始めましょう

NetApp Console setup and administration

NetApp
February 11, 2026

目次

始めましょう 1
基本を学ぶ 1
NetApp Consoleについて学ぶ 1
NetApp Consoleの導入モードについて学ぶ 4
NetApp Consoleに関連付けられたNSS資格情報を管理する 11
NetApp Consoleエージェントについて学ぶ 15
NetApp Consoleのアイデンティティとアクセス管理について学ぶ 19
NetApp Console（SaaS）を使い始める 24
開始ワークフロー（SaaS） 24
NetApp Consoleのネットワークアクセスを準備する 25
NetApp Consoleにサインアップまたはログイン 27
NetApp Consoleアシスタントの使用を開始する 29
NetApp Consoleの使用を開始する (制限モード) 29
開始ワークフロー（制限モード） 29
制限モードでの展開の準備 30
制限モードでコンソールエージェントを展開する 52
NetApp Intelligent Servicesにサブスクライブする（制限モード） 64
次にできること（制限モード） 70
プライベートモードを始める 71
開始ワークフロー（BlueXPプライベートモード） 71

始めましょう

基本を学ぶ

NetApp Consoleについて学ぶ

コンソールは、統合データ サービスを使用してハイブリッド マルチクラウド全体のストレージ管理と保護を統合し、データを保護および最適化します。

これは、サービス (SaaS) プラットフォームとして、または独自のクラウドにインストールできるセルフホスト オプションとして利用できます。ストレージ管理、データの移動、データ保護、データ分析と制御を提供します。管理機能は、 Webベースのコンソールと API を通じて提供されます。

集中ストレージ管理

コンソールを使用して、クラウドおよびオンプレミスのストレージを検出、展開、管理します。

サポートされているクラウドおよびオンプレミスのストレージ

コンソールから次の種類のストレージを管理できます。

クラウドストレージソリューション

- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Google Cloud NetApp Volumes

オンプレミスのフラッシュとオブジェクトストレージ

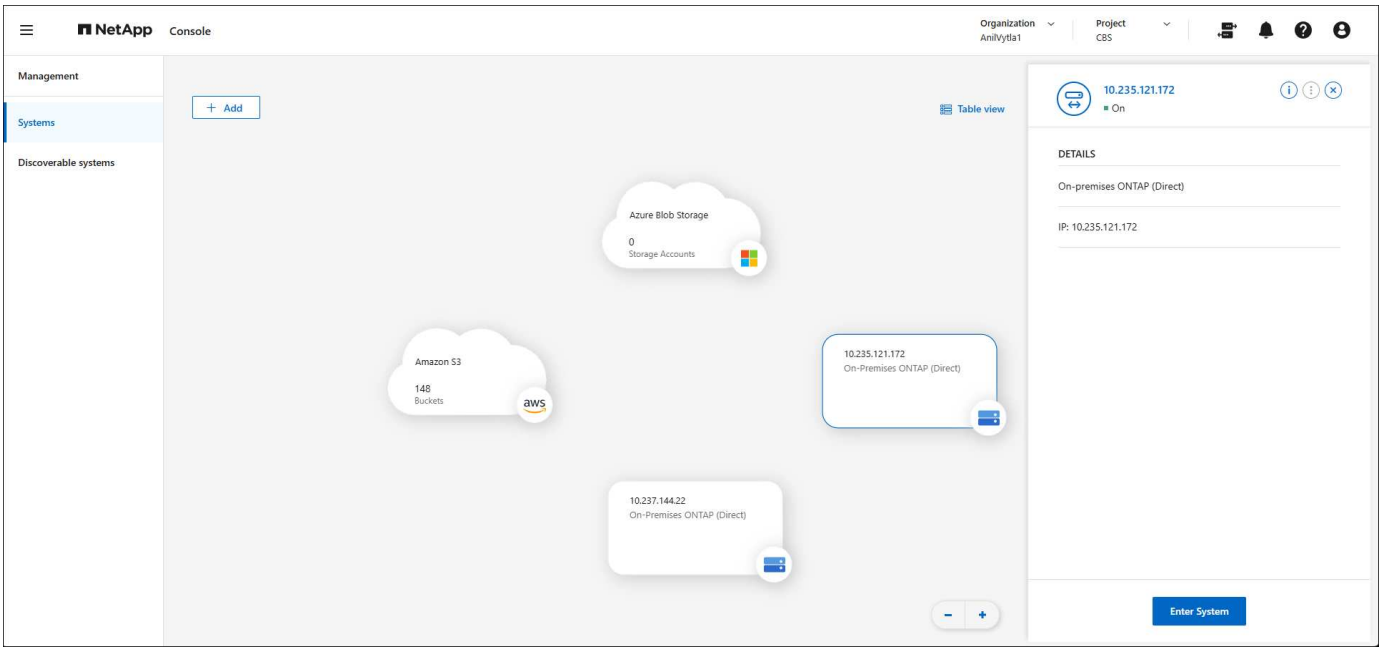
- Eシリーズシステム
- ONTAPクラスタ
- StorageGRIDシステム

クラウドオブジェクトストレージ

- Amazon S3 ストレージ
- Azure BLOB ストレージ
- Google Cloud Storage

ストレージ管理

コンソール内では、システム は検出または展開されたストレージを表します。システムを選択して、 NetApp データ サービスと統合したり、ボリュームの追加などのストレージを管理したりできます。



データの保護、セキュリティ確保、最適化のための統合データサービスとストレージ管理

コンソールは、ストレージの可用性を確保し維持するためのデータ サービスを提供します。

ストレージアラート
: ONTAP環境の容量、可用性、パフォーマンス、保護、セキュリティに関連する問題を表示します。

自動化ハブ
: スクリプト ソリューションを使用して、 NetApp製品とサービスの導入と統合を自動化します。

NetApp Backup and Recovery
: クラウドとオンプレミスのデータをバックアップおよび復元します。

NetApp Data Classification
: アプリケーション データとクラウド環境のプライバシーを準備します。

NetApp Copy and Sync
: オンプレミスとクラウド データ ストア間でデータを同期します。

NetAppデジタルアドバイザー (Active IQ)
: 予測分析とプロアクティブなサポートを使用して、データ インフラストラクチャを最適化します。

Licenses and subscriptions
: ライセンスとサブスクリプションを管理および監視します。

NetApp Disaster Recovery
: VMware Cloud on Amazon FSx for ONTAPを災害復旧サイトとして使用して、オンプレミスの VMware ワークロードを保護します。

ライフサイクルプランニング
: 現在または予測される容量が低いクラスターを特定し、データ階層化または追加容量の推奨事項を実装し

ます。

NetApp Ransomware Resilience

ランサムウェア攻撃につながる可能性のある異常を検出します。ワークロードを保護および回復します。

NetApp Replication

バックアップと災害復旧をサポートするために、ストレージ システム間でデータを複製します。

ソフトウェアアップデート

ONTAPアップグレードの評価、計画、実行を自動化します。

サステナビリティダッシュボード

ストレージ システムの持続可能性を分析します。

NetApp Cloud Tiering

オンプレミスのONTAPストレージをクラウドに拡張します。

NetApp Volume Caching

書き込み可能なキャッシュ ボリュームを作成して、データへのアクセスを高速化したり、頻繁にアクセスされるボリュームのトラフィックを軽減したりします。

NetAppワークロード

Amazon FSx for NetApp ONTAPを使用して主要なワークロードを設計、セットアップ、運用します。

"NetApp Consoleと利用可能なデータサービスの詳細"

サポートされているクラウドプロバイダー

コンソールを使用すると、クラウド ストレージを管理し、Amazon Web Services、Microsoft Azure、Google Cloud のクラウド サービスを使用できます。

料金

NetApp Consoleは無料です。クラウドにコンソール エージェントを展開したり、クラウドに展開された制限モードを使用したりする場合は、コストが発生します。一部のNetAppデータ サービスにはコストがかかります。https://bluexp.netapp.com/pricing["NetAppデータサービスの価格について"^]

NetApp Consoleの仕組み

NetApp Consoleは、SaaS レイヤー、リソースおよびアクセス管理システム、ストレージ システムを管理してNetAppデータ サービスを有効にするコンソール エージェント、およびビジネス要件を満たすさまざまな導入モードを通じて提供される Web ベースのコンソールです。

サービスとしてのソフトウェア

コンソールにアクセスするには "ウェブベースのインターフェース"および API。この SaaS エクスペリエンスにより、最新機能がリリースされると自動的にアクセスできるようになります。

アイデンティティとアクセス管理（**IAM**）

コンソールは、リソースとアクセス管理のための ID およびアクセス管理 (IAM) を提供します。この IAM モデ

ルは、リソースと権限のきめ細かな管理を提供します。

- トップレベルの組織を使用すると、さまざまなプロジェクト間のアクセスを管理できます。
- _フォルダ_を使用すると、関連するプロジェクトをグループ化できます
- リソース管理では、リソースを1つ以上のフォルダまたはプロジェクトに関連付けることができます。
- アクセス管理により、組織階層のさまざまなレベルのメンバーに役割を割り当てることができます。
- "NetApp ConsoleのIAMの詳細"

コンソールエージェント

いくつかの追加機能およびデータ サービスには、コンソール エージェントが必要です。オンプレミスとクラウド環境全体のリソースとプロセスを管理できます。一部のシステム (Cloud Volumes ONTAPなど) を管理し、一部のNetAppデータ サービスを使用するために必要です。

"コンソールエージェントの詳細" 。

SaaS とソブリンクラウドの展開

NetApp Consoleの使用を開始するには、SaaS オファリングにサインアップするか、独自のクラウドに導入します。NetApp Consoleをソブリン クラウドに導入すると、 NetApp は組織のセキュリティとコンプライアンスの要件を満たすためにアウトバウンド接続を制限します。コンソールがソブリン クラウドにデプロイされている場合、すべての機能とサービスが利用できるわけではありません。

NetApp は、アウトバウンド接続を望まないサイト向けにBlueXP を引き続き提供します。BlueXP は、アウトバウンド接続なしでネットワークにインストールできます。 "インターネットに接続できないサイト向けのBlueXP (プライベート モード) について説明します。"

"展開モードの詳細" 。

SOC 2 タイプ**2**認証

独立した公認会計士事務所とサービス監査人がコンソールを検査し、該当する Trust Services 基準に基づいて SOC 2 タイプ 2 レポートを達成したことを確認しました。

"NetAppのSOC 2レポートを見る"

NetApp Consoleの導入モードについて学ぶ

NetApp Consoleは、ビジネス要件とセキュリティ要件を満たす複数の 導入モード を提供します。

- 標準モード では、サービスとしてのソフトウェア (SaaS) レイヤーを活用して完全な機能を提供します。ユーザーはWebベースのホストインターフェースを通じてコンソールにアクセスします。
- 制限モード は、接続制限があり、 NetApp Consoleを独自のパブリック クラウドにインストールしたい組織で利用できます。ユーザーは、クラウド環境内のコンソール エージェントでホストされている Web ベースのインターフェースを通じてコンソールにアクセスします。

  NetApp Consoleは制限モードでトラフィック、通信、データを制限するため、環境 (オンプレミスおよびクラウド) が必要な規制に準拠していることを確認する必要があります。

概要

各展開モードでは、アウトバウンド接続、場所、インストール、認証、データ サービス、課金方法が異なります。

標準モード

Web ベースのコンソールから SaaS サービスを使用します。使用する予定のデータ サービスと機能に応じて、コンソール組織管理者は、ハイブリッド クラウド環境内のデータを管理するための 1 つ以上のコンソール エージェントを作成します。

