オンプレミスにエージェントをインストールする

NetApp Console setup and administration

NetApp
February 26, 2026

目次

オンプレミスにエージェントをインストールする

オンプレミスにコンソールエージェントを手動でインストールする

オンプレミスにコンソール エージェントをインストールし、ログインして、コンソール組織で動作するように設定します。

VMWare ユーザーの場合は、OVA を使用して VCenter にコンソール エージェントをインストールできます。"VCenter にエージェントをインストールする方法の詳細について説明します。"

インストールする前に、ホスト (VM または Linux ホスト) が要件を満たしていること、およびコンソール エージェントがインターネットと対象ネットワークへの送信アクセスできることを確認する必要があります。NetAppデータ サービス、またはCloud Volumes ONTAPなどのクラウド ストレージ オプションを使用する予定の場合は、コンソール エージェントがユーザーに代わってクラウド内でアクションを実行できるように、クラウド プロバイダーで資格情報を作成してコンソールに追加する必要があります。

コンソールエージェントのインストールの準備

コンソール エージェントをインストールする前に、インストール要件を満たすホスト マシンがあることを確認する必要があります。また、ネットワーク管理者と協力して、コンソール エージェントが必要なエンドポイントへの送信アクセスと対象ネットワークへの接続を持っていることを確認する必要があります。

コンソールエージェントホストの要件を確認する

オペレーティング システム、RAM、およびポートの要件を満たす x86 ホストでコンソール エージェントを実行します。コンソール エージェントをインストールする前に、ホストがこれらの要件を満たしていることを確認してください。

コンソール エージェントは、19000 ～ 19200 の UID と GID の範囲を予約します。この範囲は固定されており、変更することはできません。ホスト上のサードパーティ ソフトウェアがこの範囲内の UID または GID を使用している場合、エージェントのインストールは失敗します。NetApp、競合を回避するためにサードパーティ ソフトウェアがインストールされていないホストの使用を推奨しています。

専用ホスト

コンソール エージェントには専用のホストが必要です。次のサイズ要件を満たすアーキテクチャであれば、どれでもサポートされます。

- CPU: 8コアまたは8vCPU
- メモリ: 32 GB
- ディスク容量: ホストには 165 GB が推奨され、パーティション要件は次のとおりです。
  - `/opt`: 120 GiBの空き容量が必要です

    エージェントは `/opt`インストールするには `/opt/application/netapp`ディレクトリとその内容。

- `/var`: 40 GiBの空き容量が必要です

  コンソールエージェントにはこのスペースが必要です `/var`Podman または Docker は、このディレクトリ内にコンテナを作成するように設計されているためです。具体的には、`/var/lib/containers/storage`ディレクトリと `/var/lib/docker`Docker用。このスペースでは外部マウントまたはシンボリックリンクは機能しません。

ハイパーバイザー

サポートされているオペレーティング システムを実行することが認定されているベア メタルまたはホスト型ハイパーバイザーが必要です。

オペレーティングシステムとコンテナの要件

コンソールを標準モードまたは制限モードで使用する場合、コンソール エージェントは次のオペレーティング システムでサポートされます。エージェントをインストールする前に、コンテナ オーケストレーション ツールが必要です。

オペレーティング システム	サポートされる**OS** バージョン	サポートされているエージェントのバージョン	必要なコンテナツール	**SELinux**
Red Hat Enterprise Linux		9.6 • 英語版のみ。 • ホストは Red Hat Subscription Management に登録されている必要があります。登録されていない場合、ホストはエージェントのインストール中に必要なサードパーティ製ソフトウェアを更新するためにリポジトリにアクセスできません。	4.0.0 以降、コンソールが標準モードまたは制限モード	Podman バージョン 5.4.0 と podman-compose 1.5.0。 Podman の構成要件を表示する 。

オペレーティングシステム	サポートされるOSバージョン	サポートされているエージェントのバージョン	必要なコンテナツール	SELinux
強制モードまたは許可モードでサポートされます		9.1～9.4 • 英語版のみ。 • ホストは Red Hat Subscription Management に登録されている必要があります。登録されていない場合、ホストはエージェントのインストール中に必要なサードパーティ製ソフトウェアを更新するためにリポジトリにアクセスできません。	3.9.50 以降、コンソールが標準モードまたは制限モード	Podman バージョン 4.9.4 と podman-compose 1.5.0。 Podman の構成要件を表示する 。
強制モードまたは許可モードでサポートされます		8.6～8.10 • 英語版のみ。 • ホストは Red Hat Subscription Management に登録されている必要があります。登録されていない場合、ホストはエージェントのインストール中に必要なサードパーティ製ソフトウェアを更新するためにリポジトリにアクセスできません。	3.9.50 以降、コンソールが標準モードまたは制限モード	Podman バージョン 4.6.1 または 4.9.4 と podman-compose 1.0.6。 Podman の構成要件を表示する 。
強制モードまたは許可モードでサポートされます	Ubuntu		24.04 LTS	3.9.45 以降、NetApp Consoleが標準モードまたは制限モード
Docker エンジン 23.06 から 28.0.0。	サポート対象外		22.04 LTS	3.9.50以降

コンソールエージェントのネットワークアクセスを設定する

コンソール エージェントがリソースを管理できるようにネットワーク アクセスを設定します。ターゲット ネットワークへの接続と特定のエンドポイントへのアウトバウンド インターネット アクセスが必要です。

ターゲットネットワークへの接続

コンソール エージェントには、システムを作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムまたはストレージ システムを作成する予定のネットワークなどです。

アウトバウンドインターネットアクセス

コンソール エージェントを展開するネットワークの場所には、特定のエンドポイントに接続するための送信インターネット接続が必要です。

Webベースの**NetApp Console**を使用する際にコンピュータから接続されるエンドポイント

Web ブラウザからコンソールにアクセスするコンピュータは、複数のエンドポイントに接続できる必要があります。コンソール エージェントを設定し、コンソールを日常的に使用するには、コンソールを使用する必要があります。

"NetAppコンソールのネットワークを準備する" 。

コンソールエージェントから接続されたエンドポイント

コンソール エージェントは、日常業務でパブリック クラウド環境内のリソースとプロセスを管理するために、次のエンドポイントに接続するために、送信インターネット アクセスを必要とします。

以下にリストされているエンドポイントはすべて CNAME エントリです。

オンプレミスにインストールされたコンソール エージェントは、Google Cloud 内のリソースを管理できません。 Google Cloud リソースを管理するには、Google Cloud にエージェントをインストールする必要があります。

AWS

コンソール エージェントをオンプレミスでインストールする場合、AWS に導入されたNetAppシステム (Cloud Volumes ONTAPなど) を管理するために、次の AWS エンドポイントへのネットワーク アクセスが必要です。

コンソールエージェントから接続されたエンドポイント

コンソール エージェントは、日常業務でパブリック クラウド環境内のリソースとプロセスを管理するために、次のエンドポイントに接続するために、送信インターネット アクセスを必要とします。

以下にリストされているエンドポイントはすべて CNAME エントリです。

エンドポイント	目的
AWS サービス (amazonaws.com): • クラウドフォーメーション • エラスティックコンピューティングクラウド (EC2) • アイデンティティとアクセス管理（IAM） • キー管理サービス (KMS) • セキュリティトークンサービス（STS） • シンプルストレージサービス（S3）	AWS リソースを管理します。エンドポイントは AWS リージョンによって異なります。 "詳細についてはAWSドキュメントを参照してください"
NetApp ONTAP用の Amazon FsX: • api.workloads.netapp.com	Web ベースのコンソールは、このエンドポイントに接続して Workload Factory API と対話し、FSx for ONTAPベースのワークロードを管理および操作します。
https://mysupport.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信します。
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェアアップデートを受信します。

エンドポイント	目的
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、NetApp、ファイアウォールルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

Azure

コンソール エージェントがオンプレミスにインストールされている場合、Azure にデプロイされたNetAppシステム (Cloud Volumes ONTAPなど) を管理するために、次の Azure エンドポイントへのネットワーク アクセスが必要です。

エンドポイント	目的
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Azure パブリック リージョン内のリソースを管理します。
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Azure China リージョンのリソースを管理します。

エンドポイント	目的
https://mysupport.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信します。
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェアアップデートを受信します。
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、NetApp、ファイアウォールルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

プロキシ サーバ

NetApp は明示的プロキシ構成と透過的プロキシ構成の両方をサポートしています。透過プロキシを使用している場合は、プロキシ サーバーの証明書のみを提供する必要があります。明示的なプロキシを使用している場合は、IP アドレスと資格情報も必要になります。

- IPアドレス
- Credentials
- HTTPS証明書

ポート

ユーザーが開始した場合、またはCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用された場合を除いて、コンソール エージェントへの着信トラフィックはありません。

- HTTP (80) と HTTPS (443) は、まれにしか使用されないローカル UI へのアクセスを提供します。
- SSH（22）は、トラブルシューティングのためにホストに接続する必要がある場合にのみ必要です。
- アウトバウンド インターネット接続が利用できないサブネットにCloud Volumes ONTAPシステムを展開する場合は、ポート 3128 経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムにAutoSupportメッセージを送信するためのアウトバウンド インターネット接続がない場合、コンソールは、コンソール エージェントに含まれているプロキシ サーバーを使用するようにそれらのシステムを自動的に構成します。唯一の要件は、コンソール エージェントのセキュリティ グループがポート 3128 経由の受信接続を許可していることを確認することです。コンソール エージェントを展開した後、このポートを開く必要があります。

NTP を有効にする

NetApp Data Classificationを使用して企業のデータ ソースをスキャンする予定の場合は、システム間で時刻が同期されるように、コンソール エージェントとNetApp Data Classificationシステムの両方で Network Time Protocol (NTP) サービスを有効にする必要があります。 "NetAppデータ分類の詳細"

AWS または **Azure** のコンソール エージェント クラウド権限を作成する

オンプレミスのコンソールエージェントを使用して AWS または Azure のNetAppデータ サービスを使用する場合は、クラウド プロバイダーで権限を設定し、インストール後にコンソールエージェントに資格情報を追加する必要があります。

