Cloud Manager
をセットアップおよび管理する
Set up and administration

NetApp
April 13, 2022

目次

Cloud Manager をセットアップおよび管理する

リリースノート

新機能

Cloud Manager の管理機能の新機能であるネットアップのアカウント、コネクタ、クラウドプロバイダのクレデンシャルなどについて説明します。

2022 年 2 月 27 日

Google Cloud の **Connector** 強化

Google Cloud で新しいコネクタを作成すると、 Cloud Manager に既存のすべてのファイアウォールポリシーが表示されるようになります。以前は、 Cloud Manager にはターゲットタグがないポリシーは表示されませんでした。

2022 年 1 月 30 日

ネットアップサポートサイトのアカウントに関する注意事項

現在、ネットアップでは、サポートとライセンスに固有の認証サービスを提供するアイデンティティプロバイダとして、 Microsoft Azure Active Directory を使用しています。この更新の結果、 Cloud Manager は、以前に追加した既存のアカウントのネットアップサポートサイト（ NSS ）のクレデンシャルの更新を求めます。

NSS アカウントを IDaaS に移行していない場合は、まずアカウントを移行してから、 Cloud Manager でクレデンシャルを更新する必要があります。

- "ネットアップによるアイデンティティ管理での Microsoft Azure AD の使用方法の詳細については、こちらをご覧ください"
- "NSS アカウントを新しい認証方法に更新する方法について説明します"

