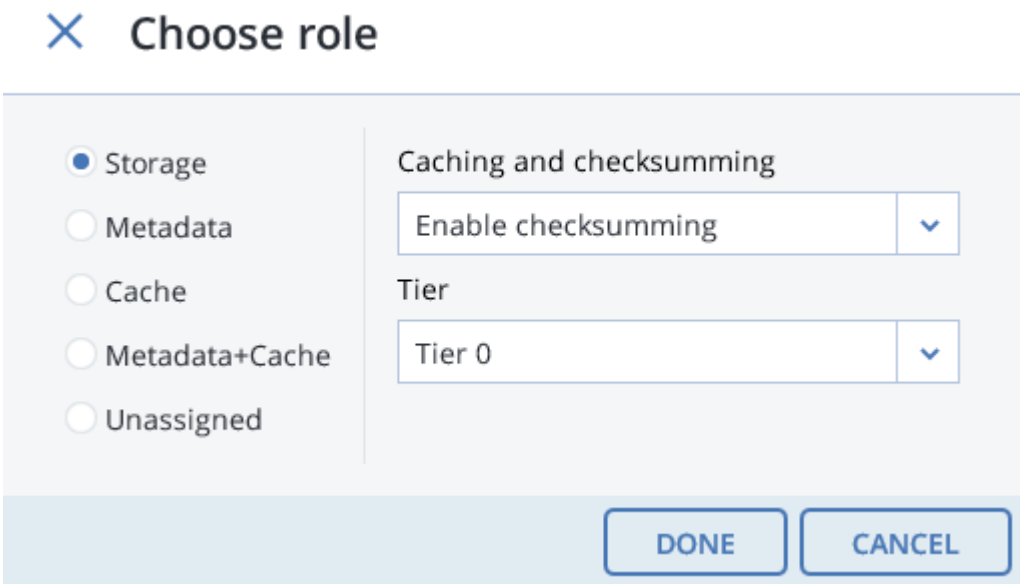
1. 複数のノードのクラスターを使用している場合、冗長性の要因からノードを同じサイズにする必要があります。これにより、データはノード全体に均一に広がります。詳細については、Understanding Allocatable Disk Space を参照してください。
2. 同じサイズのディスクを使用することで、負荷をより均一に分散できるようになります。クラスターの内部では、ディスクの使用率が、ディスクのサイズに比例します。たとえば、10TB のディスクと 2TB のディスクがある場合、50% のクラスター負荷では、それぞれ 5TB と 1TB を使用することになります。

ストレージクラスターの物理領域を拡張したい場合、ノードに新しい仮想ディスクを追加できます。Acronis Cyber Infrastructure 仮想マシンで、VMware vSphere の **[ディスク拡張]** オプションを使用しないでください。このオプションでは、ファイルシステムのサイズが適切に変更されないためです。それで以下で説明するように、新しい仮想ディスクを作成して、お使いの仮想マシンに追加してください。

「新しいハードディスクを仮想マシンに追加する」で説明されているように、新しい仮想ディスクをお使いの仮想マシンに追加します。その後、追加されたディスクは、Acronis Cyber Infrastructure の管理者パネルでノードのディスクの一覧に表示されます。

管理者パネルで、次の手順を実行して新しいディスクを構成します。

1. **[インフラストラクチャ] > [ノード]** 画面で、作成されたディスクのノードをクリックします。**[ディスク]** セクションをクリックして、ノードのすべてのディスクを表示します。
2. **[割り当て解除]** ロールのディスクが、先に作成したディスクです。これを選択して、右側で **[割り当て]** をクリックします。
3. **[ロールを選択]** 画面で、**[ストレージ]** ロール、ティア、また必要に応じて [チェックサム機能を有効にする] を選択します。詳細については、Assigning Disk Roles Manually を参照してください。


Choose role
Storage
Metadata
Cache
Metadata+Cache
Unassigned
Caching and checksumming
Enable checksumming
Tier
Tier 0
DONE
CANCEL

第 6 章

Backup Gateway を経由した Acronis Backup ソフトウェアとストレージバックエンドの接続

Backup Gateway ストレージアクセスポイント（ゲートウェイともいう）は、Acronis Backup Cloud や Acronis Backup Advanced を使用していて、クライアントのバックアップデータのオンプレミスストレージを編成したいと考えているサービスプロバイダーを対象にしています。

