NetApp Consoleの使用を開始する (制限モード)

NetApp Console setup and administration

NetApp
February 11, 2026

目次

NetApp Consoleの使用を開始する (制限モード)

開始ワークフロー（制限モード）

環境を準備し、コンソール エージェントを展開して、制限モードでNetApp Consoleの使用を開始します。

制限モードは通常、AWS GovCloud および Azure Government リージョンでの展開を含む、州政府や地方自治体、規制対象企業によって使用されます。始める前に、以下の点を理解しておいてください。"コンソール エージェント"そして"展開モード"。

"展開の準備"

1. CPU、RAM、ディスク容量、コンテナ オーケストレーション ツールなどの要件を満たす専用の Linux ホストを準備します。
2. ターゲット ネットワークへのアクセス、手動インストール用のアウトバウンド インターネット アクセス、および日常的なアクセス用のアウトバウンド インターネットを提供するネットワークをセットアップします。
3. クラウド プロバイダーで権限を設定し、展開後にそれらの権限をコンソール エージェント インスタンスに関連付けることができるようにします。

"コンソールエージェントを展開する"

1. クラウド プロバイダーのマーケットプレイスからコンソール エージェントをインストールするか、独自の Linux ホストにソフトウェアを手動でインストールします。
2. Web ブラウザを開き、Linux ホストの IP アドレスを入力して、 NetApp Consoleを設定します。
3. 以前に設定した権限をコンソール エージェントに提供します。

"NetApp Intelligent Servicesに加入する（オプション）"

オプション: クラウド プロバイダーのマーケットプレイスからNetApp Intelligent Servicesにサブスクライブして、時間単位の料金 (PAYGO) または年間契約でデータ サービスの料金を支払います。 NetApp Intelligent Servicesには、 NetApp Backup and Recovery、 Cloud Volumes ONTAP、 NetApp Cloud Tiering、 NetApp Ransomware Resilience 、 NetApp Disaster Recovery が含まれます。 NetApp Data Classification は追加料金なしでサブスクリプションに含まれています。

制限モードでの展開の準備

NetApp Consoleを制限モードで展開する前に、環境を準備します。ホストの要件を確認し、ネットワークを準備し、権限を設定するなどする必要があります。

ステップ**1:** 制限モードの仕組みを理解する

開始する前に、 NetApp Consoleが制限モードでどのように動作するかを理解してください。

インストールされたNetApp Consoleエージェントからローカルで利用できるブラウザベースのインターフェイスを使用します。 SaaS レイヤーを通じて提供される Web ベースのコンソールからNetApp Consoleにアクセスすることはできません。

また、すべてのコンソール機能とNetAppデータ サービスが利用できるわけではありません。

"制限モードの仕組みを学ぶ" 。

ステップ2: インストールオプションを確認する

制限モードでは、コンソール エージェントをクラウドにのみインストールできます。次のインストール オプションが利用可能です。

- AWSマーケットプレイスから
- Azure Marketplaceから
- AWS、Azure、または Google Cloud で実行されている独自の Linux ホストにコンソール エージェントを手動でインストールする

ステップ3: ホストの要件を確認する

コンソール エージェントを実行するには、ホストが特定の OS、RAM、およびポートの要件を満たしている必要があります。

AWS または Azure Marketplace からコンソールエージェントをデプロイする場合、イメージには必要な OS およびソフトウェア コンポーネントが含まれます。 CPU と RAM の要件を満たすインスタンス タイプを選択するだけです。

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。

AWS EC2インスタンスタイプ

CPU と RAM の要件を満たすインスタンス タイプ。 NetAppt3.2xlarge を推奨します。

Azure VM サイズ

CPU と RAM の要件を満たすインスタンス タイプ。 NetAppStandard_D8s_v3 を推奨します。

Google Cloud マシンタイプ

CPU と RAM の要件を満たすインスタンス タイプ。NetAppn2-standard-8 を推奨しています。

コンソールエージェントは、Google Cloud の VM インスタンスで、以下の OS がサポートする環境でサポートされます。 "シールドされたVMの機能"

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

ステップ4: PodmanまたはDocker Engineをインストールする

コンソール エージェントを手動でインストールするには、Podman または Docker Engine をインストールしてホストを準備します。

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
```

ステップ5: ネットワークアクセスを準備する

コンソール エージェントがパブリック クラウド内の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。コンソール エージェント用の仮想ネットワークとサブネットがあることに加えて、次の要件が満たされていることを確認する必要があります。

ターゲットネットワークへの接続

コンソール エージェントがストレージの場所へのネットワーク接続を持っていることを確認します。たとえば、 Cloud Volumes ONTAPをデプロイする予定の VPC または VNet、またはオンプレミスのONTAPクラスターが存在するデータセンターなどです。

NetApp Consoleへのユーザーアクセスのためのネットワークを準備する

制限モードでは、ユーザーはコンソール エージェント VM からコンソールにアクセスします。コンソール エージェントは、データ管理タスクを完了するためにいくつかのエンドポイントに接続します。これらのエンドポイントは、コンソールから特定のアクションを完了するときに、ユーザーのコンピューターから接続されます。

バージョン 4.0.0 より前のコンソール エージェントには追加のエンドポイントが必要です。4.0.0 以降にアップグレードした場合は、許可リストから古いエンドポイントを削除できます。"4.0.0 より前のバージョンに必要なネットワーク アクセスの詳細について説明します。"

+

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.bluexp.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。
https://cdn.auth0.com https://services.cloud.netapp.com	Web ブラウザはこれらのエンドポイントに接続し、NetApp Consoleを通じて集中的なユーザー認証を行います。

日常業務のためのアウトバウンドインターネットアクセス

コンソール エージェントのネットワークの場所には、送信インターネット アクセスが必要です。 NetApp Consoleの SaaS サービスと、それぞれのパブリック クラウド環境内のエンドポイントにアクセスできる必要があります。

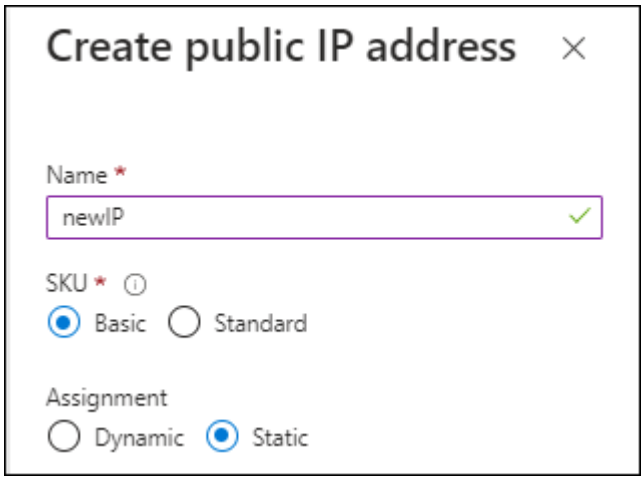
エンドポイント	目的
AWS 環境	AWS サービス (amazonaws.com): • クラウドフォーメーション • エラスティックコンピューティングクラウド (EC2) • アイデンティティとアクセス管理（IAM） • キー管理サービス (KMS) • セキュリティトークンサービス（STS） • シンプルストレージサービス（S3）
AWS リソースを管理します。エンドポイントは AWS リージョンによって異なります。 "詳細についてはAWSドキュメントを参照してください"	NetApp ONTAP用の Amazon FsX: • api.workloads.netapp.com
Web 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。	**Azure** 環境
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.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	Azure Government 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
Google Cloud 環境	https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://config.googleapis.com/v1/projects
Google Cloud 内のリソースを管理します。	• NetApp Consoleエンドポイント*
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.bluexp.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。

エンドポイント	目的
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のパブリック**IP**アドレス

Azure のコンソール エージェント VM でパブリック IP アドレスを使用する場合は、コンソールがこのパブリック IP アドレスを使用するように、IP アドレスで Basic SKU を使用する必要があります。



代わりに標準 SKU IP アドレスを使用する場合、コンソールはパブリック IP ではなく、コンソール エージェントのプライベート IP アドレスを使用します。コンソールにアクセスするために使用しているマシンがそのプライベート IP アドレスにアクセスできない場合、コンソールからのアクションは失敗します。

"Azure ドキュメント: パブリック IP SKU"

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"

クラウド プロバイダーのマーケットプレイスからコンソール エージェントを作成する予定の場合は、コンソール エージェントを作成した後にこのネットワーク要件を実装します。

ステップ6: クラウド権限を準備する

コンソール エージェントには、仮想ネットワークにCloud Volumes ONTAPを展開し、 NetAppデータ サービスを使用するために、クラウド プロバイダーからの権限が必要です。クラウド プロバイダーで権限を設定し、それらの権限をコンソール エージェントに関連付ける必要があります。

必要な手順を表示するには、クラウド プロバイダーで使用する認証オプションを選択します。

AWS IAM ロール

IAM ロールを使用して、コンソール エージェントに権限を付与します。

AWS Marketplace からコンソールエージェントを作成している場合は、EC2 インスタンスを起動するときにその IAM ロールを選択するように求められます。

独自の Linux ホストに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、ロールを EC2 インスタンスにアタッチします。

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。
3. IAM ロールを作成します。
   a. *[ロール] > [ロールの作成]*を選択します。
   b. **AWS** サービス **> EC2** を選択します。
   c. 作成したポリシーを添付して権限を追加します。
   d. 残りの手順を完了してロールを作成します。

結果

これで、コンソール エージェント EC2 インスタンスの IAM ロールが作成されました。

AWS アクセスキー

IAM ユーザーの権限とアクセスキーを設定します。コンソールエージェントをインストールしてコンソールを設定した後、コンソールに AWS アクセスキーを提供する必要があります。

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。

Azure ロール

必要な権限を持つ Azure カスタム ロールを作成します。このロールをコンソール エージェント VM に割り当てます。

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"

手順

1. 独自のホストにソフトウェアを手動でインストールする予定の場合は、カスタム ロールを通じて必要な Azure アクセス許可を提供できるように、VM でシステム割り当てマネージド ID を有効にします。

   "Microsoft Azure ドキュメント: Azure ポータルを使用して VM 上の Azure リソースのマネージド ID を構成する"

2. の内容をコピーします"コネクタのカスタムロール権限"JSON ファイルに保存します。
3. 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。

   NetApp Consoleで使用する各 Azure サブスクリプションの ID を追加する必要があります。

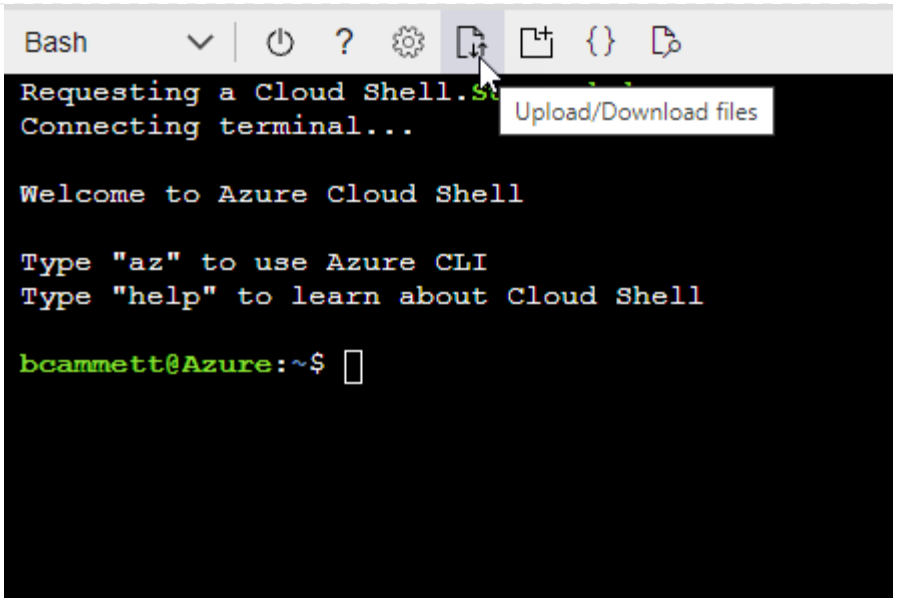
   例

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

4. 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。

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



c. 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
```

