# 管理と監視

## NetApp Console setup and administration

NetApp
February 09, 2026

# 目次

# 管理と監視

## NetAppサポートアカウントの関連付け

### NetApp Consoleに関連付けられたNSS資格情報を管理する

ストレージ管理の主要なワークフローを有効にするには、 NetAppサポート サイト アカウントをコンソール組織に関連付けます。これらの NSS 認証情報は組織全体に関連付けられています。

コンソールでは、ユーザー アカウントごとに 1 つの NSS アカウントを関連付けることもサポートされています。"ユーザーレベルの資格情報を管理する方法を学ぶ" 。

概要

次のタスクを有効にするには、 NetAppサポート サイトの資格情報を特定のコンソール アカウントのシリアル番号に関連付ける必要があります。

- BYOL（個人ライセンス使用）時にCloud Volumes ONTAP を導入する

  コンソールがライセンス キーをアップロードし、購入した期間のサブスクリプションを有効にするには、NSS アカウントを提供する必要があります。これには、期間更新の自動更新が含まれます。

- 従量課金制のCloud Volumes ONTAPシステムの登録

  システムのサポートを有効にし、 NetAppテクニカル サポート リソースにアクセスするには、NSS アカウントを提供する必要があります。

- Cloud Volumes ONTAPソフトウェアを最新リリースにアップグレードする

これらの資格情報は、特定のコンソール アカウントのシリアル番号に関連付けられています。ユーザーは、サポート **> NSS** 管理 からこれらの資格情報にアクセスできます。

**NSS**アカウントを追加する

コンソール内のサポート ダッシュボードから、コンソールで使用するNetAppサポート サイト アカウントを追加および管理できます。

NSS アカウントを追加すると、コンソールはライセンスのダウンロード、ソフトウェア アップグレードの検証、将来のサポート登録などにこの情報を使用します。

組織に複数の NSS アカウントを関連付けることはできますが、同じ組織内に顧客アカウントとパートナー アカウントを持つことはできません。

NetApp は、サポートとライセンスに固有の認証サービスの ID プロバイダーとして Microsoft Entra ID を使用します。

手順

1. 管理 **>** サポート。

2. *NSS管理*を選択します。
3. *NSS アカウントの追加*を選択します。
4. *続行*を選択すると、Microsoft ログイン ページにリダイレクトされます。
5. ログイン ページで、 NetAppサポート サイトに登録した電子メール アドレスとパスワードを入力します。

   ログインが成功すると、 NetApp はNSS ユーザー名を保存します。

   これは、メールにマッピングされるシステム生成の ID です。 *NSS管理*ページでは、 ••• メニュー。

   - ログイン認証トークンを更新する必要がある場合は、 ••• メニュー。

     このオプションを使用すると、再度ログインするよう求められます。これらのアカウントのトークンは 90 日後に期限切れになることに注意してください。これを知らせる通知が投稿されます。

次の手順

ユーザーは、新しいCloud Volumes ONTAPシステムを作成するとき、および既存のCloud Volumes ONTAPシステムを登録するときにアカウントを選択できるようになりました。

- "AWS でCloud Volumes ONTAP を起動"
- "Azure でCloud Volumes ONTAP を起動する"
- "Google Cloud でCloud Volumes ONTAP を起動"
- "従量課金制システムの登録"

**NSS**クレデンシャルの更新

セキュリティ上の理由から、NSS 認証情報は 90 日ごとに更新する必要があります。 NSS 認証情報の有効期限が切れた場合は、コンソールの通知センターで通知されます。"通知センターについて学ぶ" 。

資格情報の有効期限が切れると、次のような問題が発生する可能性があります (ただし、これらに限定されません)。

- ライセンスが更新され、新しく購入した容量を利用できなくなります。
- サポートケースを送信および追跡する機能。

さらに、組織に関連付けられている NSS アカウントを変更する場合は、組織に関連付けられている NSS 資格情報を更新することもできます。たとえば、NSS アカウントに関連付けられている人物が退職した場合などです。

手順

1. 管理 **>** サポート。
2. *NSS管理*を選択します。
3. 更新したいNSSアカウントについては、 •••次に、[資格情報の更新]を選択します。
4. プロンプトが表示されたら、[続行] を選択して、Microsoft ログイン ページにリダイレクトします。

   NetApp は、サポートおよびライセンスに関連する認証サービスの ID プロバイダーとして Microsoft Entra

ID を使用します。

5. ログイン ページで、 NetAppサポート サイトに登録した電子メール アドレスとパスワードを入力します。

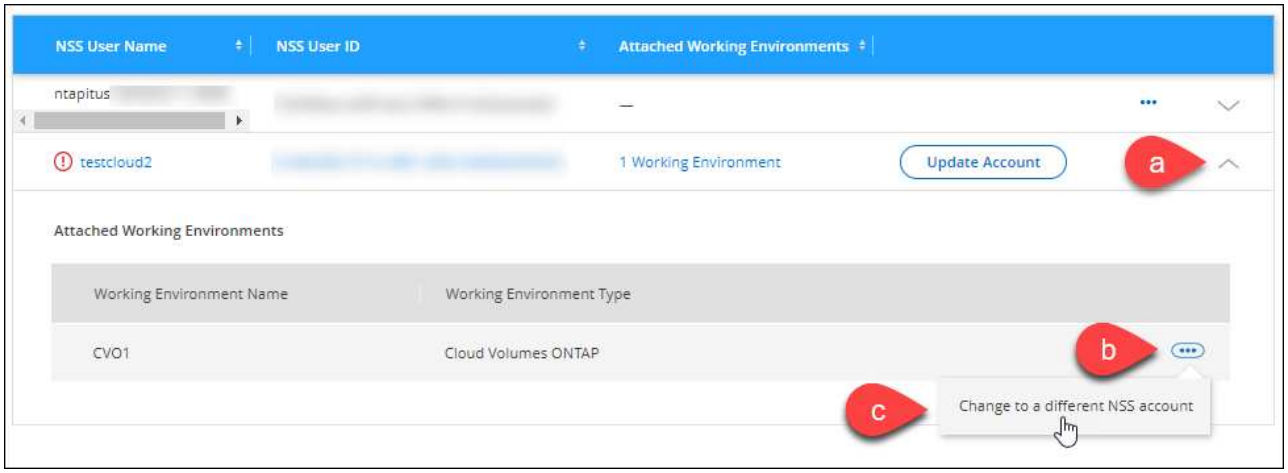
### システムを別の**NSS**アカウントに接続する

組織に複数のNetAppサポート サイト アカウントがある場合は、 Cloud Volumes ONTAPシステムに関連付けるアカウントを変更できます。

まずアカウントをコンソールに関連付ける必要があります。

手順

1. 管理 **>** サポート。
2. *NSS管理*を選択します。
3. NSS アカウントを変更するには、次の手順を実行します。
   a. システムが現在関連付けられているNetAppサポート サイト アカウントの行を展開します。
   b. 関連付けを変更するシステムについては、 •••
   c. *別のNSSアカウントに変更*を選択します。




   d. アカウントを選択し、[保存] を選択します。

### **NSS**アカウントのメールアドレスを表示する

セキュリティ上の理由から、NSS アカウントに関連付けられた電子メール アドレスはデフォルトでは表示されません。 NSS アカウントの電子メール アドレスと関連付けられたユーザー名を表示できます。

NSS 管理ページに移動すると、コンソールはテーブル内の各アカウントに対してトークンを生成します。そのトークンには、関連付けられた電子メール アドレスに関する情報が含まれます。ページを離れるとトークンは削除されます。情報はキャッシュされないため、プライバシーが保護されます。

手順

1. 管理 **>** サポート。

2. *NSS管理*を選択します。
3. 更新したいNSSアカウントについては、次に、[メールアドレスを表示]を選択します。コピーボタンを使用してメールアドレスをコピーできます。

#### NSSアカウントを削除する

コンソールで使用しなくなった NSS アカウントを削除します。

現在Cloud Volumes ONTAPシステムに関連付けられているアカウントは削除できません。まず最初にこれらのシステムを別のNSSアカウントに接続する。

手順

1. 管理 > サポート。
2. *NSS管理*を選択します。
3. 削除したいNSSアカウントについては、次に、[削除] を選択します。
4. *削除*を選択して確認します。

## NetApp Consoleログインに関連付けられた資格情報を管理する

コンソールで実行したアクションに応じて、 ONTAP資格情報とNetAppサポート サイト (NSS) 資格情報がユーザー ログインに関連付けられている場合があります。関連付けた資格情報を表示および管理できます。たとえば、これらの資格情報のパスワードを変更する場合は、コンソールでパスワードを更新する必要があります。

#### ONTAP認証情報

コンソールでONTAPクラスターを検出するには、ユーザーはONTAP管理者の認証情報が必要です。ただし、ONTAP System Manager へのアクセスは、コンソール エージェントを使用しているかどうかによって異なります。

コンソールエージェントなし

ユーザーは、クラスタのONTAP System Manager にアクセスするために、 ONTAP認証情報を入力するよう求められます。ユーザーはこれらの資格情報をコンソールに保存することを選択できます。これにより、毎回資格情報を入力する必要がなくなります。ユーザー資格情報はそれぞれのユーザーのみに表示され、「ユーザー資格情報」ページから管理できます。

コンソールエージェントを使用

デフォルトでは、ユーザーはONTAP System Manager にアクセスするためにONTAP認証情報を入力するように求められません。ただし、コンソール管理者（組織管理者ロールを持つ）は、ユーザーにONTAP認証情報の入力を求めるようにコンソールを設定できます。この設定を有効にすると、ユーザーは毎回ONTAP認証情報を入力する必要があります。

"詳細情報"

#### NSS認証情報

NetApp Consoleログインに関連付けられた NSS 資格情報により、サポート登録、ケース管理、およびDigital Advisorへのアクセスが可能になります。

- サポート > リソース にアクセスしてサポートに登録すると、NSS 資格情報をログインに関連付けるように求められます。

  これにより、組織またはアカウントがサポートに登録され、サポート資格が有効になります。サポートに登録し、サポート資格を有効にするには、組織内の 1 人のユーザーのみがNetAppサポート サイト アカウントをログインに関連付ける必要があります。これが完了すると、リソース ページにアカウントがサポートに登録されていることが表示されます。

  "サポート登録方法を学ぶ"

- 管理 > サポート > ケース管理 にアクセスすると、まだ入力していない場合は NSS 資格情報を入力するように求められます。このページでは、NSS アカウントおよび会社に関連付けられたサポート ケースを作成および管理できます。
- コンソールでDigital Advisorにアクセスすると、NSS 資格情報を入力してDigital Advisorにログインするように求められます。

ログインに関連付けられている NSS アカウントについては、次の点に注意してください。

- アカウントはユーザーレベルで管理されるため、ログインした他のユーザーには表示されません。
- Digital AdvisorおよびサポートケースマネジメントにリンクされているNSSアカウントは、ユーザーごとに1つだけです。
- NetAppサポート サイト アカウントをCloud Volumes ONTAPシステムに関連付ける場合は、自分が所属する組織に追加された NSS アカウントからのみ選択できます。

  NSS アカウント レベルの資格情報は、ログインに関連付けられている NSS アカウントとは異なります。NSS アカウント レベルの認証情報を使用すると、BYOL を使用してCloud Volumes ONTAPをデプロイし、PAYGO システムを登録し、ソフトウェアをアップグレードできます。

  "NetApp Console組織またはアカウントで NSS 認証情報を使用する方法の詳細" 。

ユーザー資格情報を管理する

ユーザー名とパスワードを更新するか、資格情報を削除して、ユーザー資格情報を管理します。

手順

1. *管理 > 資格情報*を選択します。
2. *ユーザー資格情報*を選択します。
3. まだユーザー資格情報がない場合は、「**NSS** 資格情報の追加」を選択して、 NetAppサポート サイト アカウントを追加できます。
4. [アクション] メニューから次のオプションを選択して、既存の資格情報を管理します。
   - 資格情報の更新: アカウントのユーザー名とパスワードを更新します。
   - 資格情報の削除: コンソール ログインに関連付けられている NSS アカウントを削除します。

# コンソールエージェント

# NetApp Consoleエージェントについて学ぶ

コンソール エージェントを使用して、 NetApp Consoleをインフラストラクチャに接続し、AWS、Azure、Google Cloud、オンプレミス環境全体でストレージ ソリューションを安全にオーケストレーションし、データ保護サービスを使用します。

コンソール エージェントを使用すると、次のことが可能になります。

- Cloud Volumes ONTAP のプロビジョニング、ストレージ ボリュームの設定、データ分類の使用など、NetApp Consoleからストレージ管理タスクを調整します。
- サブスクリプション課金統合のためにクラウドプロバイダーのIAMロールを使用して認証する
- 高度なデータ サービス (NetApp Backup and Recovery、 NetApp Disaster Recovery、 NetApp Ransomware Resilience、 NetApp Cloud Tiering) を使用する
- コンソールを制限モードで使用します。

高度なオーケストレーションやデータ保護が必要ない場合は、エージェントを導入せずに、オンプレミスのONTAPクラスターとクラウドネイティブ ストレージ サービスを一元管理できます。監視およびデータ移動ツールも利用できます。

次の表は、コンソール エージェントの有無にかかわらず使用できる機能とサービスを示しています。

| | エージェントで利用可能 | エージェントなしで利用可能 |
|---|---|---|
| サポートされているストレージ システム: | | |
| Amazon FSx for ONTAP | はい（検出および管理機能） | はい（検出のみ） |
| Amazon S3 ストレージ | はい | いいえ |
| Azure BLOB ストレージ | はい | はい |
| Azure NetApp Files | はい | はい |
| Cloud Volumes ONTAP | はい | いいえ |
| Eシリーズシステム | はい | いいえ |
| Google Cloud NetApp Volumes | はい | はい |
| Google Cloud ストレージ バケット | はい | いいえ |
| StorageGRIDシステム | はい | いいえ |

| | エージェントで利用可能 | エージェントなしで利用可能 |
|---|---|---|
| オンプレミスのONTAPクラスタ（高度な管理と検出） | はい（高度な管理と検出） | いいえ（基本的な検出のみ） |
| 利用可能なストレージ管理サービス: | | |
| アラート | はい | いいえ |
| 自動化ハブ | はい | はい |
| Digital Advisor（Active IQ） | はい | いいえ |
| ライセンスとサブスクリプションの管理 | はい | いいえ |
| 経済効率 | はい | いいえ |
| ホームページダッシュボードのメトリクス | はい[2] | いいえ |
| ライフサイクルプランニング | はい | いいえ[1] |
| 持続可能性 | はい | いいえ |
| ソフトウェアアップデート | はい | はい |
| NetAppワークロード | はい | はい |
| 利用可能なデータサービス: | | |
| NetApp Backup and Recovery | はい | いいえ |
| データ分類 | はい | いいえ |
| NetApp Cloud Tiering | はい | いいえ |
| NetApp Copy and Sync | はい | いいえ |
| NetApp Disaster Recovery | はい | いいえ |
| NetApp Ransomware Resilience | はい | いいえ |
| NetApp Volume Caching | はい | いいえ |

[1] コンソール エージェントがなくてもライフサイクル プランニングを表示できますが、アクションを開始す

るにはコンソール エージェントが必要です。

[2] ホーム ページで正確なメトリックを得るには、適切なサイズと構成のコンソール エージェントが必要です。

## コンソールエージェントは常に動作している必要があります

コンソール エージェントは、 NetApp Consoleの基本的な部分です。関連するエージェントが常に稼働し、動作し、アクセス可能であることを確認するのはお客様側の責任です。コンソールはエージェントの短時間の停止に対処できますが、インフラストラクチャの障害は迅速に修正する必要があります。

このドキュメントは EULA によって管理されます。ドキュメントの指示に従わずに製品を操作すると、製品の機能や EULA の権利に影響する可能性があります。

## サポートされている場所

エージェントは次の場所にインストールできます。

- Amazon Web Services
- Microsoft Azure

  管理対象のCloud Volumes ONTAPシステムと同じリージョンの Azure にコンソール エージェントをデプロイします。あるいは、 "Azure リージョン ペア" 。これにより、 Cloud Volumes ONTAPとそれに関連付けられたストレージ アカウント間で Azure Private Link 接続が使用されるようになります。 "Cloud Volumes ONTAP がAzure Private Link を使用する方法を学ぶ"

- Google Cloud

  Google Cloud でコンソールとデータサービスを使用するには、Google Cloud にエージェントをデプロイします。

- お客様の敷地内

## クラウドプロバイダーとのコミュニケーション

エージェントは、AWS、Azure、Google Cloud へのすべての通信に TLS 1.3 を使用します。

## 制限モード

コンソールを制限モードで使用するには、コンソール エージェントをインストールし、コンソール エージェント上でローカルに実行されているコンソール インターフェイスにアクセスします。

"NetApp Consoleの導入モードについて学ぶ" 。

## コンソールエージェントのインストール方法

コンソール エージェントは、コンソールから直接インストールすることも、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ことも、独自の Linux ホストまたは VCenter 環境にソフトウェアを手動でインストールすることもできます。

- "NetApp Consoleの導入モードについて学ぶ"
- "NetApp Consoleを標準モードで使い始める"

- "制限モードでNetApp Consoleを使い始める"

クラウドプロバイダーの権限

NetApp Consoleからコンソール エージェントを直接作成するには特定の権限が必要であり、コンソール エージェント自体には別の権限セットが必要です。コンソールから直接 AWS または Azure にコンソールエージェントを作成すると、コンソールは必要な権限を持つコンソールエージェントを作成します。

コンソールを標準モードで使用する場合、権限を付与する方法は、コンソール エージェントを作成する方法によって異なります。

権限の設定方法については、以下を参照してください。

- 標準モード
  - "AWS でのエージェントのインストールオプション"
  - "Azure のエージェントのインストール オプション"
  - "Google Cloud のエージェントのインストール オプション"
  - "オンプレミス展開用のクラウド権限を設定する"
- "制限モードの権限を設定する"

コンソール エージェントが日常の操作に必要な正確な権限を確認するには、次のページを参照してください。

- "コンソールエージェントがAWS権限を使用する方法を学ぶ"
- "コンソールエージェントがAzureの権限を使用する方法を学ぶ"
- "コンソール エージェントが Google Cloud 権限を使用する方法を説明します。"

以降のリリースで新しい権限が追加された場合、コンソール エージェント ポリシーを更新するのはユーザーの責任となります。リリース ノートには新しい権限がリストされています。

エージェントのアップグレード

NetApp は、機能の追加と安定性の向上のためにエージェント ソフトウェアを毎月更新します。 Cloud Volumes ONTAPやオンプレミスのONTAPクラスタ管理などの一部のコンソール機能は、コンソール エージェントのバージョンと設定に依存します。

エージェントをクラウドにインストールすると、インターネットにアクセスできる場合はコンソール エージェントが自動的に更新されます。

オペレーティングシステムと**VM**のメンテナンス

コンソール エージェント ホスト上のオペレーティング システムの保守はお客様の責任となります。たとえば、お客様側では、会社の標準的なオペレーティング システム配布手順に従って、コンソール エージェント ホスト上のオペレーティング システムにセキュリティ更新を適用する必要があります。

マイナーなセキュリティ更新を適用するときに、コンソール gent ホスト上のサービスを停止する必要がないことに注意してください。

顧客がコンソール エージェント VM を停止してから起動する必要がある場合は、クラウド プロバイダーのコ

ンソールから実行するか、オンプレミス管理の標準手順を使用して実行する必要があります。

コンソールエージェントは常に動作している必要があります 。

複数のシステムとエージェント

エージェントは複数のシステムを管理し、コンソールでデータ サービスをサポートできます。展開サイズと使用するデータ サービスに基づいて、単一のエージェントを使用して複数のシステムを管理できます。

大規模な導入の場合は、 NetApp の担当者と協力して環境のサイズを決定してください。問題が発生した場合は、 NetAppサポートにお問い合わせください。

エージェントの展開の例をいくつか示します。

- マルチクラウド環境 (AWS と Azure など) があり、AWS に 1 つのエージェントを配置し、Azure に別のエージェントを配置することを希望しています。それぞれが、それらの環境で実行されているCloud Volumes ONTAPシステムを管理します。
- サービス プロバイダーは、1 つのコンソール組織を使用して顧客にサービスを提供しながら、別の組織を使用してビジネス ユニットの 1 つに災害復旧サービスを提供する場合があります。各組織には独自のエージェントが必要です。

## コンソールエージェントを展開する

### AWS

#### AWS のコンソールエージェントのインストールオプション

AWS でコンソールエージェントを作成する方法はいくつかあります。 NetApp Console から直接行うのが最も一般的な方法です。

次のインストール オプションが利用可能です。

- "コンソールから直接コンソールエージェントを作成する"（これが標準オプションです）

  このアクションにより、選択した VPC で Linux とコンソール エージェント ソフトウェアを実行する EC2 インスタンスが起動されます。

- "AWS Marketplaceからコンソールエージェントを作成する"

  このアクションでは、Linux とコンソールエージェントソフトウェアを実行する EC2 インスタンスも起動しますが、デプロイメントはコンソールからではなく AWS Marketplace から直接開始されます。

- "自分のLinuxホストにソフトウェアをダウンロードして手動でインストールする"

選択したインストール オプションは、インストールの準備方法に影響します。これには、AWS でリソースを認証および管理するために必要な権限をコンソールに付与する方法が含まれます。

#### NetApp ConsoleからAWSにコンソールエージェントを作成する

NetApp Consoleから直接 AWS にコンソール エージェントを作成できます。コンソールから AWS にコンソールエージェントを作成する前に、ネットワークを設定し、AWS 権

## 限を準備する必要があります。

開始する前に

- あなたは"コンソールエージェントの理解"。
- 確認すべき"コンソールエージェントの制限"。

### ステップ**1: AWS**にコンソールエージェントを展開するためのネットワークを設定する

コンソール エージェントをインストールする予定のネットワークの場所が次の要件をサポートしていることを確認します。これらの要件により、コンソール エージェントはハイブリッド クラウド内のリソースとプロセスを管理できるようになります。

**VPC**とサブネット

コンソール エージェントを作成するときは、そのエージェントが存在する VPC とサブネットを指定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。

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):<br>• クラウドフォーメーション<br>• エラスティックコンピューティングクラウド (EC2)<br>• アイデンティティとアクセス管理（IAM）<br>• キー管理サービス (KMS)<br>• セキュリティトークンサービス（STS）<br>• 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" |

| エンドポイント | 目的 |
| --- | --- |
| NetApp ONTAP用の Amazon FsX:<br><br>• 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。 |
| 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<br>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。<br><br>• 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。<br><br>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" 。<br><br>• 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。 |

**NetApp**コンソールから接続されたエンドポイント

SaaS レイヤーを通じて提供される Web ベースのNetApp Consoleを使用すると、複数のエンドポイントに接続してデータ管理タスクが完了します。これには、コンソールからコンソール エージェントを展開するために接続されるエンドポイントが含まれます。

"NetAppコンソールから接続されたエンドポイントのリストを表示します" 。

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"

コンソール エージェントを作成した後、このネットワーク要件を実装する必要があります。

ステップ**2:** コンソールエージェントの**AWS**権限を設定する

コンソールは、VPC にコンソールエージェントをデプロイする前に、AWS で認証する必要があります。次のいずれかの認証方法を選択できます。

- コンソールに必要な権限を持つIAMロールを割り当てます
- 必要な権限を持つIAMユーザーにAWSアクセスキーとシークレットキーを提供します

どちらのオプションを使用する場合でも、最初のステップは IAM ポリシーを作成することです。このポリシーには、コンソールから AWS のコンソールエージェントを起動するために必要な権限のみが含まれています。

必要に応じて、IAMを使用してIAMポリシーを制限することができます。 `Condition`要素。 "AWS ドキュメント: 条件要素"

手順

1. AWS IAM コンソールに移動します。
2. *ポリシー > ポリシーの作成*を選択します。
3. 「JSON」を選択します。
4. 次のポリシーをコピーして貼り付けます。

   このポリシーには、コンソールから AWS のコンソールエージェントを起動するために必要な権限のみが含まれています。コンソールがコンソールエージェントを作成すると、コンソールエージェントが AWS リソースを管理できるようにする新しい権限セットがコンソールエージェントに適用されます。"コンソールエージェント自体に必要な権限の表示"。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
```

```
            "iam:TagRole",
            "kms:ListAliases",
            "cloudformation:ListStacks"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:TerminateInstances"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/OCCMInstance": "*"
            }
        },
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ]
    }
  ]
}
```

5. 必要に応じて、[次へ] を選択し、タグを追加します。
6. *次へ*を選択し、名前と説明を入力します。
7. *ポリシーの作成*を選択します。
8. コンソールが引き受けることができる IAM ロールまたは IAM ユーザーにポリシーをアタッチして、コンソールにアクセスキーを提供できるようにします。
   - (オプション 1) コンソールが引き受けることができる IAM ロールを設定します。
     i. ターゲットアカウントの AWS IAM コンソールに移動します。
     ii. [アクセス管理] で、**[ロール] > [ロールの作成]** を選択し、手順に従ってロールを作成します。
     iii. *信頼されたエンティティタイプ*で、*AWS アカウント*を選択します。
     iv. *別のAWSアカウント*を選択し、コンソールSaaSアカウントのIDを入力します: 952013314444
     v. 前のセクションで作成したポリシーを選択します。
     vi. ロールを作成したら、コンソール エージェントを作成するときにコンソールに貼り付けることができるように、ロール ARN をコピーします。
   - (オプション 2) コンソールにアクセスキーを提供できるように、IAM ユーザーの権限を設定します。
     i. AWS IAM コンソールから [ユーザー] を選択し、ユーザー名を選択します。
     ii. *権限の追加 > 既存のポリシーを直接添付*を選択します。
     iii. 作成したポリシーを選択します。
     iv. *次へ*を選択し、*権限の追加*を選択します。

v. IAM ユーザーのアクセスキーとシークレットキーがあることを確認します。

結果

これで、必要な権限を持つ IAM ロールまたは必要な権限を持つ IAM ユーザーが作成されているはずです。コンソールからコンソール エージェントを作成するときに、ロールまたはアクセス キーに関する情報を提供できます。

ステップ**3:** コンソールエージェントを作成する

コンソールの Web ベースのコンソールから直接コンソール エージェントを作成します。

タスク概要

- コンソールからコンソール エージェントを作成すると、デフォルト設定を使用して AWS に EC2 インスタンスがデプロイされます。コンソールエージェントを作成した後、CPU や RAM が少ない小さな EC2 インスタンスに切り替えないでください。"コンソールエージェントのデフォルト構成について学習します" 。
- コンソールがコンソール エージェントを作成すると、エージェントの IAM ロールとプロファイルが作成されます。このロールには、コンソールエージェントが AWS リソースを管理できるようにする権限が含まれています。将来のリリースで新しい権限が追加されたら、ロールが更新されるようにしてください。"コンソールエージェントのIAMポリシーの詳細"。

開始する前に

次のものが必要です:

- AWS 認証方法: 必要な権限を持つ IAM ユーザーの IAM ロールまたはアクセスキーのいずれか。
- ネットワーク要件を満たす VPC とサブネット。
- EC2 インスタンスのキーペア。
- 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。
- 設定"ネットワーク要件"。
- 設定"AWS 権限"。

手順

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 > AWS*を選択します。
3. ウィザードの手順に従ってコンソール エージェントを作成します。
4. *はじめに*ページではプロセスの概要を説明します
5. **AWS** 認証情報 ページで、AWS リージョンを指定し、認証方法 (コンソールが引き受けることができる IAM ロール、または AWS アクセスキーとシークレットキーのいずれか) を選択します。

役割を引き受ける を選択した場合は、コンソール エージェント展開ウィザードから最初の資格情報セットを作成できます。追加の資格情報セットは、「資格情報」ページから作成する必要があります。これらはウィザードのドロップダウン リストで利用できるようになります。"追加の資格情報を追加する方法を学ぶ" 。

6. *詳細*ページで、コンソール エージェントに関する詳細を入力します。
   - 名前を入力してください。
   - カスタム タグ (メタデータ) を追加します。
   - コンソールで必要な権限を持つ新しいロールを作成するか、または既存のロールを選択するかを選択します。"必要な権限" 。
   - コンソール エージェントの EBS ディスクを暗号化するかどうかを選択します。デフォルトの暗号化キーを使用するか、カスタム キーを使用するかを選択できます。
7. ネットワーク ページで、エージェントの VPC、サブネット、キーペアを指定し、パブリック IP アドレスを有効にするかどうかを選択し、必要に応じてプロキシ設定を指定します。

   コンソール エージェント仮想マシンにアクセスするための正しいキー ペアがあることを確認します。キーペアがないとアクセスできません。
8. セキュリティ グループ ページで、新しいセキュリティ グループを作成するか、必要な受信ルールと送信ルールを許可する既存のセキュリティ グループを選択するかを選択します。

   "AWS のセキュリティグループルールを表示する" 。
9. 選択内容を確認して、セットアップが正しいことを確認します。
   a. エージェント構成の検証 チェック ボックスはデフォルトでオンになっており、展開時にコンソールによってネットワーク接続要件が検証されます。コンソールがエージェントの展開に失敗した場合、トラブルシューティングに役立つレポートが提供されます。デプロイメントが成功した場合、レポートは提供されません。

   まだ使用している場合は"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、チェックボックスをオフにして検証チェックをスキップします。
10. *追加*を選択します。

    コンソールは約 10 分でエージェントを展開します。プロセスが完了するまでこのページに留まります。

結果

プロセスが完了すると、コンソール エージェントはコンソールから使用できるようになります。

デプロイメントが失敗した場合は、コンソールからレポートとログをダウンロードして、問題の解決に役立てることができます。"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。"

コンソールエージェントを作成したのと同じ AWS アカウントに Amazon S3 バケットがある場合は、システム ページに Amazon S3 作業環境が自動的に表示されます。 "NetApp Consoleから S3 バケットを管理する方法を学びます"

**AWS Marketplace**からコンソールエージェントを作成する

## AWS Marketplace から直接 AWS にコンソールエージェントを作成します。 AWS

Marketplace からコンソールエージェントを作成するには、ネットワークを設定し、AWS のアクセス許可を準備し、インスタンスの要件を確認してから、コンソールエージェントを作成する必要があります。

開始する前に

- あなたは"コンソールエージェントの理解"。
- 確認すべき"コンソールエージェントの制限"。

ステップ**1:** ネットワークを設定する

ハイブリッド クラウド リソースを管理するには、コンソール エージェントのネットワークの場所が次の要件を満たしていることを確認します。

**VPC**とサブネット

コンソール エージェントを作成するときは、そのエージェントが存在する VPC とサブネットを指定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。

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):<br>• クラウドフォーメーション<br>• エラスティックコンピューティングクラウド (EC2)<br>• アイデンティティとアクセス管理（IAM）<br>• キー管理サービス (KMS)<br>• セキュリティトークンサービス（STS）<br>• 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" |

| エンドポイント | 目的 |
| --- | --- |
| NetApp ONTAP用の Amazon FsX:<br><br>• 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。 |
| 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<br>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。<br><br>• 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。<br><br>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" 。<br><br>• 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"

コンソール エージェントを作成した後、このネットワーク アクセスを実装します。

ステップ**2: AWS**権限を設定する

マーケットプレイスの展開を準備するには、AWS で IAM ポリシーを作成し、それを IAM ロールにアタッチします。 AWS Marketplace からコンソールエージェントを作成すると、その IAM ロールを選択するように求められます。

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 サービスに基づいて、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 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、AWS Marketplace からのデプロイ時に EC2 インスタンスに関連付けることができる IAM ロールが作成されました。

ステップ**3:** インスタンス要件を確認する

コンソールエージェントを作成するときは、次の要件を満たす EC2 インスタンスタイプを選択する必要があります。

**CPU**

8コアまたは8vCPU

**RAM**

32 GB

**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。

ステップ**4:** コンソールエージェントを作成する

AWS Marketplace から直接コンソールエージェントを作成します。

タスク概要

AWS Marketplace からコンソールエージェントを作成すると、デフォルト設定を使用して AWS に EC2 インスタンスがデプロイされます。"コンソールエージェントのデフォルト構成について学習します" 。

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 VPC とサブネット。
- 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。
- 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。
- インスタンスの CPU および RAM 要件を理解すること。
- 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。

  AWS は指定された設定でコンソールエージェントを起動し、コンソールエージェントは約 10 分で実行されます。

  インストールが失敗した場合は、トラブルシューティングに役立つログとレポートを表示できます。"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。"

8. コンソール エージェント仮想マシンに接続しているホストとコンソール エージェントの URL から Web ブラウザーを開きます。
9. ログイン後、コンソール エージェントを設定します。
   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。

      コンソールを標準モードで使用するには、制限モードを無効にしておきます。安全な環境があり、このアカウントをコンソールのバックエンド サービスから切断する場合にのみ、制限モードを有効にする必要があります。もしそうなら、"NetApp Consoleを制限モードで使い始めるための手順" 。
   d. *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。

ウェブブラウザを開いて、 "NetApp Console"コンソールでコンソール エージェントの使用を開始します。

コンソールエージェントを作成したのと同じ AWS アカウントに Amazon S3 バケットがある場合は、システム ページに Amazon S3 作業環境が自動的に表示されます。 "NetApp Consoleから S3 バケットを管理する方法を学びます"

**AWS**にコンソールエージェントを手動でインストールする

# AWS で実行されている 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。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には、ホスト要件を確認し、ネットワークを設定し、AWS 権限を準備し、コンソールエージェントをインストールして、準備した権限を付与する必要があります。

開始する前に

- あなたは"コンソールエージェントの理解"。
- 確認すべき"コンソールエージェントの制限"。

ステップ**1:** ホストの要件を確認する

コンソール エージェント ソフトウェアを実行しているホストが、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していることを確認します。

> 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。

**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。

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<br>• 英語版のみ。<br>• 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。<br>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<br>• 英語版のみ。<br>• 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。<br>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<br>• 英語版のみ。<br>• 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。<br>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 |

鍵ペア

コンソールエージェントを作成するときは、インスタンスで使用する EC2 キーペアを選択する必要があります。

**IMDSv2** 使用時の **PUT** 応答ホップ制限

IMDSv2 が有効になっている場合 (新しい EC2 インスタンスのデフォルト)、PUT 応答ホップ制限を 3 に設定します。そうしないと、エージェントのセットアップ中に UI 初期化エラーが表示されます。

- "Amazon EC2 インスタンスで IMDSv2 の使用を必須にする"
- "AWSドキュメント: PUTレスポンスのホップ制限を変更する"

ステップ**2: 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
```

ステップ**3:** ネットワークを設定する

コンソール エージェントがハイブリッド クラウド内のリソースを管理できるように、ネットワークの場所が次の要件をサポートし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。

| エンドポイント | 目的 |
| --- | --- |
| AWS サービス (amazonaws.com):<br>• クラウドフォーメーション<br>• エラスティックコンピューティングクラウド (EC2)<br>• アイデンティティとアクセス管理（IAM）<br>• キー管理サービス (KMS)<br>• セキュリティトークンサービス（STS）<br>• 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" |

| エンドポイント | 目的 |
| --- | --- |
| NetApp ONTAP用の Amazon FsX:<br><br>• 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。 |
| 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<br>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。<br><br>• 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。<br><br>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" 。<br><br>• 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"

ステップ**4:** コンソールの**AWS**権限を設定する

次のいずれかのオプションを使用して、 NetApp Consoleに AWS 権限を付与します。

- オプション 1: IAM ポリシーを作成し、EC2 インスタンスに関連付けることができる IAM ロールにポリシーをアタッチします。
- オプション 2: 必要な権限を持つ IAM ユーザーの AWS アクセスキーをコンソールに提供します。

コンソールの権限を準備するには、手順に従ってください。

**IAM**のロール

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 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

コンソールエージェントをインストールした後、EC2 インスタンスに関連付けることができる IAM ロールが作成されます。

**AWS** アクセスキー

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 ユーザーと、コンソールに提供できるアクセス キーが作成されました。

ステップ**5:** コンソールエージェントをインストールする

前提条件を満たしたら、Linux ホストにソフトウェアを手動で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。

◦ 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。

2. インストールが完了するまでお待ちください。

   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。

   インストールが失敗した場合は、インストール レポートとログを表示して問題の解決に役立てることができます。"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。"

1. コンソール エージェント仮想マシンに接続しているホストから Web ブラウザを開き、次の URL を入力します。

   <a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

2. ログイン後、コンソール エージェントを設定します。

   a. コンソール エージェントに関連付ける組織を指定します。

   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。

      以下の手順ではコンソールを標準モードで使用する方法について説明しているため、制限モードは無効にしておく必要があります。安全な環境があり、このアカウントをバックエンド サービスから切断する場合にのみ、制限モードを有効にする必要があります。もしそうなら、"NetApp Consoleを制限モードで使い始めるための手順に従います" 。

d. *始めましょう*を選択します。

コンソールエージェントを作成したのと同じ AWS アカウントに Amazon S3 バケットがある場合は、[システム] ページに Amazon S3 ストレージ システムが自動的に表示されます。 "NetApp ConsolePからS3バケットを管理する方法を学ぶ"

ステップ**6: NetApp Console**に権限を付与する

コンソールエージェントをインストールした後、コンソールエージェントが AWS 内のデータとストレージインフラストラクチャを管理できるように、設定した AWS 権限を提供します。

**IAM**のロール

作成した IAM ロールをコンソールエージェント EC2 インスタンスにアタッチします。

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。

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

**AWS** アクセスキー

必要な権限を持つ IAM ユーザーの AWS アクセスキーをコンソールに提供します。

手順

1. コンソールで正しいコンソール エージェントが現在選択されていることを確認します。
2. *管理 > 資格情報*を選択します。
3. *組織の資格情報*を選択します。
4. *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。

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

**Azure**

**Azure** のコンソール エージェントのインストール オプション

# Azure でコンソール エージェントを作成するには、いくつかの方法があります。NetApp Consoleから直接行うのが最も一般的な方法です。

次のインストール オプションが利用可能です。

- "NetApp Consoleから直接コンソールエージェントを作成する"（これが標準オプションです）

  このアクションにより、選択した VNet で Linux とコンソール エージェント ソフトウェアを実行する VM が起動します。

- "Azure Marketplace からコンソール エージェントを作成する"

  このアクションでは、Linux とコンソール エージェント ソフトウェアを実行する VM も起動しますが、展開はコンソールからではなく、Azure Marketplace から直接開始されます。

- "自分のLinuxホストにソフトウェアをダウンロードして手動でインストールする"

選択したインストール オプションは、インストールの準備方法に影響します。これには、Azure でリソースを認証および管理するために必要なアクセス許可をコンソール エージェントに付与する方法が含まれます。

**NetApp Console**から **Azure** にコンソール エージェントを作成する

# NetApp Consoleから Azure にコンソール エージェントを作成するには、ネットワークを設定し、Azure 権限を準備してから、コンソール エージェントを作成する必要があります。

開始する前に

- あなたは"コンソールエージェントの理解"。
- 確認すべき"コンソールエージェントの制限"。

ステップ**1:** ネットワークを設定する

コンソール エージェントをインストールする予定のネットワークの場所が次の要件をサポートしていることを確認します。これらの要件により、コンソール エージェントはハイブリッド クラウド リソースを管理できるようになります。

**Azure**リージョン

Cloud Volumes ONTAPを使用する場合、コンソールエージェントは、管理するCloud Volumes ONTAPシステムと同じAzureリージョン、または "Azure リージョン ペア"Cloud Volumes ONTAPシステム用。この要件により、 Cloud Volumes ONTAPとそれに関連付けられたストレージ アカウント間で Azure Private Link 接続が使用されるようになります。

"Cloud Volumes ONTAP がAzure Private Link を使用する方法を学ぶ"

**VNet**とサブネット

コンソール エージェントを作成するときは、そのエージェントが存在する VNet とサブネットを指定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。

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 |
| --- | --- |
| 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。 |
| 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<br>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。<br><br>• 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。<br><br>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" 。<br><br>• 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。 |

**NetApp**コンソールから接続されたエンドポイント

SaaS レイヤーを通じて提供される Web ベースのNetApp Consoleを使用すると、複数のエンドポイントに接続してデータ管理タスクが完了します。これには、コンソールからコンソール エージェントを展開するために接続されるエンドポイントが含まれます。

"NetAppコンソールから接続されたエンドポイントのリストを表示します" 。

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"

コンソール エージェントを作成した後、このネットワーク要件を実装する必要があります。

ステップ **2:** コンソール エージェント展開ポリシー **(**カスタム ロール**)** を作成する

Azure にコンソール エージェントをデプロイする権限を持つカスタム ロールを作成する必要があります。

Azure アカウントまたは Microsoft Entra サービス プリンシパルに割り当てることができる Azure カスタム ロールを作成します。コンソールは Azure で認証し、これらのアクセス許可を使用してユーザーに代わってコンソール エージェントを作成します。

コンソールはAzureにコンソールエージェントVMを展開し、 "システム割り当てマネージドID"必要なロールを作成し、それを VM に割り当てます。"コンソールが権限をどのように使用するかを確認します" 。

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"

手順

1. Azure の新しいカスタム ロールに必要なアクセス許可をコピーし、JSON ファイルに保存します。

   このカスタム ロールには、コンソールから Azure のコンソール エージェント VM を起動するために必要なアクセス許可のみが含まれています。このポリシーを他の状況では使用しないでください。コンソールは、コンソール エージェントを作成するときに、コンソール エージェントが Azure リソースを管理できるようにする新しいアクセス許可セットをコンソール エージェント VM に適用します。

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
```

```
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/subnets/read",
    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Network/publicIPAddresses/read",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/read",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/rea
d",
    "Microsoft.Network/networkInterfaces/ipConfigurations/read",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Resources/deployments/validate/action",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/operationresults/read",
    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Authorization/roleDefinitions/write",
```