Backup Gateway を使用するサービスプロバイダーは、Acronis 専用の重複除外対応のデータ形式に合わせたストレージを簡単に設定できます。

Backup Gateway では、以下のストレージバックエンドがサポートされています。

- イレージャーコーディングによってソフトウェアの冗長性を確保したストレージクラスター
- NFS 共有
- パブリッククラウド（幾つかの S3 ソリューションや、Microsoft Azure、OpenStack Swift、Google Cloud Platform など）

シナリオや要件に基づいてバックエンドを選択するのは当然ですが、Acronis Backup のデータの保存先としてはローカルストレージクラスターをお勧めします。そうすれば、WAN の最適化とデータのローカル性によって最適なパフォーマンスが得られます。NFS 共有やパブリッククラウドにバックアップを保存すると、データ転送などのオーバーヘッドが避けられず、全体的なパフォーマンスが低下します。

以下の点に注意してください。

- Backup Gateway を設定する時には、Acronis Backup ソフトウェアの管理者アカウントの資格情報を指定する必要があります。
- Backup Gateway で、ローカルストレージではなく外部ストレージ（NFS など）を使用する場合は、その外部ストレージで冗長性を確保しなければなりません。Backup Gateway 自体はデータ冗長性がなく、データ重複除外を実行しません。

- Acronis Backup Cloud で Backup Gateway を登録できるようにするには、パートナーアカウントで二要素認証（2FA）を無効にする必要があります。

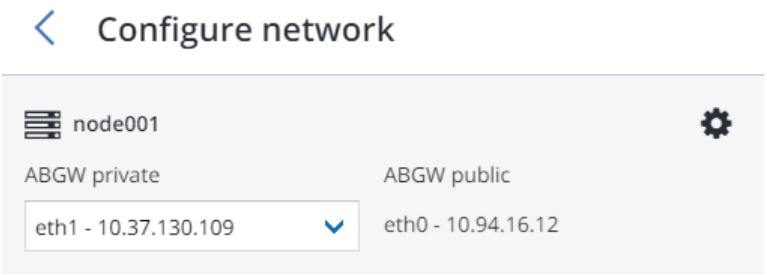
6.1 Backup Gateway を経由したローカルストレージクラスターへの接続