このモードでは、パブリックインターネット経由で暗号化されたデータ転送が使用されます。

制限モード

コンソール エージェントをクラウド（政府、主権、または商業地域）にインストールし、 NetApp ConsoleSaaS レイヤーへの送信接続が制限されます。

このモードは通常、州政府や地方自治体、規制対象企業によって使用されます。

SaaS レイヤーへのアウトバウンド接続の詳細 。

BlueXPプライベート モード **(**従来の**BlueXP**インターフェイスのみ**)**

BlueXPプライベート モード (レガシーBlueXPインターフェイス) は通常、インターネット接続がなく、AWS Secret Cloud、AWS Top Secret Cloud、Azure IL6 などの安全なクラウド領域があるオンプレミス環境で使用されます。 NetApp は、従来のBlueXPインターフェースを使用してこれらの環境を引き続きサポートします。"BlueXPプライベートモードの PDF ドキュメント"

次の表は、 NetAppコンソールの比較を示しています。

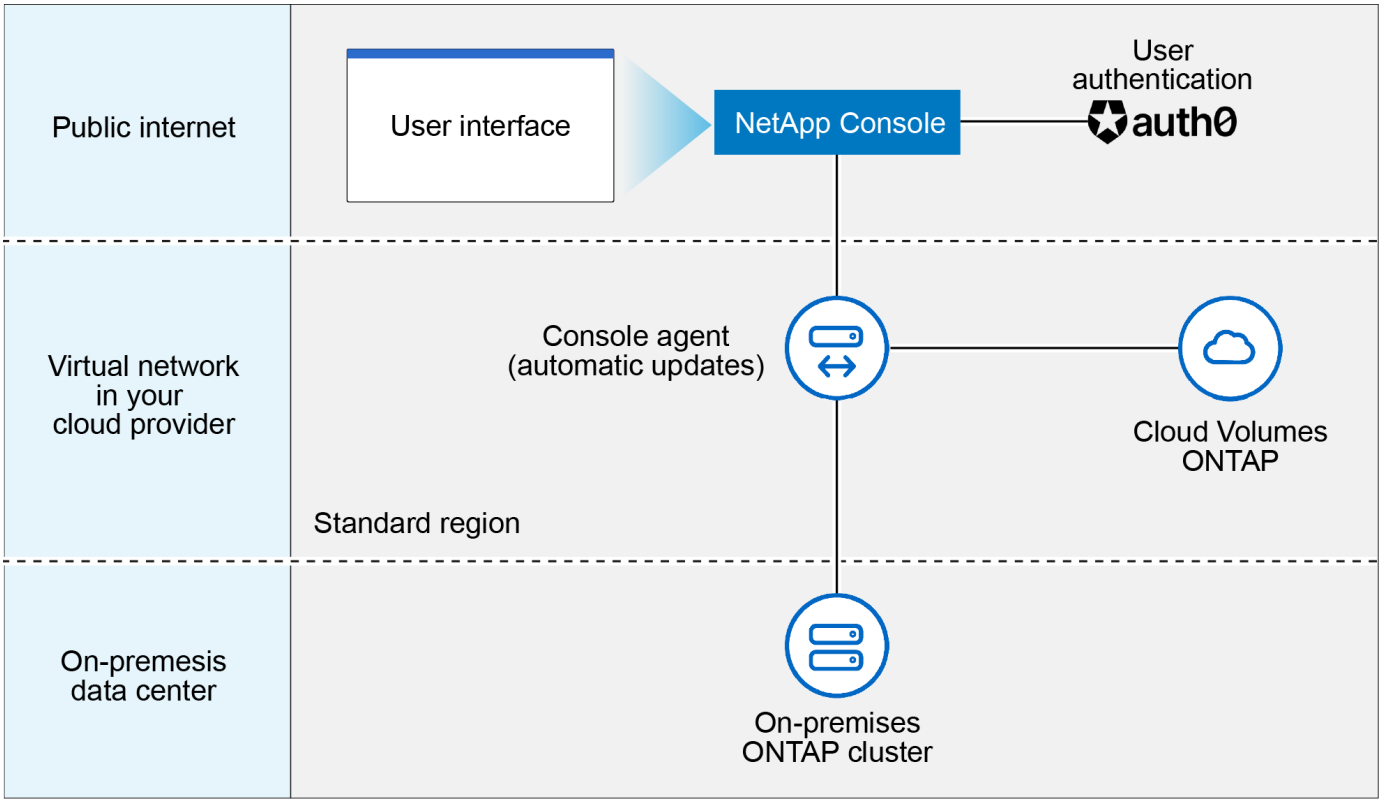
	標準モード	制限モード
NetApp ConsoleSaaS レイヤーへの接続が必要ですか**?**	はい	発信のみ
クラウド プロバイダーへの接続が必要ですか**?**	はい	はい、地域内です
コンソールエージェントのインストール	コンソール、クラウドマーケットプレイス、または手動インストールから	クラウドマーケットプレイスまたは手動インストール
コンソールエージェントのアップグレード	自動アップグレード	自動アップグレード
UIアクセス	コンソールSaaSレイヤーから	エージェントVMからローカルに
APIエンドポイント	コンソールSaaSレイヤー	コンソールエージェント
認証	auth0、NSSログイン、またはIDフェデレーションを使用したSaaS経由	auth0またはIDフェデレーションを使用したSaaSを通じて
多要素認証	ローカルユーザーが利用可能	使用不可
ストレージおよびデータサービス	すべてサポートされています	多くが支持されている

	標準モード	制限モード
データサービスライセンスオプション	マーケットプレイスのサブスクリプションとBYOL	マーケットプレイスのサブスクリプションとBYOL

サポートされているNetApp Consoleの機能とサービスなど、これらのモードの詳細については、次のセクションをお読みください。

標準モード

次の画像は標準モードの展開の例です。



コンソールは標準モードでは次のように動作します。

アウトバウンドコミュニケーション

コンソール エージェントからコンソール SaaS レイヤー、クラウド プロバイダーの公開リソース、および日常の運用に不可欠なその他のコンポーネントへの接続が必要です。

- "AWS でエージェントが接続するエンドポイント"
- "Azure でエージェントが接続するエンドポイント"
- "Google Cloud でエージェントが接続するエンドポイント"

エージェントがサポートされる場所

標準モードでは、エージェントはクラウドまたはオンプレミスでサポートされます。

コンソールエージェントのインストール

次のいずれかの方法でエージェントをインストールできます。

- コンソールから
- AWS または Azure Marketplace から
- Google Cloud SDKから
- データセンターまたはクラウド内の Linux ホストでインストーラーを手動で使用する
- 提供された OVA を VCenter 環境で使用します。

コンソールエージェントのアップグレード

NetApp はエージェントを毎月自動的にアップグレードします。

ユーザーインターフェースアクセス

ユーザー インターフェイスには、SaaS レイヤーを通じて提供される Web ベースのコンソールからアクセスできます。

APIエンドポイント

API呼び出しは次のエンドポイントに対して行われます: https://api.bluexp.netapp.com

認証

auth0 またはNetAppサポート サイト (NSS) ログインによる認証。アイデンティティ連携が利用可能です。

サポートされているデータサービス

すべてのNetAppデータ サービスがサポートされています。"NetAppデータサービスの詳細" 。

サポートされているライセンスオプション

マーケットプレイスのサブスクリプションと BYOL は標準モードでサポートされていますが、サポートされるライセンス オプションは使用しているNetAppデータ サービスによって異なります。利用可能なライセンス オプションの詳細については、各サービスのドキュメントを確認してください。

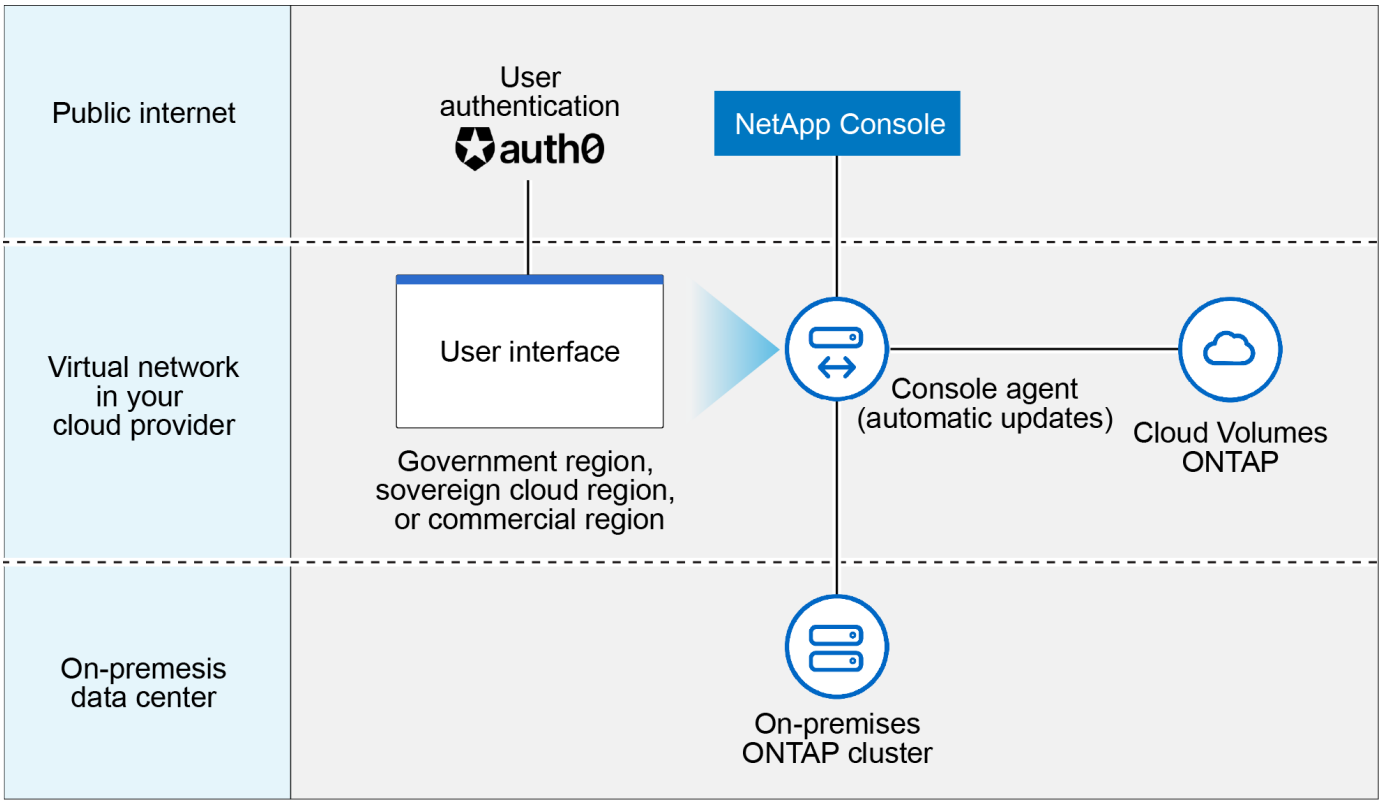
標準モードの開始方法

に行く "NetApp Console"そしてサインアップしてください。

"標準モードの開始方法を学ぶ" 。

制限モード

次の画像は、制限モードの展開の例です。



制限モードではコンソールは次のように動作します。

アウトバウンドコミュニケーション

エージェントは、データ サービス、ソフトウェア アップグレード、認証、メタデータの転送のために、コンソール SaaS レイヤーへの送信接続を必要とします。

コンソール SaaS レイヤーはエージェントへの通信を開始しません。エージェントは、コンソール SaaS レイヤーとのすべての通信を開始し、必要に応じてデータをプルまたはプッシュします。