```
    "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Authorization/roleAssignments/read"
  ],
  "NotActions": [],
  "AssignableScopes": [],
  "Description": "Azure SetupAsService",
  "IsCustom": "true"
}
```

2. 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 を変更します。

   例

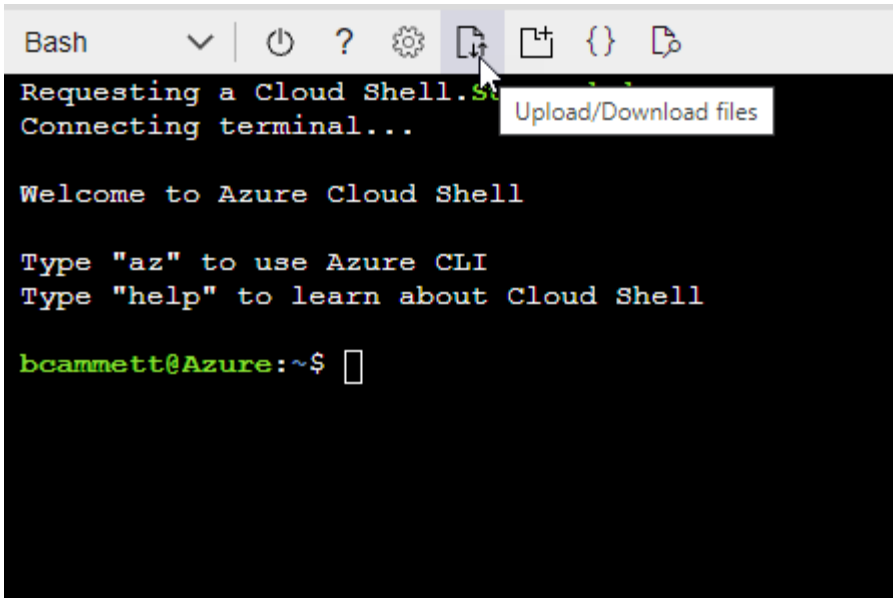
```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
]
```

3. 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. 次の Azure CLI コマンドを入力します。

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

これで、*Azure SetupAsService* というカスタム ロールが作成されました。このカスタム ロールは、ユーザー アカウントまたはサービス プリンシパルに適用できます。

ステップ**3:** 認証を設定する

コンソールからコンソール エージェントを作成するときは、コンソールが Azure で認証して VM をデプロイできるようにするためのログインを提供する必要があります。次の 2 つのオプションがあります。

1. プロンプトが表示されたら、Azure アカウントでSign in。このアカウントには特定の Azure 権限が必要です。これがデフォルトのオプションです。
2. Microsoft Entra サービス プリンシパルに関する詳細を提供します。このサービス プリンシパルには特定のアクセス許可も必要です。

コンソールで使用するために、これらの認証方法のいずれかを準備するには、手順に従ってください。

**Azure**アカウント

コンソールからコンソール エージェントを展開するユーザーにカスタム ロールを割り当てます。

手順

1. Azure ポータルで、サブスクリプション サービスを開き、ユーザーのサブスクリプションを選択します。
2. アクセス制御 **(IAM)** をクリックします。
3. 追加 > ロール割り当ての追加 をクリックし、権限を追加します。
   a. **Azure SetupAsService** ロールを選択し、次へ をクリックします。

   Azure SetupAsService は、Azure のコンソール エージェント展開ポリシーで提供される既定の名前です。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。

   b. *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。
   c. *メンバーを選択*をクリックし、ユーザーアカウントを選択して*選択*をクリックします。
   d. *次へ*をクリックします。
   e. *レビュー+割り当て*をクリックします。

サービスプリンシパル

Azure アカウントでログインするのではなく、必要な権限を持つ Azure サービス プリンシパルの資格情報をコンソールに提供できます。

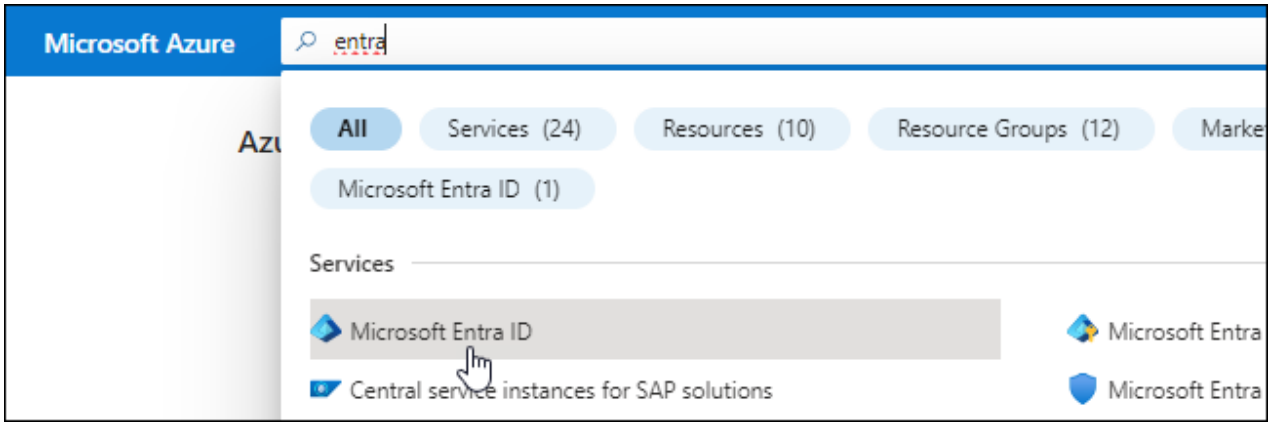
Microsoft Entra ID でサービス プリンシパルを作成して設定し、コンソールに必要な Azure 資格情報を取得します。

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。

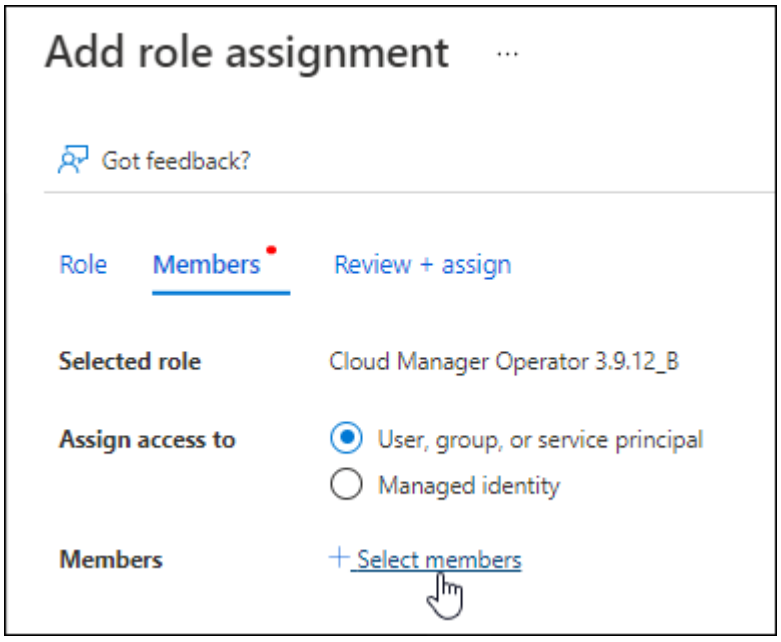


3. メニューで*アプリ登録*を選択します。
4. *新規登録*を選択します。
5. アプリケーションの詳細を指定します。
   - 名前: アプリケーションの名前を入力します。
   - アカウント タイプ: アカウント タイプを選択します (いずれのタイプもNetApp Consoleで使用できます)。
   - リダイレクト **URI**: このフィールドは空白のままにすることができます。
6. *登録*を選択します。

   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。

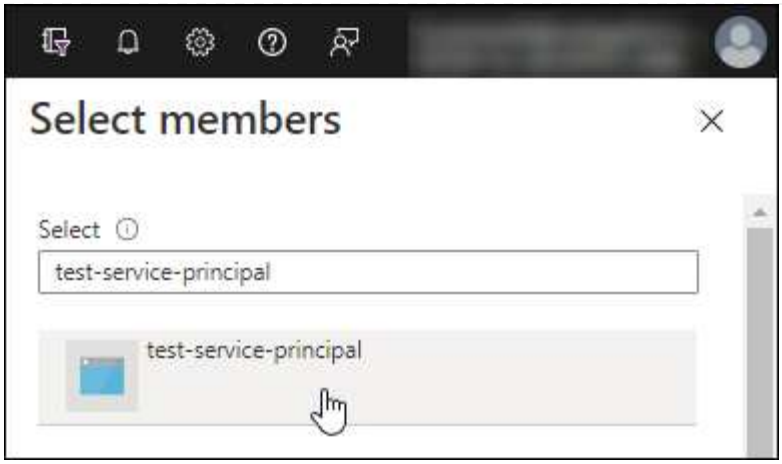
アプリケーションにカスタムロールを割り当てる

1. 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。
2. サブスクリプションを選択します。
3. アクセス制御 **(IAM) >** 追加 **>** ロール割り当ての追加 をクリックします。
4. *役割*タブで、*コンソールオペレーター*役割を選択し、*次へ*をクリックします。
5. *メンバー*タブで、次の手順を実行します。
   a. *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。
   b. *メンバーを選択*をクリックします。




   c. 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。




a. アプリケーションを選択し、「選択」をクリックします。

b. *次へ*をクリックします。

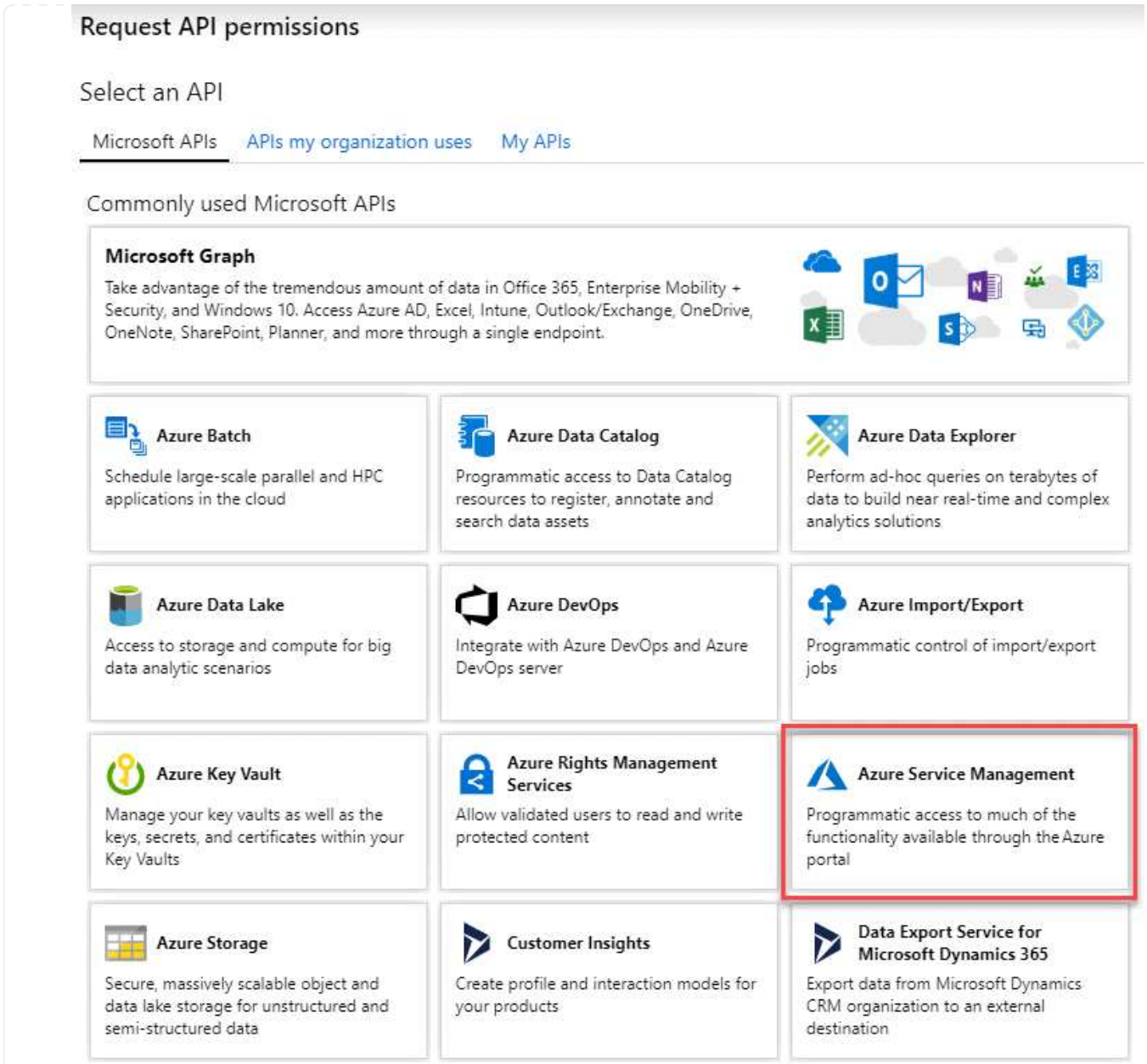
6. *レビュー+割り当て*をクリックします。

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。

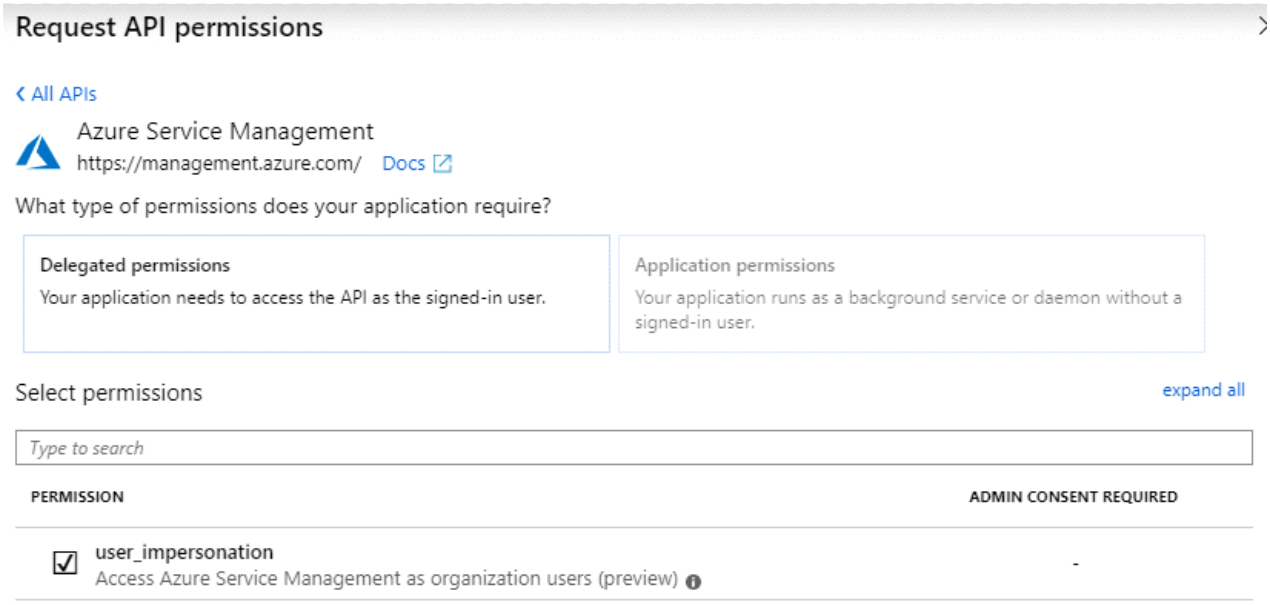
複数の Azure サブスクリプションのリソースを管理する場合は、サービス プリンシパルを各サブスクリプションにバインドする必要があります。たとえば、コンソールを使用すると、 Cloud Volumes ONTAPをデプロイするときに使用するサブスクリプションを選択できます。

**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。

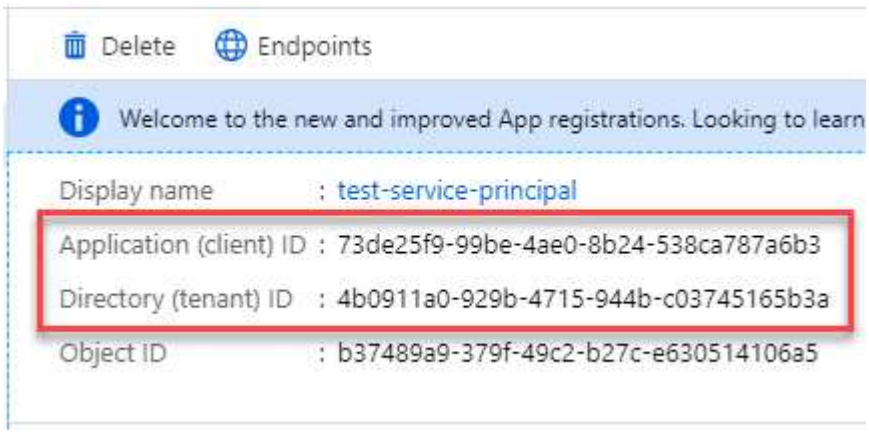



4. 組織ユーザーとして **Azure** サービス管理にアクセスする を選択し、権限の追加 を選択します。




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。コンソール エージェントを作成するときに、この情報をコンソールに入力する必要があります。

ステップ**4:** コンソールエージェントを作成する

NetApp Consoleから直接コンソール エージェントを作成します。

タスク概要

- コンソールからコンソール エージェントを作成すると、既定の構成を使用して Azure に仮想マシンがデプロイされます。コンソール エージェントを作成した後、CPU や RAM が少ない小さな VM インスタンスに切り替えないでください。"コンソールエージェントのデフォルト構成について学習します" 。
- コンソールはコンソール エージェントを展開するときに、カスタム ロールを作成し、それをコンソール エージェント VM に割り当てます。このロールには、コンソール エージェントが Azure リソースを管理できるようにする権限が含まれています。後続のリリースで新しい権限が追加されるので、ロールが最新の状態に保たれ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のカスタムロールの詳細" 。

開始する前に

次のものが必要です:

- Azure サブスクリプション。
- 選択した Azure リージョン内の VNet とサブネット。
- 組織ですべての送信インターネット トラフィックにプロキシが必要な場合のプロキシ サーバーの詳細:
  - IPアドレス
  - Credentials
  - HTTPS証明書
- コンソール エージェント仮想マシンにその認証方法を使用する場合は、SSH 公開キー。認証方法のもう 1 つのオプションは、パスワードを使用することです。

  "Azure の Linux VM への接続について学習します"

- コンソールエージェント用のAzureロールをコンソールが自動的に作成しないようにするには、独自のロールを作成する必要があります。"このページのポリシーを使用する" 。

  これらの権限は、コンソール エージェント自体に適用されます。これは、コンソール エージェント VM を展開するために以前に設定した権限セットとは異なります。

手順

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 > Azure*を選択します。
3. レビュー ページで、エージェントを展開するための要件を確認します。これらの要件についてはこのページの上部にも詳しく記載されています。
4. *仮想マシン認証*ページで、Azure のアクセス許可の設定方法に一致する認証オプションを選択します。
   - ログイン を選択して、必要な権限を持つ Microsoft アカウントにログインします。

     このフォームは Microsoft によって所有およびホストされています。資格情報がNetAppに提供されていません。

     すでに Azure アカウントにログインしている場合は、コンソールは自動的にそのアカウントを使用します。複数のアカウントをお持ちの場合は、正しいアカウントを使用していることを確認するために、最初にログアウトする必要がある場合があります。

   - 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するには、**Active Directory** サービス プリンシパル を選択します。
     - 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

   サービスプリンシパルのこれらの値を取得する方法を学びます 。
5. 仮想マシン認証 ページで、Azure サブスクリプション、場所、新しいリソース グループまたは既存のリソース グループを選択し、作成するコンソール エージェント仮想マシンの認証方法を選択します。

   仮想マシンの認証方法は、パスワードまたは SSH 公開キーです。

   "Azure の Linux VM への接続について学習します"
6. *詳細*ページで、エージェントの名前を入力し、タグを指定して、コンソールで必要な権限を持つ新しいロールを作成するか、または既存のロールを選択するかを選択します。"必要な権限" 。

   このロールに関連付けられた Azure サブスクリプションを選択できることに注意してください。選択した各サブスクリプションは、そのサブスクリプション内のリソースを管理するためのコンソール エージェント権限を付与します (たとえば、 Cloud Volumes ONTAP)。
7. ネットワーク ページで、VNet とサブネットを選択し、パブリック IP アドレスを有効にするかどうかを選択し、必要に応じてプロキシ構成を指定します。
   - セキュリティ グループ ページで、新しいセキュリティ グループを作成するか、必要な受信ルールと送信ルールを許可する既存のセキュリティ グループを選択するかを選択します。

     "Azure のセキュリティ グループ ルールを表示する" 。
8. 選択内容を確認して、セットアップが正しいことを確認します。
   a. エージェント構成の検証 チェック ボックスはデフォルトでオンになっており、展開時にコンソールによってネットワーク接続要件が検証されます。コンソールがエージェントの展開に失敗した場合、ト

ラブルシューティングに役立つレポートが提供されます。デプロイメントが成功した場合、レポートは提供されません。

まだ使用している場合は"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、チェックボックスをオフにして検証チェックをスキップします。

9. *追加*を選択します。

コンソールは約 10 分でエージェントを準備します。プロセスが完了するまでこのページに留まります。

結果

プロセスが完了すると、コンソール エージェントはコンソールから使用できるようになります。

デプロイメントが失敗した場合は、コンソールからレポートとログをダウンロードして、問題の解決に役立てることができます。"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。"

コンソール エージェントを作成したのと同じ Azure アカウントに Azure Blob ストレージがある場合は、システム ページに Azure Blob ストレージが自動的に表示されます。 "NetApp Consoleから Azure Blob ストレージを管理する方法を学びます"

#### Azure Marketplace からコンソール エージェントを作成する

## Azure Marketplace から直接、Azure にコンソール エージェントを作成できます。Azure Marketplace からコンソール エージェントを作成するには、ネットワークを設定し、Azure のアクセス許可を準備し、インスタンスの要件を確認してから、コンソール エージェントを作成する必要があります。

開始する前に

- あなたは"コンソールエージェントの理解"。
- レビュー"コンソールエージェントの制限"。

ステップ**1:** ネットワークを設定する

コンソール エージェントをインストールする予定のネットワークの場所が次の要件をサポートしていることを確認します。これらの要件により、コンソール エージェントはハイブリッド クラウド内のリソースを管理できるようになります。

**Azure**リージョン

Cloud Volumes ONTAPを使用する場合、コンソールエージェントは、管理するCloud Volumes ONTAPシステムと同じAzureリージョン、または "Azure リージョン ペア"Cloud Volumes ONTAPシステム用。この要件により、 Cloud Volumes ONTAPとそれに関連付けられたストレージ アカウント間で Azure Private Link 接続が使用されるようになります。

"Cloud Volumes ONTAP がAzure Private Link を使用する方法を学ぶ"

**VNet**とサブネット

コンソール エージェントを作成するときは、そのエージェントが存在する VNet とサブネットを指定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。

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 |
| --- | --- |
| 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。 |
| 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<br>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。<br><br>• 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。<br><br>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" 。<br><br>• 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"

コンソール エージェントを作成した後、ネットワーク要件を実装します。

ステップ**2: VM**の要件を確認する

コンソール エージェントを作成するときは、次の要件を満たす仮想マシンの種類を選択します。

**CPU**

8コアまたは8vCPU

**RAM**

32 GB

**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。

ステップ**3:** 権限を設定する

権限は次の方法で付与できます。

- オプション 1: システム割り当てマネージド ID を使用して、Azure VM にカスタム ロールを割り当てます。
- オプション 2: 必要な権限を持つ Azure サービス プリンシパルの資格情報をコンソールに提供します。

コンソールの権限を設定するには、次の手順に従います。

カスタムロール

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。

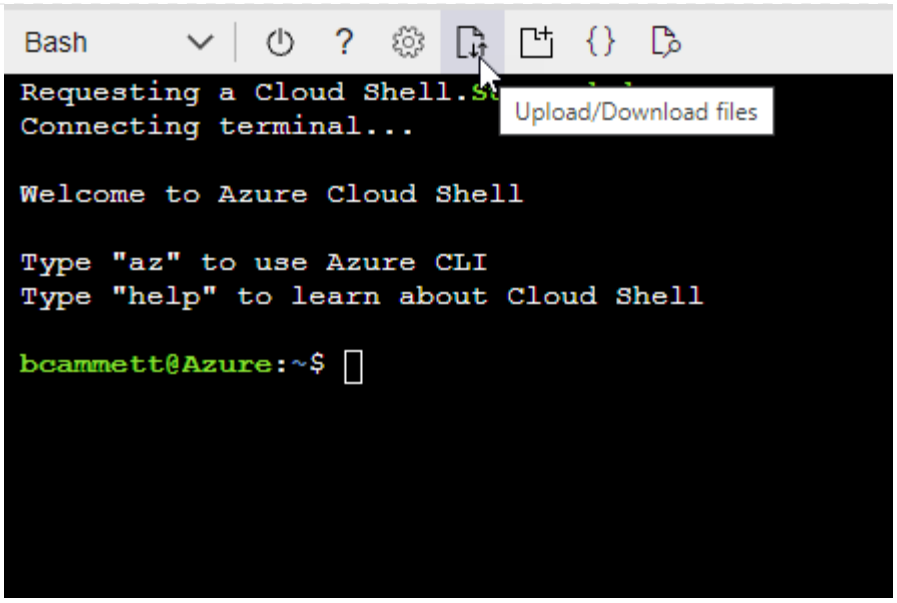
   例

   ```
   "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
```

サービスプリンシパル

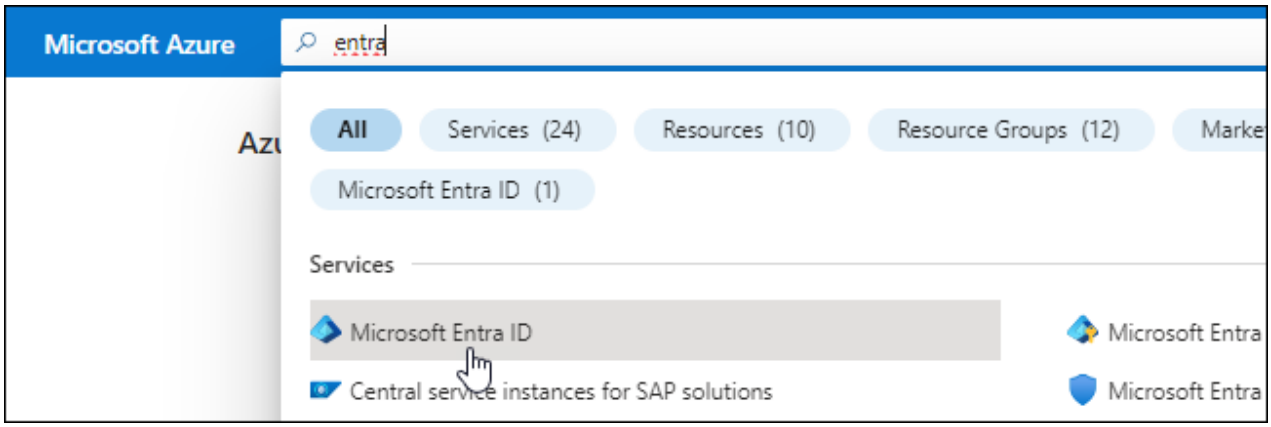
Microsoft Entra ID でサービス プリンシパルを作成して設定し、コンソールに必要な Azure 資格情報を取得します。

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。

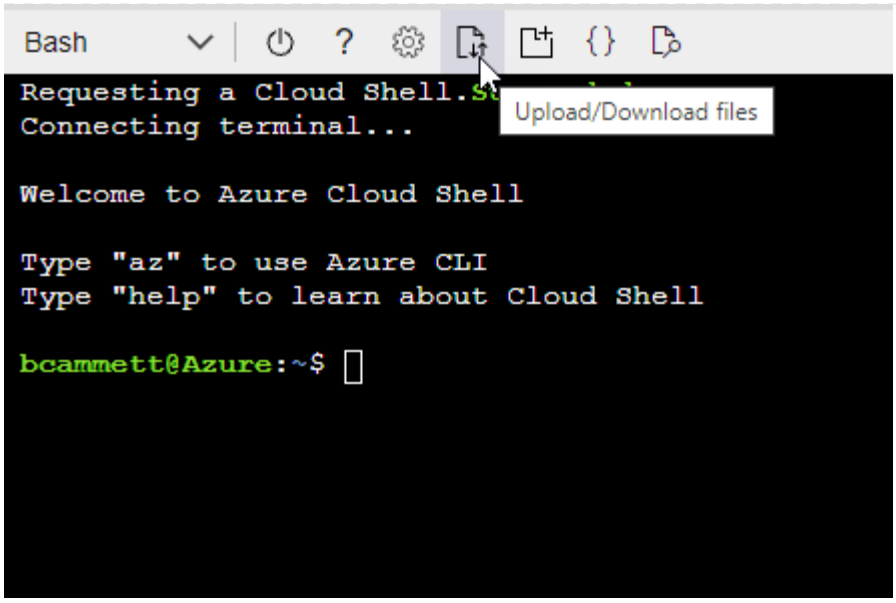
      例

      ```
      "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。

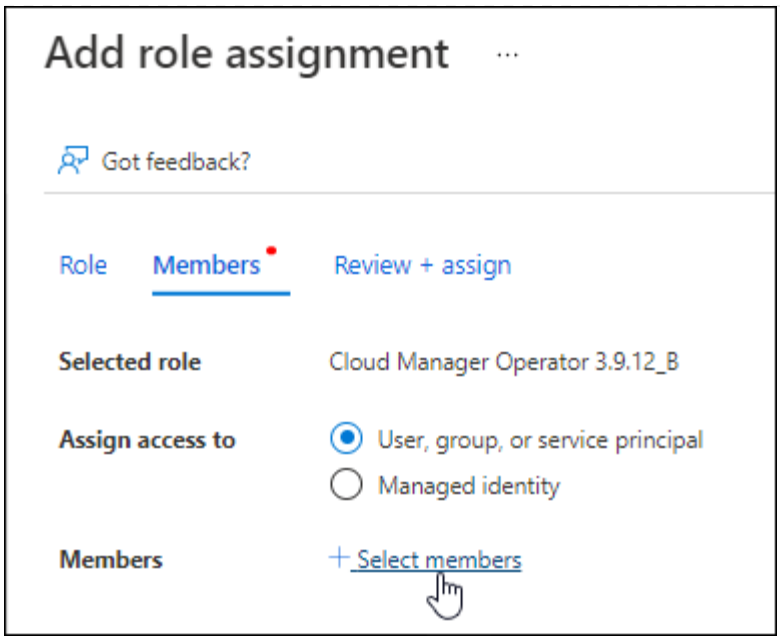
b. サブスクリプションを選択します。

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。

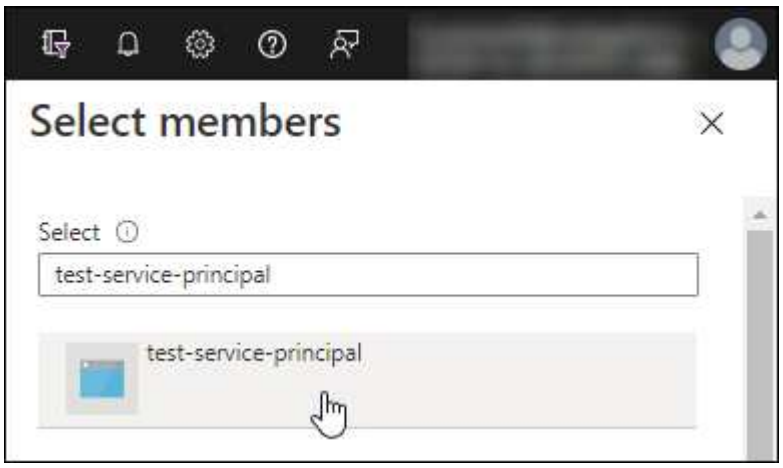
e. *メンバー*タブで、次の手順を実行します。

- *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。

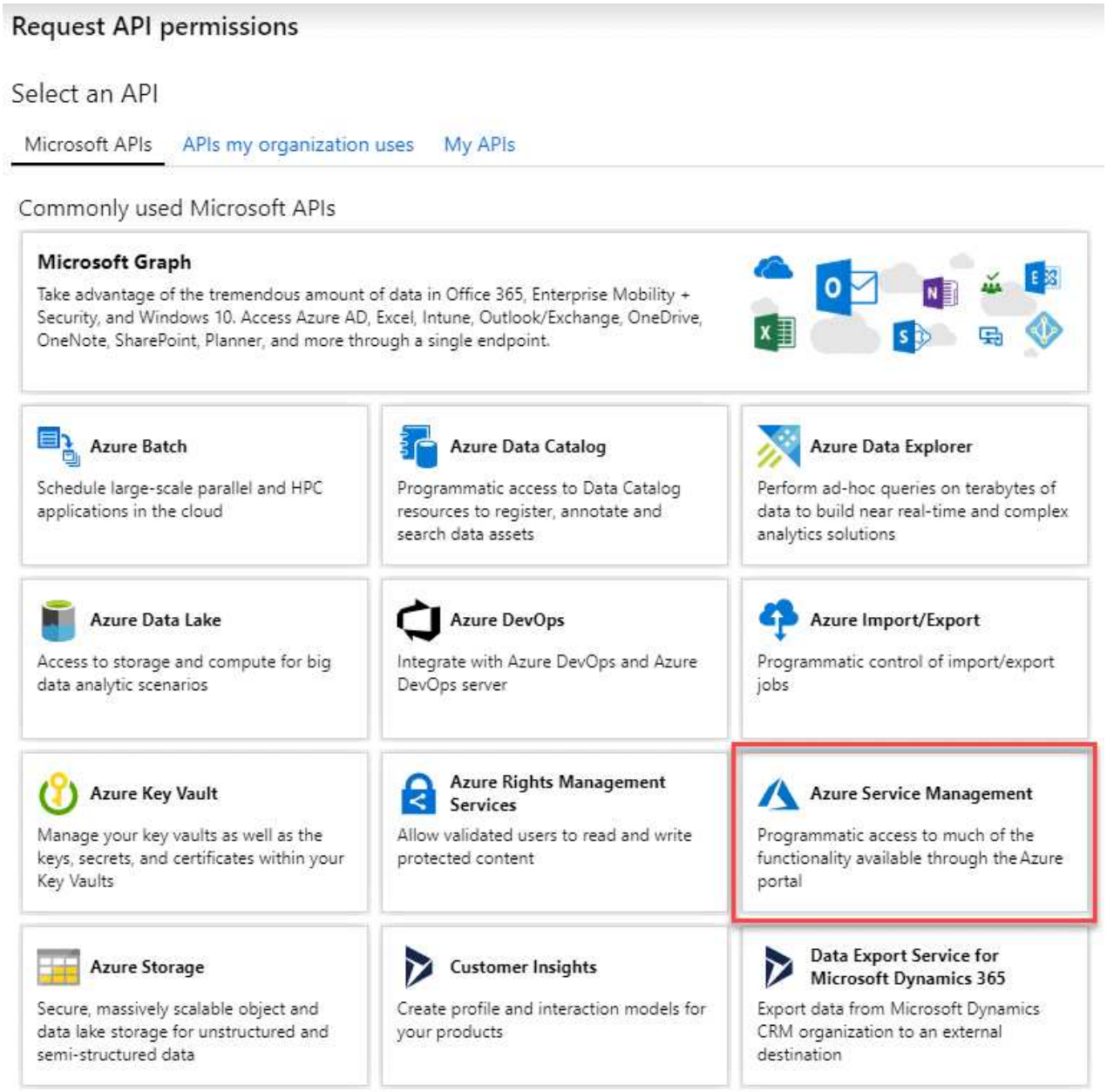
これで、サービス プリンシパルに、コンソール エージェントをデプロイするために必要な Azure アクセス許可が付与されました。

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。

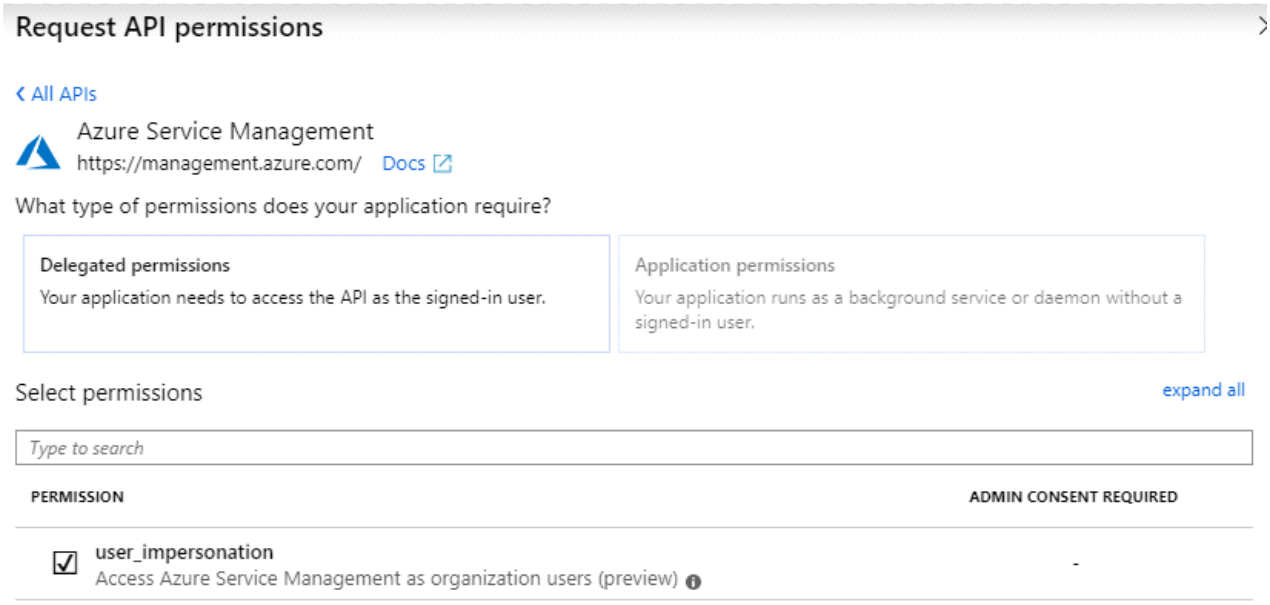
**Windows Azure** サービス管理 **API** 権限を追加する

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。

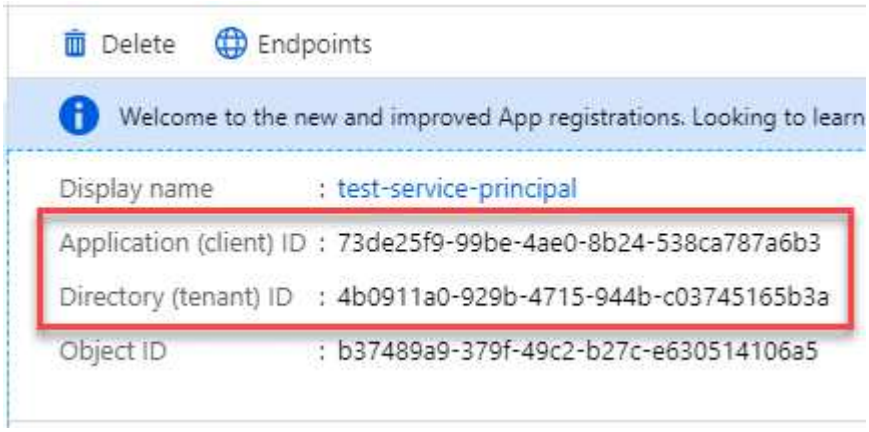



4. 組織ユーザーとして **Azure** サービス管理にアクセスする を選択し、権限の追加 を選択します。




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

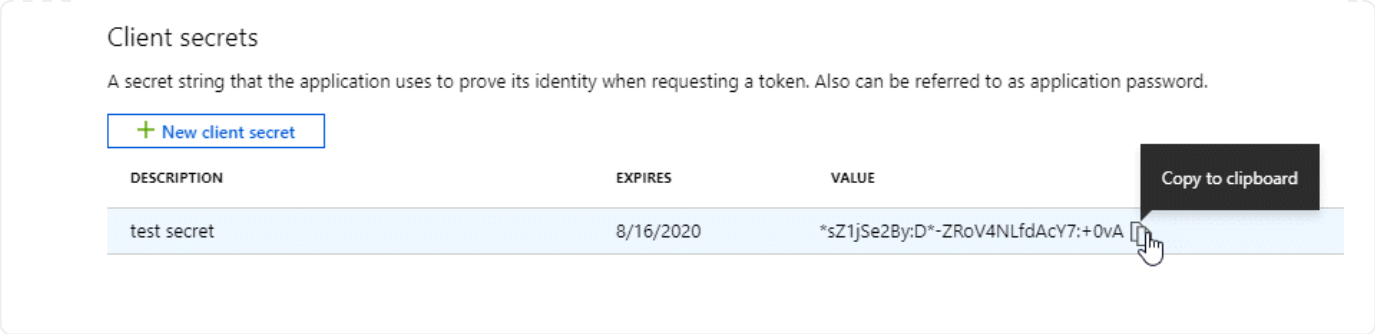
1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. アプリケーション **(**クライアント**) ID** と ディレクトリ **(**テナント**) ID** をコピーします。




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。




ステップ**4:** コンソールエージェントを作成する

Azure Marketplace からコンソール エージェントを直接起動します。

タスク概要

Azure Marketplace からコンソール エージェントを作成すると、既定の構成で仮想マシンが設定されます。"コンソールエージェントのデフォルト構成について学習します" 。

開始する前に

次のものが必要です:

- Azure サブスクリプション。
- 選択した Azure リージョン内の VNet とサブネット。
- 組織ですべての送信インターネット トラフィックにプロキシが必要な場合のプロキシ サーバーの詳細:
  - IPアドレス
  - Credentials
  - HTTPS証明書
- コンソール エージェント仮想マシンにその認証方法を使用する場合は、SSH 公開キー。認証方法のもう 1 つのオプションは、パスワードを使用することです。

  "Azure の Linux VM への接続について学習します"

- コンソールエージェント用のAzureロールをコンソールが自動的に作成しないようにするには、独自のロールを作成する必要があります。"このページのポリシーを使用する" 。

  これらの権限は、コンソール エージェント インスタンス自体に適用されます。これは、コンソール エージェント VM を展開するために以前に設定した権限セットとは異なります。

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"

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。
- 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。

  この設定は重要です。マネージド ID を使用すると、コンソール エージェント仮想マシンは資格情報を提供せずに Microsoft Entra ID に対して自身を識別できるためです。 "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。

   Azure は指定された設定で仮想マシンをデプロイします。約 10 分以内に仮想マシンとコンソール エージェント ソフトウェアが実行されるはずです。

   インストールが失敗した場合は、トラブルシューティングに役立つログとレポートを表示できます。"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。"

5. コンソール エージェント仮想マシンに接続しているホストから Web ブラウザを開き、次の URL を入力します。

   <a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

6. ログイン後、コンソール エージェントを設定します。
   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。

      コンソールを標準モードで使用するには、制限モードを無効にしておきます。安全な環境があり、このアカウントをコンソールのバックエンド サービスから切断する場合にのみ、制限モードを有効にする必要があります。もしそうなら、"制限モードでコンソールを開始するには、以下の手順に従ってください。" 。

   d. *始めましょう*を選択します。

結果

これで、コンソール エージェントがインストールされ、コンソール組織で設定されました。

コンソール エージェントを作成したのと同じ Azure サブスクリプションに Azure Blob ストレージがある場合は、システム ページに Azure Blob ストレージ システムが自動的に表示されます。 "コンソールから Azure Blob ストレージを管理する方法を学びます"

ステップ**5:** コンソールエージェントに権限を付与する

コンソール エージェントを作成したので、以前に設定した権限をエージェントに付与する必要があります。権限を付与すると、コンソール エージェントは Azure 内のデータとストレージ インフラストラクチャを管理できるようになります。

カスタムロール

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。

次の手順

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

サービスプリンシパル

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。

**Azure** にコンソール エージェントを手動でインストールする

# 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には、ホストの要件を確認し、ネットワークを設定し、Azure のアクセス許可を準備し、コンソール エージェントをインストールして、準備したアクセス許可を付与する必要があります。

開始する前に

- あなたは"コンソールエージェントの理解"。
- 確認すべき"コンソールエージェントの制限"。

ステップ**1:** ホストの要件を確認する

コンソール エージェント ソフトウェアは、特定のオペレーティング システム要件、RAM 要件、ポート要件などを満たすホスト上で実行する必要があります。

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。

**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。

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<br>• 英語版のみ。<br>• 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。<br>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<br>• 英語版のみ。<br>• 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。<br>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<br>• 英語版のみ。<br>• 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。<br>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**2: 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 **2.** 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**3:** ネットワークを設定する

コンソール エージェントをインストールする予定のネットワークの場所が次の要件をサポートしていることを確認します。これらの要件を満たすことで、コンソール エージェントはハイブリッド クラウド環境内のリソースとプロセスを管理できるようになります。

**Azure**リージョン

Cloud Volumes ONTAPを使用する場合、コンソールエージェントは、管理するCloud Volumes ONTAPシステムと同じAzureリージョン、または "Azure リージョン ペア"Cloud Volumes ONTAPシステム用。この要件により、 Cloud Volumes ONTAPとそれに関連付けられたストレージ アカウント間で Azure Private Link 接続が使用されるようになります。

"Cloud Volumes ONTAP がAzure Private Link を使用する方法を学ぶ"

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。

| 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.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://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。<br><br>• 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。<br><br>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" 。<br><br>• 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"

ステップ**4:** コンソールエージェントの展開権限を設定する

次のいずれかのオプションを使用して、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。

- オプション 1: システム割り当てマネージド ID を使用して、Azure VM にカスタム ロールを割り当てます。
- オプション 2: 必要なアクセス許可を持つ Azure サービス プリンシパルの資格情報をコンソール エージェントに提供します。

手順に従って、コンソール エージェントの権限を準備します。

コンソールエージェントの展開用のカスタムロールを作成する

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。

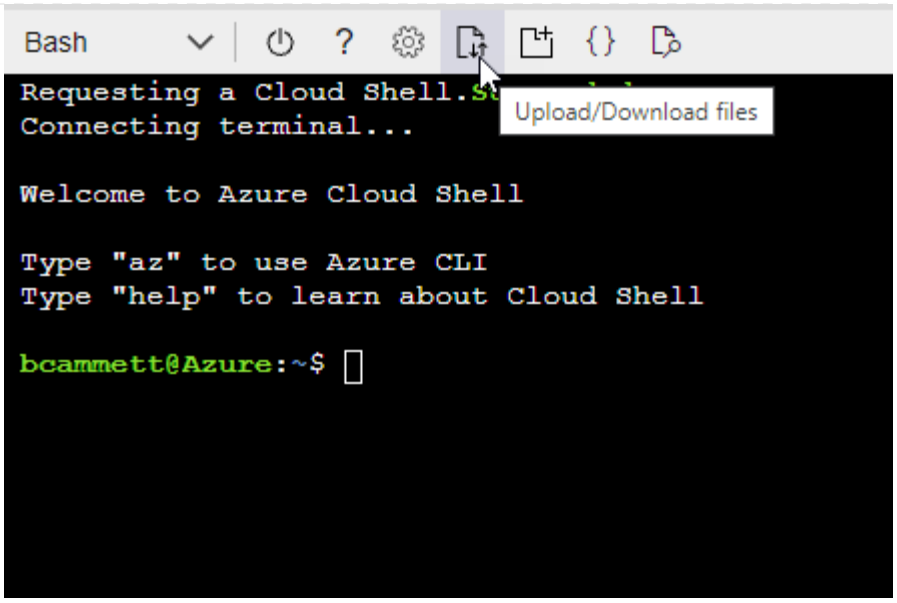
   例

   ```
   "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
```

サービスプリンシパル

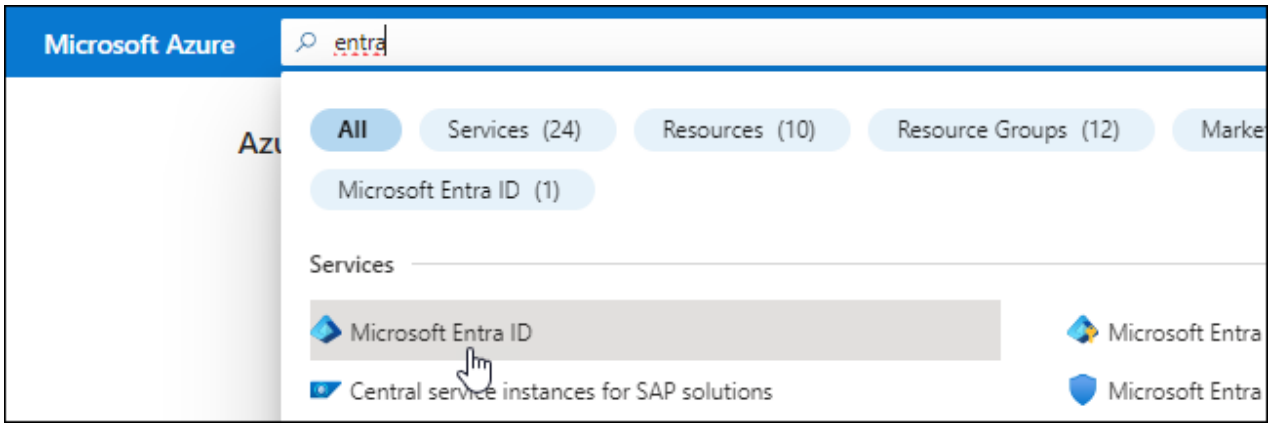
Microsoft Entra ID でサービス プリンシパルを作成して設定し、コンソール エージェントに必要な Azure 資格情報を取得します。

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。

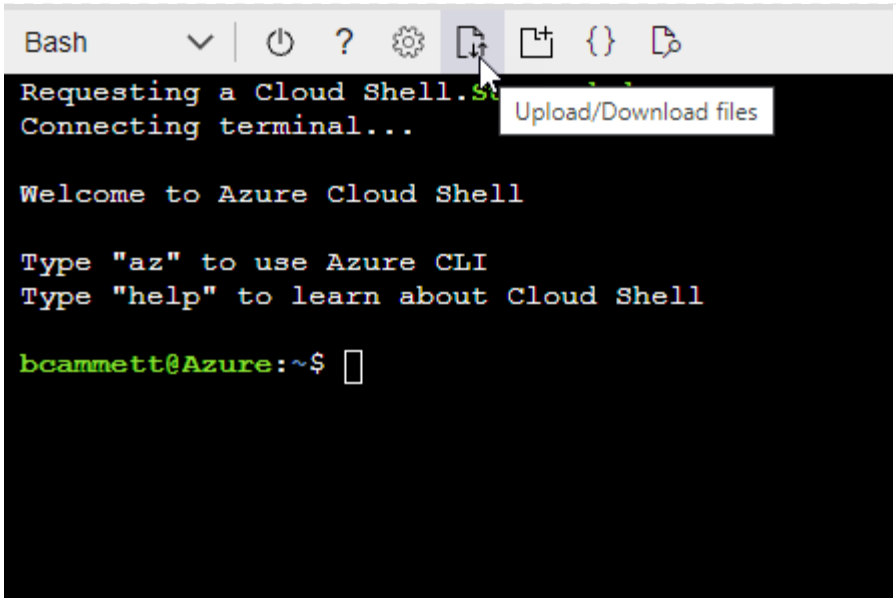
      例

      ```
      "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。

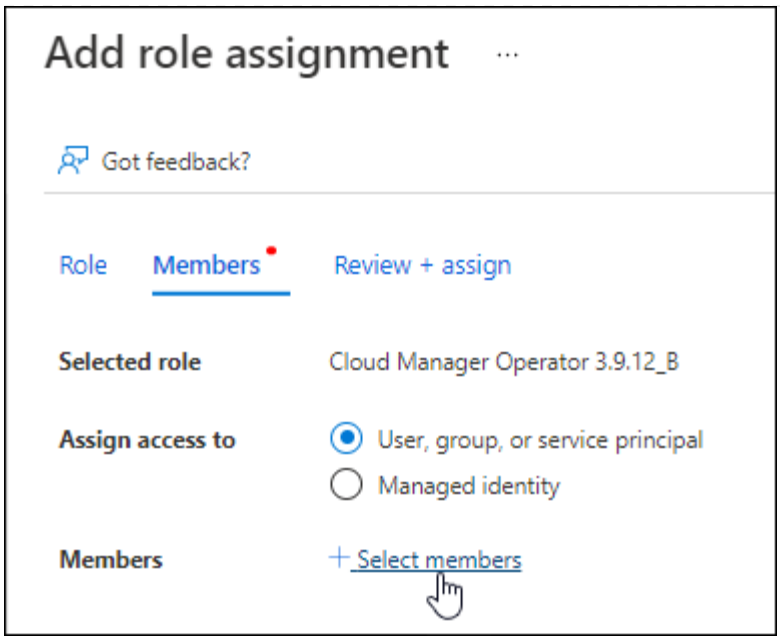
b. サブスクリプションを選択します。

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。

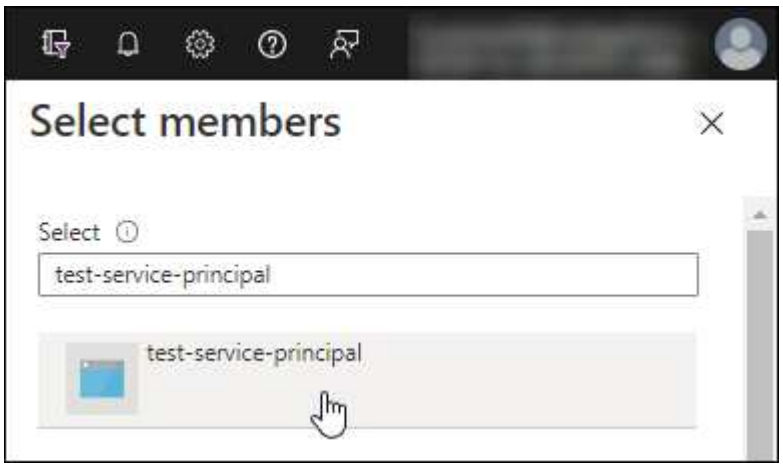
e. *メンバー*タブで、次の手順を実行します。

- *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。

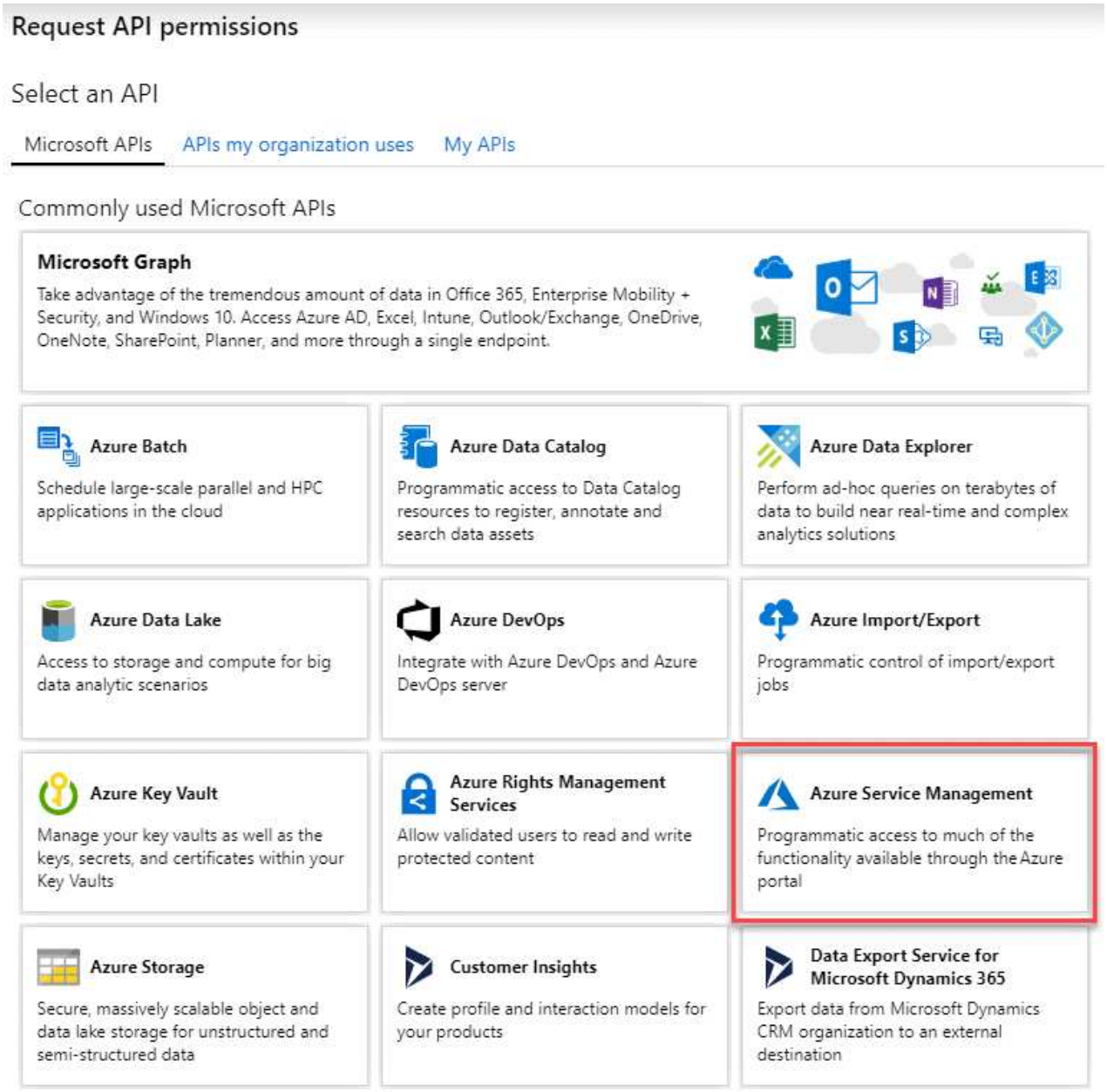
これで、サービス プリンシパルに、コンソール エージェントをデプロイするために必要な Azure アクセス許可が付与されました。

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。

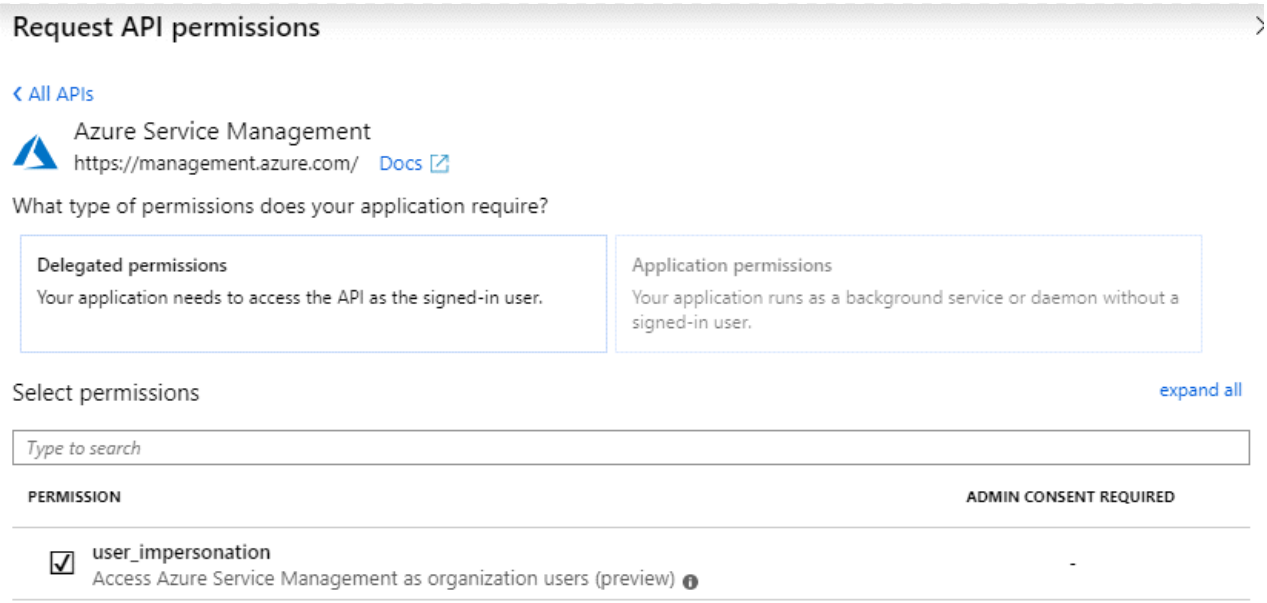
**Windows Azure** サービス管理 **API** 権限を追加する

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。

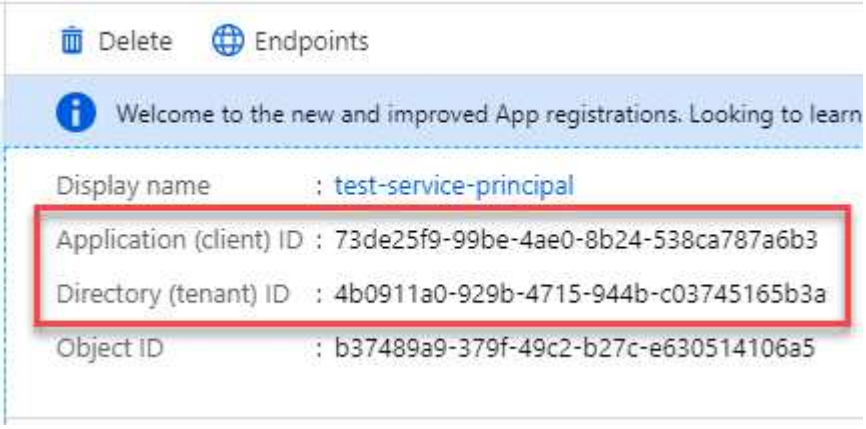



4. 組織ユーザーとして **Azure** サービス管理にアクセスする を選択し、権限の追加 を選択します。




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。

ステップ**5:** コンソールエージェントをインストールする

前提条件が完了したら、独自の Linux ホストにソフトウェア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"。

- 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、Azure の VM で有効になっているマネージド ID。

  "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"

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。

2. インストールが完了するまでお待ちください。

   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。

   インストールが失敗した場合は、インストール レポートとログを表示して問題の解決に役立てることができます。"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。"

1. コンソール エージェント仮想マシンに接続しているホストから Web ブラウザを開き、次の URL を入力します。

<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

2. ログイン後、コンソール エージェントを設定します。
   a. コンソール エージェントに関連付ける組織を指定します。
   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。

      以下の手順ではコンソールを標準モードで使用する方法について説明しているため、制限モードは無効にしておく必要があります。安全な環境があり、このアカウントをバックエンド サービスから切断する場合にのみ、制限モードを有効にする必要があります。もしそうなら、"NetApp Consoleを制限モードで使い始めるための手順に従います" 。

   d. *始めましょう*を選択します。

コンソール エージェントを作成したのと同じ Azure サブスクリプションに Azure Blob ストレージがある場合は、システム ページに Azure Blob ストレージ システムが自動的に表示されます。 "NetApp ConsoleからAzure Blob ストレージを管理する方法を学びます"

ステップ**6: NetApp Console**に権限を付与する

コンソール エージェントをインストールしたので、以前に設定した Azure アクセス許可をコンソール エージェントに付与する必要があります。権限を付与すると、コンソールで Azure のデータとストレージ インフラストラクチャを管理できるようになります。

カスタムロール

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。

次の手順

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

サービスプリンシパル

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。

## Google Cloud

### Google Cloud のコンソール エージェントのインストール オプション

Google Cloud でコンソール エージェントを作成するには、いくつかの方法があります。 NetApp Consoleから直接行うのが最も一般的な方法です。

次のインストール オプションが利用可能です。

- "コンソールから直接コンソールエージェントを作成する"（これが標準オプションです）

  このアクションにより、選択した VPC で Linux とコンソール エージェント ソフトウェアを実行する VM インスタンスが起動します。

- "Google プラットフォームを使用してコンソール エージェントを作成する"

  このアクションでは、Linux とコンソール エージェント ソフトウェアを実行する VM インスタンスも起動しますが、デプロイはコンソールからではなく Google Cloud から直接開始されます。

- "自分のLinuxホストにソフトウェアをダウンロードして手動でインストールする"

選択したインストール オプションは、インストールの準備方法に影響します。これには、Google Cloud でリソースを認証および管理するために必要な権限をコンソールに付与する方法が含まれます。

### NetApp Consoleから Google Cloud にコンソール エージェントを作成する

コンソールから Google Cloud にコンソール エージェントを作成できます。ネットワークを設定し、Google Cloud の権限を準備し、Google Cloud API を有効にして、コンソール エージェントを作成する必要があります。

開始する前に

- あなたは"コンソールエージェントの理解"。
- 確認すべき"コンソールエージェントの制限"。

ステップ**1:** ネットワークを設定する

コンソール エージェントがターゲット ネットワークへの接続とアウトバウンド インターネット アクセスを使用してリソースを管理できるように、ネットワークを設定します。

**VPC**とサブネット

コンソール エージェントを作成するときは、そのエージェントが存在する VPC とサブネットを指定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。

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 |
| --- | --- |
| https://www.googleapis.com/compute/v1/<br>https://compute.googleapis.com/compute/v1<br>https://cloudresourcemanager.googleapis.com/v1/projects<br>https://www.googleapis.com/compute/beta<br>https://storage.googleapis.com/storage/v1<br>https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1<br>https://cloudkms.googleapis.com/v1<br>https://config.googleapis.com/v1/projects | Google Cloud 内のリソースを管理します。 |
| 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。 |
| https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com<br>https://netapp-cloud-account.us.auth0.com https://console.netapp.com<br>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<br>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。<br><br>• 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。<br><br>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" 。<br><br>• 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。 |

**NetApp**コンソールから接続されたエンドポイント

SaaS レイヤーを通じて提供される Web ベースのNetApp Consoleを使用すると、複数のエンドポイントに接続してデータ管理タスクが完了します。これには、コンソールからコンソール エージェントを展開するために接続されるエンドポイントが含まれます。

"NetAppコンソールから接続されたエンドポイントのリストを表示します" 。

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"

コンソール エージェントを作成した後、このネットワーク要件を実装します。

ステップ**2:** コンソールエージェントを作成するための権限を設定する

コンソールからコンソール エージェントをデプロイする前に、コンソール エージェント VM をデプロイする Google プラットフォーム ユーザーの権限を設定する必要があります。

手順

1. Google プラットフォームでカスタムロールを作成します。

   a. 次の権限を含む YAML ファイルを作成します。

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
```

```
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- config.deployments.create
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
```

```
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

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

c. 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「agentDeployment」という名前のロールを作成します。

gcloud iam ロール コネクタデプロイメントを作成 --project=myproject --file=agent-deployment.yaml

"Google Cloud ドキュメント: カスタムロールの作成と管理"

2. このカスタムロールは、コンソールから、または gcloud を使用してコンソール エージェントをデプロイするユーザーに割り当てます。

"Google Cloud ドキュメント: 単一のロールを付与する"

ステップ **3:** エージェントで使用する **Google Cloud** サービス アカウントを作成する

Google Cloud 内のリソースを管理するためにコンソールが必要とする権限をコンソール エージェントに付与するには、Google Cloud サービス アカウントが必要です。コンソール エージェントを作成するときは、このサービス アカウントをコンソール エージェント VM に関連付ける必要があります。

以降のリリースで新しい権限が追加された場合、カスタム ロールを更新するのはお客様の責任となります。新しい権限が必要な場合は、リリース ノートに記載されます。

手順

1. Google Cloud でカスタムロールを作成します。

a. 以下の内容を含むYAMLファイルを作成します。"コンソールエージェントのサービスアカウント権限"。

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

c. 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 connector --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、そのサービス アカウントにロールを割り当てます。

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"

3. コンソール エージェントが存在するプロジェクトとは異なるプロジェクトにCloud Volumes ONTAPシステムを展開する予定の場合は、コンソール エージェントのサービス アカウントにそれらのプロジェクトへのアクセス権を付与する必要があります。

たとえば、コンソール エージェントがプロジェクト 1 にあり、プロジェクト 2 にCloud Volumes ONTAPシステムを作成するとします。プロジェクト 2 のサービス アカウントにアクセス権を付与する必要があります。

a. IAM & Admin サービスから、 Cloud Volumes ONTAPシステムを作成する Google Cloud プロジェクトを選択します。

b. **IAM** ページで、アクセスを許可 を選択し、必要な詳細を入力します。

- コンソール エージェントのサービス アカウントの電子メールを入力します。
- コンソール エージェントのカスタム ロールを選択します。
- *保存*を選択します。

詳細については、 "Google Cloud ドキュメント"

ステップ**4:** 共有**VPC**権限を設定する

共有 VPC を使用してリソースをサービス プロジェクトにデプロイする場合は、権限を準備する必要があります。

この表は参考用であり、IAM 構成が完了すると、環境に権限表が反映されるはずです。

共有 **VPC** 権限を表示する

| 身元 | クリエイター | 開催地 | サービスプロジェクトの権限 | ホストプロジェクトの権限 | 目的 |
|---|---|---|---|---|---|
| エージェントを展開するためのGoogleアカウント | カスタム | 奉仕プロジェクト | "エージェント展開ポリシー" | compute.networkUser | サービスプロジェクトにエージェントをデプロイする |
| エージェントサービスアカウント | カスタム | 奉仕プロジェクト | "エージェント サービス アカウント ポリシー" | compute.networkUser デプロイメントマネージャー.エディター | サービス プロジェクトでCloud Volumes ONTAPとサービスをデプロイおよび保守する |
| Cloud Volumes ONTAP サービスアカウント | カスタム | 奉仕プロジェクト | storage.admin メンバー: serviceAccount.user としてのNetApp Consoleサービスアカウント | 該当なし | （オプション） NetApp Cloud TieringおよびNetApp Backup and Recoveryの場合 |
| Google API サービス エージェント | Google Cloud | 奉仕プロジェクト | (デフォルト) エディター | compute.networkUser | デプロイメントに代わって Google Cloud API と対話します。コンソールが共有ネットワークを使用できるようにします。 |
| Google Compute Engine のデフォルトのサービスアカウント | Google Cloud | 奉仕プロジェクト | (デフォルト) エディター | compute.networkUser | デプロイメントに代わって、Google Cloud インスタンスとコンピューティング インフラストラクチャをデプロイします。コンソールが共有ネットワークを使用できるようにします。 |

注：

1. ファイアウォール ルールをデプロイメントに渡さず、コンソールで自動的に作成するように選択した場合にのみ、ホスト プロジェクトで deploymentmanager.editor が必要になります。ルールが指定されていない場合、 NetApp Consoleは、VPC0 ファイアウォール ルールを含むデプロイメントをホスト プロジェクトに作成します。
2. firewall.create と firewall.delete は、デプロイメントにファイアウォール ルールを渡さず、コンソールで自動的に作成するように選択した場合にのみ必要です。これらの権限は、コンソール アカウントの .yaml ファイルにあります。共有 VPC を使用して HA ペアを展開する場合、これらの権限は VPC1、2、3 のファイアウォール ルールを作成するために使用されます。他のすべてのデプロイメントでは、これらの権限は VPC0 のルールの作成にも使用されます。
3. クラウド階層化の場合、階層化サービス アカウントには、プロジェクト レベルだけでなく、サービス アカウントに対する serviceAccount.user ロールが必要です。現在、プロジェクト レベルで serviceAccount.user を割り当てると、getIAMPolicy を使用してサービス アカウントをクエリしても

権限が表示されません。

### ステップ5: Google Cloud APIを有効にする

Console エージェントとCloud Volumes ONTAPをデプロイする前に、いくつかの Google Cloud API を有効にする必要があります。

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）

"Google Cloud ドキュメント: API の有効化"

### ステップ6: コンソールエージェントを作成する

コンソールから直接コンソール エージェントを作成します。

コンソール エージェントを作成すると、デフォルト構成を使用して Google Cloud に仮想マシン インスタンスがデプロイされます。コンソール エージェントを作成した後、CPU や RAM が少ない小さな VM インスタンスに切り替えないでください。"コンソールエージェントのデフォルト構成について学習します" 。

Google Cloud にエージェントをデプロイすると、エージェントによってデプロイ ファイルを保存するためのバケットが作成されます。

開始する前に

次のものが必要です:

- コンソール エージェントとコンソール エージェント VM のサービス アカウントを作成するために必要な Google Cloud 権限。
- ネットワーク要件を満たす VPC とサブネット。
- 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。

手順

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 > Google Cloud*を選択します。

3. *エージェントのデプロイ*ページで、必要なものの詳細を確認します。次の 2 つのオプションがあります。
   a. 製品内ガイドを使用して展開の準備をするには、[続行] を選択します。製品内ガイドの各ステップには、ドキュメントのこのページに記載されている情報が含まれています。
   b. このページの手順に従ってすでに準備している場合は、[展開にスキップ] を選択します。
4. ウィザードの手順に従ってコンソール エージェントを作成します。
   - プロンプトが表示されたら、仮想マシン インスタンスを作成するために必要な権限を持つ Google アカウントにログインします。

     このフォームは Google が所有し、ホストしています。資格情報がNetAppに提供されていません。

   - 詳細: 仮想マシン インスタンスの名前を入力し、タグを指定して、プロジェクトを選択し、必要な権限を持つサービス アカウントを選択します (詳細については上記のセクションを参照してください)。
   - 場所: インスタンスのリージョン、ゾーン、VPC、サブネットを指定します。
   - ネットワーク: パブリック IP アドレスを有効にするかどうかを選択し、オプションでプロキシ構成を指定します。
   - ネットワーク タグ: 透過プロキシを使用している場合は、コンソール エージェント インスタンスにネットワーク タグを追加します。ネットワーク タグは小文字で始まる必要があり、小文字、数字、ハイフンを含めることができます。タグは小文字または数字で終わる必要があります。たとえば、「console-agent-proxy」というタグを使用できます。
   - ファイアウォール ポリシー: 新しいファイアウォール ポリシーを作成するか、必要な受信ルールと送信ルールを許可する既存のファイアウォール ポリシーを選択するかを選択します。

     "Google Cloud のファイアウォール ルール"

5. 選択内容を確認して、セットアップが正しいことを確認します。
   a. エージェント構成の検証 チェック ボックスはデフォルトでオンになっており、展開時にコンソールによってネットワーク接続要件が検証されます。コンソールがエージェントの展開に失敗した場合、トラブルシューティングに役立つレポートが提供されます。デプロイメントが成功した場合、レポートは提供されません。

   まだ使用している場合は"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、チェックボックスをオフにして検証チェックをスキップします。

6. *追加*を選択します。

   エージェントは約 10 分で準備完了します。プロセスが完了するまでページに留まってください。

結果

プロセスが完了すると、コンソール エージェントが使用できるようになります。

デプロイメントが失敗した場合は、コンソールからレポートとログをダウンロードして、問題の解決に役立てることができます。"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。"

コンソール エージェントを作成したのと同じ Google Cloud アカウントに Google Cloud Storage バケットがある場合は、[システム] ページに Google Cloud Storage システムが自動的に表示されます。 "コンソールから Google Cloud Storage を管理する方法を学びます"

**Google Cloud** からコンソール エージェントを作成する

# Google Cloud を使用して Google Cloud にコンソール エージェントを作成するには、ネットワークを設定し、Google Cloud の権限を準備し、Google Cloud API を有効にして、コンソール エージェントを作成する必要があります。

開始する前に

- あなたは"コンソールエージェントの理解"。
- 確認すべき"コンソールエージェントの制限"。

ステップ**1:** ネットワークを設定する

コンソール エージェントがリソースを管理し、ターゲット ネットワークおよびインターネットに接続できるようにネットワークを設定します。

**VPC**とサブネット

コンソール エージェントを作成するときは、そのエージェントが存在する VPC とサブネットを指定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。

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 |
| --- | --- |
| https://www.googleapis.com/compute/v1/<br>https://compute.googleapis.com/compute/v1<br>https://cloudresourcemanager.googleapis.com/v1/projects<br>https://www.googleapis.com/compute/beta<br>https://storage.googleapis.com/storage/v1<br>https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1<br>https://cloudkms.googleapis.com/v1<br>https://config.googleapis.com/v1/projects | Google Cloud 内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.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://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。<br><br>• 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。<br><br>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" 。<br><br>• 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。 |

**NetApp**コンソールから接続されたエンドポイント

SaaS レイヤーを通じて提供される Web ベースのNetApp Consoleを使用すると、複数のエンドポイントに接続してデータ管理タスクが完了します。これには、コンソールからコンソール エージェントを展開するために接続されるエンドポイントが含まれます。

"NetAppコンソールから接続されたエンドポイントのリストを表示します" 。

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"

コンソール エージェントを作成した後、このネットワーク要件を実装します。

ステップ**2:** コンソールエージェントを作成するための権限を設定する

Google Cloud ユーザーが Google Cloud からコンソール エージェント VM をデプロイするための権限を設定します。

手順

1. Google プラットフォームでカスタムロールを作成します。

   a. 次の権限を含む YAML ファイルを作成します。

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console
agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- config.deployments.create
```

```
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

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

c. 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「connectorDeployment」という名前のロールを作成します。

gcloud iam ロール コネクタデプロイメントを作成 --project=myproject --file=connector
-deployment.yaml

"Google Cloud ドキュメント: カスタムロールの作成と管理"

2. このカスタムロールを、Google Cloud からコンソール エージェントをデプロイするユーザーに割り当てます。

"Google Cloud ドキュメント: 単一のロールを付与する"

ステップ**3:** コンソールエージェント操作の権限を設定する

Google Cloud 内のリソースを管理するためにコンソールが必要とする権限をコンソール エージェントに付与するには、Google Cloud サービス アカウントが必要です。コンソール エージェントを作成するときは、このサービス アカウントをコンソール エージェント VM に関連付ける必要があります。

以降のリリースで新しい権限が追加された場合、カスタム ロールを更新するのはお客様の責任となります。新しい権限が必要な場合は、リリース ノートに記載されます。

手順

1. Google Cloud でカスタムロールを作成します。

   a. 以下の内容を含むYAMLファイルを作成します。"コンソールエージェントのサービスアカウント権限"。
   b. Google Cloud から Cloud Shell を有効にします。
   c. 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 connector --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、そのサービス アカウントにロールを割り当てます。

   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"

3. コンソール エージェントが存在するプロジェクトとは異なるプロジェクトにCloud Volumes ONTAPシステムを展開する予定の場合は、コンソール エージェントのサービス アカウントにそれらのプロジェクトへのアクセス権を付与する必要があります。

   たとえば、コンソール エージェントがプロジェクト 1 にあり、プロジェクト 2 にCloud Volumes ONTAP

システムを作成するとします。プロジェクト 2 のサービス アカウントにアクセス権を付与する必要があります。

a. IAM & Admin サービスから、 Cloud Volumes ONTAPシステムを作成する Google Cloud プロジェクトを選択します。

b. **IAM** ページで、アクセスを許可 を選択し、必要な詳細を入力します。

- コンソール エージェントのサービス アカウントの電子メールを入力します。
- コンソール エージェントのカスタム ロールを選択します。
- *保存*を選択します。

詳細については、 "Google Cloud ドキュメント"

ステップ**4:** 共有**VPC**権限を設定する

共有 VPC を使用してリソースをサービス プロジェクトにデプロイする場合は、権限を準備する必要があります。

この表は参考用であり、IAM 構成が完了すると、環境に権限表が反映されるはずです。

共有 **VPC** 権限を表示する

| 身元 | クリエイター | 開催地 | サービスプロジェクトの権限 | ホストプロジェクトの権限 | 目的 |
|---|---|---|---|---|---|
| エージェントを展開するためのGoogleアカウント | カスタム | 奉仕プロジェクト | "エージェント展開ポリシー" | compute.networkUser | サービスプロジェクトにエージェントをデプロイする |
| エージェントサービスアカウント | カスタム | 奉仕プロジェクト | "エージェント サービス アカウント ポリシー" | compute.networkUser デプロイメントマネージャー.エディター | サービス プロジェクトでCloud Volumes ONTAPとサービスをデプロイおよび保守する |
| Cloud Volumes ONTAP サービスアカウント | カスタム | 奉仕プロジェクト | storage.admin メンバー: serviceAccount.user としてのNetApp Consoleサービスアカウント | 該当なし | （オプション） NetApp Cloud TieringおよびNetApp Backup and Recoveryの場合 |
| Google API サービス エージェント | Google Cloud | 奉仕プロジェクト | (デフォルト) エディター | compute.networkUser | デプロイメントに代わって Google Cloud API と対話します。コンソールが共有ネットワークを使用できるようにします。 |
| Google Compute Engine のデフォルトのサービスアカウント | Google Cloud | 奉仕プロジェクト | (デフォルト) エディター | compute.networkUser | デプロイメントに代わって、Google Cloud インスタンスとコンピューティング インフラストラクチャをデプロイします。コンソールが共有ネットワークを使用できるようにします。 |

注：

1. ファイアウォール ルールをデプロイメントに渡さず、コンソールで自動的に作成するように選択した場合にのみ、ホスト プロジェクトで deploymentmanager.editor が必要になります。ルールが指定されていない場合、 NetApp Consoleは、VPC0 ファイアウォール ルールを含むデプロイメントをホスト プロジェクトに作成します。
2. firewall.create と firewall.delete は、デプロイメントにファイアウォール ルールを渡さず、コンソールで自動的に作成するように選択した場合にのみ必要です。これらの権限は、コンソール アカウントの .yaml ファイルにあります。共有 VPC を使用して HA ペアを展開する場合、これらの権限は VPC1、2、3 のファイアウォール ルールを作成するために使用されます。他のすべてのデプロイメントでは、これらの権限は VPC0 のルールの作成にも使用されます。
3. クラウド階層化の場合、階層化サービス アカウントには、プロジェクト レベルだけでなく、サービス アカウントに対する serviceAccount.user ロールが必要です。現在、プロジェクト レベルで serviceAccount.user を割り当てると、getIAMPolicy を使用してサービス アカウントをクエリしても

権限が表示されません。

### ステップ**5: Google Cloud API**を有効にする

Console エージェントとCloud Volumes ONTAP をデプロイする前に、いくつかの Google Cloud API を有効にします。

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）

"Google Cloud ドキュメント: API の有効化"

### ステップ**6:** コンソールエージェントを作成する

Google Cloud を使用してコンソール エージェントを作成します。

コンソール エージェントを作成すると、デフォルト構成で Google Cloud に VM インスタンスがデプロイされます。コンソール エージェントを作成した後、CPU や RAM が少ない小さな VM インスタンスに切り替えないでください。"コンソールエージェントのデフォルト構成について学習します" 。

開始する前に

次のものが必要です:

- コンソール エージェントとコンソール エージェント VM のサービス アカウントを作成するために必要な Google Cloud 権限。
- ネットワーク要件を満たす VPC とサブネット。
- VM インスタンスの要件を理解していること。
  - **CPU**: 8 コアまたは 8 vCPU
  - **RAM**: 32 GB
  - マシンタイプ: n2-standard-8 を推奨します。

    Console エージェントは、Shielded VM 機能をサポートする OS を搭載した VM インスタンス上の Google Cloud でサポートされます。

手順

1. お好みの方法で Google Cloud SDK にログインします。

   この例では、gcloud SDK がインストールされたローカル シェルを使用していますが、Google Cloud Shell を使用することもできます。

   Google Cloud SDKの詳細については、"Google Cloud SDK ドキュメント ページ" 。

2. 上記のセクションで定義されている必要な権限を持つユーザーとしてログインしていることを確認します。

   ```
   gcloud auth list
   ```

   出力には次のように表示されます。* ユーザー アカウントは、ログインに使用するユーザー アカウントです。

   ```
   Credentialed Accounts
   ACTIVE  ACCOUNT
        some_user_account@domain.com
   *    desired_user_account@domain.com
   To set the active account, run:
    $ gcloud config set account `ACCOUNT`
   Updates are available for some Cloud SDK components. To install them,
   please run:
   $ gcloud components update
   ```

3. 実行 `gcloud compute instances create`指示：

   ```
   gcloud compute instances create <instance-name>
     --machine-type=n2-standard-8
     --image-project=netapp-cloudmanager
     --image-family=cloudmanager
     --scopes=cloud-platform
     --project=<project>
     --service-account=<service-account>
     --zone=<zone>
     --no-address
     --tags <network-tag>
     --network <network-path>
     --subnet <subnet-path>
     --boot-disk-kms-key <kms-key-path>
   ```

   インスタンス名
   : VM インスタンスの希望するインスタンス名。

プロジェクト
: (オプション) VM をデプロイするプロジェクト。

サービスアカウント
: 手順 2 の出力で指定されたサービス アカウント。

ゾーン
: VMを展開するゾーン

住所なし
: (オプション) 外部 IP アドレスは使用されません (トラフィックをパブリック インターネットにルーティングするには、クラウド NAT またはプロキシが必要です)

ネットワークタグ
: (オプション) ネットワーク タグ付けを追加して、タグを使用してファイアウォール ルールをコンソール エージェント インスタンスにリンクします。

ネットワークパス
: (オプション) コンソールエージェントをデプロイするネットワークの名前を追加します (共有 VPC の場合はフルパスが必要です)

サブネットパス
: (オプション) コンソールエージェントをデプロイするサブネットの名前を追加します (共有 VPC の場合はフルパスが必要です)

**kms**キーパス
: (オプション) コンソール エージェントのディスクを暗号化するための KMS キーを追加します (IAM 権限も適用する必要があります)

  これらの旗の詳細については、"Google Cloud Compute SDK ドキュメント" 。

コマンドを実行すると、コンソール エージェントがデプロイされます。コンソール エージェント インスタンスとソフトウェアは、約 5 分以内に実行されるはずです。

4. 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。

5. ログイン後、コンソール エージェントを設定します。
   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。

      "アイデンティティとアクセス管理について学ぶ" 。

   b. システムの名前を入力します。

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。

ウェブブラウザを開いて、 "NetApp Console"コンソール エージェントの使用を開始します。

**Google Cloud** にコンソール エージェントを手動でインストールする

# 独自の Linux ホストに Console エージェントを手動でインストールするには、ホストの要件を確認し、ネットワークを設定し、Google Cloud の権限を準備し、Google Cloud API を有効にし、Console をインストールして、準備した権限を付与する必要があります。

開始する前に

- あなたは"コンソールエージェントの理解"。
- 確認すべき"コンソールエージェントの制限"。

ステップ**1:** ホストの要件を確認する

コンソール エージェント ソフトウェアは、特定のオペレーティング システム要件、RAM 要件、ポート要件などを満たすホスト上で実行する必要があります。

> 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。

**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<br>• 英語版のみ。<br>• 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。<br>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<br>• 英語版のみ。<br>• 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。<br>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<br>• 英語版のみ。<br>• 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。<br>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 |

**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"

ステップ**2: 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 **3.** 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**3:** ネットワークを設定する

コンソール エージェントがハイブリッド クラウド環境内のリソースとプロセスを管理できるようにネットワークを設定します。たとえば、ターゲット ネットワークへの接続が利用可能であること、および発信インターネット アクセスが利用可能であ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。

| エンドポイント | 目的 |
| --- | --- |
| https://www.googleapis.com/compute/v1/<br>https://compute.googleapis.com/compute/v1<br>https://cloudresourcemanager.googleapis.com/v1/projects<br>https://www.googleapis.com/compute/beta<br>https://storage.googleapis.com/storage/v1<br>https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1<br>https://cloudkms.googleapis.com/v1<br>https://config.googleapis.com/v1/projects | Google Cloud 内のリソースを管理します。 |
| 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。 |

| エンドポイント | 目的 |
| --- | --- |
| 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。 |
| 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。<br><br>• 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。<br><br>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" 。<br><br>• 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"

ステップ**4:** コンソールエージェントの権限を設定する

Google Cloud 内のリソースを管理するためにコンソールが必要とする権限をコンソール エージェントに付与するには、Google Cloud サービス アカウントが必要です。コンソール エージェントを作成するときは、このサービス アカウントをコンソール エージェント VM に関連付ける必要があります。

以降のリリースで新しい権限が追加された場合、カスタム ロールを更新するのはお客様の責任となります。新しい権限が必要な場合は、リリース ノートに記載されます。

手順

1. Google Cloud でカスタムロールを作成します。

   a. 以下の内容を含むYAMLファイルを作成します。"コンソールエージェントのサービスアカウント権限"。
   b. Google Cloud から Cloud Shell を有効にします。
   c. 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 connector --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、そのサービス アカウントにロールを割り当てます。
   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"

3. コンソール エージェントが存在するプロジェクトとは異なるプロジェクトにCloud Volumes ONTAPシステムを展開する予定の場合は、コンソール エージェントのサービス アカウントにそれらのプロジェクトへのアクセス権を付与する必要があります。

   たとえば、コンソール エージェントがプロジェクト 1 にあり、プロジェクト 2 にCloud Volumes ONTAPシステムを作成するとします。プロジェクト 2 のサービス アカウントにアクセス権を付与する必要があります。

   a. IAM & Admin サービスから、 Cloud Volumes ONTAPシステムを作成する Google Cloud プロジェクトを選択します。
   b. **IAM** ページで、アクセスを許可 を選択し、必要な詳細を入力します。
      - コンソール エージェントのサービス アカウントの電子メールを入力します。
      - コンソール エージェントのカスタム ロールを選択します。
      - *保存*を選択します。

   詳細については、 "Google Cloud ドキュメント"

ステップ**5:** 共有**VPC**権限を設定する

共有 VPC を使用してリソースをサービス プロジェクトにデプロイする場合は、権限を準備する必要があります。

この表は参考用であり、IAM 構成が完了すると、環境に権限表が反映されるはずです。

共有 **VPC** 権限を表示する

| 身元 | クリエイター | 開催地 | サービスプロジェクトの権限 | ホストプロジェクトの権限 | 目的 |
|---|---|---|---|---|---|
| エージェントを展開するためのGoogleアカウント | カスタム | 奉仕プロジェクト | "エージェント展開ポリシー" | compute.networkUser | サービスプロジェクトにエージェントをデプロイする |
| エージェントサービスアカウント | カスタム | 奉仕プロジェクト | "エージェント サービス アカウント ポリシー" | compute.networkUser デプロイメントマネージャー.エディター | サービス プロジェクトでCloud Volumes ONTAPとサービスをデプロイおよび保守する |
| Cloud Volumes ONTAP サービスアカウント | カスタム | 奉仕プロジェクト | storage.admin メンバー: serviceAccount.user としてのNetApp Consoleサービスアカウント | 該当なし | （オプション） NetApp Cloud TieringおよびNetApp Backup and Recoveryの場合 |
| Google API サービス エージェント | Google Cloud | 奉仕プロジェクト | (デフォルト) エディター | compute.networkUser | デプロイメントに代わって Google Cloud API と対話します。コンソールが共有ネットワークを使用できるようにします。 |
| Google Compute Engine のデフォルトのサービスアカウント | Google Cloud | 奉仕プロジェクト | (デフォルト) エディター | compute.networkUser | デプロイメントに代わって、Google Cloud インスタンスとコンピューティング インフラストラクチャをデプロイします。コンソールが共有ネットワークを使用できるようにします。 |

注：

1. ファイアウォール ルールをデプロイメントに渡さず、コンソールで自動的に作成するように選択した場合にのみ、ホスト プロジェクトで deploymentmanager.editor が必要になります。ルールが指定されていない場合、 NetApp Consoleは、VPC0 ファイアウォール ルールを含むデプロイメントをホスト プロジェクトに作成します。
2. firewall.create と firewall.delete は、デプロイメントにファイアウォール ルールを渡さず、コンソールで自動的に作成するように選択した場合にのみ必要です。これらの権限は、コンソール アカウントの .yaml ファイルにあります。共有 VPC を使用して HA ペアを展開する場合、これらの権限は VPC1、2、3 のファイアウォール ルールを作成するために使用されます。他のすべてのデプロイメントでは、これらの権限は VPC0 のルールの作成にも使用されます。
3. クラウド階層化の場合、階層化サービス アカウントには、プロジェクト レベルだけでなく、サービス アカウントに対する serviceAccount.user ロールが必要です。現在、プロジェクト レベルで serviceAccount.user を割り当てると、getIAMPolicy を使用してサービス アカウントをクエリしても

権限が表示されません。

### ステップ6: Google Cloud APIを有効にする

Google Cloud にコンソール エージェントをデプロイする前に、いくつかの Google Cloud API を有効にする必要があります。

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）

"Google Cloud ドキュメント: API の有効化"

### ステップ7: コンソールエージェントをインストールする

前提条件が完了したら、独自の Linux ホストにソフトウェアを手動でインストールできます。

エージェントをデプロイすると、デプロイ ファイルを保存するための Google Cloud バケットも作成されます。

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。
   - 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。

2. インストールが完了するまでお待ちください。

   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。

インストールが失敗した場合は、インストール レポートとログを表示して問題の解決に役立てることができます。"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。"

1. コンソール エージェント仮想マシンに接続しているホストから Web ブラウザを開き、次の URL を入力します。

   <a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

2. ログイン後、コンソール エージェントを設定します。

   a. コンソール エージェントに関連付ける組織を指定します。

   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。

      以下の手順ではコンソールを標準モードで使用する方法について説明しているため、制限モードは無効にしておく必要があります。安全な環境があり、このアカウントをバックエンド サービスから切断する場合にのみ、制限モードを有効にする必要があります。もしそうなら、"NetApp Consoleを制限モードで使い始めるための手順に従います" 。

   d. *始めましょう*を選択します。

   インストールが失敗した場合は、トラブルシューティングに役立つログとレポートを表示できます。"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。"

コンソール エージェントを作成したのと同じ Google Cloud アカウントに Google Cloud Storage バケットがある場合は、[システム] ページに Google Cloud Storage システムが自動的に表示されます。 "NetApp Consoleから Google Cloud Storage を管理する方法を学びます"

ステップ**8:** コンソールエージェントに権限を付与する

以前に設定した Google Cloud 権限をコンソール エージェントに提供する必要があります。権限を付与すると、コンソール エージェントが Google Cloud 内のデータとストレージ インフラストラクチャを管理できるようになります。

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 Google Cloud プロジェクトのリソースを管理する場合は、コンソール エージェントの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権を付与します。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。

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<br>• 英語版のみ。<br>• 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。<br>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 | | 9.1～9.4<br>• 英語版のみ。<br>• 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。<br>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 | | 8.6～8.10<br>• 英語版のみ。<br>• 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。<br>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):<br>• クラウドフォーメーション<br>• エラスティックコンピューティングクラウド (EC2)<br>• アイデンティティとアクセス管理（IAM）<br>• キー管理サービス (KMS)<br>• セキュリティトークンサービス（STS）<br>• 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:<br>• 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.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://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。<br><br>• 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。<br><br>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" 。<br><br>• 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.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://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。<br><br>• 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。<br><br>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" 。<br><br>• 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**

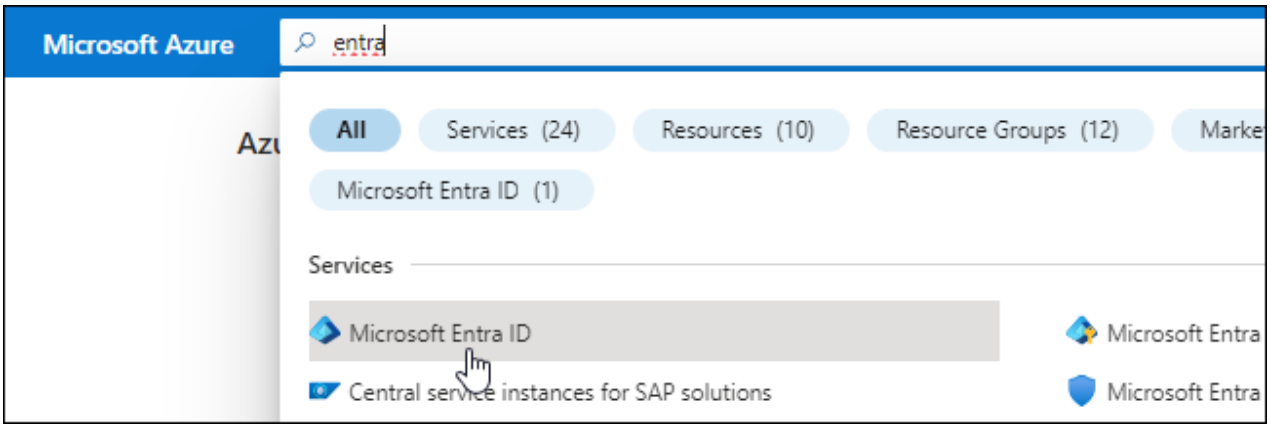
コンソール エージェントがオンプレミスでインストールされている場合は、Microsoft Entra ID でサービス プリンシパルを設定し、コンソール エージェントに必要な Azure 資格情報を取得して、コンソール エージェントに Azure 権限を付与する必要があります。

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。

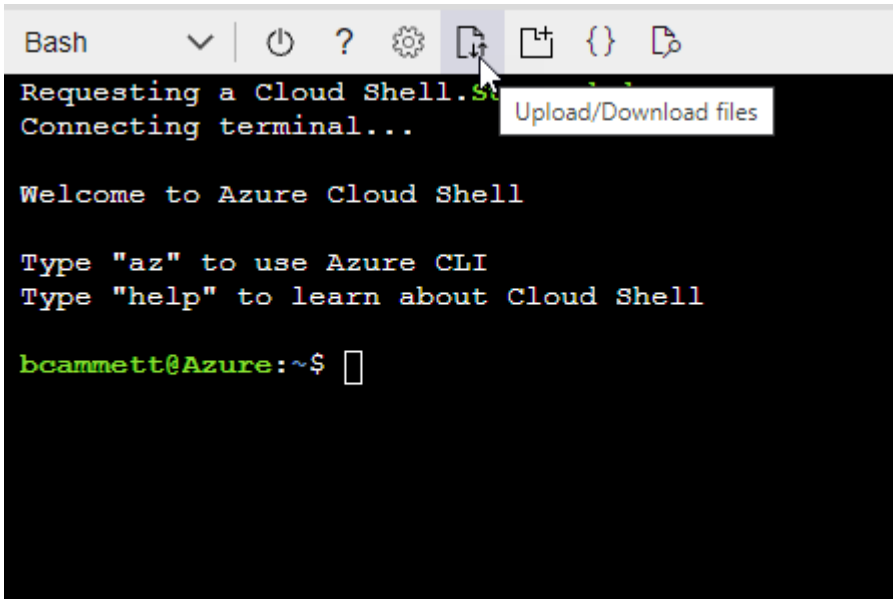
      例