Google Cloud に存在するリソースを管理するには、Google Cloud に Console エージェントをインストールする必要があります。

AWS

コンソール エージェントがオンプレミスにインストールされている場合は、必要な権限を持つ IAM ユーザーのアクセス キーを追加して、コンソールに AWS 権限を付与する必要があります。

コンソール エージェントがオンプレミスにインストールされている場合は、この認証方法を使用する必要があります。 IAM ロールは使用できません。

手順

1. AWS コンソールにログインし、IAM サービスに移動します。
2. ポリシーを作成します。

   a. *ポリシー > ポリシーの作成*を選択します。

   b. *JSON*を選択し、その内容をコピーして貼り付けます。"コンソールエージェントのIAMポリシー" 。

   c. 残りの手順を完了してポリシーを作成します。

      使用する予定のNetAppデータ サービスによっては、2 番目のポリシーを作成する必要がある場合があります。

   標準リージョンの場合、権限は 2 つのポリシーに分散されます。 AWS の管理ポリシーの最大文字サイズ制限により、2 つのポリシーが必要になります。"コンソールエージェントのIAMポリシーの詳細" 。

3. IAM ユーザーにポリシーをアタッチします。
   - "AWSドキュメント: IAMロールの作成"
   - "AWSドキュメント: IAMポリシーの追加と削除"
4. コンソール エージェントをインストールした後、 NetApp Consoleに追加できるアクセス キーがユーザーにあることを確認します。

結果

これで、必要な権限を持つ IAM ユーザーのアクセス キーを取得できるはずです。コンソール エージェントをインストールした後、コンソールからこれらの資格情報をコンソール エージェントに関連付けます。

Azure

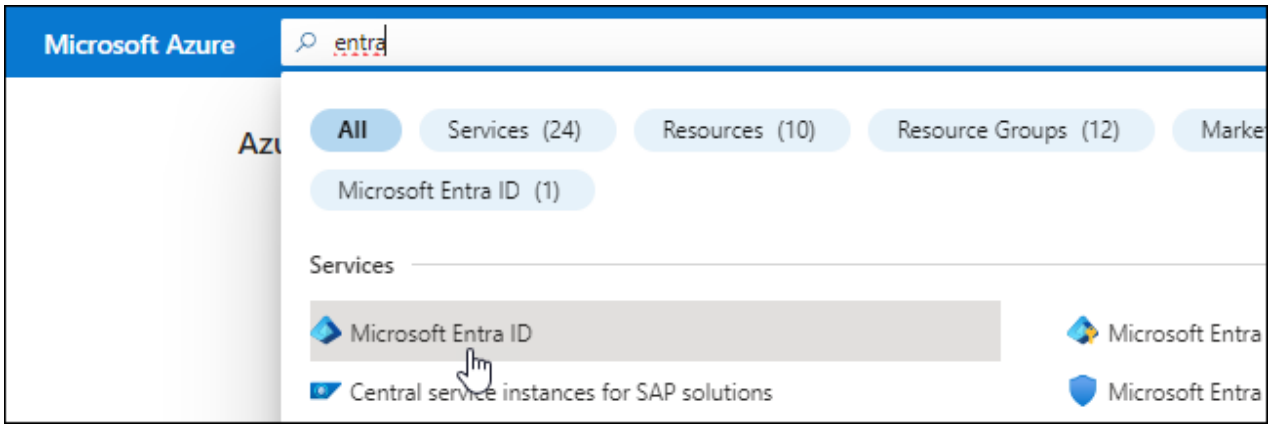
コンソール エージェントがオンプレミスでインストールされている場合は、Microsoft Entra ID でサービス プリンシパルを設定し、コンソール エージェントに必要な Azure 資格情報を取得して、コンソール エージェントに Azure 権限を付与する必要があります。

ロールベースのアクセス制御用の **Microsoft Entra** アプリケーションを作成する

1. Azure で Active Directory アプリケーションを作成し、そのアプリケーションをロールに割り当てるためのアクセス許可があることを確認します。

   詳細については、 "Microsoft Azure ドキュメント: 必要な権限"

2. Azure ポータルから、**Microsoft Entra ID** サービスを開きます。



3. メニューで*アプリ登録*を選択します。
4. *新規登録*を選択します。
5. アプリケーションの詳細を指定します。
   - 名前: アプリケーションの名前を入力します。
   - アカウント タイプ: アカウント タイプを選択します (いずれのタイプもNetApp Consoleで使用できます)。
   - リダイレクト **URI**: このフィールドは空白のままにすることができます。
6. *登録*を選択します。

   AD アプリケーションとサービス プリンシパルを作成しました。

アプリケーションをロールに割り当てる

1. カスタム ロールを作成します。

   Azure ポータル、Azure PowerShell、Azure CLI、または REST API を使用して、Azure カスタム ロールを作成できます。次の手順は、Azure CLI を使用してロールを作成する方法を示しています。別の方法をご希望の場合は、 "Azureドキュメント"

   a. の内容をコピーします"コンソールエージェントのカスタムロール権限"JSON ファイルに保存します。
   b. 割り当て可能なスコープに Azure サブスクリプション ID を追加して、JSON ファイルを変更します。

      ユーザーがCloud Volumes ONTAPシステムを作成する各 Azure サブスクリプションの ID を追加する必要があります。

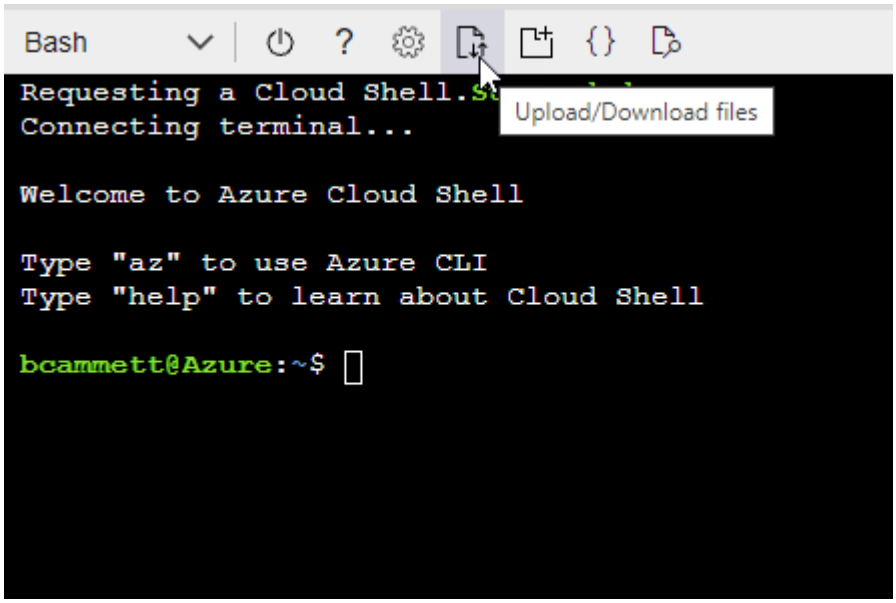
      例

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
]
```

c. JSON ファイルを使用して、Azure でカスタム ロールを作成します。

次の手順では、Azure Cloud Shell で Bash を使用してロールを作成する方法について説明します。

- 始める "Azure クラウド シェル"Bash 環境を選択します。
- JSON ファイルをアップロードします。



- Azure CLI を使用してカスタム ロールを作成します。