リージョン内からクラウド プロバイダー リソースへの接続も必要です。

エージェントがサポートされる場所

制限モードでは、エージェントはクラウド（政府リージョン、主権リージョン、または商用リージョン）でサポートされます。

コンソールエージェントのインストール

AWS または Azure Marketplace からインストールすることも、独自の Linux ホストに手動でインストールすることも、VCenter 環境でダウンロード可能な OVA を使用することもできます。

コンソールエージェントのアップグレード

NetApp は、毎月のアップデートでエージェント ソフトウェアを自動的にアップグレードします。

ユーザーインターフェースアクセス

ユーザー インターフェースには、クラウド リージョンにデプロイされたエージェント仮想マシンからアクセスできます。

APIエンドポイント

API 呼び出しはエージェント仮想マシンに対して行われます。

認証

認証は auth0 を通じて提供されます。アイデンティティフェデレーションも利用可能です。

サポートされているストレージ管理およびデータサービス

制限モードの次のストレージおよびデータ サービス:

サポートされているサービス	注記
Azure NetApp Files	完全サポート
バックアップとリカバリ	制限モードの政府地域および商用地域でサポートされます。制限モードの主権地域ではサポートされません。制限モードでは、 NetApp Backup and Recovery はONTAPボリューム データのみのバックアップと復元をサポートします。 "ONTAPデータのサポートされているバックアップ先のリストを表示します"アプリケーション データおよび仮想マシン データのバックアップと復元はサポートされていません。
NetApp Data Classification	制限モードの政府地域でサポートされます。商用地域または制限モードのソブリン地域ではサポートされません。
Cloud Volumes ONTAP	完全サポート
Licenses and subscriptions	制限モードでサポートされている以下のライセンス オプションを使用して、ライセンスおよびサブスクリプション情報にアクセスできます。
オンプレミスのONTAPクラスタ	コンソール エージェントを使用した検出とコンソール エージェントを使用しない検出 (直接検出) の両方がサポートされています。コンソール エージェントなしでオンプレミス クラスターを検出する場合、詳細ビュー (システム マネージャー) はサポートされません。
レプリケーション	制限モードの政府地域でサポートされます。商用地域または制限モードのソブリン地域ではサポートされません。

サポートされているライセンスオプション

制限モードでは、次のライセンス オプションがサポートされています。

- マーケットプレイスのサブスクリプション（時間単位および年間契約）

  次の点に注意してください。

  - Cloud Volumes ONTAPの場合、容量ベースのライセンスのみがサポートされます。
  - Azure では、政府地域では年間契約はサポートされていません。

- BYOL

  Cloud Volumes ONTAPの場合、容量ベースのライセンスとノードベースのライセンスの両方が BYOL でサポートされます。

制限モードの開始方法

NetApp Console組織を作成するときに、制限モードを有効にする必要があります。

まだ組織がない場合は、手動でインストールした、またはクラウド プロバイダーのマーケットプレイスから作成したコンソール エージェントから初めてコンソールにログインするときに、組織を作成して制限モードを有効にするように求められます。

組織を作成した後は、制限モード設定を変更することはできません。

"制限モードの開始方法を学ぶ" 。

サービスと機能の比較

次の表は、制限モードでサポートされているサービスと機能をすぐに識別するのに役立ちます。

一部のサービスは制限付きでサポートされる場合がありますのでご了承ください。これらのサービスが制限モードでどのようにサポートされるかの詳細については、上記のセクションを参照してください。

製品分野	**NetApp**データサービスまたは機能	制限モード
ストレージ 表のこの部分には、コンソールからのストレージ システム管理のサポートがリストされています。 NetApp Backup and Recoveryでサポートされているバックアップ先は示されません。	Amazon FSx for ONTAP	いいえ
	Amazon S3	いいえ
	Azure ブロブ	いいえ
	Azure NetApp Files	はい
	Cloud Volumes ONTAP	はい
	Google Cloud NetApp Volumes	いいえ
	Google Cloud Storage	いいえ
	オンプレミスのONTAPクラスタ	はい
	Eシリーズ	いいえ
	StorageGRID	いいえ

製品分野	**NetApp**データサービスまたは機能	制限モード
データサービス	NetAppバックアップとリカバリ	はいhttps://docs.netapp.com/us-en/data-services-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-limited-internet-connectivity["ONTAPボリュームデータのサポートされているバックアップ先のリストを表示します"^]
	NetApp Data Classification	はい
	NetApp Copy and Sync	いいえ
	NetApp Disaster Recovery	いいえ
	NetApp Ransomware Resilience	いいえ
	NetApp Replication	はい
	NetApp Cloud Tiering	いいえ
	NetAppボリュームキャッシュ	いいえ
	NetAppワークロード ファクトリー	いいえ
特徴	アラート	いいえ
	Digital Advisor	いいえ
	ライセンスとサブスクリプションの管理	はい
	アイデンティティとアクセス管理	はい
	Credentials	はい
	フェデレーション	はい
	ライフサイクルプランニング	いいえ
	多要素認証	はい
	NSSアカウント	はい
	通知	はい
	検索	はい
	ソフトウェアアップデート	いいえ
	持続可能性	いいえ
	監査	はい

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

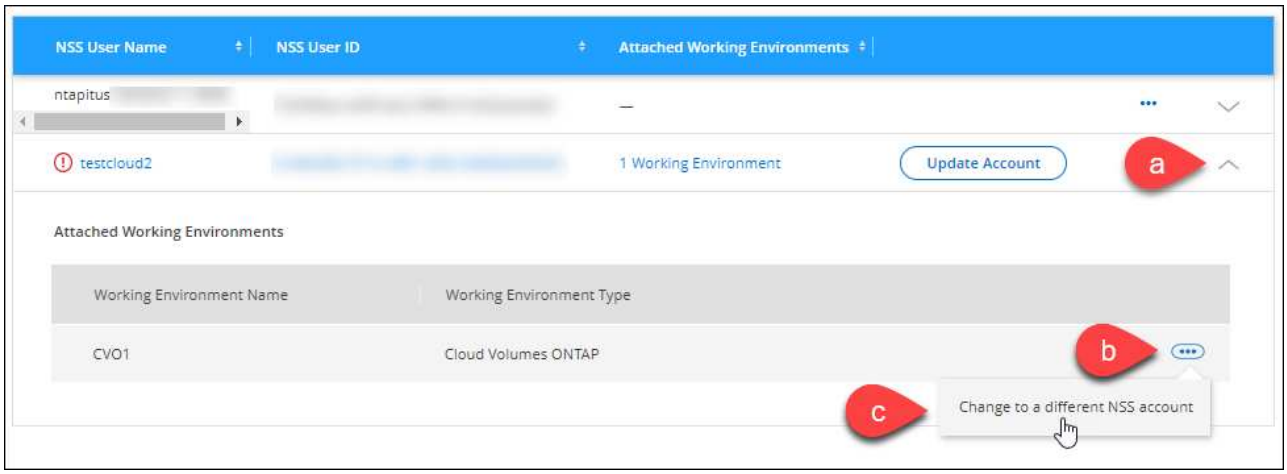
組織に複数のNetAppサポート サイト アカウントがある場合は、 Cloud Volumes ONTAPシステムに関連付けるアカウントを変更できます。

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

	エージェントで利用可能	エージェントなしで利用可能
StorageGRIDシステム	はい	いいえ
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。

NetApp Consoleのアイデンティティとアクセス管理について学ぶ

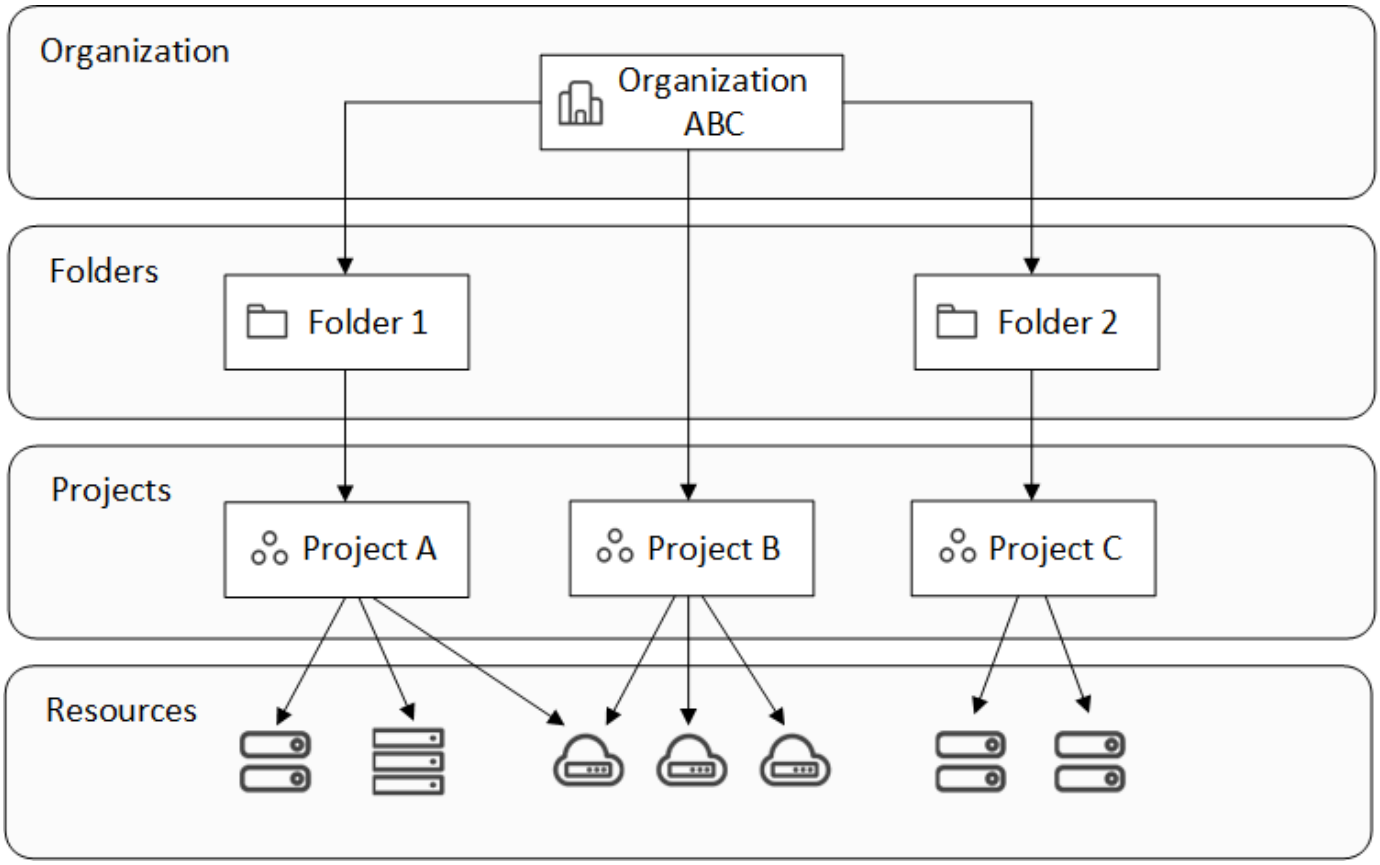
NetAppコンソールの ID およびアクセス管理 (IAM) を使用して、 NetAppリソースを整理し、場所、部門、プロジェクトなどのビジネス構造に応じてアクセスを制御します。