```
"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。

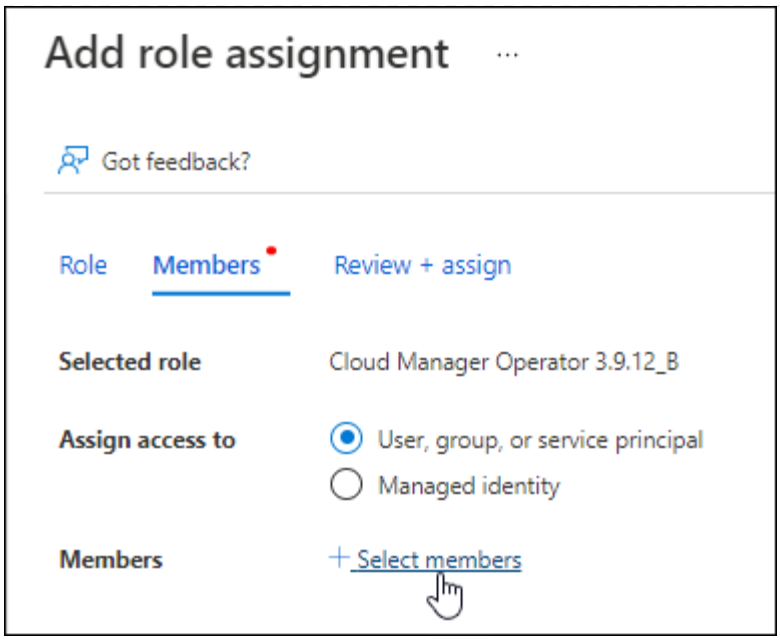
```
az role definition create --role-definition agent_Policy.json
```

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。

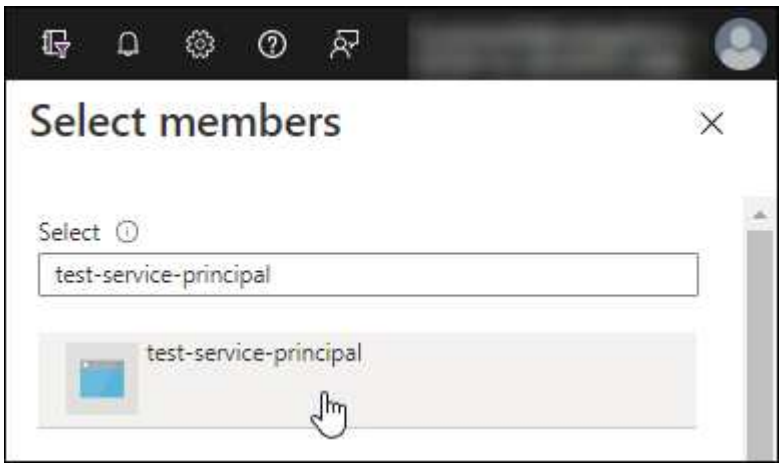
a. Azure ポータルから、サブスクリプション サービスを開きます。
b. サブスクリプションを選択します。
c. アクセス制御 **(IAM) >** 追加 **>** ロール割り当ての追加 を選択します。
d. *役割*タブで、*コンソールオペレーター*役割を選択し、*次へ*を選択します。
e. *メンバー*タブで、次の手順を実行します。

- *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。

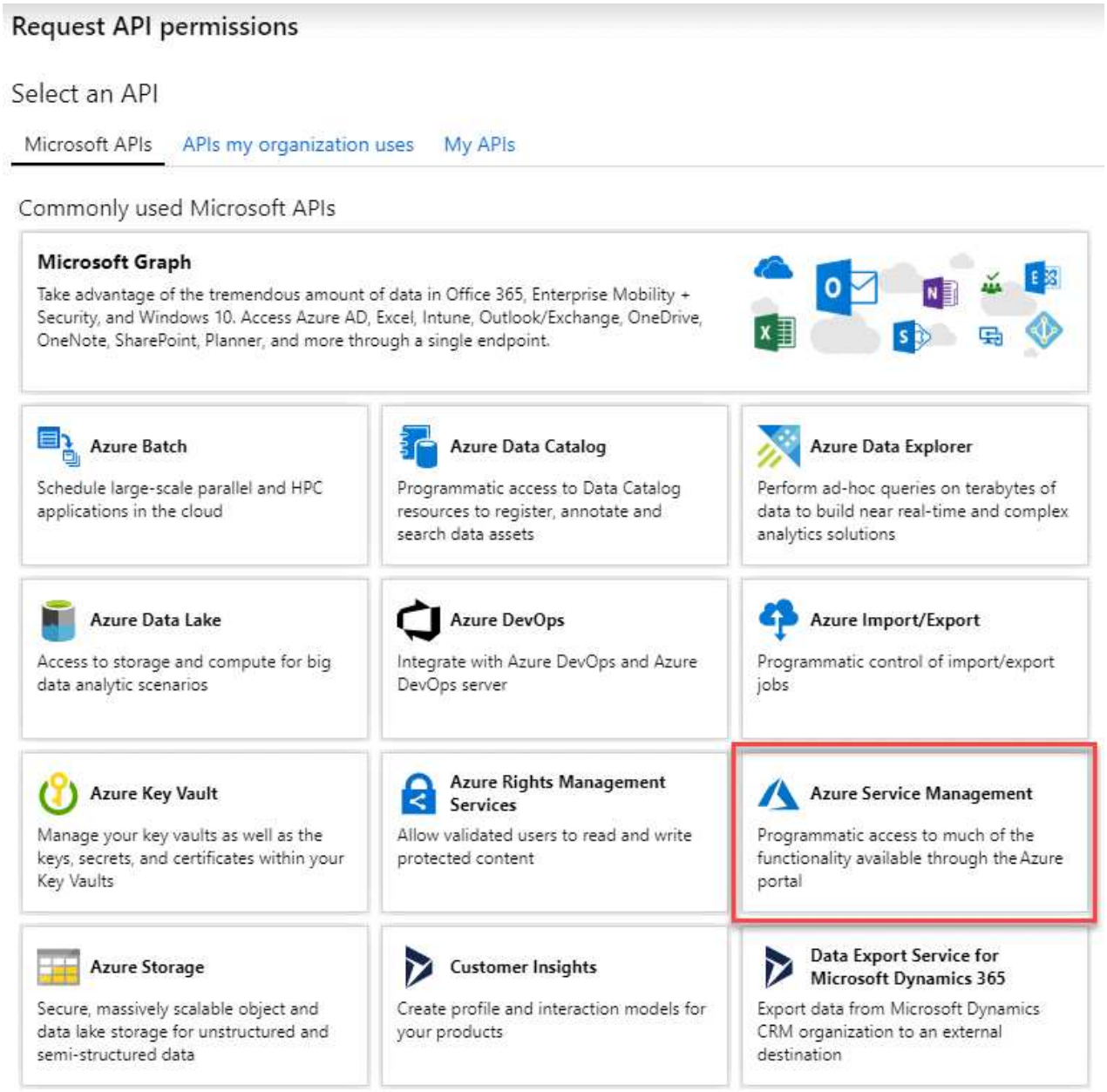
これで、サービス プリンシパルに、コンソール エージェントをデプロイするために必要な Azure アクセス許可が付与されました。

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。

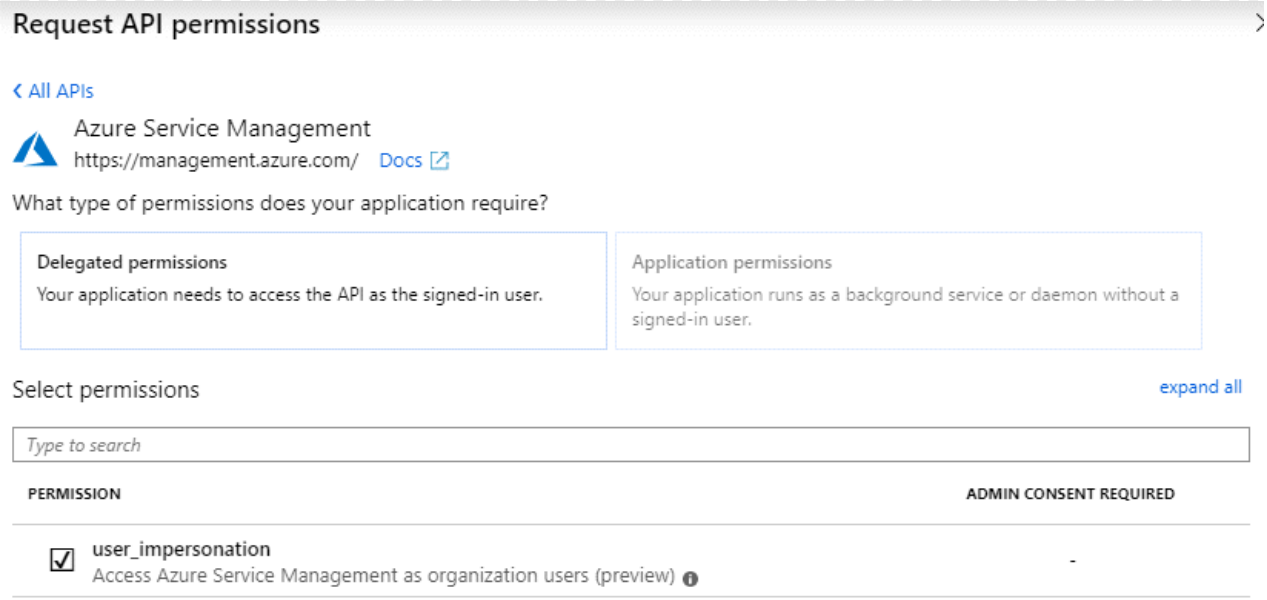
**Windows Azure** サービス管理 **API** 権限を追加する

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。

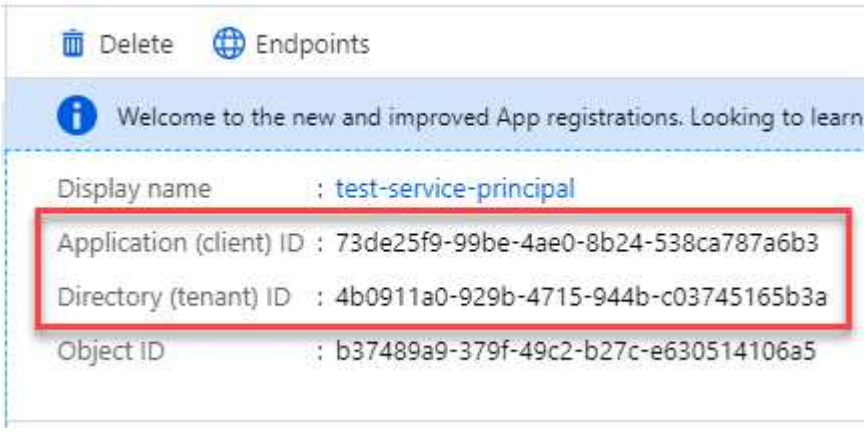



4. 組織ユーザーとして **Azure** サービス管理にアクセスする を選択し、権限の追加 を選択します。




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

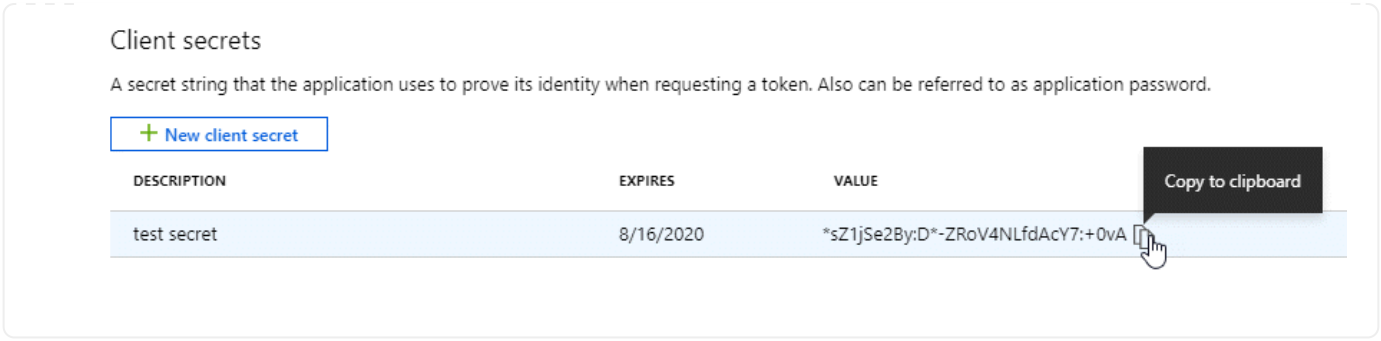
1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. アプリケーション **(**クライアント**) ID** と ディレクトリ **(**テナント**) ID** をコピーします。




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 **4.** 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。

   - 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。

# 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):<br>• クラウドフォーメーション<br>• エラスティックコンピューティングクラウド (EC2)<br>• アイデンティティとアクセス管理（IAM）<br>• キー管理サービス (KMS)<br>• セキュリティトークンサービス（STS）<br>• 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:<br>• 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.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://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。<br><br>• 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。<br><br>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" 。<br><br>• 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.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://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。<br><br>• 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。<br><br>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" 。<br><br>• 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**

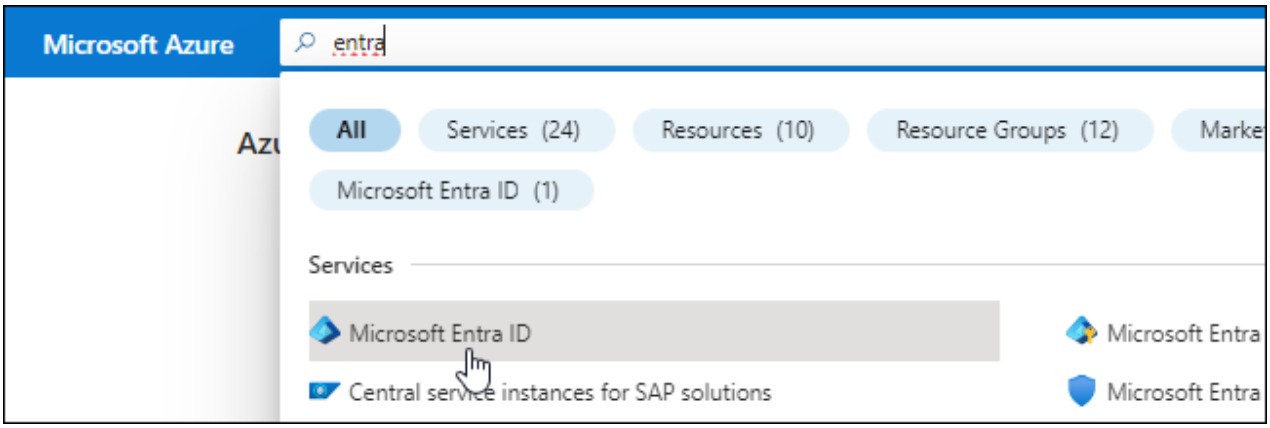
コンソール エージェントがオンプレミスでインストールされている場合は、Microsoft Entra ID でサービス プリンシパルを設定し、コンソール エージェントに必要な Azure 資格情報を取得して、コンソール エージェントに Azure 権限を付与する必要があります。

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。

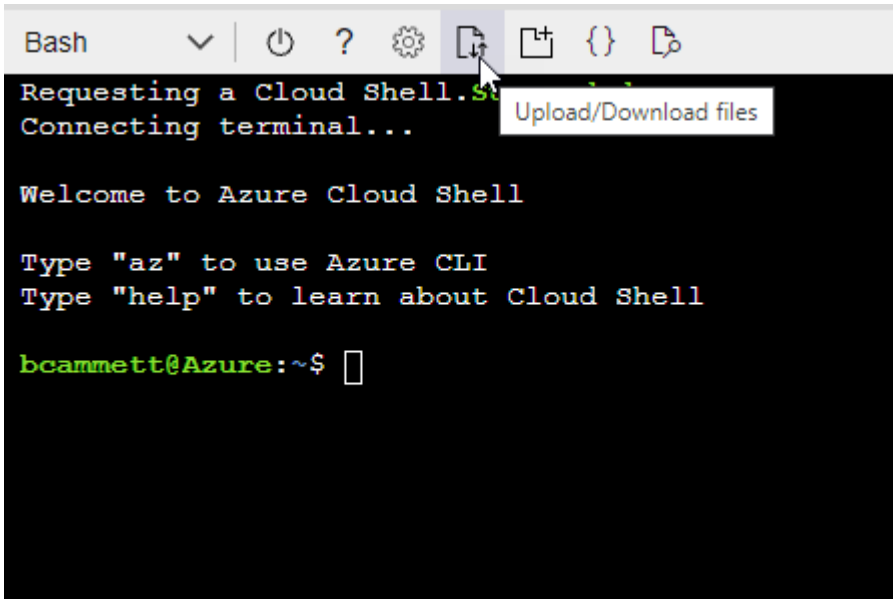
      例

```
"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。

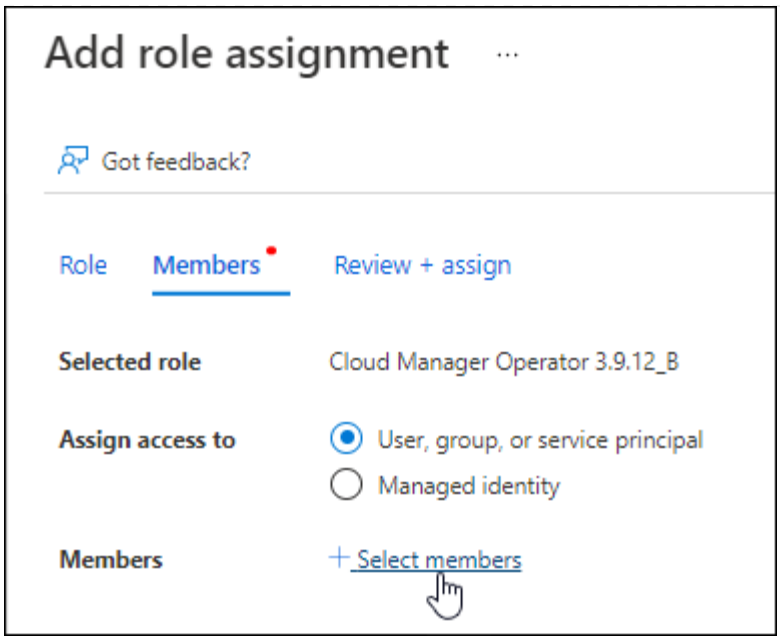
```
az role definition create --role-definition agent_Policy.json
```

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。

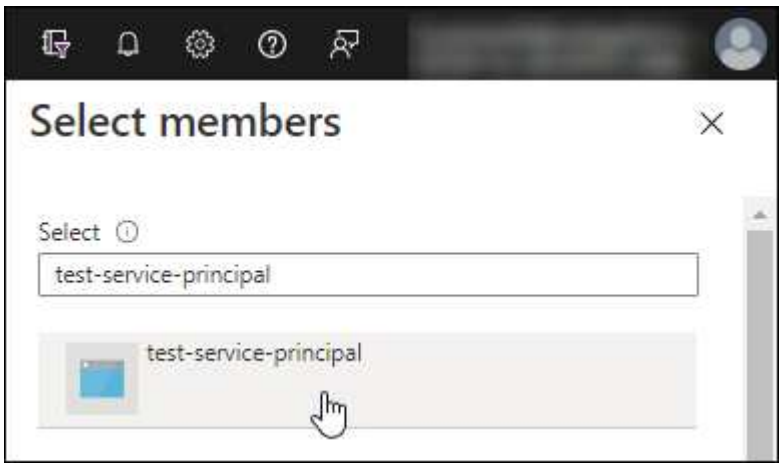
a. Azure ポータルから、サブスクリプション サービスを開きます。
b. サブスクリプションを選択します。
c. アクセス制御 **(IAM) >** 追加 **>** ロール割り当ての追加 を選択します。
d. *役割*タブで、*コンソールオペレーター*役割を選択し、*次へ*を選択します。
e. *メンバー*タブで、次の手順を実行します。

- *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。

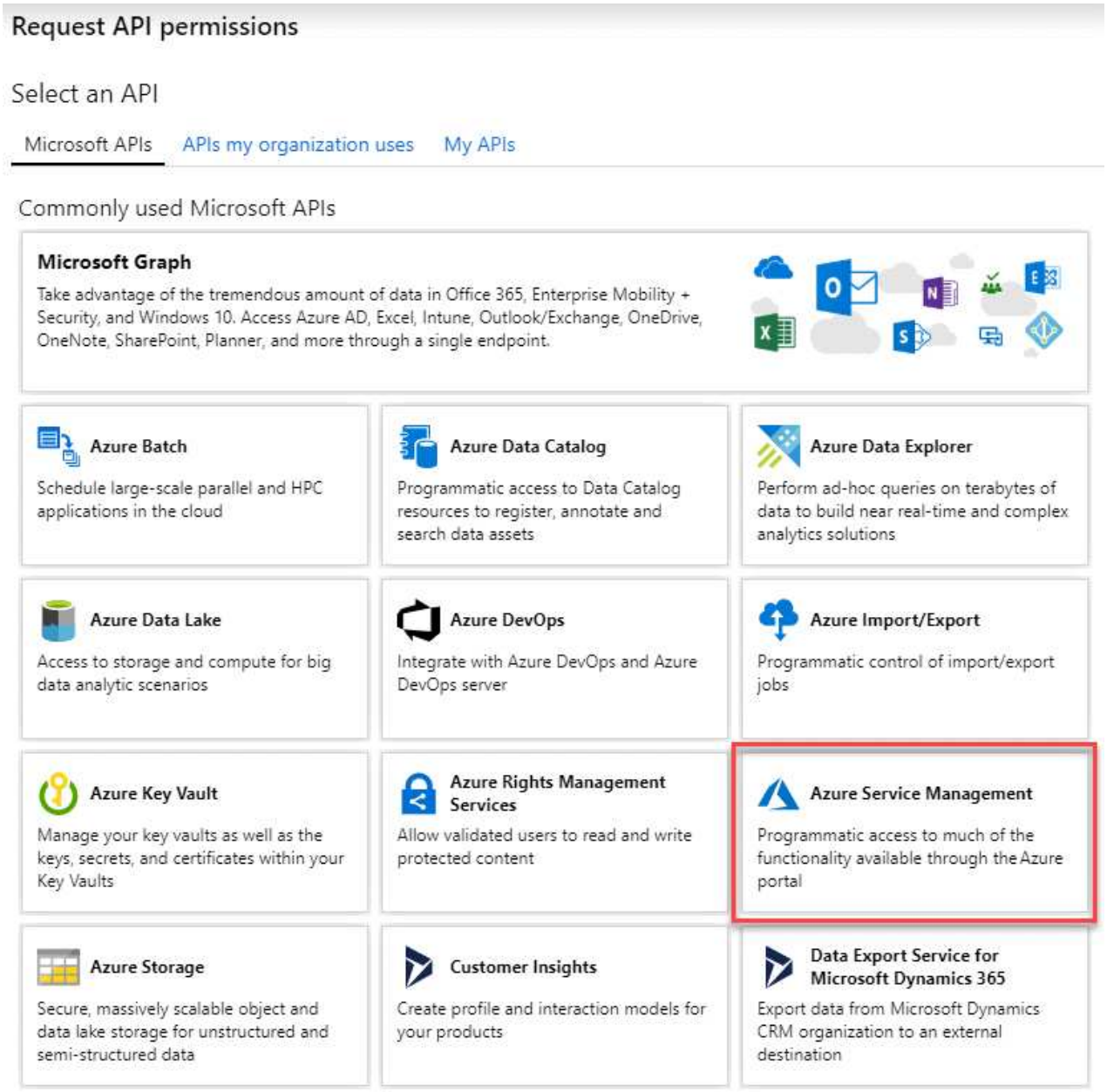
これで、サービス プリンシパルに、コンソール エージェントをデプロイするために必要な Azure アクセス許可が付与されました。

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。

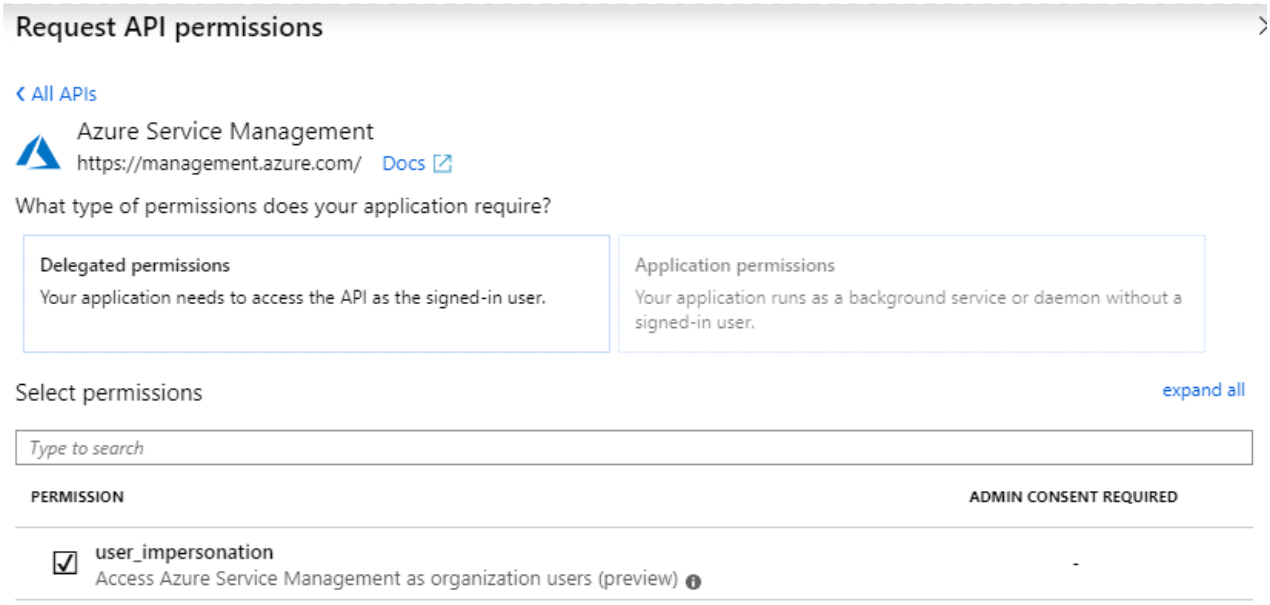
**Windows Azure** サービス管理 **API** 権限を追加する

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。

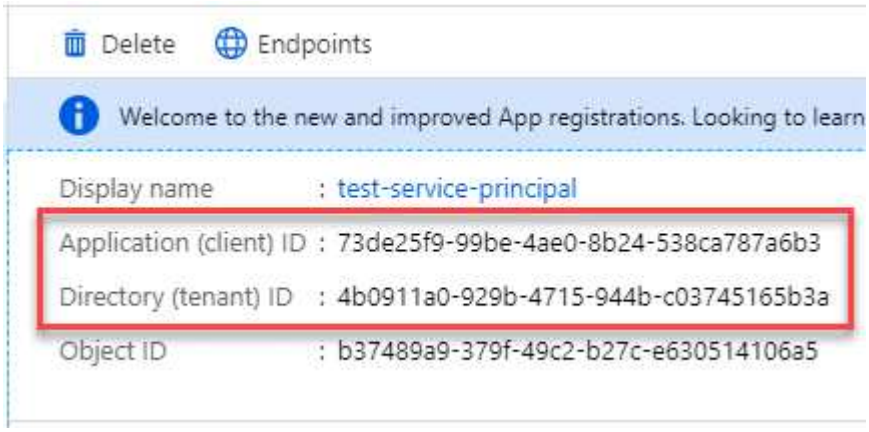



4. 組織ユーザーとして **Azure** サービス管理にアクセスする を選択し、権限の追加 を選択します。




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

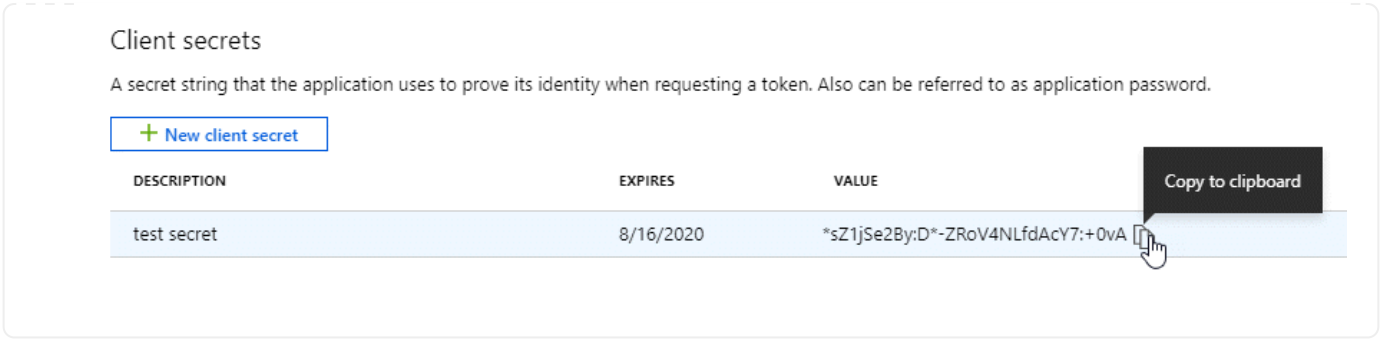
1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. アプリケーション **(**クライアント**) ID** と ディレクトリ **(**テナント**) ID** をコピーします。




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。

# 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<br>• 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 |

## コンソールエージェントのメンテナンス

コンソールエージェント用の **VCenter** または **ESXi** ホストを維持する

# コンソール エージェントを展開した後、既存の VCenter または ESXi ホストに変更を加えることができます。たとえば、コンソール エージェントをホストする VM インスタンスの CPU または RAM を増やすことができます。

VM Web コンソールを使用して次のメンテナンス タスクを実行します。

- ディスクサイズを増やす
- エージェントを再起動する
- 静的ルートを更新する
- 検索ドメインを更新する

制限事項

コンソール経由でのエージェントのアップグレードはまだサポートされていません。さらに、IP アドレス、DNS、ゲートウェイに関する情報のみを表示できます。

**VM**メンテナンスコンソールにアクセスする

VSphere クライアントからメンテナンス コンソールにアクセスできます。

手順

1. VSphere クライアントを開き、VCenter にログインします。
2. コンソール エージェントをホストする VM インスタンスを選択します。
3. **Web** コンソールの起動 を選択します。
4. VM インスタンスの作成時に指定したユーザー名とパスワードを使用して、VM インスタンスにログインします。ユーザー名は `maint`パスワードは、VM インスタンスの作成時に指定したパスワードです。

### メインユーザーのパスワードを変更する

パスワードを変更することができます `maint`ユーザー。

手順

1. VSphere クライアントを開き、VCenter にログインします。
2. コンソール エージェントをホストする VM インスタンスを選択します。
3. **Web** コンソールの起動 を選択します。
4. VM インスタンスの作成時に指定したユーザー名とパスワードを使用して、VM インスタンスにログインします。ユーザー名は `maint`パスワードは、VM インスタンスの作成時に指定したパスワードです。
5. 入力 `1`表示するには `System Configuration`メニュー。
6. 入力 `1`メンテナンス ユーザーのパスワードを変更し、画面の指示に従います。

### **VM**インスタンスの**CPU**または**RAM**を増やす

コンソール エージェントをホストする VM インスタンスの CPU または RAM を増やすことができます。

VCenter または ESXi ホストで VM インスタンス設定を編集し、メンテナンス コンソールを使用して変更を適用します。

**VSphere**クライアントでの手順

1. VSphere クライアントを開き、VCenter にログインします。
2. コンソール エージェントをホストする VM インスタンスを選択します。
3. VM インスタンスを右クリックし、[設定の編集] を選択します。
4. /opt または /var パーティションに使用されるハード ドライブの領域を増やします。
   a. /opt に使用されるハード ドライブの領域を増やすには、ハード ディスク **2** を選択します。
   b. /var に使用されるハードドライブの容量を増やすには、ハード ディスク **3** を選択します。
5. 変更を保存します。

メンテナンスコンソールの手順

1. VSphere クライアントを開き、VCenter にログインします。
2. コンソール エージェントをホストする VM インスタンスを選択します。
3. **Web** コンソールの起動 を選択します。
4. VM インスタンスの作成時に指定したユーザー名とパスワードを使用して、VM インスタンスにログインします。ユーザー名は `maint`パスワードは、VM インスタンスの作成時に指定したパスワードです。
5. 入力 `1 to view the `System Configuration`メニュー。
6. 入力 `2`画面上の指示に従います。コンソールは新しい設定をスキャンし、パーティションのサイズを増やします。

### エージェント**VM**のネットワーク設定を表示する

VSphere クライアントでエージェント VM のネットワーク設定を表示して、ネットワークの問題を確認またはトラブルシューティングします。次のネットワーク設定は表示のみ可能で、更新はできません: IP アドレス

と DNS の詳細。

手順

1. VSphere クライアントを開き、VCenter にログインします。
2. コンソール エージェントをホストする VM インスタンスを選択します。
3. **Web** コンソールの起動 を選択します。
4. VM インスタンスの作成時に指定したユーザー名とパスワードを使用して、VM インスタンスにログインします。ユーザー名は `maint`パスワードは、VM インスタンスの作成時に指定したパスワードです。
5. 入力 `2`表示するには `Network Configuration`メニュー。
6. 対応するネットワーク設定を表示するには、1 ～ 6 の数字を入力します。

### エージェント**VM**の静的ルートを更新する

必要に応じて、エージェント VM の静的ルートを追加、更新、または削除します。

手順

1. VSphere クライアントを開き、VCenter にログインします。
2. コンソール エージェントをホストする VM インスタンスを選択します。
3. **Web** コンソールの起動 を選択します。
4. VM インスタンスの作成時に指定したユーザー名とパスワードを使用して、VM インスタンスにログインします。ユーザー名は `maint`パスワードは、VM インスタンスの作成時に指定したパスワードです。
5. 入力 `2`表示するには `Network Configuration`メニュー。
6. 入力 `7`静的ルートを更新し、画面の指示に従います。
7. Enterキーを押します。
8. 必要に応じて、追加の変更を加えます。
9. 入力 `9`変更をコミットします。

### エージェント**VM**のドメイン検索設定を更新する

エージェント VM の検索ドメイン設定を更新できます。

手順

1. VSphere クライアントを開き、VCenter にログインします。
2. コンソール エージェントをホストする VM インスタンスを選択します。
3. **Web** コンソールの起動 を選択します。
4. VM インスタンスの作成時に指定したユーザー名とパスワードを使用して、VM インスタンスにログインします。ユーザー名は `maint`パスワードは、VM インスタンスの作成時に指定したパスワードです。
5. 入力 `2``表示するには `Network Configuration`メニュー。
6. 入力 `8`ドメイン検索設定を更新し、画面の指示に従います。
7. Enterキーを押します。
8. 必要に応じて、追加の変更を加えます。

9. 入力 `9`変更をコミットします。

エージェント診断ツールにアクセスする

コンソール エージェントの問題をトラブルシューティングするための診断ツールにアクセスします。 NetApp サポートは、問題のトラブルシューティング時にこれを実行するように依頼する場合があります。

手順

1. VSphere クライアントを開き、VCenter にログインします。
2. コンソール エージェントをホストする VM インスタンスを選択します。
3. **Web** コンソールの起動 を選択します。
4. VM インスタンスの作成時に指定したユーザー名とパスワードを使用して、VM インスタンスにログインします。ユーザー名は `maint`パスワードは、VM インスタンスの作成時に指定したパスワードです。
5. 入力 `3`サポートと診断メニューを表示します。
6. 入力 `1`診断ツールにアクセスし、画面上の指示に従います。 + たとえば、すべてのエージェント サービスが実行されていることを確認できます。"コンソールエージェントのステータスを確認する" 。

エージェント診断ツールにリモートでアクセスする

Putty などのツールを使用して、診断ツールにリモートでアクセスできます。ワンタイム パスワードを割り当てて、エージェント VM への SSH アクセスを有効にします。

SSH アクセスにより、コピー アンド ペーストなどの高度なターミナル機能が有効になります。

手順

1. VSphere クライアントを開き、VCenter にログインします。
2. コンソール エージェントをホストする VM インスタンスを選択します。
3. **Web** コンソールの起動 を選択します。
4. VM インスタンスの作成時に指定したユーザー名とパスワードを使用して、VM インスタンスにログインします。ユーザー名は `maint`パスワードは、VM インスタンスの作成時に指定したパスワードです。
5. 入力 `3`表示するには `Support and Diagnostics`メニュー。
6. 入力 `2`診断ツールにアクセスし、画面上の指示に従って 24 時間で期限が切れるワンタイム パスワードを設定します。
7. PuttyなどのSSHツールを使用して、ユーザー名でエージェントVMに接続します。 `diag`および設定したワンタイムパスワード。

**Web**ベースのコンソールアクセス用に**CA**署名証明書をインストールする

NetApp Consoleを制限モードで使用する場合、クラウド リージョンまたはオンプレミスに展開されているコンソール エージェント仮想マシンからユーザー インターフェイスにアクセスできます。デフォルトでは、コンソールは自己署名 SSL 証明書を使用して、コンソール エージェント上で実行されている Web ベースのコンソールへの安全な HTTPS アクセスを提供します。

ビジネスで必要な場合は、証明機関 (CA) によって署名された証明書をインストールできます。これにより、

自己署名証明書よりも優れたセキュリティ保護が提供されます。証明書をインストールすると、ユーザーがWeb ベースのコンソールにアクセスするときに、コンソールは CA 署名付き証明書を使用します。

#### HTTPS証明書をインストールする

コンソール エージェント上で実行されている Web ベースのコンソールに安全にアクセスするために、CA によって署名された証明書をインストールします。

タスク概要

次のいずれかのオプションを使用して証明書をインストールできます。

- コンソールから証明書署名要求 (CSR) を生成し、証明書要求を CA に送信して、CA 署名証明書をコンソール エージェントにインストールします。

  コンソールが CSR を生成するために使用するキー ペアは、コンソール エージェントに内部的に保存されます。コンソール エージェントに証明書をインストールすると、コンソールは同じキー ペア (秘密キー) を自動的に取得します。

- すでに持っている CA 署名付き証明書をインストールします。

  このオプションを選択すると、CSR はコンソールを通じて生成されません。 CSR を別途生成し、秘密鍵を外部に保存します。証明書をインストールするときに、コンソールに秘密キーを提供します。

手順

1. *管理 > エージェント*を選択します。
2. *概要*ページで、コンソール エージェントのアクション メニューを選択し、*HTTPS セットアップ*を選択します。

   編集するには、コンソール エージェントに接続する必要があります。

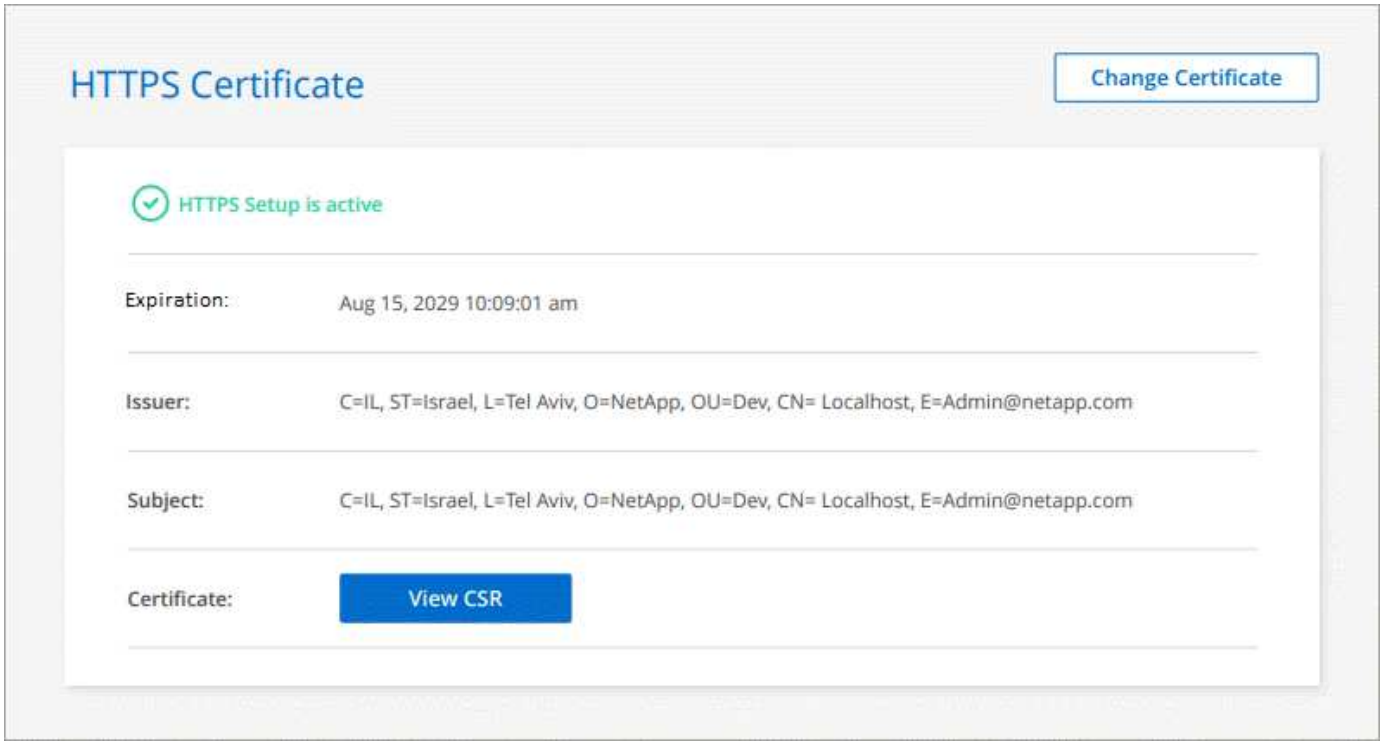
3. HTTPS セットアップ ページで、証明書署名要求 (CSR) を生成するか、独自の CA 署名証明書をインストールして証明書をインストールします。

| オプション | 説明 |
| --- | --- |
| CSRを生成する | a. コンソール エージェント ホストのホスト名または DNS (共通名) を入力し、[CSR の生成] を選択します。<br><br>コンソールに証明書署名要求が表示されます。<br><br>b. CSR を使用して、SSL 証明書要求を CA に送信します。<br><br>証明書には、Privacy Enhanced Mail (PEM) Base-64 エンコード X.509 形式を使用する必要があります。<br><br>c. 証明書ファイルをアップロードし、[インストール] を選択します。 |

| オプション | 説明 |
| --- | --- |
| 独自のCA署名証明書をインストールする | a. *CA 署名証明書のインストール*を選択します。<br>b. 証明書ファイルと秘密キーの両方をロードし、[インストール] を選択します。<br><br>証明書には、Privacy Enhanced Mail (PEM) Base-64 エンコード X.509 形式を使用する必要があります。 |

結果

コンソール エージェントは、CA 署名証明書を使用して安全な HTTPS アクセスを提供するようになりました。次の画像は、安全なアクセス用に構成されたエージェントを示しています。




### コンソールの**HTTPS**証明書を更新する

安全なアクセスを確保するには、エージェントの HTTPS 証明書が期限切れになる前に更新する必要があります。証明書の有効期限が切れる前に更新しないと、ユーザーが HTTPS を使用して Web コンソールにアクセスしたときに警告が表示されます。

手順

1. *管理 > エージェント*を選択します。
2. *概要*ページで、コンソール エージェントのアクション メニューを選択し、*HTTPS セットアップ*を選択します。

   有効期限を含む証明書の詳細が表示されます。
3. *証明書の変更*を選択し、手順に従って CSR を生成するか、独自の CA 署名証明書をインストールします。

プロキシサーバーを使用するようにコンソールエージェントを構成する

# 企業ポリシーでインターネットへのすべての通信にプロキシ サーバーの使用が求められている場合は、そのプロキシ サーバーを使用するようにエージェントを構成する必要があります。インストール時にコンソール エージェントがプロキシ サーバーを使用するように構成しなかった場合は、いつでもそのプロキシ サーバーを使用するようにコンソール エージェントを構成できます。

エージェントのプロキシ サーバーは、パブリック IP または NAT ゲートウェイなしでアウトバウンドのインターネット アクセスを可能にします。プロキシ サーバーは、Cloud Volumes ONTAPシステムではなく、コンソール エージェントに対してのみ送信接続を提供します。

Cloud Volumes ONTAPシステムにアウトバウンド インターネット アクセスがない場合、コンソールはコンソール エージェントのプロキシ サーバーを使用するようにシステムを構成します。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必要があります。コンソール エージェントを展開した後、このポートを開きます。

コンソール エージェント自体に送信インターネット接続がない場合、 Cloud Volumes ONTAPシステムは構成されたプロキシ サーバーを使用できません。

## サポートされている構成

- Cloud Volumes ONTAPシステムにサービスを提供するエージェントでは、透過プロキシ サーバーがサポートされています。 Cloud Volumes ONTAPでNetAppデータ サービスを使用する場合は、透過プロキシ サーバーを使用できるCloud Volumes ONTAP専用のエージェントを作成します。
- 明示的なプロキシ サーバーは、 Cloud Volumes ONTAPシステムを管理するエージェントやNetAppデータ サービスを管理するエージェントを含むすべてのエージェントでサポートされています。
- HTTP と HTTPS。
- プロキシ サーバーはクラウドまたはネットワーク内に配置できます。

> プロキシを設定したら、プロキシの種類を変更することはできません。プロキシ タイプを変更する必要がある場合は、コンソール エージェントを削除し、新しいプロキシ タイプで新しいエージェントを追加します。

## コンソールエージェントで明示的なプロキシを有効にする

プロキシ サーバーを使用するようにコンソール エージェントを構成すると、そのエージェントとそれが管理するCloud Volumes ONTAPシステム (HA メディエーターを含む) はすべてプロキシ サーバーを使用します。

この操作により、コンソール エージェントが再起動されます。続行する前に、コンソール エージェントがアイドル状態であることを確認してください。

### 手順

1. *管理 > エージェント*を選択します。
2. *概要*ページで、コンソール エージェントのアクション メニューを選択し、*エージェントの編集*を選択します。

   編集するには、コンソール エージェントがアクティブである必要があります。

3. *HTTP プロキシ構成*を選択します。
4. 構成タイプ フィールドで 明示的なプロキシ を選択します。
5. *プロキシを有効にする*を選択します。
6. 構文を使用してサーバーを指定します <a href="http://<em>address:port</em>" class="bare">http://<em>address:port</em></a>または <a href="https://<em>address:port</em>" class="bare">https://<em>address:port</em></a>
7. サーバーに基本認証が必要な場合は、ユーザー名とパスワードを指定します。

   次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 ユーザーになります。
   - ドメインユーザーの場合は、\ の ASCII コードを次のように入力する必要があります: domain-name%92user-name

     例: netapp%92proxy

   - コンソールは @ 文字を含むパスワードをサポートしていません。
8. *保存*を選択します。

コンソールエージェントの透過プロキシを有効にする

Cloud Volumes ONTAPのみが、コンソール エージェントでの透過プロキシの使用をサポートしています。Cloud Volumes ONTAPに加えてNetAppデータ サービスを使用する場合は、データ サービス用またはCloud Volumes ONTAP用として別のエージェントを作成する必要があります。

透過プロキシを有効にする前に、次の要件が満たされていることを確認してください。

- エージェントは、透過プロキシ サーバーと同じネットワークにインストールされます。
- プロキシ サーバーで TLS 検査が有効になっています。
- 透過プロキシ サーバーで使用されている証明書と一致する PEM 形式の証明書があります。
- Cloud Volumes ONTAP以外のNetAppデータ サービスにはコンソール エージェントを使用しないでください。

既存のエージェントを透過プロキシ サーバーを使用するように構成するには、コンソール エージェント ホストのコマンド ラインから使用できるコンソール エージェント メンテナンス ツールを使用します。

プロキシ サーバーを構成すると、コンソール エージェントが再起動します。続行する前に、コンソール エージェントがアイドル状態であることを確認してください。

手順

プロキシ サーバーの PEM 形式の証明書ファイルがあることを確認します。証明書がない場合は、ネットワーク管理者に問い合わせて取得してください。

1. コンソール エージェント ホストでコマンド ライン インターフェイスを開きます。
2. コンソール エージェント メンテナンス ツール ディレクトリに移動します。
   `/opt/application/netapp/service-manager-2/agent-maint-console`
3. 透過プロキシを有効にするには、次のコマンドを実行します。 `/home/ubuntu/<certificate-file>.pem`プロ

キシ サーバーのディレクトリと証明書ファイルの名前です。