```
az role definition create --role-definition agent_Policy.json
```

これで、コンソール エージェント仮想マシンに割り当てることができる、コンソール オペレーターと呼ばれるカスタム ロールが作成されます。

2. アプリケーションをロールに割り当てます。

a. Azure ポータルから、サブスクリプション サービスを開きます。

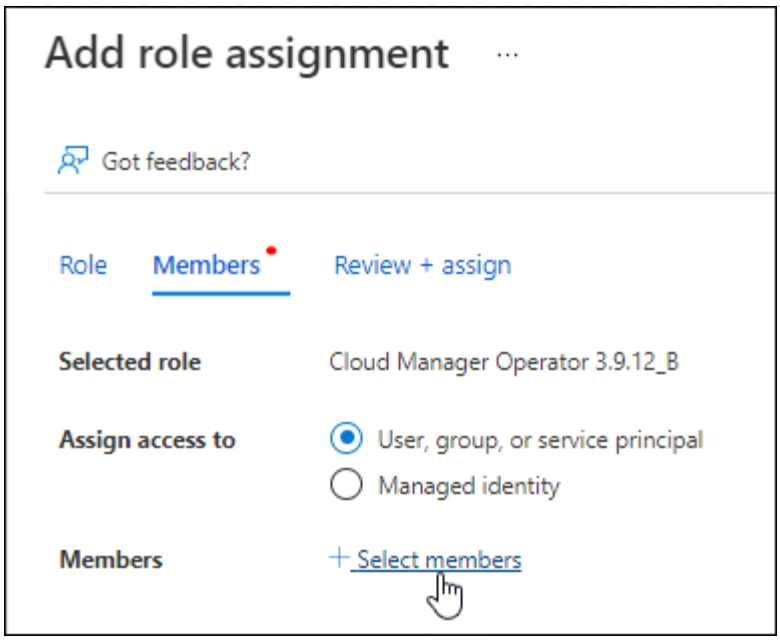
b. サブスクリプションを選択します。

c. アクセス制御 **(IAM) >** 追加 **>** ロール割り当ての追加 を選択します。

d. *役割*タブで、*コンソールオペレーター*役割を選択し、*次へ*を選択します。

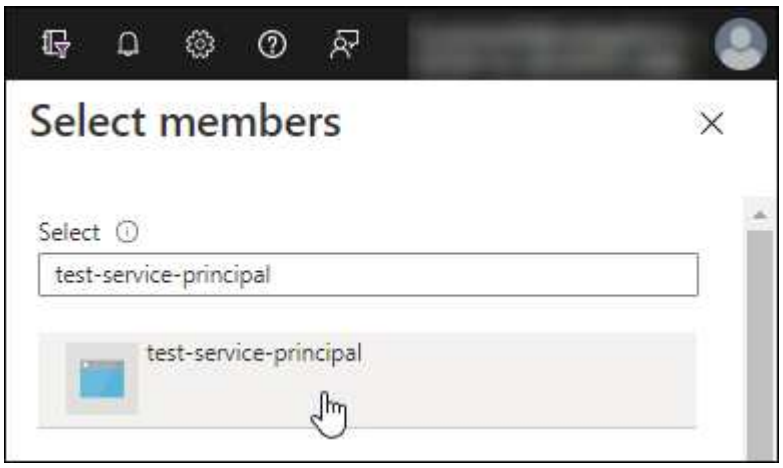
e. *メンバー*タブで、次の手順を実行します。

- *ユーザー、グループ、またはサービス プリンシパル*を選択したままにします。
- *メンバーを選択*を選択します。



- アプリケーションの名前を検索します。

  次に例を示します。



- アプリケーションを選択し、[選択] を選択します。
- *次へ*を選択します。

f. *レビュー + 割り当て*を選択します。

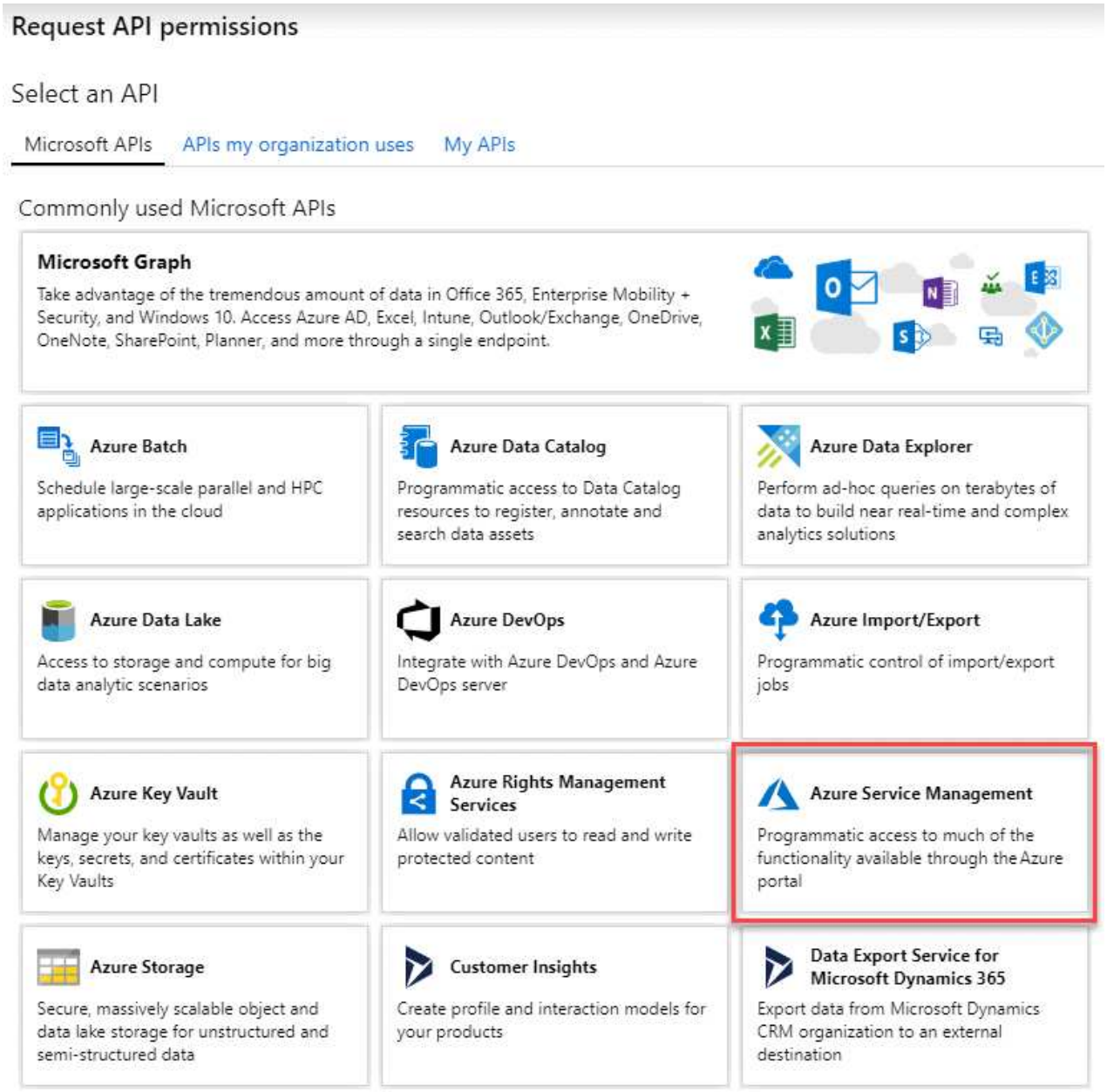
これで、サービス プリンシパルに、コンソール エージェントをデプロイするために必要な Azure アクセス許可が付与されました。

複数の Azure サブスクリプションからCloud Volumes ONTAPをデプロイする場合は、サービス プリンシパルを各サブスクリプションにバインドする必要があります。 NetApp Consoleでは、 Cloud Volumes ONTAP をデプロイするときに使用するサブスクリプションを選択できます。

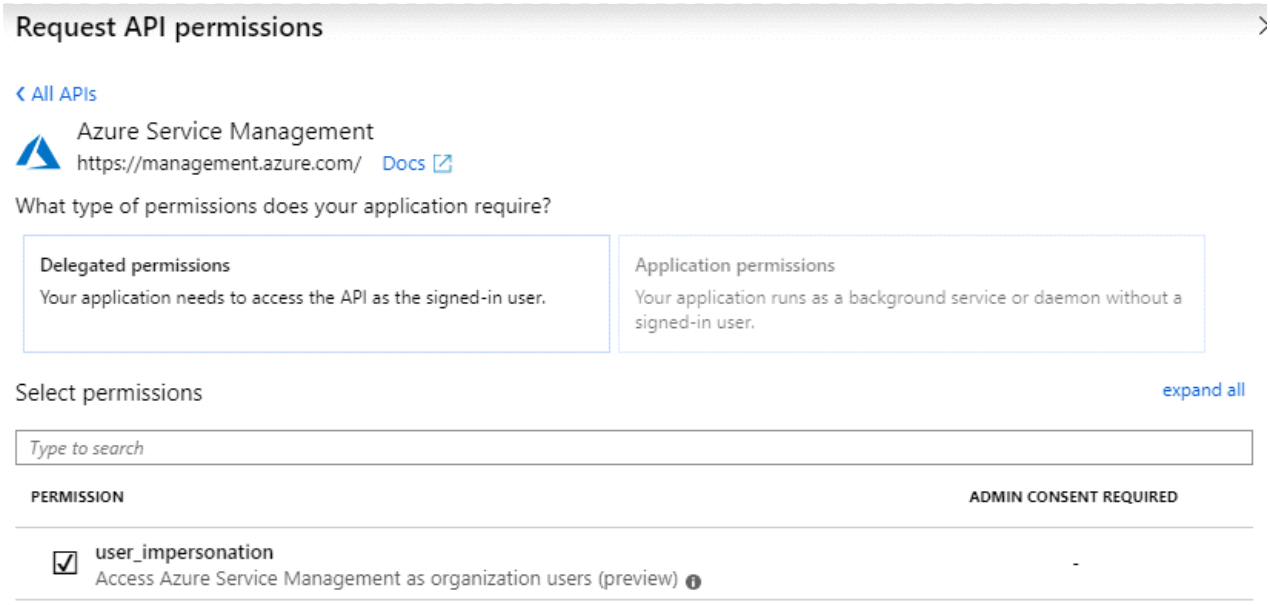
Windows Azure サービス管理 **API** 権限を追加する

1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. **API** 権限 **>** 権限の追加 を選択します。

3. **Microsoft API** の下で、**Azure Service Management** を選択します。

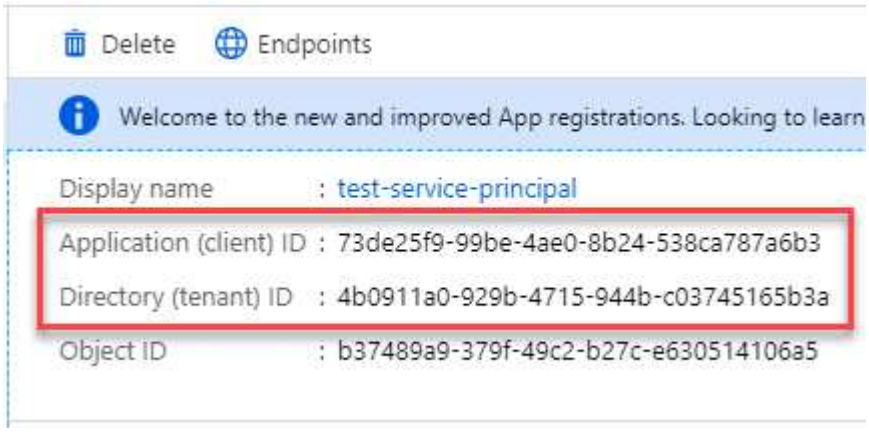


4. 組織ユーザーとして **Azure** サービス管理にアクセスする を選択し、権限の追加 を選択します。



アプリケーションのアプリケーション**ID**とディレクトリ**ID**を取得します

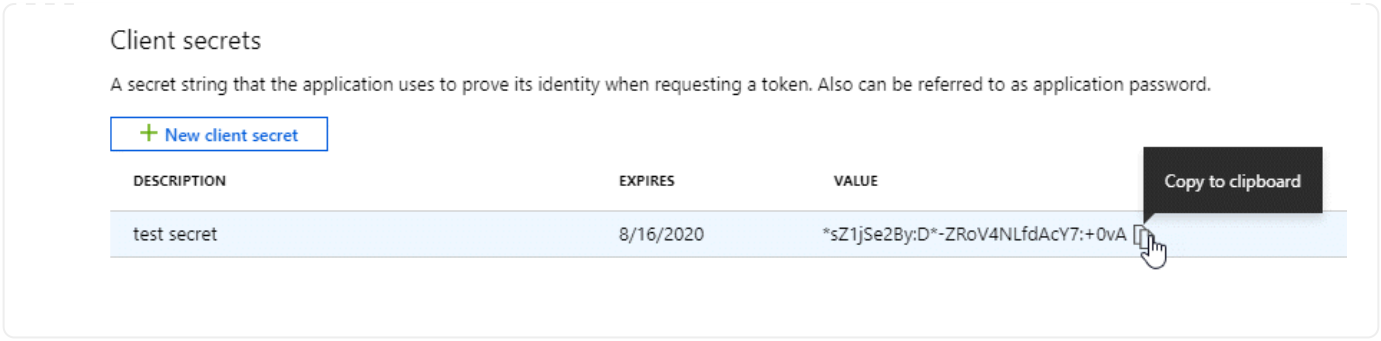
1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. アプリケーション **(**クライアント**) ID** と ディレクトリ **(**テナント**) ID** をコピーします。



Azure アカウントをコンソールに追加するときは、アプリケーションのアプリケーション (クライアント) ID とディレクトリ (テナント) ID を指定する必要があります。コンソールは ID を使用してプログラムでサインインします。

クライアントシークレットを作成する

1. **Microsoft Entra ID** サービスを開きます。
2. *アプリ登録*を選択し、アプリケーションを選択します。
3. *証明書とシークレット > 新しいクライアント シークレット*を選択します。
4. シークレットの説明と期間を指定します。
5. *追加*を選択します。
6. クライアント シークレットの値をコピーします。



コンソールエージェントを手動でインストールする

コンソール エージェントを手動でインストールする場合は、要件を満たすようにマシン環境を準備する必要があります。 Linux マシンが必要であり、Linux オペレーティング システムに応じて Podman または Docker をインストールする必要があります。

Podmanまたは**Docker Engine**をインストールする

オペレーティング システムに応じて、エージェントをインストールする前に Podman または Docker Engine のいずれかが必要になります。

- Red Hat Enterprise Linux 8 および 9 には Podman が必要です。

  サポートされているPodmanのバージョンを表示する 。

- Ubuntu には Docker Engine が必要です。

  サポートされている Docker エンジンのバージョンを表示する 。

例 **1.** 手順

ポッドマン

Podman をインストールして設定するには、次の手順に従います。

- podman.socket サービスを有効にして起動します
- Python3をインストールする
- podman-compose パッケージ バージョン 1.0.6 をインストールします。
- podman-composeをPATH環境変数に追加する
- Red Hat Enterprise Linux を使用している場合は、Podman バージョンが CNI ではなく Netavark Aardvark DNS を使用していることを確認してください。

DNS ポートの競合を避けるために、エージェントをインストールした後、aardvark-dns ポート (デフォルト: 53) を調整します。指示に従ってポートを構成します。

手順

1. ホストに podman-docker パッケージがインストールされている場合は削除します。

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Podman をインストールします。

   Podman は、公式の Red Hat Enterprise Linux リポジトリから入手できます。

   a. Red Hat Enterprise Linux 9.6 の場合:

   ```
   sudo dnf install podman-5:<version>
   ```

   <version> は、インストールする Podman のサポートされているバージョンです。サポートされているPodmanのバージョンを表示する 。

   b. Red Hat Enterprise Linux 9.1 から 9.4 の場合:

   ```
   sudo dnf install podman-4:<version>
   ```

   <version> は、インストールする Podman のサポートされているバージョンです。サポートされているPodmanのバージョンを表示する 。

   c. Red Hat Enterprise Linux 8 の場合:

   ```
   sudo dnf install podman-4:<version>
   ```

<version> は、インストールする Podman のサポートされているバージョンです。サポートされているPodmanのバージョンを表示する 。

3. podman.socket サービスを有効にして起動します。