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（SaaS）を使い始める

開始ワークフロー（SaaS）

NetApp Console(SaaS) の使用を開始するには、コンソールのネットワークを準備し、サインアップしてアカウントを作成し、コンソール アシスタントを使用して初期機能を設定します。

NetAppの Software-as-a-service (SaaS) 製品としてホストされているWebベースのコンソールにアクセスします。コンソールを使用して、ハイブリッド クラウド ストレージ環境を管理し、 NetAppデータ サービスを使用できます。

"NetAppコンソールを使用するためのネットワークの準備"

NetAppコンソールにアクセスするコンピューターが必要なエンドポイントにネットワーク アクセスできることを確認します。

"NetAppコンソールのネットワークを準備する方法を学びます。"

"サインアップして組織を作成する"

に行く "NetAppコンソール" そしてサインアップしてください。組織を作成するように求められた場合、会社にすでに組織が存在すると思われる場合は、ダイアログ ボックスを閉じて、組織の管理者に連絡してください。現在、会社に組織管理者がいない場合は、この役割を申請できます。 "組織管理者に連絡する方法について説明します。"

この時点でログインしており、 NetAppアシスタントを使用してコンソールの構成を開始できます。まず、NetAppサポート アカウントとコンソール エージェントを関連付けて、完全な機能を有効にします。

NetAppアシスタントを使用しない、またはコンソール エージェントをインストールしない場合は、ストレージの管理を開始し、 Digital Advisor、 Amazon FSx for ONTAP、 Azure NetApp Filesなどのサービスを使用できます。"コンソールエージェントなしで何ができるかを学ぶ"。

NetApp Support Site（NSS）アカウントを関連付ける

NetApp Support Site(NSS) アカウントをコンソールに関連付けると、ライセンスとサブスクリプションをより簡単に管理できるだけでなく、コンソールから直接サポート リソースにアクセスできるようになります。

コンソールエージェントを作成する

高度なストレージ管理機能と一部のNetAppデータ サービスを使用するには、コンソール エージェントをインストールする必要があります。コンソール エージェントにより、コンソールはハイブリッド 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。

クラウドまたはオンプレミス ネットワークにコンソール エージェントを作成できます。

- "コンソールエージェントが必要な状況とその動作について詳しくは、"

- "AWS でコンソールエージェントを作成する方法を学ぶ"
- "Azure でコンソール エージェントを作成する方法を学びます"
- "Google Cloud でコンソール エージェントを作成する方法を学びます"
- "オンプレミスでコンソールエージェントを作成する方法を学ぶ"

5 コンソールにストレージシステムを追加する

NetApp Console内で、ストレージ システムを追加または検出して、ハイブリッド クラウド ストレージ環境を管理できます。NetAppアシスタントを使用して、最初のストレージ システムを追加します。

AWS、Microsoft Azure、または Google Cloud にコンソール エージェントをインストールすると、コンソールはエージェントがインストールされている場所にあるAmazon S3バケット、Azure Blob ストレージ、または Google Cloud Storage バケットに関する情報を自動的に検出します。これらのシステムは自動的に システム ページに追加されます。

- "ONTAPシステムの検出方法を学ぶ"
- "StorageGRIDシステムの検出方法を学ぶ"
- "Eシリーズ システムの発見方法を学ぶ"

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

クラウド プロバイダを通じて、時間単位 (PAYGO) または年額課金でNetApp Intelligent Servicesにサインアップします。サブスクリプションには、 NetApp Backup and Recovery、 Cloud Volumes ONTAP、 NetApp Cloud Tiering、 NetApp Ransomware Resilience、 NetApp Disaster Recovery、 NetApp Data Classificationが含まれます。

NetApp Consoleのネットワークアクセスを準備する

NetApp Console、 NetApp Consoleエージェント、およびNetAppデータ サービスには、アウトバウンド インターネット アクセスと、必要なエンドポイントに接続する機能が必要です。

次のネットワーク アクセスを設定する必要があります。

- NetApp Consoleに SaaS (Software as a Service) としてアクセスするコンピュータ
- オンプレミスまたはクラウドにインストールするコンソール エージェント。コンソールエージェント。

4.0.0 では、 NetApp はコンソールとコンソール エージェントに必要なネットワーク エンドポイントを削減し、セキュリティを強化して導入を簡素化しました。重要なのは、バージョン 4.0.0 より前のすべてのデプロイメントが引き続き完全にサポートされることです。以前のエンドポイントは既存のエージェントで引き続き使用できますが、 NetApp、エージェントのアップグレードが成功したことを確認した後、ファイアウォール ルールを現在のエンドポイントに更新することを強くお勧めします。"エンドポイント リストを更新する方法について説明します。"

NetApp Consoleおよびコンソールエージェントが接続するエンドポイント

導入する各エージェントとNetApp Consoleにアクセスする各コンピューターは、以下にリストされているエンドポイントに接続する必要があります。

クラウド プロバイダーに展開されているコンソール エージェントは、そのクラウド プロバイダーに対応するエンドポイントにアクセスできる必要があります。

エンドポイント	目的
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。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、 NetApp、ファイアウォール ルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

クラウドプロバイダーのエンドポイントがコンソールエージェントに接続しました

コンソール エージェントがクラウド プロバイダーに展開されている場合、追加のエンドポイントにアクセスできる必要があります。

コンソール エージェントをインストールする前に、クラウド プロバイダー ネットワーク エンドポイント アクセスを設定します。

- "コンソールエージェントの AWS ネットワークアクセスを設定する"
- "コンソール エージェントの Azure ネットワーク アクセスを設定する"
- "コンソール エージェントの Google Cloud 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接続するデータサービスエンドポイント

一部のNetAppデータ サービスとCloud Volumes ONTAP、エージェントに追加のアウトバウンド インターネット アクセスが必要です。

Cloud Volumes ONTAPのエンドポイント

- "AWS のCloud Volumes ONTAPのエンドポイント"
- "Azure のCloud Volumes ONTAPのエンドポイント"
- "Google Cloud のCloud Volumes ONTAPのエンドポイント"

ワークロードのエンドポイント

コンソール エージェントは、 NetAppワークロードの次のエンドポイントにアクセスできる必要があります。

エンドポイント	目的
https://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。

NetApp Consoleにサインアップまたはログイン

コンソールを使用するには、 NetApp Support Siteの認証情報を使用してサインアップまたはログインするか、 NetApp Consoleのログインを作成します。社内で最初にサインアップする場合は、管理者として新しい組織を作成します。会社にすでに組織がある場合は、既存のNetApp Support Siteの認証情報または会社のシングル サインオン (SSO) を使用してサインアップまたはログインします。

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。最初のユーザーは組織管理者となり、ユーザー アカウントと権限を管理します。後からロールを更新したり、管理者を追加したりすることもできます。

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。

+ 初めてのユーザーおよび組織管理者は、ガイド付きのプロセスに従ってストレージ リソースの追加、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。

NetApp Consoleアシスタントの使用を開始する

組織管理者ロールを持つNetApp Console(SaaS) を初めて使用する場合は、コンソール アシスタントを使用して初期セットアップ プロセスをガイドできます。アシスタントを使用すると、 NetApp Support Site(NSS) アカウントの追加、コンソール エージェントの追加、クラスターの追加、ライセンスまたはサブスクリプションの追加が可能になり、データの管理を簡単に開始できるようになります。

コンソールアシスタントにアクセスするために必要な役割

コンソール アシスタントは、組織管理者の役割を持つユーザーのみが利用できます。

デフォルトでは、 NetApp Consoleは、組織管理者ロールを持つ初めてのユーザーのホーム ページにコンソール アシスタントを表示します。コンソール エージェントの作成とシステムの追加という必須タスクが完了するまで、引き続き使用できます。

アシスタントを使用して次のタスクを完了します。これにより、 NetApp Console環境の最小限のセットアップが提供されます。

- NetAppサポート サイト (NSS) アカウントを追加します。

  "NSSアカウントを追加する方法を学ぶ"。

- コンソール エージェントを展開してストレージ エステートに接続します。

  "オンプレミスでコンソール エージェントをインストールする方法を学習します。"

- クラスターを追加または検出してストレージ システムを管理する
- マーケットプレイスのサブスクリプションまたは PAYGO ライセンスを追加します。

  "ライセンスとサブスクリプションを追加する方法を学ぶ"。

- データ サービス情報を確認します。

NetApp Consoleの使用を開始する (制限モード)

開始ワークフロー（制限モード）

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

制限モードは通常、AWS GovCloud および Azure Government リージョンでの展開を含む、州政府や地方自

治体、規制対象企業によって使用されます。始める前に、以下の点を理解しておいてください。"コンソールエージェント"そして"展開モード"。

1 "展開の準備"

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

2 "コンソールエージェントを展開する"

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

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

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

制限モードでの展開の準備

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

ステップ**1:** 制限モードの仕組みを理解する

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

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

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

"制限モードの仕組みを学ぶ" 。

ステップ**2:** インストールオプションを確認する

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

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

ステップ**3:** ホストの要件を確認する

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

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

専用ホスト

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

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

    エージェントは `/opt`インストールするには `/opt/application/netapp`ディレクトリとその内容。
  - `/var`: 40 GiBの空き容量が必要です

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

AWS EC2インスタンスタイプ

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

Azure VM サイズ

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

Google Cloud マシンタイプ

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

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

ハイパーバイザー

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

オペレーティングシステムとコンテナの要件

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

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

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

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

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

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

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

  サポートされているPodmanのバージョンを表示する 。

- Ubuntu には Docker Engine が必要です。

  サポートされている Docker エンジンのバージョンを表示する 。

例 **1.** 手順

ポッドマン

Podman をインストールして設定するには、次の手順に従います。

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

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

手順

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

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

2. Podman をインストールします。

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

   a. Red Hat Enterprise Linux 9.6 の場合:

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

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

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

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

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

   c. Red Hat Enterprise Linux 8 の場合:

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

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

3. podman.socket サービスを有効にして起動します。

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

4. python3 をインストールします。

```
sudo dnf install python3
```

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

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

6. Red Hat Enterprise 9 を使用している場合:

   a. EPEL リポジトリ パッケージをインストールします。

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

   +

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

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

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

   a. EPEL リポジトリ パッケージをインストールします。

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

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

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

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

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

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

```
podman info | grep networkBackend
```

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

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

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

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

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

v. podman を再起動します。

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

Dockerエンジン

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

手順

1. "Dockerからのインストール手順を見る"

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

2. Docker が有効になっていて実行されていることを確認します。

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

ステップ**5:** ネットワークアクセスを準備する

コンソール エージェントがパブリック クラウド内のリソースを管理できるように、ネットワーク アクセスを設定します。コンソール エージェント用の仮想ネットワークとサブネットがあることに加えて、次の要件が満たされていることを確認する必要があります。