2022 年 1 月 2 日

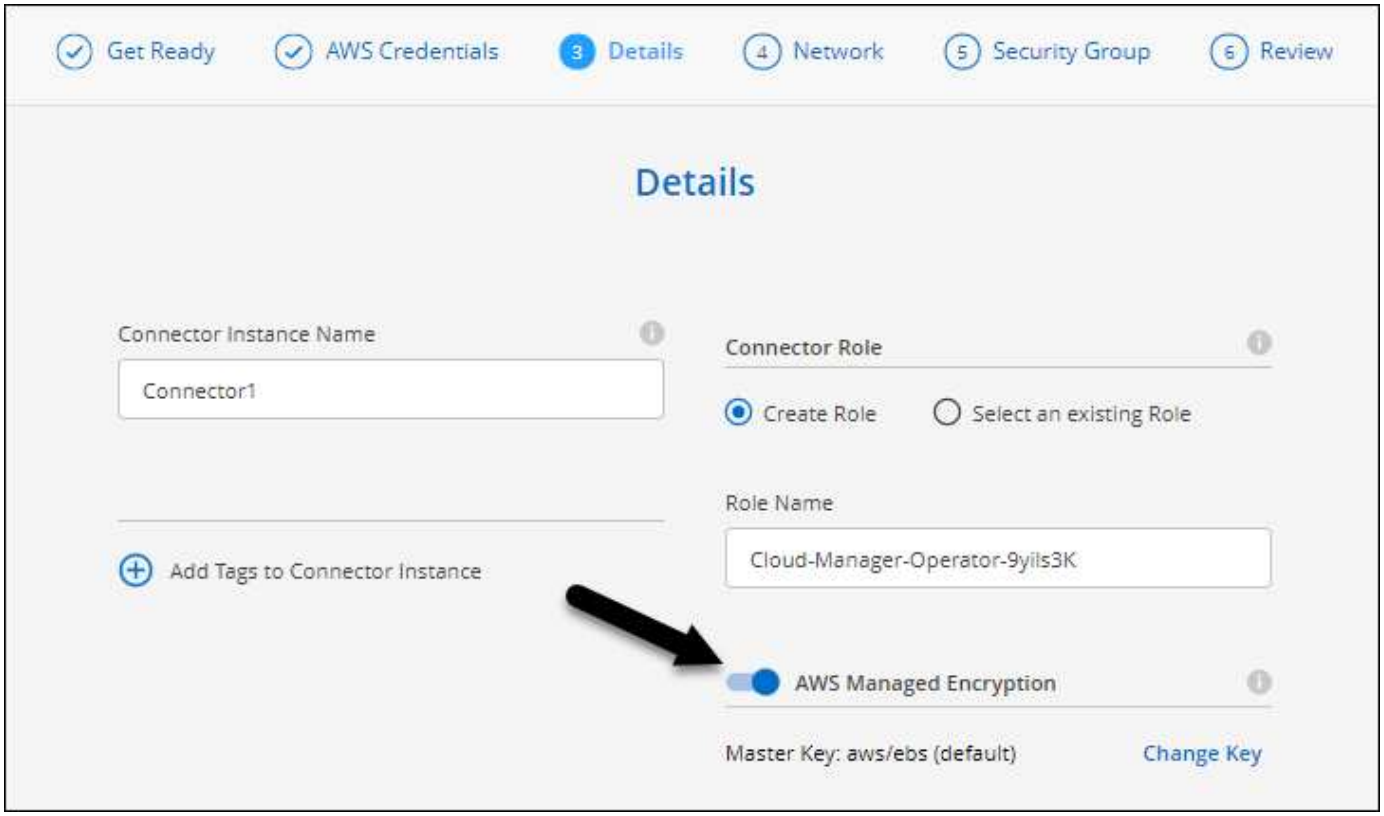
コネクタのエンドポイントが減少しました

パブリッククラウド環境内でリソースやプロセスを管理するためにコネクタが接続する必要があるエンドポイントの数を削減しました。

"必要なエンドポイントのリストを表示します"。

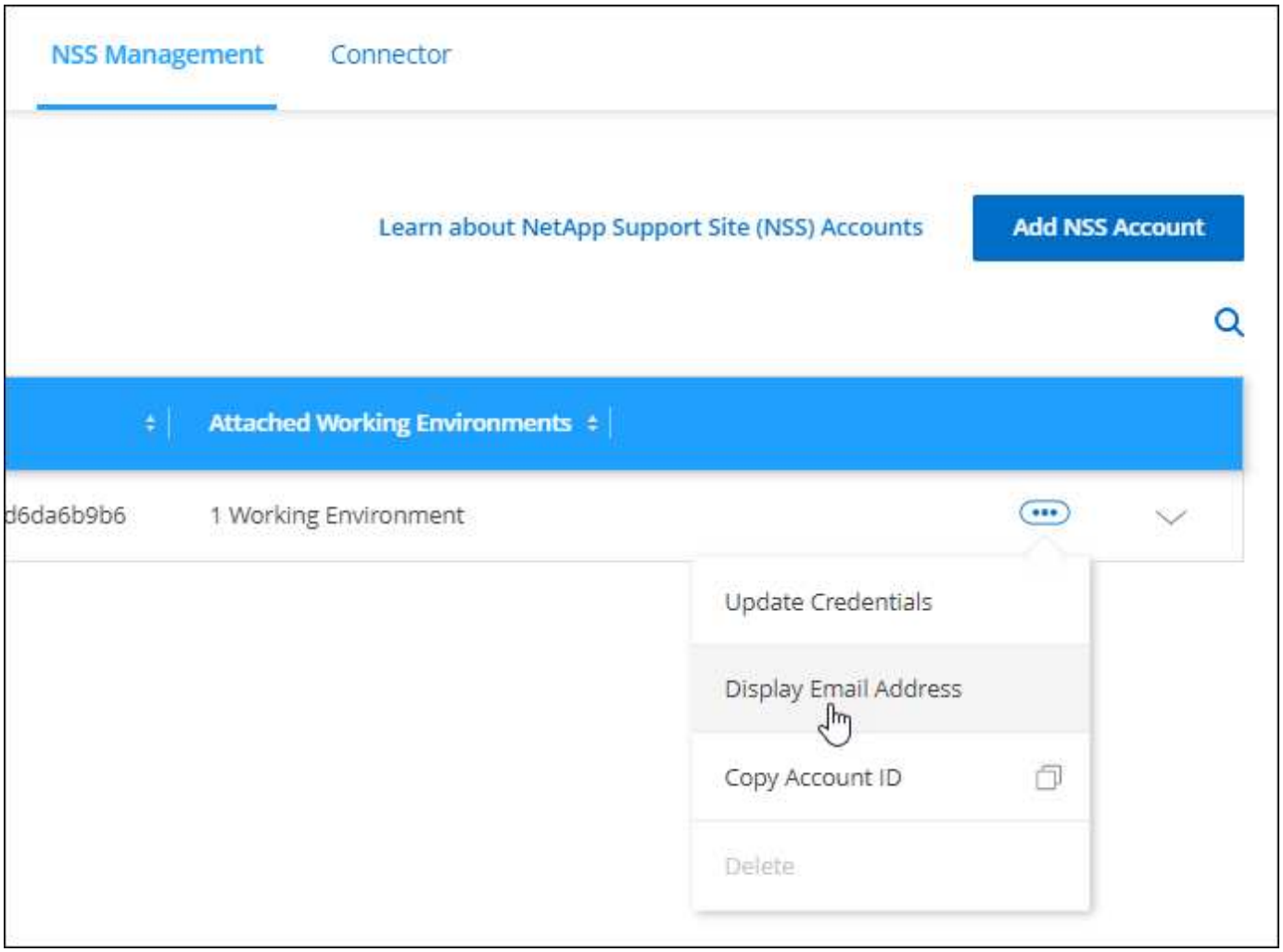
コネクタの **EBS** ディスク暗号化

Cloud Manager から AWS に新しいコネクタを導入する際に、デフォルトのマスターキーまたは管理対象キーを使用してコネクタの EBS ディスクを暗号化できるようになりました。



NSS アカウントの **E** メールアドレス

Cloud Manager に、ネットアップサポートサイトのアカウントに関連付けられている E メールアドレスが表示されるようになりました。



2021 年 11 月 28 日

ネットアップサポートサイトのアカウントを更新する必要があります

2021 年 12 月以降、ネットアップは、サポートとライセンスに固有の認証サービスのアイデンティティプロバイダとして Microsoft Azure Active Directory を使用するようになりました。この更新によって、 Cloud Manager は、以前に追加した既存のネットアップサポートサイトのアカウントのクレデンシャルの更新を求めます。

- "NSS アカウントを新しい認証方法に更新する方法について説明します"。
- "ネットアップによるアイデンティティ管理での Microsoft Azure AD の使用方法の詳細については、こちらをご覧ください"

Cloud Volumes ONTAP の **NSS** アカウントを変更します

組織内に複数のネットアップサポートサイトのアカウントがある場合、 Cloud Volumes ONTAP システムに関連付けられているアカウントを変更できるようになりました。

"作業環境を別の NSS アカウントに接続する方法について説明します"。

2021 年 11 月 4 日

SOC 2 Type 2 認定

独立機関の公認会計士であり、サービス監査役は、 Cloud Manager 、 Cloud Sync 、 Cloud Tiering 、 Cloud Data Sense 、 Cloud Backup （ Cloud Manager プラットフォーム）を調査し、該当する信頼サービス基準に基づいて SOC 2 Type 2 のレポートを達成したことを確認しました。

"ネットアップの SOC 2 レポートをご覧ください"。

コネクタはプロキシとしてサポートされなくなりました

AutoSupport から Cloud Volumes ONTAP メッセージを送信するためのプロキシサーバとして Cloud Manager Connector を使用することはできなくなりました。この機能は削除され、サポートも終了しています。AutoSupport 接続は、 NAT インスタンスまたは環境のプロキシサービスを介して提供する必要があります。

"Cloud Volumes ONTAP による AutoSupport の検証の詳細については、こちらをご覧ください"

2021 年 10 月 31 日

サービスプリンシパルを使用した認証

Microsoft Azure で新しいコネクタを作成する際、 Azure アカウントのクレデンシャルではなく Azure サービスプリンシパルで認証できるようになりました。

"Azure サービスプリンシパルでの認証方法について説明します"。

クレデンシャルの機能拡張

クレデンシャルページのデザインを見直し、使いやすく、 Cloud Manager のインターフェイスの外観に合わせて刷新しました。

2021 年 9 月 2 日

新しい通知サービスが追加されました

通知サービスが導入され、現在のログインセッションで開始した Cloud Manager の処理のステータスを表示できるようになりました。処理が成功したかどうか、または失敗したかどうかを確認できます。 "アカウントの操作を監視する方法については、を参照してください"。