作業を進める前に、ターゲットストレージに既存のバックアップと新しいバックアップのための十分な領域があることを確認してください。

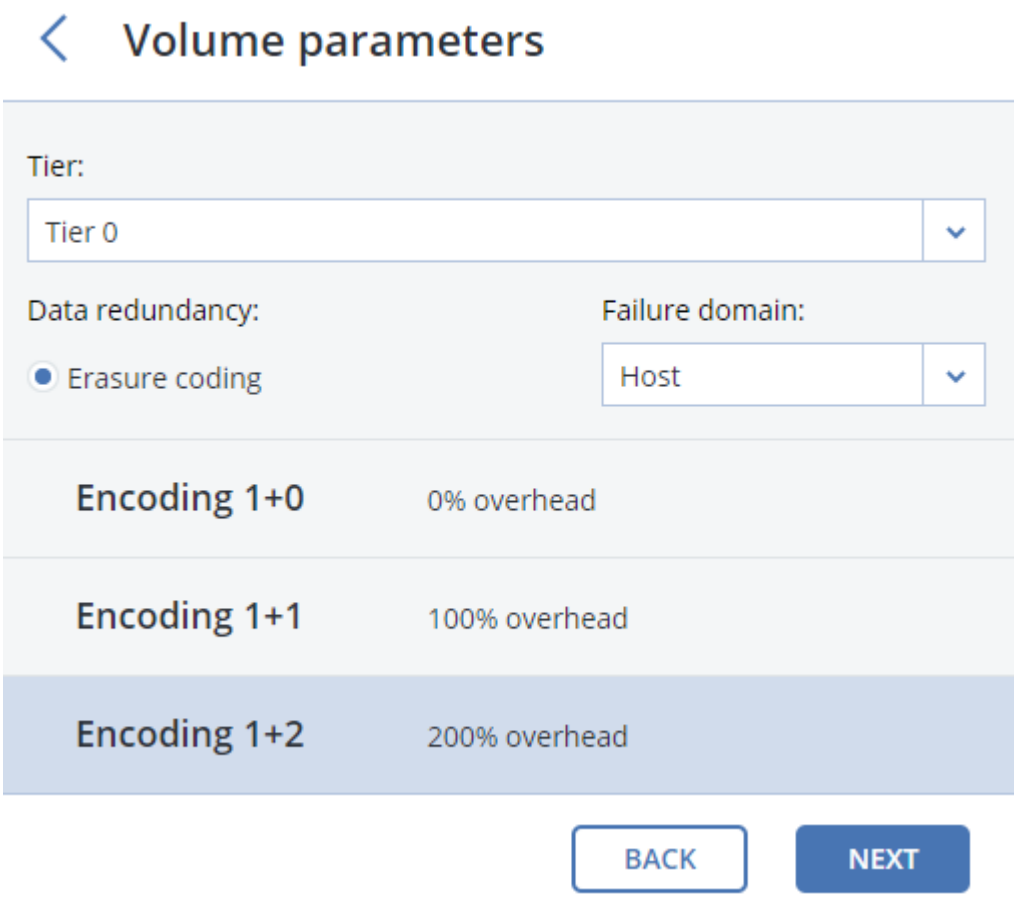
Backup Gateway をセットアップするには、以下の手順を実行します。

1. **[インフラストラクチャ] > [ネットワーク]** 画面で、**[ABGW プライベート]** と **[ABGW パブリック]** のトラフィックタイプが、使用するネットワークに追加されていることを確認します。
2. 左のメニューで、**[ストレージサービス] > [バックアップストレージ]** をクリックします。
3. ゲートウェイサービスを実行するノードを選択し、右のメニューで **[ゲートウェイを作成]** をクリックします。
4. ストレージタイプとして **[この Acronis Cyber Infrastructure クラスター]** を選択します。
5. ドロップダウンリストで正しいネットワークインターフェースが選択されていることを確認します。**[次へ]** をクリックします。

   必要に応じて、歯車のアイコンをクリックし、**[ネットワークの構成]** 画面でノードのネットワークインターフェースを設定します。



6. **[ボリュームパラメータ]** タブで、対象のティア、障害のあるドメイン、データ冗長性モードを選択します。詳細については、Understanding Storage Tiers、Understanding Failure Domains、および Understanding Data Redundancy を参照してください。



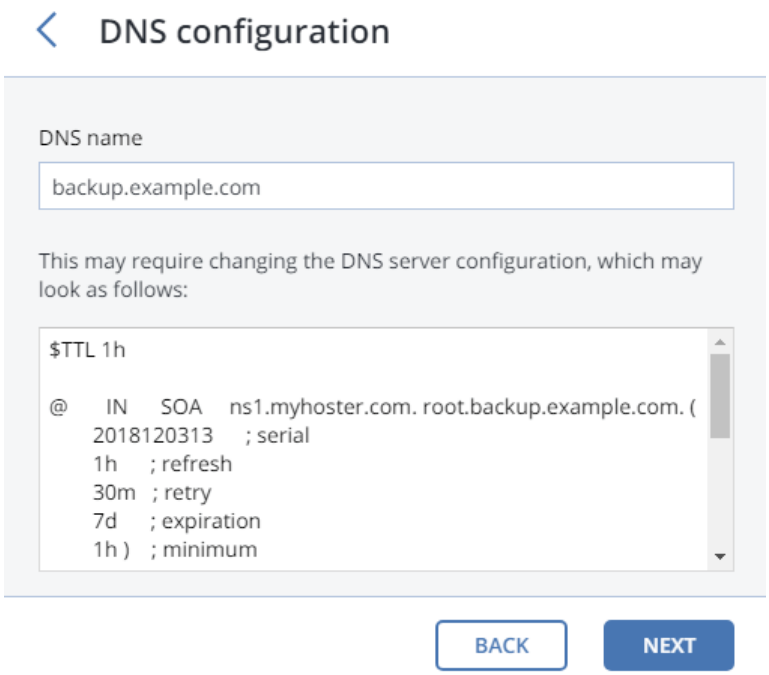
レプリケーションによる冗長性は、Backup Gateway ではサポートされていません。イレージャーコーディングの場合、クラスターのパフォーマンスを低下させる恐れがあるため、冗長性スキームの変更は無効化されています。再エンコードには、長時間にわたり大量のクラスターリソースを要するというのがその理由です。上記に関わらず冗長性スキーム変更をご希望の場合は、テクニカルサポートまでご連絡ください。