```
sudo systemctl enable --now podman.socket
```

4. python3 をインストールします。

```
sudo dnf install python3
```

5. システムにまだインストールされていない場合は、EPEL リポジトリ パッケージをインストールします。

   podman-compose は、Extra Packages for Enterprise Linux (EPEL) リポジトリから入手できるため、この手順は必須です。

6. Red Hat Enterprise 9 を使用している場合:

   a. EPEL リポジトリ パッケージをインストールします。

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   +

   a. podman-compose パッケージ 1.5.0 をインストールします。

```
sudo dnf install podman-compose-1.5.0
```

7. Red Hat Enterprise Linux 8 を使用している場合:

   a. EPEL リポジトリ パッケージをインストールします。

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   b. podman-compose パッケージ 1.0.6 をインストールします。

```
sudo dnf install podman-compose-1.0.6
```

使用して `dnf install`コマンドは、PATH 環境変数に podman-compose を追加するための要件を満たしています。インストールコマンドは、すでにインストールされているpodman-composeを/usr/binに追加します。 `secure_path`ホスト上のオプション。

c. Red Hat Enterprise Linux 8 を使用している場合は、Podman バージョンが CNI ではなく Aardvark DNS を備えた NetAvark を使用していることを確認します。

i. 次のコマンドを実行して、networkBackend が CNI に設定されているかどうかを確認します。

```
podman info | grep networkBackend
```

ii. networkBackendが `CNI`、それを変更する必要があります `netavark`。

iii. インストール `netavark`そして `aardvark-dns`次のコマンドを使用します。

```
dnf install aardvark-dns netavark
```

iv. 開く `/etc/containers/containers.conf`ファイルを編集し、network_backend オプションを変更して、「cni」の代わりに「netavark」を使用します。

もし `/etc/containers/containers.conf`存在しない場合は、設定を変更してください `/usr/share/containers/containers.conf`。

v. podman を再起動します。

```
systemctl restart podman
```

vi. 次のコマンドを使用して、networkBackend が「netavark」に変更されていることを確認します。

```
podman info | grep networkBackend
```

Dockerエンジン

Docker のドキュメントに従って Docker Engine をインストールします。

手順

1. "Dockerからのインストール手順を見る"

   サポートされている Docker エンジン バージョンをインストールするには、手順に従ってください。最新バージョンはコンソールでサポートされていないため、インストールしないでください。

2. Docker が有効になっていて実行されていることを確認します。

```
sudo systemctl enable docker && sudo systemctl start docker
```

コンソールエージェントを手動でインストールする

オンプレミスの既存の Linux ホストにコンソール エージェント ソフトウェアをダウンロードしてインストールします。

開始する前に

次のものが必要です:

- コンソール エージェントをインストールするためのルート権限。
- コンソール エージェントからのインターネット アクセスにプロキシが必要な場合のプロキシ サーバーの詳細。

  インストール後にプロキシ サーバーを構成するオプションがありますが、これを行うにはコンソール エージェントを再起動する必要があります。

- プロキシ サーバーが HTTPS を使用する場合、またはプロキシがインターセプト プロキシである場合は、CA 署名証明書。

> コンソール エージェントを手動でインストールする場合、透過プロキシ サーバーの証明書を設定することはできません。透過プロキシ サーバーの証明書を設定する必要がある場合は、インストール後にメンテナンス コンソールを使用する必要があります。詳細はこちら "エージェントメンテナンスコンソール"。

タスク概要

インストール後、新しいバージョンが利用可能な場合、コンソール エージェントは自動的に更新されます。

手順

1. ホストに *http_proxy* または *https_proxy* システム変数が設定されている場合は、それらを削除します。

   ```
   unset http_proxy
   unset https_proxy
   ```

   これらのシステム変数を削除しないと、インストールは失敗します。

2. コンソール エージェント ソフトウェアをダウンロードし、Linux ホストにコピーします。 NetApp ConsoleまたはNetAppサポート サイトからダウンロードできます。

   - NetApp Console: エージェント > 管理 > エージェントのデプロイ > オンプレミス > 手動インストールに移動します。

     エージェント インストーラー ファイルのダウンロードまたはファイルへの URL を選択します。

ネットワークまたはクラウドで使用するための「オンライン」エージェント インストーラーをダウンロードします。NetApp Console エージェントには別の「オフライン」インストーラーが用意されていますが、プライベート モードの展開でのみサポートされます。

- NetAppサポート サイト (コンソールにまだアクセスできない場合に必要) "NetAppサポート サイト" 、

3. スクリプトを実行するための権限を割り当てます。

```
chmod +x NetApp_Console_Agent_Cloud_<version>
```

<version> は、ダウンロードしたコンソール エージェントのバージョンです。

4. Government Cloud 環境にインストールする場合は、構成チェックを無効にします。"手動インストールの構成チェックを無効にする方法を説明します。"
5. インストール スクリプトを実行します。

```
./NetApp_Console_Agent_Cloud_<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

ネットワークでインターネットアクセスにプロキシが必要な場合は、プロキシ情報を追加する必要があります。インストール中に明示的にプロキシを追加できます。 `--proxy`および `--cacert`パラメータはオプションであり、追加を要求されることはありません。明示的なプロキシ サーバがある場合は、示されているようにパラメータを入力する必要があります。

透過プロキシを設定する場合は、インストール後に設定できます。 "エージェントメンテナンスコンソールについて学ぶ"