2021 年 8 月 1 日

RHEL 7.9 はコネクタでサポートされます

Red Hat Enterprise Linux 7.9 を実行しているホストでは、コネクタがサポートされるようになりました。

"コネクタのシステム要件を確認します"。

2021 年 7 月 7 日

コネクタの追加ウィザードの機能拡張

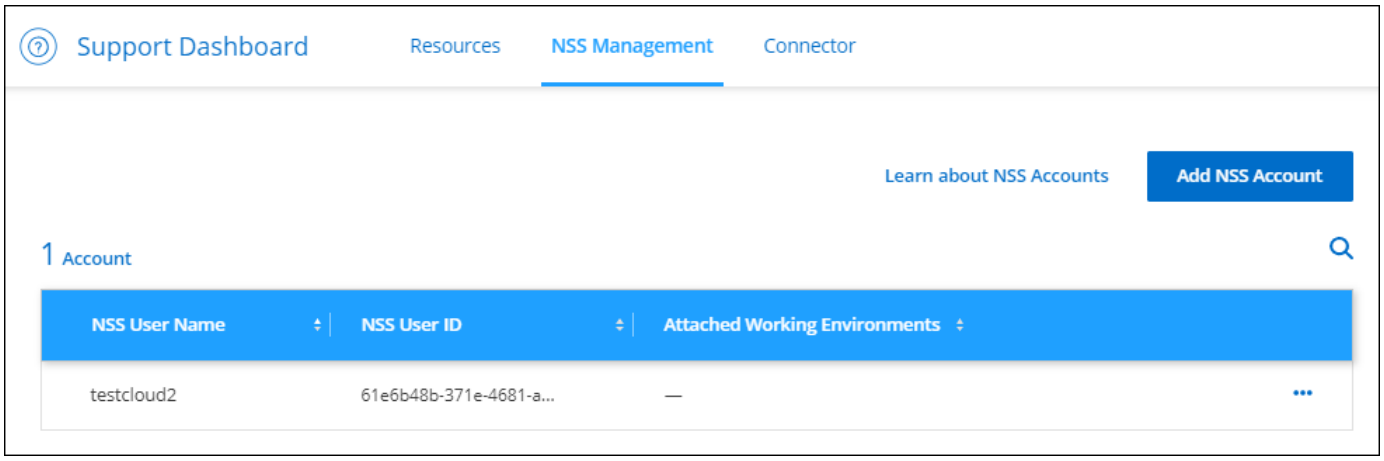
新しいオプションを追加して使いやすくするために、 * コネクターの追加 * ウィザードを再設計しました。タグの追加、ロール（ AWS または Azure ）の指定、プロキシサーバのルート証明書のアップロード、 Terraform Automation のコードの表示、進捗状況の詳細の表示などが可能になりました。

- "AWS でコネクタを作成します"
- "Azure でコネクタを作成します"
- "GCP でコネクターを作成します"

NSS アカウントの管理をサポートダッシュボードから行うこともできます

ネットアップサポートサイト（ NSS ）アカウントは、設定メニューではなくサポートダッシュボードで管理できるようになりました。この変更により、すべてのサポート関連情報を 1 箇所から簡単に検索して管理できるようになります。

"NSS アカウントを管理する方法について説明します"。



2021 年 5 月 5 日

タイムラインのアカウント

Cloud Manager のタイムラインに、アカウント管理に関連する操作とイベントが表示されるようになりました。アクションには、ユーザーの関連付け、ワークスペースの作成、コネクタの作成などがあります。タイムラインのチェックは、特定のアクションを実行したユーザーを特定する必要がある場合や、アクションのステータスを特定する必要がある場合に役立ちます。

"タイムラインをテナンシーサービスにフィルタリングする方法について説明します"。

2021 年 4 月 11 日

Cloud Manager に直接 **API** で呼び出します

プロキシサーバを設定している場合、プロキシを経由せずに Cloud Manager に API 呼び出しを直接送信するオプションを有効にできるようになりました。このオプションは、 AWS または Google Cloud で実行されて

いるコネクタでサポートされます。

"この設定の詳細については、こちらをご覧ください"。

サービスアカウントユーザ

サービスアカウントユーザを作成できるようになりました。

サービスアカウントは「ユーザ」の役割を果たし、 Cloud Manager に対して自動化のための許可された API 呼び出しを実行できます。これにより、自動化スクリプトを作成する必要がなくなります。自動化スクリプトは、会社を離れることができる実際のユーザアカウントに基づいて作成する必要がなくなります。フェデレーションを使用している場合は、クラウドから更新トークンを生成することなくトークンを作成できます。

"サービスアカウントの使用方法の詳細については、こちらをご覧ください"。

プライベートプレビュー

アカウントのプライベートプレビューで、新しい NetApp クラウドサービスが Cloud Manager のプレビューとして利用できるようになりました。

"このオプションの詳細については、こちらをご覧ください"。

サードパーティのサービス

また、アカウント内のサードパーティサービスが Cloud Manager で使用可能なサードパーティサービスにアクセスできるようにすることもできます。

"このオプションの詳細については、こちらをご覧ください"。

2021 年 2 月 9 日

サポートダッシュボードの強化

サポートダッシュボードが更新され、ネットアップサポートサイトのクレデンシャルを追加できるようになりました。このクレデンシャルをサポートに登録してください。ネットアップサポートケースは、ダッシュボードから直接開始することもできます。[ヘルプ] アイコンをクリックして、 [**Support**] をクリックします。

既知の制限

既知の制限事項は、このリリースの製品でサポートされていないプラットフォーム、デバイス、機能、または製品と正しく相互運用できない機能を特定します。これらの制限事項を慎重に確認してください

これらの制限事項は、 Cloud Manager のセットアップと管理に固有のもので、コネクタ、 SaaS プラットフォームなどが該当します。

コネクタの制限

HTTP プロキシサーバのみがサポートされています

社内ポリシーで、インターネットへのすべての HTTP 通信にプロキシサーバを使用する必要がある場合は、その HTTP プロキシサーバを使用するようにコネクタを設定する必要があります。プロキシサーバは、クラウドまたはネットワークに配置できます。

Cloud Manager では、コネクタでの HTTPS プロキシの使用はサポートされていません。

SSL 復号化はサポートされていません

Cloud Manager では、 SSL 復号化が有効になっているファイアウォール設定はサポートされていません。SSL 復号化が有効になっている場合、 Cloud Manager にエラーメッセージが表示され、 Connector インスタンスが非アクティブと表示されます。