Azure サービスプリンシパル

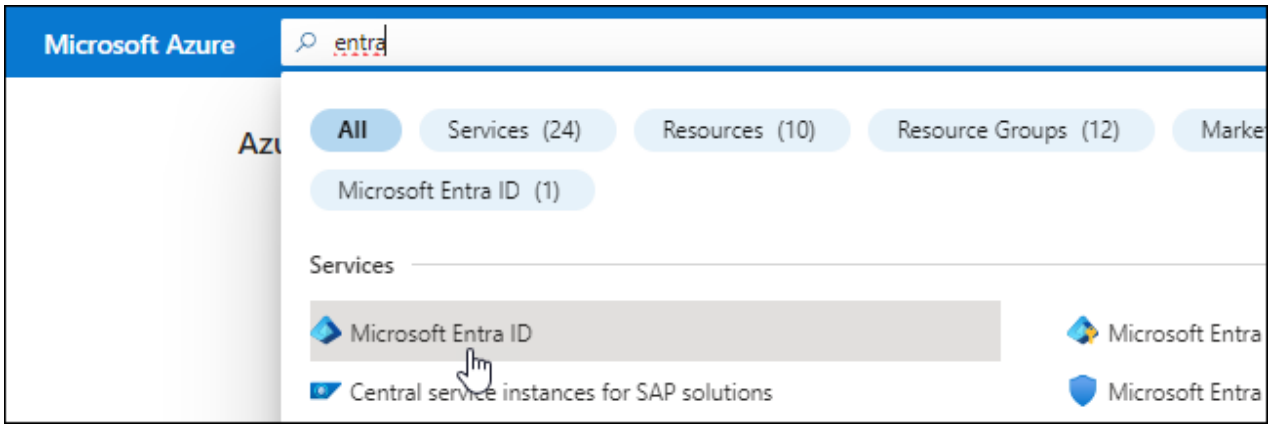
Microsoft Entra ID でサービス プリンシパルを作成して設定し、コンソールに必要な Azure 資格情報を取得します。コンソール エージェントをインストールした後、コンソールにこれらの資格情報を提供する必要があります。