```
./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

証明書ファイルが PEM 形式であり、コマンドと同じディレクトリに存在することを確認するか、証明書ファイルへのフルパスを指定します。

```
./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

コンソールエージェントの透過プロキシを変更する

コンソールエージェントの既存の透過プロキシサーバーを更新するには、 `proxy update`コマンドを使用して透過プロキシサーバーを削除するか、 `proxy remove`指示。詳細については、次のドキュメントを参照してください。"エージェントメンテナンスコンソール" 。

プロキシを設定したら、プロキシの種類を変更することはできません。プロキシ タイプを変更する必要がある場合は、コンソール エージェントを削除し、新しいプロキシ タイプで新しいエージェントを追加します。

インターネットへのアクセスが失われた場合は、コンソールエージェントプロキシを更新します。

ネットワークのプロキシ構成が変更されると、エージェントはインターネットにアクセスできなくなる可能性があります。たとえば、誰かがプロキシ サーバーのパスワードを変更したり、証明書を更新したりした場合などです。この場合、コンソール エージェント ホストから直接 UI にアクセスし、設定を更新する必要があります。コンソール エージェント ホストへのネットワーク アクセスがあり、コンソールにログインできることを確認します。

直接**API**トラフィックを有効にする

プロキシ サーバーを使用するようにコンソール エージェントを構成した場合は、プロキシを経由せずに API 呼び出しをクラウド プロバイダー サービスに直接送信するために、コンソール エージェントで直接 API トラフィックを有効にすることができます。AWS、Azure、または Google Cloud で実行されているエージェントはこのオプションをサポートします。

Cloud Volumes ONTAPで Azure Private Links を無効にしてサービス エンドポイントを使用する場合は、直接 API トラフィックを有効にします。そうしないと、トラフィックは適切にルーティングされません。

"Cloud Volumes ONTAPで Azure Private Link またはサービス エンドポイントを使用する方法の詳細"

手順

1. *管理 > エージェント*を選択します。
2. *概要*ページで、コンソール エージェントのアクション メニューを選択し、*エージェントの編集*を選択します。

   編集するには、コンソール エージェントがアクティブである必要があります。

3. *直接 API トラフィックのサポート*を選択します。

4. チェックボックスを選択してオプションを有効にし、[保存] を選択します。

コンソールエージェントのトラブルシューティング

# コンソール エージェントの問題をトラブルシューティングするには、自分で問題を確認するか、 NetAppサポートに問い合わせて、システム ID、エージェント バージョン、または最新のAutoSupportメッセージを尋ねられることがあります。

NetAppサポートサイトのアカウントをお持ちの場合は、"NetAppナレッジベース。"

一般的なエラーメッセージと解決策

次の表に、一般的なエラー メッセージとその修正方法を示します。

| エラー メッセージ | 説明 | 何をするか |
| --- | --- | --- |
| コンソールエージェントUIを読み込めません | エージェントのインストールに失敗しました | • Service Manager サービスがアクティブであることを確認します。<br>• すべてのコンテナが実行されていることを確認します。<br>• ファイアウォールがポート 8888 でのサービスへのアクセスを許可していることを確認してください。<br>• それでも問題が解決しない場合は、サポートにお問い合わせください。 |
| NetAppエージェントUIにアクセスできません | このメッセージは、エージェントの IP アドレスにアクセスしようとしたときに表示されます。エージェントに適切なネットワーク アクセスがない場合や不安定な場合は、初期化に失敗する可能性があります。 | • コンソール エージェントに接続します。<br>• サービスマネージャサービスを確認する<br>• エージェントに必要なネットワーク アクセス権があることを確認します。"必要なネットワーク アクセス エンドポイントの詳細について説明します。" |
| エージェント設定を読み込めません | エージェント設定ページにアクセスしようとすると、コンソールにこのメッセージが表示されます。 | • OCCM コンテナが実行中であり、動作しているかどうかを確認します。<br>• 問題が解決しない場合は、サポートにお問い合わせください。 |

| エラー メッセージ | 説明 | 何をするか |
| --- | --- | --- |
| エージェントのサポート情報を読み込めません。 | エージェントがサポート アカウントにアクセスできない場合、このメッセージが表示されます。 | • 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権を持っていることを確認します。"必要なネットワーク アクセス エンドポイントの詳細について説明します。" |

コンソールエージェントのステータスを確認する

コンソール エージェントを確認するには、次のいずれかのコマンドを使用します。すべてのサービスのステータスは「実行中」になっている必要があります。そうでない場合は、 NetAppサポートにお問い合わせください。

コンソール エージェント診断へのアクセスの詳細については、次のトピックを参照してください。

- "コンソール エージェントのステータスを確認する (Linux ホスト展開の場合)"
- "コンソール エージェントのステータスを確認する (VCenter 展開の場合)"

**Docker (Ubuntu** および **VCenter** のデプロイメント用)

```
docker ps -a
```

**Podman (RedHat Enterprise Linux** デプロイメント用)

```
podman ps -a
```

コンソールエージェントのバージョンを表示する

コンソール エージェントのバージョンを表示してアップグレードを確認するか、 NetApp の担当者と共有してください。

手順

1. *管理 > サポート > エージェント*を選択します。

   コンソールのページ上部にバージョンが表示されます。

ネットワークアクセスを確認する

コンソール エージェントに必要なネットワーク アクセスがあることを確認します。"必要なネットワーク アクセス ポイントの詳細について説明します。"

コンソールエージェントで構成チェックを実行する

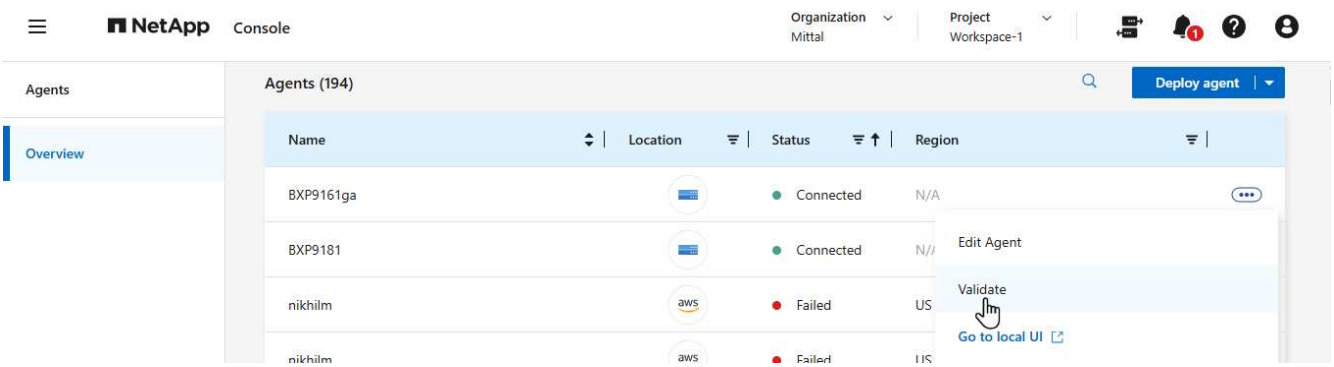
コンソールまたはエージェント メンテナンス コンソールからコンソール エージェントの構成チェックを実行し、それらが接続されていることを確認します。

エージェント メンテナンス コンソールを使用して構成チェックを実行することもできます。"config-checker validate コマンドの使用について詳しく学習します。"

ステータスが「接続済み」であるエージェントのみを検証できます。

コンソールからの手順

1. *管理 > エージェント*を選択します。
2. 確認するコンソール エージェントのアクション メニューを選択し、[検証] を選択します。




検証には最大 15 分かかる場合があります。完了すると結果が表示されます。

コンソールエージェントのインストールに関する問題

インストールに失敗した場合は、レポートとログを表示して問題を解決してください。

次のディレクトリにあるコンソール エージェント ホストから、JSON 形式の検証レポートと構成ログに直接アクセスすることもできます。

```
/tmp/netapp-console-agents/logs

/tmp/netapp-console-agents/results.json
```

- 新しいエージェントの展開では、 NetApp は次のエンドポイントをチェックします。"ここに記載" 。アップグレードに使用した以前のエンドポイントを使用している場合、この構成チェックはエラーで失敗します。"ここに記載" 。 NetAppは、現在のエンドポイントへのアクセスを許可し、以前のエンドポイントへのアクセスをブロックするようにファイアウォールルールを更新することを推奨します。"ネットワークをアップデートする方法を学ぶ" 。
- ファイアウォールのエンドポイントを更新しても、既存のエージェントは引き続き動作します。

手動インストールの構成チェックを無効にする

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る場合があります。たとえば、Government Cloud 環境にエージェントを手動でインストールする場合は、構成チェックを無効にする必要があります。無効にしないと、インストールは失敗します。

手順

*com/opt/application/netapp/service-manager-2/config.json* ファイルで *skipConfigCheck* フラグを設定することで、構成チェックを無効にします。デフォルトでは、このフラグは false に設定されており、構成チェックによってエージェントの送信アクセスが検証されます。チェックを無効にするには、このフラグを true に設定します。この手順を完了する前に、JSON 構文を理解しておいてください。

構成チェックを再度有効にするには、次の手順に従い、*skipConfigCheck* フラグを false に設定します。

手順

1. コンソール エージェント ホストに root または sudo 権限でアクセスします。
2. 変更を元に戻せるように、*/opt/application/netapp/service-manager-2/config.json* ファイルのバックアップコピーを作成します。
3. 次のコマンドを実行して、サービス マネージャー 2 サービスを停止します。

```
systemctl stop netapp-service-manager.service
```

1. */opt/application/netapp/service-manager-2/config.json* ファイルを編集し、*skipConfigCheck* フラグの値を true に変更します。

```
  "skipConfigCheck": true
```

2. ファイルを保存します。
3. 次のコマンドを実行して、サービス マネージャー 2 サービスを再起動します。

```
systemctl restart netapp-service-manager.service
```

#### NetAppサポートと連携する

コンソール エージェントの問題を解決できない場合は、 NetAppサポートにお問い合わせください。 NetAppサポートでは、コンソール エージェント ID を要求したり、コンソール エージェント ログがまだない場合はそれを送信するよう要求したりすることがあります。

#### コンソールエージェントIDを見つける

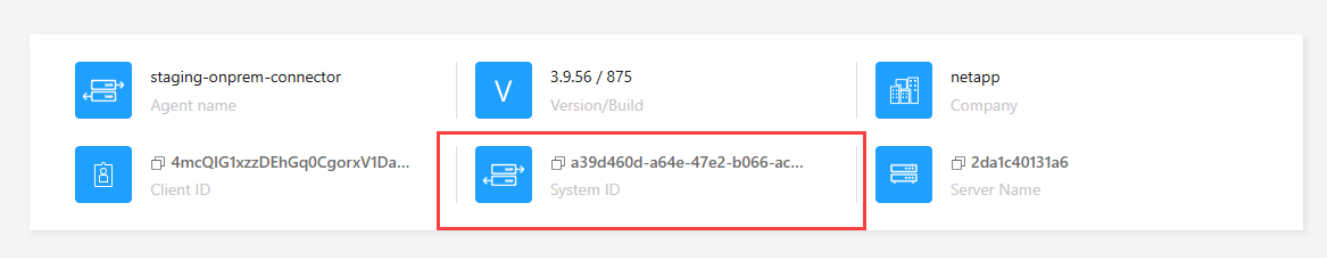
作業を開始するには、コンソール エージェントのシステム ID が必要になる場合があります。 ID は通常、ライセンスとトラブルシューティングの目的で使用されます。

手順

1. *管理 > サポート > エージェント*を選択します。

   システム ID はページの上部にあります。

   例




2. ID にマウスを合わせてクリックするとコピーできます。

### AutoSupportメッセージをダウンロードまたは送信する

問題が発生した場合、 NetApp はトラブルシューティングのためにAutoSupportメッセージをNetAppサポートに送信するように依頼することがあります。

NetApp Consoleは、負荷分散のため、 AutoSupportメッセージを送信するのに最大 5 時間かかります。緊急の場合は、ファイルをダウンロードして手動で送信してください。

手順

1. *管理 > サポート > エージェント*を選択します。
2. NetAppサポートに情報を送信する方法に応じて、次のいずれかのオプションを選択します。
   a. AutoSupportメッセージをローカル マシンにダウンロードするオプションを選択します。その後、優先する方法を使用してNetAppサポートに送信できます。
   b. **Send AutoSupport** を選択すると、メッセージがNetAppサポートに直接送信されます。

#### Google Cloud NAT ゲートウェイ使用時のダウンロード失敗を修正

コンソール エージェントは、 Cloud Volumes ONTAPのソフトウェア アップデートを自動的にダウンロードします。 Google Cloud NAT ゲートウェイを使用している場合、設定によりダウンロードが失敗する可能性があります。ソフトウェア イメージを分割する部分の数を制限することで、この問題を修正できます。この手順は API を使用して完了する必要があります。

手順

1. 次の JSON を本文として、PUT リクエストを /occm/config に送信します。

```
{
  "maxDownloadSessions": 32
}
```

*maxDownloadSessions* の値は 1 または 1 より大きい任意の整数にすることができます。値が 1 の場合、ダウンロードされたイメージは分割されません。

32 は例の値であることに注意してください。値は NAT 構成と同時セッションの数によって異なります。

"/occm/config API呼び出しの詳細"

**NetApp**ナレッジベースからヘルプを入手する

"NetAppサポートチームが作成したトラブルシューティング情報を表示します" 。

コンソールエージェントをアンインストールして削除する

問題をトラブルシューティングしたり、ホストから完全に削除したりするには、コンソール エージェントをアンインストールします。実行する必要がある手順は、使用している展開モードによって異なります。環境からコンソール エージェントを削除したら、コンソールからも削除できます。

"NetApp Consoleの導入モードについて学ぶ" 。

標準モードまたは制限モードを使用している場合はエージェントをアンインストールします

標準モードまたは制限モードを使用している場合 (つまり、エージェント ホストに送信接続がある場合)、以下の手順に従ってエージェントをアンインストールする必要があります。

手順

1. エージェントの Linux VM に接続します。
2. Linux ホストから、アンインストール スクリプトを実行します。

   ```
   /opt/application/netapp/service-manager-2/uninstall.sh [silent]
   ```

   *silent* は確認を求めることなくスクリプトを実行します。

コンソールからコンソールエージェントを削除する

エージェント VM を削除した場合、またはエージェントをアンインストールした場合は、コンソールのエージェントのリストからそれを削除する必要があります。エージェント VM を削除するか、エージェント ソフトウェアをアンインストールすると、コンソールでエージェントのステータスが 切断 と表示されます。

コンソール エージェントを削除する場合は、次の点に注意してください。

- このアクションでは仮想マシンは削除されません。
- このアクションは元に戻すことはできません。コンソール エージェントを削除すると、再度追加することはできません。

手順

1. *管理 > エージェント*を選択します。
2. *概要*ページで、切断されたエージェントのアクション メニューを選択し、*エージェントの削除*を選択します。
3. 確認のためにエージェントの名前を入力し、「削除」を選択します。

## クラウド プロバイダの資格情報を管理する

# AWS

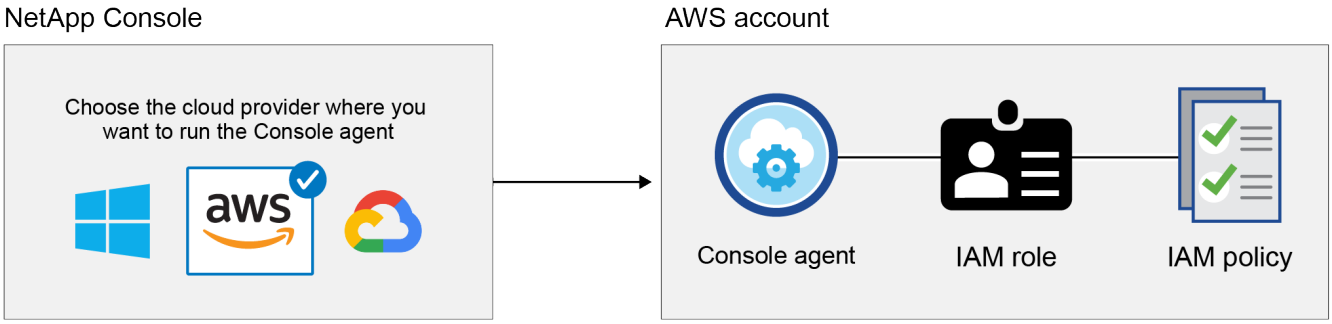
## NetApp ConsoleのAWS認証情報と権限について学習します

コンソールエージェントの導入時に適切な IAM 認証情報を提供し、課金のためにそれらを AWS Marketplace サブスクリプションに関連付けることで、 NetApp ConsoleからAWS 認証情報とマーケットプレイス サブスクリプションを直接管理し、 Cloud Volumes ONTAPやその他のデータ サービスの安全な導入を確保します。

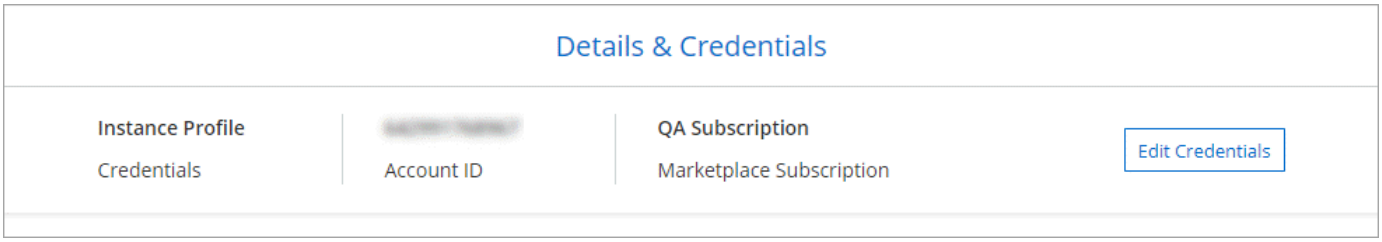
### 初期AWS認証情報

コンソールからコンソールエージェントをデプロイする場合は、IAM ロールの ARN または IAM ユーザーのアクセスキーを指定する必要があります。認証方法には、AWS にコンソールエージェントをデプロイするための権限が必要です。必要な権限は、"AWS のエージェント展開ポリシー" 。

コンソールが AWS でコンソールエージェントを起動すると、エージェントの IAM ロールとプロファイルが作成されます。また、コンソールエージェントにその AWS アカウント内のリソースとプロセスを管理するための権限を付与するポリシーも添付します。"エージェントが権限をどのように使用するか確認する"。




新しいCloud Volumes ONTAPシステムを追加すると、コンソールはデフォルトで次の AWS 認証情報を選択します。




初期の AWS 認証情報を使用してすべてのCloud Volumes ONTAPシステムを展開するか、追加の認証情報を追加することができます。

### 追加のAWS認証情報

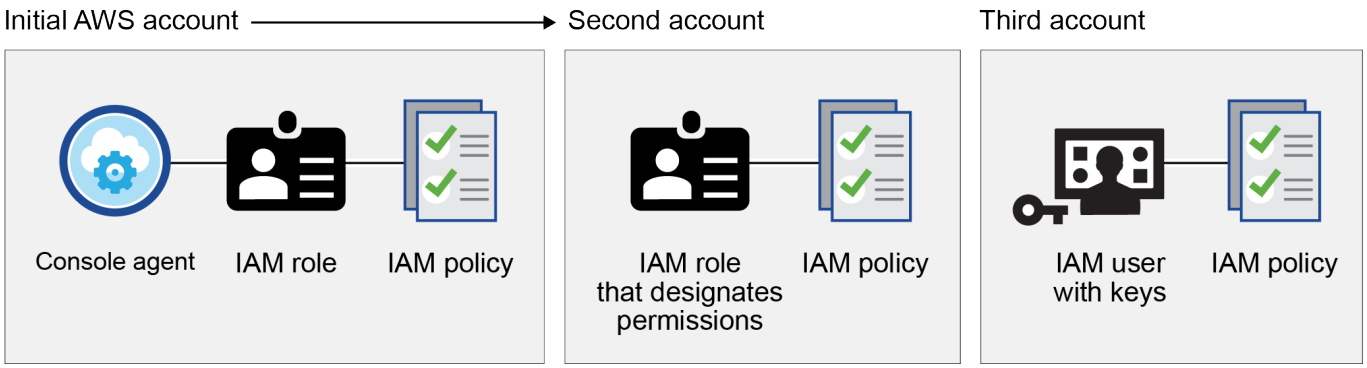
次の場合には、コンソールに追加の AWS 認証情報を追加する必要があるかもしれません。

- 既存のコンソールエージェントを追加のAWSアカウントで使用するには
- 特定のAWSアカウントに新しいエージェントを作成するには
- FSx for ONTAPファイルシステムを作成および管理するには

詳細については、以下のセクションを確認してください。

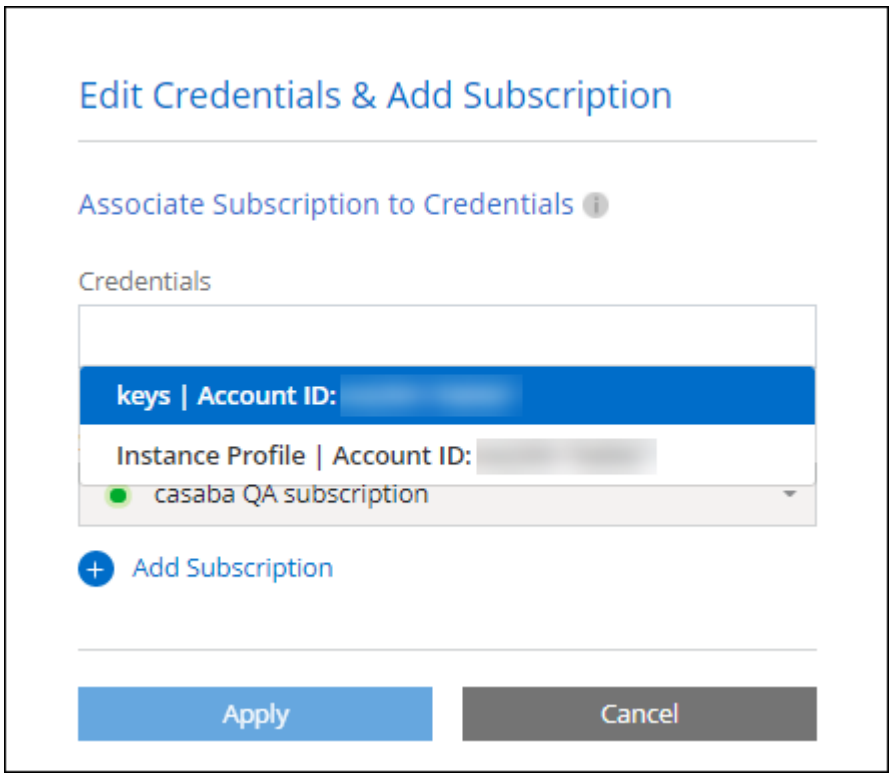
別の **AWS** アカウントでコンソールエージェントを使用するには、**AWS** 認証情報を追加します。

追加の AWS アカウントでコンソールを使用するには、信頼できるアカウントの AWS キーまたはロールの ARN を指定します。次の図は、信頼できるアカウントの IAM ロールを通じて権限を提供するアカウントと、IAM ユーザーの AWS キーを通じて権限を提供するアカウントの 2 つの追加アカウントを示しています。




IAM ロールの Amazon リソースネーム (ARN) または IAM ユーザーの AWS キーを指定して、コンソールにアカウント認証情報を追加します。

たとえば、新しいCloud Volumes ONTAPシステムを作成するときに、資格情報を切り替えることができます。




"既存のエージェントに AWS 認証情報を追加する方法を学びます。"

### コンソールエージェントを作成するには**AWS**認証情報を追加します

AWS 認証情報を追加すると、コンソールエージェントを作成するための権限が付与されます。

"コンソールエージェントを作成するためにコンソールにAWS認証情報を追加する方法を学びます"

### **FSx for ONTAP**に **AWS** 認証情報を追加する

FSx for ONTAPシステムを作成および管理するために必要な権限を付与するには、コンソールに AWS 認証情報を追加します。

"Amazon FSx for ONTAPのコンソールに AWS 認証情報を追加する方法を学びます"

### 資格情報とマーケットプレイスのサブスクリプション

Cloud Volumes ONTAPやその他のNetAppデータ サービスの料金を時間単位 (PAYGO) または年間契約で支払うには、コンソール エージェントに追加する認証情報を AWS Marketplace サブスクリプションに関連付ける必要があります。"AWSサブスクリプションを関連付ける方法を学ぶ"。

AWS 認証情報とマーケットプレイスサブスクリプションについては、次の点に注意してください。

- AWS 認証情報のセットに関連付けることができるのは、1 つの AWS Marketplace サブスクリプションのみです。
- 既存のマーケットプレイスサブスクリプションを新しいサブスクリプションに置き換えることができます

### FAQ

次の質問は、資格情報とサブスクリプションに関連しています。

#### **AWS** 認証情報を安全にローテーションするにはどうすればよいですか**?**

上のセクションで説明したように、コンソールでは、コンソールエージェントに関連付けられた IAM ロール、信頼できるアカウントでの IAM ロールの引き受け、または AWS アクセスキーの提供など、いくつかの方法で AWS 認証情報を提供できます。

最初の 2 つのオプションでは、コンソールは AWS セキュリティ トークン サービスを使用して、常にローテーションする一時的な認証情報を取得します。このプロセスはベストプラクティスであり、自動かつ安全です。

コンソールに AWS アクセスキーを提供する場合は、コンソールで定期的にキーを更新してキーをローテーションする必要があります。これは完全に手動のプロセスです。

#### **Cloud Volumes ONTAP**システムの **AWS Marketplace** サブスクリプションを変更できますか**?**

はい、できます。認証情報セットに関連付けられている AWS Marketplace サブスクリプションを変更すると、既存および新規のすべてのCloud Volumes ONTAPシステムに新しいサブスクリプションの料金が課金されます。

"AWSサブスクリプションを関連付ける方法を学ぶ" 。

### それぞれ異なるマーケットプレイスサブスクリプションを持つ複数の **AWS** 認証情報を追加できますか**?**

同じ AWS アカウントに属するすべての AWS 認証情報は、同じ AWS Marketplace サブスクリプションに関連付けられます。

異なる AWS アカウントに属する複数の AWS 認証情報がある場合、それらの認証情報は、同じ AWS Marketplace サブスクリプションまたは異なるサブスクリプションに関連付けることができます。

### 既存の**Cloud Volumes ONTAP**システムを別の **AWS** アカウントに移動できますか**?**

いいえ、 Cloud Volumes ONTAPシステムに関連付けられている AWS リソースを別の AWS アカウントに移動することはできません。

### マーケットプレイスの展開とオンプレミスの展開では資格情報はどのように機能しますか**?**

上記のセクションでは、コンソールからのコンソール エージェントの推奨展開方法について説明しています。また、AWS Marketplace から AWS にエージェントを展開し、独自の Linux ホストまたは VCenter にコンソールエージェントソフトウェアを手動でインストールすることもできます。

Marketplace を使用する場合も、同様の方法で権限が提供されます。 IAM ロールを手動で作成して設定し、追加のアカウントに権限を付与するだけです。

オンプレミス展開の場合、コンソールに IAM ロールを設定することはできませんが、AWS アクセスキーを使用して権限を付与することはできます。

権限の設定方法については、次のページを参照してください。

- 標準モード
  - "AWS Marketplace デプロイメントの権限を設定する"
  - "オンプレミス展開の権限を設定する"
- 制限モード
  - "制限モードの権限を設定する"

**NetApp Console**の **AWS** 認証情報とマーケットプレイス サブスクリプションを管理する

AWS 認証情報を追加および管理して、 NetApp Consoleから AWS アカウント内のクラウド リソースを展開および管理できるようにします。複数の AWS Marketplace サブスクリプションを管理する場合は、[認証情報] ページから各サブスクリプションを異なる AWS 認証情報に割り当てることができます。

#### 概要

AWS 認証情報を既存のコンソールエージェントに追加することも、コンソールに直接追加することもできます。

- 既存のエージェントにAWS認証情報を追加する

  クラウド リソースを管理するには、コンソール エージェントに AWS 認証情報を追加します。コンソールエージェントにAWS認証情報を追加する方法を学びます 。

- コンソールエージェントを作成するためにコンソールにAWS認証情報を追加する

  コンソールに新しい AWS 認証情報を追加すると、コンソールエージェントを作成するために必要な権限が付与されます。NetApp ConsoleにAWS認証情報を追加する方法を学びます 。

- FSx for ONTAPのコンソールに AWS 認証情報を追加する

  FSx for ONTAPを作成および管理するには、コンソールに新しい AWS 認証情報を追加します。 "FSx for ONTAPの権限を設定する方法を学びます"

資格情報をローテーションする方法

NetApp Consoleを使用すると、エージェント インスタンスに関連付けられた IAM ロール、信頼できるアカウントでの IAM ロールの引き受け、または AWS アクセス キーの提供など、いくつかの方法で AWS 認証情報を提供できます。"AWS の認証情報と権限について詳しく見る" 。

最初の 2 つのオプションでは、コンソールは AWS セキュリティ トークン サービスを使用して、常にローテーションする一時的な認証情報を取得します。このプロセスは自動かつ安全であるため、ベストプラクティスです。

コンソールで更新して、AWS アクセスキーを手動でローテーションします。

コンソールエージェントに追加の資格情報を追加する

コンソールエージェントに追加の AWS 認証情報を追加して、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必要な権限を付与します。別のアカウントの IAM ロールの ARN を提供するか、AWS アクセスキーを提供することができます。

"NetApp ConsoleがAWS認証情報と権限を使用する方法を学ぶ"。

権限を付与する

コンソールエージェントに AWS 認証情報を追加する前に、権限を付与します。権限により、コンソールエージェントはその AWS アカウント内のリソースとプロセスを管理できるようになります。信頼できるアカウントのロールの ARN または AWS キーを使用して、アクセス許可を付与できます。

> コンソールからコンソールエージェントを展開した場合、コンソールエージェントを展開したアカウントの AWS 認証情報が自動的に追加されます。これにより、リソースを管理するために必要な権限が確保されます。

選択肢

- 別のアカウントの IAM ロールを引き受けて権限を付与する
- AWSキーを提供して権限を付与する

別のアカウントの **IAM** ロールを引き受けて権限を付与する

IAM ロールを使用して、コンソールエージェントをデプロイしたソース AWS アカウントと他の AWS アカウントの間に信頼関係を設定できます。次に、信頼できるアカウントの IAM ロールの ARN をコンソールに提供します。

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、この認証方法は使用できません。AWS キーを使用する必要があります。

手順

1. コンソール エージェントに権限を付与するターゲット アカウントの IAM コンソールに移動します。
2. [アクセス管理] で、**[ロール] > [ロールの作成]** を選択し、手順に従ってロールを作成します。

   必ず次のことを行ってください。

   - *信頼されたエンティティタイプ*で、*AWS アカウント*を選択します。
   - 別の **AWS** アカウント を選択し、コンソールエージェントインスタンスが存在するアカウントの ID を入力します。
   - の内容をコピーして貼り付けて必要なポリシーを作成します。"コンソールエージェントのIAMポリシー" 。
3. 後でコンソールに貼り付けることができるように、IAM ロールのロール ARN をコピーします。

結果

アカウントには必要な権限があります。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なりました。

**AWS**キーを提供して権限を付与する

コンソールに IAM ユーザーの AWS キーを提供する場合は、そのユーザーに必要な権限を付与する必要があります。コンソール IAM ポリシーは、コンソールが使用できる AWS アクションとリソースを定義します。

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. IAMコンソールから、以下の内容をコピーして貼り付けることでポリシーを作成します。"コンソールエージェントのIAMポリシー" 。

   "AWSドキュメント: IAMポリシーの作成"

2. ポリシーを IAM ロールまたは IAM ユーザーにアタッチします。
   - "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"

既存のエージェントに資格情報を追加する

AWS アカウントに必要な権限を付与したら、そのアカウントの認証情報を既存のエージェントに追加できます。これにより、同じエージェントを使用してそのアカウントでCloud Volumes ONTAPシステムを起動できるようになります。

クラウド プロバイダーの新しい資格情報が使用可能になるまでに数分かかる場合があります。

手順

1. 上部のナビゲーション バーを使用して、資格情報を追加するコンソール エージェントを選択します。

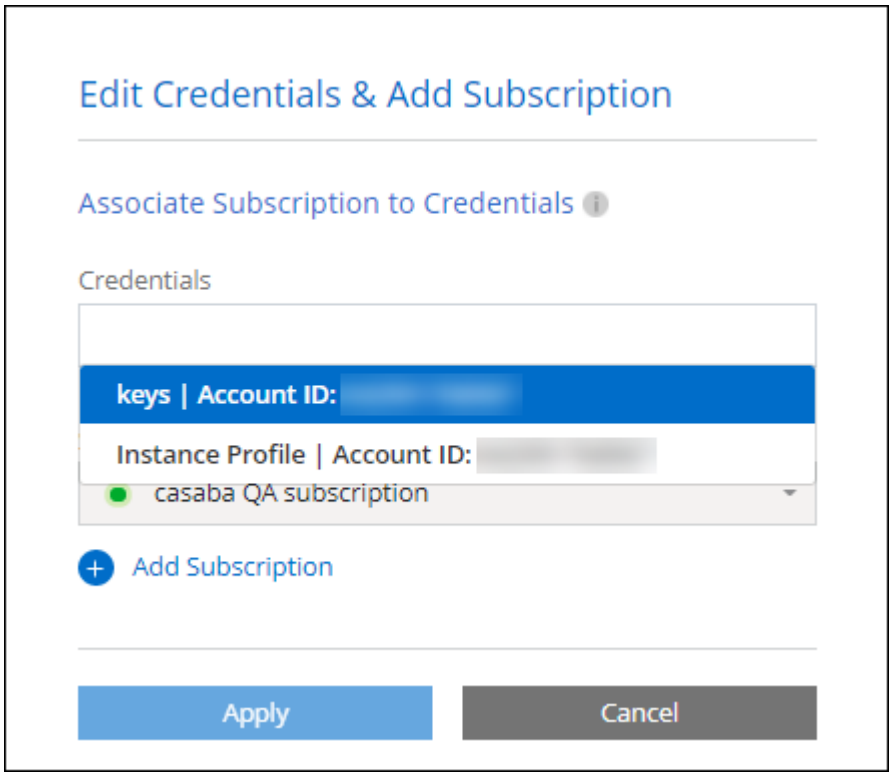
2. 左側のナビゲーション バーで、管理 > 資格情報 を選択します。
3. *組織の資格情報*ページで、*資格情報の追加*を選択し、ウィザードの手順に従います。
   a. 資格情報の場所: *Amazon Web Services > エージェント*を選択します。
   b. 認証情報の定義: 信頼できる IAM ロールの ARN (Amazon リソース名) を指定するか、AWS アクセスキーとシークレットキーを入力します。
   c. マーケットプレイス サブスクリプション: 今すぐサブスクライブするか、既存のサブスクリプションを選択して、マーケットプレイス サブスクリプションをこれらの資格情報に関連付けます。

      時間単位の料金 (PAYGO) または年間契約でサービス料金を支払うには、AWS 認証情報を AWS Marketplace サブスクリプションに関連付ける必要があります。

   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

コンソールにサブスクリプションを追加するときに、[詳細と資格情報] ページから別の資格情報セットに切り替えることができるようになりました。




コンソールエージェントを作成するためにコンソールに資格情報を追加します

コンソールエージェントの作成に必要な権限を付与する IAM ロールの ARN を指定して、AWS 認証情報を追加します。新しいエージェントを作成するときに、これらの資格情報を選択できます。

**IAM**ロールを設定する

NetApp Consoleのソフトウェア サービス (SaaS) レイヤーがロールを引き受けることができる IAM ロールを設定します。

手順

1. ターゲットアカウントの IAM コンソールに移動します。
2. [アクセス管理] で、**[ロール] > [ロールの作成]** を選択し、手順に従ってロールを作成します。

   必ず次のことを行ってください。

   - *信頼されたエンティティタイプ*で、*AWS アカウント*を選択します。
   - *別のAWSアカウント*を選択し、 NetApp ConsoleSaaSのIDを入力します：952013314444
   - 特にAmazon FSx for NetApp ONTAPの場合は、信頼関係 ポリシーを編集して "AWS": "arn:aws:iam::952013314444:root" を含めます。

     たとえば、ポリシーは次のようになります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::952013314444:root",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

   +
   参照"AWS Identity and Access Management (IAM) ドキュメント" IAM でのクロスアカウント リソース アクセスの詳細については、こちらをご覧ください。

   - コンソール エージェントを作成するために必要な権限を含むポリシーを作成します。
     - "FSx for ONTAPに必要な権限を表示する"
     - "エージェント展開ポリシーを表示する"
3. 次のステップでコンソールに貼り付けることができるように、IAM ロールのロール ARN をコピーします。

結果

IAM ロールに必要な権限が付与されました。コンソールに追加できるようになりました。

資格情報を追加する

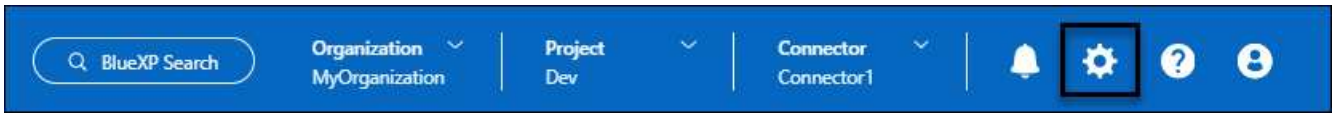
IAM ロールに必要な権限を付与したら、ロール ARN をコンソールに追加します。

開始する前に

IAM ロールを作成したばかりの場合は、使用できるよう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、数分お待ちください。

手順

1. *管理 > 資格情報*を選択します。




2. *組織の資格情報*ページで、*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. 認証情報の場所: **Amazon Web Services >** コンソール を選択します。
   b. 認証情報の定義: IAM ロールの ARN (Amazon リソース名) を指定します。
   c. 確認: 新しい資格情報の詳細を確認し、[追加] を選択します。

### **Amazon FSx for ONTAP**のコンソールに認証情報を追加する

詳細については、 "Amazon FSx for ONTAPのコンソールドキュメント"

### **AWS**サブスクリプションを設定する

AWS 認証情報を追加したら、その認証情報を使用して AWS Marketplace サブスクリプションを設定できます。サブスクリプションを使用すると、 NetAppデータ サービスとCloud Volumes ONTAPの料金を時間単位 (PAYGO) または年間契約で支払うことができます。

認証情報を追加した後に AWS Marketplace サブスクリプションを構成するシナリオは 2 つあります。

- 資格情報を最初に追加したときに、サブスクリプションを構成しませんでした。
- AWS 認証情報に設定されている AWS Marketplace サブスクリプションを変更します。

  現在のマーケットプレイス サブスクリプションを新しいサブスクリプションに置き換えると、既存のCloud Volumes ONTAPシステムとすべての新しいシステムのマーケットプレイス サブスクリプションが変更されます。

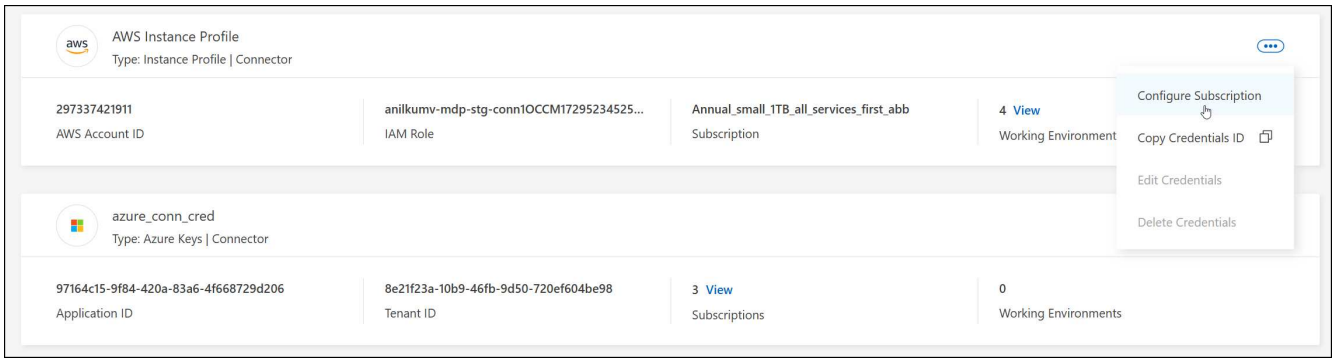
開始する前に

サブスクリプションを構成する前に、コンソール エージェントを作成する必要があります。"コンソールエージェントの作成方法を学ぶ" 。

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。

既存のサブスクリプションを組織に関連付ける

AWS Marketplace からサブスクライブする場合、プロセスの最後のステップは、サブスクリプションを組織に関連付けることです。この手順を完了しなかった場合、組織でサブスクリプションを使用することはできません。

- "コンソールの展開モードについて学ぶ"
- "コンソールのIDとアクセス管理について学ぶ"

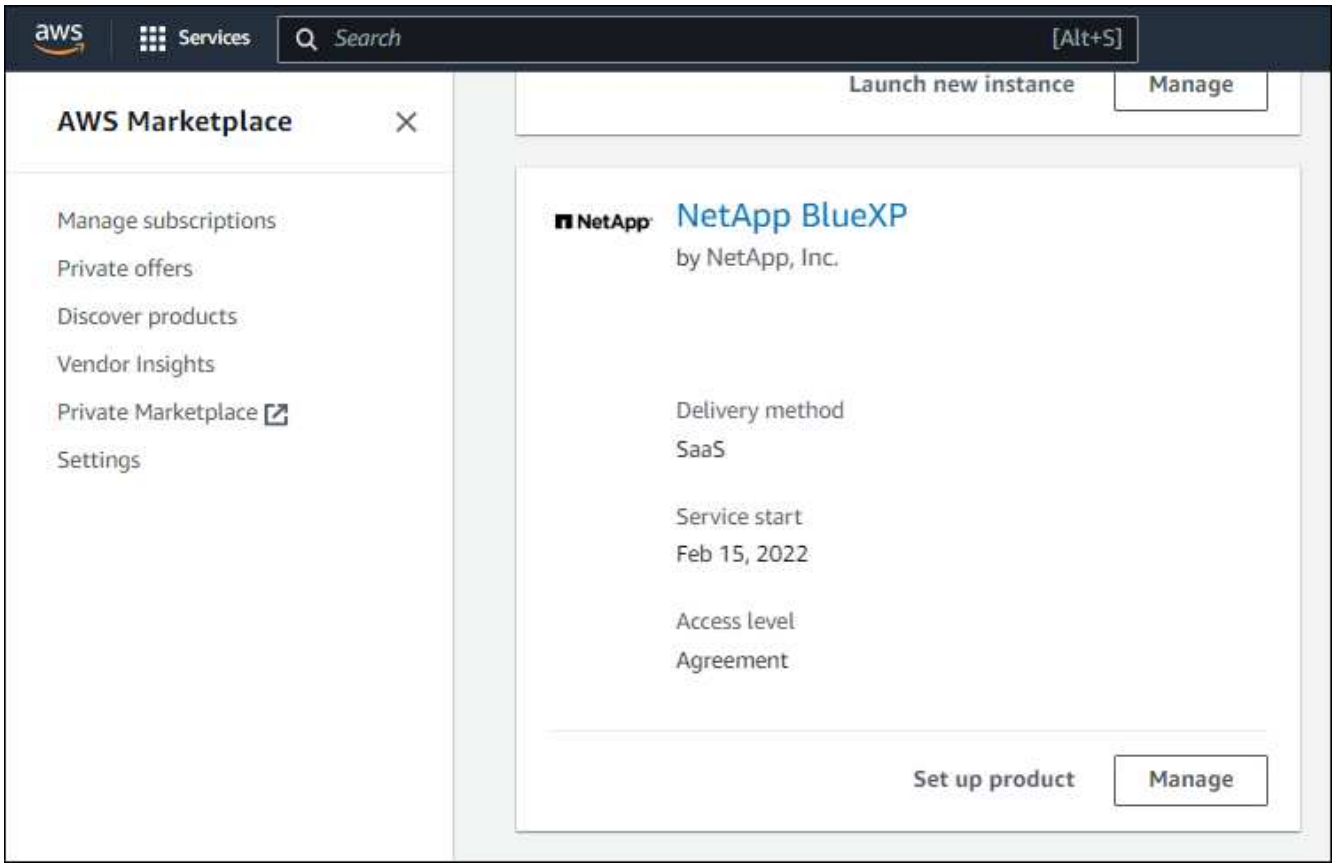
AWS Marketplace からNetApp Intelligent Servicesにサブスクライブしたが、サブスクリプションをアカウントに関連付ける手順を忘れた場合は、以下の手順に従ってください。

手順

1. サブスクリプションをコンソール組織に関連付けていないことを確認します。
   a. ナビゲーション メニューから、*管理 >Licenses and subscriptions*を選択します。
   b. *サブスクリプション*を選択します。
   c. サブスクリプションが表示されていないことを確認します。

      現在表示している組織またはアカウントに関連付けられているサブスクリプションのみが表示されます。サブスクリプションが表示されない場合は、次の手順に進みます。

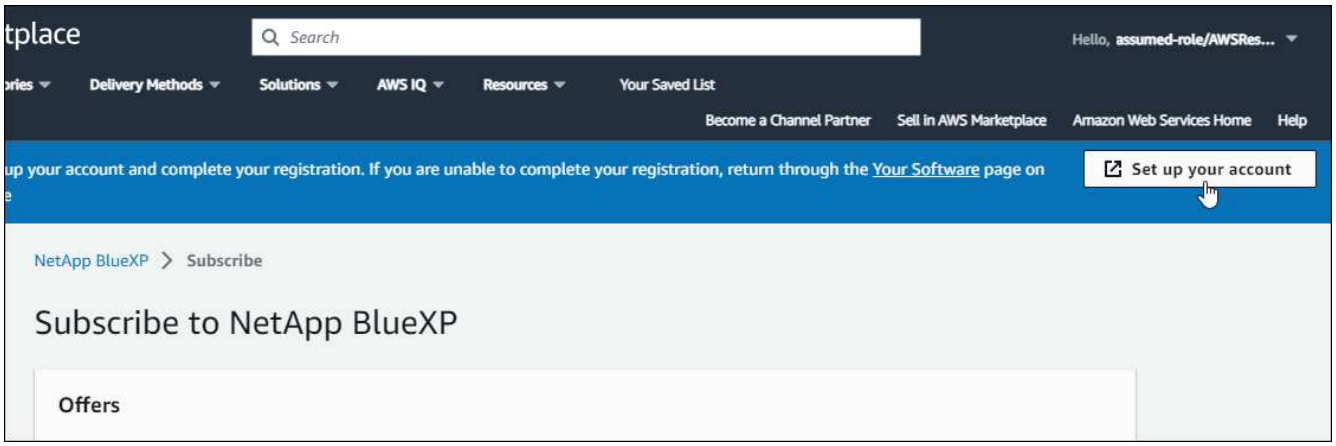
2. AWS コンソールにログインし、*AWS Marketplace サブスクリプション*に移動します。
3. サブスクリプションを見つけます。




4. *製品のセットアップ*を選択します。

   サブスクリプション オファー ページは、新しいブラウザ タブまたはウィンドウに読み込まれます。

5. *アカウントを設定*を選択します。




netapp.com の サブスクリプションの割り当て ページが新しいブラウザ タブまたはウィンドウに読み込まれます。

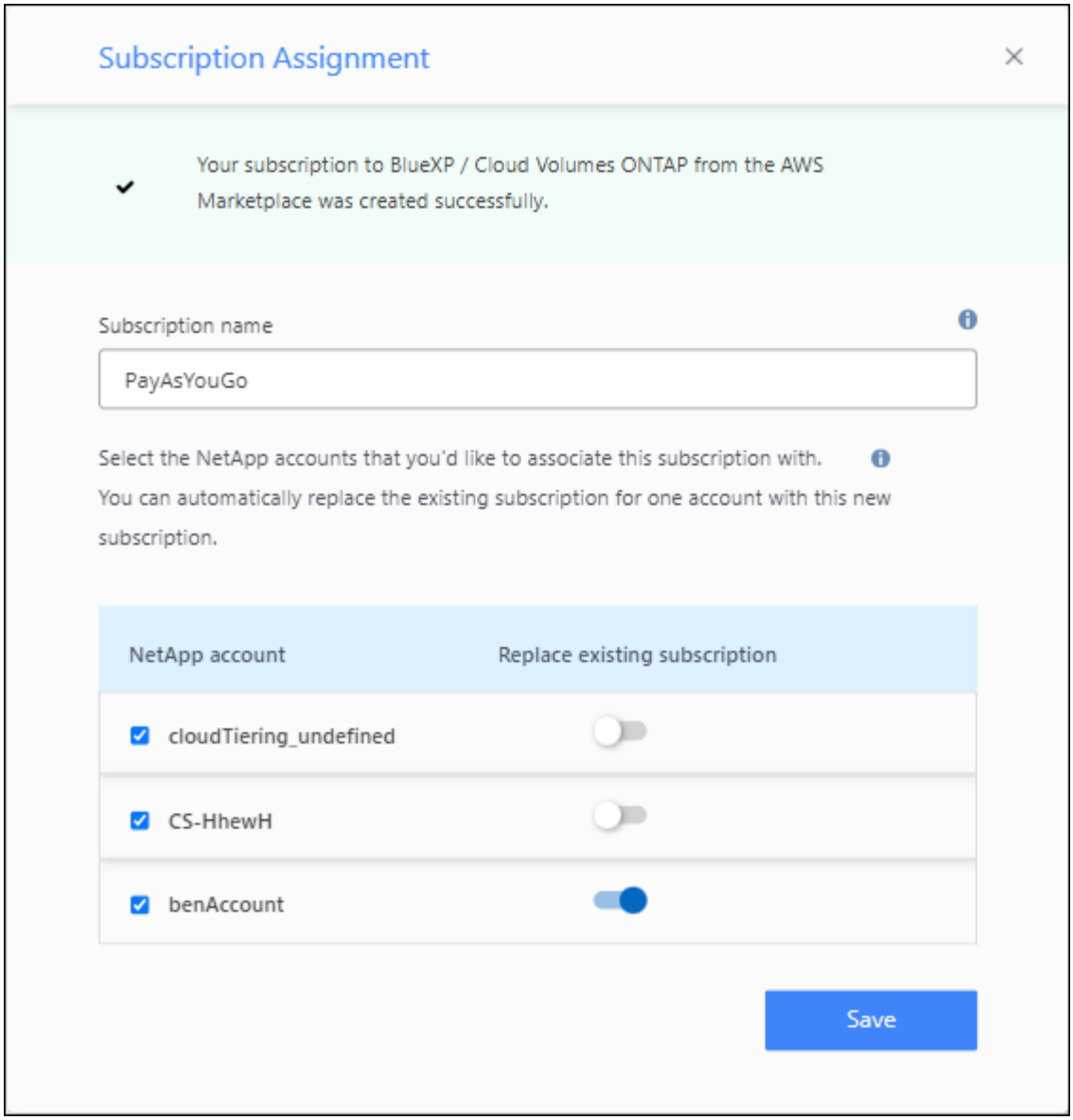
最初にコンソールにログインするように求められる場合があります。

6. *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。

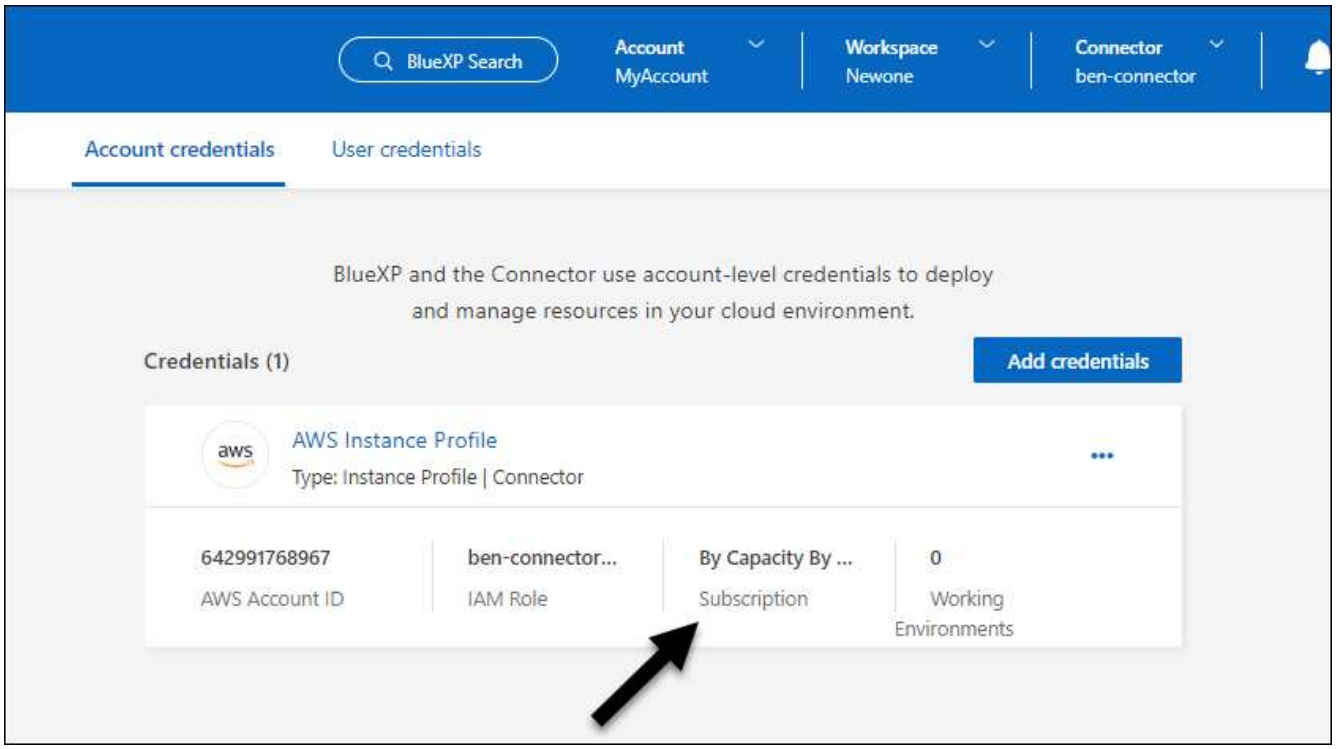
     コンソールは、組織またはアカウント内のすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。資格情報のセットがサブスクリプションに関連付けられたことがない場合、この新しいサブスクリプションはそれらの資格情報に関連付けられません。

     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。




7. サブスクリプションが組織に関連付けられていることを確認します。
   a. ナビゲーション メニューから、*管理 > ライセンスとサブスクリプション*を選択します。
   b. *サブスクリプション*を選択します。
   c. サブスクリプションが表示されていることを確認します。
8. サブスクリプションが AWS 認証情報に関連付けられていることを確認します。
   a. *管理 > 資格情報*を選択します。
   b. *組織の認証情報*ページで、サブスクリプションが AWS 認証情報に関連付けられていることを確認します。

      ここに例があります。




資格情報を編集する

アカウントの種類 (AWS キーまたはロールの引き受け) を変更したり、名前を編集したり、認証情報自体 (キーまたはロール ARN) を更新したりして、AWS 認証情報を編集します。

コンソールエージェントインスタンスまたはAmazon FSx for ONTAPインスタンスに関連付けられているインスタンスプロファイルの認証情報を編集することはできません。FSx for ONTAPインスタンスの資格情報の名前のみを変更できます。

手順

1. *管理 > 資格情報*を選択します。
2. *組織の資格情報*ページで、資格情報セットのアクション メニューを選択し、*資格情報の編集*を選択します。
3. 必要な変更を加えて、[適用] を選択します。

資格情報を削除する

資格情報セットが不要になった場合は、削除できます。システムに関連付けられていない資格情報のみを削除できます。

コンソール エージェントに関連付けられているインスタンス プロファイルの資格情報を削除することはできません。

手順

1. *管理 > 資格情報*を選択します。
2. 組織の資格情報 または アカウントの資格情報 ページで、資格情報セットのアクション メニューを選択し、資格情報の削除 を選択します。

3. *削除*を選択して確認します。

## Azure

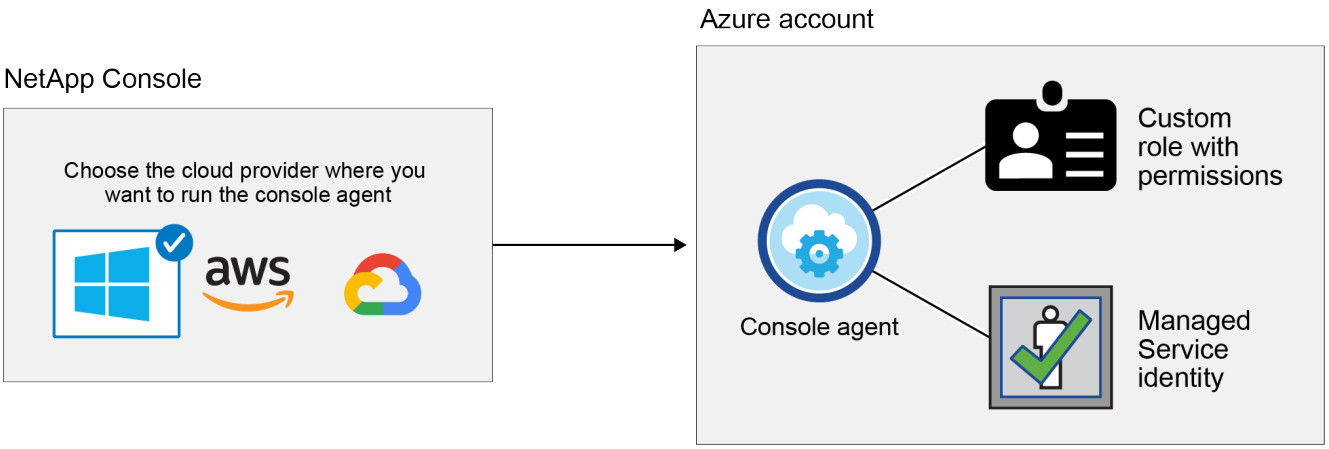
### NetApp Consoleの Azure 資格情報と権限について学習します

NetApp ConsoleがAzure 資格情報を使用してユーザーに代わってアクションを実行する方法と、それらの資格情報がマーケットプレイスのサブスクリプションと関連付けられる方法について説明します。これらの詳細を理解しておくと、1 つ以上の Azure サブスクリプションの資格情報を管理するときに役立ちます。たとえば、コンソールに追加の Azure 資格情報を追加するタイミングを知りたい場合があります。

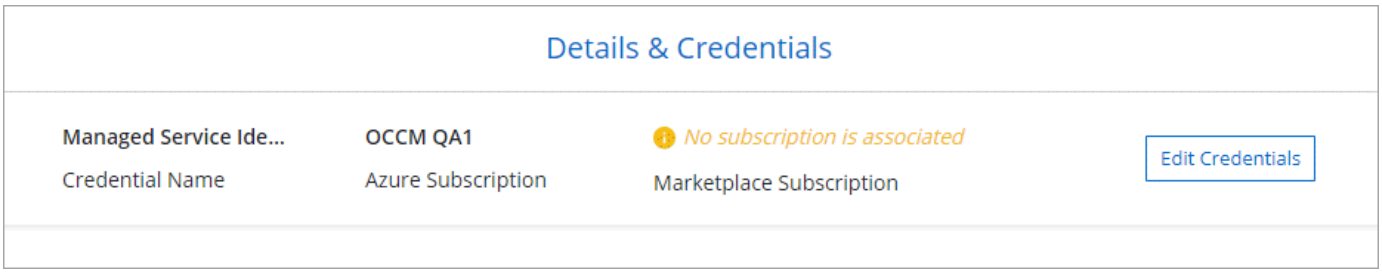
#### 初期の Azure 資格情報

コンソールからコンソール エージェントを展開する場合は、コンソール エージェント仮想マシンを展開する権限を持つ Azure アカウントまたはサービス プリンシパルを使用する必要があります。必要な権限は、"Azure のエージェント展開ポリシー" 。

コンソールがAzureにコンソールエージェント仮想マシンを展開すると、 "システム割り当てマネージドID"仮想マシン上でカスタム ロールを作成し、それを仮想マシンに割り当てます。このロールは、その Azure サブスクリプション内のリソースとプロセスを管理するために必要な権限をコンソールに提供します。"コンソールが権限をどのように使用するかを確認します" 。




Cloud Volumes ONTAP用に新しいシステムを作成する場合、コンソールはデフォルトで次の Azure 資格情報を選択します。



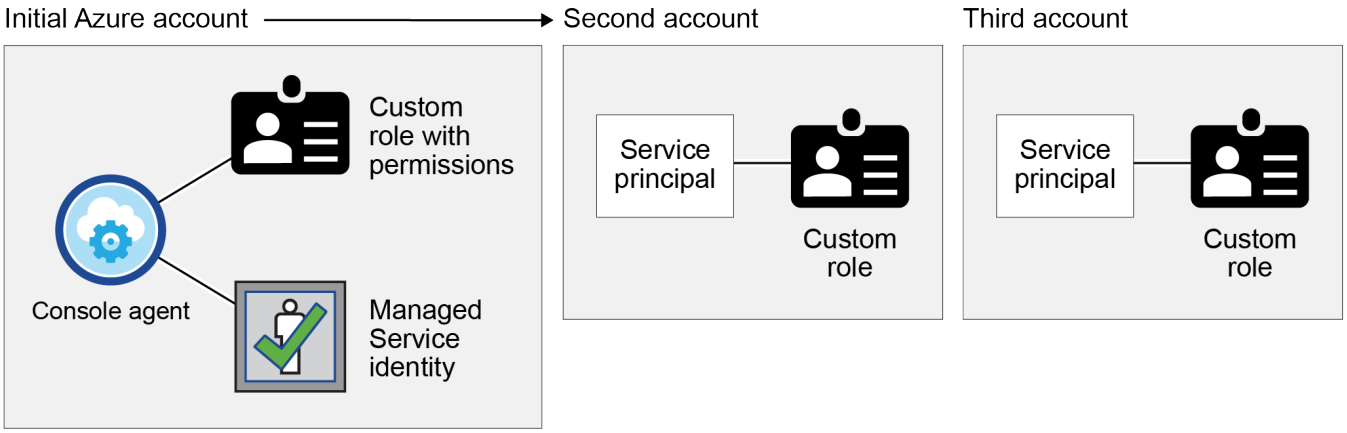

初期の Azure 資格情報を使用してすべてのCloud Volumes ONTAPシステムを展開することも、追加の資格情報を追加することもできます。

### マネージド ID 用の追加の Azure サブスクリプション

コンソール エージェント VM に割り当てられたシステム割り当てマネージド ID は、コンソール エージェントを起動したサブスクリプションに関連付けられています。別のAzureサブスクリプションを選択する場合は、"マネージドIDをそれらのサブスクリプションに関連付ける" 。

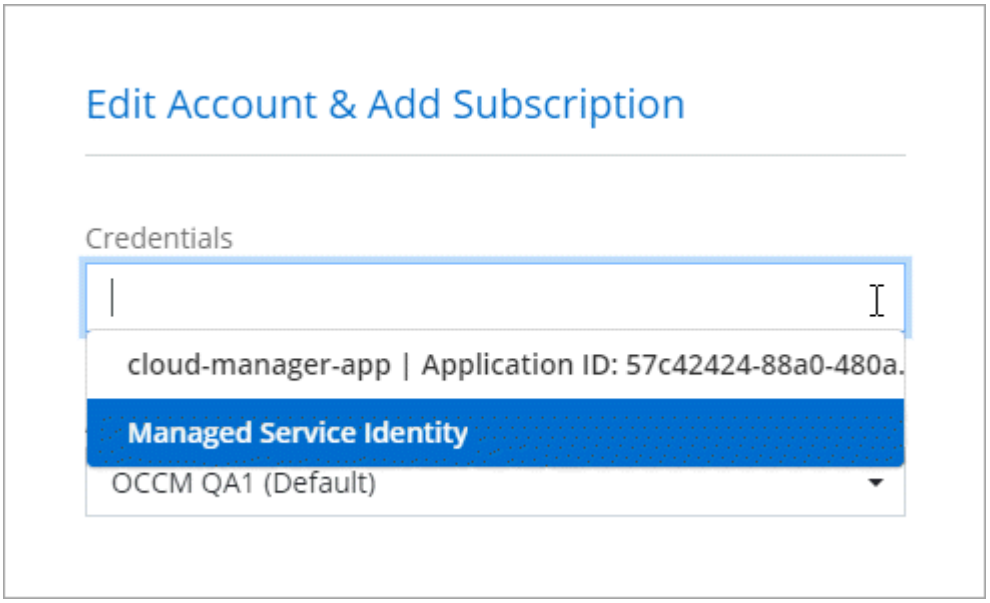
### 追加のAzure資格情報

コンソールで異なるAzure資格情報を使用する場合は、必要な権限を付与する必要があります。"Microsoft Entra ID でサービス プリンシパルを作成して設定する" Azure アカウントごとに。次の図は、それぞれサービス プリンシパルと、アクセス許可を提供するカスタム ロールが設定された 2 つの追加アカウントを示しています。




そうすると"コンソールにアカウント資格情報を追加する"AD サービス プリンシパルに関する詳細を提供します。

たとえば、新しいCloud Volumes ONTAPシステムを作成するときに、資格情報を切り替えることができます。



資格情報とマーケットプレイスのサブスクリプション

コンソール エージェントに追加する資格情報は、Azure Marketplace サブスクリプションに関連付ける必要があります。これにより、 Cloud Volumes ONTAPの料金を時間単位 (PAYGO) またはNetAppデータ サービス、あるいは年間契約で支払うことができます。

"Azureサブスクリプションを関連付ける方法を学ぶ" 。

Azure 資格情報とマーケットプレース サブスクリプションについては、次の点に注意してください。

- Azure 資格情報のセットに関連付けることができるのは、1 つの Azure Marketplace サブスクリプションのみです。
- 既存のマーケットプレイスサブスクリプションを新しいサブスクリプションに置き換えることができます

**FAQ**

次の質問は、資格情報とサブスクリプションに関連しています。

**Cloud Volumes ONTAP**システムの **Azure Marketplace** サブスクリプションを変更できますか**?**

はい、できます。 Azure 資格情報のセットに関連付けられている Azure Marketplace サブスクリプションを変更すると、既存および新しいすべてのCloud Volumes ONTAPシステムに新しいサブスクリプションに対して課金されます。

"Azureサブスクリプションを関連付ける方法を学ぶ" 。

それぞれ異なるマーケットプレイス サブスクリプションを持つ複数の **Azure** 資格情報を追加できますか**?**

同じ Azure サブスクリプションに属するすべての Azure 資格情報は、同じ Azure Marketplace サブスクリプションに関連付けられます。

異なる Azure サブスクリプションに属する複数の Azure 資格情報がある場合、それらの資格情報は、同じ Azure Marketplace サブスクリプションまたは異なるマーケットプレイス サブスクリプションに関連付けることができます。

既存の**Cloud Volumes ONTAP**システムを別の **Azure** サブスクリプションに移動できますか**?**

いいえ、 Cloud Volumes ONTAPシステムに関連付けられている Azure リソースを別の Azure サブスクリプションに移動することはできません。

マーケットプレイスの展開とオンプレミスの展開では資格情報はどのように機能しますか**?**

上記のセクションでは、コンソールからのコンソール エージェントの推奨展開方法について説明しています。 Azure Marketplace から Azure にコンソール エージェントをデプロイし、独自の Linux ホストにコンソール エージェント ソフトウェアをインストールすることもできます。

Marketplace を使用する場合は、コンソール エージェント VM とシステム割り当てマネージド ID にカスタム ロールを割り当てることでアクセス許可を付与することも、Microsoft Entra サービス プリンシパルを使用することもできます。

オンプレミス展開の場合、コンソール エージェントのマネージド ID を設定することはできませんが、サービス プリンシパルを使用してアクセス許可を付与することはできます。

権限の設定方法については、次のページを参照してください。

- 標準モード
  - "Azure Marketplace のデプロイの権限を設定する"
  - "オンプレミス展開の権限を設定する"
- 制限モード
  - "制限モードの権限を設定する"

**NetApp Console**の **Azure** 資格情報とマーケットプレイス サブスクリプションを管理する

Azure 資格情報を追加および管理して、 NetApp ConsoleがAzure サブスクリプション内のクラウド リソースを展開および管理するために必要な権限を持つようにします。複数の Azure Marketplace サブスクリプションを管理する場合は、[資格情報] ページから各サブスクリプションを異なる Azure 資格情報に割り当てることができます。

概要

コンソールで追加の Azure サブスクリプションと資格情報を追加するには、2 つの方法があります。

1. 追加の Azure サブスクリプションを Azure マネージド ID に関連付けます。
2. 異なる Azure 資格情報を使用してCloud Volumes ONTAPをデプロイするには、サービス プリンシパルを使用して Azure 権限を付与し、その資格情報をコンソールに追加します。

追加の **Azure** サブスクリプションをマネージド **ID** に関連付ける

コンソールを使用すると、Cloud Volumes ONTAPをデプロイする Azure 資格情報と Azure サブスクリプションを選択できます。マネージドIDプロファイルに別のAzureサブスクリプションを選択することはできません。 "マネージドID"それらのサブスクリプションで。

タスク概要

マネージドIDとは"最初のAzureアカウント"コンソールからコンソール エージェントを展開する場合。コンソール エージェントを展開すると、コンソールはコンソール エージェント仮想マシンにコンソール オペレータ ロールを割り当てます。

手順

1. Azure ポータルにログインします。
2. サブスクリプション サービスを開き、 Cloud Volumes ONTAPをデプロイするサブスクリプションを選択します。
3. アクセス制御 **(IAM)** を選択します。
   a. 追加 > ロールの割り当ての追加 を選択し、権限を追加します。
      - コンソールオペレーター ロールを選択します。

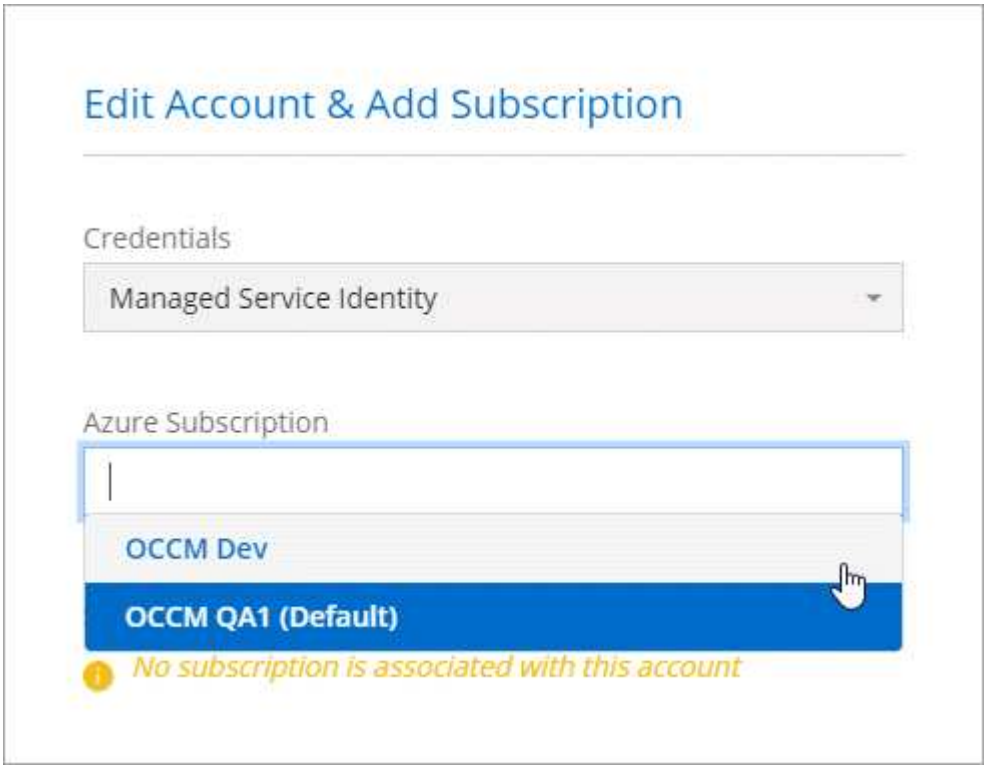
> コンソール オペレータは、コンソール エージェント ポリシーで提供されるデフォルト名です。ロールに別の名前を選択した場合は、代わりにその名前を選択します。

- *仮想マシン*へのアクセスを割り当てます。
- 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ます。
- コンソール エージェント仮想マシンを選択します。
- *保存*を選択します。

4. 追加のサブスクリプションについては、これらの手順を繰り返します。

結果

新しいシステムを作成するときに、マネージド ID プロファイルに対して複数の Azure サブスクリプションから選択できるようになりました。




**NetApp Console**に **Azure** 資格情報を追加する

コンソールからコンソール エージェントを展開すると、コンソールは必要なアクセス許可を持つ仮想マシン上でシステム割り当てのマネージド ID を有効にします。 Cloud Volumes ONTAPの新しいシステムを作成するときに、コンソールはデフォルトでこれらの Azure 資格情報を選択します。

既存のシステムにコンソール エージェント ソフトウェアを手動でインストールした場合、資格情報の初期セットは追加されません。"Azure の資格情報と権限について学習する" 。

異なる Azure 資格情報を使用してCloud Volumes ONTAPをデプロイする場合は、Azure アカウントごとに Microsoft Entra ID でサービス プリンシパルを作成して設定し、必要な権限を付与する必要があります。その後、新しい資格情報をコンソールに追加できます。

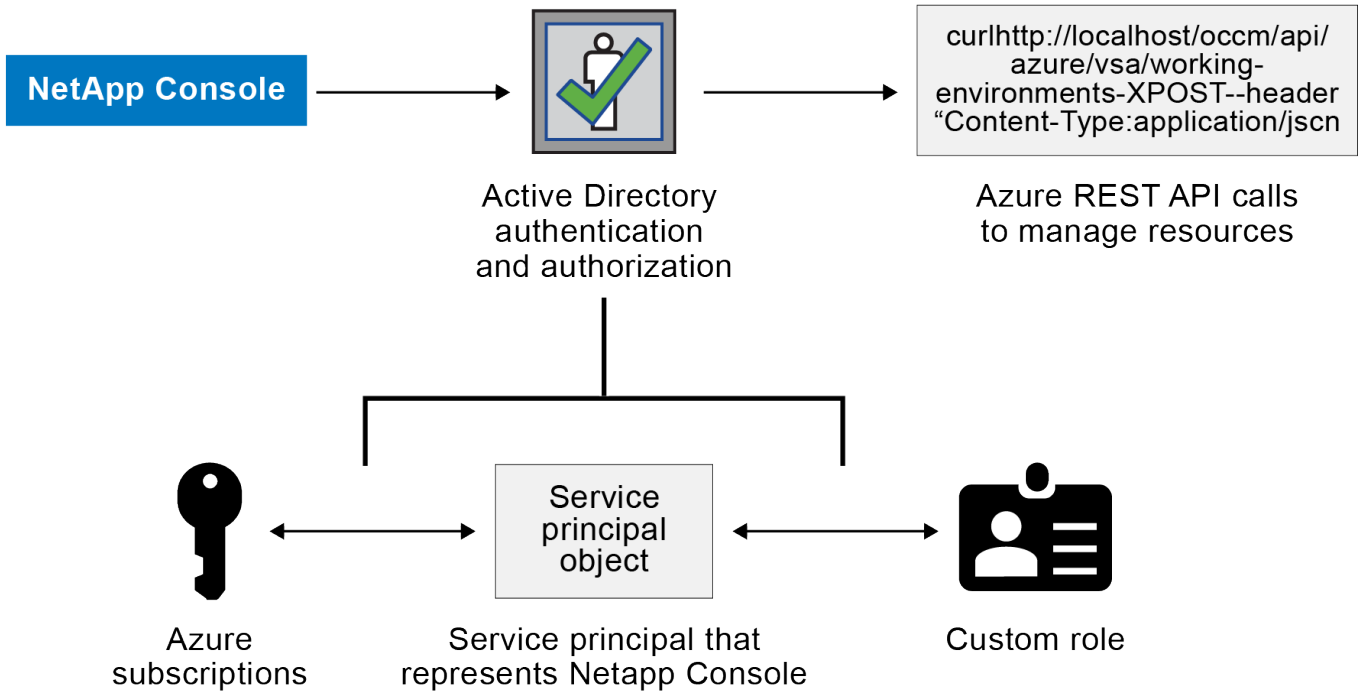
サービス プリンシパルを使用して **Azure** 権限を付与する

コンソールには、Azure でアクションを実行するための権限が必要です。 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 資格情報を取得することで、Azure アカウントに必要

な権限を付与できます。

タスク概要

次の図は、コンソールが Azure で操作を実行するための権限を取得する方法を示しています。 1 つ以上の Azure サブスクリプションに関連付けられたサービス プリンシパル オブジェクトは、Microsoft Entra ID のコンソールを表し、必要なアクセス許可を許可するカスタム ロールに割り当てられます。




手順

1. Microsoft Entra アプリケーションを作成する 。
2. [アプリケーションをロールに割り当てる] 。
3. Windows Azure サービス管理 API 権限を追加する 。
4. アプリケーションIDとディレクトリIDを取得する 。
5. [クライアントシークレットを作成する] 。

**Microsoft Entra** アプリケーションを作成する

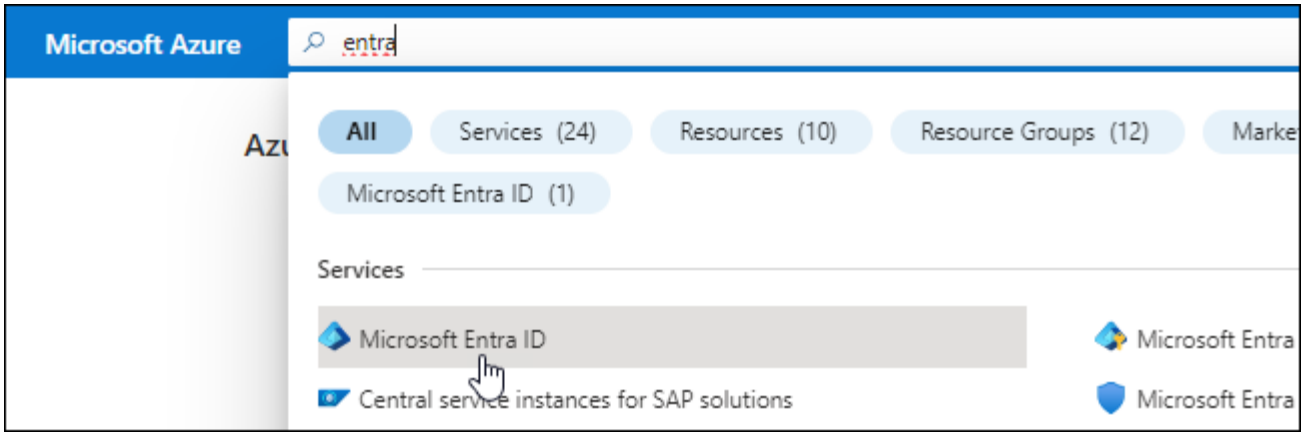
コンソールがロールベースのアクセス制御に使用できる Microsoft Entra アプリケーションとサービス プリンシパルを作成します。

手順

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

サービス プリンシパルを 1 つ以上の Azure サブスクリプションにバインドし、カスタムの「コンソール オペレーター」ロールを割り当てて、コンソールに Azure での権限を与える必要があります。

手順

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。

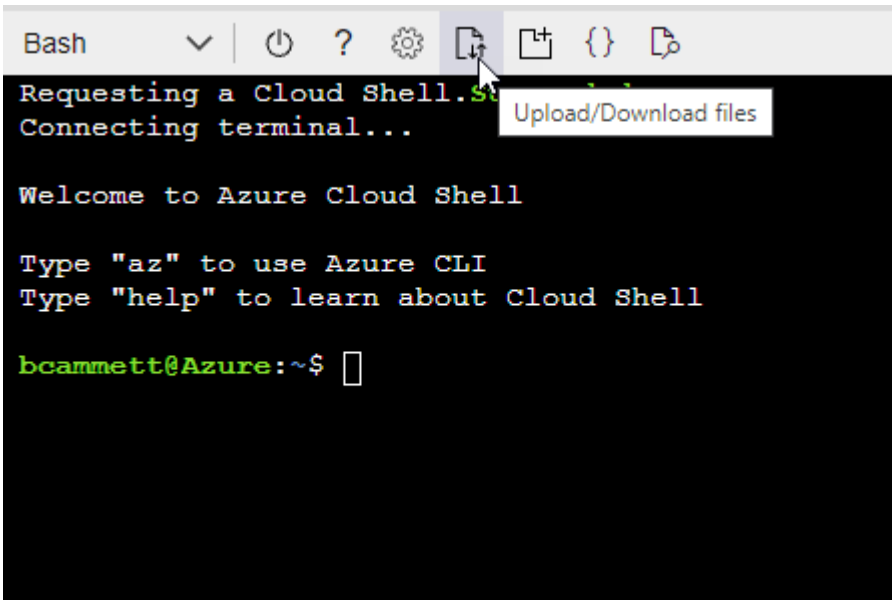
      例