セキュリティを強化するには、を選択します "認証局（ CA ）が署名した HTTPS 証明書をインストールする"。

ローカル **UI** のロード時に空白ページが表示される

コネクタのローカルユーザインターフェイスをロードすると、 UI が表示されない場合があり、空白のページが表示されるだけです。

この問題は、キャッシュの問題に関連しています。回避策では、 incognito モードまたはプライベート Web ブラウザセッションを使用します。

SaaS の制限

政府機関では **SaaS** プラットフォームが無効になっています

コネクタを AWS GovCloud リージョン、 Azure Government リージョン、または Azure DoD リージョンに導入した場合、 Cloud Manager へのアクセスはコネクタのホスト IP アドレスからのみ可能です。SaaS プラットフォームへのアクセスは、アカウント全体で無効になります。

つまり、エンドユーザの内部 VPC / VNet にアクセスできる特権ユーザのみが Cloud Manager の UI または API を使用できます。

また、次のサービスが Cloud Manager から利用できないことも意味します。

- クラウドデータの意味
- Kubernetes
- クラウド階層化
- グローバルファイルキャッシュ

これらのサービスを使用するには、 SaaS プラットフォームが必要です。

Cloud Backup 、 Cloud Data Sense 、 Monitoring サービスは、政府機関でサポートされていて利用できます。

市場の制約

従量課金制の **Azure** と **Google Cloud** のパートナーは利用できません

Microsoft Cloud 解決策 Provider （ CSP ）パートナー様または Google Cloud パートナー様は、従量課金制のサブスクリプションをご利用いただけません。ライセンスを購入し、 BYOL ライセンスを使用した NetApp クラウドソリューションを導入する必要があります。

従量課金制のサブスクリプションは、次の NetApp クラウドサービスでは利用できません。

- Cloud Volumes ONTAP
- クラウド階層化
- クラウドバックアップ
- クラウドデータの意味

はじめに

Cloud Manager の詳細をご確認ください

Cloud Manager を使用すると、 IT エキスパートやクラウドアーキテクトは、ネットアップのクラウドソリューションを使用してハイブリッドマルチクラウドインフラを一元管理できます。

の機能

Cloud Manager は、エンタープライズクラスの SaaS ベースの管理プラットフォームであり、格納場所に関係なくデータを管理できます。

- をセットアップして使用します "Cloud Volumes ONTAP" 複数のクラウドにわたって効率的なマルチプロトコルデータ管理を実現します。
- ファイルストレージサービスをセットアップして使用
  - "Azure NetApp Files の特長"
  - "ONTAP 対応の Amazon FSX"
  - "Cloud Volumes Service for AWS"
  - "Cloud Volumes Service for Google Cloud"
- ボリュームの作成、クラウドへのバックアップ、ハイブリッドクラウド間でのデータのレプリケート、クラウドへのコールドデータの階層化を行うことで、オンプレミスの ONTAP クラスタを検出して管理できます。
- 次のような統合 クラウド サービス を有効にします。
  - "クラウドデータの意味"
  - "Cloud Insights の機能です"
  - "クラウドバックアップ"

"Cloud Manager の詳細については、こちらをご覧ください"。

サポートされているオブジェクトストレージプロバイダ

Cloud Manager を使用して、 Amazon Web Services 、 Microsoft Azure 、 Google Cloud でクラウドストレージを管理したりクラウドサービスを使用したりできます。

コスト

Cloud Manager ソフトウェアはネットアップから無償で入手できます。

ほとんどのタスクでは、 Cloud Manager からクラウドネットワークにコネクタを導入するよう求められます。その結果、コンピューティングインスタンスと関連ストレージについてクラウドプロバイダから料金が発生します。Connector ソフトウェアをオンプレミスで実行することもできます。

Cloud Manager の仕組み

Cloud Manager には、 NetApp Cloud Central と統合される SaaS ベースのインターフェイスと、 Cloud Volumes ONTAP やその他のクラウドサービスを管理するコネクタがあります。

ソフトウェアサービス

Cloud Manager には、からアクセスできます "SaaS ベースのユーザインターフェイス" API を使用できます。この SaaS エクスペリエンスを利用すると、リリース時に最新機能に自動的にアクセスしたり、ネットアップのアカウントとコネクタを簡単に切り替えることができます。

NetApp Cloud Central

"NetApp Cloud Central" 一元的な場所でアクセスと管理を行うことができます "ネットアップのクラウドサービス"。一元化されたユーザ認証を使用すると、同じクレデンシャルを使用して Cloud Manager と Cloud Insights などのその他のクラウドサービスにアクセスできます。

ネットアップアカウント

Cloud Manager に初めてログインするときは、 _netapp アカウント _ を作成するように求められます。このアカウントはマルチテナンシーを提供し、分離されたワークスペース内でユーザとリソースを整理することができます。

コネクタ

ほとんどの場合、アカウント管理者は _ コネクタ _ をクラウドまたはオンプレミスネットワークに導入する必要があります。Connector を使用すると、 Cloud Manager 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できます。

コネクタは常時稼働している必要があります。有効にするサービスの継続的な健常性と運用性にとって重要です。

たとえば、 Cloud Volumes ONTAP PAYGO システムの正常性と運用においては、コネクタが重要な要素です。コネクタの電源がオフの場合、 Cloud Volumes ONTAP PAYGO システムは、コネクタとの通信を 14 日以上失った後にシャットダウンします。

"コネクタが必要になる状況とその方法については、こちらをご覧ください 仕事"。

SOC 2 Type 2 認定

独立機関の公認会計士であり、サービス監査役は、 Cloud Manager 、 Cloud Sync 、 Cloud Tiering 、 Cloud Data Sense 、 Cloud Backup （ Cloud Manager プラットフォーム）を調査し、該当する信頼サービス基準に基づいて SOC 2 Type 2 のレポートを達成したことを確認しました。

"ネットアップの SOC 2 レポートをご覧ください"

はじめにチェックリスト

このチェックリストを使用して、 Connector からアウトバウンドのインターネットアクセスが設定されている一般的な環境で Cloud Manager を使用するために必要な作業を把握してください。

NetApp Cloud Central へのログイン

にサインアップする必要があります "NetApp Cloud Central" これで、 Cloud Manager などのクラウドサービスにアクセスできるようになります。