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。

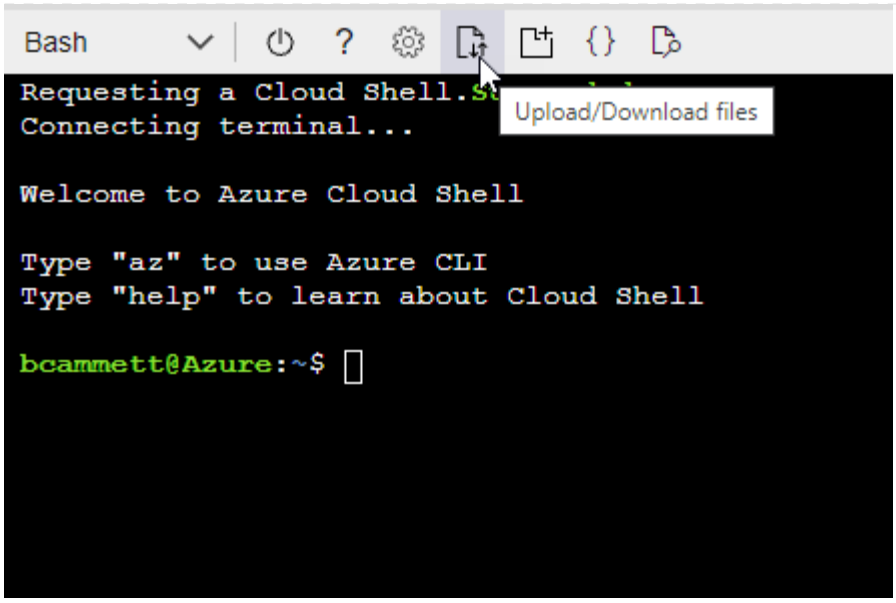
      例

      ```
      "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。

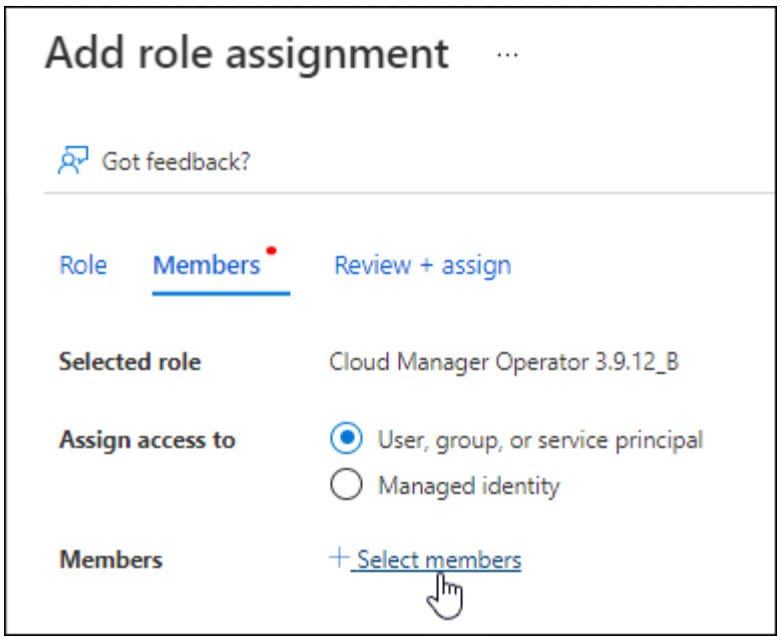
b. サブスクリプションを選択します。

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。

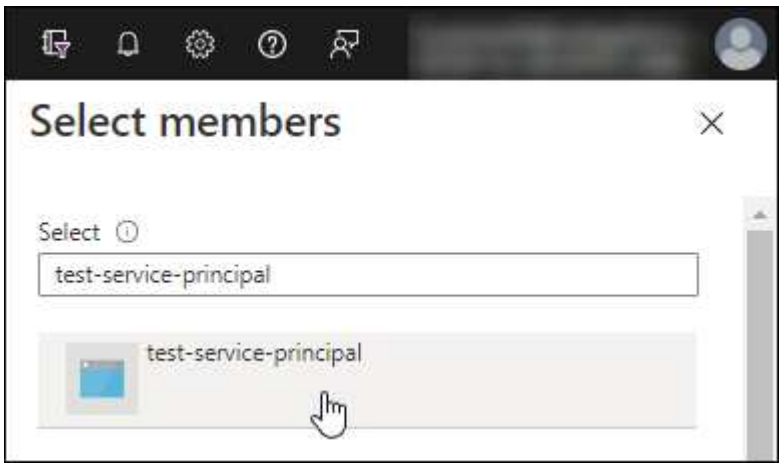
e. *メンバー*タブで、次の手順を実行します。

- *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。

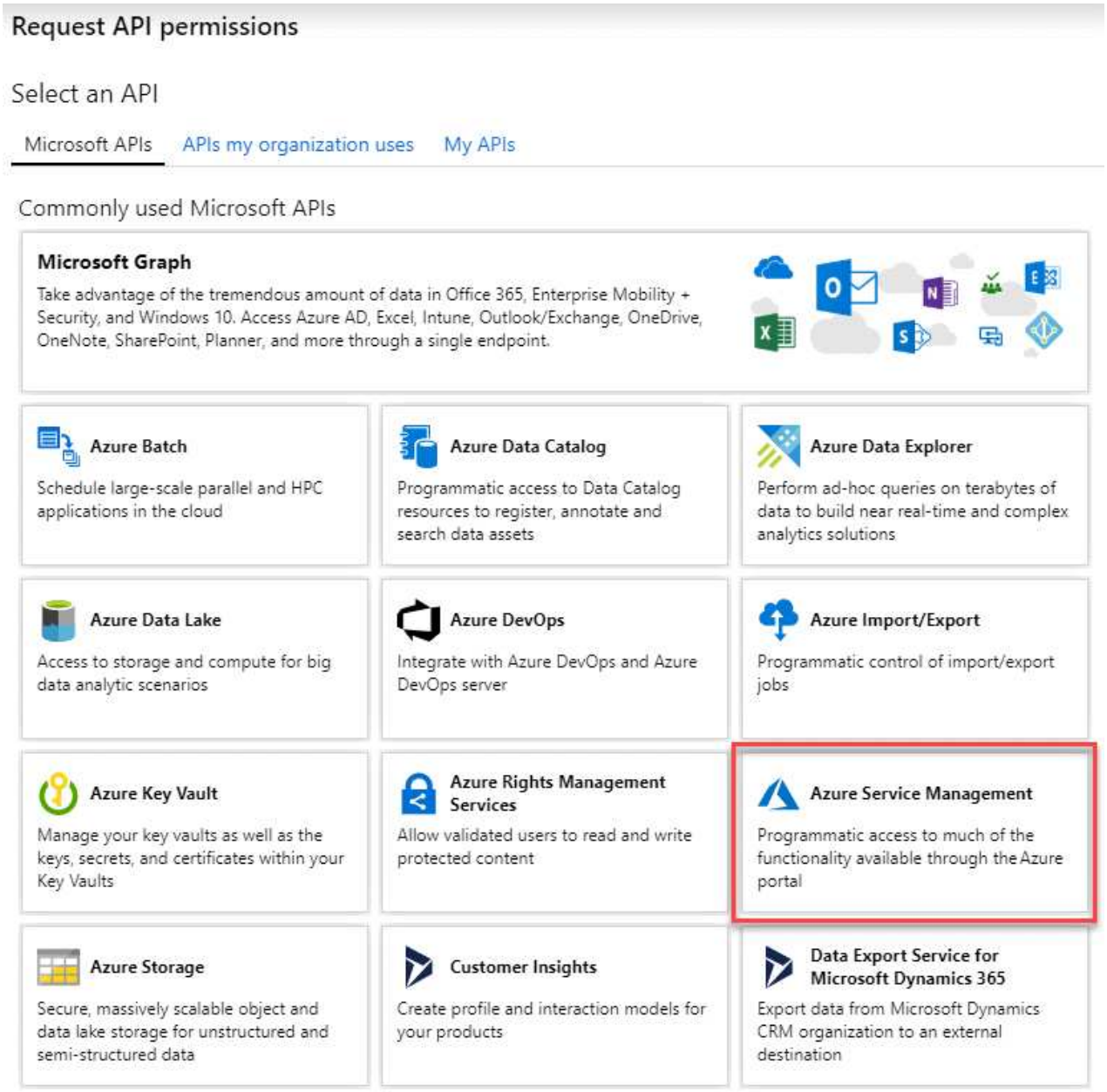
これで、サービス プリンシパルに、コンソール エージェントをデプロイするために必要な Azure アクセス許可が付与されました。