```
"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。

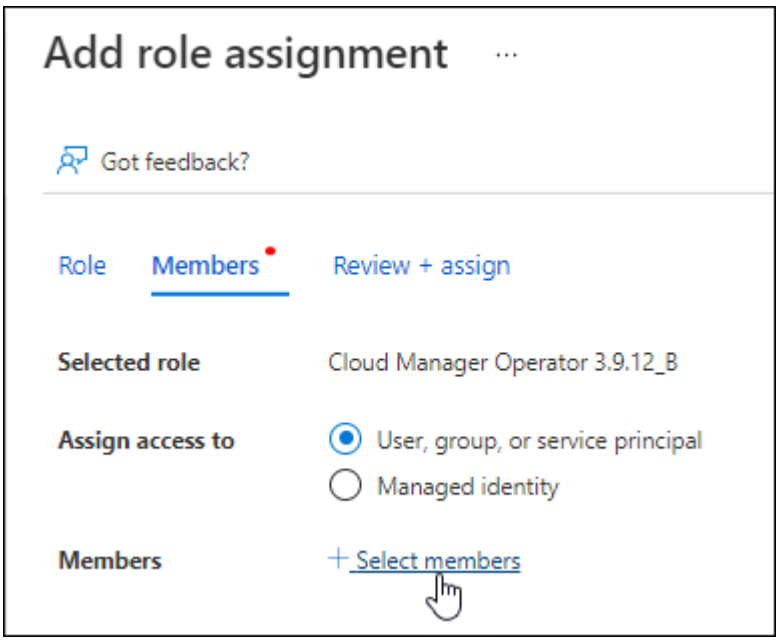
b. サブスクリプションを選択します。

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。

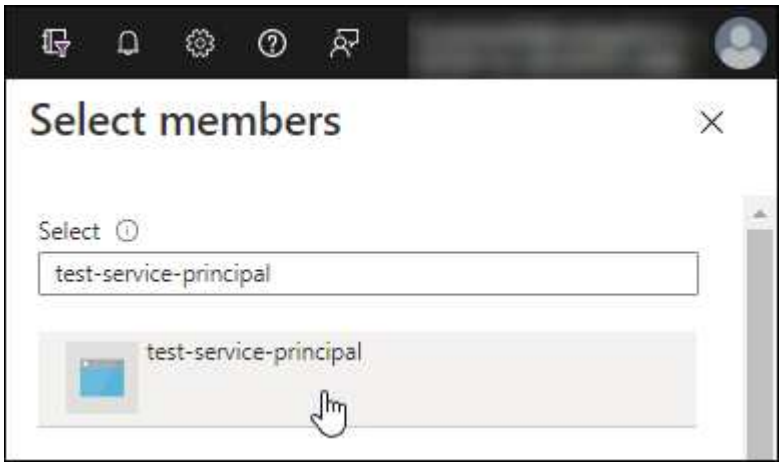
e. *メンバー*タブで、次の手順を実行します。

- *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。

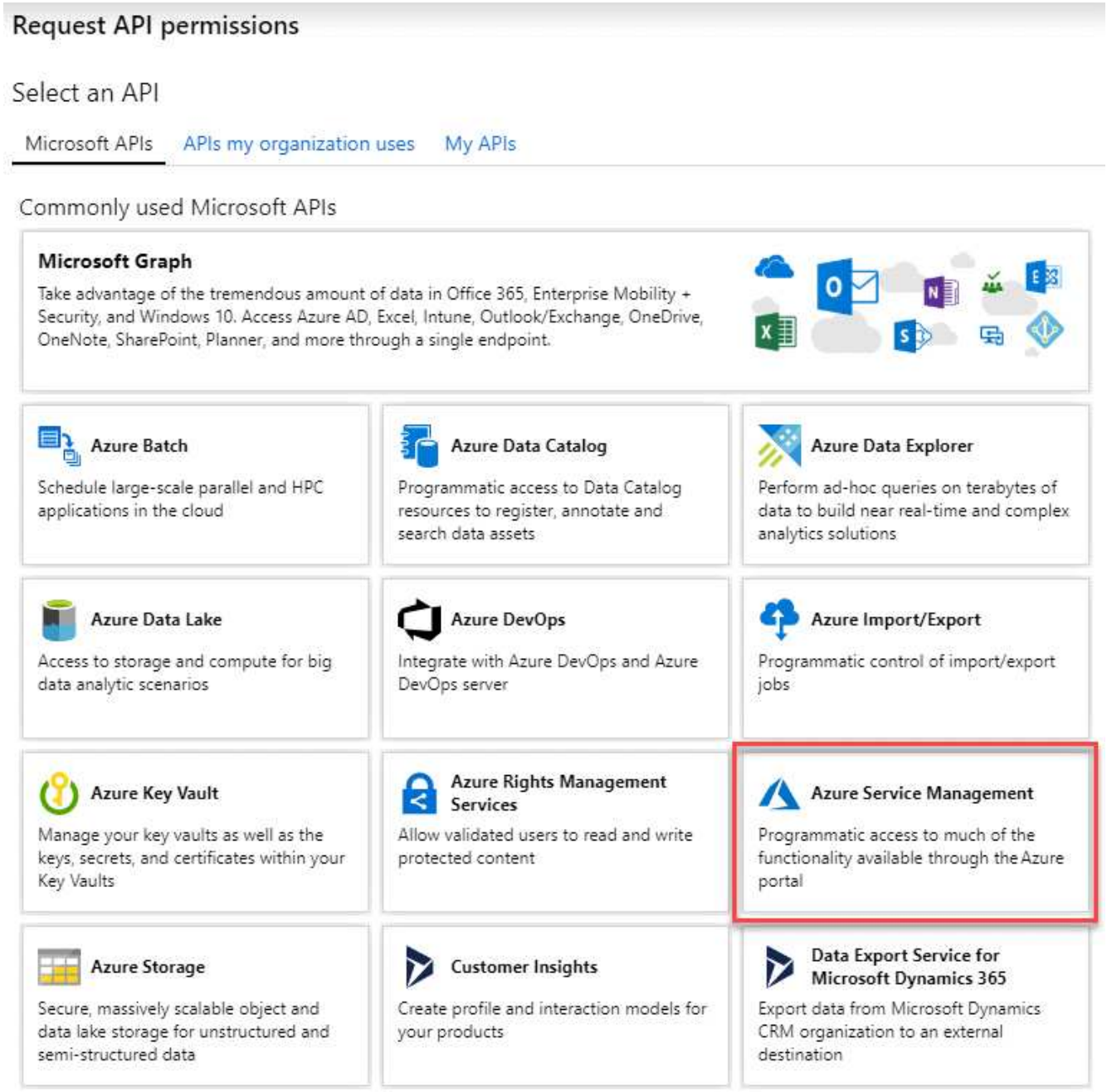
複数の Azure サブスクリプションからCloud Volumes ONTAPをデプロイする場合は、サービス プリンシパルを各サブスクリプションにバインドする必要があります。 NetApp Consoleでは、 Cloud Volumes ONTAP をデプロイするときに使用するサブスクリプションを選択できます。

### Windows Azure サービス管理 API 権限を追加する

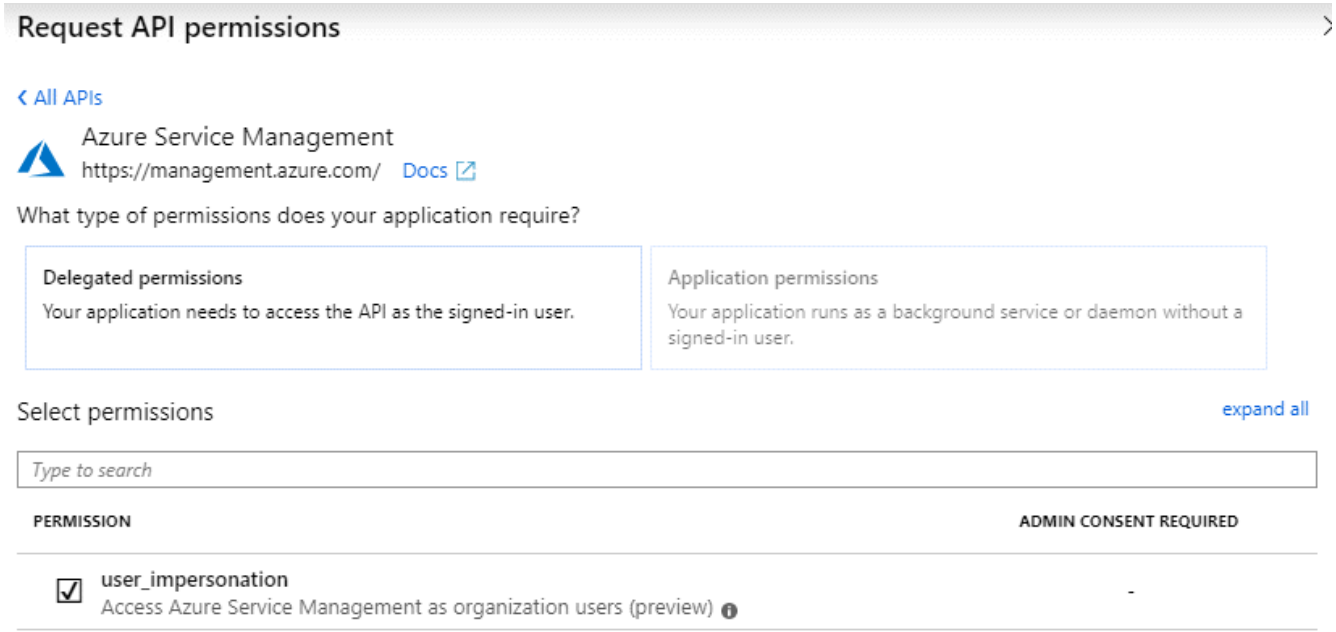
サービス プリンシパルに「Windows Azure サービス管理 API」権限を割り当てる必要があります。

手順

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。

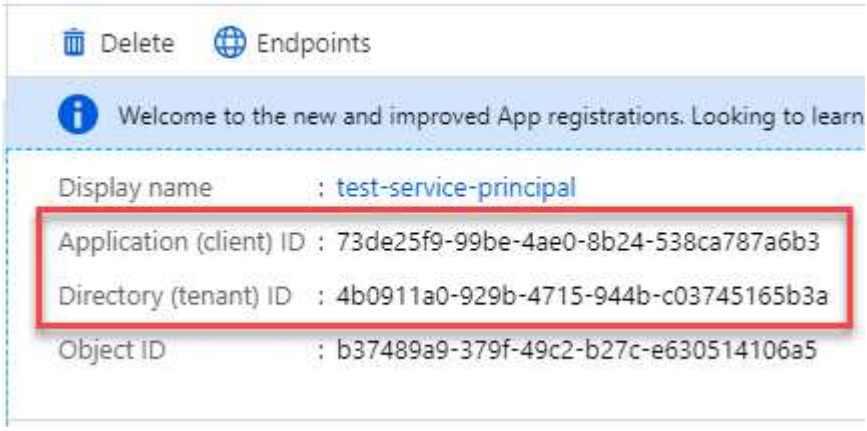



アプリケーション**ID**とディレクトリ**ID**を取得する

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。

手順

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

クライアント シークレットを作成し、その値をコンソールに提供して、Microsoft Entra ID による認証を行います。

手順

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。

## コンソールに資格情報を追加する

Azure アカウントに必要な権限を付与したら、そのアカウントの資格情報をコンソールに追加できます。この手順を完了すると、さまざまな Azure 資格情報を使用してCloud Volumes ONTAP を起動できるようになります。

### 開始する前に

クラウド プロバイダーでこれらの資格情報を作成したばかりの場合は、使用できるよう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、数分お待ちください。

### 開始する前に

コンソール設定を変更する前に、コンソール エージェントを作成する必要があります。"コンソールエージェントの作成方法を学ぶ" 。

### 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

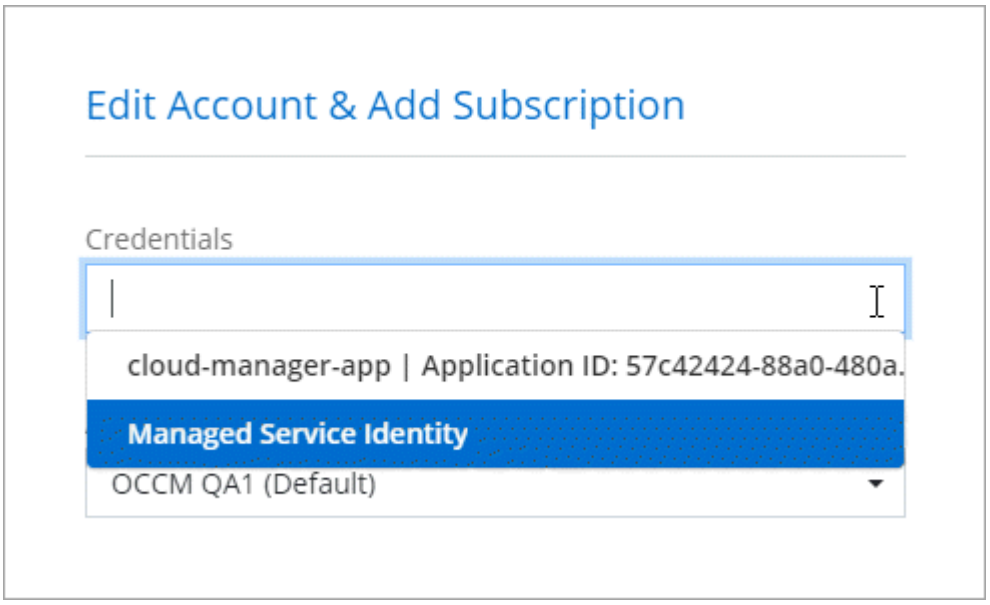
- クライアントシークレット

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

詳細と資格情報ページから別の資格情報セットに切り替えることができます "コンソールにシステムを追加するとき"




既存の資格情報を管理する

Marketplace サブスクリプションを関連付けたり、資格情報を編集したり、削除したりすることで、コンソールに既に追加した Azure 資格情報を管理します。

**Azure Marketplace** サブスクリプションを資格情報に関連付ける

Azure 資格情報をコンソールに追加したら、Azure Marketplace サブスクリプションをそれらの資格情報に関連付けることができます。サブスクリプションを使用すると、従量課金制のCloud Volumes ONTAPシステムを作成し、 NetAppデータ サービスにアクセスできます。

コンソールに資格情報を追加した後に、Azure Marketplace サブスクリプションを関連付けるシナリオは 2 つあります。

- 資格情報をコンソールに最初に追加したときに、サブスクリプションを関連付けませんでした。
- Azure 資格情報に関連付けられている Azure Marketplace サブスクリプションを変更します。

  現在のマーケットプレイス サブスクリプションを置き換えると、既存および新しいCloud Volumes ONTAPシステム用に更新されます。

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. 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。

資格情報を編集する

コンソールで Azure 資格情報を編集します。たとえば、サービス プリンシパル アプリケーションに新しいシークレットが作成された場合は、クライアント シークレットを更新できます。

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. 資格情報セットのアクション メニューを選択し、[資格情報の編集] を選択します。
4. 必要な変更を加えて、[適用] を選択します。

資格情報を削除する

資格情報セットが不要になった場合は、削除できます。システムに関連付けられていない資格情報のみを削除できます。

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. *組織の資格情報*ページで、資格情報セットのアクション メニューを選択し、*資格情報の削除*を選択します。
4. *削除*を選択して確認します。

## Google Cloud

### Google Cloud プロジェクトと権限について学ぶ

NetApp ConsoleがGoogle Cloud 認証情報を使用してユーザーに代わってアクションを実行する方法と、それらの認証情報がマーケットプレイスのサブスクリプションとどのように関連付けられるかについて説明します。これらの詳細を理解しておくと、1 つ以上の Google Cloud プロジェクトの認証情報を管理するときに役立ちます。たとえば、コンソール エージェント VM に関連付けられているサービス アカウントについて知りたい場合があります。

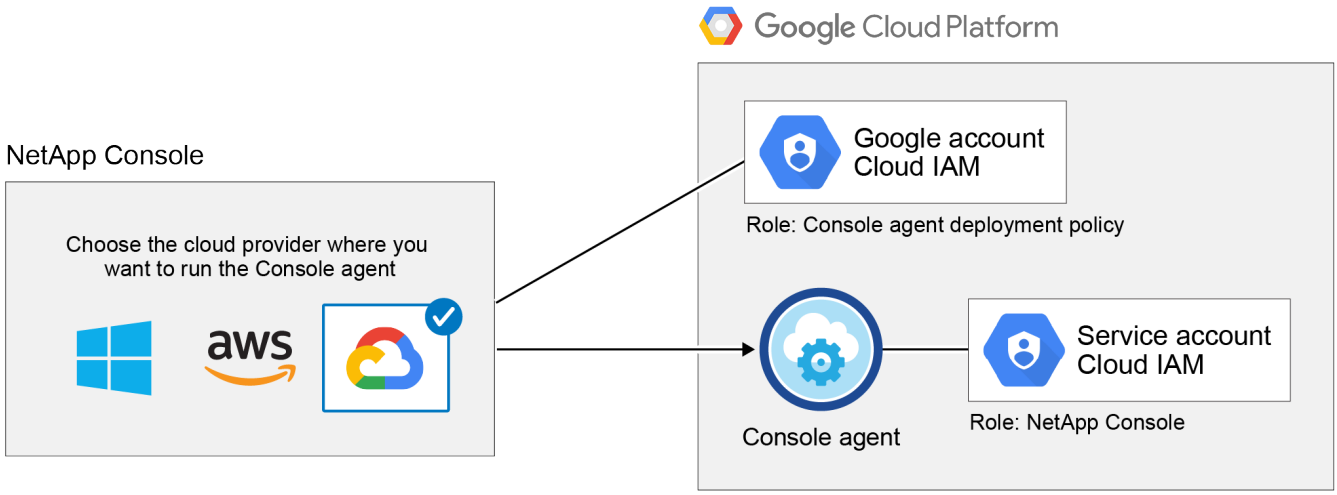
#### NetApp Consoleのプロジェクトと権限

コンソールを使用して Google Cloud プロジェクト内のリソースを管理する前に、まずコンソール エージェントをデプロイする必要があります。エージェントは、オンプレミスまたは別のクラウド プロバイダーで実行することはできません。

コンソール エージェントをコンソールから直接展開する前に、次の 2 セットの権限を設定する必要があります。

1. コンソールからコンソール エージェントを起動する権限を持つ Google アカウントを使用して、コンソール エージェントを展開する必要があります。
2. コンソールエージェントを展開する際には、 "サービスアカウント"エージェントの場合、コンソールはサービス アカウントから権限を取得し、 Cloud Volumes ONTAPシステムの作成と管理、 NetAppバックアップとリカバリを使用したバックアップの管理などを行います。権限は、サービス アカウントにカスタム ロールを添付することによって提供されます。

次の図は、上記の 1 および 2 で説明した許可要件を示しています。




権限の設定方法については、次のページを参照してください。

- "標準モードの Google Cloud 権限を設定する"
- "制限モードの権限を設定する"

資格情報とマーケットプレイスのサブスクリプション

Google Cloud にコンソール エージェントをデプロイすると、コンソールは、コンソール エージェントが存在するプロジェクト内の Google Cloud サービス アカウントのデフォルトの認証情報セットを作成します。Cloud Volumes ONTAPおよびNetAppデータサービスの料金を支払うには、これらの認証情報を Google Cloud Marketplace サブスクリプションに関連付ける必要があります。

"Google Cloud Marketplace サブスクリプションを関連付ける方法を学びます" 。

Google Cloud の認証情報とマーケットプレイスのサブスクリプションについては、次の点に注意してください。

- コンソール エージェントに関連付けることができるのは、Google Cloud 認証情報の 1 セットのみです。
- 認証情報に関連付けることができるのは、Google Cloud Marketplace サブスクリプション 1 つだけです。
- 既存のマーケットプレイスサブスクリプションを新しいサブスクリプションに置き換えることができます

**Cloud Volumes ONTAP**プロジェクト

Cloud Volumes ONTAP は、コンソール エージェントと同じプロジェクトに存在することも、別のプロジェクトに存在することもできます。 Cloud Volumes ONTAP を別のプロジェクトにデプロイするには、まずそのプロジェクトにコンソール エージェントのサービス アカウントとロールを追加する必要があります。

- "サービスアカウントの設定方法を学ぶ"
- "Google Cloud でCloud Volumes ONTAPをデプロイし、プロジェクトを選択する方法を学びます"

**Google Cloud** デプロイメントのコンソール エージェント権限を管理する

## NetApp、Google Cloud にコンソール エージェントをデプロイするときに、コンソール エージェントに使用されるサービス アカウントに必要な権限を更新することがあります。

"必要なGoogle権限リストを確認する"。

Google Cloud Console を使用して、サービス アカウントに割り当てられた IAM ロールを新しい権限セットに合わせて更新します。

"Google Cloud ドキュメント: カスタムロールを編集する"

# アイデンティティとアクセス管理

## **NetApp Console**のアイデンティティとアクセス管理について学ぶ

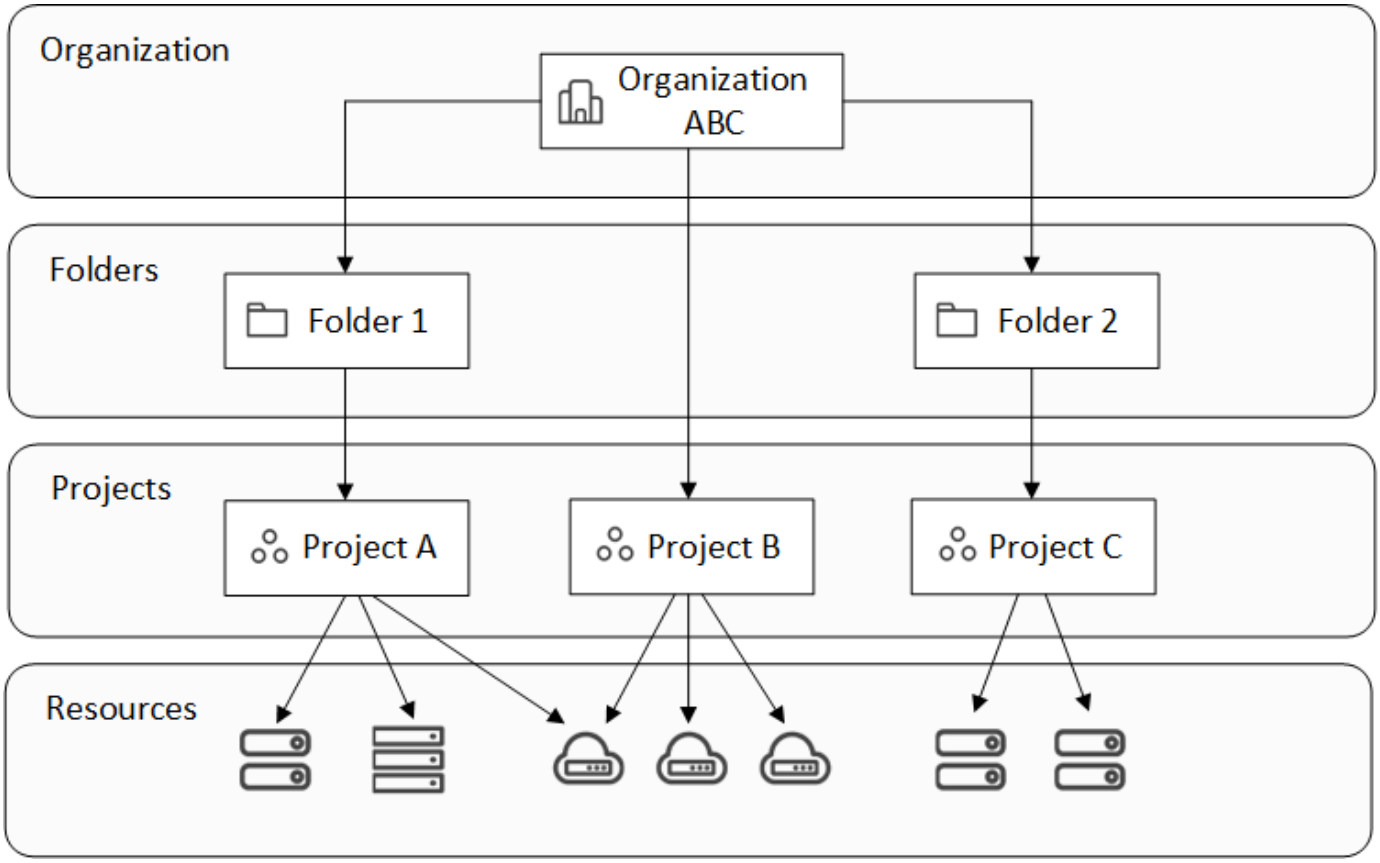
NetAppコンソールの ID およびアクセス管理 (IAM) を使用して、 NetAppリソースを整理し、場所、部門、プロジェクトなどのビジネス構造に応じてアクセスを制御します。

リソースは階層的に配置されます。つまり、組織が一番上にあり、次にフォルダー (他のフォルダーまたはプロジェクトを含むことができます)、そしてプロジェクト (ストレージ システム、ワークロード、エージェントを含む) が続きます。

組織、フォルダ、またはプロジェクトレベルでアクセスロールを割り当てて、ユーザーがリソースに適切にアクセスできるようにします。

NetApp Consoleで IAM を管理するには、スーパー管理者、組織管理者、または フォルダまたはプロジェクト管理者 のロールが必要です。

次の図は、この階層を基本レベルで示しています。



]

アイデンティティおよびアクセス管理コンポーネント

NetApp Consoleでは、組織コンポーネント、リソース コンポーネント、ユーザー アクセス コンポーネントという 3 つの主要コンポーネントを使用してストレージ リソースを整理します。

組織内のプロジェクトとフォルダ

IAM 構造内では、組織、プロジェクト、フォルダという 3 つの組織コンポーネントを操作します。これらのいずれかのレベルでユーザーにロールを割り当てることで、ユーザーにアクセスを許可できます。

組織

組織は、コンソール IAM システムの最上位レベルであり、通常は会社を表します。組織は、フォルダー、プロジェクト、メンバー、ロール、リソースで構成されます。エージェントは組織内の特定のプロジェクトに関連付けられます。

プロジェクト

プロジェクト は、ストレージ リソースへのアクセスを提供するために使用されます。誰かがアクセスできるようにするには、プロジェクトにリソースを割り当てる必要があります。1 つのプロジェクトに複数のリソースを割り当てたり、複数のプロジェクトを持つこともできます。次に、ユーザーにプロジェクトへの権限を割り当てて、プロジェクト内のリソースにアクセスできるようにします。