Web ブラウザから複数のエンドポイントへのネットワークアクセス

Cloud Manager のユーザインターフェイスに Web ブラウザからアクセスできます。Cloud Manager ユーザインターフェイスを使用する際に、複数のエンドポイントにアクセスしてデータ管理タスクを実行します。Web ブラウザを実行するマシンは、次のエンドポイントに接続する必要があります。

エンドポイント	目的
\ http://cloudmanager.netapp.com	Web ブラウザは、 SaaS UI を使用するときにこの URL にアクセスします。
AWS サービス（ amazonaws.com ）： • クラウド形成 • 認知人 • 柔軟なコンピューティングクラウド（ EC2 ） • キー管理サービス（ KMS ） • セキュリティトークンサービス（ STS ） • シンプルなストレージサービス（ S3 ）	AWS の Cloud Manager からコネクタを導入する場合に必要です。正確なエンドポイントは、コネクタを配置するリージョンによって異なります。 "詳細については、 AWS のマニュアルを参照してください。"
https://management.azure.com https://login.microsoftonline.com	ほとんどの Azure リージョンで Cloud Manager からコネクタを導入する場合に必要です。
https://management.microSoftazure.de https://login.microsoftonline.de	Azure ドイツのリージョンで Cloud Manager から Connector を導入する場合は必須です。
https://management.usgovcloudapi.net/ https://login.microsoftonline.com	Azure US Government リージョンの Cloud Manager からコネクタを導入するために必要です。
\ https://www.googleapis.com	Google Cloud の Cloud Manager からコネクタを導入する場合に必要です。
\ https://signin.b2c.netapp.com	ネットアップサポートサイト（ NSS ）のクレデンシャルを更新するか、 Cloud Manager に新しい NSS クレデンシャルを追加する必要があります。
¥ https://netapp-cloud-account.auth0.com ¥ 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 Cloud Central を介してユーザ認証を一元化します。
\ https://widget.intercom.io	製品内でのチャットにより、ネットアップのクラウドエキスパートと会話できます。

エンドポイント	目的
コネクタの IP アドレス	ほとんどの場合、 Cloud Manager は SaaS UI で処理しますが "ローカル UI を使用する場合は"Web ブラウザからホストの IP アドレスを入力する必要があります。 クラウドプロバイダへの接続に応じて、ホストに割り当てられたプライベート IP またはパブリック IP を使用します。 • プライベート IP は、 VPN があり、仮想ネットワークに直接アクセスできる場合に機能します • パブリック IP は、あらゆるネットワークシナリオで機能します いずれの場合も、セキュリティグループルールで許可された IP またはサブネットからのアクセスのみを許可することで、ネットワークアクセスを保護します。

コネクタのアウトバウンドネットワーク

Cloud Manager にログインしたら、アカウント管理者がクラウドプロバイダまたはオンプレミスネットワークに _ Connector _ を導入する必要があります。Connector を使用すると、 Cloud Manager 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できます。Azure NetApp Files 、 Cloud Volumes Service 、 Cloud Sync のコネクタは必要ありませんが、 Cloud Manager のその他のすべてのサービスや機能に必要です。 "コネクターの詳細とその仕組みについては、こちらをご覧ください"。

- コネクタを配置するネットワークの場所には、アウトバウンドのインターネット接続が必要です。

  Connector では、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アウトバウンドインターネットアクセスが必要です。

エンドポイント	目的
\ https://support.netapp.com	ライセンス情報を取得し、ネットアップサポートに AutoSupport メッセージを送信するため。
\ https://*.cloudmanager.cloud.netapp.com	Cloud Manager 内で SaaS の機能やサービスを提供できます。
¥ https://cloudmanagerinfraprod.azurecr.io ¥ https://*.blob.core.windows.net	をクリックして、 Connector と Docker コンポーネントをアップグレードします。

- Connector を手動でインストールする場合（ Cloud Manager インターフェイスから直接インストールしない場合）は、インストールプロセスで Connector のインストーラが次のエンドポイントにアクセスする必要があります。
  - https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
  - https://s3.amazonaws.com/aws-cli/awscli-bundle.zip
  - ¥ https://*.blob.core.windows.net または ¥ https://hub.docker.com

ホストは、インストール中にオペレーティングシステムパッケージの更新を試みる可能性があります。ホストは、これらの OS パッケージの別のミラーリングサイトにアクセスできます。

- コネクタへの着信トラフィックは、開始しない限りありません。

  HTTP （ 80 ）と HTTPS （ 443 ）はローカル UI へのアクセスを提供しますが、これはまれに使用されます。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。

クラウドプロバイダの権限

Cloud Manager から直接クラウドプロバイダに Connector を導入するための権限を持つアカウントが必要です。

コネクタを作成するには、別の方法があります。からコネクタを作成できます "AWS Marketplace"、 "Azure Marketplace で入手できます"または、次の操作を実行できます "ソフトウェアを手動でインストールします"。

場所	手順の概要	詳細な手順
AWS	1. AWS で IAM ポリシーを作成するために必要な権限を含む JSON ファイルを使用します。 2. IAM ロールまたは IAM ユーザにポリシーを関連付けます。 3. コネクタを作成するときは、 Cloud Manager に IAM ロールの ARN 、または IAM ユーザの AWS アクセスキーとシークレットキーを提供します。	"詳細な手順については、ここをクリックしてください"。
Azure	1. Azure でカスタムロールを作成するには、必要な権限が含まれた JSON ファイルを使用します。 2. Cloud Manager からコネクタを作成するユーザにロールを割り当てます。 3. Connector を作成するときは、必要な権限（ Microsoft が所有およびホストしているログインプロンプト）を持つ Microsoft アカウントでログインします。	"詳細な手順については、ここをクリックしてください"。
Google Cloud	1. Google Cloud でカスタムロールを作成するために必要な権限を含む YAML ファイルを使用します。 2. Cloud Manager からコネクタを作成するユーザにそのロールを割り当てます。 3. Cloud Volumes ONTAP を使用する場合は、必要な権限を持つサービスアカウントを設定します。 4. Google Cloud API を有効にします 5. Connector を作成するときに、必要な権限を持つ Google アカウントでログインします（ログインプロンプトは Google が所有およびホストします）。	"詳細な手順については、ここをクリックしてください"。

個々のサービスのネットワーク

セットアップが完了したら、 Cloud Manager から提供されるサービスを使い始めることができます。各サービスには独自のネットワーク要件があります。詳細については、次のページを参照してください。