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。

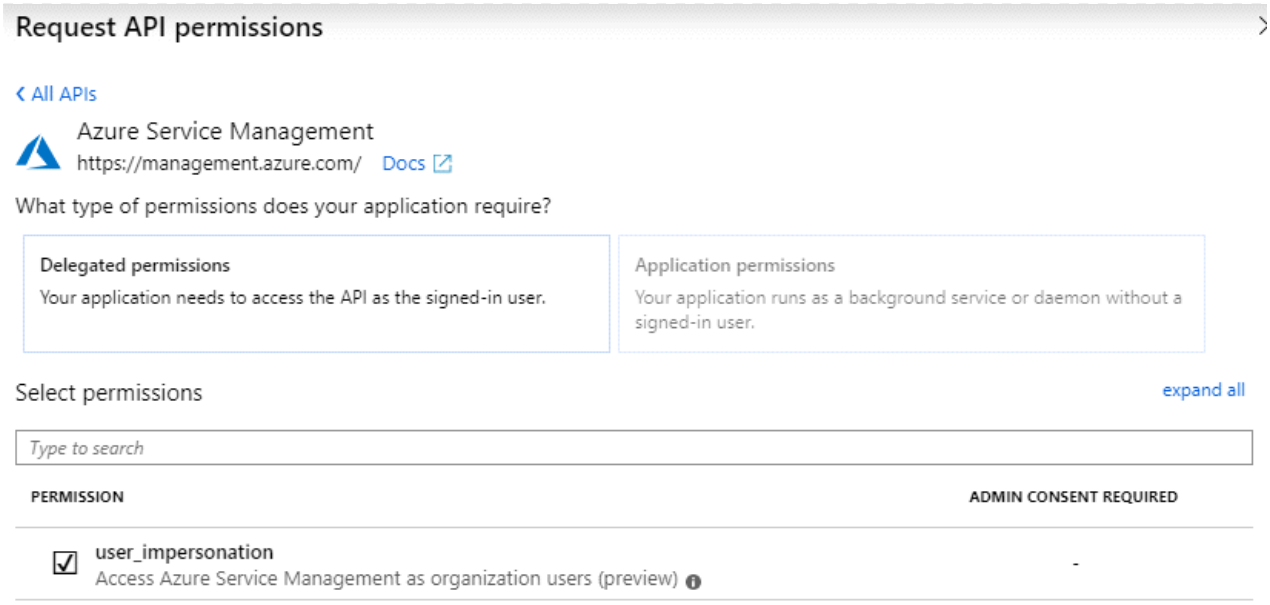
Windows Azure サービス管理 **API** 権限を追加する

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。

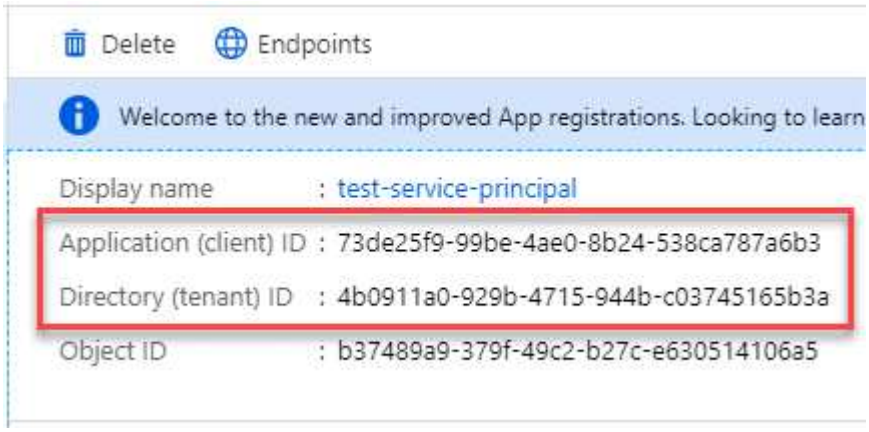


4. 組織ユーザーとして **Azure** サービス管理にアクセスする を選択し、権限の追加 を選択します。



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。

結果

これでサービス プリンシパルが設定され、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、およびクライアント シークレットの値がコピーされているはずです。 Azure アカウントを追加するときに、コンソールにこの情報を入力する必要があります。

Google Cloud サービス アカウント

ロールを作成し、コンソール エージェント VM インスタンスに使用するサービス アカウントに適用します。

手順

1. Google Cloud でカスタムロールを作成します。

   a. 定義された権限を含むYAMLファイルを作成します。"Google Cloud のコンソール エージェント ポリシー" 。

   b. Google Cloud から Cloud Shell を有効にします。

   c. コンソール エージェントに必要な権限を含む YAML ファイルをアップロードします。

   d. カスタムロールを作成するには、 `gcloud iam roles create`指示。

      次の例では、プロジェクト レベルで「agent」という名前のロールを作成します。

```
gcloud iam roles create agent --project=myproject --file=agent.yaml
```

   +
   "Google Cloud ドキュメント: カスタムロールの作成と管理"

2. Google Cloud でサービス アカウントを作成します。

   a. IAM & Admin サービスから、サービス アカウント > サービス アカウントの作成 を選択します。

   b. サービス アカウントの詳細を入力し、[作成して続行] を選択します。

   c. 作成したロールを選択します。

   d. 残りの手順を完了してロールを作成します。

      "Google Cloud ドキュメント: サービス アカウントの作成"

ステップ7: Google Cloud APIを有効にする

Google Cloud にCloud Volumes ONTAPをデプロイするには、いくつかの API が必要です。

手順

1. "プロジェクトで次の Google Cloud API を有効にします"
    - クラウド デプロイメント マネージャー V2 API
    - クラウド インフラストラクチャ マネージャー API
    - クラウドロギングAPI
    - クラウド リソース マネージャー API
    - コンピューティングエンジン API
    - アイデンティティとアクセス管理 (IAM) API
    - Cloud Key Management Service（KMS）API（お客様が管理する暗号化キー（CMEK）でNetApp Backup and Recoveryを使用する予定の場合のみ必要）
    - Cloud Quotas API（Infrastructure Managerを使用したCloud Volumes ONTAPデプロイメントに必要）

制限モードでコンソールエージェントを展開する

制限されたアウトバウンド接続でNetApp Consoleを使用できるように、コンソール エージェントを制限モードで展開します。開始するには、コンソール エージェントをインストールし、コンソール エージェントで実行されているユーザー インターフェイスにアクセスしてコンソールをセットアップし、以前に設定したクラウド権限を提供します。

ステップ1: コンソールエージェントをインストールする

コンソール エージェントをクラウド プロバイダーのマーケットプレイスからインストールするか、Linux ホストに手動でインストールします。

コンソール エージェントをインストールする前に、環境を準備しておく必要があります。AWS Marketplace から、Azure Marketplace から、または AWS、Azure、Google Cloud で実行されている独自の Linux ホストに手動でインストールできます。

AWS コマーシャルマーケットプレイス

開始する前に

以下のものを用意してください。

- ネットワーク要件を満たす VPC とサブネット。

  "ネットワーク要件について学ぶ"

- コンソール エージェントに必要な権限を含むポリシーがアタッチされた IAM ロール。

  "AWS権限の設定方法を学ぶ"

- IAM ユーザーが AWS Marketplace にサブスクライブしたり、サブスクライブ解除したりするための権限。
- エージェントの CPU および RAM 要件を理解していること。

  "エージェントの要件を確認する"。

- EC2 インスタンスのキーペア。

手順

1. に行く "AWS Marketplace でのNetApp Consoleエージェントのリスト"
2. マーケットプレイス ページで、[サブスクリプションを続行] を選択します。
3. ソフトウェアをサブスクライブするには、「利用規約に同意」を選択します。

   サブスクリプションのプロセスには数分かかる場合があります。

4. サブスクリプションプロセスが完了したら、[構成に進む] を選択します。
5. *このソフトウェアを構成する*ページで、正しいリージョンが選択されていることを確認し、*起動を続行*を選択します。
6. このソフトウェアの起動 ページの アクションの選択 で、**EC2** 経由で起動 を選択し、起動 を選択します。

   EC2 コンソールを使用してインスタンスを起動し、IAM ロールをアタッチします。これは、**Web** サイトから起動 アクションでは不可能です。

7. プロンプトに従ってインスタンスを構成してデプロイします。
   - 名前とタグ: インスタンスの名前とタグを入力します。
   - アプリケーションと **OS** イメージ: このセクションはスキップします。コンソール エージェント AMI はすでに選択されています。
   - インスタンス タイプ: リージョンの可用性に応じて、RAM と CPU の要件を満たすインスタンス タイプを選択します (t3.2xlarge が事前に選択されており、推奨されています)。
   - キーペア (ログイン): インスタンスに安全に接続するために使用するキーペアを選択します。
   - ネットワーク設定: 必要に応じてネットワーク設定を編集します。
     - 必要な VPC とサブネットを選択します。

- インスタンスにパブリック IP アドレスを割り当てるかどうかを指定します。
- コンソール エージェント インスタンスに必要な接続方法 (SSH、HTTP、HTTPS) を有効にするセキュリティ グループ設定を指定します。

  "AWS のセキュリティグループルールを表示する" 。

◦ ストレージの構成: ルート ボリュームのデフォルトのサイズとディスク タイプを維持します。

ルートボリュームで Amazon EBS 暗号化を有効にする場合は、[詳細] を選択し、[ボリューム **1**] を展開して、[暗号化] を選択し、KMS キーを選択します。

◦ 詳細: **IAM** インスタンス プロファイル で、コンソール エージェントに必要な権限を含む IAM ロールを選択します。

◦ 概要: 概要を確認し、*インスタンスの起動*を選択します。

結果

AWS は指定された設定でソフトウェアを起動します。コンソール エージェントは約 5 分で展開されます。

次の手順

NetApp Consoleをセットアップします。

AWS Gov マーケットプレイス

開始する前に

以下のものを用意してください。

- ネットワーク要件を満たす VPC とサブネット。

  "ネットワーク要件について学ぶ"