[次へ] をクリックします。

7. **[DNS 構成]** タブで、このゲートウェイの外部 FQDN（`backupgateway.example.com` など）を指定します。ゲートウェイサービスを実行する各ノードで、発信インターネット接続と Acronis Backup ソフトウェアからの着信接続のためのポートが開いていることを確認します。バックアップエージェントはそのアドレスとポートを使用してバックアップデータをアップロードします。

重要: 管理者パネルに表示されるサンプルに従って DNS サーバーを設定します。

重要: Backup Gateway クラスター内のノードを変更するたびに、その変更に合わせて DNS 設定を調整してください。



[次へ] をクリックします。

8. [バックアップソフトウェアで登録します] ペインで、対象の Acronis 製品について以下の情報を指定します。

重要: パートナーアカウントで二要素認証（2FA）が無効になっていることを確認してください。また、2FA を有効にしたテナント内の特定のユーザー（Acronis Cyber Cloud の資料を参照）の認証を無効にして、ユーザーの資格情報を指定することもできます。

   - [アドレス] で、Acronis Backup Cloud の管理ポータルのアドレス（https://cloud.acronis.com/など）または Acronis Backup Advanced の管理サーバーのホスト名/IP アドレスとポート（http://192.168.1.2:9877など）を指定します。
   - [アカウント] で、クラウド内のパートナーアカウントまたはローカル管理サーバー上の組織管理者の資格情報を入力します。

9. 最後に [完了] をクリックします。

6.2 Backup Gateway を経由した外部 NFS 共有への接続

以下の制限事項に注意してください。

- Acronis Cyber Infrastructure では、NFS ボリュームの上でデータ冗長性を実現することはできません。実装環境によっては、NFS 共有で独自のハードウェア冗長性やソフトウェア冗長性を使用することも可能です。
- 現行バージョンの Acronis Cyber Infrastructure では、NFS ボリュームでバックアップを保管できるのは、1 つのクラスターノードに限られます。

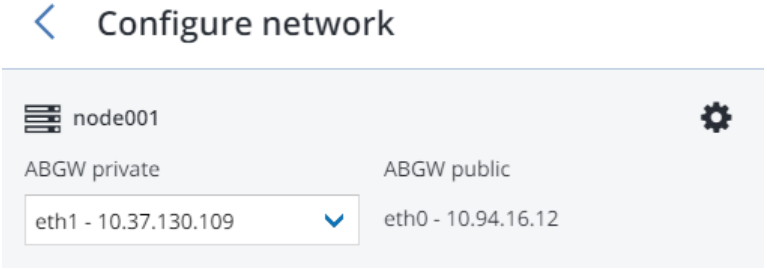
作業を進めるために、以下の点を確認してください。

1. NFS 共有にバックアップ用の十分な領域があります。
2. 各 NFS エクスポートを 1 つのゲートウェイだけが使用しています。特に、2 つの Acronis Cyber Infrastructure インストール環境がバックアップストレージとして同じ NFS エクスポートを使用するような設定は行わないでください。