- "Cloud Volumes ONTAP for AWS"
- "Cloud Volumes ONTAP for Azure"
- "Cloud Volumes ONTAP for GCP の略"
- "ONTAP システム間のデータレプリケーション"
- "Cloud Data Sense の導入"
- "オンプレミスの ONTAP クラスタ"
- "クラウド階層化"
- "クラウドバックアップ"

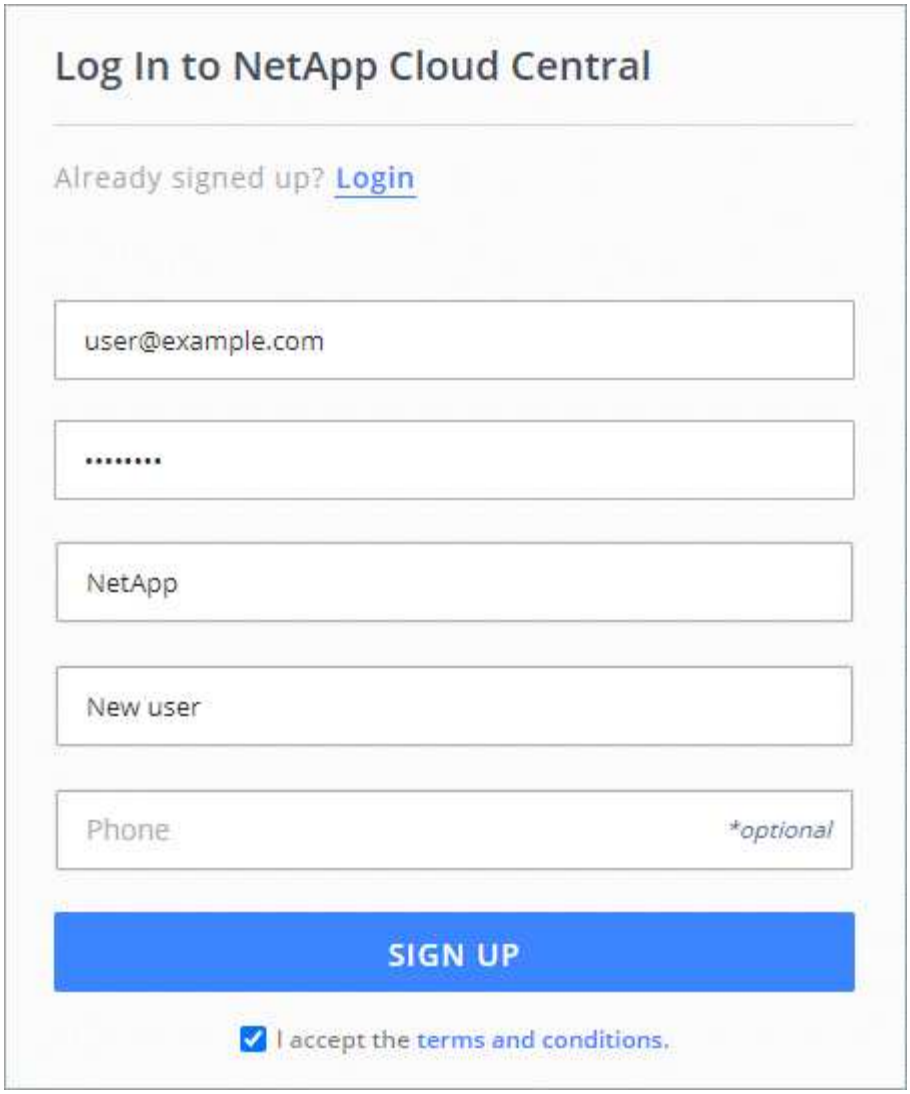
NetApp Cloud Central に登録する

NetApp Cloud Central に登録して、ネットアップのクラウドサービスにアクセスできます。

シングルサインオンを使用して、社内ディレクトリ（フェデレーション ID ）からのクレデンシャルを使用してログインできます。詳細については、を参照してください "Cloud Central ヘルプセンター" 次に、 * Cloud Central サインインオプション * をクリックします。