ターゲットネットワークへの接続

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

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

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

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

+

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

日常業務のためのアウトバウンドインターネットアクセス

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

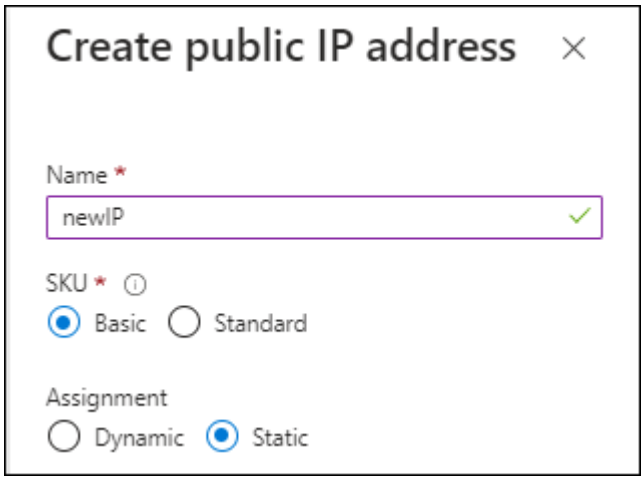
エンドポイント	目的
AWS 環境	AWS サービス (amazonaws.com): • クラウドフォーメーション • エラスティックコンピューティングクラウド (EC2) • アイデンティティとアクセス管理（IAM） • キー管理サービス (KMS) • セキュリティトークンサービス（STS） • シンプルストレージサービス（S3）
AWS リソースを管理します。エンドポイントは AWS リージョンによって異なります。 "詳細についてはAWSドキュメントを参照してください"	NetApp ONTAP用の Amazon FsX: • api.workloads.netapp.com
Web ベースのコンソールは、このエンドポイントに接続して Workload Factory API と対話し、FSx for ONTAPベースのワークロードを管理および操作します。	**Azure** 環境
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Azure パブリック リージョン内のリソースを管理します。
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	Azure Government リージョン内のリソースを管理します。
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Azure China リージョンのリソースを管理します。

エンドポイント	目的
Google Cloud 環境	https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://config.googleapis.com/v1/projects
Google Cloud 内のリソースを管理します。	• NetApp Consoleエンドポイント*
https://mysupport.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信します。
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェアアップデートを受信します。
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。

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

Azureのパブリック**IP**アドレス

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



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

"Azure ドキュメント: パブリック IP SKU"

プロキシ サーバ

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

- IPアドレス
- Credentials
- HTTPS証明書

ポート

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

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

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

NTP を有効にする

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

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

ステップ**6:** クラウド権限を準備する

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

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

AWS IAM ロール

IAM ロールを使用して、コンソール エージェントに権限を付与します。

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

独自の Linux ホストにコンソールエージェントを手動でインストールする場合は、ロールを EC2 インスタンスにアタッチします。

手順

1. AWS コンソールにログインし、IAM サービスに移動します。
2. ポリシーを作成します。
   a. *ポリシー > ポリシーの作成*を選択します。
   b. *JSON*を選択し、その内容をコピーして貼り付けます。"コンソールエージェントのIAMポリシー" 。
   c. 残りの手順を完了してポリシーを作成します。
3. IAM ロールを作成します。
   a. *[ロール] > [ロールの作成]*を選択します。
   b. **AWS** サービス **> EC2** を選択します。
   c. 作成したポリシーを添付して権限を追加します。
   d. 残りの手順を完了してロールを作成します。

結果

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

AWS アクセスキー

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

手順

1. AWS コンソールにログインし、IAM サービスに移動します。
2. ポリシーを作成します。
   a. *ポリシー > ポリシーの作成*を選択します。
   b. *JSON*を選択し、その内容をコピーして貼り付けます。"コンソールエージェントのIAMポリシー" 。
   c. 残りの手順を完了してポリシーを作成します。

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

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

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

Azure ロール

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

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

手順

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

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

2. の内容をコピーします"コネクタのカスタムロール権限"JSON ファイルに保存します。
3. 割り当て可能なスコープに Azure サブスクリプション ID を追加して、JSON ファイルを変更します。

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

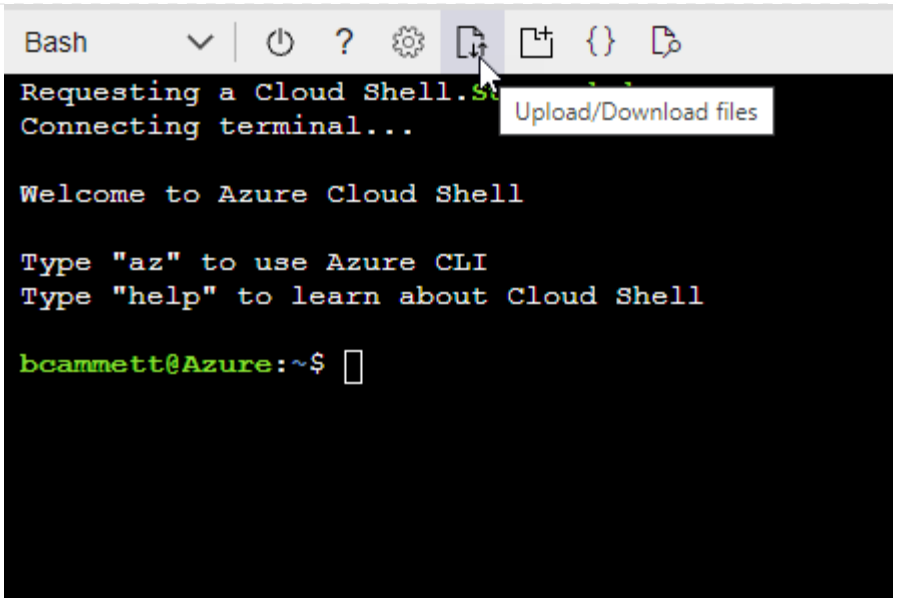
   例

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

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

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

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



c. Azure CLI を使用してカスタム ロールを作成します。

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

Azure サービスプリンシパル

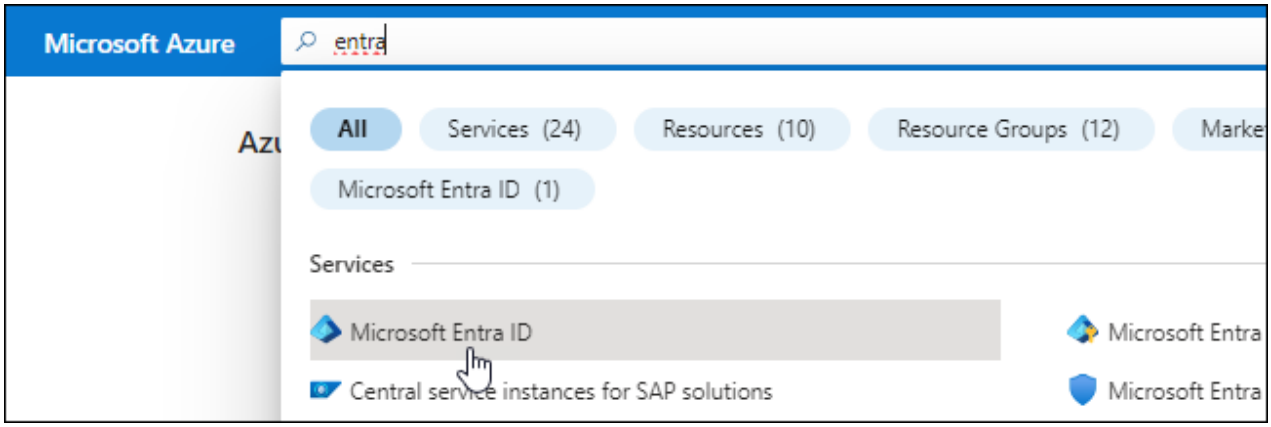
Microsoft Entra ID でサービス プリンシパルを作成して設定し、コンソールに必要な Azure 資格情報を取得します。コンソール エージェントをインストールした後、コンソールにこれらの資格情報を提供する必要があります。