+

CA 署名証明書を使用して明示的なプロキシ サーバーを構成する例を次に示します。

+

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert /tmp/cacert/certificate.cer
```

+
`--proxy` 次のいずれかの形式を使用して、Console エージェントが HTTP または HTTPS プロキシ サーバを使用するように設定します：

+ * http://address:port * http://user-name:password@address:port * http://domain-name%92user-name:password@address:port * https://address:port * https://user-name:password@address:port * https://domain-name%92user-name:password@address:port

+ 以下の点に注意してください：

+ ユーザーは、ローカル ユーザーまたはドメイン ユーザーにすることができます。 ドメイン ユーザーの場合は、上記のように \ の ASCII コードを使用する必要があります。 **Console** エージェントは、**@** 文字を含むユーザー名またはパスワードをサポートしていません。 パスワードに次の特殊文字が含まれている場合は、その特殊文字の前にバックスラッシュを付けてエスケープする必要があります：& または !

+ 例：

+ http://bxpproxyuser:netapp1\!@address:3128

1. Podman を使用した場合は、aardvark-dns ポートを調整する必要があります。

   a. コンソール エージェント仮想マシンに SSH で接続します。

   b. podman */usr/share/containers/containers.conf* ファイルを開き、Aardvark DNS サービス用に選択したポートを変更します。たとえば、54 に変更します。

      ```
      vi /usr/share/containers/containers.conf
      ```

      例えば：

   ```
   # Port to use for dns forwarding daemon with netavark in rootful bridge
   # mode and dns enabled.
   # Using an alternate port might be useful if other DNS services should
   # run on the machine.
   #
   dns_bind_port = 54
   ```

   a. コンソール エージェント仮想マシンを再起動します。

次は何？

NetApp Console内でコンソール エージェントを登録する必要があります。

NetApp Consoleにコンソールエージェントを登録する

コンソールにログインし、コンソール エージェントを組織に関連付けます。ログイン方法は、コンソールを使用しているモードによって異なります。コンソールを標準モードで使用している場合は、SaaS Web サイトからログインします。コンソールを制限モードまたはプライベート モードで使用している場合は、コンソール エージェント ホストからローカルにログインします。

手順

1. Web ブラウザを開き、コンソール エージェント ホストの URL を入力します。

   コンソール ホスト URL は、ホストの構成に応じて、ローカルホスト、プライベート IP アドレス、またはパブリック IP アドレスになります。たとえば、コンソール エージェントがパブリック IP アドレスのないパブリック クラウドにある場合は、コンソール エージェント ホストに接続しているホストのプライベート IP アドレスを入力する必要があります。

2. サインアップまたはログインしてください。

3. ログイン後、コンソールを設定します。
   a. コンソール エージェントに関連付けるコンソール組織を指定します。
   b. システムの名前を入力します。
   c. 安全な環境で実行していますか**?** の下で、制限モードを無効のままにします。

      コンソール エージェントがオンプレミスにインストールされている場合、制限モードはサポートされません。

   d. *始めましょう*を選択します。

NetApp Consoleにクラウドプロバイダーの資格情報を提供する

コンソール エージェントをインストールしてセットアップしたら、コンソール エージェントが AWS または Azure でアクションを実行するために必要な権限を持つように、クラウド資格情報を追加します。

AWS

開始する前に

これらの AWS 認証情報を作成したばかりの場合は、使用可能になるまでに数分かかることがあります。資格情報をコンソールに追加する前に、数分待ってください。

手順

1. *管理 > 資格情報*を選択します。
2. *組織の資格情報*を選択します。
3. *資格情報の追加*を選択し、ウィザードの手順に従います。
   a. 資格情報の場所: *Amazon Web Services > エージェントを選択します。
   b. 資格情報の定義: AWS アクセスキーとシークレットキーを入力します。
   c. マーケットプレイス サブスクリプション: 今すぐサブスクライブするか、既存のサブスクリプションを選択して、マーケットプレイス サブスクリプションをこれらの資格情報に関連付けます。
   d. 確認: 新しい資格情報の詳細を確認し、[追加] を選択します。

これで、 "NetApp Console"コンソール エージェントの使用を開始します。

Azure

開始する前に

これらの Azure 資格情報を作成したばかりの場合は、使用可能になるまでに数分かかることがあります。コンソール エージェントに資格情報を追加する前に、数分間お待ちください。

手順

1. *管理 > 資格情報*を選択します。
2. *資格情報の追加*を選択し、ウィザードの手順に従います。
   a. 資格情報の場所: **Microsoft Azure >** エージェント を選択します。
   b. 資格情報の定義: 必要な権限を付与する Microsoft Entra サービス プリンシパルに関する情報を入力します。
      - アプリケーション（クライアント）ID
      - ディレクトリ（テナント）ID
      - クライアントシークレット
   c. マーケットプレイス サブスクリプション: 今すぐサブスクライブするか、既存のサブスクリプションを選択して、マーケットプレイス サブスクリプションをこれらの資格情報に関連付けます。
   d. 確認: 新しい資格情報の詳細を確認し、[追加] を選択します。

結果

これで、コンソール エージェントには、ユーザーに代わって Azure でアクションを実行するために必要なアクセス許可が付与されました。これで、 "NetApp Console"コンソール エージェントの使用を開始します。

VCenter を使用してオンプレミスにコンソール エージェントをインストールする

VMWare ユーザーの場合は、OVA を使用して VCenter にコンソール エージェントをインストールできます。 OVA のダウンロードまたは URL は、NetApp Consoleから入手できます。

VCenter ツールと共にコンソール エージェントをインストールすると、VM Web コンソールを使用してメンテナンス タスクを実行できます。"エージェントの VM コンソールの詳細について説明します。"

コンソールエージェントのインストールの準備

インストールする前に、VM ホストが要件を満たしており、コンソール エージェントがインターネットおよび対象のネットワークにアクセスできることを確認してください。 NetAppデータ サービスまたはCloud Volumes ONTAP を使用するには、コンソール エージェントがユーザーに代わってアクションを実行できるように、クラウド プロバイダの資格情報を作成します。

コンソールエージェントホストの要件を確認する

コンソール エージェントをインストールする前に、ホスト マシンがインストール要件を満たしていることを確認してください。

- CPU: 8コアまたは8vCPU
- メモリ: 32 GB
- ディスク容量: 165 GB (シックプロビジョニング)
- vSphere 7.0以降
- ESXi ホスト 7.03 以上

エージェントを ESXi ホストに直接インストールするのではなく、vCenter 環境にインストールします。

コンソールエージェントのネットワークアクセスを設定する

ネットワーク管理者と協力して、コンソール エージェントが必要なエンドポイントへの送信アクセスと対象ネットワークへの接続を持っていることを確認します。

ターゲットネットワークへの接続

コンソール エージェントには、システムを作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムまたはストレージ システムを作成する予定のネットワークなどです。

アウトバウンドインターネットアクセス

コンソール エージェントを展開するネットワークの場所には、特定のエンドポイントに接続するための送信インターネット接続が必要です。

Webベースの**NetApp Console**を使用する際にコンピュータから接続されるエンドポイント

Web ブラウザからコンソールにアクセスするコンピュータは、複数のエンドポイントに接続できる必要があります。コンソール エージェントを設定し、コンソールを日常的に使用するには、コンソールを使用する必要があります。

"NetAppコンソールのネットワークを準備する" 。

コンソールエージェントから接続されたエンドポイント

コンソール エージェントは、日常業務でパブリック クラウド環境内のリソースとプロセスを管理するために、次のエンドポイントに接続するために、送信インターネット アクセスを必要とします。

以下にリストされているエンドポイントはすべて CNAME エントリです。

> オンプレミスにコンソール エージェントがインストールされている場合、Google Cloud のリソースを管理することはできません。 Google Cloud リソースを管理するには、Google Cloud にエージェントをインストールします。