たとえば、ニーズに応じて、オンプレミスのONTAPシステムを単一のプロジェクトまたは組織内のすべてのプロジェクトに関連付けることができます。

"組織にプロジェクトを追加する方法を学びます。"

フォルダ

関連するプロジェクトを フォルダー にグループ化して、場所、サイト、またはビジネス ユニットごとに整理します。リソースをフォルダーに直接関連付けることはできませんが、フォルダー レベルでユーザーにロールを割り当てると、そのフォルダー内のすべてのプロジェクトにアクセスできるようになります。

"組織にフォルダーを追加する方法について説明します。"

リソース

リソース は、コンソールが認識し、プロジェクトに割り当てることができるエンティティです。リソース には、ストレージシステム、Keystone サブスクリプション、一部のバックアップおよびリカバリのワークロード、および Console エージェントが含まれます。

+ 誰かがリソースにアクセスするには、そのリソースをプロジェクトに関連付ける必要があります。

+

たとえば、 Cloud Volumes ONTAPシステムを 1 つのプロジェクトまたは組織内のすべてのプロジェクトに関連付けることができます。リソースを関連付ける方法は、組織のニーズによって異なります。

+

"リソースをプロジェクトに関連付ける方法を学習します。"

ストレージシステムと**Keystone**サブスクリプション

ストレージシステムは、NetApp Consoleで管理する主要なリソースです。NetApp Consoleは、オンプレミスとクラウドの両方のストレージシステムの管理をサポートしています。プロジェクトに割り当てられたユーザーがアクセスできるように、ストレージシステムをプロジェクトに追加する必要があります。

ストレージ システム

ストレージシステムは、追加されたプロジェクトに自動的に関連付けられますが、*Resources*ページから他のプロジェクトやフォルダに関連付けることもできます。FSx for NetApp ONTAPストレージシステムをプロジェクトやフォルダに関連付けることはできませんが、*Systems*ページまたはWorkloadsから表示できます。

**Keystone**のサブスクリプション

Keystoneサブスクリプションは、 NetApp Consoleでユーザーにサブスクリプションへのアクセスを許可するためにプロジェクトに関連付けることができるリソースでもあります。

バックアップとリカバリのワークロード（**Oracle** および **Microsoft SQL Server**）

一部の Backup and Recovery ワークロードもリソースと見なされます。ユーザーに Backup and Recovery へのアクセス権限を割り当てることができます。

コンソールエージェント

組織管理者は、ストレージ システムを管理し、 NetAppデータ サービスを有効にするためにコンソール エージェントを作成します。エージェントは最初は作成されたプロジェクトに関連付けられますが、管理者はエージェント ページから他のプロジェクトやフォルダーに追加できます。

エージェントをプロジェクトに関連付けると、そのプロジェクト内のリソースを管理できるようになります。一方、エージェントをフォルダに関連付けると、フォルダ管理者またはプロジェクト管理者はどのプロジェクトでエージェントを使用するかを決定できるようになります。管理機能を提供するには、エージェントを特定のプロジェクトにリンクする必要があります。

"エージェントをプロジェクトに関連付ける方法を学習します。"

メンバーと役割

メンバー

組織のメンバーは、ユーザー アカウントまたはサービス アカウントです。サービス アカウントは通常、アプリケーションによって、人間の介入なしに指定されたタスクを完了するために使用されます。

NetApp Consoleにサインアップした後、メンバーを組織に追加する必要があります。追加したら、リソースへのアクセスを提供するロールを割り当てることができます。コンソール内からサービス アカウントを手動で追加することも、 NetApp ConsoleIAM API を通じてサービス アカウントの作成と管理を自動化することもできます。

"組織にメンバーを追加する方法を学びます。"

アクセスロール

コンソールには、組織のメンバーに割り当てることができるアクセス ロールが用意されています。

メンバーをロールに関連付けると、組織全体、特定のフォルダー、または特定のプロジェクトに対してそのロールを付与できます。選択したロールにより、階層の選択した部分にあるリソースに対する権限がメンバーに付与されます。

NetApp Consoleは、「最小権限」の原則に準拠したきめ細かなロールを提供します。つまり、アクセスロールは、ユーザーに必要なものだけへのアクセスを許可するように設計されています。

つまり、ユーザーの職務が拡大するにつれて、複数のロールが割り当てられる可能性があります。

"アクセスロールについて学ぶ" 。

## IAM戦略の例

### 小規模組織戦略

ユーザー数が 50 人未満で、ストレージ管理が集中している組織の場合は、スーパー管理者とスーパー閲覧者のロールを使用した簡素化されたアプローチを検討してください。

例：**ABC**株式会社（**5**人チーム）

- 構造**:** 3 つのプロジェクト (プロダクション、開発、バックアップ) を持つ単一の組織
- 役割**:**
  - 上級メンバー 2 名: 完全な管理アクセス権限を持つ スーパー管理者 ロール
  - 3 人のチームメンバー: 変更権限のない監視用の スーパー ビューアー ロール
- エージェント戦略**:** 共有リソースアクセスのためにすべてのプロジェクトに関連付けられた単一のエージェント
- 利点**:** 管理が簡素化され、役割の複雑さが軽減され、幅広いアクセスを必要とするチームに適しています

### 多地域企業戦略

地域的な事業や専門チームを持つ大規模な組織の場合は、地理的または事業部門の境界を表すフォルダーを使用して階層的なアプローチを実装します。

例**: XYZ**株式会社（多国籍企業）

- 構造**:** 組織 > 地域フォルダ (北米、ヨーロッパ、アジア太平洋) > 地域ごとのプロジェクトフォルダ
- プラットフォームの役割**:**
  - 1 組織管理者: グローバルな監視とポリシー管理
  - 3 フォルダまたはプロジェクト管理者: 地域管理 (地域ごとに 1 人)
  - 1 フェデレーション管理者: 企業IDプロバイダーの統合
- リージョン別のストレージの役割**:**
  - 9 ストレージ管理者: 割り当てられたリージョン内のストレージ システムを検出して管理します
  - 2 ストレージビューア: リージョン間のストレージリソースを監視する
  - 1 システムヘルススペシャリスト: システムを変更せずにストレージのヘルスを管理します
- データ サービスの役割**:**
  - バックアップおよびリカバリ管理者: バックアップ責任に基づいたプロジェクトごと
  - ランサムウェア耐性管理者: プロジェクト全体のセキュリティチームの監視

- エージェント戦略: 適切な地理的プロジェクトに関連付けられた地域エージェント
- 利点: 役割の分離、地域の自治、現地の規制への準拠によるセキュリティの強化

部門別専門化戦略

特定のデータ サービス アクセスを必要とする専門チームを持つ組織の場合は、機能上の責任に基づいて対象を絞ったロールの割り当てを使用します。

例: **TechCorp** (中規模テクノロジー企業)

- 構造: 組織 > 部門フォルダ (IT、セキュリティ、開発) > プロジェクト固有のリソース
- 専門的な役割:
  - セキュリティ チーム: ランサムウェア耐性管理者 および 分類閲覧者 の役割
  - バックアップ チーム: 包括的なバックアップ操作を担当する バックアップおよびリカバリ スーパー管理者
  - 開発チーム:テスト環境管理のための ストレージ管理者
  - コンプライアンス チーム: 監視およびサポートケース管理を行う 運用サポート アナリスト
- エージェント戦略: リソースの所有権に基づいて部門プロジェクトにリンクされたエージェント
- 利点: カスタマイズされたアクセス制御、運用効率の向上、専門的なタスクに対する明確な説明責任

**NetApp Console**での**IAM**の次のステップ

- "NetApp ConsoleでIAMを使い始める"
- "IAMアクティビティを監視または監査する"
- "NetApp ConsoleIAMのAPIについて学ぶ"

## NetApp ConsoleでIDとアクセスを開始する

NetApp Consoleにサインアップすると、新しい組織を作成するように求められます。組織には、メンバー 1 人 (組織管理者) とデフォルト プロジェクト 1 つが含まれます。ビジネス ニーズを満たすように ID およびアクセス管理 (IAM) を設定するには、組織の階層をカスタマイズし、メンバーを追加し、リソースを追加または検出し、それらのリソースを階層全体に関連付ける必要があります。

組織の ID とアクセスを管理するには、組織管理者 または スーパー管理者 の権限が必要です。*フォルダーまたはプロジェクト管理者*権限があれば、アクセスできるフォルダーとプロジェクトのみを管理できます。

新しい組織を設定するには、次の手順に従ってください。順序は組織のニーズに応じて異なる場合があります。

1. デフォルトのプロジェクトを編集するか、組織の階層に追加します

デフォルトのプロジェクトを使用するか、ビジネス階層に一致する追加のプロジェクトとフォルダーを作成します。

"フォルダとプロジェクトを使ってリソースを整理する方法を学びます" 。

2 メンバーを組織に関連付ける

ユーザーがNetApp Consoleにサインアップしたら、そのユーザーをコンソール組織に明示的に追加する必要があります。組織にサービス アカウントを追加することもできます。

"メンバーとその権限を管理する方法を学ぶ" 。

3 リソースを追加または発見する

コンソールにリソース (システム) を追加または検出します。組織のメンバーはプロジェクト内からシステムを管理します。

リソースを作成または検出する方法を学びます。

- "Amazon FSx for NetApp ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes ONTAP"
- "Eシリーズシステム"
- "オンプレミスのONTAPクラスタ"
- "StorageGRID"

4 リソースを追加プロジェクトに関連付ける

コンソールでシステムを追加または検出すると、リソースが現在選択されているプロジェクトに自動的に関連付けられます。そのリソースを組織内の別のプロジェクトで使用できるようにするには、それぞれのプロジェクトに関連付けます。リソースの管理にコンソール エージェントを使用する場合は、コンソール エージェントをそれぞれのプロジェクトに関連付けます。

- "組織のリソース階層を管理する方法を学ぶ" 。
- "コンソールエージェントをフォルダまたはプロジェクトに関連付ける方法を学びます" 。

関連情報

- "NetApp Consoleのアイデンティティとアクセス管理について学ぶ"
- "IDとアクセスのためのAPIについて学ぶ"

## コンソール組織を設定する

### **NetApp Console**組織にフォルダとプロジェクトを追加する

ビジネス構造に合わせてフォルダーとプロジェクトを追加します。フォルダーとプロジェクトを作成したら、それらにリソースを関連付け、それらのプロジェクトへのメンバー アクセスを管理できます。

新しい組織を作成すると、コンソールによって 1 つのプロジェクトが自動的に作成されます。ほとんどの組

織では、複数のプロジェクトと、整理するためのフォルダーが必要です。"NetApp Consoleのリソース階層について学ぶ"。

フォルダーとプロジェクトを使用してリソースを整理する

NetApp Consoleでは、組織にはリソースを整理するのに役立つフォルダーとプロジェクトが含まれています。フォルダーは関連するプロジェクトをグループ化するのに役立ち、プロジェクトはリソースとメンバーのアクセスを管理するのに役立ちます。

フォルダ

フォルダーは関連するプロジェクトを整理するのに役立ちます。ネストされたフォルダーを作成して、組織の構造のさまざまなレベルを表すことができます。たとえば、各ビジネス ユニットの最上位フォルダーを作成し、そのビジネス ユニット内のさまざまなチームに対してサブフォルダーを作成することができます。次に、フォルダー内にプロジェクトを作成します。

フォルダーを使用すると、ロールの継承を使用してメンバーのアクセスをより効率的に管理することもできます。フォルダー レベルでメンバーにロールを割り当てると、メンバーはすべての子プロジェクトとフォルダーの権限を継承します。

フォルダは組織ツールであり、組織管理者、フォルダまたはプロジェクト管理者、スーパー管理者のロールなどの IAM 権限を持たないメンバーには表示されません。メンバーはフォルダーではなくプロジェクトにアクセスします。

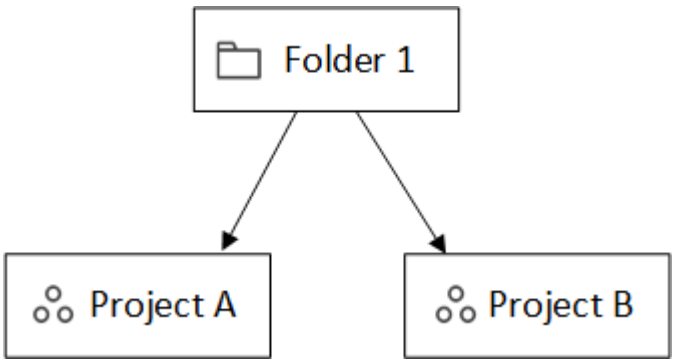
組織管理者はフォルダーを作成して管理責任を委任できます。フォルダーを作成した後、組織管理者はメンバーに特定のフォルダーのフォルダー管理者またはプロジェクト管理者の役割を割り当てることができます。これらのメンバーは、組織全体にアクセスすることなく、そのフォルダー内のすべてのプロジェクトを管理できます。

フォルダーには他のフォルダーやプロジェクトを子として持つことができますが、リソースを直接関連付けることはできません。リソースはプロジェクトに関連付ける必要があります。

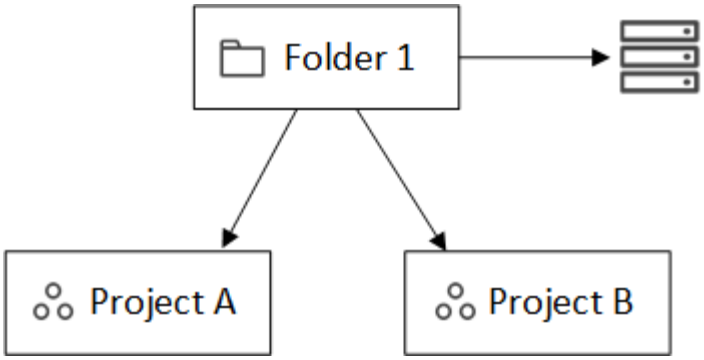
リソースをフォルダに関連付けるタイミング

組織管理者 はリソースをフォルダーに関連付けることができるため、フォルダーまたはプロジェクト管理者 はリソースをフォルダー内の適切なプロジェクトにリンクできます。

たとえば、次の 2 つのプロジェクトを含むフォルダーがあるとします。

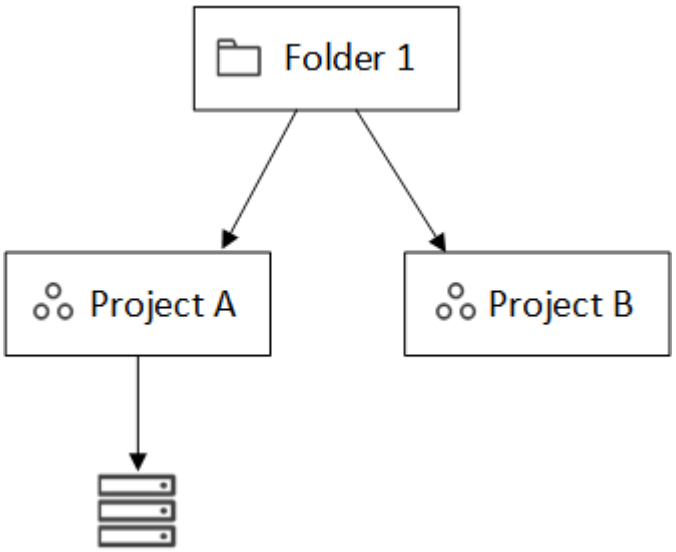



組織管理者は、リソースをフォルダに関連付けることができます。




リソースをフォルダーに関連付けても、すべてのプロジェクトがそのリソースにアクセスできるようになるわけではありません。フォルダーまたはプロジェクトの管理者 のみがそれを表示できます。 フォルダーまたはプロジェクト管理者 は、どのプロジェクトがアクセスできるかを決定し、リソースを適切なプロジェクトに関連付けます。

この例では、管理者はリソースをプロジェクト A に関連付けます。




プロジェクト A の権限を持つメンバーは、リソースにアクセスできるようになりました。

プロジェクト

リソースをプロジェクトに関連付けて、メンバーが管理できるようにします。管理とユーザー アクセスのために、リソースをプロジェクトに関連付ける必要があります。

組織は 1 つまたは複数のプロジェクトを持つことができます。プロジェクトは組織の直下またはフォルダー内に配置できます。エージェントを使用してプロジェクト内のリソースを検出する場合は、そのエージェントをそのプロジェクトに関連付ける必要もあります。

ユーザーは、システム ページで割り当てられたプロジェクト間を移動して、各プロジェクトに関連付けられたリソースを管理します。

フォルダまたはプロジェクトを追加する

リソースを管理するプロジェクトと、関連するプロジェクトをグループ化するフォルダーを追加します。新しい組織を作成すると、コンソールに 1 つのプロジェクトが含まれます。

組織のリソース構造内に最大 7 レベルのフォルダーとプロジェクトを作成できます。必要に応じてリソースを整理するためにネストされたフォルダーを作成します。

手順

1. *管理 > IDとアクセス*を選択します。
2. *組織*を選択します。
3. *組織*ページから、*フォルダーまたはプロジェクトの追加*を選択します。
4. *フォルダー*または*プロジェクト*を選択します。
5. フォルダまたはプロジェクトの詳細を入力してください:
   - 名前と場所: フォルダーまたはプロジェクトの名前を入力し、場所を選択します。フォルダーまたはプロジェクトを組織の下または別のフォルダー内に配置できます。
   - リソース: このフォルダーまたはプロジェクトに関連付けるリソースを選択します。コンソールにストレージ システムをまだ追加していない場合は、この手順を後で実行できます。

     メンバーは、リソースがプロジェクトに割り当てられるまで、フォルダー内のリソースにアクセスできません。必要なプロジェクトを作成するまで、フォルダーを使用してリソースを一時的に保持します。これにより、組織管理者はリソースの割り当てをフォルダまたはプロジェクト管理者に委任し、フォルダ内のプロジェクトにリソースを割り当てることができます。

   - アクセス: アクセスとロールを割り当てるには、*メンバーの追加*を選択します。プロジェクトまたはフォルダーへのメンバーの追加や削除はいつでも可能です。

     "アクセスロールについて学ぶ" 。
6. *追加*を選択します。

### フォルダまたはプロジェクトの名前を変更する

必要に応じてフォルダーまたはプロジェクトの名前を変更します。名前を変更しても、関連付けられているリソースやメンバー アクセスには影響しません。

手順

1. *組織*ページで、テーブル内のプロジェクトまたはフォルダに移動し、•••次に、*フォルダーの編集*または*プロジェクトの編集*を選択します。
2. *編集*ページで新しい名前を入力し、*適用*を選択します。

### フォルダまたはプロジェクトを削除する

チームの再編成やプロジェクトの完了後など、不要になったフォルダーやプロジェクトを削除します。

フォルダーまたはプロジェクトを削除する前に、そこにリソースが含まれていないことを確認してください。リソースを削除する方法を学ぶ。

手順

1. *組織*ページで、テーブル内のプロジェクトまたはフォルダに移動し、•••次に、[削除] を選択します。
2. フォルダーまたはプロジェクトを削除することを確認します。

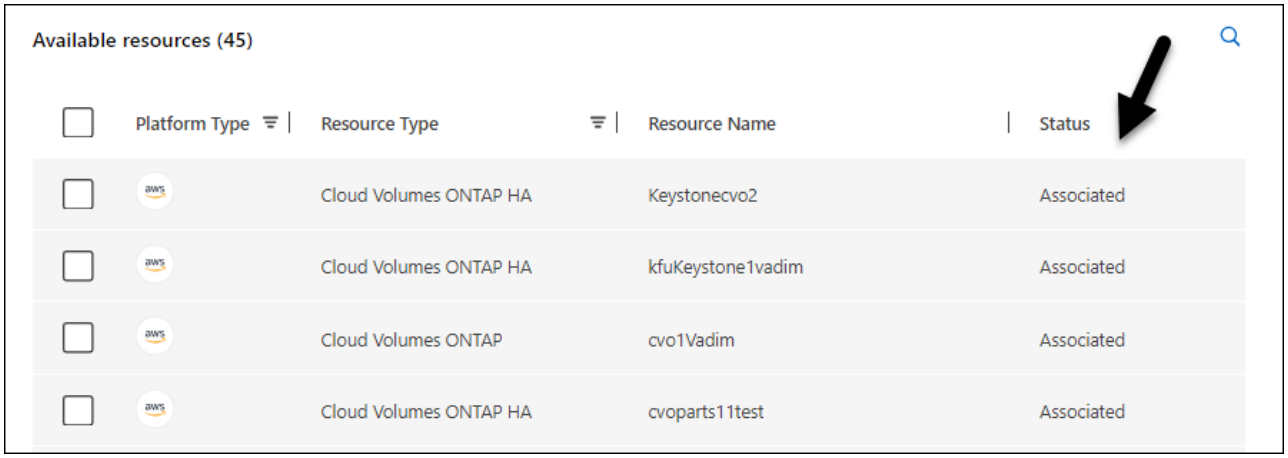
フォルダまたはプロジェクトに関連付けられたリソースを表示する

フォルダーまたはプロジェクトに関連付けられているリソースとメンバーを表示します。

手順

1. *組織*ページで、テーブル内のプロジェクトまたはフォルダに移動し、次に、*フォルダーの編集*または*プロジェクトの編集*を選択します。


2. *編集*ページでは、*リソース*または*アクセス*セクションを展開して、選択したフォルダーまたはプロジェクトの詳細を表示できます。
   - 関連するリソースを表示するには、[リソース] を選択します。表の ステータス 列には、フォルダーまたはプロジェクトに関連付けられているリソースが識別されます。




フォルダまたはプロジェクトに関連付けられたリソースを変更する

組織のニーズの変化に応じて、フォルダーまたはプロジェクトに関連付けられているリソースを変更できます。

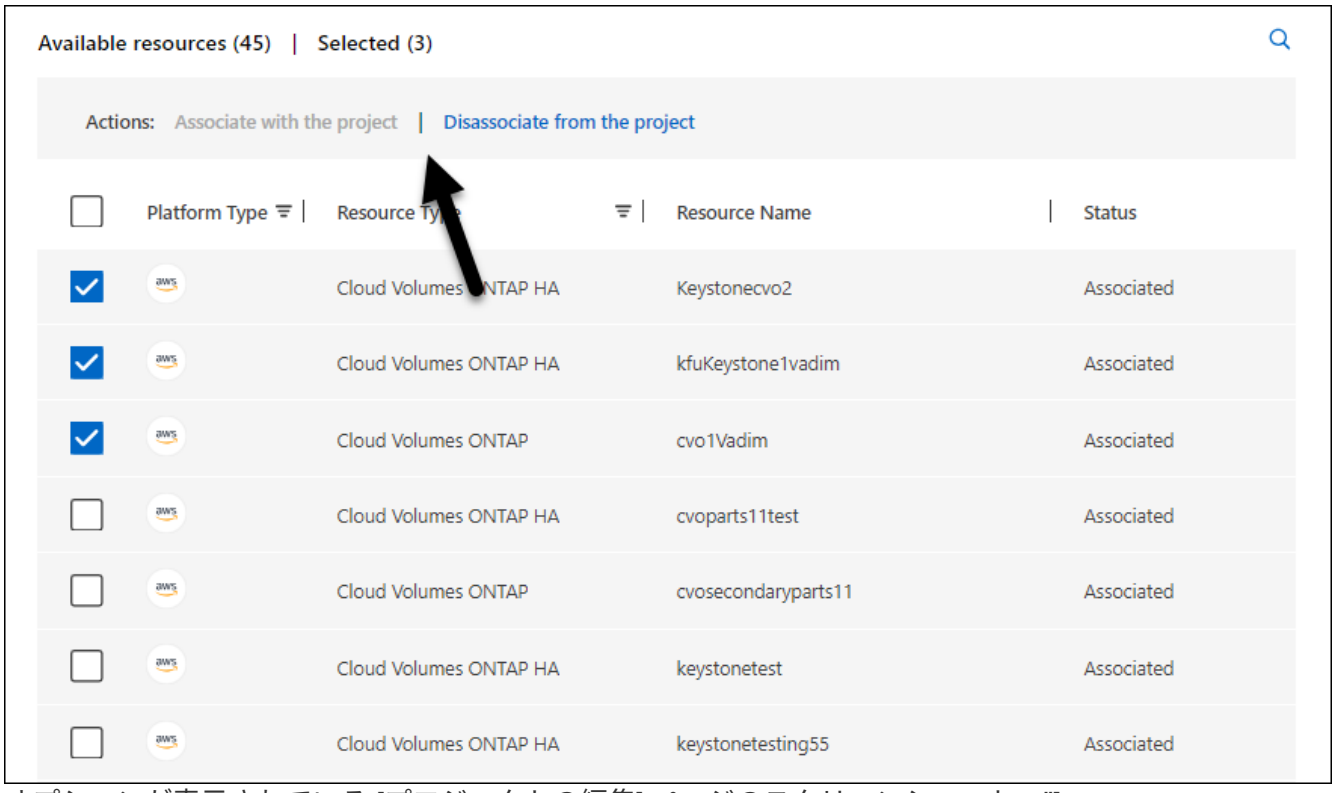
手順

1. *組織*ページで、テーブル内のプロジェクトまたはフォルダに移動し、次に、*フォルダーの編集*または*プロジェクトの編集*を選択します。
2. *編集*ページで*リソース*を選択します。

   表の ステータス 列には、フォルダーまたはプロジェクトに関連付けられているリソースが識別されます。

3. 関連付けまたは関連付けを解除するリソースを選択します。

4. 選択したリソースに基づいて、*プロジェクトに関連付ける*または*プロジェクトとの関連付けを解除する*のいずれかを選択します。



オプションが表示されている [プロジェクトの編集] ページのスクリーンショット。"]

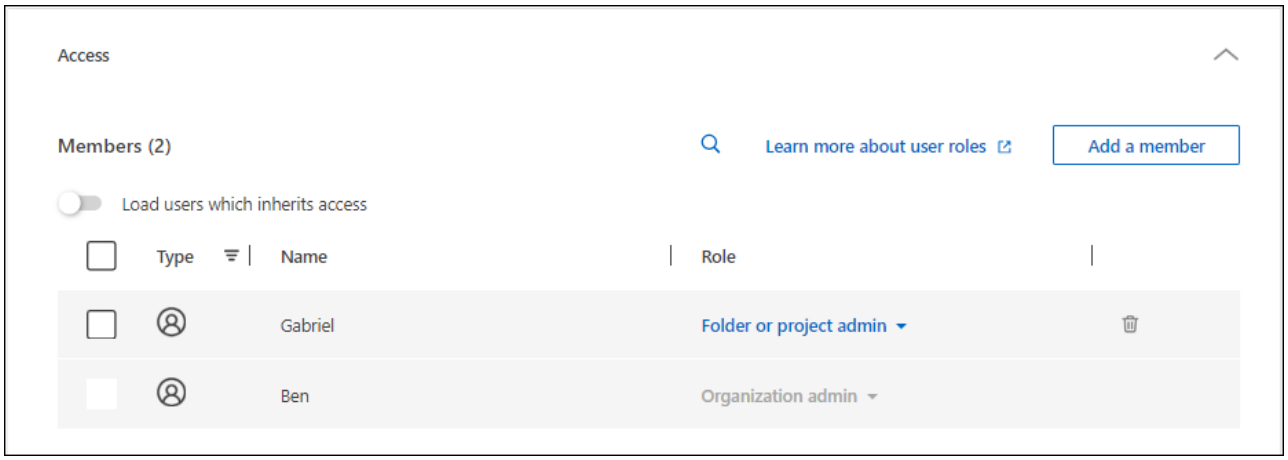
5. *適用*を選択します。

フォルダまたはプロジェクトに関連付けられたメンバーを表示する

組織 ページから、フォルダーまたはプロジェクトに関連付けられているメンバーを表示できます。

手順

1. *組織*ページで、テーブル内のプロジェクトまたはフォルダに移動し、•••次に、*フォルダーの編集*または*プロジェクトの編集*を選択します。
2. *編集*ページで*アクセス*を選択すると、選択したフォルダーまたはプロジェクトにアクセスできるメンバーのリストが表示されます。
    - フォルダーまたはプロジェクトにアクセスできるメンバーを表示するには、「アクセス」を選択します。




フォルダまたはプロジェクトへのメンバーアクセスを変更する

メンバー アクセスを変更してリソース アクセスを制御します。フォルダー レベルで割り当てられたロールは、すべての子プロジェクトとフォルダーに継承されることに注意してください。

フォルダーまたは組織レベルから継承されたメンバー アクセスを下位レベルで変更することはできません。上位階層レベルでメンバーの権限を変更してアクセスを変更するか、 "メンバーページから権限を管理する"。

手順

1. *組織*ページで、テーブル内のプロジェクトまたはフォルダに移動し、次に、*フォルダーの編集*または*プロジェクトの編集*を選択します。
2. *編集*ページで*アクセス*を選択すると、選択したフォルダーまたはプロジェクトにアクセスできるメンバーのリストが表示されます。
3. メンバーアクセスの変更:
   - メンバーを追加: フォルダーまたはプロジェクトに追加するメンバーを選択し、役割を割り当てます。
   - メンバーの役割を変更する: 組織管理者以外の役割を持つメンバーの場合は、既存の役割を選択してから、新しい役割を選択します。
   - メンバーのアクセスを削除: 表示しているフォルダーまたはプロジェクトで定義されたロールを持つメンバーのアクセスを削除できます。
4. *適用*を選択します。

関連情報

- "NetApp ConsoleのIDとアクセスについて学ぶ"
- "アイデンティティとアクセスを始める"
- "アイデンティティとアクセスAPIについて学ぶ"

**NetApp Console**のフォルダとプロジェクトにリソースを追加する

NetApp Console組織内のプロジェクトとフォルダにリソースを追加して、ユーザーのリソース アクセスを制御します。プロジェクト レベルでユーザーにアクセス権を付与します。

リソース は、ストレージ リソース、コンソール エージェント、バックアップおよびリカバリ ワークロードなど、コンソールが認識するエンティティです。

コンソールの*リソース*ページからリソースを表示および管理できます。

### コンソールリソースの種類

NetApp Console組織内のプロジェクトには、いくつかの種類のリソースを関連付けることができます。

ストレージリソース

ストレージ リソースは、組織内で最も一般的なタイプのリソースであり、オンプレミスとクラウド ストレージ システムの両方を表します。コンソールにストレージ システムを追加するときに、それをフォルダーまたはプロジェクトに追加できます。それまでは、コンソールはそれを未検出としてマークし、リソース ページには表示しません。

コンソールエージェント

コンソール エージェントを使用してストレージ システムを検出した場合は、エージェントを同じフォルダーまたはプロジェクトに追加します。これにより、ユーザーはデータ サービスやコンソール ネイティブのストレージ管理などのエージェント対応機能を実行できます。コンソールの エージェント ページから、フォルダーまたはプロジェクトにエージェントを追加できます。"コンソールエージェントをフォルダまたはプロジェクトに関連付ける方法を学びます"。

**Keystone**のサブスクリプション

組織内でKeystoneサブスクリプションがある場合は、リソース ページでそれを表示できます。Keystoneサブスクリプションをフォルダーまたはプロジェクトに関連付けて、それらのフォルダーまたはプロジェクトに対する権限を持つメンバーにアクセスを提供することができます。

### 組織内のリソースを表示する

組織に関連付けられている検出されたリソースと未検出のリソースの両方を表示できます。システムはストレージ リソースを検出し、コンソールに追加されるまでそれらを未検出としてマークします。

ユーザーがAmazon FSx for NetApp ONTAPリソースが除外されます。これらのリソースは、システム ページまたはワークロードから表示できます。

手順

1. *管理 > IDとアクセス*を選択します。
2. *リソース*を選択します。
3. *高度な検索とフィルタリング*を選択します。
4. 利用可能なオプションを使用してリソースを見つけます。
   - リソース名で検索: テキスト文字列を入力し、*追加*を選択します。
   - プラットフォーム: Amazon Web Services など、1 つ以上のプラットフォームを選択します。
   - リソース: Cloud Volumes ONTAPなどの 1 つ以上のリソースを選択します。
   - 組織、フォルダー、またはプロジェクト: 組織全体、特定のフォルダー、または特定のプロジェクトを選択します。
5. *検索*を選択します。

### リソースをフォルダやプロジェクトに関連付ける

リソースをフォルダーまたはプロジェクトに関連付けると、そのフォルダーまたはプロジェクトに対する権限を持つメンバーがリソースを利用できるようになります。

手順

1. リソース*ページで、テーブル内のリソースに移動し、 ••• 次に、[*フォルダーまたはプロジェクトに関連付ける]を選択します。
2. フォルダーまたはプロジェクトを選択し、[承認] を選択します。
3. 追加のフォルダーまたはプロジェクトを関連付けるには、[フォルダーまたはプロジェクトの追加] を選択し、フォルダーまたはプロジェクトを選択します。

   管理者権限を持つフォルダーとプロジェクトからのみ選択できることに注意してください。

4. *リソースの関連付け*を選択します。
   - リソースをプロジェクトに関連付けると、それらのプロジェクトに対する権限を持つメンバーは、コンソールからリソースにアクセスできるようになります。
   - リソースをフォルダーに関連付けると、フォルダーまたはプロジェクトの管理者がリソースにアクセスし、フォルダー内のプロジェクトに関連付けることができるようになります。"リソースをフォルダに関連付ける方法について学習します"。

終了後の操作

コンソール エージェントを使用してリソースを検出する場合は、コンソール エージェントをプロジェクトに関連付けてアクセスを許可します。そうでない場合、組織管理者 ロールを持たないメンバーはコンソール エージェントとその関連リソースにアクセスできません。

"コンソールエージェントをフォルダまたはプロジェクトに関連付ける方法を学びます"。

### リソースに関連付けられたフォルダとプロジェクトを表示する

特定のリソースに関連付けられているフォルダーとプロジェクトを表示できます。

どの組織メンバーがリソースにアクセスできるのかを確認する必要がある場合は、"リソースに関連付けられているフォルダとプロジェクトにアクセスできるメンバーを表示します" 。

手順

1. *リソース*ページで、テーブル内のリソースに移動し、 ••• 次に、[詳細を表示] を選択します。

次の例は、1 つのプロジェクトに関連付けられているリソースを示しています。

どの組織メンバーがリソースにアクセスできるのかを確認するには、"関連付けられたフォルダとプロジェクトへのアクセス権を持つメンバーを表示する" 。

フォルダまたはプロジェクトからリソースを削除する

フォルダーまたはプロジェクトからリソースを削除するには、その関連付けを削除します。これにより、メンバーはそのフォルダーまたはプロジェクト内のリソースを管理できなくなります。

検出されたリソースを組織全体から削除するには、「システム」ページに移動してシステムを削除します。

手順

1. *リソース*ページで、テーブル内のリソースに移動し、次に、[詳細を表示] を選択します。
2. フォルダまたはプロジェクトからリソースを削除するには、 フォルダーまたはプロジェクトの横にあります。
3. 関連付けを削除するには、[削除] を選択します。

関連情報

- "NetApp ConsoleのIDとアクセスについて学ぶ"
- "NetApp ConsoleでIDとアクセスを開始する"
- "IDとアクセスのためのAPIについて学ぶ"

コンソールエージェントを他のフォルダやプロジェクトに関連付ける

コンソール エージェントを特定のプロジェクトに関連付けて、リソース管理とデータ サービス アクセスを有効にします。コンソール エージェントを通じて検出されたリソースでは、チーム アクセスのために、リソースとエージェントの両方が同じそれぞれのプロジェクトに関連付けられている必要があります。

スーパー管理者と組織管理者はエージェントを作成し、任意のエージェントを任意のプロジェクトまたはフォルダに関連付けることができます。フォルダーまたはプロジェクトの管理者は、権限を持つフォルダーとプロジェクトにのみ既存のエージェントを関連付けることができます。"フォルダまたはプロジェクト管理者が実行できるアクションの詳細"。

手順

1. 管理 **> ID**とアクセス > *エージェント*を選択します。
2. 表から、関連付けるコンソール エージェントを見つけます。

   特定のコンソール エージェントを検索するには、表の上にある検索機能を使用するか、リソース階層で表をフィルター処理します。

3. コンソールエージェントにリンクされたフォルダとプロジェクトを表示するには、次に、[詳細を表示] を選択します。

   このページには、コンソール エージェントに関連付けられているフォルダーとプロジェクトの詳細が表示されます。

4. *フォルダーまたはプロジェクトに関連付ける*を選択します。
5. フォルダーまたはプロジェクトを選択し、[承認] を選択します。
6. コンソール エージェントを追加のフォルダーまたはプロジェクトに関連付けるには、[フォルダーまたはプロジェクトの追加] を選択し、フォルダーまたはプロジェクトを選択します。
7. *Associate Agent*を選択します。

終了後の操作

コンソール エージェントのリソースを、リソース ページの同じフォルダーおよびプロジェクトに関連付けます。

"リソースをフォルダやプロジェクトに関連付ける方法を学びます" 。

関連情報

- "NetApp Consoleエージェントについて学ぶ"
- "NetApp Consoleのアイデンティティとアクセス管理について学ぶ"
- "アイデンティティとアクセスを始める"
- "IDとアクセス管理のためのAPIについて学ぶ"

## コンソール組織にユーザーを追加する

### NetApp Console組織にユーザーを追加する

コンソール内で、アクセス ロールに応じてユーザーにプロジェクトまたはフォルダーへのアクセス権を付与します。アクセス ロール には、メンバー (ユーザーまたはサービス アカウント) がリソース階層の割り当てられたレベルで特定のアクションを実行できるようにする一連の権限が含まれています。

必要なアクセスロール

スーパー管理者、組織管理者、またはフォルダーまたはプロジェクトの管理者（管理しているフォルダーとプロジェクトの場合）。"アクセスロールについて学ぶ"。

#### NetApp Consoleでアクセスを許可する方法を理解する

NetApp Consoleは、ロールベースのアクセス制御 (RBAC) を使用して権限を管理します。ユーザーに個別に、またはフェデレーション グループを通じてロールを割り当てます。各ロールは、特定のリソースに対して許可されるアクションを定義します。

NetApp Consoleでアクセス権を付与する場合は、次の点に注意してください。

- すべてのユーザーは、リソースへのアクセスを許可する前に、まずNetApp Consoleにサインアップする必要があります。
- ロールが割り当てられたフェデレーション グループのメンバーであっても、ユーザーがリソースにアクセスするには、コンソールで各ユーザーにロールを明示的に割り当てる必要があります。
- コンソールから直接サービス アカウントを追加し、ロールを割り当てることができます。

NetApp Consoleは、ユーザー アカウント、サービス アカウント、フェデレーション グループの 3 種類のメンバーをサポートしています。

ユーザーがフェデレーション グループに属している場合でも、ユーザーを追加してロールを割り当てるには、その前にNetApp Consoleにサインアップする必要があります。コンソールで直接サービス アカウントを作成します。

リソースにアクセスするには、すべてのメンバーに少なくとも 1 つのロールが明示的に割り当てられている必要があります。

メンバーを追加するときは、リソース レベル (組織、フォルダー、またはプロジェクト) を選択し、必要な権限を持つロールを割り当てます。

## ユーザーを追加する

ユーザーはNetApp Consoleにサインアップしますが、リソースにアクセスできるように、組織管理者またはフォルダまたはプロジェクト管理者がユーザーを組織、フォルダ、またはプロジェクトに追加する必要があります。

開始する前に：

ユーザーはNetApp Consoleにすでにサインアップしている必要があります。まだ登録していない場合は、"NetApp Consoleにサインアップします。"

> フェデレーション グループに属するユーザーを追加する場合は、そのユーザーがすでにNetApp Consoleにサインアップしており、コンソールでロールが明示的に割り当てられていることを確認してください。NetApp、組織閲覧者などの最小限のアクセス ロールを割り当てることを推奨しています。

手順

1. *管理 > IDとアクセス*を選択します。
2. *メンバー*を選択します。
3. *メンバーを追加*を選択します。
4. *メンバータイプ*では*ユーザー*を選択したままにします。
5. *ユーザーのメール*には、ユーザーが作成したログインに関連付けられているメール アドレスを入力します。
6. *組織、フォルダ、またはプロジェクトを選択*セクションを使用して、メンバーに権限を与えるリソース階層のレベルを選択します。

   次の点に注意してください。

   - 権限を持つフォルダーとプロジェクトのみを選択できます。
   - 組織またはフォルダを選択すると、そのすべてのコンテンツに対する権限がメンバーに付与されます。
   - 組織管理者 ロールは組織レベルでのみ割り当てることができます。
7. *カテゴリを選択*し、選択した組織、フォルダ、またはプロジェクトに関連付けられているリソースに対する権限をメンバーに付与する*ロール*を選択します。

"アクセスロールについて学ぶ" 。

8. さらに多くのフォルダー、プロジェクト、またはロールへのアクセス権を付与するには、[ロールの追加]を選択し、フォルダー、プロジェクト、またはロールのカテゴリを選択して、ロールを選択します。
9. *追加*を選択します。

   コンソールはユーザーに指示を電子メールで送信します。

## サービスアカウントを追加する

サービス アカウントを使用すると、タスクを自動化し、コンソール API に安全に接続できます。簡単なセットアップの場合はクライアント ID とシークレットを選択し、自動化環境またはクラウドネイティブ環境でのセキュリティを強化する場合は JWT (JSON Web Token) を選択します。セキュリティ要件を満たす方法を選択してください。

開始する前に：

JWT 認証の場合は、公開鍵または証明書を準備します。

手順

1. *管理 > IDとアクセス*を選択します。
2. *メンバー*を選択します。
3. *メンバーを追加*を選択します。
4. *メンバータイプ*では*サービスアカウント*を選択します。
5. サービス アカウントの名前を入力します。
6. JWT 認証を使用するには、[秘密キー **JWT** 認証を使用する] を選択し、公開 RSA キーまたは証明書をアップロードします。クライアント ID とシークレットを使用する場合はスキップします。

   X.509 証明書。PEM、CRT、または CER 形式である必要があります。

   a. 証明書の有効期限通知を設定します。 7日間または30日間を選択します。有効期限通知は、スーパー管理者または組織管理者のロールを持つユーザーにメールで送信され、コンソールに表示されます。
7. *組織、フォルダ、またはプロジェクトを選択*セクションを使用して、メンバーに権限を与えるリソース階層のレベルを選択します。

   次の点に注意してください。

   - 権限を持つフォルダーとプロジェクトからのみ選択できます。
   - 組織またはフォルダを選択すると、そのすべてのコンテンツに対する権限がメンバーに付与されます。
   - 組織管理者 ロールは組織レベルでのみ割り当てることができます。
8. *カテゴリー*を選択し、選択した組織、フォルダ、またはプロジェクト内のリソースに対するメンバー権限を付与する*ロール*を選択します。

   "アクセスロールについて学ぶ" 。

9. さらに多くのフォルダー、プロジェクト、またはロールへのアクセス権を付与するには、[ロールの追加]

を選択し、フォルダー、プロジェクト、またはロールのカテゴリを選択して、ロールを選択します。

10. JWT 認証を使用しない場合は、クライアント ID とクライアント シークレットをダウンロードまたはコピーします。

    コンソールにはクライアント シークレットが 1 回だけ表示されます。安全にコピーしておけば、紛失した場合でも後で再作成できます。

11. JWT 認証を選択した場合は、クライアント ID と JWT オーディエンスをダウンロードまたはコピーします。コンソールにはこの情報が一度だけ表示され、後で取得することはできません。
12. *閉じる*を選択します。

### 組織にフェデレーショングループを追加する

アイデンティティ プロバイダー (IdP) から組織にフェデレーション グループを追加し、それに 1 つ以上のロールを割り当てることができます。フェデレーション グループのメンバーは、コンソールでグループに割り当てたロールを継承します。

フェデレーション グループにロールを割り当てる前に、次の点を確認してください。

- IdP とコンソール間のフェデレーションを設定します。 "フェデレーションを設定する方法を学習します。"
- グループは既に IdP に存在し、コンソールへのアプリ アクセスが割り当てられている必要があります。
- グループに属するユーザーは、すでにNetApp Consoleにサインアップしており、コンソールで明示的にロールが割り当てられている必要があります。NetApp、組織閲覧者などの最小限のアクセス ロールを割り当てることを推奨しています。

手順

1. *管理 > IDとアクセス*を選択します。
2. *メンバー*を選択します。
3. *メンバーを追加*を選択します。
4. *メンバータイプ*では*フェデレーショングループ*を選択します。
5. グループがメンバーである連盟を選択します
6. *グループ名*には、IdP 内のグループの正確な名前を入力します。
7. *組織、フォルダ、またはプロジェクトを選択*セクションを使用して、メンバーに権限を与えるリソース階層のレベルを選択します。

    次の点に注意してください。

    - 権限を持つフォルダーとプロジェクトからのみ選択できます。
    - 組織またはフォルダを選択すると、そのすべてのコンテンツに対する権限がメンバーに付与されます。
    - 組織管理者 ロールは組織レベルでのみ割り当てることができます。

8. *カテゴリー*を選択し、選択した組織、フォルダ、またはプロジェクト内のリソースに対するメンバー権限を付与する*ロール*を選択します。

    "アクセスロールについて学ぶ" 。

9. さらに多くのフォルダー、プロジェクト、またはロールへのアクセス権を付与するには、[ロールの追加]を選択し、フォルダー、プロジェクト、またはロールのカテゴリを選択して、ロールを選択します。

関連情報

- "NetApp Consoleのアイデンティティとアクセス管理について学ぶ"
- "アイデンティティとアクセスを始める"
- "NetApp Consoleアクセスロール"
- "IDとアクセスのためのAPIについて学ぶ"

# ユーザーアクセスとセキュリティを管理する

## **NetApp Console**のロールベースアクセス制御（**RBAC**）について学ぶ

ロールベースのアクセス制御 (RBAC) を使用してNetApp Consoleへのユーザー アクセスを管理し、組織、フォルダ、またはプロジェクト レベルで事前定義されたロールを割り当てます。各ロールは、割り当てられたスコープ内でユーザーが実行できるアクションを定義する特定の権限を付与します。

NetApp は最小限の権限でコンソール ロールを設計しているため、各ロールにはそのタスクに必要な権限のみが含まれます。このアプローチでは、各メンバーが必要なものへのアクセスを制限することでセキュリティが強化されます。

リソースをフォルダーとプロジェクトに整理した後、組織のメンバーに特定のフォルダーまたはプロジェクトに対するロールを割り当て、メンバーが自分の責任のみを実行できるようにします。

たとえば、特定のプロジェクト レベルのランサムウェア レジリエンス管理者ロールをメンバーに割り当てて、組織全体へのより広範なアクセス権を付与することなく、そのプロジェクト内のリソースに対してランサムウェア レジリエンス操作を実行できるようにすることができます。同じユーザーに、組織内の複数のプロジェクトの役割を付与できます。

ユーザーの責任に応じて、同じスコープまたは異なるスコープに対して複数のロールを割り当てることができます。たとえば、小規模な組織では、同じユーザーが組織レベルでランサムウェア耐性とバックアップとリカバリの両方のタスクを管理する可能性がありますが、大規模な組織では、プロジェクト レベルで各ロールに異なるユーザーが割り当てられている可能性があります。

### コンソール組織メンバーの種類

NetApp Console組織には、次の 3 種類のメンバーがあります。 * ユーザー アカウント: リソースを管理するためにNetApp Consoleにログインする個々のユーザー。ユーザーは、組織に追加される前にNetApp Consoleにサインアップする必要があります。* サービス アカウント: API 経由でNetApp Consoleと対話するためにアプリケーションまたはサービスによって使用される人間以外のアカウント。サービス アカウントをコンソール組織に直接追加できます。* フェデレーション グループ: アイデンティティ プロバイダー (IdP) から同期されたグループで、複数のユーザーのアクセスをまとめて管理できます。フェデレーション グループ内の各ユーザーは、グループに付与されたリソースにアクセスする前に、 NetApp Consoleにサインアップし、アクセス ロールを持って組織に追加されている必要があります。

"組織にメンバーを追加する方法を学びます。"

#### NetApp Consoleの事前定義されたロール

NetApp Consoleには、組織のメンバーに割り当てることができる定義済みのロールが含まれています。各ロールには、割り当てられた範囲 (組織、フォルダ、またはプロジェクト) 内でメンバーが実行できるアクションを指定する権限が含まれています。

NetApp Consoleのロールでは、メンバーがタスクに必要な権限のみを持つようにする最小権限の原則が採用されており、ロールは提供されるアクセスの種類によって分類されます。

- プラットフォームの役割: コンソール管理権限を付与する
- データ サービス ロール: ランサムウェア耐性やバックアップとリカバリなどの特定のデータ サービスを管理するための権限を提供します。
- アプリケーション ロール: ストレージの管理とコンソール イベントおよびアラートの監査の権限を提供します。

メンバーの責任に基づいて、複数の役割を割り当てることができます。たとえば、特定のプロジェクトに対して、メンバーにランサムウェア耐性管理者ロールとバックアップとリカバリ管理者ロールの両方を割り当てることができます。

"NetApp Consoleで利用可能な定義済みロールについて学習します"。

### NetApp Consoleでメンバーアクセスを管理する

コンソール組織内のメンバー アクセスを管理します。権限を設定するためにロールを割り当てます。メンバーが退会したら削除します。

必要なアクセスロール

スーパー管理者、組織管理者、またはフォルダーまたはプロジェクトの管理者（管理しているフォルダーとプロジェクトの場合）。リンク:reference-iam-predefined-roles.html[アクセス ロールについて学ぶ]

プロジェクトまたはフォルダーごとにアクセス ロールを割り当てることができます。たとえば、特定の 2 つのプロジェクトに対してユーザーにロールを割り当てたり、フォルダー レベルでロールを割り当てて、フォルダー内のすべてのプロジェクトに対する Ransomware Resilience 管理者ロールをユーザーに付与したりすることができます。

ユーザーにアクセスを割り当てる前に、フォルダーとプロジェクトを追加します。 "フォルダーとプロジェクトを追加する方法を学びます。"

#### NetApp Consoleでアクセスを許可する方法を理解する

NetApp Consoleは、ロールベースのアクセス制御 (RBAC) モデルを使用してユーザー権限を管理します。事前定義されたロールをメンバーに個別に割り当てることも、フェデレーション グループを通じて割り当てることもできます。サービス アカウントやフェデレーション グループにロールを追加して割り当てることができます。各ロールは、メンバーが関連付けられたリソースで実行できるアクションを定義します。

NetApp Consoleでアクセス権を付与する場合は、次の点に注意してください。

- すべてのユーザーは、リソースへのアクセス権を付与される前に、まずNetApp Consoleにサインアップする必要があります。
- ロールが割り当てられたフェデレーション グループのメンバーであっても、ユーザーがリソースにアクセ

スするには、コンソールで各ユーザーにロールを明示的に割り当てる必要があります。

- コンソールから直接サービス アカウントを追加し、ロールを割り当てることができます。

### ロール継承の使用

NetApp Consoleで組織、フォルダ、またはプロジェクト レベルでロールを割り当てると、そのロールは選択したスコープ内のすべてのリソースに自動的に継承されます。たとえば、フォルダ レベルのロールはその中に含まれるすべてのプロジェクトに適用されますが、プロジェクト レベルのロールはそのプロジェクト内のすべてのリソースに適用されます。

#### 組織メンバーを表示

メンバーが利用できるリソースと権限を理解するには、組織のリソース階層のさまざまなレベルでメンバーに割り当てられているロールを表示できます。"ロールを使用してコンソール リソースへのアクセスを制御する方法を学習します。"

手順

1. *管理 > IDとアクセス*を選択します。
2. *メンバー*を選択します。

   メンバー テーブルには組織のメンバーがリストされます。

3. *メンバー*ページで、テーブル内のメンバーに移動し、•••次に、[詳細を表示] を選択します。

#### メンバーに割り当てられた役割を表示する

現在割り当てられているロールを確認できます。

フォルダーまたはプロジェクト管理者 ロールを持っている場合、ページには組織内のすべてのメンバーが表示されます。ただし、メンバー権限を表示および管理できるのは、権限を持つフォルダーとプロジェクトのみです。"フォルダまたはプロジェクト管理者が実行できるアクションの詳細" 。

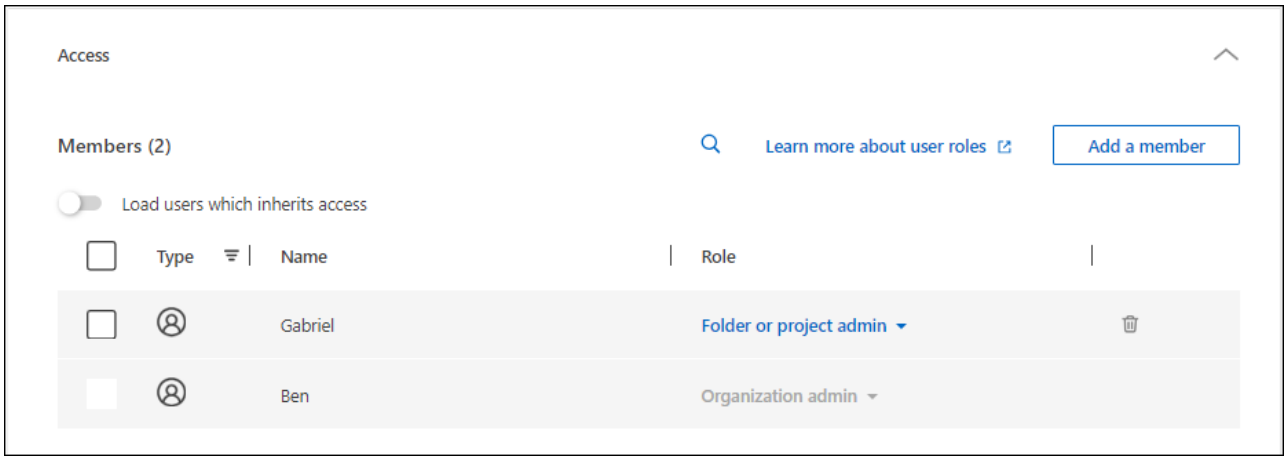
1. *メンバー*ページで、テーブル内のメンバーに移動し、 ••• 次に、[詳細を表示] を選択します。
2. 表で、メンバーに割り当てられたロールを表示する組織、フォルダ、またはプロジェクトのそれぞれの行を展開し、「ロール」列で「表示」を選択します。

#### フォルダまたはプロジェクトに関連付けられたメンバーを表示する

特定のフォルダーまたはプロジェクトにアクセスできるメンバーを表示できます。

手順

1. *管理 > IDとアクセス*を選択します。
2. *組織*を選択します。
3. *組織*ページで、テーブル内のプロジェクトまたはフォルダに移動し、•••次に、*フォルダーの編集*または*プロジェクトの編集*を選択します。
   - フォルダーまたはプロジェクトにアクセスできるメンバーを表示するには、「アクセス」を選択します。




メンバーアクセスの割り当てまたは変更

ユーザーがNetApp Consoleにサインアップしたら、そのユーザーを組織に追加し、リソースへのアクセスを提供するロールを割り当てることができます。 "組織にメンバーを追加する方法を学びます。"

必要に応じて役割を追加または削除することで、メンバーのアクセスを調整できます。

メンバーにアクセスロールを追加する

通常、組織にメンバーを追加するときにロールを割り当てますが、ロールを削除または追加することでいつでも更新できます。

組織、フォルダ、またはプロジェクトへのアクセス ロールをユーザーに割り当てることができます。

メンバーは、同じプロジェクト内および異なるプロジェクト内で複数の役割を持つことができます。たとえば、小規模な組織では、利用可能なすべてのアクセス ロールを同じユーザーに割り当てる場合がありますが、大規模な組織では、ユーザーにさらに専門的なタスクを実行させる場合があります。あるいは、組織レベルで 1 人のユーザーに Ransomware Resilience 管理者ロールを割り当てることもできます。この例では、ユーザーは組織内のすべてのプロジェクトでランサムウェア耐性タスクを実行できるようになります。

アクセス ロール戦略は、 NetAppリソースの編成方法と一致する必要があります。

手順

1. *管理 > IDとアクセス*を選択します。
2. *メンバー*を選択します。
3. メンバータブのいずれかを選択します: ユーザー、サービス アカウント、または フェデレーション グループ。
4. アクションメニューを選択•••役割を割り当てるメンバーの横にある をクリックし、[役割の追加] を選択します。
5. ロールを追加するには、ダイアログ ボックスの手順を完了します。
   - 組織、フォルダ、またはプロジェクトを選択: メンバーに権限を与えるリソース階層のレベルを選択します。

     組織またはフォルダを選択した場合、メンバーにはその組織またはフォルダ内に存在するすべてのものに対する権限が付与されます。

- カテゴリを選択: 役割のカテゴリを選択します。"アクセスロールについて学ぶ" 。
- *ロール*を選択: 選択した組織、フォルダ、またはプロジェクトに関連付けられているリソースに対する権限をメンバーに付与するロールを選択します。
- ロールの追加: 組織内の追加のフォルダーまたはプロジェクトへのアクセス権を付与する場合は、*ロールの追加*を選択し、別のフォルダーまたはプロジェクトまたはロールのカテゴリを指定してから、ロールのカテゴリと対応するロールを選択します。

6. *新しいロールを追加*を選択します。

### メンバーに割り当てられた役割を変更する

メンバーの役割を変更してアクセスを更新します。

ユーザーには少なくとも 1 つのロールが割り当てられている必要があります。ユーザーからすべてのロールを削除することはできません。すべてのロールを削除する必要がある場合は、組織からユーザーを削除する必要があります。

#### 手順

1. *管理 > IDとアクセス*を選択します。
2. *メンバー*を選択します。
3. メンバータブのいずれかを選択します: ユーザー、サービス アカウント、または フェデレーション グループ。
4. *メンバー*ページで、テーブル内のメンバーに移動し、次に、[詳細を表示] を選択します。
5. 表で、メンバーに割り当てられたロールを変更する組織、フォルダ、またはプロジェクトのそれぞれの行を展開し、「ロール」列で「表示」を選択して、このメンバーに割り当てられているロールを表示します。
6. メンバーの既存の役割を変更したり、役割を削除したりできます。
   a. メンバーの役割を変更するには、変更したい役割の横にある「変更」を選択します。ロールを変更できるのは、同じロール カテゴリ内のロールのみです。たとえば、あるデータ サービス ロールから別のデータ サービス ロールに変更できます。変更を確認します。
   b. メンバーの役割の割り当てを解除するには、 をクリックすると、メンバーから該当するロールが削除されます。削除の確認を求められます。

### 組織からメンバーを削除する

メンバーが組織を離れる場合は、そのメンバーを削除します。

メンバーを削除すると、そのメンバーのコンソール権限は取り消されますが、コンソールとNetApp Support Siteのアカウントは保持されます。

連合メンバー

- フェデレーション ユーザーは、IdP から削除されると、自動的にNetApp Consoleにアクセスできなくなります。ただし、メンバーリストを最新の状態に保つには、コンソール組織からそれらのメンバーを削除する必要があります。
- IdP のフェデレーション グループからユーザーを削除すると、そのグループに関連付けられているコンソール アクセスが失われます。ただし、コンソールで明示的に割り当てられたロールに関連付けられたアクセス権は引き続き保持されます。

手順

1. *管理 > IDとアクセス*を選択します。
2. *メンバー*を選択します。
3. メンバータブのいずれかを選択します: ユーザー、サービス アカウント、または フェデレーション グループ。
4. メンバー*ページで、テーブル内のメンバーに移動し、 ••• 次に、[*ユーザーの削除]を選択します。
5. 組織からメンバーを削除することを確認します。