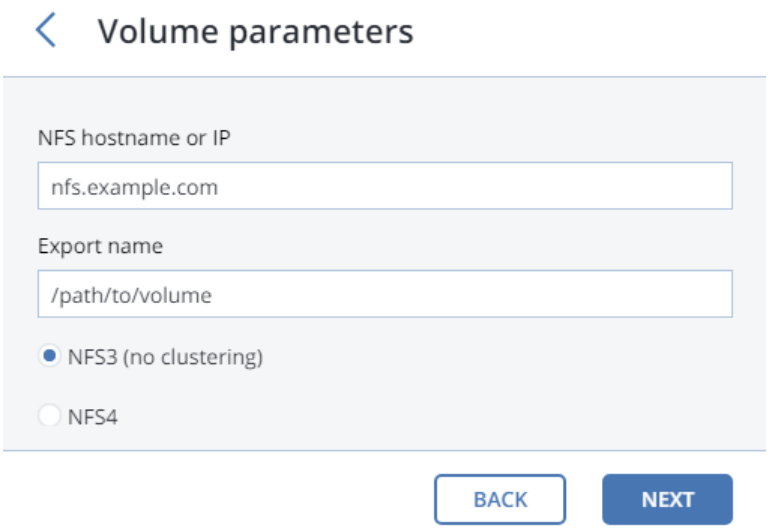
Backup Gateway をセットアップするには、以下の手順を実行します。

1. **[インフラストラクチャ] > [ネットワーク]** 画面で、**[ABGW プライベート]** と **[ABGW パブリック]** のトラフィックタイプが、使用するネットワークに追加されていることを確認します。
2. 左のメニューで、**[ストレージサービス] > [バックアップストレージ]** をクリックします。
3. ゲートウェイサービスを実行するノードを選択し、右のメニューで **[ゲートウェイを作成]** をクリックします。
4. ストレージタイプとして **[ネットワークファイルシステム]** を選択します。
5. ドロップダウンリストで正しいネットワークインターフェースが選択されていることを確認します。**[次へ]** をクリックします。

   必要に応じて、歯車のアイコンをクリックし、**[ネットワークの構成]** 画面でノードのネットワークインターフェースを設定します。



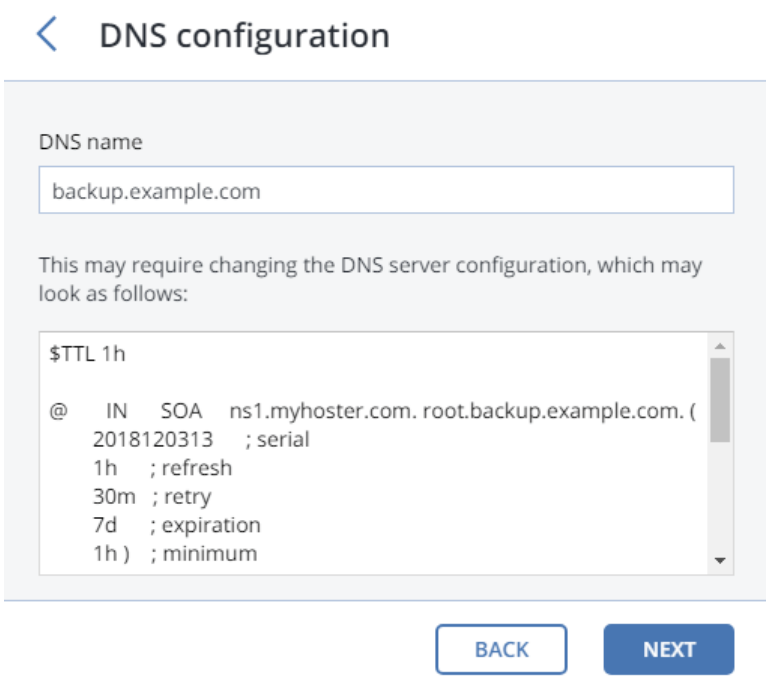
6. **[ボリュームパラメータ]** タブで、NFS 共有のホスト名または IP アドレスとエクスポート名を指定します。**[次へ]** をクリックします。



7. **[DNS 構成]** タブで、このゲートウェイの外部 FQDN（`backupgateway.example.com` など）を指定します。ゲートウェイサービスを実行する各ノードで、発信インターネット接続と Acronis Backup ソフトウェアからの着信接続のためのポートが開いていることを確認します。バックアップエージェントはそのアドレスとポートを使用してバックアップデータをアップロードします。

重要: 管理者パネルに表示されるサンプルに従って DNS サーバーを設定します。

重要: Backup Gateway クラスター内のノードを変更するたびに、その変更に合わせて DNS 設定を調整してください。



[次へ] をクリックします。

8. [バックアップソフトウェアで登録します] ペインで、対象の Acronis 製品について以下の情報を指定します。

重要: パートナーアカウントで二要素認証（2FA）が無効になっていることを確認してください。また、2FA を有効にしたテナント内の特定のユーザー（Acronis Cyber Cloud の資料を参照）の認証を無効にして、ユーザーの資格情報を指定することもできます。