AWS

コンソール エージェントをオンプレミスでインストールする場合、AWS に導入されたNetAppシステム (Cloud Volumes ONTAPなど) を管理するために、次の AWS エンドポイントへのネットワーク アクセスが必要です。

コンソールエージェントから接続されたエンドポイント

コンソール エージェントは、日常業務でパブリック クラウド環境内のリソースとプロセスを管理するために、次のエンドポイントに接続するために、送信インターネット アクセスを必要とします。

以下にリストされているエンドポイントはすべて CNAME エントリです。

エンドポイント	目的
AWS サービス (amazonaws.com): • クラウドフォーメーション • エラスティックコンピューティングクラウド (EC2) • アイデンティティとアクセス管理（IAM） • キー管理サービス (KMS) • セキュリティトークンサービス（STS） • シンプルストレージサービス（S3）	AWS リソースを管理します。エンドポイントは AWS リージョンによって異なります。 "詳細についてはAWSドキュメントを参照してください"
NetApp ONTAP用の Amazon FsX: • api.workloads.netapp.com	Web ベースのコンソールは、このエンドポイントに接続して Workload Factory API と対話し、FSx for ONTAPベースのワークロードを管理および操作します。
https://mysupport.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信します。
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェアアップデートを受信します。

エンドポイント	目的
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、NetApp、ファイアウォールルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

Azure

コンソール エージェントがオンプレミスにインストールされている場合、Azure にデプロイされたNetAppシステム (Cloud Volumes ONTAPなど) を管理するために、次の Azure エンドポイントへのネットワーク アクセスが必要です。

エンドポイント	目的
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Azure パブリック リージョン内のリソースを管理します。
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Azure China リージョンのリソースを管理します。

エンドポイント	目的
https://mysupport.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信します。
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェアアップデートを受信します。
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、NetApp、ファイアウォールルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

プロキシ サーバ

NetApp は明示的プロキシ構成と透過的プロキシ構成の両方をサポートしています。透過プロキシを使用している場合は、プロキシ サーバーの証明書のみを提供する必要があります。明示的なプロキシを使用している場合は、IP アドレスと資格情報も必要になります。

- IPアドレス
- Credentials
- HTTPS証明書

ポート

ユーザーが開始した場合、またはCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用された場合を除いて、コンソール エージェントへの着信トラフィックはありません。

- HTTP (80) と HTTPS (443) は、まれにしか使用されないローカル UI へのアクセスを提供します。
- SSH（22）は、トラブルシューティングのためにホストに接続する必要がある場合にのみ必要です。
- アウトバウンド インターネット接続が利用できないサブネットにCloud Volumes ONTAPシステムを展開する場合は、ポート 3128 経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムにAutoSupportメッセージを送信するためのアウトバウンド インターネット接続がない場合、コンソールは、コンソール エージェントに含まれているプロキシ サーバーを使用するようにそれらのシステムを自動的に構成します。唯一の要件は、コンソール エージェントのセキュリティ グループがポート 3128 経由の受信接続を許可していることを確認することです。コンソール エージェントを展開した後、このポートを開く必要があります。

NTP を有効にする

NetApp Data Classificationを使用して企業のデータ ソースをスキャンする予定の場合は、システム間で時刻が同期されるように、コンソール エージェントとNetApp Data Classificationシステムの両方で Network Time Protocol (NTP) サービスを有効にする必要があります。 "NetAppデータ分類の詳細"

AWS または **Azure** のコンソール エージェント クラウド権限を作成する

オンプレミスのコンソールエージェントを使用して AWS または Azure のNetAppデータ サービスを使用する場合は、インストール後にコンソールエージェントに資格情報を追加できるように、クラウド プロバイダーで権限を設定する必要があります。

オンプレミスにコンソール エージェントがインストールされている場合、Google Cloud のリソースを管理することはできません。 Google Cloud リソースを管理するには、Google Cloud にエージェントをインストールする必要があります。

AWS

オンプレミスのコンソールエージェントの場合は、IAM ユーザーアクセスキーを追加して AWS 権限を付与します。

オンプレミスのコンソール エージェントには IAM ユーザー アクセス キーを使用します。オンプレミスのコンソール エージェントでは IAM ロールはサポートされていません。

手順

1. AWS コンソールにログインし、IAM サービスに移動します。
2. ポリシーを作成します。

   a. *ポリシー > ポリシーの作成*を選択します。

   b. *JSON*を選択し、その内容をコピーして貼り付けます。"コンソールエージェントのIAMポリシー" 。

   c. 残りの手順を完了してポリシーを作成します。

      使用する予定のNetAppデータ サービスによっては、2 番目のポリシーを作成する必要がある場合があります。

   標準リージョンの場合、権限は 2 つのポリシーに分散されます。 AWS の管理ポリシーの最大文字サイズ制限により、2 つのポリシーが必要になります。"コンソールエージェントのIAMポリシーの詳細" 。

3. IAM ユーザーにポリシーをアタッチします。
   - "AWSドキュメント: IAMロールの作成"
   - "AWSドキュメント: IAMポリシーの追加と削除"
4. コンソール エージェントをインストールした後、 NetApp Consoleに追加できるアクセス キーがユーザーにあることを確認します。

結果

これで、必要な権限を持つ IAM ユーザー アクセス キーを取得できるはずです。コンソール エージェントをインストールした後、コンソールからこれらの認証情報をコンソール エージェントに関連付けます。

Azure

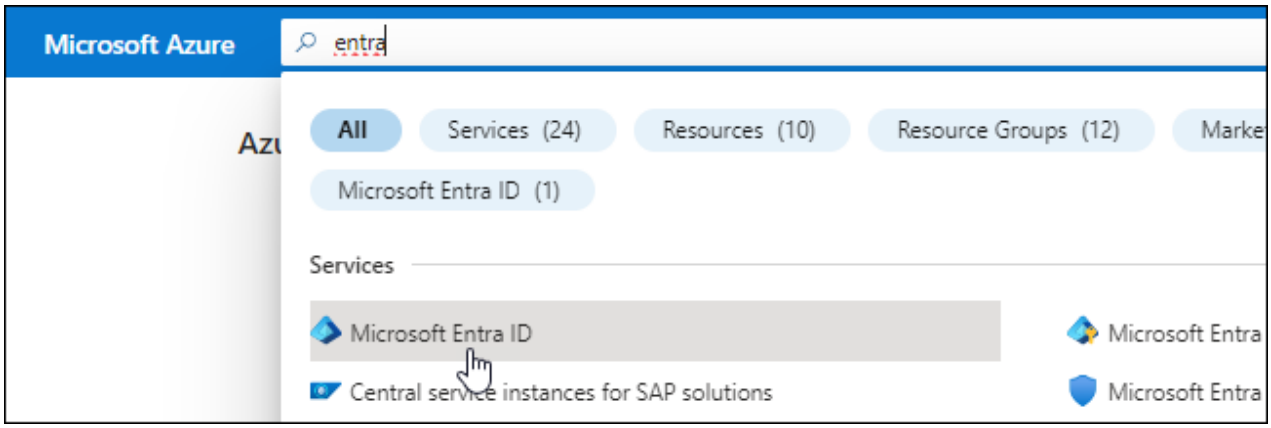
コンソール エージェントがオンプレミスでインストールされている場合は、Microsoft Entra ID でサービス プリンシパルを設定し、コンソール エージェントに必要な Azure 資格情報を取得して、コンソール エージェントに Azure 権限を付与する必要があります。

ロールベースのアクセス制御用の **Microsoft Entra** アプリケーションを作成する

1. Azure で Active Directory アプリケーションを作成し、そのアプリケーションをロールに割り当てるためのアクセス許可があることを確認します。

   詳細については、 "Microsoft Azure ドキュメント: 必要な権限"

2. Azure ポータルから、**Microsoft Entra ID** サービスを開きます。



3. メニューで*アプリ登録*を選択します。
4. *新規登録*を選択します。
5. アプリケーションの詳細を指定します。
   - 名前: アプリケーションの名前を入力します。
   - アカウント タイプ: アカウント タイプを選択します (いずれのタイプもNetApp Consoleで使用できます)。
   - リダイレクト **URI**: このフィールドは空白のままにすることができます。
6. *登録*を選択します。

AD アプリケーションとサービス プリンシパルを作成しました。

アプリケーションをロールに割り当てる

1. カスタム ロールを作成します。

   Azure ポータル、Azure PowerShell、Azure CLI、または REST API を使用して、Azure カスタム ロールを作成できます。次の手順は、Azure CLI を使用してロールを作成する方法を示しています。別の方法をご希望の場合は、 "Azureドキュメント"

   a. の内容をコピーします"コンソールエージェントのカスタムロール権限"JSON ファイルに保存します。
   b. 割り当て可能なスコープに Azure サブスクリプション ID を追加して、JSON ファイルを変更します。

      ユーザーがCloud Volumes ONTAPシステムを作成する各 Azure サブスクリプションの ID を追加する必要があります。

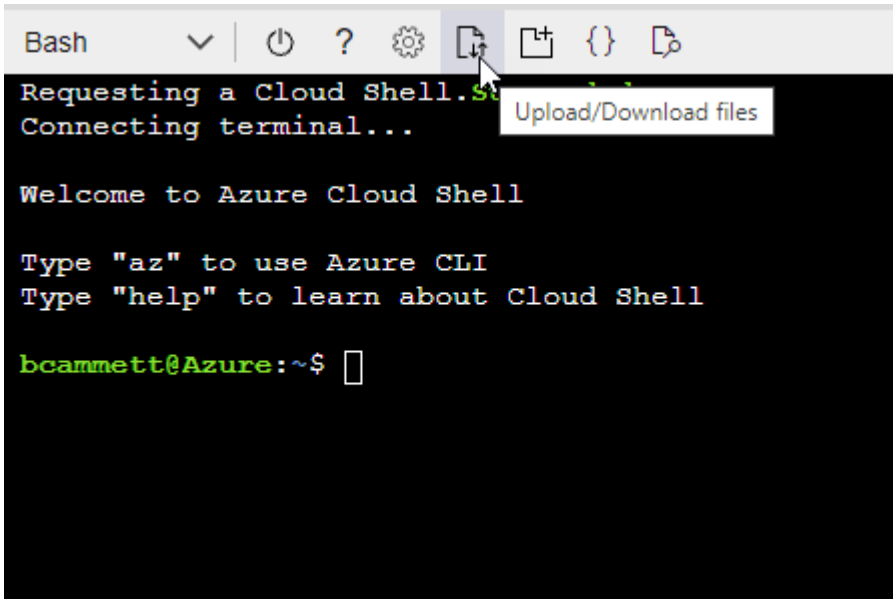
      例

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
]
```