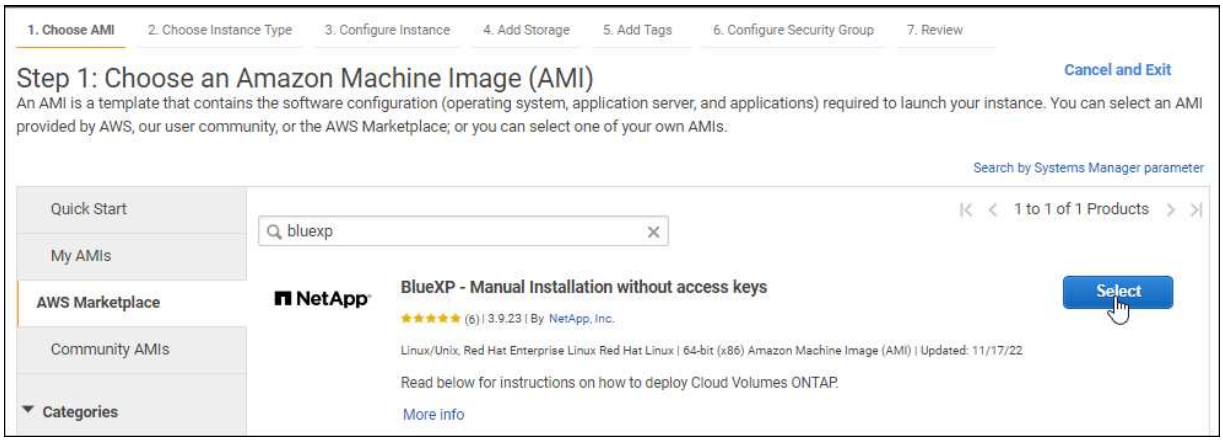
- コンソール エージェントに必要な権限を含むポリシーがアタッチされた IAM ロール。

  "AWS権限の設定方法を学ぶ"

- IAM ユーザーが AWS Marketplace にサブスクライブしたり、サブスクライブ解除したりするための権限。
- EC2 インスタンスのキーペア。

手順

1. AWS Marketplace で提供されているNetApp Consoleエージェントにアクセスします。
   a. EC2 サービスを開き、*インスタンスの起動*を選択します。
   b. *AWS Marketplace*を選択します。
   c. NetApp Consoleを検索し、オファリングを選択します。



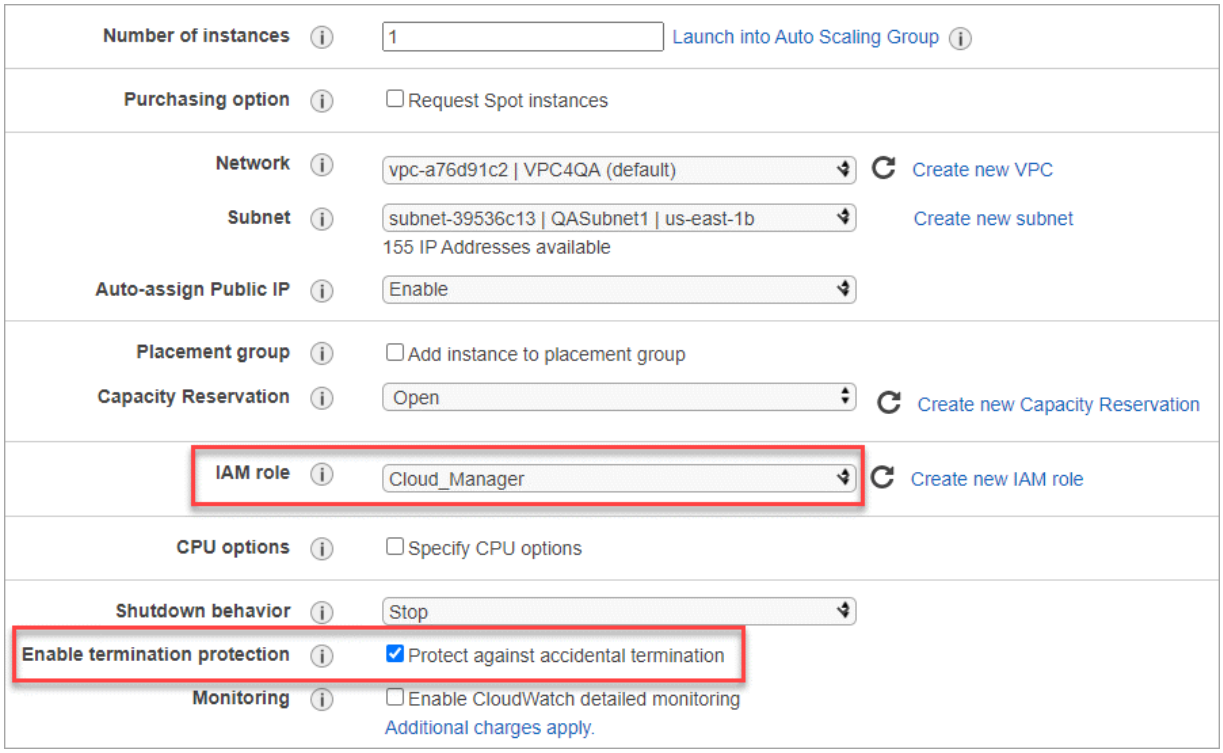
d. *続行*を選択します。

2. プロンプトに従ってインスタンスをセットアップして起動します。

   - インスタンス タイプを選択: リージョンの可用性に応じて、サポートされているインスタンス タイプのいずれかを選択します (t3.2xlarge が推奨されます)。

     "インスタンス要件を確認する" 。

   - インスタンスの詳細の設定: VPC とサブネットを選択し、手順 1 で作成した IAM ロールを選択し、終了保護を有効にして (推奨)、要件を満たすその他の設定オプションを選択します。



   - ストレージの追加: デフォルトのストレージ オプションをそのままにします。
   - タグの追加: 必要に応じて、インスタンスのタグを入力します。
   - セキュリティ グループの構成: コンソール エージェント インスタンスに必要な接続方法 (SSH 、HTTP、HTTPS) を指定します。
   - 確認: 選択内容を確認し、*起動*を選択します。

結果

AWS は指定された設定でソフトウェアを起動します。コンソール エージェントは約 5 分で展開されます。

次の手順

コンソールをセットアップします。

Azure Gov マーケットプレイス

開始する前に

次のものが必要です:

- ネットワーク要件を満たす VNet とサブネット。

  "ネットワーク要件について学ぶ"

- コンソール エージェントに必要なアクセス許可を含む Azure カスタム ロール。

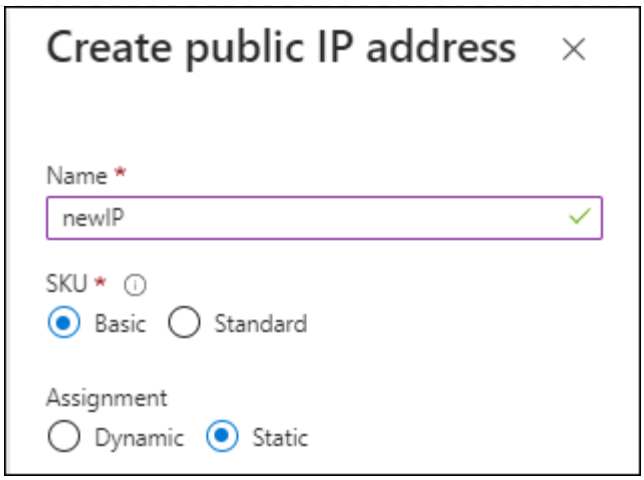
  "Azure の権限を設定する方法を学ぶ"

手順

1. Azure Marketplace のNetApp Consoleエージェント VM ページに移動します。
   - "商用リージョン向けの Azure Marketplace ページ"
   - "Azure Government リージョンの Azure Marketplace ページ"
2. *今すぐ入手*を選択し、*続行*を選択します。
3. Azure ポータルから [作成] を選択し、手順に従って仮想マシンを構成します。

   VM を構成する際には、次の点に注意してください。

   - **VM** サイズ: CPU と RAM の要件を満たす VM サイズを選択します。 Standard_D8s_v3 をお勧めします。
   - ディスク: コンソール エージェントは、HDD ディスクまたは SSD ディスクのいずれでも最適に動作します。
   - パブリック **IP**: コンソール エージェント VM でパブリック IP アドレスを使用するには、Basic SKU を選択します。



代わりに標準 SKU IP アドレスを使用する場合、コンソールはパブリック IP ではなく、コンソール エージェントのプライベート IP アドレスを使用します。コンソールにアクセスするために使用するマシンがプライベート IP アドレスに到達できない場合、コンソールは機能しません。

"Azure ドキュメント: パブリック IP SKU"