   - [アドレス] で、Acronis Backup Cloud の管理ポータルのアドレス（https://cloud.acronis.com/など）または Acronis Backup Advanced の管理サーバーのホスト名/IP アドレスとポート（http://192.168.1.2:9877など）を指定します。
   - [アカウント] で、クラウド内のパートナーアカウントまたはローカル管理サーバー上の組織管理者の資格情報を入力します。

9. 最後に [完了] をクリックします。

6.3 Backup Gateway を経由したパブリッククラウドストレージへの接続

Backup Gateway を使用する場合は、Acronis Backup Cloud または Acronis Backup Advanced によって、さまざまなパブリッククラウドとオンプレミスのオブジェクトストレージソリューションにバックアップを保管できます。

- Amazon S3
- IBM Cloud
- Alibaba Cloud
- IIJ
- Cleversafe
- Cloudian
- Microsoft Azure
- Swift オブジェクトストレージ
- Softlayer（Swift）
- Google Cloud Platform
- Wasabi
- S3 を使用するその他のソリューション

しかし、パブリッククラウドにバックアップデータを保管すると、ローカルストレージクラスターの場合よりもあらゆる入出力要求の待機時間が長くなり、パフォーマンスが低下します。それで、ストレージバックエンドとしてローカルストレージクラスターを使用することをお勧めします。

バックアップは特定のアクセスパターンによるコールドデータです。つまり、データに頻繁にアクセスが発生することはありませんが、アクセスがあった際には即座に利用できることが想定されています。このような頻繁にデータへのアクセスが発生しないケースの場合、コスト効率の面では、長期間の稼働を想定したストレージクラスを選択するのが最適です。推奨ストレージクラスを以下に挙げます。

- Amazon S3 の**低頻度アクセス**
- Microsoft Azure の**クール BLOB Storage**
- Google Cloud Platform の**ニアライン/コールドライン**ストレージ

Amazon S3 Glacier、Azure Archive Blob、Google Archive のようなアーカイブストレージクラスは、データへの即時アクセスが行われないため、バックアップには使用できません。アクセス時の待機時間が長い（数時間単位）と、アーカイブの参照、高速なデータ復元、増分バックアップの作成が技術的に不可能になります。アーカイブストレージは一般的に非常に低コストだとしても、複数のコスト要因があることに留意してください。パブリッククラウドストレージの実際のコストは、データの格納、オペレーション、トラフィック、データの復旧、早期の削除

などに要する費用の合計になります。たとえば、アーカイブストレージサービスの場合、わずか 1 回のデータ再呼び出し操作に 6 ヶ月分のストレージ料金が請求されることもあります。ストレージデータへのアクセスが頻繁に発生することが見込まれる場合は、コストが追加されてデータストレージの総コストが大幅に増加します。データ復旧率の低下を避けつつコストを削減するには、バックアップデータの格納に Acronis Cyber Cloud を使用することをお勧めします。

6.3.1 重要な要件と制限事項

1. Backup Gateway はパブリッククラウドを操作する時に、ローカルストレージをステージング域として使用したり、サービス情報の保管場所にしたりします。つまり、パブリッククラウドにアップロードされるデータは、まずローカル環境で保管されてからターゲットに送信されるということです。それで、ローカルストレージの永続性と冗長性を確保してデータが失われないようにすることが重要です。ローカルストレージの永続性と冗長性を確保する方法は幾つかあります。Backup Gateway を複数のクラスターノードに配置して、適切な冗長性モードを選択できます。Acronis Cyber Infrastructure とゲートウェイを 1 つの物理ノードにデプロイする場合は、複数のローカルディスク間でストレージをレプリケートすることでローカルストレージを冗長化できます。Acronis Cyber Infrastructure とゲートウェイを仮想マシンにデプロイする場合は、基盤になっている仮想環境ソリューションによって冗長化してください。

2. ローカルストレージクラスターにステージング用の論理領域を十分に確保してください。たとえば、毎日バックアップを実行する場合、少なくとも 1.5 日分のバックアップに十分な領域を確保してください。日単位のバックアップの合計量が 2TB なら、最低でも 3TB の論理領域を確保するということです。必要なローストレージは、エンコードモードによって異なります。1+2 モードなら 9TB（1 ノードあたり 3TB）、3+2 モードなら 5TB（1 ノードあたり 1TB）といった具合になります。