c. JSON ファイルを使用して、Azure でカスタム ロールを作成します。

次の手順では、Azure Cloud Shell で Bash を使用してロールを作成する方法について説明します。

- 始める "Azure クラウド シェル"Bash 環境を選択します。
- JSON ファイルをアップロードします。



- Azure CLI を使用してカスタム ロールを作成します。

```
az role definition create --role-definition agent_Policy.json
```

これで、コンソール エージェント仮想マシンに割り当てることができる、コンソール オペレーターと呼ばれるカスタム ロールが作成されます。

2. アプリケーションをロールに割り当てます。

a. Azure ポータルから、サブスクリプション サービスを開きます。

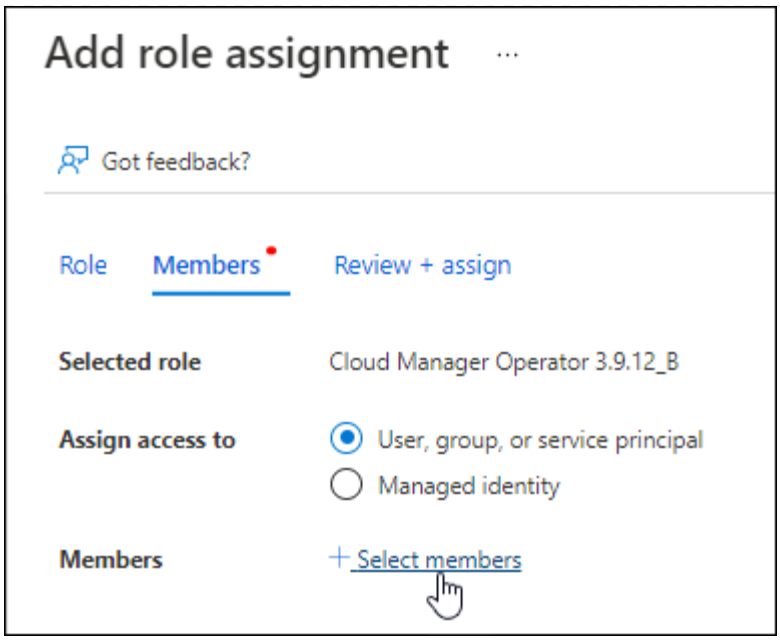
b. サブスクリプションを選択します。

c. アクセス制御 **(IAM) >** 追加 **>** ロール割り当ての追加 を選択します。

d. *役割*タブで、*コンソールオペレーター*役割を選択し、*次へ*を選択します。

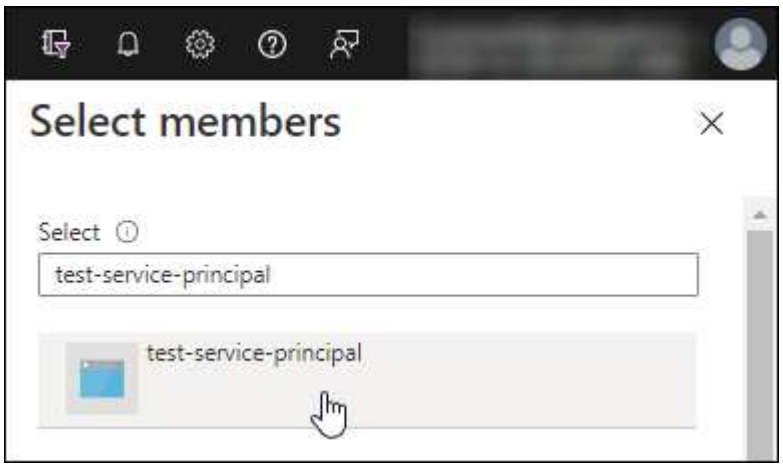
e. *メンバー*タブで、次の手順を実行します。

- *ユーザー、グループ、またはサービス プリンシパル*を選択したままにします。
- *メンバーを選択*を選択します。



- アプリケーションの名前を検索します。

  次に例を示します。



- アプリケーションを選択し、[選択] を選択します。
- *次へ*を選択します。

f. *レビュー + 割り当て*を選択します。

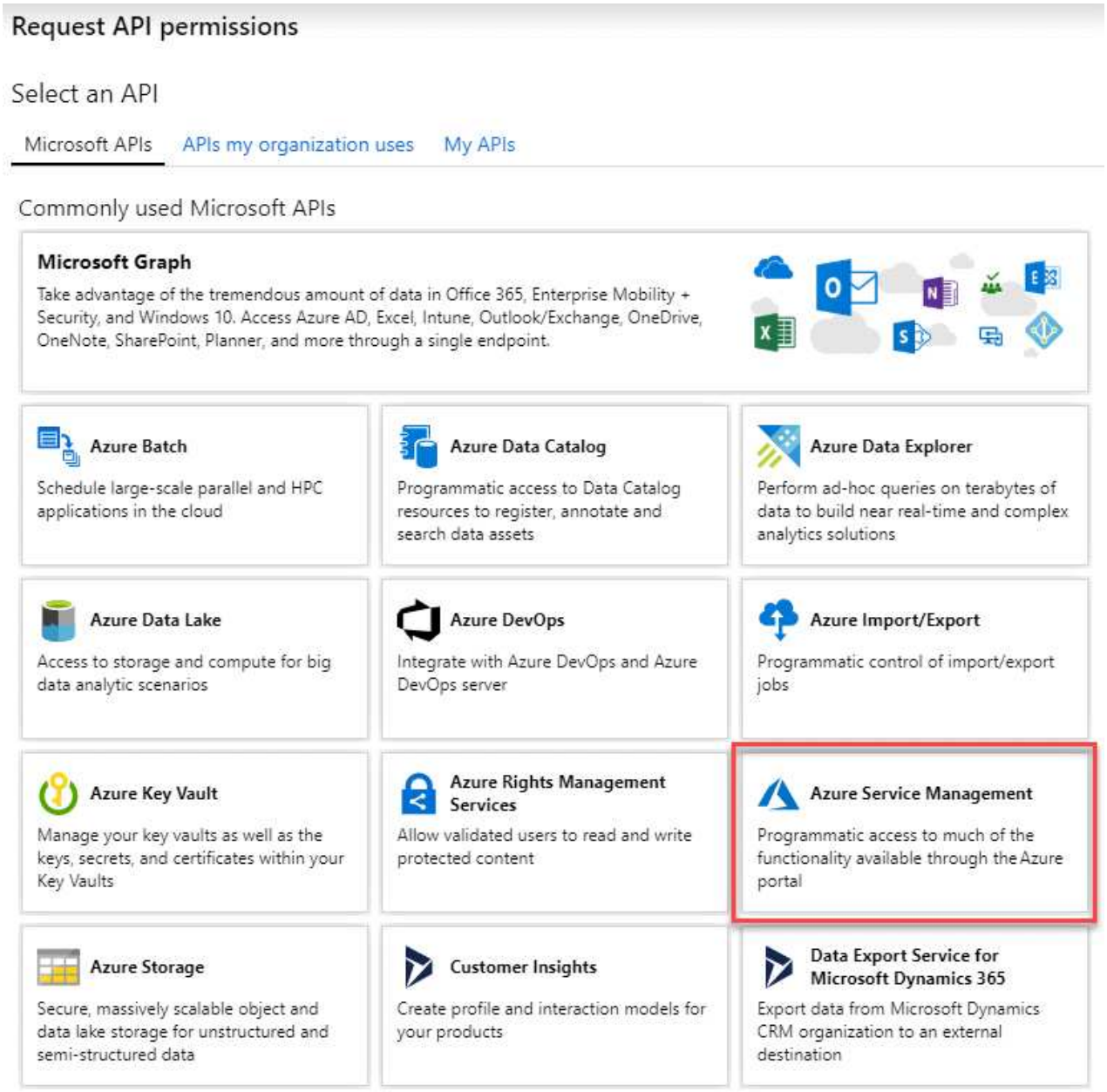
これで、サービス プリンシパルに、コンソール エージェントをデプロイするために必要な Azure アクセス許可が付与されました。

複数の Azure サブスクリプションからCloud Volumes ONTAPをデプロイする場合は、サービス プリンシパルを各サブスクリプションにバインドする必要があります。 NetApp Consoleでは、 Cloud Volumes ONTAP をデプロイするときに使用するサブスクリプションを選択できます。

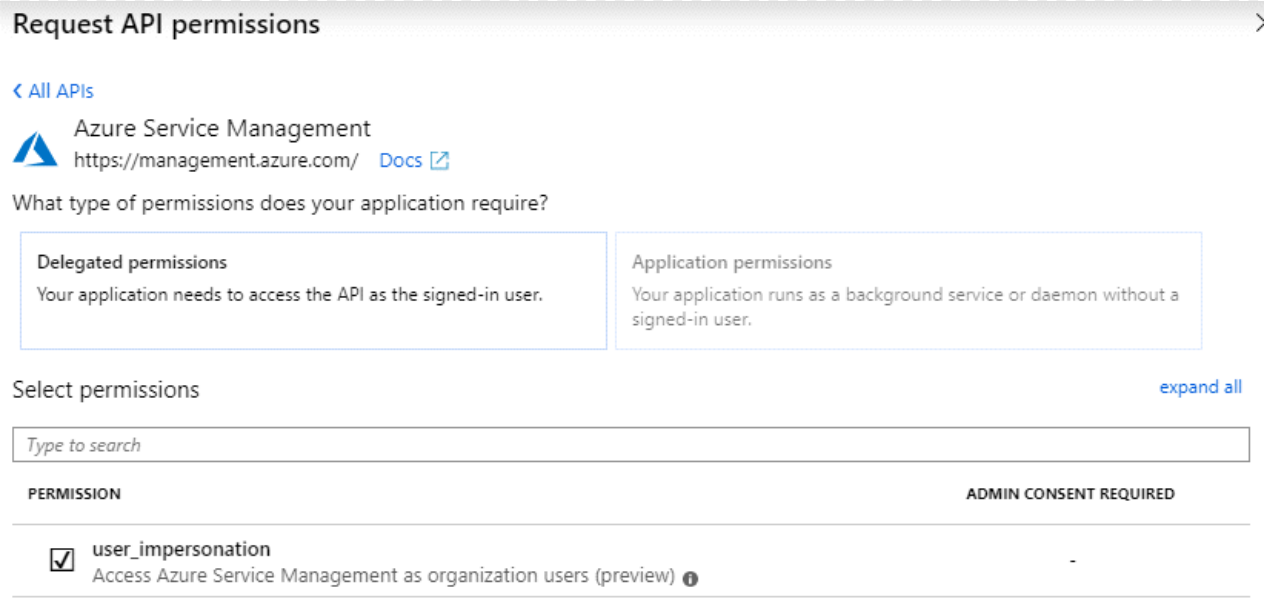
Windows Azure サービス管理 **API** 権限を追加する

1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. **API** 権限 **>** 権限の追加 を選択します。

3. **Microsoft API** の下で、**Azure Service Management** を選択します。

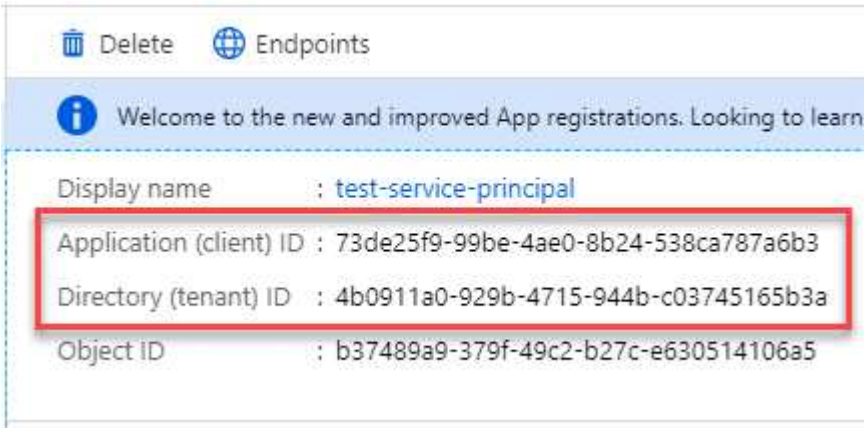


4. 組織ユーザーとして **Azure** サービス管理にアクセスする を選択し、権限の追加 を選択します。



アプリケーションのアプリケーション**ID**とディレクトリ**ID**を取得します

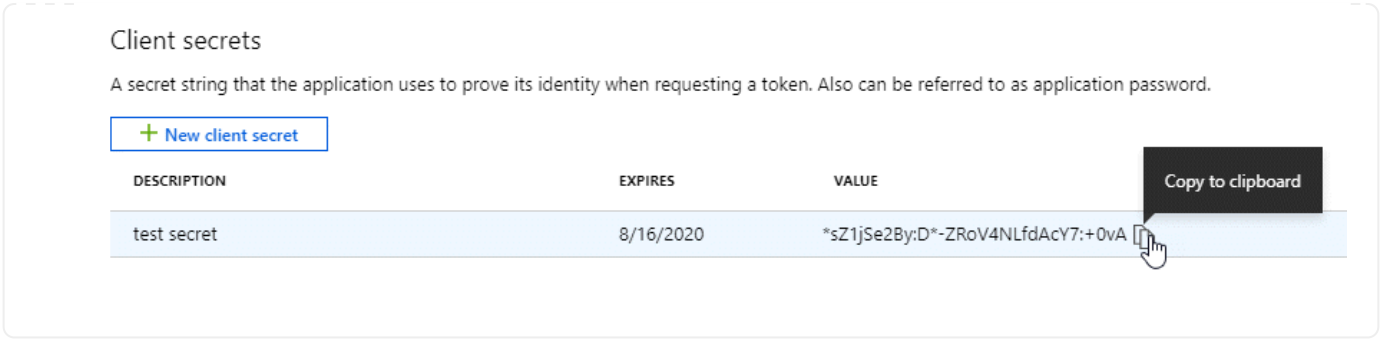
1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. アプリケーション **(**クライアント**) ID** と ディレクトリ **(**テナント**) ID** をコピーします。