ユーザーセキュリティ

## メンバーのセキュリティ設定を管理して、 NetApp Console組織へのユーザー アクセスを保護します。ユーザー パスワードをリセットしたり、多要素認証 (MFA) を管理したり、サービス アカウントの認証情報を再作成したりできます。

必要なアクセスロール

スーパー管理者、組織管理者、またはフォルダーまたはプロジェクトの管理者（管理しているフォルダーとプロジェクトの場合）。リンク:reference-iam-predefined-roles.html[アクセス ロールについて学ぶ]

ユーザーパスワードをリセットする（ローカルユーザーのみ）

組織管理者はローカル ユーザーのユーザー パスワードをリセットできません。ただし、ユーザーに自分のパスワードをリセットするように指示することはできます。

コンソールのログイン ページで [パスワードを忘れた場合] を選択して、ユーザーにパスワードをリセットするよう指示します。

このオプションは、フェデレーション組織内のユーザーには使用できません。

ユーザーの多要素認証（**MFA**）を管理する

ユーザーが MFA デバイスにアクセスできなくなった場合は、MFA 構成を削除するか無効にすることができます。

多要素認証はローカル ユーザーのみが利用できます。フェデレーション ユーザーは MFA を有効にできません。

ユーザーは、削除後にログインするときに、MFA を再度設定する必要があります。ユーザーが一時的に MFA デバイスにアクセスできなくなった場合、保存した回復コードを使用してログインできます。

回復コードがない場合は、一時的に MFA を無効にしてログインを許可します。ユーザーの MFA を無効にすると、8 時間だけ無効になり、その後自動的に再度有効になります。その間、ユーザーは MFA なしで 1 回のログインが許可されます。8 時間経過後、ユーザーは MFA を使用してログインする必要があります。

ユーザーの多要素認証を管理するには、影響を受けるユーザーと同じドメインのメール アドレスが必要です。

手順

1. *管理 > IDとアクセス*を選択します。
2. *メンバー*を選択します。

   メンバー テーブルには組織のメンバーがリストされます。

3. メンバー*ページで、テーブル内のメンバーに移動し、次に、[*多要素認証の管理]を選択します。
4. ユーザーの MFA 構成を削除するか無効にするかを選択します。

サービス アカウントの認証情報を再作成する

サービスの資格情報を紛失した場合や更新する必要がある場合は、新しい資格情報を作成できます。

新しい資格情報を作成すると、古い資格情報は削除されます。古い資格情報は使用できません。

手順

1. *管理 > IDとアクセス*を選択します。
2. *メンバー*を選択します。
3. メンバー*テーブルでサービスアカウントに移動し、次に、[*シークレットの再作成]を選択します。
4. *再作成*を選択します。
5. クライアント ID とクライアント シークレットをダウンロードまたはコピーします。

   コンソールにはクライアント シークレットが 1 回だけ表示されます。必ずコピーまたはダウンロードして安全に保管してください。

## NetApp Consoleアクセスロール

### NetApp Consoleのアクセスロールについて学ぶ

NetApp Consoleの ID およびアクセス管理 (IAM) では、リソース階層のさまざまなレベルにわたって組織のメンバーに割り当てることができる定義済みのロールが提供されます。これらのロールを割り当てる前に、各ロールに含まれる権限を理解しておく必要があります。ロールは、プラットフォーム、アプリケーション、データ サービスというカテゴリに分類されます。

プラットフォームの役割

プラットフォーム ロールは、ロールの割り当てやユーザー管理などのNetApp Console管理権限を付与します。コンソールにはいくつかのプラットフォーム ロールがあります。

| プラットフォームの役割 | 責任 |
| --- | --- |
| "組織管理者" | ユーザーは、組織内のすべてのプロジェクトとフォルダに無制限にアクセスでき、任意のプロジェクトまたはフォルダにメンバーを追加できるほか、任意のタスクを実行したり、明示的にロールが関連付けられていない任意のデータ サービスを使用したりできます。このロールを持つユーザーは、適切な資格情報を持っている場合、フォルダーとプロジェクトの作成、ロールの割り当て、ユーザーの追加、システムの管理を行うことで組織を管理します。これは、コンソール エージェントを作成できる唯一のアクセス ロールです。 |
| "フォルダまたはプロジェクトの管理者" | 割り当てられたプロジェクトとフォルダーへのユーザーの無制限アクセスを許可します。管理するフォルダーまたはプロジェクトにメンバーを追加できるほか、割り当てられたフォルダーまたはプロジェクト内のリソースに対して任意のタスクを実行したり、任意のデータ サービスやアプリケーションを使用したりすることもできます。フォルダーまたはプロジェクト管理者はコンソール エージェントを作成できません。 |
| "連盟管理者" | ユーザーがコンソールを使用してフェデレーションを作成および管理し、シングル サインオン (SSO) を有効にすることを許可します。 |
| "連盟ビューア" | ユーザーがコンソールを使用して既存のフェデレーションを表示できるようにします。フェデレーションを作成または管理できません。 |
| "パートナーシップ管理者" | ユーザーがパートナーシップを作成および管理できるようにします。 |
| "パートナーシップビューアー" | ユーザーが既存のパートナーシップを表示できるようにします。パートナーシップを作成または管理することはできません。 |
| "スーパー管理者" | ユーザーに管理者ロールのサブセットを付与します。この役割は、コンソールの責任を複数のユーザーに分散する必要がない小規模な組織向けに設計されています。 |
| "スーパービューアー" | ユーザーにサブセット閲覧者ロールを付与します。この役割は、コンソールの責任を複数のユーザーに分散する必要がない小規模な組織向けに設計されています。 |

アプリケーションロール

以下は、アプリケーション カテゴリ内のロールの一覧です。各ロールは、指定された範囲内で特定の権限を付与します。必要なアプリケーションまたはプラットフォームのロールを持たないユーザーは、それぞれのアプリケーションにアクセスできません。

| アプリケーションロール | 責任 |
| --- | --- |
| "Google Cloud NetApp Volumes管理者" | Google Cloud NetApp Volumesロールを持つユーザーは、Google Cloud NetApp Volumes を検出して管理できます。 |
| "Google Cloud NetApp Volumes閲覧者" | Google Cloud NetApp Volumesユーザーロールを持つユーザーは、Google Cloud NetApp Volumes を表示できます。 |
| "Keystone管理者" | Keystone管理者ロールを持つユーザーは、サービス リクエストを作成できます。ユーザーがアクセスしているKeystoneテナント内の使用状況、リソース、および管理の詳細を監視および表示できるようにします。 |

| アプリケーションロール | 責任 |
| --- | --- |
| "Keystoneビューア" | Keystoneビューア ロールを持つユーザーは、サービス リクエストを作成できません。ユーザーがアクセスしているKeystoneテナント内の消費量、資産、管理情報を監視および表示できるようにします。 |
| ONTAPメディエーターのセットアップロール | ONTAP Mediator セットアップ ロールを持つサービス アカウントは、サービス リクエストを作成できます。このロールは、サービスアカウントでインスタンスを構成するために必要です。"ONTAPクラウドメディエーター" 。 |
| "オペレーションサポートアナリスト" | アラートおよび監視ツールへのアクセスと、サポートケースの入力および管理機能を提供します。 |
| "Storage Admin" | ストレージの健全性とガバナンス機能を管理し、ストレージ リソースを検出し、既存のシステムを変更および削除します。 |
| "ストレージビューア" | ストレージの健全性とガバナンス機能を表示し、以前に検出されたストレージ リソースも表示します。既存のストレージ システムを検出、変更、または削除することはできません。 |
| "システムヘルススペシャリスト" | ストレージとヘルスおよびガバナンス機能を管理します。ストレージ管理者のすべての権限がありますが、既存のシステムを変更または削除することはできません。 |

データサービスの役割

以下は、データ サービス カテゴリのロールの一覧です。各ロールは、指定された範囲内で特定の権限を付与します。必要なデータ サービス ロールまたはプラットフォーム ロールを持たないユーザーは、データ サービスにアクセスできません。

| データサービスの役割 | 責任 |
| --- | --- |
| "バックアップとリカバリのスーパー管理者" | NetApp Backup and Recoveryで任意のアクションを実行します。 |
| "バックアップとリカバリの管理者" | ローカル スナップショットへのバックアップ、セカンダリ ストレージへの複製、オブジェクト ストレージへのバックアップを実行します。 |
| "バックアップとリカバリの復元管理者" | バックアップとリカバリでワークロードを復元します。 |
| "バックアップとリカバリのクローン管理者" | バックアップとリカバリでアプリケーションとデータを複製します。 |
| "バックアップとリカバリビューア" | バックアップとリカバリの情報を表示します。 |
| "災害復旧管理者" | NetApp Disaster Recoveryサービスで任意のアクションを実行します。 |
| "災害復旧フェイルオーバー管理者" | フェイルオーバーと移行を実行します。 |
| "災害復旧アプリケーション管理者" | レプリケーション プランを作成し、レプリケーション プランを変更し、テスト フェイルオーバーを開始します。 |
| "災害復旧ビューア" | 情報の表示のみ。 |

| データサービスの役割 | 責任 |
| --- | --- |
| 分類ビューア | ユーザーがNetApp Data Classificationスキャン結果を表示できるようにします。このロールを持つユーザーは、コンプライアンス情報を表示し、アクセス権限を持つリソースのレポートを生成できます。これらのユーザーは、ボリューム、バケット、またはデータベース スキーマのスキャンを有効または無効にすることはできません。分類には管理者の役割がありません。 |
| "ランサムウェア耐性管理者" | NetApp Ransomware Resilienceの「保護」、「アラート」、「回復」、「設定」、「レポート」タブでアクションを管理します。 |
| "ランサムウェア耐性ビューア" | ランサムウェア耐性で、ワークロード データを表示し、アラート データを表示し、回復データをダウンロードし、レポートをダウンロードします。 |
| "ランサムウェア耐性ユーザー行動管理者" | Ransomware Resilience で、疑わしいユーザー行動の検出、アラート、監視を構成、管理、表示します。 |
| "ランサムウェア耐性ユーザー行動ビューア" | ランサムウェア耐性で疑わしいユーザー行動のアラートと分析情報を表示します。 |
| SnapCenter管理者 | NetApp Backup and Recovery for Applications を使用してオンプレミスのONTAPクラスターからスナップショットをバックアップする機能を提供します。このロールを持つメンバーは、次のアクションを実行できます。 * [バックアップとリカバリ] > [アプリケーション] から任意のアクションを実行する * 権限を持つプロジェクトおよびフォルダ内のすべてのシステムを管理する * すべてのNetApp ConsoleサービスをSnapCenterには、閲覧者ロールはありません。 |

関連リンク

- "NetApp Consoleのアイデンティティとアクセス管理について学ぶ"
- "NetApp ConsoleIAMを使い始める"
- "NetApp Consoleのメンバーとその権限を管理する"
- "NetApp ConsoleIAMのAPIについて学ぶ"

**NetApp Console**プラットフォームアクセスロール

## ユーザーにプラットフォーム ロールを割り当てて、 NetApp Consoleの管理、ロールの割り当て、ユーザーの追加、コンソール エージェントの作成、フェデレーションの管理を行う権限を付与します。

大規模な多国籍組織の組織役割の例

XYZ 社は、北米、ヨーロッパ、アジア太平洋の地域別にデータ ストレージ アクセスを整理し、集中管理による地域制御を実現しています。

XYZ 社のコンソールの 組織管理者 は、初期組織と各リージョンの個別のフォルダーを作成します。各リージョンの*フォルダーまたはプロジェクト管理者*は、リージョンのフォルダー内のプロジェクト (および関連するリソース) を整理します。

フォルダーまたはプロジェクト管理者 の役割を持つ地域管理者は、リソースとユーザーを追加することでフォルダーを積極的に管理します。これらの地域管理者は、管理するフォルダやプロジェクトを追加、削除、または名前変更することもできます。組織管理者 は新しいリソースの権限を継承し、組織全体のストレージ使用状況の可視性を維持します。

同じ組織内で、1 人のユーザーに フェデレーション管理者 ロールが割り当てられ、組織の企業 IdP とのフェデレーションを管理します。このユーザーはフェデレーション組織を追加または削除できますが、組織内のユーザーまたはリソースを管理することはできません。組織管理者 は、フェデレーション ステータスを確認し、フェデレーション組織を表示するための フェデレーション ビューアー ロールをユーザーに割り当てます。

次の表は、各コンソール プラットフォーム ロールが実行できるアクションを示しています。

組織管理の役割

| Task | 組織管理者 | フォルダまたはプロジェクトの管理者 |
|---|---|---|
| エージェントを作成する | はい | いいえ |
| コンソールからシステムを作成、変更、または削除する（システムの追加または検出） | はい | はい |
| フォルダとプロジェクトの作成（削除を含む） | はい | いいえ |
| 既存のフォルダとプロジェクトの名前を変更する | はい | はい |
| 役割を割り当ててユーザーを追加する | はい | はい |
| リソースをフォルダとプロジェクトに関連付ける | はい | はい |
| エージェントをフォルダとプロジェクトに関連付ける | はい | いいえ |
| フォルダとプロジェクトからエージェントを削除する | はい | いいえ |
| エージェントの管理（証明書、設定などの編集） | はい | いいえ |
| 管理 > 資格情報から資格情報を管理する | はい | はい |
| フェデレーションの作成、管理、表示 | はい | いいえ |
| コンソールからサポートに登録し、ケースを送信します | はい | はい |
| 明示的なアクセス ロールに関連付けられていないデータ サービスを使用する | はい | はい |
| 監査ページと通知を表示する | はい | はい |

連盟の役割

| Task | 連盟管理者 | 連盟ビューア |
|---|---|---|
| 連盟を作成する | はい | いいえ |
| ドメインを確認する | はい | いいえ |
| フェデレーションにドメインを追加する | はい | いいえ |
| フェデレーションを無効化および削除する | はい | いいえ |
| テスト連盟 | はい | いいえ |
| 連盟とその詳細を表示する | はい | はい |

パートナーシップの役割

| Task | パートナーシップ管理者 | パートナーシップビューアー |
|---|---|---|
| パートナーシップを構築できる | はい | いいえ |
| パートナーメンバーに役割を割り当てる | はい | いいえ |
| パートナーシップにメンバーを追加できます | はい | いいえ |
| 組織のパートナーシップの詳細を表示できます | はい | はい |

スーパー管理者と閲覧者の役割

スーパー管理者 ロールには、コンソールの機能、ストレージ、およびデータ サービスを管理するための完全なアクセス権が付与されます。この役割は、管理とガバナンスを監督する人に適しています。対照的に、スーパー ビューアー ロールは読み取り専用アクセスを提供するため、変更を加えずに可視性を必要とする監査人や関係者に最適です。

組織は、セキュリティ リスクを最小限に抑え、最小権限の原則に従うために、スーパー管理者 アクセスを控えめに使用する必要があります。ほとんどの組織では、リスクを軽減し、監査可能性を向上させるために、必要な権限のみを持つきめ細かいロールを割り当てる必要があります。

スーパーロールの例

ABC コーポレーションには、データ サービスとストレージ管理にNetApp Consoleを活用する 5 人の小規模なチームがあります。複数の役割を配分する代わりに、ユーザー管理やリソース構成などのすべての管理タスクを担当する 2 人の上級チーム メンバーに スーパー管理者 の役割を割り当てます。残りの 3 人のチーム メンバーには スーパー ビューアー ロールが割り当てられており、設定を変更する権限なしで、ストレージの健全性とデータ サービスの状態を監視できます。

| ロール | 継承された役割 |
|---|---|
| スーパー管理者 | • 組織管理者<br>• フォルダまたはプロジェクトの管理者<br>• 連盟管理者<br>• パートナーシップ管理者<br>• ランサムウェア耐性管理者<br>• 災害復旧管理者<br>• バックアップスーパー管理者<br>• Storage Admin<br>• Keystone管理者<br>• Google Cloud NetApp Volumes 管理者 |

| ロール | 継承された役割 |
| --- | --- |
| スーパービューアー | • 組織閲覧者<br>• 連盟ビューア<br>• パートナーシップビューアー<br>• ランサムウェア耐性ビューア<br>• 災害復旧ビューア<br>• バックアップビューア<br>• ストレージビューア<br>• Keystoneビューア<br>• Google Cloud NetApp Volumes 閲覧者 |

アプリケーションロール

#### NetApp ConsoleのGoogle Cloud NetApp Volumesロール

ユーザーに次のロールを割り当てて、 NetApp ConsoleでGoogle Cloud NetApp Volumes にアクセスできるようにすることができます。

Google Cloud NetApp Volumes は次のロールを使用します。

- * Google Cloud NetApp Volumes管理者*: コンソールでGoogle Cloud NetApp Volumes を検出し、管理します。
- * Google Cloud NetApp Volumes閲覧者*: コンソールでGoogle Cloud NetApp Volumesを表示します。

#### NetApp ConsoleのKeystoneアクセス ロール

Keystoneロールは、 Keystoneダッシュボードへのアクセスを提供し、ユーザーがKeystoneサブスクリプションを表示および管理できるようにします。 Keystone の役割には、 Keystone管理者とKeystoneビューアーの 2 つがあります。 2 つのロールの主な違いは、 Keystoneで実行できるアクションです。 Keystone管理者ロールは、サービス リクエストの作成やサブスクリプションの変更が許可される唯一のロールです。

#### NetApp ConsoleのKeystoneロールの例

XYZ 社には、 Keystoneサブスクリプション情報を閲覧できる、さまざまな部門のストレージ エンジニアが 4 人います。これらのユーザー全員がKeystoneサブスクリプションを監視する必要がありますが、サービス リクエストを作成できるのはチーム リーダーのみです。チーム メンバーのうち 3 名に * Keystoneビューア* ロールが付与され、チーム リーダーには * Keystone管理者* ロールが付与されるため、会社のサービス リクエストを制御できるようになります。

次の表は、各Keystoneロールが実行できるアクションを示しています。

| 特徴とアクション | **Keystone**管理者 | **Keystone**ビューア |
| --- | --- | --- |
| 次のタブを表示します: サブスクリプション、資産、モニター、管理 | はい | はい |
| * Keystoneサブスクリプションページ*: | | |
| サブスクリプションを表示 | はい | はい |
| サブスクリプションの修正または更新 | はい | いいえ |
| * Keystoneアセット ページ*: | | |
| アセットを表示 | はい | はい |
| 資産管理 | はい | いいえ |
| * Keystoneアラートページ*: | | |
| アラートを表示 | はい | はい |
| アラートを管理する | はい | いいえ |
| 自分用のアラートを作成する | はい | はい |
| **Licenses and subscriptions**: | | |
| ライセンスとサブスクリプションを表示できます | はい | はい |
| * Keystoneレポートページ*: | | |
| レポートをダウンロード | はい | はい |
| レポートを管理する | はい | はい |
| 自分用のレポートを作成する | はい | はい |
| サービスリクエスト: | | |
| サービスリクエストを作成する | はい | いいえ |
| 組織内の任意のユーザーが作成したサービスリクエストを表示する | はい | はい |

**NetApp Console**の運用サポートアナリスト アクセス ロール

ユーザーに運用サポートアナリストの役割を割り当てて、アラートと監視へのアクセスを許可することができます。この役割を持つユーザーはサポートケースを開くこともできます。

運用サポートアナリスト

| Task | 実行できる |
| --- | --- |
| 設定 > 資格情報から自分のユーザー資格情報を管理します | はい |
| 発見されたリソースを表示する | はい |
| コンソールからサポートに登録し、ケースを送信します | はい |
| 監査ページと通知を表示する | はい |
| アラートの表示、ダウンロード、設定 | はい |

**NetApp Console**のストレージアクセスロール

ユーザーに次のロールを割り当てて、 NetApp Consoleのストレージ管理機能へのアクセスを許可できます。ユーザーに、ストレージを管理するための管理者ロールまたは監視するための閲覧者ロールを割り当てることができます。

これらのロールは、NetApp Consoleパートナーシップ API からは使用できません。

管理者は、次のストレージ リソースと機能についてユーザーにストレージ ロールを割り当てることができます。

ストレージ リソース:

- オンプレミスのONTAPクラスタ
- StorageGRID
- Eシリーズ

コンソールのサービスと機能:

- デジタルアドバイザー
- ソフトウェアアップデート
- ライフサイクルプランニング
- 持続可能性

**NetApp Console**のストレージロールの例

多国籍企業である XYZ 社には、大規模なストレージ エンジニアとストレージ管理者のチームが存在します。これにより、このチームは、ユーザー管理、エージェントの作成、ライセンス管理などのコアコンソールタスクへのアクセスを制限しながら、担当リージョンのストレージ資産を管理できるようになります。

12 人のチーム内で、2 人のユーザーに ストレージ閲覧者 ロールが付与され、割り当てられたコンソール プロジェクトに関連付けられたストレージ リソースを監視できるようになります。残りの 9 人には、ソフトウェア更新の管理、コンソール経由のONTAP System Manager へのアクセス、ストレージ リソースの検出 (システムの追加) などの機能を含む **Storage admin** ロールが付与されます。チームの 1 人に システム ヘルス スペシャリスト の役割が付与され、担当リージョン内のストレージ リソースのヘルスを管理できるようになりま

すが、システムを変更または削除することはできません。このユーザーは、割り当てられたプロジェクトのストレージ リソースに対してソフトウェア更新を実行することもできます。

組織には、ユーザー管理、エージェント作成、ライセンス管理など、コンソールのあらゆる側面を管理できる組織管理者 ロールを持つ 2 人の追加ユーザーと、割り当てられているフォルダーとプロジェクトのコンソール管理タスクを実行できる フォルダーまたはプロジェクト管理者 ロールを持つ複数のユーザーがいます。

次の表は、各ストレージ ロールが実行するアクションを示しています。

| 特徴とアクション | **Storage Admin** | システムヘルススペシャリスト | ストレージビューア |
|---|---|---|---|
| ストレージ管理: | | | |
| 新しいリソースを発見する（システムを作成する） | はい | はい | いいえ |
| 検出されたシステムを表示 | はい | はい | いいえ |
| コンソールからシステムを削除する | はい | いいえ | いいえ |
| システムを変更する | はい | いいえ | いいえ |
| エージェントを作成する | いいえ | いいえ | いいえ |
| デジタルアドバイザー | | | |
| すべてのページと機能を表示 | はい | はい | はい |
| **Licenses and subscriptions** | | | |
| すべてのページと機能を表示 | いいえ | いいえ | いいえ |
| ソフトウェアアップデート | | | |
| ランディングページと推奨事項を表示 | はい | はい | はい |
| 潜在的なバージョンの推奨事項と主な利点を確認する | はい | はい | はい |
| クラスターの更新の詳細を表示する | はい | はい | はい |
| 更新前のチェックを実行し、アップグレードプランをダウンロードする | はい | はい | はい |
| ソフトウェアアップデートをインストールする | はい | はい | いいえ |
| ライフサイクルプランニング | | | |
| キャパシティプランニングの状況を確認する | はい | はい | はい |

| 特徴とアクション | **Storage Admin** | システムヘルススペシャリスト | ストレージビューア |
|---|---|---|---|
| 次のアクションを選択する（ベストプラクティス、階層） | はい | いいえ | いいえ |
| コールドデータをクラウドストレージに階層化してストレージを解放する | はい | はい | いいえ |
| リマインダーを設定する | はい | はい | はい |
| 持続可能性 | | | |
| ダッシュボードと推奨事項を表示する | はい | はい | はい |
| レポートデータをダウンロード | はい | はい | はい |
| 炭素削減率を編集 | はい | はい | いいえ |
| 修正の推奨事項 | はい | はい | いいえ |
| 推奨を延期する | はい | はい | いいえ |
| システム管理者アクセス | | | |
| 資格情報を入力できます | はい | はい | いいえ |
| 資格 | | | |
| ユーザ クレデンシャル | はい | はい | いいえ |

データサービスの役割

#### NetApp ConsoleのNetApp Backup and Recoveryの役割

コンソール内でNetApp Backup and Recoveryにアクセスできるように、ユーザーに次のロールを割り当てることができます。バックアップとリカバリのロールにより、組織内でユーザーが実行する必要があるタスクに固有のロールを柔軟に割り当てることができます。ロールの割り当て方法は、独自のビジネスおよびストレージ管理の実践によって異なります。

このサービスは、NetApp Backup and Recoveryに固有の次のロールを使用します。

- バックアップおよびリカバリ スーパー管理者: NetApp Backup and Recoveryであらゆるアクションを実行します。
- バックアップとリカバリ バックアップ管理者: NetApp Backup and Recoveryで、ローカル スナップショットへのバックアップ、セカンダリ ストレージへの複製、オブジェクト ストレージへのバックアップ アクションを実行します。
- バックアップおよびリカバリの復元管理者: NetApp Backup and Recoveryを使用してワークロードを復元

します。

- バックアップおよびリカバリ クローン管理者: NetApp Backup and Recoveryを使用してアプリケーションとデータをクローンします。
- バックアップおよびリカバリ ビューア: NetApp Backup and Recoveryの情報を表示しますが、アクションは実行しません。

NetApp Consoleのアクセスロールの詳細については、 "コンソールのセットアップと管理に関するドキュメント" 。

一般的なアクションに使用されるロール

次の表は、すべてのワークロードに対して各NetApp Backup and Recoveryロールが実行できるアクションを示しています。

| 特徴とアクション | バックアップとリカバリのスーパー管理者 | バックアップとリカバリのバックアップ管理者 | バックアップとリカバリの復元管理者 | バックアップとリカバリのクローン管理者 | バックアップとリカバリビューア |
|---|---|---|---|---|---|
| ホストを追加、編集、または削除する | はい | いいえ | いいえ | いいえ | いいえ |
| プラグインをインストールする | はい | いいえ | いいえ | いいえ | いいえ |
| 資格情報を追加する（ホスト、インスタンス、vCenter） | はい | いいえ | いいえ | いいえ | いいえ |
| ダッシュボードとすべてのタブを表示 | はい | はい | はい | はい | はい |
| 無料トライアルを始める | はい | いいえ | いいえ | いいえ | いいえ |
| ワークロードの検出を開始する | いいえ | はい | はい | はい | いいえ |
| ライセンス情報を表示 | はい | はい | はい | はい | はい |
| ライセンスを有効化 | はい | いいえ | いいえ | いいえ | いいえ |
| ホストを表示 | はい | はい | はい | はい | はい |
| スケジュール: | | | | | |
| スケジュールをアクティブ化 | はい | はい | はい | はい | いいえ |
| スケジュールを中断 | はい | はい | はい | はい | いいえ |
| ポリシーと保護: | | | | | |
| 保護プランを見る | はい | はい | はい | はい | はい |

| 特徴とアクション | バックアップとリカバリのスーパー管理者 | バックアップとリカバリのバックアップ管理者 | バックアップとリカバリの復元管理者 | バックアップとリカバリのクローン管理者 | バックアップとリカバリビューア |
|---|---|---|---|---|---|
| 保護プランを作成、変更、または削除する | はい | はい | いいえ | いいえ | いいえ |
| ワークロードを復元する | はい | いいえ | はい | いいえ | いいえ |
| クローンを作成、分割、または削除する | はい | いいえ | いいえ | はい | いいえ |
| ポリシーの作成、変更、または削除 | はい | はい | いいえ | いいえ | いいえ |
| レポート: | | | | | |
| レポートを表示 | はい | はい | はい | はい | はい |
| レポートを作成する | はい | はい | はい | はい | いいえ |
| レポートを削除する | はい | いいえ | いいえ | いいえ | いいえ |
| * SnapCenterからインポートしてホストを管理する*: | | | | | |
| インポートされたSnapCenterデータを表示する | はい | はい | はい | はい | はい |
| SnapCenterからデータをインポートする | はい | はい | いいえ | いいえ | いいえ |
| ホストの管理（移行） | はい | はい | いいえ | いいえ | いいえ |
| 設定を構成する: | | | | | |
| ログ ディレクトリを設定 | はい | はい | はい | いいえ | いいえ |
| インスタンス資格情報の関連付けまたは削除 | はい | はい | はい | いいえ | いいえ |
| バケツ: | | | | | |
| バケットを表示 | はい | はい | はい | はい | はい |
| バケットを作成、編集、または削除する | はい | はい | いいえ | いいえ | いいえ |

ワークロード固有のアクションに使用されるロール

次の表は、各NetApp Backup and Recoveryロールが特定のワークロードに対して実行できるアクションを示しています。

**Kubernetes** ワークロード

この表は、Kubernetes ワークロードに固有のアクションに対して各NetApp Backup and Recoveryロールが実行できるアクションを示しています。

| 特徴とアクション | バックアップとリカバリのスーパー管理者 | バックアップとリカバリのバックアップ管理者 | バックアップとリカバリの復元管理者 | バックアップとリカバリビューア |
|---|---|---|---|---|
| クラスター、名前空間、ストレージ クラス、API リソースを表示する | はい | はい | はい | はい |
| 新しいKubernetesクラスターを追加する | はい | はい | いいえ | いいえ |
| クラスタ構成を更新する | はい | いいえ | いいえ | いいえ |
| 管理からクラスタを削除する | はい | いいえ | いいえ | いいえ |
| アプリケーションを表示する | はい | はい | はい | はい |
| 新しいアプリケーションの作成と定義 | はい | はい | いいえ | いいえ |
| アプリケーション構成を更新する | はい | はい | いいえ | いいえ |
| 管理からアプリケーションを削除する | はい | はい | いいえ | いいえ |
| 保護されたリソースとバックアップステータスを表示する | はい | はい | はい | はい |
| バックアップを作成し、ポリシーでアプリケーションを保護する | はい | はい | いいえ | いいえ |
| アプリの保護を解除し、バックアップを削除する | はい | はい | いいえ | いいえ |
| リカバリポイントとリソースビューアの結果を表示する | はい | はい | はい | はい |
| リカバリポイントからアプリケーションを復元する | はい | いいえ | はい | いいえ |
| Kubernetes バックアップ ポリシーを表示する | はい | はい | はい | はい |
| Kubernetes バックアップ ポリシーを作成する | はい | はい | はい | いいえ |
| バックアップポリシーを更新する | はい | はい | はい | いいえ |

| 特徴とアクション | バックアップとリカバリのスーパー管理者 | バックアップとリカバリのバックアップ管理者 | バックアップとリカバリの復元管理者 | バックアップとリカバリビューア |
|---|---|---|---|---|
| バックアップポリシーを削除する | はい | はい | はい | いいえ |
| 実行フックとフックソースを表示する | はい | はい | はい | はい |
| 実行フックとフックソースを作成する | はい | はい | はい | いいえ |
| 実行フックとフックソースを更新する | はい | はい | はい | いいえ |
| 実行フックとフックソースを削除する | はい | はい | はい | いいえ |
| 実行フックテンプレートを表示する | はい | はい | はい | はい |
| 実行フックテンプレートを作成する | はい | はい | はい | いいえ |
| 実行フックテンプレートを更新する | はい | はい | はい | いいえ |
| 実行フックテンプレートを削除する | はい | はい | はい | いいえ |
| ワークロードの概要と分析ダッシュボードを表示する | はい | はい | はい | はい |
| StorageGRIDバケットとストレージターゲットを表示する | はい | はい | はい | はい |

**NetApp Console**の**NetApp Disaster Recovery**ロール

コンソール内でNetApp Disaster Recoveryにアクセスできるように、ユーザーに次のロールを割り当てることができます。災害復旧ロールを使用すると、組織内でユーザーが実行する必要があるタスクに固有のロールを柔軟に割り当てることができます。ロールの割り当て方法は、独自のビジネスおよびストレージ管理の実践によって異なります。

災害復旧では次のロールが使用されます。

- 災害復旧管理者: あらゆるアクションを実行します。
- 災害復旧フェールオーバー管理者: フェールオーバーと移行を実行します。
- 災害復旧アプリケーション管理者: レプリケーション プランを作成します。レプリケーション プランを変更します。テストフェイルオーバーを開始します。
- 災害復旧ビューアー: 情報の表示のみ。

次の表は、各ロールが実行できるアクションを示しています。

| 特徴とアクション | 災害復旧管理者 | 災害復旧フェイルオーバー管理者 | 災害復旧アプリケーション管理者 | 災害復旧ビューア |
|---|---|---|---|---|
| ダッシュボードとすべてのタブを表示 | はい | はい | はい | はい |
| 無料トライアルを始める | はい | いいえ | いいえ | いいえ |
| ワークロードの検出を開始する | はい | いいえ | いいえ | いいえ |
| ライセンス情報を表示 | はい | はい | はい | はい |
| ライセンスを有効化 | はい | いいえ | はい | いいえ |
| サイトタブ: | | | | |
| サイトを表示 | はい | はい | はい | はい |
| サイトの追加、変更、削除 | はい | いいえ | いいえ | いいえ |
| レプリケーション プラン タブで: | | | | |
| レプリケーションプランの表示 | はい | はい | はい | はい |
| レプリケーションプランの詳細を表示する | はい | はい | はい | はい |
| レプリケーションプランを作成または変更する | はい | はい | はい | いいえ |
| レポートを作成する | はい | いいえ | いいえ | いいえ |
| スナップショットを表示 | はい | はい | はい | はい |
| フェイルオーバーテストを実行する | はい | はい | はい | いいえ |
| フェイルオーバーを実行する | はい | はい | いいえ | いいえ |
| フェイルバックを実行する | はい | はい | いいえ | いいえ |
| 移行を実行する | はい | はい | いいえ | いいえ |
| リソース グループ タブで: | | | | |
| リソース グループを表示する | はい | はい | はい | はい |
| リソース グループの作成、変更、または削除 | はい | いいえ | はい | いいえ |
| ジョブ監視タブで: | | | | |

| 特徴とアクション | 災害復旧管理者 | 災害復旧フェイルオーバー管理者 | 災害復旧アプリケーション管理者 | 災害復旧ビューア |
|---|---|---|---|---|
| ジョブの表示 | はい | いいえ | はい | はい |
| ジョブをキャンセルする | はい | はい | はい | いいえ |

**NetApp Console**のランサムウェア耐性アクセス ロール

ランサムウェア レジリエンス ロールは、ユーザーにNetApp Ransomware Resilienceへのアクセスを提供します。ランサムウェア耐性は次の役割をサポートします。

ベースラインロール

- ランサムウェア耐性管理者 - ランサムウェア耐性設定を構成し、暗号化アラートを調査して対応します
- ランサムウェア耐性ビューア - 暗号化インシデント、レポート、検出設定を表示

ユーザー行動アクティビティの役割"不審なユーザーアクティビティの検出"アラートは、ファイル アクティビティ イベントなどのデータの可視性を提供します。これらのアラートには、ファイル名と、ユーザーが実行したファイル アクション (読み取り、書き込み、削除、名前の変更など) が含まれます。このデータの可視性を制限するために、これらのロールを持つユーザーのみがこれらのアラートを管理または表示できます。

- ランサムウェア耐性ユーザー行動管理者 - 疑わしいユーザーアクティビティの検出を有効にし、疑わしいユーザーアクティビティのアラートを調査して対応します
- ランサムウェア耐性ユーザー行動ビューア - 疑わしいユーザーアクティビティアラートを表示

ユーザー ビヘイビア ロールはスタンドアロン ロールではなく、ランサムウェア レジリエンス管理者ロールまたは閲覧者ロールに追加されるように設計されています。詳細については、 [ユーザーの行動の役割]。

各ロールの詳細な説明については、次の表を参照してください。

ベースラインロール

次の表は、ランサムウェア耐性管理者および閲覧者ロールで使用できるアクションを示しています。

| 特徴とアクション | ランサムウェア耐性管理者 | ランサムウェア耐性ビューア |
|---|---|---|
| ダッシュボードとすべてのタブを表示 | はい | はい |
| ダッシュボードで推奨事項のステータスを更新する | はい | いいえ |
| 無料トライアルを始める | はい | いいえ |
| ワークロードの検出を開始する | はい | いいえ |

| 特徴とアクション | ランサムウェア耐性管理者 | ランサムウェア耐性ビューア |
| --- | --- | --- |
| ワークロードの再検出を開始する | はい | いいえ |
| [保護]タブで: | | |
| 暗号化ポリシーの保護プランを追加、変更、または削除する | はい | いいえ |
| ワークロードを保護する | はい | いいえ |
| データ分類で機密データへの露出を特定 | はい | いいえ |
| 保護プランと詳細を一覧表示する | はい | はい |
| 保護グループの一覧 | はい | はい |
| 保護グループの詳細を表示する | はい | はい |
| 保護グループの作成、編集、または削除 | はい | いいえ |
| データをダウンロード | はい | はい |
| アラートタブ: | | |
| 暗号化アラートとアラートの詳細を表示する | はい | はい |
| 暗号化インシデントステータスの編集 | はい | いいえ |
| 回復のために暗号化アラートをマークする | はい | いいえ |
| 暗号化インシデントの詳細を表示 | はい | はい |
| 暗号化インシデントを無視または解決する | はい | いいえ |
| 暗号化イベントで影響を受けるファイルの完全なリストを取得します | はい | いいえ |
| 暗号化イベントアラートデータをダウンロードする | はい | はい |
| ユーザーをブロックする（Workload Securityエージェント構成を使用） | はい | いいえ |
| [回復]タブで: | | |
| 暗号化イベントから影響を受けるファイルをダウンロードする | はい | いいえ |

| 特徴とアクション | ランサムウェア耐性管理者 | ランサムウェア耐性ビューア |
| --- | --- | --- |
| 暗号化イベントからのワークロードの復元 | はい | いいえ |
| 暗号化イベントから回復データをダウンロードする | はい | はい |
| 暗号化イベントからのレポートをダウンロード | はい | はい |
| 設定タブで: | | |
| バックアップ先を追加または変更する | はい | いいえ |
| バックアップ先の一覧 | はい | はい |
| 接続されたSIEMターゲットを表示する | はい | はい |
| SIEMターゲットの追加または変更 | はい | いいえ |
| 準備訓練を構成する | はい | いいえ |
| 準備訓練を開始、リセット、または編集する | はい | いいえ |
| 準備訓練の状況を確認する | はい | はい |
| 検出構成の更新 | はい | いいえ |
| 検出構成の表示 | はい | はい |
| レポートタブ: | | |
| レポートをダウンロード | はい | はい |

ユーザーの行動の役割

疑わしいユーザーの行動設定を構成し、アラートに応答するには、ユーザーは Ransomware Resilience ユーザー行動管理者ロールを持っている必要があります。疑わしいユーザー行動アラートのみを表示するには、ユーザーは Ransomware Resilience ユーザー行動閲覧者ロールを持っている必要があります。

ランサムウェア耐性の管理者または閲覧者権限を持つユーザーで、アクセスが必要なユーザーには、ユーザー行動ロールを付与する必要があります。"不審なユーザーアクティビティの設定とアラート" 。たとえば、ランサムウェア耐性管理者ロールを持つユーザーには、ユーザー アクティビティ エージェントを構成し、ユーザーをブロックまたはブロック解除するための、ランサムウェア耐性ユーザー動作管理者ロールが付与される必要があります。ランサムウェア耐性ユーザー動作管理者ロールは、ランサムウェア耐性ビューアに付与しないでください。

不審なユーザー アクティビティの検出を有効にするには、コンソール組織管理者のロールが必要です。

次の表は、ランサムウェア耐性ユーザー動作の管理者および閲覧者ロールで使用できるアクションを示しています。

| 特徴とアクション | ランサムウェア耐性ユーザー行動管理者 | ランサムウェア耐性ユーザー行動ビューア |
|---|---|---|
| 設定タブで: | | |
| ユーザーアクティビティエージェントの作成、変更、または削除 | はい | いいえ |
| ユーザーディレクトリコネクタの作成または削除 | はい | いいえ |
| データコレクターを一時停止または再開する | はい | いいえ |
| データ侵害対策訓練を実施する | はい | いいえ |
| [保護]タブで: | | |
| _疑わしいユーザー行動_ポリシーの保護プランを追加、変更、または削除する | はい | いいえ |
| アラートタブ: | | |
| ユーザーアクティビティアラートとアラートの詳細を表示する | はい | はい |
| ユーザーアクティビティインシデントステータスの編集 | はい | いいえ |
| 回復のためにユーザーアクティビティアラートをマークする | はい | いいえ |
| ユーザーアクティビティインシデントの詳細を表示する | はい | はい |
| ユーザーアクティビティインシデントを無視または解決する | はい | いいえ |
| 疑わしいユーザーによる影響を受けたファイルの完全なリストを取得する | はい | はい |
| ユーザーアクティビティイベントアラートデータをダウンロードする | はい | はい |
| ユーザーをブロックまたはブロック解除する | はい | いいえ |
| [回復]タブで: | | |
| ユーザーアクティビティイベントの影響を受けるファイルをダウンロードする | はい | いいえ |
| ユーザーアクティビティイベントからワークロードを復元する | はい | いいえ |

| 特徴とアクション | ランサムウェア耐性ユーザー行動管理者 | ランサムウェア耐性ユーザー行動ビューア |
| --- | --- | --- |
| ユーザーアクティビティイベントから回復データをダウンロードする | はい | はい |
| ユーザーアクティビティイベントからレポートをダウンロードする | はい | はい |

# アイデンティティとアクセスAPI

## 組織IDとプロジェクトID

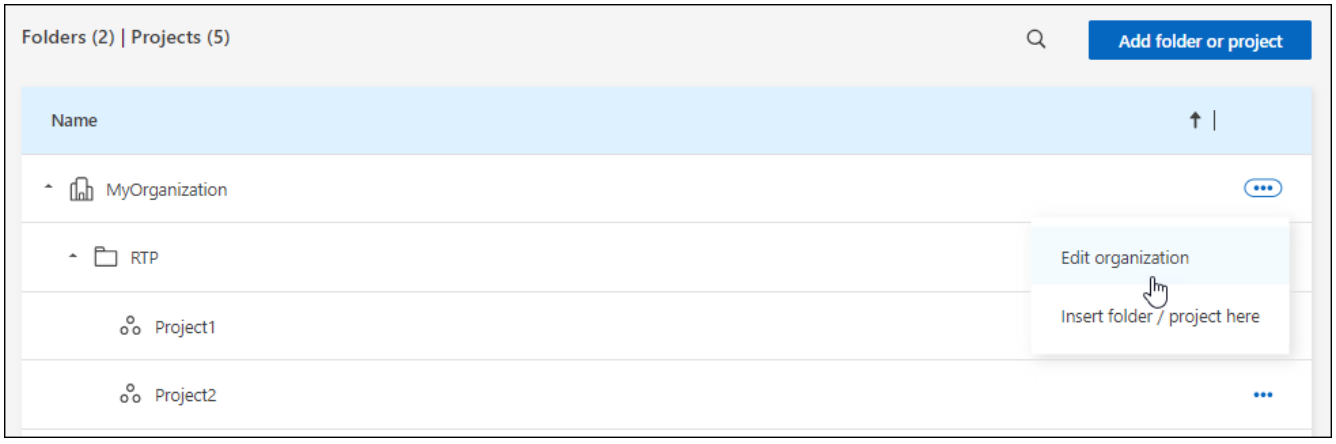
NetApp Console組織には名前と ID があります。組織を識別しやすいように、組織の名前を選択できます。特定の統合では組織 ID を取得する必要がある場合もあります。

### 組織名を変更する

組織の名前を変更できます。複数の組織をサポートする場合に役立ちます。

手順

1. *管理 > IDとアクセス*を選択します。
2. *組織*を選択します。
3. *組織*ページで、表の最初の行に移動し、次に、[組織の編集] を選択します。




4. 新しい組織名を入力し、「適用」を選択します。

### 組織IDを取得する

組織 ID は、コンソールとの特定の統合に使用されます。

組織ページから組織 ID を表示し、必要に応じてクリップボードにコピーすることができます。

手順

1. 管理 **> ID** とアクセス > 組織 を選択します。
2. 組織 ページの概要バーで組織 ID を探し、クリップボードにコピーします。これを後で使用するために保存することも、必要な場所に直接コピーすることもできます。

プロジェクトのIDを取得する

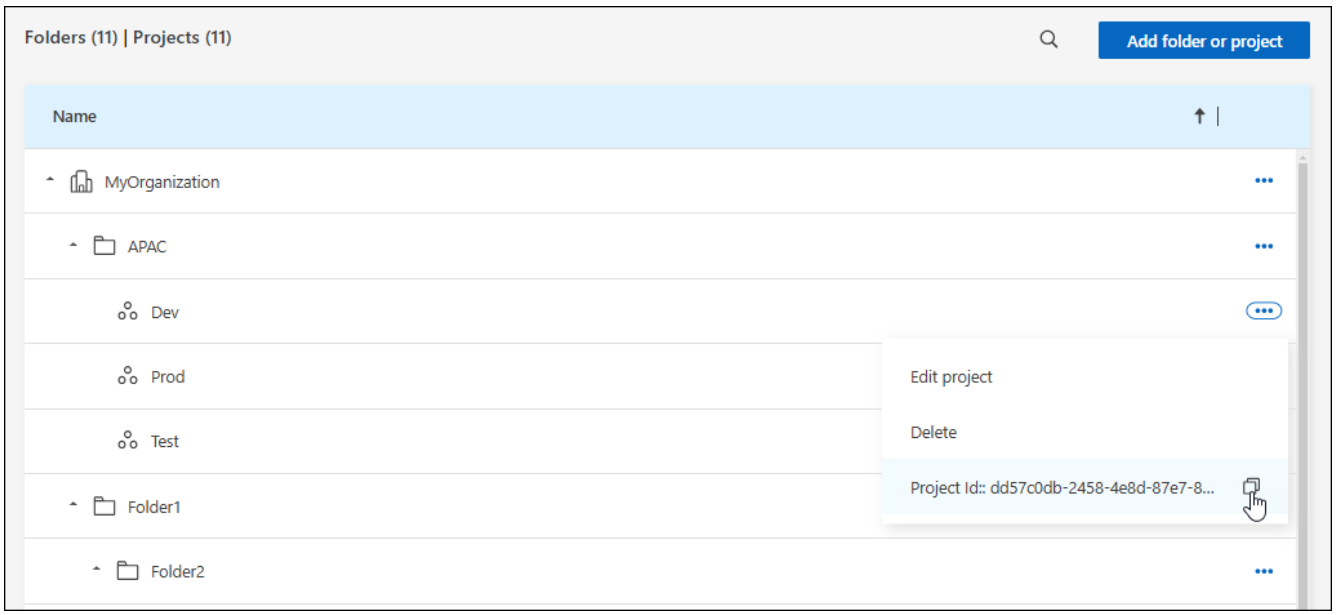
API を使用している場合は、プロジェクトの ID を取得する必要があります。たとえば、 Cloud Volumes ONTAPシステムを作成する場合などです。

手順

1. *組織*ページで、表内のプロジェクトに移動し、 •••

   プロジェクト ID が表示されます。

2. ID をコピーするには、コピー ボタンを選択します。




関連情報

- "アイデンティティとアクセス管理について学ぶ"
- "アイデンティティとアクセスを始める"
- "IDとアクセスのためのAPIについて学ぶ"

# セキュリティとコンプライアンス

## アイデンティティ連携

**NetApp Console**で**ID**フェデレーションを使用してシングルサインオンを有効にする

シングル サインオン (フェデレーション) により、ユーザーは企業の認証情報を使用してNetApp Consoleにログインできるため、ログイン プロセスが簡素化され、セキュリティが強化されます。アイデンティティ プロバイダー (IdP) またはNetAppサポート サイトを使用してシングル サインオン (SSO) を有効にできます。

必要な役割

組織管理者、フェデレーション管理者、フェデレーション閲覧者。"アクセス ロールの詳細について説明しま

す。"

#### NetApp Support Site でのシングルサインオン

NetAppサポート サイトと連携すると、ユーザーは同じ資格情報を使用してコンソール、 Active IQ Digital Advisor、およびその他の関連アプリケーションにログインできるようになります。

NetAppサポート サイトと連携する場合、企業の ID 管理プロバイダーとも連携することはできません。組織に最適なものを選択してください。

手順

1. ダウンロードして完了 "NetAppフェデレーション リクエスト フォーム"。
2. フォームに指定されたメールアドレスにフォームを送信します。

   NetAppサポート チームがお客様のリクエストを確認し、処理します。

#### IDプロバイダーによるシングルサインオン

コンソールのシングル サインオン (SSO) を有効にするには、ID プロバイダーとのフェデレーション接続を設定できます。このプロセスでは、 NetApp をサービス プロバイダーとして信頼するように ID プロバイダーを構成し、コンソールで接続を作成します。

以前にNetApp Cloud Central (コンソールの外部アプリケーション) を使用してフェデレーションを構成した場合は、コンソール内でフェデレーションを管理するために、フェデレーションページを使用してフェデレーションをインポートする必要があります。"フェデレーションをインポートする方法を学びます。"

##### サポートされているIDプロバイダー

NetApp は、フェデレーション用に次のプロトコルと ID プロバイダーをサポートしています。

プロトコル

- セキュリティアサーションマークアップ言語（SAML）IDプロバイダー
- アクティブ ディレクトリ フェデレーション サービス (AD FS)

アイデンティティプロバイダー

- Microsoft Entra ID
- PingFederate

#### NetApp Consoleワークフローとの連携

NetApp は、サービス プロバイダー開始 (SP開始) SSO のみをサポートします。まず、 NetApp をサービス プロバイダーとして信頼するように ID プロバイダーを構成する必要があります。次に、コンソールで ID プロバイダーの構成を使用する接続を作成できます。

自分のメールドメインまたは自分が所有する別のドメインと連携できます。メール ドメインとは異なるドメインとフェデレーションするには、まずそのドメインを所有していることを確認します。


ドメインを確認する（メールドメインを使用していないとき）

メール ドメインとは異なるドメインとフェデレーションするには、そのドメインを所有していることを確認します。追加の手順なしで電子メールドメインを統合できます。


**IdP** を設定して、 **NetApp** をサービス プロバイダーとして信頼します。

新しいアプリケーションを作成し、ACS URL、エンティティ ID、その他の資格情報などの詳細を指定して、NetAppを信頼するように ID プロバイダーを構成します。サービス プロバイダー情報は ID プロバイダーによって異なるため、詳細については特定の ID プロバイダーのドキュメントを参照してください。この手順を完了するには、IdP 管理者と協力する必要があります。


コンソールでフェデレーション接続を作成する

接続を作成するには、ID プロバイダーからの SAML メタデータ URL またはファイルを指定します。この情報は、コンソールと ID プロバイダー間の信頼関係を確立するために使用されます。提供する情報は、使用している IdP によって異なります。たとえば、Microsoft Entra ID を使用している場合は、クライアント ID、シークレット、ドメインを指定する必要があります。


コンソールでフェデレーションをテストする

フェデレーション接続を有効にする前にテストしてください。コンソールのフェデレーション ページのテスト オプションを使用して、テスト ユーザーが正常に認証できることを確認します。テストが成功した場合は、接続を有効にできます。


コンソールで接続を有効にする

接続を有効にすると、ユーザーは企業の資格情報を使用してコンソールにログインできるようになります。

開始するには、それぞれのプロトコルまたは IdP のトピックを確認してください。

- "AD FSとのフェデレーション接続を設定する"
- "Microsoft Entra ID とのフェデレーション接続を設定する"
- "PingFederateでフェデレーション接続を設定する"
- "SAML ID プロバイダとのフェデレーション接続を設定する"

ドメイン検証

フェデレーション接続のメールドメインを確認する

電子メール ドメインとは異なるドメインとフェデレーションを行う場合は、まずそのドメインを所有していることを確認する必要があります。フェデレーションには検証済みのドメインのみを使用できます。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーション

ビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

ドメインを確認するには、ドメインの DNS 設定に TXT レコードを追加する必要があります。このレコードは、ドメインを所有していることを証明するために使用され、 NetApp Consoleがフェデレーションのためにドメインを信頼できるようにします。この手順を完了するには、IT またはネットワーク管理者との調整が必要になる場合があります。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federation** ページを表示するには、**Federation** を選択します。
3. *新しいフェデレーションの構成*を選択します。
4. *ドメインの所有権を確認*を選択します。
5. 検証するドメインを入力し、「続行」を選択します。
6. 提供された TXT レコードをコピーします。
7. ドメインの DNS 設定に移動し、ドメインの TXT レコードとして提供された TXT 値を設定します。必要に応じて、IT 管理者またはネットワーク管理者と協力してください。
8. TXT レコードが追加されたら、コンソールに戻り、[検証] を選択します。

フェデレーションを構成する

#### NetApp ConsoleをActive Directory フェデレーション サービス (AD FS) と連携する

Active Directory フェデレーション サービス (AD FS) をNetApp Consoleと連携させて、NetApp Consoleのシングル サインオン (SSO) を有効にします。これにより、ユーザーは企業の資格情報を使用してコンソールにログインできるようになります。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーション ビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

企業の IdP またはNetAppサポート サイトと連携できます。 NetApp、両方ではなく、どちらか一方を選択することを推奨しています。

NetApp は、サービス プロバイダー開始 (SP開始) SSO のみをサポートします。まず、 NetApp Consoleをサービス プロバイダーとして信頼するように ID プロバイダーを構成します。次に、ID プロバイダーの構成を使用してコンソールで接続を作成します。

AD FS サーバーとのフェデレーションを設定して、 NetApp Consoleのシングル サインオン (SSO) を有効にすることができます。このプロセスでは、コンソールをサービス プロバイダーとして信頼するように AD FS を構成し、 NetApp Consoleで接続を作成します。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federation** ページを表示するには、**Federation** を選択します。
3. *新しいフェデレーションの構成*を選択します。

4. ドメインの詳細を入力してください:
   a. 検証済みドメインを使用するか、メールドメインを使用するかを選択します。電子メール ドメインは、ログインしているアカウントに関連付けられているドメインです。
   b. 構成するフェデレーションの名前を入力します。
   c. 検証済みのドメインを選択する場合は、リストからドメインを選択します。
5. *次へ*を選択します。
6. 接続方法として、[プロトコル] を選択し、[**Active Directory** フェデレーション サービス **(AD FS)**] を選択します。
7. *次へ*を選択します。
8. AD FS サーバーに証明書利用者信頼を作成します。 PowerShell を使用することも、AD FS サーバー上で手動で構成することもできます。証明書利用者信頼を作成する方法の詳細については、AD FS のドキュメントを参照してください。
   a. 次のスクリプトを使用して PowerShell を使用して信頼を作成します。

```
(new-object Net.WebClient -property @{Encoding = [Text.Encoding]
::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
auth0/master/AD FS.ps1") | iex
AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
cloud-account.auth0.com/login/callback"
```

   b. または、AD FS 管理コンソールで信頼を手動で作成することもできます。信頼を作成するときは、次のNetApp Consoleの値を使用します。
      - 信頼信頼識別子を作成するときは、**YOUR_TENANT** 値を使用します。 `netapp-cloud-account`
      - **WS-Federation** のサポートを有効にする を選択した場合は、**YOUR_AUTH0_DOMAIN** 値を使用します。 `netapp-cloud-account.auth0.com`
   c. 信頼を作成した後、AD FS サーバーからメタデータ URL をコピーするか、フェデレーション メタデータ ファイルをダウンロードします。コンソールで接続を完了するには、この URL またはファイルが必要になります。

NetApp、メタデータ URL を使用してNetApp Consoleが最新の AD FS 構成を自動的に取得できるようにすることをお勧めします。フェデレーション メタデータ ファイルをダウンロードした場合は、AD FS 構成に変更があるたびに、 NetApp Consoleで手動で更新する必要があります。

9. コンソールに戻り、[次へ] を選択して接続を作成します。
10. AD FS との接続を作成します。
    a. 前の手順で AD FS サーバーからコピーした **AD FS URL** を入力するか、AD FS サーバーからダウンロードしたフェデレーション メタデータ ファイルをアップロードします。
11. *接続を作成*を選択します。接続の作成には数秒かかる場合があります。
12. *次へ*を選択します。
13. 接続をテストするには、[接続テスト] を選択します。IdP サーバーのログイン ページに移動します。IdP のクレデンシャルを使用してログインします。ログイン後、コンソールに戻って接続を有効にします。

コンソールを制限モードで使用する場合は、URL をシークレット ブラウザ ウィンドウまたは別のブラウザにコピーして IdP にログインします。

14. コンソールで、[次へ] を選択して概要ページを確認します。
15. 通知を設定します。

    7日間または30日間を選択します。システムは、スーパー管理者、組織管理者、フェデレーション管理者、フェデレーション閲覧者の役割を持つすべてのユーザーに有効期限通知を電子メールで送信し、コンソールに表示します。

16. フェデレーションの詳細を確認し、[フェデレーションを有効にする] を選択します。
17. プロセスを完了するには、[完了] を選択します。

フェデレーションを有効にすると、ユーザーは企業の資格情報を使用してNetApp Consoleにログインします。

#### NetApp ConsoleをMicrosoft Entra ID と連携する

## Microsoft Entra ID IdP プロバイダーと連携して、 NetApp Consoleのシングル サインオン (SSO) を有効にします。これにより、ユーザーは企業の資格情報を使用してログインできるようになります。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーション ビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

企業の IdP またはNetAppサポート サイトと連携できます。 NetApp、両方ではなく、どちらか一方を選択することを推奨しています。

NetApp は、サービス プロバイダー開始 (SP開始) SSO のみをサポートします。まず、 NetApp をサービス プロバイダーとして信頼するように ID プロバイダーを構成する必要があります。次に、コンソールで ID プロバイダーの構成を使用する接続を作成できます。

Microsoft Entra ID とのフェデレーション接続を設定して、コンソールのシングル サインオン (SSO) を有効にすることができます。このプロセスでは、コンソールをサービス プロバイダーとして信頼するように Microsoft Entra ID を構成し、コンソールで接続を作成します。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federation** ページを表示するには、**Federation** を選択します。
3. *新しいフェデレーションの構成*を選択します。

ドメインの詳細

1. ドメインの詳細を入力してください:
    a. 検証済みドメインを使用するか、メールドメインを使用するかを選択します。電子メール ドメインは、ログインしているアカウントに関連付けられているドメインです。

b. 構成するフェデレーションの名前を入力します。

c. 検証済みのドメインを選択する場合は、リストからドメインを選択します。

2. *次へ*を選択します。

接続方法

1. 接続方法として、*プロバイダー*を選択し、*Microsoft Entra ID*を選択します。
2. *次へ*を選択します。

設定手順

1. NetApp をサービス プロバイダーとして信頼するように Microsoft Entra ID を構成します。この手順は Microsoft Entra ID サーバーで実行する必要があります。
   a. コンソールを信頼するには、Microsoft Entra ID アプリを登録するときに次の値を使用します。
      - *リダイレクトURL*には、 `https://services.cloud.netapp.com`
      - *返信URL*には、 `https://netapp-cloud-account.auth0.com/login/callback`
   b. Microsoft Entra ID アプリのクライアント シークレットを作成します。フェデレーションを完了するには、クライアント ID、クライアント シークレット、Entra ID ドメイン名を提供する必要があります。
2. コンソールに戻り、[次へ] を選択して接続を作成します。

接続を作成

1. Microsoft Entra IDで接続を作成する
   a. 前の手順で作成したクライアント ID とクライアント シークレットを入力します。
   b. Microsoft Entra ID ドメイン名を入力します。
2. *接続を作成*を選択します。システムは数秒で接続を作成します。

接続をテストして有効にする

1. *次へ*を選択します。
2. 接続をテストするには、[接続テスト] を選択します。IdP サーバーのログイン ページに移動します。IdP のクレデンシャルを使用してログインします。ログイン後、コンソールに戻って接続を有効にします。