- ネットワーク セキュリティ グループ: コンソール エージェントには、SSH、HTTP、および HTTPS を使用した受信接続が必要です。

  "Azure のセキュリティ グループ ルールを表示する" 。

- **ID**: 管理 の下で、システム割り当てマネージド **ID** を有効にする を選択します。

  マネージド ID を使用すると、コンソール エージェント VM は資格情報なしで Microsoft Entra ID に対して自身を識別できます。 "Azure リソースのマネージド ID の詳細" 。

4. 確認 **+** 作成 ページで選択内容を確認し、作成 を選択してデプロイを開始します。

結果

Azure は指定された設定で仮想マシンをデプロイします。仮想マシンとコンソール エージェント ソフトウェアは約 5 分以内に実行されるはずです。

次の手順

NetApp Consoleをセットアップします。

手動インストール（**Google Cloud** で使用する必要があります）

AWS、Azure、または Google Cloud で実行されている独自の Linux ホストに、コンソール エージェントを手動でインストールできます。

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"。

- インストール中に送信接続を検証する構成チェックを無効にする必要があります。このチェックが無効になっていない場合、手動インストールは失敗します。"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。"
- オペレーティング システムに応じて、コンソール エージェントをインストールする前に Podman または Docker Engine のいずれかが必要です。

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。

   - 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。

結果

コンソール エージェントがインストールされました。プロキシ サーバーを指定した場合、インストールの最後に、コンソール エージェント サービス (occm) が 2 回再起動します。

次の手順

NetApp Consoleをセットアップします。

ステップ2: NetApp Consoleをセットアップする

コンソールに初めてアクセスすると、コンソール エージェントの組織を選択するように求められ、制限モードを有効にする必要があります。

開始する前に

コンソール エージェントを設定するユーザーは、コンソール組織に属していないログインを使用してコンソールにログインする必要があります。

ログインが別の組織に関連付けられている場合は、新しいログインでサインアップする必要があります。そうしないと、セットアップ画面に制限モードを有効にするオプションが表示されません。

手順

1. コンソール エージェント インスタンスに接続しているホストから Web ブラウザを開き、インストールしたコンソール エージェントの次の URL を入力します。
2. NetApp Consoleにサインアップまたはログインします。
3. ログインしたら、コンソールを設定します。
   a. コンソール エージェントの名前を入力します。
   b. 新しいコンソール組織の名前を入力します。
   c. 安全な環境で実行していますか**?** を選択します。

d. *このアカウントで制限モードを有効にする*を選択します。

アカウントの作成後はこの設定を変更できないことに注意してください。制限モードを後から有効にしたり無効にしたりすることはできません。

コンソール エージェントを政府リージョンに展開した場合、チェック ボックスは既に有効になっており、変更できません。これは、制限モードが政府地域でサポートされている唯一のモードであるためです。

a. *始めましょう*を選択します。

結果

コンソール エージェントがインストールされ、コンソール組織に設定されました。すべてのユーザーは、コンソール エージェント インスタンスの IP アドレスを使用してコンソールにアクセスする必要があります。

次の手順

以前に設定した権限をコンソールに提供します。

ステップ3: コンソールエージェントに権限を付与する

コンソール エージェントを Azure Marketplace から、または手動でインストールした場合は、以前に設定したアクセス許可を付与する必要があります。

デプロイ中に必要な IAM ロールを選択したため、AWS Marketplace からコンソールエージェントをデプロイした場合は、これらの手順は適用されません。

"クラウド権限の準備方法を学ぶ" 。

AWS IAM ロール

以前に作成した IAM ロールを、コンソールエージェントをインストールした EC2 インスタンスにアタッチします。

これらの手順は、AWS にコンソールエージェントを手動でインストールした場合にのみ適用されます。AWS Marketplace のデプロイメントでは、コンソールエージェントインスタンスは、必要な権限を含む IAM ロールにすでに関連付けられています。

手順

1. Amazon EC2 コンソールに移動します。
2. *インスタンス*を選択します。
3. コンソール エージェント インスタンスを選択します。
4. *アクション > セキュリティ > IAM ロールの変更*を選択します。
5. IAM ロールを選択し、*IAM ロールの更新*を選択します。

AWS アクセスキー

必要な権限を持つ IAM ユーザーの AWS アクセス キーをNetApp Consoleに提供します。

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。

Azure ロール

Azure ポータルに移動し、1 つ以上のサブスクリプションのコンソール エージェント仮想マシンに Azure カスタム ロールを割り当てます。

手順

1. Azure ポータルから サブスクリプション サービスを開き、サブスクリプションを選択します。

   サブスクリプション サービスからロールを割り当てることが重要です。これは、サブスクリプション レベルでのロール割り当ての範囲を指定するためです。 *scope* は、アクセスが適用されるリソースのセットを定義します。別のレベル (たとえば、仮想マシン レベル) でスコープを指定すると、NetApp Console内からアクションを完了する機能に影響します。

   "Microsoft Azure ドキュメント: Azure RBAC のスコープを理解する"

2. 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。
3. *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。

コンソール オペレーターは、ポリシーで提供されるデフォルト名です。ロールに別の名前を選択した場合は、代わりにその名前を選択します。

4. *メンバー*タブで、次の手順を実行します。
   a. マネージド **ID** へのアクセスを割り当てます。
   b. *メンバーの選択*を選択し、コンソール エージェント仮想マシンが作成されたサブスクリプションを選択し、*マネージド ID*の下で*仮想マシン*を選択して、コンソール エージェント仮想マシンを選択します。
   c. *選択*を選択します。
   d. *次へ*を選択します。
   e. *レビュー + 割り当て*を選択します。
   f. 追加の Azure サブスクリプションのリソースを管理する場合は、そのサブスクリプションに切り替えて、これらの手順を繰り返します。

Azure サービスプリンシパル

以前に設定した Azure サービス プリンシパルの資格情報をNetApp Consoleに提供します。

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

NetApp Console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権限が付与されました。

Google Cloud サービス アカウント

サービス アカウントをコンソール エージェント VM に関連付けます。

手順

1. Google Cloud ポータルに移動し、サービス アカウントをコンソール エージェント VM インスタンスに割り当てます。

   "Google Cloud ドキュメント: インスタンスのサービス アカウントとアクセス スコープの変更"

2. 他のプロジェクトのリソースを管理する場合は、コンソール エージェント ロールを持つサービス アカウントをそのプロジェクトに追加してアクセスを許可します。プロジェクトごとにこの手順を繰り返す必要があります。

NetApp Intelligent Servicesにサブスクライブする（制限モード）

クラウド プロバイダーのマーケットプレイスからNetApp Intelligent Servicesにサブスクライブして、時間単位の料金 (PAYGO) または年間契約でデータ サービスの料金を支払います。 NetAppからライセンスを購入した場合 (BYOL)、マーケットプレイス オファリングにもサブスクライブする必要があります。最初にライセンスに対して課金が行われますが、ライセンス容量を超えた場合、またはライセンスの有効期限が切れた場合は、時間単位で課金されます。

マーケットプレイス サブスクリプションでは、制限モードで次のデータ サービスに対して課金できます。

- NetApp Backup and Recovery
- Cloud Volumes ONTAP
- NetApp Cloud Tiering
- NetApp Ransomware Resilience
- NetApp Disaster Recovery

NetApp Data Classification はサブスクリプションを通じて有効になりますが、分類の使用には料金はかかりません。

開始する前に

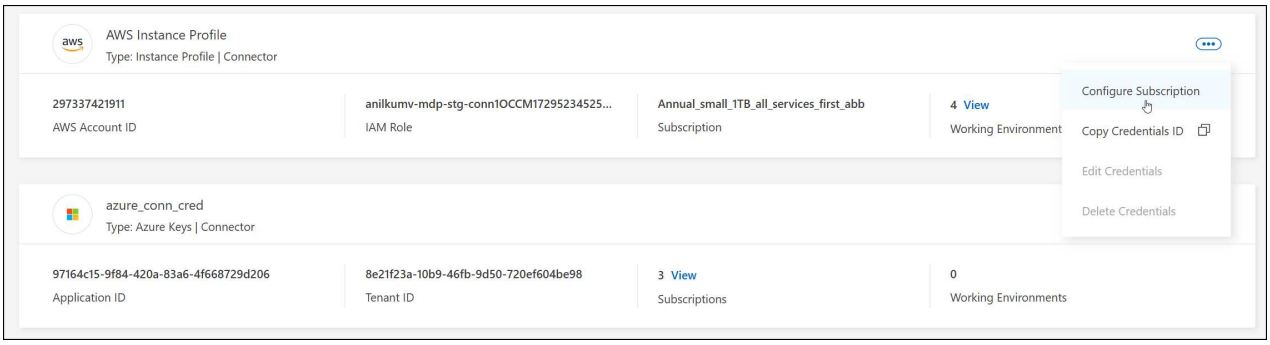
データ サービスをサブスクライブするには、コンソール エージェントをすでに展開しておく必要があります。コンソール エージェントに接続されたクラウド資格情報にマーケットプレイス サブスクリプションを関連付ける必要があります。