手順

1. Web ブラウザを開き、に進みます "NetApp Cloud Central"。
2. [サインアップ] をクリックします。
3. フォームに入力して、「 * サインアップ * 」をクリックします。



4. NetApp Cloud Central からの E メールを待ちます。
5. E メールのリンクをクリックして、 E メールアドレスを確認します。

アクティブな Cloud Central ユーザログインが可能になりました。

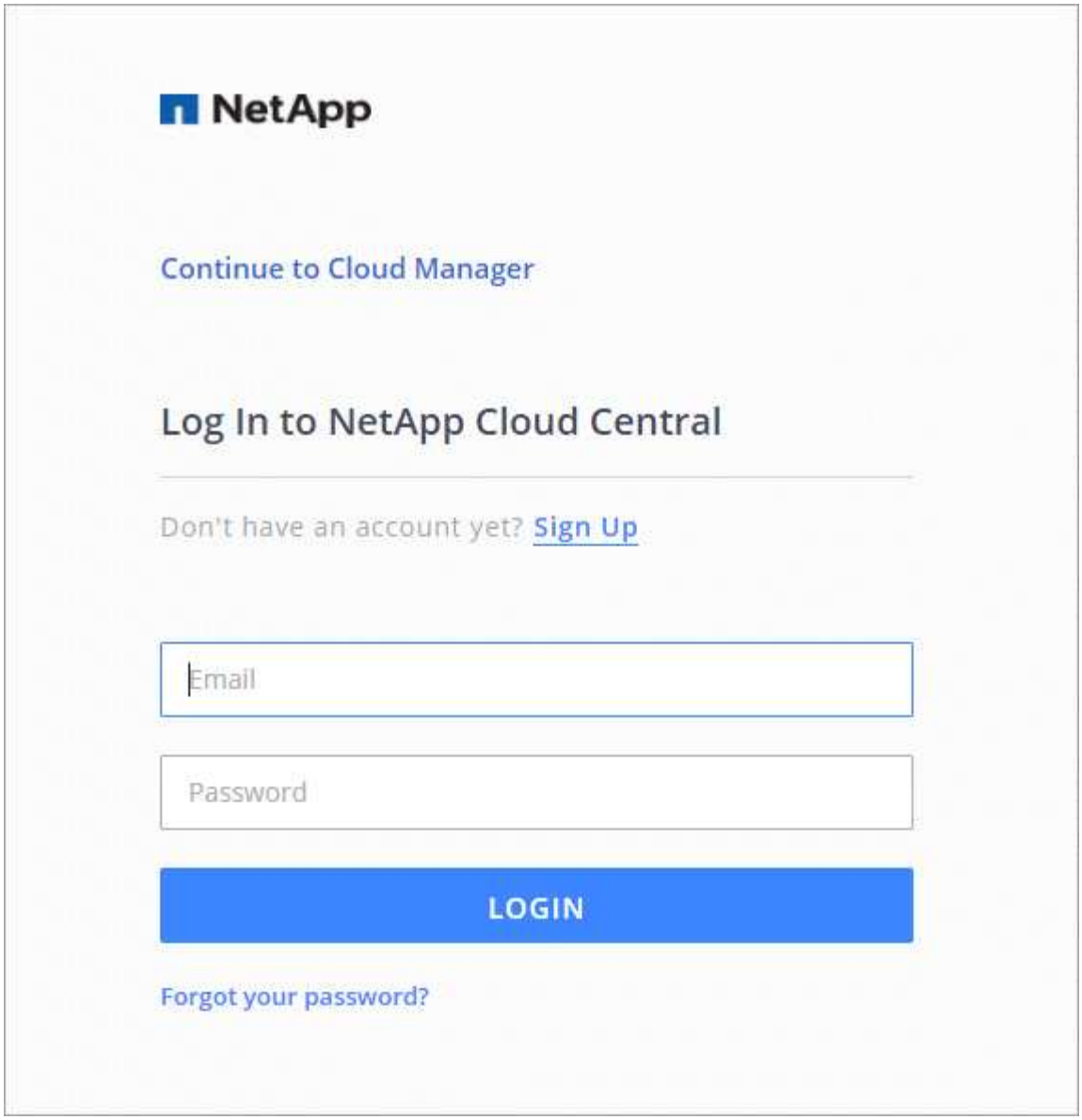
Cloud Manager にログインしています

Cloud Manager のインターフェイスには、 SaaS ベースのユーザがアクセスできます にアクセスしてインターフェイスを設定します https://cloudmanager.netapp.com。

シングルサインオンを使用して、社内ディレクトリ（フェデレーション ID ）からのクレデンシャルを使用してログインできます。詳細については、を参照してください "Cloud Central ヘルプセンター" 次に、 * Cloud Central サインインオプション * をクリックします。