   コンソールを制限モードで使用する場合は、URL をシークレット ブラウザ ウィンドウまたは別のブラウザにコピーして IdP にログインします。

3. コンソールで、[次へ] を選択して概要ページを確認します。
4. 通知を設定します。

   7日間または30日間を選択します。システムは、スーパー管理者、組織管理者、フェデレーション管理者、フェデレーション閲覧者の役割を持つすべてのユーザーに有効期限通知を電子メールで送信し、コンソールに表示します。

5. フェデレーションの詳細を確認し、[フェデレーションを有効にする] を選択します。

6. プロセスを完了するには、[完了] を選択します。

フェデレーションを有効にすると、ユーザーは企業の資格情報を使用してNetApp Consoleにログインします。

#### PingFederateでNetApp Consoleを連携

## PingFederate IdP プロバイダーと連携して、 NetApp Consoleのシングル サインオン (SSO) を有効にします。これにより、ユーザーは企業の資格情報を使用してログインできるようになります。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーション ビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

企業の IdP またはNetAppサポート サイトと連携できます。 NetApp、両方ではなく、どちらか一方を選択することを推奨しています。

NetApp は、サービス プロバイダー開始 (SP開始) SSO のみをサポートします。まず、 NetApp をサービス プロバイダーとして信頼するように ID プロバイダーを構成する必要があります。次に、コンソールで ID プロバイダーの構成を使用する接続を作成できます。

PingFederate とのフェデレーション接続を設定して、コンソールのシングル サインオン (SSO) を有効にすることができます。このプロセスでは、コンソールをサービス プロバイダーとして信頼するように PingFederate サーバーを構成し、コンソールで接続を作成します。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federation** ページを表示するには、**Federation** を選択します。
3. *新しいフェデレーションの構成*を選択します。
4. ドメインの詳細を入力してください:
   a. 検証済みドメインを使用するか、メールドメインを使用するかを選択します。電子メール ドメインは、ログインしているアカウントに関連付けられているドメインです。
   b. 構成するフェデレーションの名前を入力します。
   c. 検証済みのドメインを選択する場合は、リストからドメインを選択します。
5. *次へ*を選択します。
6. 接続方法として、*プロバイダー*を選択し、次に*PingFederate*を選択します。
7. *次へ*を選択します。
8. PingFederate サーバーを、サービス プロバイダーとしてNetApp を信頼するように構成します。この手順は PingFederate サーバーで実行する必要があります。
   a. PingFederate を構成してNetApp Consoleを信頼する場合は、次の値を使用します。
      - *返信URL*または*アサーションコンシューマーサービス（ACS）URL*の場合は、 `https://netapp-cloud-account.auth0.com/login/callback`
      - *ログアウトURL*には、 `https://netapp-cloud-account.auth0.com/logout`

- *オーディエンス/エンティティID*には、 `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>`ここで、<fed-domain-name-pingfederate> はフェデレーションのドメイン名です。たとえば、ドメインが `example.com`オーディエンス/エンティティIDは次のようになります。 `urn:auth0:netappcloud-account:fed-example-com-pingfederate`。

b. PingFederate サーバーの URL をコピーします。コンソールで接続を作成するときに、この URL が必要になります。

c. PingFederate サーバーから X.509 証明書をダウンロードします。 Base64 でエンコードされた PEM 形式 (.pem、.crt、.cer) である必要があります。

9. コンソールに戻り、[次へ] を選択して接続を作成します。

10. PingFederateで接続を作成する

a. 前の手順でコピーした PingFederate サーバーの URL を入力します。

b. X.509 署名証明書をアップロードします。証明書は PEM、CER、または CRT 形式である必要があります。

11. *接続を作成*を選択します。システムは数秒で接続を作成します。

12. *次へ*を選択します。

13. 接続をテストするには、[接続テスト] を選択します。IdP サーバーのログイン ページに移動します。IdP のクレデンシャルを使用してログインします。ログイン後、コンソールに戻って接続を有効にします。

> コンソールを制限モードで使用する場合は、URL をシークレット ブラウザ ウィンドウまたは別のブラウザにコピーして IdP にログインします。

14. コンソールで、[次へ] を選択して概要ページを確認します。

15. 通知を設定します。

    7日間または30日間を選択します。システムは、スーパー管理者、組織管理者、フェデレーション管理者、フェデレーション閲覧者の役割を持つすべてのユーザーに有効期限通知を電子メールで送信し、コンソールに表示します。

16. フェデレーションの詳細を確認し、[フェデレーションを有効にする] を選択します。

17. プロセスを完了するには、[完了] を選択します。

フェデレーションを有効にすると、ユーザーは企業の資格情報を使用してNetApp Consoleにログインします。

**SAML ID** プロバイダとの連携

## SAML 2.0 IdP プロバイダーと連携して、NEtApp コンソールのシングル サインオン (SSO) を有効にします。これにより、ユーザーは企業の資格情報を使用してログインできるようになります。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーション ビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

企業の IdP またはNetAppサポート サイトと連携できます。両方と連携することはできません。

NetApp は、サービス プロバイダー開始 (SP開始) SSO のみをサポートします。まず、 NetApp をサービス プロバイダーとして信頼するように ID プロバイダーを構成する必要があります。次に、コンソールで ID プロバイダーの構成を使用する接続を作成できます。

SAML 2.0 プロバイダーとのフェデレーション接続を設定して、コンソールのシングル サインオン (SSO) を有効にすることができます。このプロセスでは、プロバイダーがNetApp をサービス プロバイダーとして信頼するように構成し、コンソールで接続を作成します。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federation** ページを表示するには、**Federation** を選択します。
3. *新しいフェデレーションの構成*を選択します。
4. ドメインの詳細を入力してください:
   a. 検証済みドメインを使用するか、メールドメインを使用するかを選択します。電子メール ドメインは、ログインしているアカウントに関連付けられているドメインです。
   b. 構成するフェデレーションの名前を入力します。
   c. 検証済みのドメインを選択する場合は、リストからドメインを選択します。
5. *次へ*を選択します。
6. 接続方法として、*プロトコル*を選択し、*SAML ID プロバイダー*を選択します。
7. *次へ*を選択します。
8. SAML ID プロバイダーを構成して、 NetApp をサービス プロバイダーとして信頼します。この手順は SAML プロバイダー サーバーで実行する必要があります。
   a. IdPに属性があることを確認する `email`ユーザーのメールアドレスに設定されます。これは、コンソールがユーザーを正しく識別するために必要です。

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        <saml:AttributeValue
xsi:type="xs:string">email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

1. SAML アプリケーションをコンソールに登録するときは、次の値を使用します。
   - *返信URL*または*アサーションコンシューマーサービス（ACS）URL*の場合は、 https://netapp-cloud-account.auth0.com/login/callback

- *ログアウトURL*には、 https://netapp-cloud-account.auth0.com/logout
- *オーディエンス/エンティティID*には、 `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>`ここで、<fed-domain-name-saml> はフェデレーションに使用するドメイン名です。たとえば、ドメインが `example.com`オーディエンス/エンティティIDは次のようになります。 `urn:auth0:netapp-cloud-account:fed-example-com-samlp`。

2. 信頼を作成したら、SAML プロバイダー サーバーから次の値をコピーします。
   - サインインURL
   - サインアウトURL（オプション）
3. SAML プロバイダー サーバーから X.509 証明書をダウンロードします。 PEM、CER、または CRT 形式である必要があります。
   a. コンソールに戻り、[次へ] を選択して接続を作成します。
   b. SAML を使用して接続を作成します。
4. SAML サーバーの サインイン **URL** を入力します。
5. SAML プロバイダー サーバーからダウンロードした X.509 証明書をアップロードします。
6. 必要に応じて、SAML サーバーの サインアウト **URL** を入力します。
   a. *接続を作成*を選択します。システムは数秒で接続を作成します。
   b. *次へ*を選択します。
   c. 接続をテストするには、[接続テスト] を選択します。IdP サーバーのログイン ページに移動します。IdPのクレデンシャルを使用してログインします。ログイン後、コンソールに戻って接続を有効にします。

      コンソールを制限モードで使用する場合は、URL をシークレット ブラウザ ウィンドウまたは別のブラウザにコピーして IdP にログインします。

   d. コンソールで、[次へ] を選択して概要ページを確認します。
   e. 通知を設定します。

      7日間または30日間を選択します。システムは、スーパー管理者、組織管理者、フェデレーション管理者、フェデレーション閲覧者の役割を持つすべてのユーザーに有効期限通知を電子メールで送信し、コンソールに表示します。

   f. フェデレーションの詳細を確認し、[フェデレーションを有効にする] を選択します。
   g. プロセスを完了するには、[完了] を選択します。

フェデレーションを有効にすると、ユーザーは企業の資格情報を使用してNetApp Consoleにログインします。

## フェデレーションの管理

### NetApp Consoleでフェデレーションを管理する

NetApp Consoleでフェデレーションを管理できます。無効にしたり、期限切れの資格情報を更新したり、不要になった場合に無効にしたりすることができます。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーション ビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

既存のフェデレーションに検証済みのドメインを追加することもできます。これにより、フェデレーション接続に複数のドメインを使用できるようになります。

- NetApp Cloud Central を使用してフェデレーションを構成した場合は、フェデレーション ページからインポートして、コンソールで管理します。"フェデレーションをインポートする方法を学ぶ"
- 監査ページでは、フェデレーションの有効化、無効化、更新などのフェデレーション管理イベントを表示できます。 "NetApp Consoleでの操作の監視について詳しく学習します。"

フェデレーションを有効にする

フェデレーションを作成したが有効になっていない場合は、フェデレーション ページから有効にすることができます。フェデレーションを有効にすると、フェデレーションに関連付けられたユーザーは、企業の資格情報を使用してコンソールにログインできるようになります。フェデレーションを有効にする前に、フェデレーションを作成してテストしてください。

手順

1. *管理 > IDとアクセス*を選択します。
2. *Federation*タブを選択します。
3. アクションメニューを選択 ••• 有効にするフェデレーションの横にある をクリックし、[有効] を選択します。

検証済みのドメインを既存のフェデレーションに追加する

コンソールで既存のフェデレーションに検証済みのドメインを追加して、同じ ID プロバイダー (IdP) で複数のドメインを使用できます。

ドメインをフェデレーションに追加する前に、コンソールでドメインを検証しておく必要があります。ドメインをまだ確認していない場合は、以下の手順に従って確認することができます。"コンソールでドメインを確認する" 。

手順

1. *管理 > IDとアクセス*を選択します。
2. *Federation*タブを選択します。
3. アクションメニューを選択 ⋮ 検証済みドメインを追加するフェデレーションの横にある をクリックし、[ドメインの更新] を選択します。 ドメインの更新 ダイアログ ボックスには、このフェデレーションにすでに関連付けられているドメインが表示されます。
4. 利用可能なドメインのリストから検証済みのドメインを選択します。
5. *更新*を選択します。新しいドメイン ユーザーは、30 秒以内にフェデレーション コンソール アクセスを取得できます。

### 期限切れのフェデレーション接続の更新

コンソールでフェデレーションの詳細を更新できます。たとえば、証明書やクライアント シークレットなどの資格情報の有効期限が切れた場合は、フェデレーションを更新する必要があります。必要に応じて通知日を更新し、接続が期限切れになる前に更新するよう通知します。

ログインの問題を回避するには、IdP を更新する前にまずコンソールを更新してください。プロセス中はコンソールにログインしたままにしてください。

手順

1. *管理 > IDとアクセス*を選択します。
2. *Federation*タブを選択します。
3. 更新するフェデレーションの横にあるアクション メニュー (縦に並んだ 3 つのドット) を選択し、フェデレーションの更新 を選択します。
4. 必要に応じてフェデレーションの詳細を更新します。
5. *更新*を選択します。

### 既存のフェデレーションをテストする

既存のフェデレーションの接続をテストして、それが機能することを確認します。これにより、フェデレーションに関する問題を特定し、トラブルシューティングすることができます。

手順

1. *管理 > IDとアクセス*を選択します。
2. *Federation*タブを選択します。
3. アクションメニューを選択:検証済みドメインを追加するフェデレーションの横にある をクリックし、[テスト接続] を選択します。
4. *テスト*を選択します。システムは、企業の資格情報を使用してログインするように要求します。接続が成功すると、 NetApp Consoleにリダイレクトされます。接続に失敗した場合は、フェデレーションの問題を示すエラー メッセージが表示されます。
5. *完了*を選択して*連合*タブに戻ります。

### フェデレーションを無効にする

フェデレーションが不要になった場合は、無効にすることができます。これにより、フェデレーションに関連付けられたユーザーが企業の資格情報を使用してコンソールにログインできなくなります。必要に応じて、後でフェデレーションを再度有効にすることができます。

IdP を廃止する場合やフェデレーションを中止する場合など、フェデレーションを削除する前に無効にします。これにより、必要に応じて後で再度有効にすることができます。

手順

1. *管理 > IDとアクセス*を選択します。
2. *Federation*タブを選択します。
3. アクションメニューを選択:検証済みドメインを追加するフェデレーションの横にある をクリックし、[無効にする] を選択します。

フェデレーションを削除する

フェデレーションが不要になった場合は、削除できます。これにより、フェデレーションが削除され、フェデレーションに関連付けられたすべてのユーザーが企業の資格情報を使用してコンソールにログインできなくなります。たとえば、IdP が廃止される場合や、フェデレーションが不要になった場合などです。

フェデレーションを削除した後は、回復することはできません。新しいフェデレーションを作成する必要があります。

フェデレーションを削除する前に無効にする必要があります。フェデレーションを削除した後で、元に戻すことはできません。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federations** ページを表示するには、**Federations** を選択します。
3. アクションメニューを選択:検証済みドメインを追加するフェデレーションの横にある をクリックし、[削除] を選択します。

**NetApp Console**にフェデレーションをインポートする

以前にNetApp Cloud Central ( NetApp Consoleの外部アプリケーション) を通じてフェデレーションを設定したことがある場合は、フェデレーション ページで、既存のフェデレーション接続をコンソールにインポートして、新しいインターフェイスで管理できるようにするように求められます。そうすれば、フェデレーション接続を再作成しなくても、最新の拡張機能を活用できるようになります。

既存のフェデレーションをインポートした後、フェデレーション ページからフェデレーションを管理できます。"フェデレーションの管理について詳しく学びます。"

必要な役割

組織管理者またはフェデレーション管理者。"アクセス ロールの詳細について説明します。"

手順

1. *管理 > IDとアクセス*を選択します。
2. *Federation*タブを選択します。
3. *インポートフェデレーション*を選択します。

## ONTAP Advanced View（ONTAP System Manager）のONTAP権限を適用する

デフォルトでは、コンソール エージェントの認証情報により、ユーザーは詳細ビュー (ONTAP System Manager) にアクセスできます。代わりに、ユーザーにONTAP認証情報の入力を求めることもできます。これにより、ユーザーが Cloud Volumes ONTAP とONTAPオンプレミス クラスターの両方でONTAPクラスターを操作するときに、ユーザーのONTAP権限が確実に適用されます。

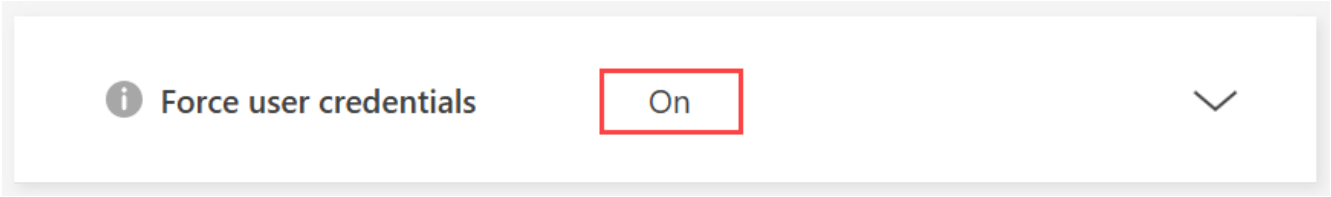
コンソール エージェントの設定を編集するには、組織管理者のロールが必要です。

手順

1. *管理 > エージェント*を選択します。
2. *概要*ページで、コンソール エージェントのアクション メニューを選択し、*エージェントの編集*を選択します。

   編集するには、コンソール エージェントがアクティブである必要があります。

3. *資格情報の強制*オプションを展開します。
4. *資格情報の強制*オプションを有効にするにはチェックボックスをオンにして、*保存*を選択します。
5. *資格情報の強制*オプションが有効になっていることを確認します。




## NetApp Console組織の読み取り専用モードを有効にする

セキュリティ上の予防措置として、 NetApp Console組織に対して読み取り専用モードを有効にすることができます。読み取り専用モードでは、ユーザーはリソースと設定を表示できますが、変更することはできません。

読み取り専用モードでは、管理者ロールを持つユーザーは変更を行うために手動で権限を昇格する必要があり、これにより変更が意図的なものであることが保証されます。

必要なアクセスロール

スーパー管理者または組織管理者。

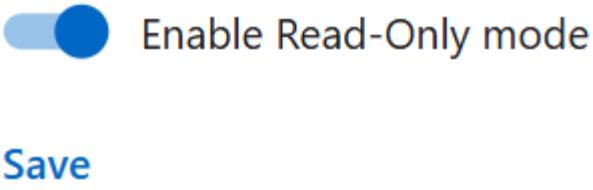
コンソール組織で読み取り専用モードを有効にする

コンソール組織への変更を制限するには、読み取り専用モードを有効にします。すべてのユーザーは引き続きリソースを表示できます。管理者ロールを持つユーザーは、権限を手動で昇格させなければ、コンソールでアクションを実行することはできません。

読み取り専用モードが有効になっている場合、組織が読み取り専用モードであることを通知するバナーがユーザーに表示されます。ユーザーは、役割を昇格するにはユーザー設定に移動する必要があります。

手順

1. *管理 > IDとアクセス*を選択します。
2. *組織*タブから、読み取り専用モードに設定する組織の*組織設定の編集*を選択します。
3. *読み取り専用モード*セクションで、トグルを*オン*の位置に移動して読み取り専用モードを有効にし、*保存*を選択します。




**NetApp Console**に初期組織管理者としてサインアップする

会社にNetApp Console組織がない場合は、サインアップして作成してください。最初のユーザーは管理者であり、アカウントと権限を管理します。後でロールを更新したり、管理者を追加したりできます。

手順

1. ウェブブラウザを開いて、 "NetApp Console"
2. NetApp Support Siteのアカウントをお持ちの場合は、ログイン ページでアカウントに関連付けられている電子メール アドレスを直接入力します。

   コンソールは、この最初のログインの一部として、NetApp Support Siteの資格情報を使用してサインアップします。

3. コンソール ログインを作成してサインアップする場合は、[サインアップ] を選択します。
   a. *サインアップ*ページで必要な情報を入力し、*次へ*を選択します。

      サインアップフォームでは英語の文字のみ使用できます。

   b. 受信トレイで、電子メール アドレスを確認するための手順が記載されたNetAppからの電子メールを確認してください。

      サインアップを完了するには、メールアドレスを確認してください。

4. ログイン後、エンドユーザー使用許諾契約書を確認して同意します。
5. *ようこそ*ページで組織を作成します。
6. *始めましょう*を選択します。

+ 初めての管理者は、ガイド付きのプロセスに従ってストレージの追加、コンソール エージェントの作成などを行います。 "コンソール アシスタントの使用について説明します。"

次のステップ

管理者は、コンソール アシスタントに含まれる手順を完了した後、ID とアクセス戦略を計画し、組織にユーザーを追加し、ロールを割り当てる必要があります。 "NetApp ConsoleのIDとアクセス管理について学ぶ"

組織がすでに存在する場合は、 **NetApp Console**にサインアップまたはログインしてください

会社にすでにNetApp Console組織がある場合は、サインアップまたはログインしてアクセスしてください。サインアップまたはログインの方法は、会社が ID フェデレーションを使用しているか、 NetApp Support Siteの認証情報を持っているかによって異なります。そうでない場合は、 NetApp Consoleログインを作成します。

手順

1. ウェブブラウザを開いて、 "NetApp Console"
2. NetApp Support Siteのアカウントをお持ちの場合、または会社でシングル サインオン(SSO) を設定している場合は、[ログイン] ページに関連付けられている電子メール アドレスまたは SSO 資格情報を入力します。指示に従ってログインを完了してください。

   どちらの場合も、最初のログインの一環としてコンソールにサインアップされます。
3. コンソール ログインを作成してサインアップする場合は、[サインアップ] を選択します。
   a. *サインアップ*ページで必要な情報を入力し、*次へ*を選択します。

      サインアップフォームでは英語の文字のみ使用できます。

   b. 受信トレイで、電子メール アドレスを確認するための手順が記載されたNetAppからの電子メールを確認してください。

      サインアップを完了するには、メールアドレスを確認してください。
4. ログイン後、エンドユーザー使用許諾契約書を確認して同意します。
5. システムから組織の作成を求められた場合は、ダイアログ ボックスを閉じてコンソール管理者に伝え、コンソール組織に追加してアクセス権を付与してもらいます。 "組織管理者に連絡する方法について説明します。"

次のステップ

組織へのアクセス権が付与されると、ストレージの管理と割り当てられたデータ サービスの使用を開始できます。

# 組織のパートナーシップを管理する

## NetApp Console における組織パートナーシップ

NetApp Consoleで組織間のパートナーシップを構築することで、パートナーは組織の境界を越えてNetAppリソースを安全に管理し、コラボレーションを合理化し、セキュリティを強化できます。

必要な役割

パートナーシップ管理者"アクセス ロールの詳細について説明します。"

パートナーシップにより、コンソールでロール主導の関係を使用して、組織全体のNetAppリソースを安全に管理できます。開始組織はリソースへのアクセスを許可し、受け入れ組織はアクセスを許可するユーザーまたはサービス アカウントを提供します。パートナーシップはセルフサービス ワークフローを通じて確立され、開始組織は共有されるリソース、割り当てられるロール、必要に応じてパートナー アクセスをオンボード、管理、または取り消す機能などを完全に制御できます。

顧客は、複雑な設定を必要とせずに、MSP または再販業者にNetApp環境の管理を許可できます。お客様は、パートナーがアクセスできるクラスターとその役割を制御でき、セキュリティとコンプライアンスを維持するためにいつでもアクセスを取り消すことができます。

パートナーとして、顧客環境全体の一元的な可視性と制御を実現できます。顧客の組織に簡単に切り替えて、定義された境界内でリソースを管理し、データ サービスを実行し、正常性を監視できるため、カスタム ツールが削減され、各顧客のポリシーとの整合性が確保されます。

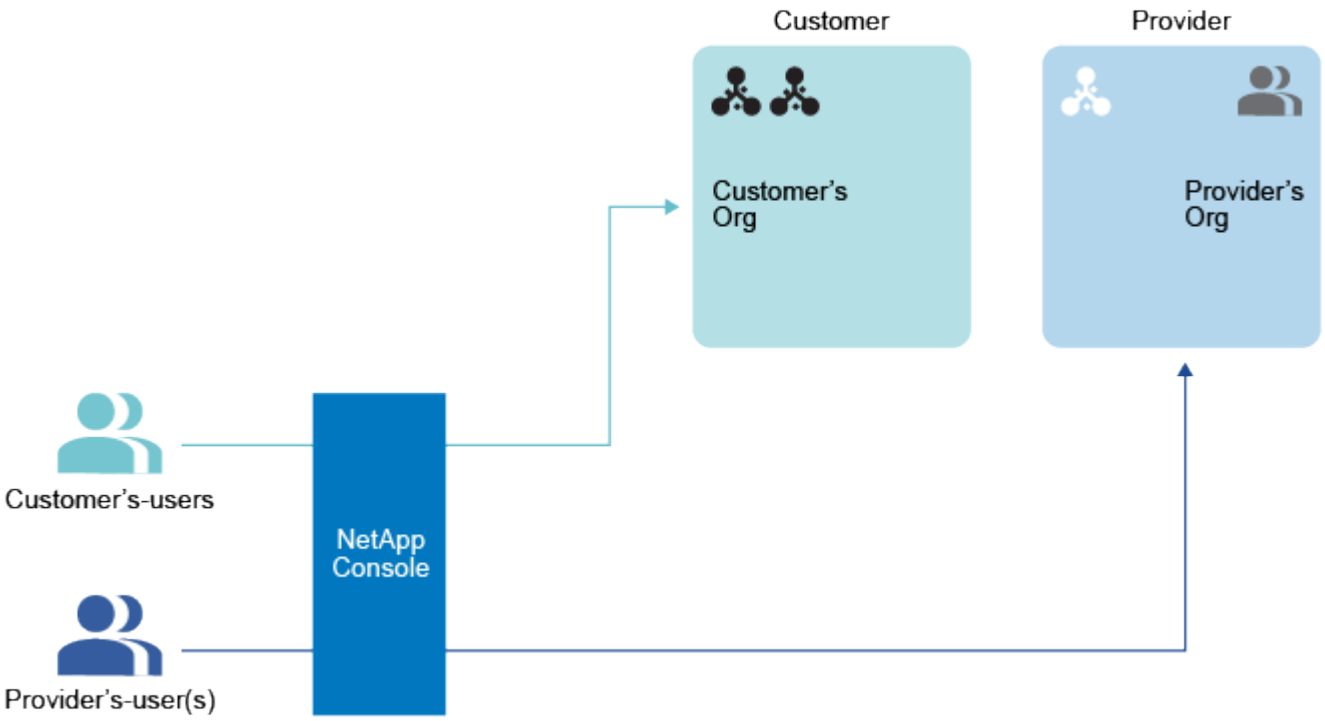
### 1 1人以上のユーザーにパートナーシップ管理者の役割を割り当てる

パートナーシップを作成および管理するには、開始組織と受信組織の両方の 1 人以上のユーザーに Partnership admin ロールを割り当てます。パートナーシップの表示のみが必要で、管理は必要ないユーザーには、Partnership viewer ロールを割り当てることができます。

### 2 組織IDを開始組織と共有する

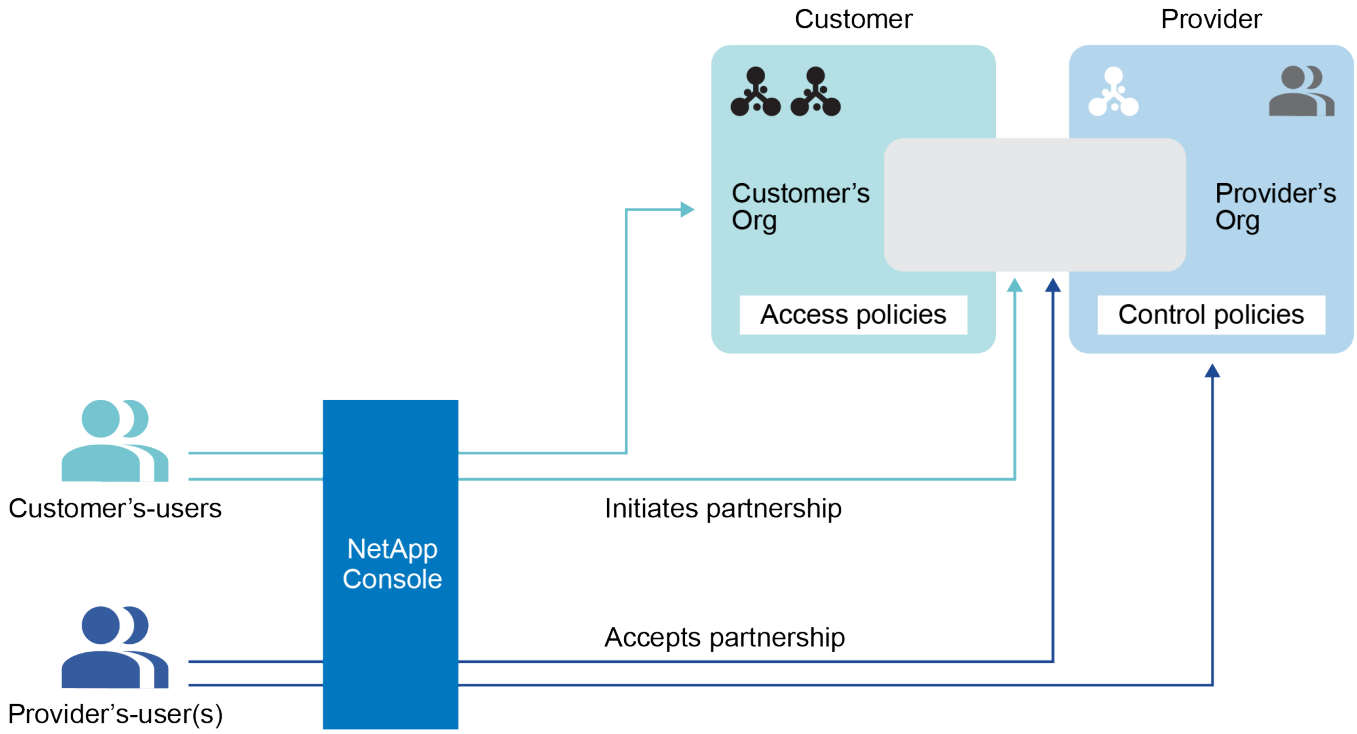
パートナーシップを開始するには、イニシエーターがターゲット組織の組織 ID を知っている必要があります。この組織 ID にアクセスできるのは、それぞれの組織のみです。電子メールまたは別の方法で、 NetApp Consoleの外部にある開始組織と直接共有します。

開始組織とは、そのリソースへのアクセスを許可する組織です。




### 3 NetApp Console内でパートナーシップを開始する

パートナーシップを開始する組織は、NetApp Console内からパートナーシップ要求を送信してパートナーシップを開始します。



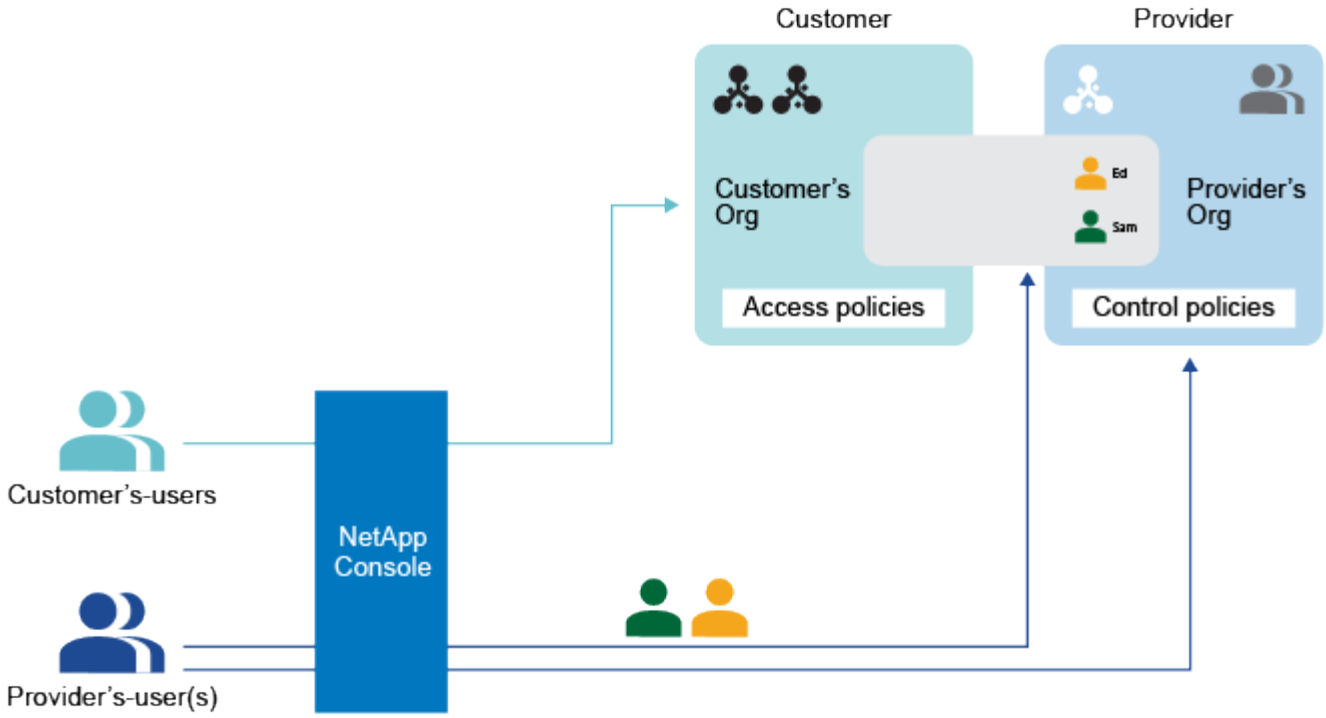

4 パートナーシップを承認する

受信組織はリクエストを承認する必要があります。

受信組織は、リソースへのアクセスを許可される組織です。

5 パートナーシップにユーザーを割り当てる

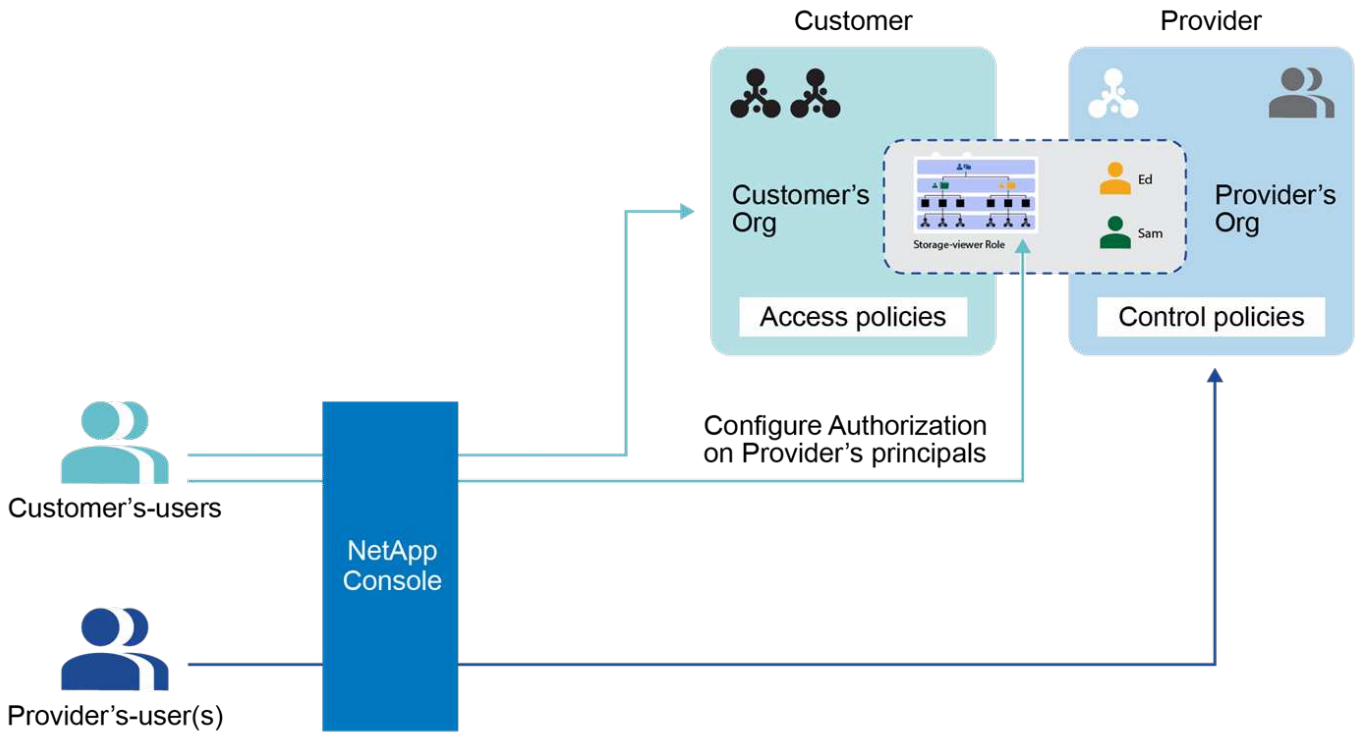
受信側組織は、組織の特定のユーザーまたはサービス アカウントをパートナーシップに割り当てます。開始組織はこれらのユーザーにロールを割り当てます。




6 割り当てられたユーザーにリソースへのアクセスを許可する

開始組織の場合は、パートナーシップに割り当てられたユーザーに特定のリソースへのアクセス権を付与できます。いつでもアクセスを取り消すことができます。

これは、組織内の特定のプロジェクトまたはフォルダーにロールを割り当てることによって行います。



# NetApp Consoleでパートナーシップを管理する

## パートナーシップを構築し、組織と信頼できるパートナーとの間で安全で管理された接続を確立して、共同でNetAppリソースを管理します。

パートナーシップにより、コンソールでロール主導の関係を使用して、境界を越えてNetAppリソースを安全に管理できます。開始組織はリソースへのアクセスを許可し、受け入れ組織はアクセスを許可するユーザーまたはサービス アカウントを提供します。パートナーシップはセルフサービス ワークフローを通じて確立され、開始組織は共有されるリソース、割り当てられるロール、必要に応じてパートナー アクセスをオンボード、管理、または取り消す機能などを完全に制御できます。

必要な役割

パートナーシップを作成および管理するには、パートナーシップ管理者 ロールが必要です。 *パートナーシップ閲覧者*はパートナーシップ ページを閲覧できます。"アクセス ロールの詳細について説明します。"

組織パートナーシップを開始する

他の組織の組織 ID がわかっている場合は、その組織とのパートナーシップをリクエストできます。パートナーシップを進める前に、受信側の組織がリクエストを承認する必要があります。

始める前に、パートナー組織の組織 ID があることと、パートナーシップ管理者 ロールが割り当てられていることを確認してください。

手順

1. *管理 > IDとアクセス*を選択します。
2. *パートナーシップ*タブを選択します。
3. *パートナーシップを追加*を選択します。
4. パートナーシップの作成 ダイアログボックスで、要求されたパートナーのパートナー組織 ID を入力し、追加 を選択します。

   パートナーシップ リクエストは、承認のためにパートナー組織に送信されます。 *パートナーシップ*ページでパートナーシップリクエストのステータスを確認できます。

組織パートナーシップを承認する

パートナーシップを進めるには、組織パートナーシップのリクエストが受信側組織によって承認される必要があります。パートナーシップを承認および管理するには、パートナーシップ管理者 の役割が必要です。

手順

1. *管理 > IDとアクセス*を選択します。
2. *パートナーシップ*を選択します。
3. *パートナーシップ受信*タブを選択します。
4. 承認したい受信したパートナーシップに移動して選択します ... 次に、[承認] を選択します。
5. パートナーシップを要求した組織の名前と組織 ID を含むパートナーシップの詳細を確認し、[次へ] を選択します。
6. オプションとして、組織のメンバーをパートナーシップに追加し、「適用」を選択します。

パートナーシップ ページからいつでもメンバーを追加できます。

追加したメンバーはパートナーの組織に表示されるようになり、パートナーはメンバーをリソースに割り当てることができます。

結果

承認したパートナーシップのステータスが「確立済み」と表示されます。どちらかの組織で パートナーシップ管理者 または パートナーシップ閲覧者 の役割を持つユーザーは、パートナーシップを表示できます。

パートナーシップのステータスを表示

パートナーシップのステータスを表示します。

必要な役割

パートナーシップ管理者、パートナーシップ閲覧者。"アクセス ロールの詳細について説明します。"

手順

1. *管理 > IDとアクセス*を選択します。
2. *パートナーシップ*を選択します。
3. *開始したパートナーシップ*または*受信したパートナーシップ*タブを選択します。
4. パートナーシップとそのステータスを表示するそれぞれの表を確認します。

組織のパートナーシップを無効にする

パートナーシップを無効にするには、開始組織のメンバーである必要があります。パートナーシップを無効にすると、パートナー組織と共有されていた組織内のすべてのリソースへのアクセスが直ちに取り消されます。

必要な役割

パートナーシップ管理者。"アクセス ロールの詳細について説明します。"

手順

1. *管理 > IDとアクセス*を選択します。
2. *パートナーシップ*を選択します。
3. *開始されたパートナーシップ*タブのいずれかを選択します。
4. パートナーシップとそのステータスを表示するそれぞれの表を確認します。
5. 無効にしたい開始済みのパートナーシップに移動し、 次に、[無効にする] を選択します。

## パートナーシップ組織のメンバーを管理する

パートナー組織にユーザーを追加することで、パートナーシップにユーザーを追加できます。ユーザーを追加したら、パートナー組織は組織内の特定のリソースに対するロールをユーザーに割り当てる責任を負います。

必要な役割

パートナーシップを作成および管理するには、パートナーシップ管理者 ロールが必要です。 *パートナーシッ

プ閲覧者*はパートナーシップ ページを閲覧できます。"アクセス ロールの詳細について説明します。"

いつでもパートナーシップからユーザーを削除できます。パートナーシップからユーザーを削除すると、パートナー組織内のすべてのリソースへのアクセス権が直ちに取り消されます。

### パートナーシップにメンバーを追加する

パートナーシップにメンバーを追加する場合、パートナー組織の パートナーシップ管理者 は、メンバーがリソースにアクセスできるようにする前に、組織内の特定のリソースに対するロールをメンバーに割り当てる必要があります。

パートナーシップにメンバーを追加すると、そのメンバーはパートナー組織のメンバーとして表示され、パートナーはメンバーをリソースに割り当てることができます。

手順

1. *管理 > IDとアクセス*を選択します。
2. *パートナーシップ*を選択します。
3. *パートナーシップ受信*タブを選択します。
4. アクションメニューを選択 メンバーに追加したい確立されたパートナーシップの横にある をクリックし、[メンバーを追加] を選択します。
5. パートナーシップに追加するメンバーを 1 人以上選択し、[追加] を選択します。

### パートナーシップからメンバーを削除する

パートナーシップからメンバーをいつでも削除できます。パートナーシップからユーザーを削除すると、パートナー組織内のすべてのリソースへのアクセス権が直ちに取り消されます。

メンバーの役割やアクセスできるリソースを調整する場合は、パートナー組織のパートナーシップ管理者がその変更を行う必要があります。

手順

1. *管理 > IDとアクセス*を選択します。
2. *パートナーシップ*を選択します。
3. *パートナーシップ受信*タブを選択します。
4. アクションメニューを選択 削除するメンバーの横にある をクリックし、[関連付けを削除] を選択します。
5. ダイアログボックスで*削除*を選択してアクションを確認します。

### ユーザーの役割情報を表示する

ユーザーに割り当てられているロールと関連付けられているリソースを表示できます。

ユーザーに関連付けられたロールを変更することはできません。提供されるリソースまたはロールについて質問がある場合は、パートナー組織の管理者にお問い合わせください。

手順

1. *管理 > IDとアクセス*を選択します。

2. *パートナーシップ*を選択します。
3. *パートナーシップ受信*タブを選択します。
4. *メンバー*ページで、テーブル内のメンバーに移動し、 次に、[詳細を表示] を選択します。
5. 表で、メンバーに割り当てられたロールを表示する組織、フォルダ、またはプロジェクトのそれぞれの行を展開し、「ロール」列の番号を選択します。

## パートナーシップユーザーにリソースへのアクセスを提供する

組織内のフォルダやプロジェクトに対する特定のロールをパートナーシップ ユーザーに割り当てることで、パートナーシップ ユーザーにアクセス権を付与できます。

必要な役割

パートナーシップ管理者。"アクセス ロールの詳細について説明します。"

パートナー組織では、まずパートナーシップにメンバーを追加してから、組織内のリソースのロールをメンバーに割り当てる必要があります。"パートナーシップにメンバーを追加する方法を学びます。"

パートナーシップユーザーの役割を理解する

自分の組織の場合と同じ方法で、パートナー組織のメンバーの役割を管理できます。ただし、パートナーシップ ユーザーはすべてのロールを利用できるわけではありません。特に、パートナー ユーザーにソフトウェアの更新を許可するロールを付与することはできません。通常、 ONTAPソフトウェアを更新するには、直接ネットワーク アクセスが必要です。

パートナー ユーザーには次のロールを割り当てることができます。

- "組織管理者"
- "フォルダまたはプロジェクトの管理者"
- "連盟管理者"
- "連盟ビューア"
- "バックアップとリカバリの管理者"
- "バックアップビューア"
- "管理者を復元"
- "クローン管理者"
- "災害復旧管理者"
- "災害復旧フェイルオーバー管理者"
- "災害復旧アプリケーション管理者"
- "災害復旧ビューア"
- "オペレーションサポートアナリスト"
- "分類ビューア"

"定義済みロールの詳細"

## パートナーユーザーに役割を追加する

メンバーにロールを追加することで、組織のリソースへのアクセス権を付与します。ロールを割り当てるときは、リソースとロールを 1 つずつ指定します。ユーザーに複数のロールを割り当てることができます。

たとえば、2 つのプロジェクトがあり、同じユーザーに両方のバックアップおよびリカバリ管理者のロールを付与したい場合は、各プロジェクトのユーザーにロールを提供する必要があります。同様に、同じプロジェクトに対してユーザーに 2 つの異なるロールを提供する場合は、各ロールを個別に割り当てる必要があります。

### 手順

1. *管理 > IDとアクセス*を選択します。
2. *パートナーシップ*を選択します。
3. *パートナーシップ開始*タブを選択します。
4. アクションメニューを選択 ••• 表示する確立されたパートナーシップの横にある をクリックし、[詳細を表示] を選択します。

   メンバー リストには、パートナー組織がパートナーシップに追加したメンバーが表示されます。

5. アクションメニューを選択 ••• 役割を割り当てるメンバーの横にある をクリックし、[役割の追加] を選択します。
6. ロールを追加するには、ダイアログ ボックスの手順を完了します。
   - 組織、フォルダ、またはプロジェクトを選択: メンバーに権限を与えるリソース階層のレベルを選択します。

     組織またはフォルダを選択した場合、メンバーにはその組織またはフォルダ内に存在するすべてのものに対する権限が付与されます。

   - カテゴリを選択: 役割のカテゴリを選択します。"アクセスロールについて学ぶ" 。
   - *ロール*を選択: 選択した組織、フォルダ、またはプロジェクトに関連付けられているリソースに対する権限をメンバーに付与するロールを選択します。
   - ロールの追加: 組織内の追加のフォルダーまたはプロジェクトへのアクセス権を付与する場合は、*ロールの追加*を選択し、別のフォルダーまたはプロジェクトまたはロールのカテゴリを指定してから、ロールのカテゴリと対応するロールを選択します。
7. *新しいロールを追加*を選択します。

## パートナーユーザーの役割を変更または削除する

パートナー組織のメンバーに割り当てたロールを変更または削除できます。

### 手順

1. *管理 > IDとアクセス*を選択します。
2. *パートナーシップ*を選択します。
3. *パートナーシップ開始*タブを選択します。
4. アクションメニューを選択 ••• 表示する確立されたパートナーシップの横にある をクリックし、[詳細を表示] を選択します。

メンバー リストには、パートナー組織がパートナーシップに追加したメンバーが表示されます。

5. *メンバー*ページで、テーブル内のメンバーに移動し、次に、[詳細を表示] を選択します。
6. 表で、メンバーに割り当てられたロールを変更する組織、フォルダ、またはプロジェクトのそれぞれの行を展開し、「ロール」列で「表示」を選択して、このメンバーに割り当てられているロールを表示します。
7. メンバーの既存の役割を変更したり、役割を削除したりできます。
   a. メンバーの役割を変更するには、変更したい役割の横にある「変更」を選択します。ロールを変更できるのは、同じロール カテゴリ内のロールのみです。たとえば、あるデータ サービス ロールから別のデータ サービス ロールに変更できます。変更を確認します。
   b. メンバーの役割の割り当てを解除するには、 をクリックすると、メンバーから該当するロールが削除されます。削除の確認を求められます。

## パートナー組織で働く

### パートナー組織でロールが付与されると、その組織に切り替えて、実行権限があるアクションを実行できるようになります。

組織メニューを使用して、自分の組織とアクセス権を持つパートナー組織を切り替えることができます。"組織とプロジェクトの切り替えについて詳しく学びます。"

パートナー組織内で共有されているリソースを確認し、割り当てられたロールに基づいてアクションを実行できるようになります。パートナーシップ管理者と協力して、アクセスする必要があるリソースに対して適切なロールがあることを確認してください。

# NetApp Consoleの操作を監視する

### コンソールが実行している操作のステータスを監視して、対処する必要がある問題があるかどうかを確認できます。監査ページや通知センターからステータスを確認したり、電子メールに通知を送信したりすることができます。

この表では、監査ページと通知センターの機能を比較して詳しく説明しています。

| 通知センター | 監査ページ |
| --- | --- |
| イベントとアクションの高レベルのステータスを表示します | さらなる調査のために各イベントまたはアクションの詳細を提供します |
| 現在のログイン セッションのステータスを表示します (ログオフ後は通知センターに情報は表示されません) | 過去1か月間のステータスを維持 |
| ユーザーインターフェースで開始されたアクションのみを表示します | UI または API からのすべてのアクションを表示します |
| ユーザーが開始したアクションを表示します | ユーザーが開始したものかシステムが開始したものかを問わず、すべてのアクションを表示します |
| 重要度で結果をフィルタリング | サービス、アクション、ユーザー、ステータスなどでフィルタリング |

| 通知センター | 監査ページ |
| --- | --- |
| ユーザーや他のユーザーに電子メール通知を送信する機能を提供します | メール機能なし |

## 監査ページからユーザーアクティビティを監査する

監査ページを使用して、アクションを実行したユーザーやそのステータスを識別します。

監査ページには、ユーザーが組織またはアカウントを管理するために実行したアクションが表示されます。これには、ユーザーの関連付け、システムの作成、エージェントの作成などの管理アクションが含まれます。

組織にメンバーを追加したユーザーや、プロジェクトが正常に削除されたかどうかを確認することもできます。

手順

1. *管理 > 監査*を選択します。
2. 表の上にあるフィルターを使用して、表に表示されるアクションを変更します。

   たとえば、サービス フィルターを使用して特定のサービスに関連するアクションを表示したり、ユーザー フィルターを使用して特定のユーザー アカウントに関連するアクションを表示したりできます。

### 監査ページから監査ログをダウンロードする

監査ページから監査ログを CSV ファイルにダウンロードできます。これにより、組織内でユーザーが実行するアクションを記録できるようになります。 CSV ファイルには、監査ページのフィルターや表示されている列に関係なく、ダウンロードした CSV ファイルのすべての列が含まれます。

手順

1. *監査*ページで、テーブルの右上隅にあるダウンロード アイコンを選択します。

## 通知センターを使用してアクティビティを監視する

通知はコンソールの操作を追跡して成功を確認します。これらを使用すると、現在のログイン セッション中に開始した多くのコンソール アクションのステータスを表示できます。すべてのコンソール サービスが通知センターに情報を報告するわけではありません。

通知ベル（  ）をクリックします。ベル内の小さなバブルの色は、アクティブな最高レベルの重大度通知を示します。したがって、赤いバブルが表示された場合は、確認する必要がある重要な通知があることを意味します。

また、特定の種類の通知を電子メールで送信するようにコンソールを構成することもできます。これにより、システムにログインしていない場合でも重要なシステム アクティビティについて通知を受けることができます。電子メールは、組織に属するすべてのユーザー、または特定の種類のシステム アクティビティを認識する必要があるその他の受信者に送信できます。方法を見るメール通知設定を設定する。

### 通知センターとアラートの比較

通知センターを使用すると、開始した操作のステータスを表示したり、特定の種類のシステム アクティビティに関するアラート通知を設定したりできます。一方、アラートを使用すると、容量、可用性、パフォーマン

ス、保護、セキュリティに関連するONTAPストレージ環境の問題や潜在的なリスクを確認できます。

"NetApp Consoleアラートの詳細"

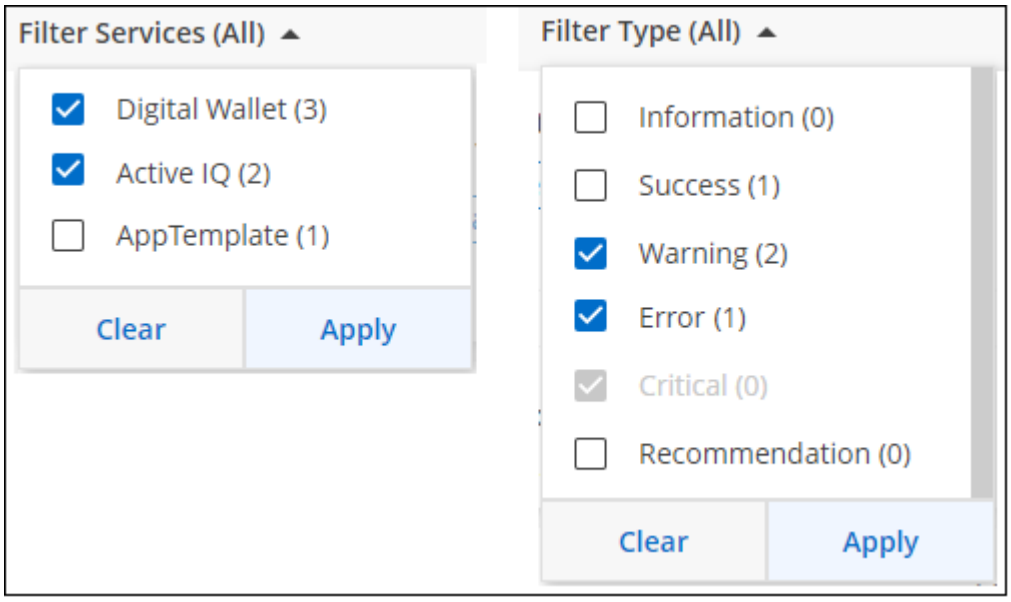
通知タイプ

コンソールは通知を次のカテゴリに分類します。

| 通知の種類 | 説明 |
| --- | --- |
| 致命的 | 問題が発生しており、すぐに対処しないとサービスが停止する可能性があります。 |
| エラー | アクションまたはプロセスは失敗して終了しました。または、修正アクションが実行されないと、失敗につながる可能性があります。 |
| 警告 | 重大な重大度に達しないように注意する必要がある問題。この重大度の通知ではサービスの中断は発生しないため、即時の修正アクションは必要ない可能性があります。 |
| 推奨事項 | システムまたは特定のサービスを改善するためのアクションを実行するためのシステム推奨事項。例: コスト削減、新しいサービスの提案、推奨されるセキュリティ構成など。 |
| 情報 | アクションまたはプロセスに関する追加情報を提供するメッセージ。 |
| 成功 | アクションまたはプロセスが正常に完了しました。 |

通知をフィルタリングする

デフォルトでは、すべてのアクティブな通知が通知センターに表示されます。表示される通知をフィルタリングして、自分にとって重要な通知だけを表示することができます。 「サービス」と通知の「タイプ」でフィルタリングできます。




たとえば、コンソール操作の「エラー」と「警告」の通知のみを表示する場合は、それらのエントリを選択すると、それらの種類の通知のみが表示されます。

## 通知を閉じる

通知を表示する必要がなくなった場合は、ページから通知を削除できます。通知は個別に、または一度にすべて閉じることができます。

すべての通知を閉じるには、通知センターで[すべて閉じる]を選択します。

個々の通知を閉じるには、通知の上にカーソルを移動し、[閉じる] を選択します。

## メール通知設定を設定する

特定の種類の通知を電子メールで送信できるため、ログインしていないときでも重要なシステム アクティビティについて通知を受けることができます。電子メールは、組織またはアカウントに属するすべてのユーザー、または特定の種類のシステム アクティビティを認識する必要があるその他の受信者に送信できます。

- コンソールは、エージェント、ライセンスとサブスクリプション、 NetApp Copy and Sync、およびNetApp Backup and Recoveryに関する電子メール通知を送信します。
- コンソール エージェントがインターネットにアクセスできないサイトにインストールされている場合、電子メール通知の送信はサポートされません。

通知センターで設定したフィルターによって、電子メールで受信する通知の種類が決まるわけではありません。デフォルトでは、すべての組織管理者はすべての「重要」および「推奨事項」通知のメールを受信します。これらの通知はすべてのサービスに渡されるため、エージェントやNetApp Backup and Recoveryなどの特定のサービスについてのみ通知を受信するように選択することはできません。

他のすべてのユーザーと受信者は通知メールを受信しないように設定されているため、追加のユーザーに対して通知設定を構成する必要があります。

通知設定をカスタマイズするには、組織管理者の役割が必要です。

### 手順

1. *管理 > 通知設定*を選択します。
2. *組織ユーザー*または*追加の受信者*を選択します。

   追加の受信者 ページでは、コンソール組織のメンバーである人々に通知するようにコンソールを設定できます。

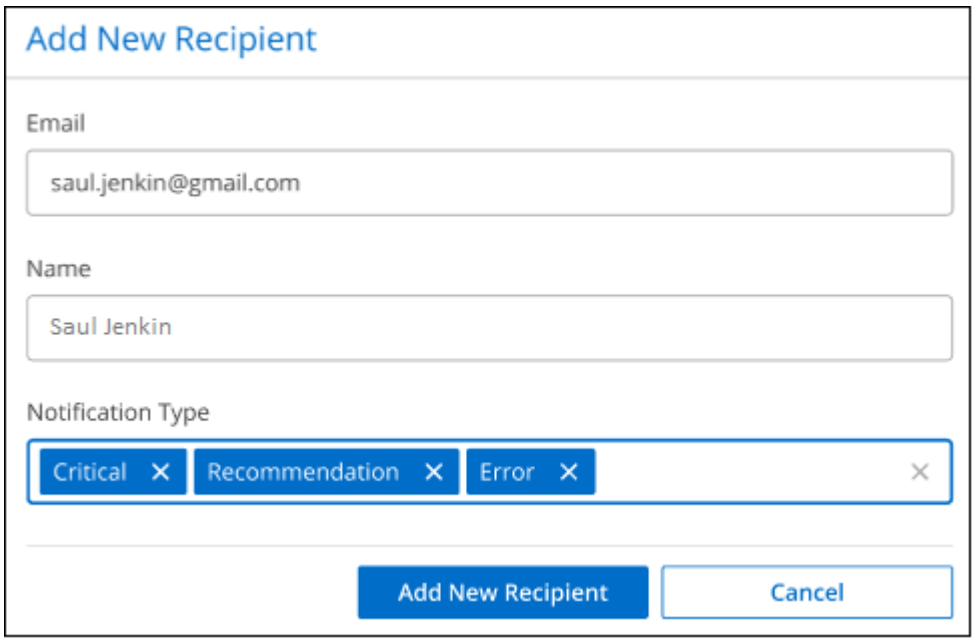
3. 組織ユーザー ページまたは 追加受信者 ページから 1 人または複数のユーザーを選択し、送信する通知の種類を選択します。
   - 1 人のユーザーに対して変更を行うには、そのユーザーの [通知] 列のメニューを選択し、送信する通知の種類をチェックして、[適用] を選択します。
   - 複数のユーザーに対して変更を行うには、各ユーザーのボックスをオンにし、「電子メール通知の管理」を選択し、送信する通知の種類をオンにして、「適用」を選択します。

## 追加のメール受信者を追加する

組織ユーザー ページに表示されるユーザーは、組織またはアカウント内のユーザーから自動的に入力されます。コンソールへのアクセス権を持たないが、特定の種類のアラートや通知について通知を受ける必要がある他のユーザーまたはグループの電子メール アドレスを [追加の受信者] ページに追加できます。

手順

1. *通知設定*ページから、*新しい受信者を追加*を選択します。




2. 名前、メールアドレスを入力し、受信者が受信する通知の種類を選択して、「新しい受信者を追加」を選択します。