AWS

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. コンソール エージェントに関連付けられている資格情報のセットのアクション メニューを選択し、[サブスクリプションの構成] を選択します。

   コンソール エージェントに関連付けられている資格情報を選択する必要があります。マーケットプレイス サブスクリプションを、 NetApp Consoleに関連付けられている資格情報に関連付けることはできません。



4. 資格情報を既存のサブスクリプションに関連付けるには、ドロップダウン リストからサブスクリプションを選択し、[構成] を選択します。
5. 認証情報を新しいサブスクリプションに関連付けるには、[サブスクリプションの追加] > [続行] を選択し、AWS Marketplace の手順に従います。

   a. *購入オプションを表示*を選択します。
   b. *購読*を選択します。
   c. *アカウントを設定*を選択します。

      NetApp Consoleにリダイレクトされます。

   d. *サブスクリプションの割り当て*ページから:

      - このサブスクリプションを関連付けるコンソール組織またはアカウントを選択します。
      - 既存のサブスクリプションを置き換える フィールドで、1 つの組織またはアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

        コンソールは、組織またはアカウント内のすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。資格情報のセットがサブスクリプションに関連付けられたことがない場合、この新しいサブスクリプションはそれらの資格情報に関連付けられません。

   他のすべての組織またはアカウントについては、これらの手順を繰り返して、サブスクリプションを手動で関連付ける必要があります。

   ◦ *保存*を選択します。

Azure

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. コンソール エージェントに関連付けられている資格情報のセットのアクション メニューを選択し、[サブスクリプションの構成] を選択します。

   コンソール エージェントに関連付けられている資格情報を選択する必要があります。マーケットプレイス サブスクリプションを、 NetApp Consoleに関連付けられている資格情報に関連付けることはできません。

4. 資格情報を既存のサブスクリプションに関連付けるには、ドロップダウン リストからサブスクリプションを選択し、[構成] を選択します。
5. 資格情報を新しいサブスクリプションに関連付けるには、[サブスクリプションの追加] > [続行] を選択し、Azure Marketplace の手順に従います。

   a. プロンプトが表示されたら、Azure アカウントにログインします。
   b. *購読*を選択します。
   c. フォームに記入し、「購読」を選択します。
   d. サブスクリプションプロセスが完了したら、「今すぐアカウントを構成」を選択します。

      NetApp Consoleにリダイレクトされます。

   e. *サブスクリプションの割り当て*ページから:
      - このサブスクリプションを関連付けるコンソール組織またはアカウントを選択します。
      - 既存のサブスクリプションを置き換える フィールドで、1 つの組織またはアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

        コンソールは、組織またはアカウント内のすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。資格情報のセットがサブスクリプションに関連付けられたことがない場合、この新しいサブスクリプションはそれらの資格情報に関連付けられません。

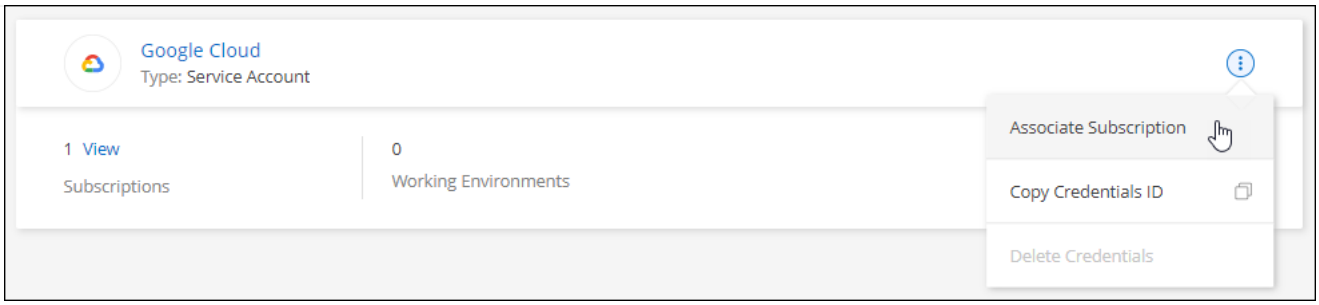
   他のすべての組織またはアカウントについては、これらの手順を繰り返して、サブスクリプションを手動で関連付ける必要があります。

   ◦ *保存*を選択します。

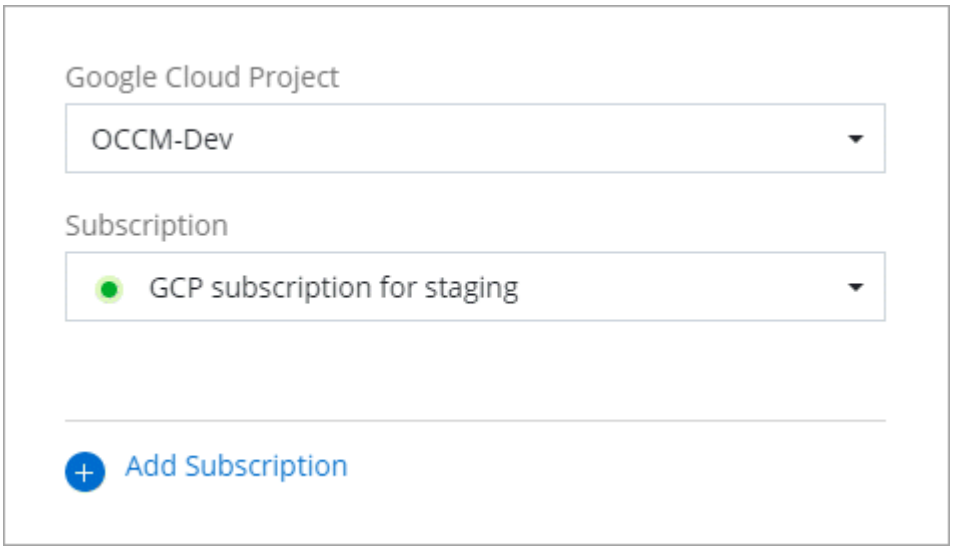
Google Cloud

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. コンソール エージェントに関連付けられている資格情報のセットのアクション メニューを選択し、[サブスクリプションの構成] を選択します。