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

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

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

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



3. メニューで*アプリ登録*を選択します。
4. *新規登録*を選択します。

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

   AD アプリケーションとサービス プリンシパルを作成しました。

アプリケーションをロールに割り当てる

1. カスタム ロールを作成します。

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

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

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

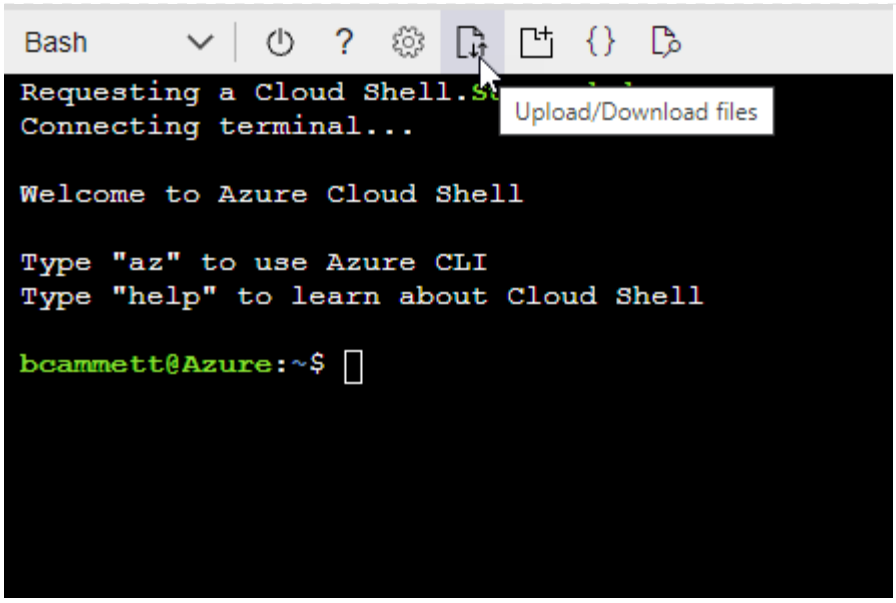
      例

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

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

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

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



- Azure CLI を使用してカスタム ロールを作成します。

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

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

2. アプリケーションをロールに割り当てます。

a. Azure ポータルから、サブスクリプション サービスを開きます。

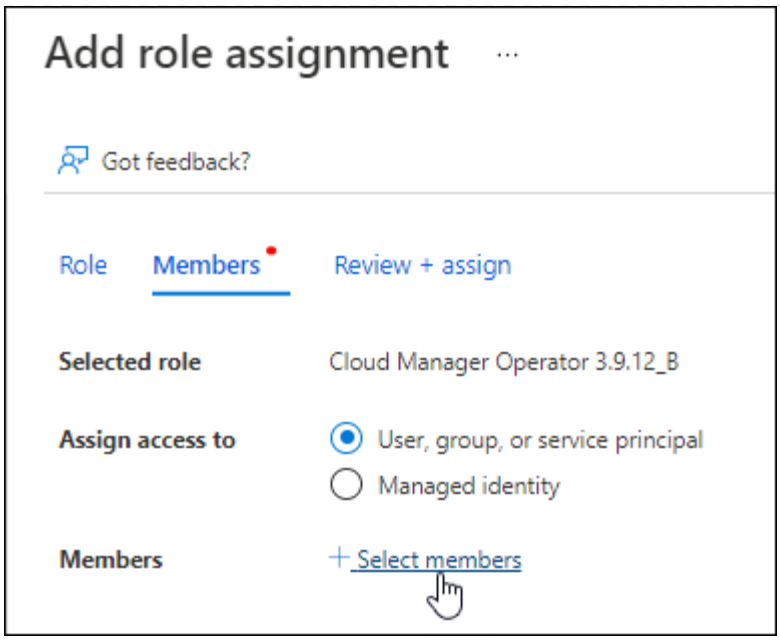
b. サブスクリプションを選択します。

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

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

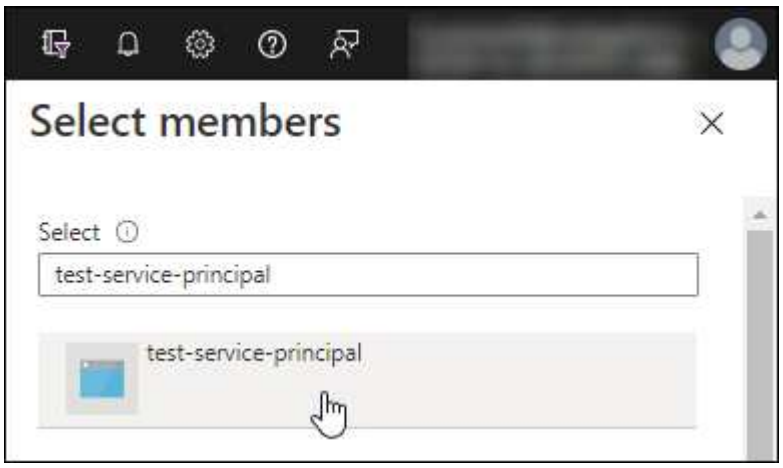
e. *メンバー*タブで、次の手順を実行します。

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



- アプリケーションの名前を検索します。

  次に例を示します。



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

f. *レビュー + 割り当て*を選択します。

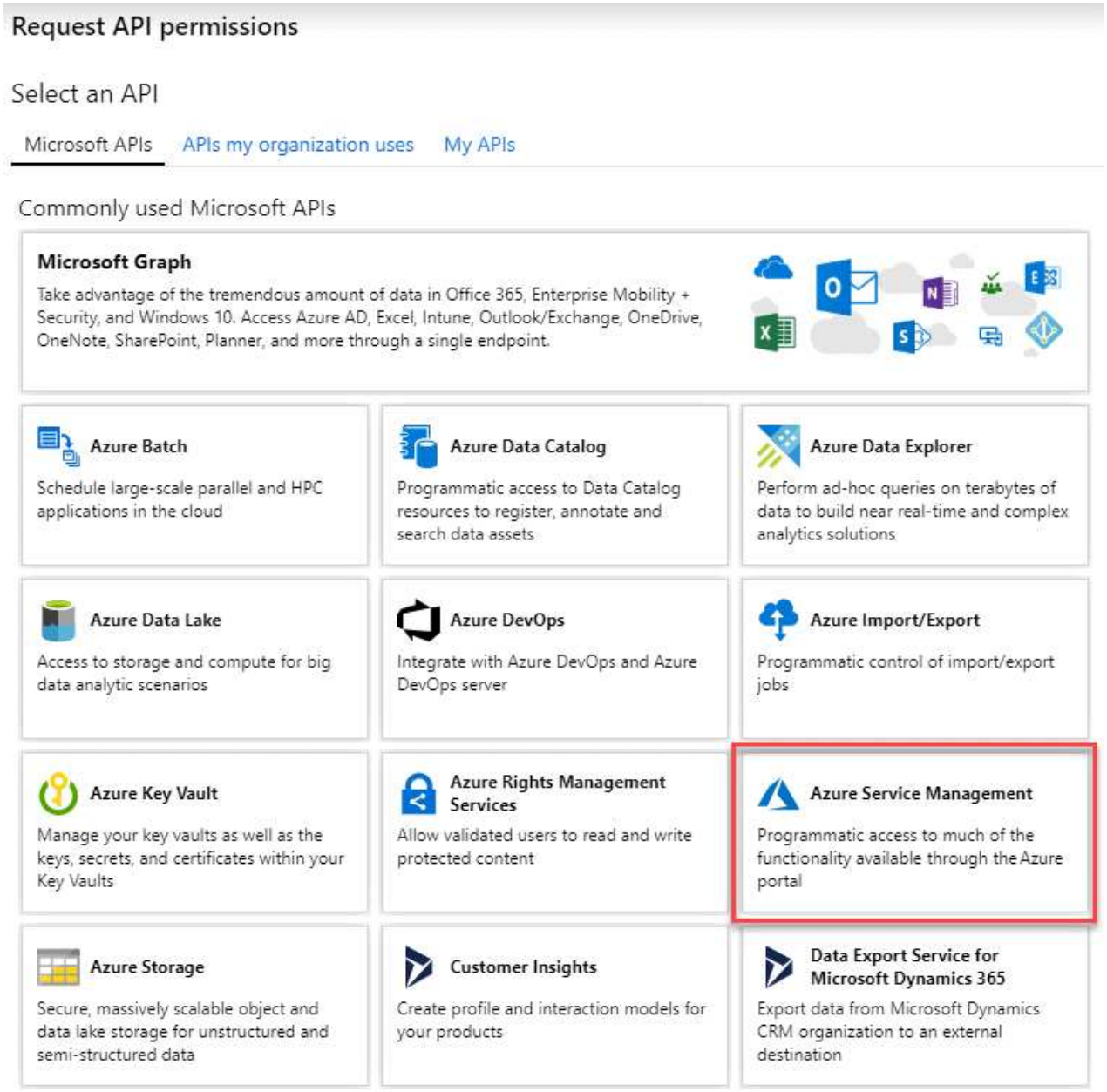
これで、サービス プリンシパルに、コンソール エージェントをデプロイするために必要な Azure アクセス許可が付与されました。

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

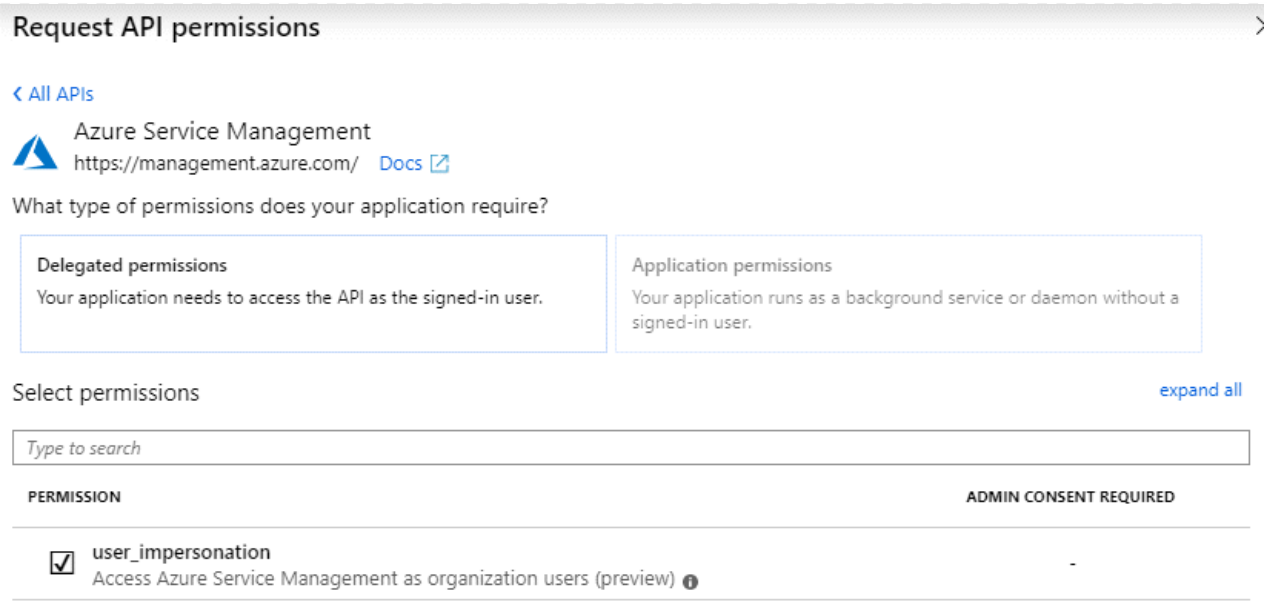
Windows Azure サービス管理 **API** 権限を追加する

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

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

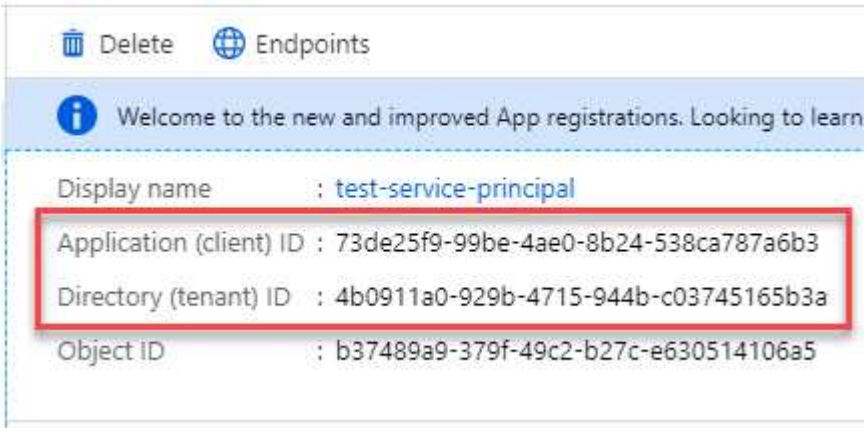


4. 組織ユーザーとして **Azure** サービス管理にアクセスする を選択し、権限の追加 を選択します。



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

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



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

クライアントシークレットを作成する

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

結果

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

Google Cloud サービス アカウント

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

手順

1. Google Cloud でカスタムロールを作成します。

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

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

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

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

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

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

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

2. Google Cloud でサービス アカウントを作成します。

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

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

   c. 作成したロールを選択します。

   d. 残りの手順を完了してロールを作成します。

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

ステップ**7: Google Cloud API**を有効にする

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

手順

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

制限モードでコンソールエージェントを展開する

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

ステップ**1:** コンソールエージェントをインストールする

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

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

AWS コマーシャルマーケットプレイス

開始する前に

以下のものを用意してください。

- ネットワーク要件を満たす VPC とサブネット。

  "ネットワーク要件について学ぶ"

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

  "AWS権限の設定方法を学ぶ"

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

  "エージェントの要件を確認する"。

- EC2 インスタンスのキーペア。

手順

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

   サブスクリプションのプロセスには数分かかる場合があります。

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

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

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

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

  "AWS のセキュリティグループルールを表示する" 。

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

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

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

◦ 概要: 概要を確認し、*インスタンスの起動*を選択します。

結果

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

次の手順

NetApp Consoleをセットアップします。

AWS Gov マーケットプレイス

開始する前に

以下のものを用意してください。

- ネットワーク要件を満たす VPC とサブネット。

  "ネットワーク要件について学ぶ"

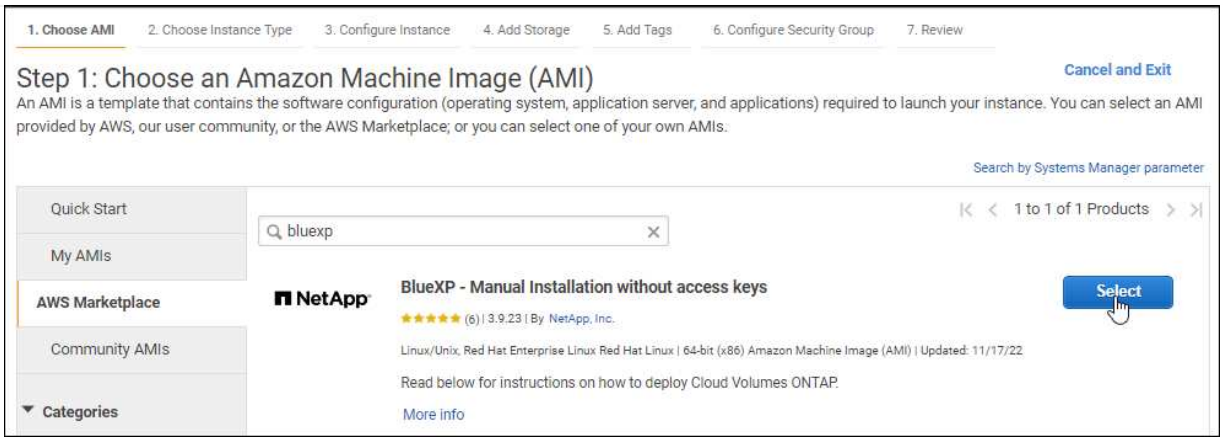
- コンソール エージェントに必要な権限を含むポリシーがアタッチされた IAM ロール。