Azure アカウントをコンソールに追加するときは、アプリケーションのアプリケーション (クライアント) ID とディレクトリ (テナント) ID を指定する必要があります。コンソールは ID を使用してプログラムでサインインします。

クライアントシークレットを作成する

1. **Microsoft Entra ID** サービスを開きます。
2. *アプリ登録*を選択し、アプリケーションを選択します。
3. *証明書とシークレット > 新しいクライアント シークレット*を選択します。
4. シークレットの説明と期間を指定します。
5. *追加*を選択します。
6. クライアント シークレットの値をコピーします。



VCenter環境にコンソールエージェントをインストールする

NetApp は、VCenter 環境へのコンソール エージェントのインストールをサポートしています。 OVA ファイルには、VMware 環境に展開できる事前構成済みの VM イメージが含まれています。ファイルのダウンロードまたは URL の展開は、 NetApp Consoleから直接行えます。コンソール エージェント ソフトウェアと自己署名証明書が含まれています。

OVAをダウンロードするかURLをコピーしてください

OVA をダウンロードするか、 NetApp Consoleから OVA URL を直接コピーします。

1. *管理 > エージェント*を選択します。
2. *概要*ページで、*エージェントのデプロイ > オンプレミス*を選択します。
3. *OVA付き*を選択してください。
4. OVA をダウンロードするか、VCenter で使用する URL をコピーするかを選択します。

VCenterにエージェントを展開する

エージェントを展開するには、VCenter 環境にログインします。

手順

1. 環境で必要な場合は、自己署名証明書を信頼できる証明書にアップロードします。インストール後にこの証明書を置き換えます。"自己署名証明書を置き換える方法を学びます。"
2. コンテンツ ライブラリまたはローカル システムから OVA を展開します。

ローカルシステムから	コンテンツライブラリから
a. 右クリックして、[OVF テンプレートのデプロイ…] を選択します。b. URL から OVA ファイルを選択するか、その場所を参照して、[次へ] を選択します。	a. コンテンツライブラリに移動し、コンソールエージェントOVAを選択します。b. アクション > *このテンプレートから新しいVM*を選択します。

3. OVF テンプレートのデプロイ ウィザードを完了して、コンソール エージェントをデプロイします。
4. VM の名前とフォルダーを選択し、[次へ] を選択します。
5. コンピューティング リソースを選択し、[次へ] を選択します。
6. テンプレートの詳細を確認し、[次へ] を選択します。
7. ライセンス契約に同意し、[次へ] を選択します。

8. 使用するプロキシ構成のタイプ（明示的プロキシ、透過プロキシ、またはプロキシなし）を選択します。
9. VM を展開するデータストアを選択し、[次へ] を選択します。ホストの要件を満たしていることを確認してください。
10. VM を接続するネットワークを選択し、[次へ] を選択します。ネットワークが IPv4 であり、必要なエンドポイントへのアウトバウンド インターネット アクセスできることを確認します。
11. *テンプレートのカスタマイズ*ウィンドウで、次のフィールドに入力します。
    - プロキシ情報
      - 明示的なプロキシを選択した場合は、プロキシ サーバーのホスト名または IP アドレスとポート番号、およびユーザー名とパスワードを入力します。
      - 透過プロキシを選択した場合は、それぞれの証明書をアップロードします。
    - 仮想マシンの構成
      - 構成チェックをスキップ: このチェックボックスはデフォルトでオフになっており、エージェントはネットワーク アクセスを検証するために構成チェックを実行します。
        - NetApp、インストールにエージェントの構成チェックが含まれるように、このボックスをオフのままにしておくことを推奨しています。構成チェックでは、エージェントが必要なエンドポイントへのネットワーク アクセス権を持っているかどうかを検証します。接続の問題によりデプロイメントが失敗した場合は、エージェント ホストから検証レポートとログにアクセスできます。場合によっては、エージェントがネットワークにアクセスできることが確実な場合は、チェックをスキップすることもできます。例えば、まだ"以前のエンドポイント"エージェントのアップグレードに使用すると、検証が失敗し、エラーが発生します。これを回避するには、検証チェックなしでインストールするためのチェックボックスをオンにします。"エンドポイントリストを更新する方法を学ぶ" 。
      - メンテナンスパスワード: `maint`エージェントメンテナンスコンソールへのアクセスを許可するユーザー。
      - **NTP** サーバー: 時刻同期用の 1 つ以上の NTP サーバーを指定します。
      - ホスト名: この VM のホスト名を設定します。検索ドメインを含めることはできません。たとえば、console10.searchdomain.company.com の FQDN は console10 と入力する必要があります。
      - プライマリ **DNS**: 名前解決に使用するプライマリ DNS サーバーを指定します。
      - セカンダリ **DNS**: 名前解決に使用するセカンダリ DNS サーバーを指定します。
      - 検索ドメイン: ホスト名を解決するときに使用する検索ドメイン名を指定します。たとえば、FQDN が console10.searchdomain.company.com の場合は、searchdomain.company.com と入力します。
      - **IPv4** アドレス: ホスト名にマッピングされる IP アドレス。
      - **IPv4** サブネット マスク: IPv4 アドレスのサブネット マスク。
      - **IPv4** ゲートウェイ アドレス: IPv4 アドレスのゲートウェイ アドレス。
12. *次へ*を選択します。
13. *完了準備完了*ウィンドウで詳細を確認し、*完了*を選択します。

    vSphere タスク バーには、コンソール エージェントの展開の進行状況が表示されます。
14. VMの電源をオンにします。

デプロイメントが失敗した場合は、エージェント ホストから検証レポートとログにアクセスできます。"インストールの問題をトラブルシューティングする方法を学びます。"

NetApp Consoleにコンソールエージェントを登録する

コンソールにログインし、コンソール エージェントを組織に関連付けます。ログイン方法は、コンソールを使用しているモードによって異なります。コンソールを標準モードで使用している場合は、SaaS Web サイトからログインします。コンソールを制限モードまたはプライベート モードで使用している場合は、コンソール エージェント ホストからローカルにログインします。

手順

1. Web ブラウザを開き、コンソール エージェント ホストの URL を入力します。

   コンソール ホスト URL は、ホストの構成に応じて、ローカルホスト、プライベート IP アドレス、またはパブリック IP アドレスになります。たとえば、コンソール エージェントがパブリック IP アドレスのないパブリック クラウドにある場合は、コンソール エージェント ホストに接続しているホストのプライベート IP アドレスを入力する必要があります。

2. サインアップまたはログインしてください。
3. ログイン後、コンソールを設定します。
   a. コンソール エージェントに関連付けるコンソール組織を指定します。
   b. システムの名前を入力します。
   c. 安全な環境で実行していますか**?** の下で、制限モードを無効のままにします。

      コンソール エージェントがオンプレミスにインストールされている場合、制限モードはサポートされません。

   d. *始めましょう*を選択します。

コンソールにクラウドプロバイダーの資格情報を追加する

コンソール エージェントをインストールしてセットアップしたら、コンソール エージェントが AWS または Azure でアクションを実行するために必要な権限を持つように、クラウド資格情報を追加します。

AWS

開始する前に

これらの AWS 認証情報を作成したばかりの場合は、使用可能になるまでに数分かかることがあります。資格情報をコンソールに追加する前に、数分待ってください。

手順

1. *管理 > 資格情報*を選択します。
2. *組織の資格情報*を選択します。
3. *資格情報の追加*を選択し、ウィザードの手順に従います。
   a. 資格情報の場所: *Amazon Web Services > エージェントを選択します。
   b. 資格情報の定義: AWS アクセスキーとシークレットキーを入力します。
   c. マーケットプレイス サブスクリプション: 今すぐサブスクライブするか、既存のサブスクリプションを選択して、マーケットプレイス サブスクリプションをこれらの資格情報に関連付けます。
   d. 確認: 新しい資格情報の詳細を確認し、[追加] を選択します。

これで、 "NetApp Console"コンソール エージェントの使用を開始します。

Azure

開始する前に

これらの Azure 資格情報を作成したばかりの場合は、使用可能になるまでに数分かかることがあります。コンソール エージェントに資格情報を追加する前に、数分間お待ちください。

手順

1. *管理 > 資格情報*を選択します。
2. *資格情報の追加*を選択し、ウィザードの手順に従います。
   a. 資格情報の場所: **Microsoft Azure >** エージェント を選択します。
   b. 資格情報の定義: 必要な権限を付与する Microsoft Entra サービス プリンシパルに関する情報を入力します。
      - アプリケーション（クライアント）ID
      - ディレクトリ（テナント）ID
      - クライアントシークレット
   c. マーケットプレイス サブスクリプション: 今すぐサブスクライブするか、既存のサブスクリプションを選択して、マーケットプレイス サブスクリプションをこれらの資格情報に関連付けます。
   d. 確認: 新しい資格情報の詳細を確認し、[追加] を選択します。

結果

これで、コンソール エージェントに、ユーザーに代わって Azure でアクションを実行するために必要なアクセス許可が付与されました。これで、 "NetApp Console"コンソール エージェントの使用を開始します。

オンプレミスのコンソールエージェントのポート

コンソール エージェントは、オンプレミスの Linux ホストに手動でインストールされる場合、受信 ポートを使用します。計画の際にはこれらのポートを参照してください。

これらの受信ルールは、すべてのNetApp Console展開モードに適用されます。

プロトコル	ポート	目的
HTTP	80	• クライアントのWebブラウザからローカルユーザーインターフェースへのHTTPアクセスを提供します • Cloud Volumes ONTAPのアップグレードプロセス中に使用されます
HTTPS	443	クライアントのWebブラウザからローカルユーザーインターフェースへのHTTPSアクセスを提供します

著作権に関する情報

商標に関する情報