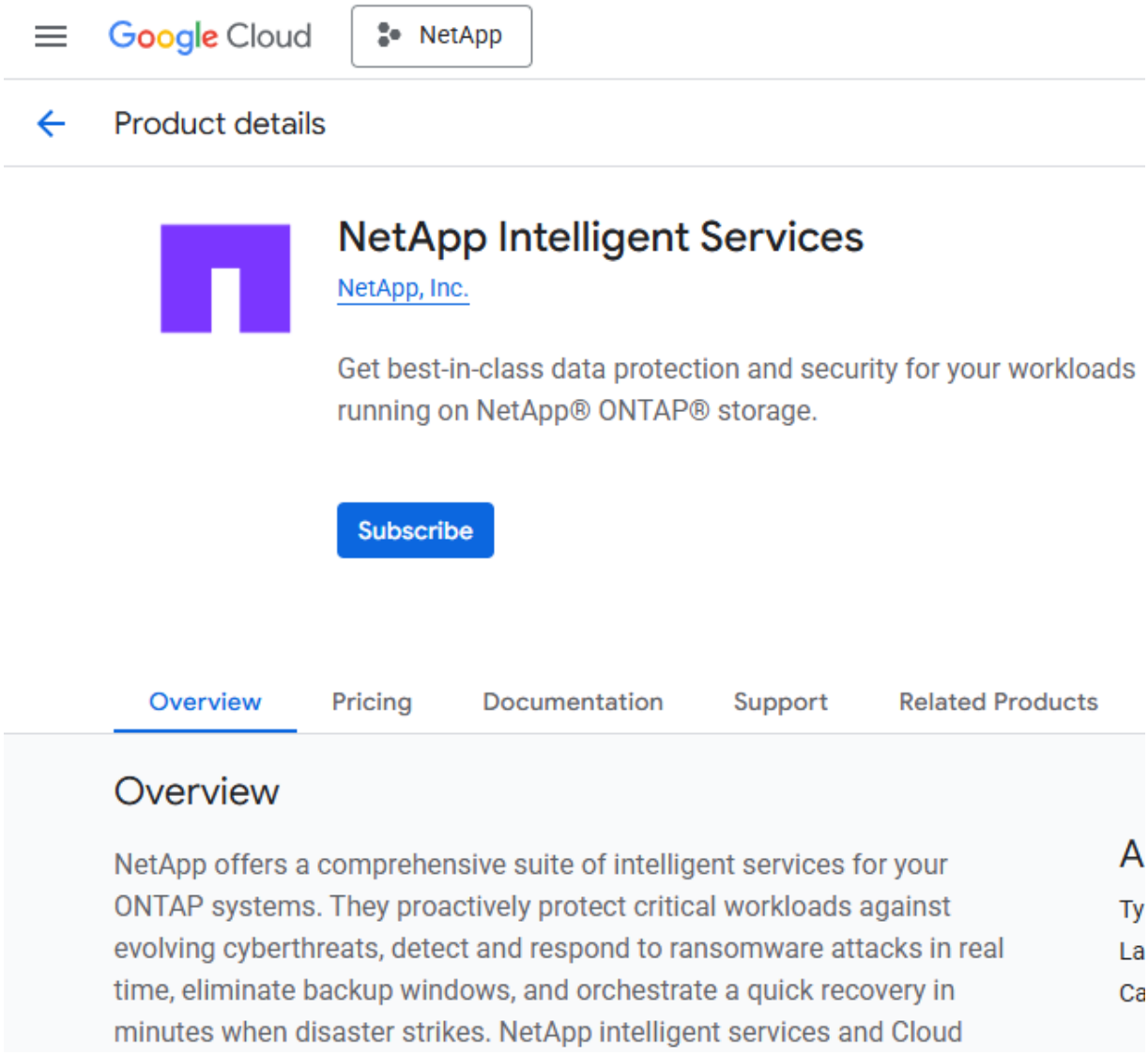
1. 選択した認証情報を使用して既存のサブスクリプションを構成するには、ドロップダウン リストから Google Cloud プロジェクトとサブスクリプションを選択し、[構成] を選択します。



2. まだサブスクリプションをお持ちでない場合は、[サブスクリプションを追加] > [続行] を選択し、Google Cloud Marketplace の手順に従います。

次の手順を完了する前に、Google Cloud アカウントの課金管理者権限とNetApp Consoleのログイン権限の両方があることを確認してください。

a. リダイレクトされたら "Google Cloud Marketplace のNetApp Intelligent Servicesページ"上部のナビゲーション メニューで正しいプロジェクトが選択されていることを確認します。

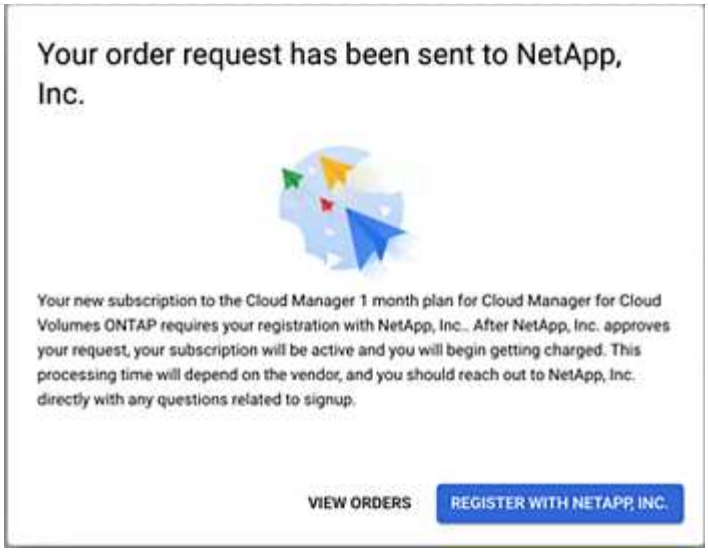


b. *購読*を選択します。
c. 適切な請求先アカウントを選択し、利用規約に同意します。
d. *購読*を選択します。

   この手順により、転送リクエストがNetAppに送信されます。

e. ポップアップダイアログボックスで、* NetApp, Inc.に登録*を選択します。

   Google Cloud サブスクリプションをコンソールの組織またはアカウントにリンクするには、この手順を完了する必要があります。このページからリダイレクトされ、コンソールにサインインするまで、サブスクリプションをリンクするプロセスは完了しません。



f. サブスクリプションの割り当て ページの手順を完了します。

> 組織内の誰かが既に請求先アカウントからマーケットプレイスサブスクリプションを利用している場合は、次のページにリダイレクトされます。 "NetApp Console内のCloud Volumes ONTAPページ"その代わり。予期しない事態が発生した場合は、 NetAppの営業チームにお問い合わせください。 Google では、Google 請求先アカウントごとに 1 つのサブスクリプションのみ有効になります。

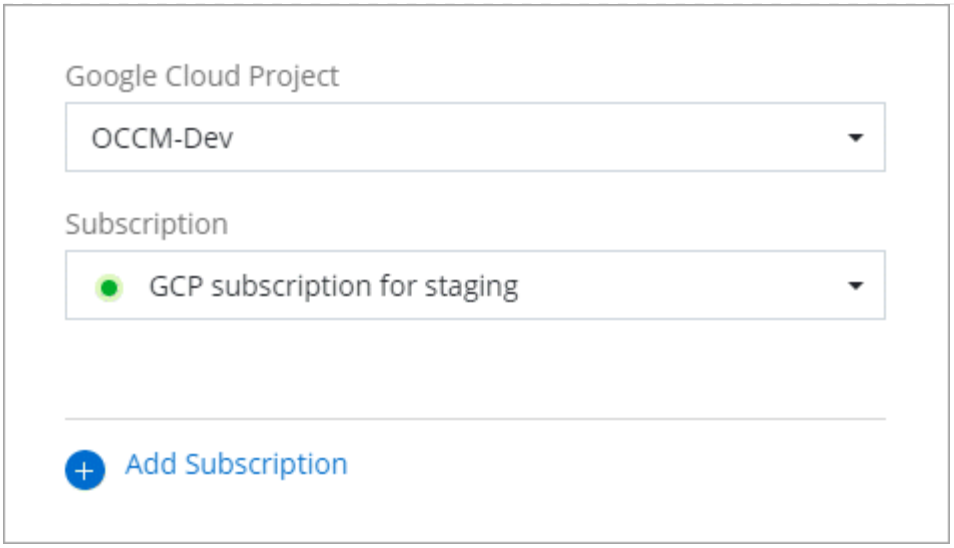
- このサブスクリプションを関連付けるコンソール組織を選択します。
- 既存のサブスクリプションを置き換える フィールドで、1 つの組織の既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

  コンソールは、組織内のすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。資格情報のセットがサブスクリプションに関連付けられたことがない場合、この新しいサブスクリプションはそれらの資格情報に関連付けられません。

他のすべての組織またはアカウントについては、これらの手順を繰り返して、サブスクリプションを手動で関連付ける必要があります。

- *保存*を選択します。

3. このプロセスが完了したら、コンソールの [資格情報] ページに戻り、この新しいサブスクリプションを選択します。



関連情報

- "Cloud Volumes ONTAPのBYOL容量ベースライセンスを管理する"
- "データサービスのBYOLライセンスを管理する"
- "AWS の認証情報とサブスクリプションを管理する"
- "Azure の資格情報とサブスクリプションを管理する"
- "Google Cloud の認証情報とサブスクリプションを管理する"

次にできること（制限モード）

NetApp Consoleを制限モードで起動して実行すると、制限モードでサポートされているサービスの使用を開始できます。

ヘルプについては、次のサービスのドキュメントを参照してください。

- "Azure NetApp Filesドキュメント"
- "バックアップとリカバリのドキュメント"
- "分類ドキュメント"
- "Cloud Volumes ONTAPドキュメント"
- "デジタルウォレットのドキュメント"
- "オンプレミスのONTAPクラスタのドキュメント"
- "レプリケーションドキュメント"

関連情報

"NetApp Consoleの展開モード"