  "AWS権限の設定方法を学ぶ"

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

手順

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



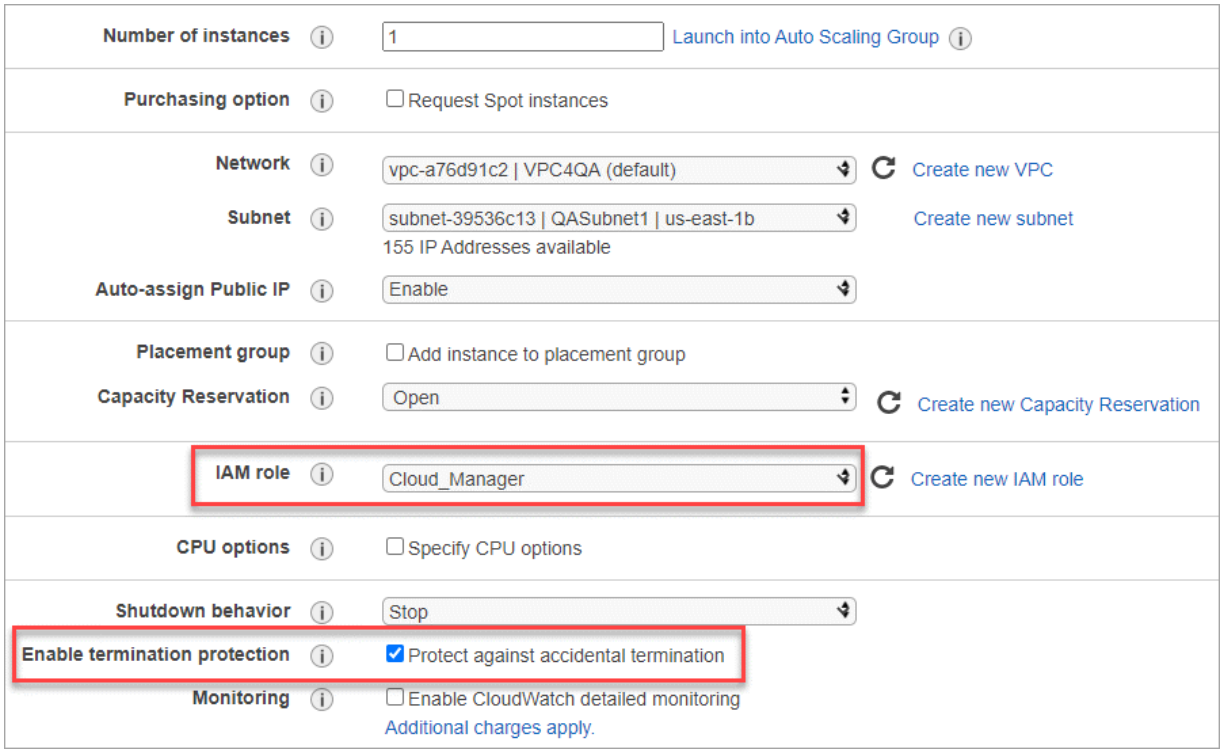
d. *続行*を選択します。

2. プロンプトに従ってインスタンスをセットアップして起動します。

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

     "インスタンス要件を確認する" 。

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



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

結果

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

次の手順

コンソールをセットアップします。

Azure Gov マーケットプレイス

開始する前に

次のものが必要です:

- ネットワーク要件を満たす VNet とサブネット。

  "ネットワーク要件について学ぶ"

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

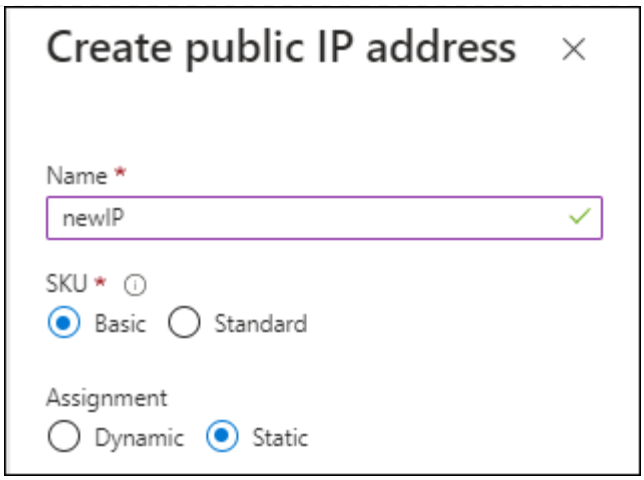
  "Azure の権限を設定する方法を学ぶ"

手順

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

   VM を構成する際には、次の点に注意してください。

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



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

"Azure ドキュメント: パブリック IP SKU"

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

  "Azure のセキュリティ グループ ルールを表示する" 。

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

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

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

結果

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

次の手順

NetApp Consoleをセットアップします。

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

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

開始する前に

次のものが必要です:

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

  インストール後にプロキシ サーバーを構成するオプションがありますが、これを行うにはコンソー

ル エージェントを再起動する必要があります。

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

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

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

タスク概要

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

手順

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

```
unset http_proxy
unset https_proxy
```

これらのシステム変数を削除しないと、インストールは失敗します。

2. コンソール エージェント ソフトウェアをダウンロードし、Linux ホストにコピーします。 NetApp ConsoleまたはNetAppサポート サイトからダウンロードできます。
   - NetApp Console: エージェント > 管理 > エージェントのデプロイ > オンプレミス > 手動インストール に移動します。

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

   - NetAppサポート サイト (コンソールにまだアクセスできない場合に必要) "NetAppサポート サイト" 、
3. スクリプトを実行するための権限を割り当てます。

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

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

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

5. インストール スクリプトを実行します。

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

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

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

+

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

+

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

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

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

+ 以下の点に注意してください：

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

+ 例：

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

1. Podman を使用した場合は、aardvark-dns ポートを調整する必要があります。
   a. コンソール エージェント仮想マシンに SSH で接続します。
   b. podman */usr/share/containers/containers.conf* ファイルを開き、Aardvark DNS サービス用に選択したポートを変更します。たとえば、54 に変更します。

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

例えば：

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

a. コンソール エージェント仮想マシンを再起動します。

結果

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

次の手順

NetApp Consoleをセットアップします。

ステップ**2: NetApp Console**をセットアップする

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

開始する前に

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

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

手順

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

d. *このアカウントで制限モードを有効にする*を選択します。

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

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

a. *始めましょう*を選択します。

結果

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

次の手順

以前に設定した権限をコンソールに提供します。

ステップ**3:** コンソールエージェントに権限を付与する

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

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

"クラウド権限の準備方法を学ぶ" 。

AWS IAM ロール

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

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

手順

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

AWS アクセスキー

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

手順

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

Azure ロール

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

手順

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

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

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

2. アクセス制御 **(IAM)** > 追加 > ロール割り当ての追加 を選択します。
3. *役割*タブで、*コンソールオペレーター*役割を選択し、*次へ*を選択します。

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

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

Azure サービスプリンシパル

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

手順

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

結果

NetApp Consoleに、ユーザーに代わって Azure でアクションを実行するために必要な権限が付与されました。

Google Cloud サービス アカウント

サービス アカウントをコンソール エージェント VM に関連付けます。

手順

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

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

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

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

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

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

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

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

開始する前に

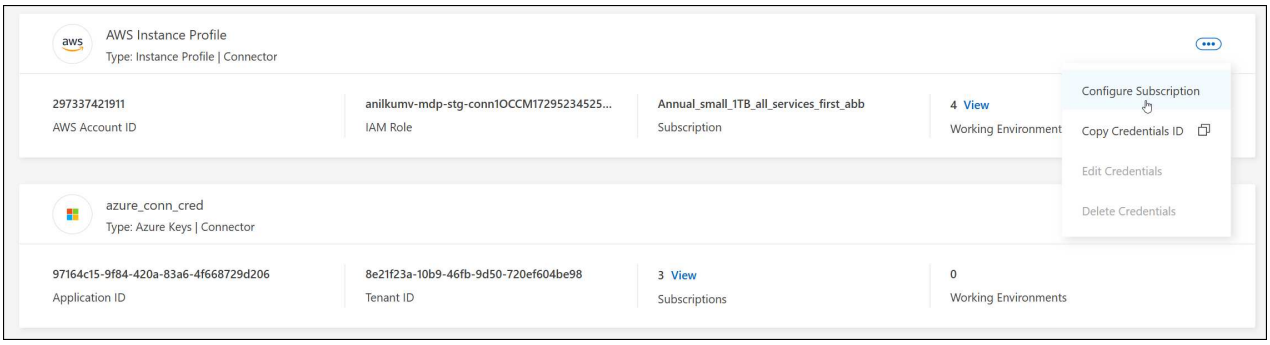
データ サービスをサブスクライブするには、コンソール エージェントをすでに展開しておく必要があります。コンソール エージェントに接続されたクラウド資格情報にマーケットプレイス サブスクリプションを関連付ける必要があります。

AWS

手順

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

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



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

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

      NetApp Consoleにリダイレクトされます。

   d. *サブスクリプションの割り当て*ページから:

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

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

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

   ◦ *保存*を選択します。

Azure

手順

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

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

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

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

      NetApp Consoleにリダイレクトされます。

   e. *サブスクリプションの割り当て*ページから:

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

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

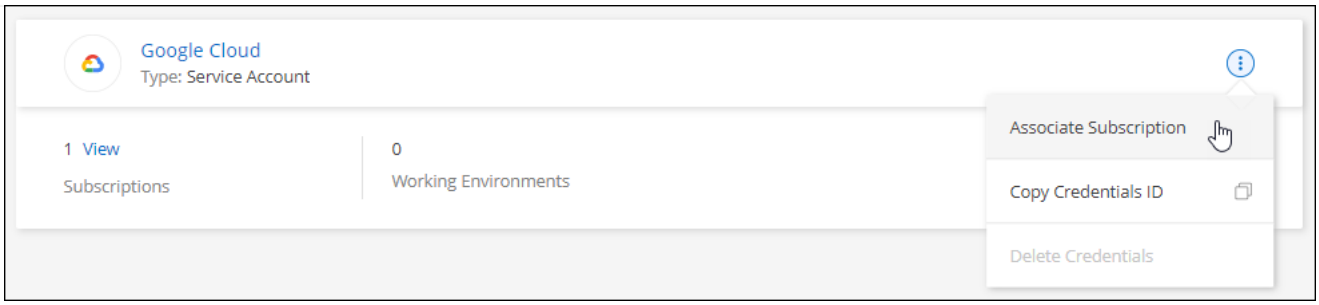
   他のすべての組織またはアカウントについては、これらの手順を繰り返して、サブスクリプションを手動で関連付ける必要があります。