3. Amazon S3 クラウドでバックアップを保管する場合は、Amazon S3 の最終的な一貫性が原因で、Backup Gateway によりそのようなバックアップをブロックされることがあります。その結果、Amazon S3 が古いデータを返してくることもあります。データの最新バージョンにアクセスできるようになるまでに、時間が必要だからです。Backup Gateway はそのような遅れを検出すると、バックアップの整合性を確保するために、クラウドが更新されるまでアクセスをブロックします。

4. Backup Gateway クラスターごとに別々のオブジェクトコンテナを使用してください。

6.3.2 Backup Gateway のセットアップ

作業を進める前に、ターゲットストレージにバックアップ用の十分なスペースがあることを確認してください。

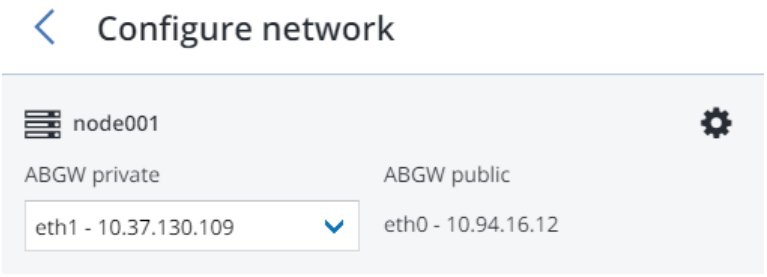
Backup Gateway をセットアップするには、以下の手順を実行します。

1. **[インフラストラクチャ] > [ネットワーク]** 画面で、**[ABGW プライベート]** と **[ABGW パブリック]** のトラフィックタイプが、使用するネットワークに追加されていることを確認します。

2. 左のメニューで、**[ストレージサービス] > [バックアップストレージ]** をクリックします。

3. ゲートウェイサービスを実行するノードを選択し、右のメニューで **[ゲートウェイを作成]** をクリックします。
4. ストレージのタイプとして **[パブリッククラウド]** を選択します。
5. ドロップダウンリストで正しいネットワークインターフェースが選択されていることを確認します。**[次へ]** をクリックします。

   必要に応じて、歯車のアイコンをクリックし、**[ネットワークの構成]** 画面でノードのネットワークインターフェースを設定します。



6. **[パブリッククラウドパラメータ]** ペインで以下の手順を実行します。

   （a）パブリッククラウドプロバイダーを選択します。プロバイダーと S3 との間に互換性があるにもかかわらず、リストに掲載されていない場合は、**[AuthV2 互換（S3）]** または **[AuthV4 互換（S3）]** を試してみてください。

   （b）プロバイダーに応じて、**[リージョン]**、**[認証（keystone）URL]**、**[エンドポイント URL]** のいずれかを指定します。

   （c）Swift オブジェクトストレージの場合は、必要な認証プロトコルのバージョンと属性を指定します。

   （d）ユーザーの資格情報を指定します。Google Cloud の場合は、アップロードするキーを組み込んだ JSON ファイルを選択します。

   （e）バックアップを保管するフォルダ（バケット、コンテナ）を指定します。書き込み可能なフォルダを指定してください。

   Backup Gateway クラスターごとに別々のオブジェクトコンテナを使用してください。

   [次へ] をクリックします。

7. **[バックアップソフトウェアで登録します]** ペインで、対象の Acronis 製品について以下の情報を指定します。

重要: パートナーアカウントで二要素認証（2FA）が無効になっていることを確認してください。また、2FA を有効にしたテナント内の特定のユーザー（Acronis Cyber Cloud の資料を参照）の認証を無効にして、ユーザーの資格情報を指定することもできます。

- **[アドレス]** で、Acronis Backup Cloud の管理ポータルのアドレス（https://cloud.acronis.com/など）または Acronis Backup Advanced の管理サーバーのホスト名/IP アドレスとポート（http://192.168.1.2:9877など）を指定します。
- **[アカウント]** で、クラウド内のパートナーアカウントまたはローカル管理サーバー上の組織管理者の資格情報を入力します。

8. 最後に **[完了]** をクリックします。