   ◦ *保存*を選択します。

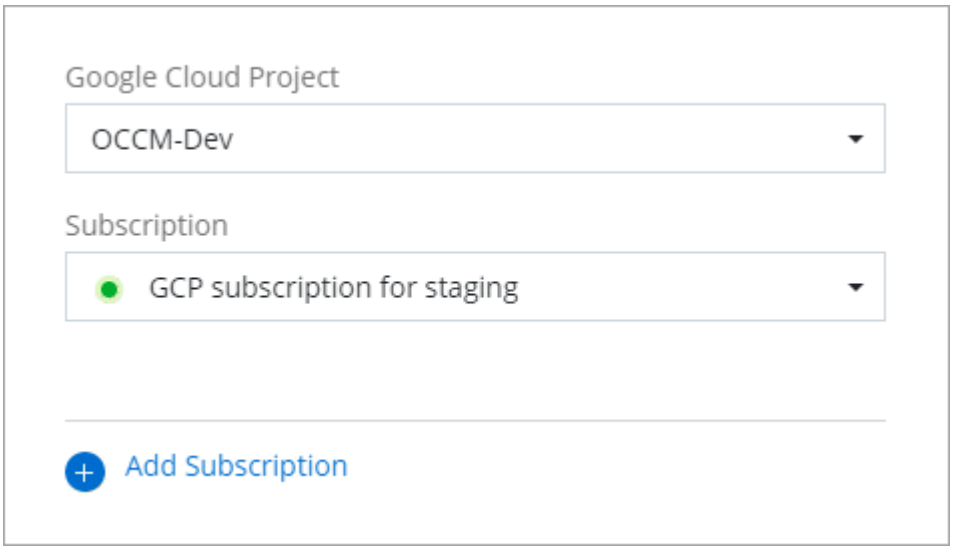
Google Cloud

手順

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



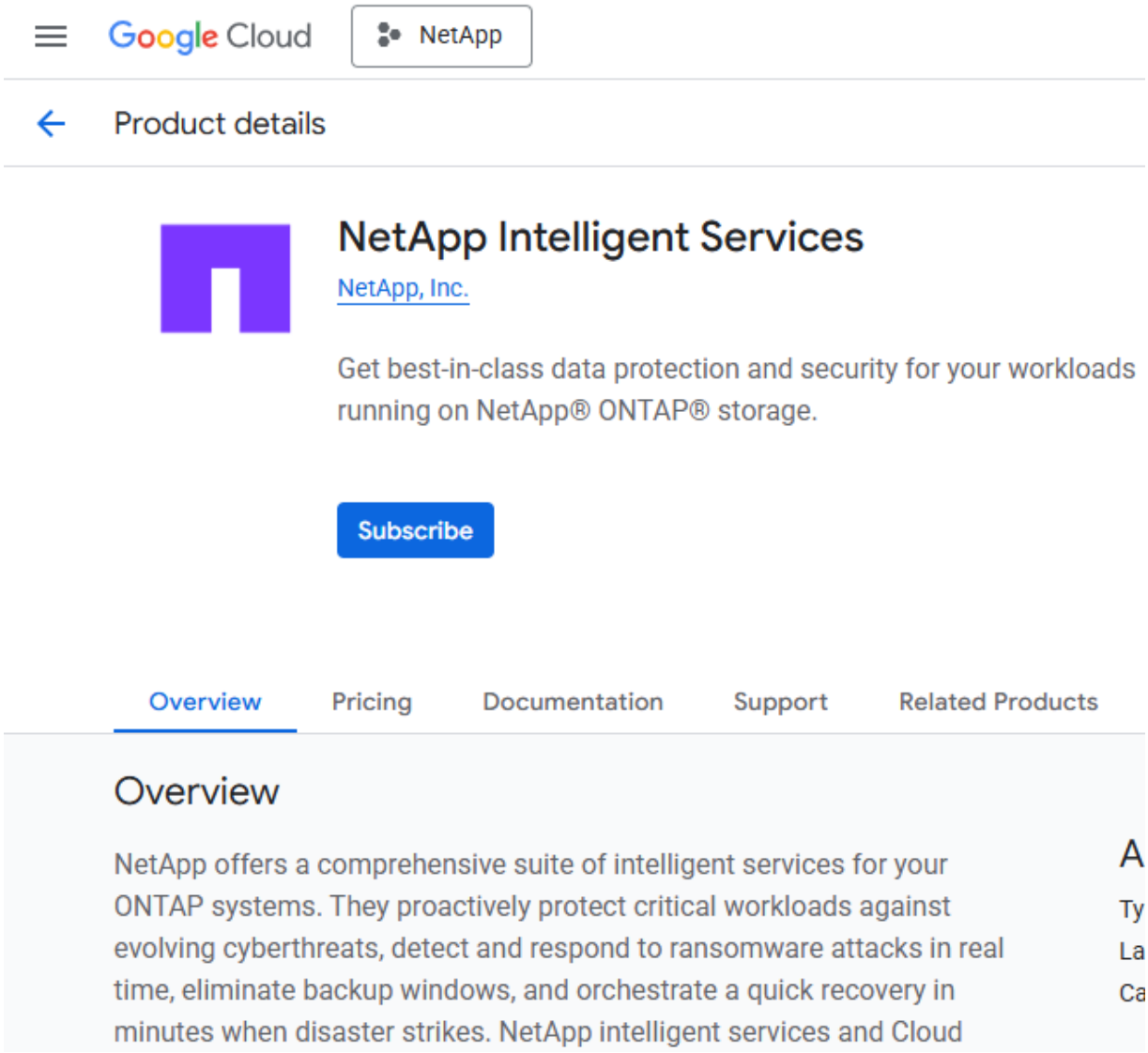
1. 選択した認証情報を使用して既存のサブスクリプションを構成するには、ドロップダウン リストから Google Cloud プロジェクトとサブスクリプションを選択し、[構成] を選択します。



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

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

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

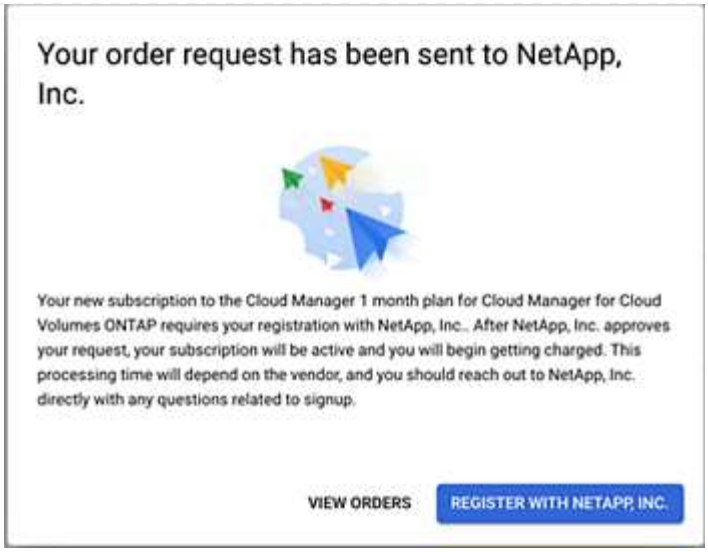


b. *購読*を選択します。
c. 適切な請求先アカウントを選択し、利用規約に同意します。
d. *購読*を選択します。

   この手順により、転送リクエストがNetAppに送信されます。

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

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



f. サブスクリプションの割り当て ページの手順を完了します。

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

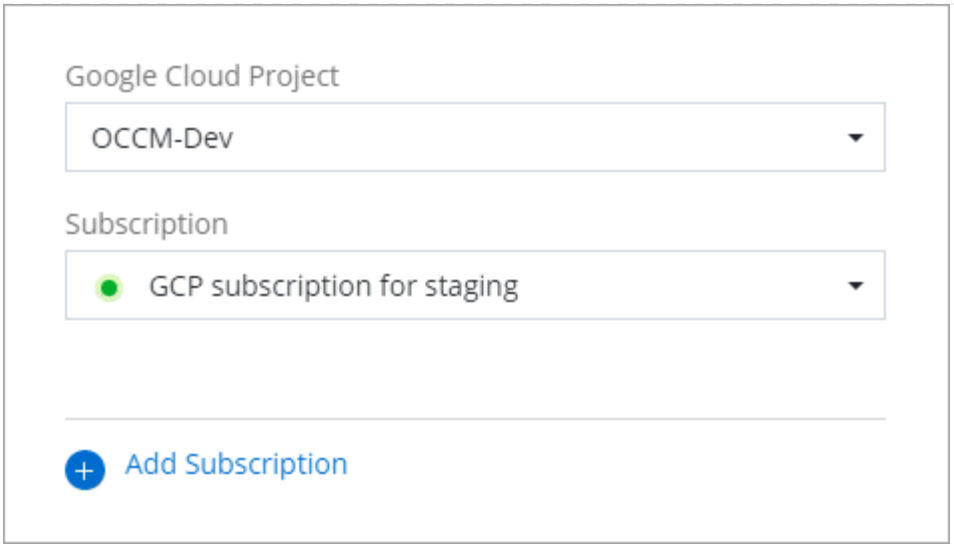
- このサブスクリプションを関連付けるコンソール組織を選択します。
- 既存のサブスクリプションを置き換える フィールドで、1 つの組織の既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

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

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

- *保存*を選択します。

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



関連情報

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

次にできること（制限モード）

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

ヘルプについては、次のサービスのドキュメントを参照してください。

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

関連情報

"NetApp Consoleの展開モード"

プライベートモードを始める

開始ワークフロー（**BlueXP**プライベートモード）

BlueXPプライベート モード (レガシーBlueXPインターフェイス) は通常、インターネット接続がなく、AWS Secret Cloud、AWS Top Secret Cloud、Azure IL6 などの安全なクラウド領域があるオンプレミス環境で使用されます。 NetApp は、従来のBlueXPインターフェースを使用してこれらの環境を引き続きサポートします。

"BlueXPプライベートモードの PDF ドキュメント"

プライベートモードでサポートされる機能とデータサービス

次の表は、どのBlueXPサービスと機能がプライベート モードでサポートされているかをすぐに識別するのに役立ちます。

一部のサービスは制限付きでサポートされる場合がありますのでご了承ください。

製品分野	**BlueXP**のサービスまたは機能	プライベートモード
作業環境 表のこの部分には、 BlueXPキャンバスからの作業環境管理のサポートがリストされています。 BlueXP backup and recoveryでサポートされているバックアップ先は示されません。	Amazon FSx for ONTAP	いいえ
	Amazon S3	いいえ
	Azure ブロブ	いいえ
	Azure NetApp Files	いいえ
	Cloud Volumes ONTAP	はい
	Google Cloud NetApp Volumes	いいえ
	Google Cloud Storage	いいえ
	オンプレミスのONTAPクラスタ	はい
	Eシリーズ	いいえ
	StorageGRID	いいえ

製品分野	**BlueXP**のサービスまたは機能	プライベートモード
サービス	アラート	いいえ
	バックアップとリカバリ	はいhttps://docs.netapp.com/us-en/data-services-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-no-internet-connectivity["ONTAPボリュームデータのサポートされているバックアップ先のリストを表示します"^]
	分類	はい
	コピーと同期	いいえ
	デジタルアドバイザー	いいえ
	デジタルウォレット	はい
	ディザスタ リカバリ	いいえ
	経済効率	いいえ
	ランサムウェア耐性	いいえ
	レプリケーション	はい
	ソフトウェアアップデート	いいえ
	持続可能性	いいえ
	階層化	いいえ
	ボリュームキャッシュ	いいえ
	ワークロードファクトリー	いいえ
特徴	アイデンティティとアクセス管理	はい
	Credentials	はい
	フェデレーション	いいえ
	多要素認証	いいえ
	NSSアカウント	いいえ
	通知	いいえ
	検索	いいえ
	スケジュール	はい