手順

1. Web ブラウザを開き、に進みます https://cloudmanager.netapp.com。
2. NetApp Cloud Central のクレデンシャルを使用してログインします。



ログインすると、 Cloud Manager を使用してハイブリッドマルチクラウドインフラを管理できるようになります。

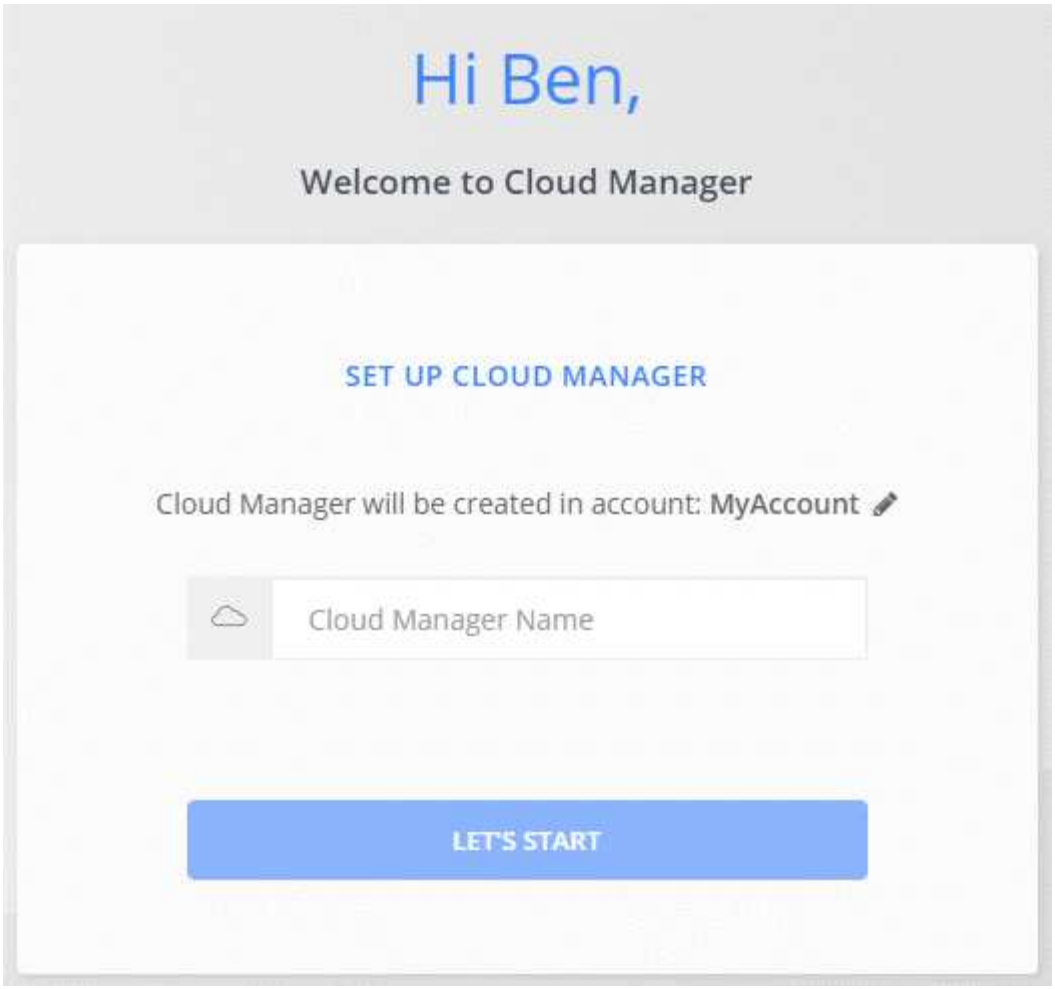
ネットアップアカウントを設定する

ネットアップアカウントについて

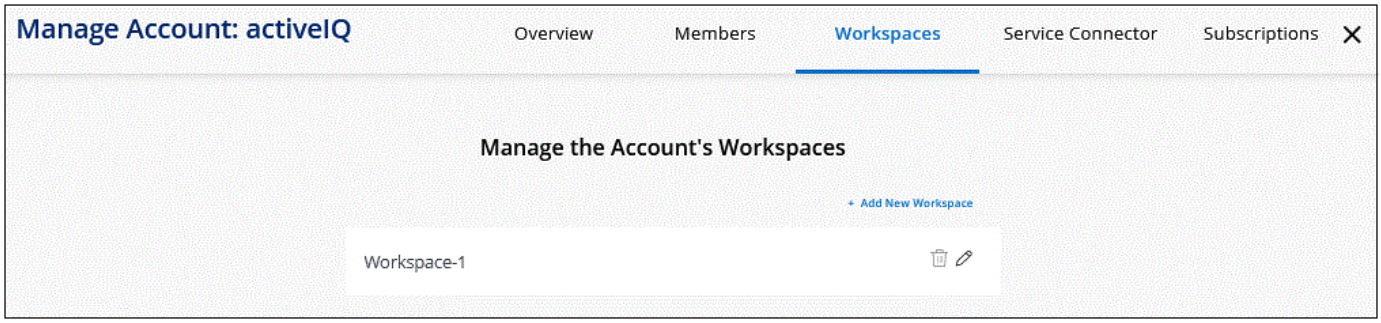
NetApp アカウント _ はマルチテナンシーを提供し、 Cloud Manager 内から分離されたワークスペース内のユーザやリソースを管理できます。

たとえば、複数のユーザが、 _workspaces という分離された環境に Cloud Volumes ONTAP システムを導入して管理できます。これらのワークスペースは、共有されていない限り、他のユーザーには表示されません。

Cloud Manager に初めてアクセスするときは、ネットアップアカウントを選択するか作成するかを尋ねられます。



アカウント管理者は、ユーザー（メンバー）、ワークスペース、コネクタ、およびサブスクリプションを管理することで、このアカウントの設定を変更できます。



手順については、を参照してください "ネットアップアカウントをセットアップする"。

MAX Cloud Volumes ONTAP システム

Cloud Volumes ONTAP システムの最大数は、使用しているライセンスモデルに関係なく、ネットアップアカウントあたり 20 に制限されます。

a_system_に は、 HA ペアまたはシングルノードシステムを指定します。たとえば、 2 つの Cloud Volumes ONTAP HA ペアと 2 つのシングルノードシステムがある場合、合計 4 つのシステムがあり、アカウントに 16 のシステムを追加で配置できます。

ご質問がある場合は、アカウント担当者または営業チームにお問い合わせください。

Account Settings （アカウント設定）

Cloud Manager のアカウント管理ウィジェットでは、アカウント管理者がネットアップアカウントを管理できます。アカウントを作成したばかりの場合は、最初から作成します。アカウントをすでに設定している場合は、アカウントに関連付けられているユーザ、ワークスペース、コネクタ、およびサブスクリプションが *all* と表示されます。

概要

概要ページには、アカウント名とアカウント ID が表示されます。一部のサービスを登録するときに、アカウント ID の入力が必要になる場合があります。このページには、 Cloud Manager の設定オプションもいくつか表示されます。

メンバー

このメンバーは、ネットアップアカウントに関連付ける NetApp Cloud Central ユーザです。ユーザーをアカウントに関連付け、そのアカウント内の 1 つ以上のワークスペースを使用すると、ユーザーは Cloud Manager で作業環境を作成して管理できます。

ユーザを関連付けると、ユーザにロールが割り当てられます。

- *Account Admin* ： Cloud Manager で任意の操作を実行できます。
- _ ワークスペース管理者 _ ：割り当てられたワークスペースでリソースを作成および管理できます。
- *Compliance Viewer*: Cloud Data Sense のコンプライアンス情報を表示し、アクセス権のあるシステムのレポートを生成することのみができます。
- _ SnapCenter Admin_ ： SnapCenter サービスを使用して、アプリケーションと整合性のあるバックアップを作成し、それらのバックアップを使用してデータをリストアできます。_ このサービスは現在ベータ版です。 _

"これらの役割の詳細については、こちらをご覧ください"。

ワークスペース

Cloud Manager では、ワークスペースによって、いくつかの _ 作業環境 _ が他の作業環境から分離されます。アカウント管理者がそのワークスペースに管理者を関連付けないと、ワークスペース管理者はワークスペース内の作業環境にアクセスできません。

稼働環境はストレージシステムを表します。

- シングルノードクラウドボリューム ONTAP システムまたは HA ペア
- ネットワーク内のオンプレミス ONTAP クラスタ
- NetApp プライベートストレージ構成の ONTAP クラスタ

"ワークスペースを追加する方法について説明します"。

コネクタ

Cloud Manager は、パブリッククラウド環境内のリソースやプロセスを管理できます。Connector は、クラウ

ドプロバイダに導入する仮想マシンインスタンス、または設定したオンプレミスホストで実行されます。

1 つのコネクタを複数のネットアップクラウドデータサービスで使用できます。たとえば、 Cloud Manager のコネクタをすでに持っている場合は、 Cloud Tiering サービスのセットアップ時にコネクタを選択できます。

"コネクタの詳細については、こちらをご覧ください"。

サブスクリプション

選択したアカウントに関連付けられているネットアップのサブスクリプションです。

クラウドプロバイダのマーケットプレイスから Cloud Manager にサブスクライブすると、 Cloud Central にリダイレクトされます。この場合、サブスクリプションを保存して特定のアカウントに関連付ける必要があります。

登録が完了すると、「アカウントの管理」ウィジェットから各サブスクリプションが利用できるようになります。現在表示しているアカウントに関連付けられている月額プランのみが表示されます。

サブスクリプションの名前を変更したり、 1 つまたは複数のアカウントからサブスクリプションの関連付けを解除したりすることができます。

たとえば、 2 つのアカウントがあり、それぞれが別々のサブスクリプションで課金されるとします。いずれかのアカウントとサブスクリプションの関連付けを解除することで、 Cloud Volume ONTAP 作業環境の作成時にそのアカウントのユーザが誤って誤ったサブスクリプションを選択しないようにすることができます。

"サブスクリプションの管理方法について説明します"。

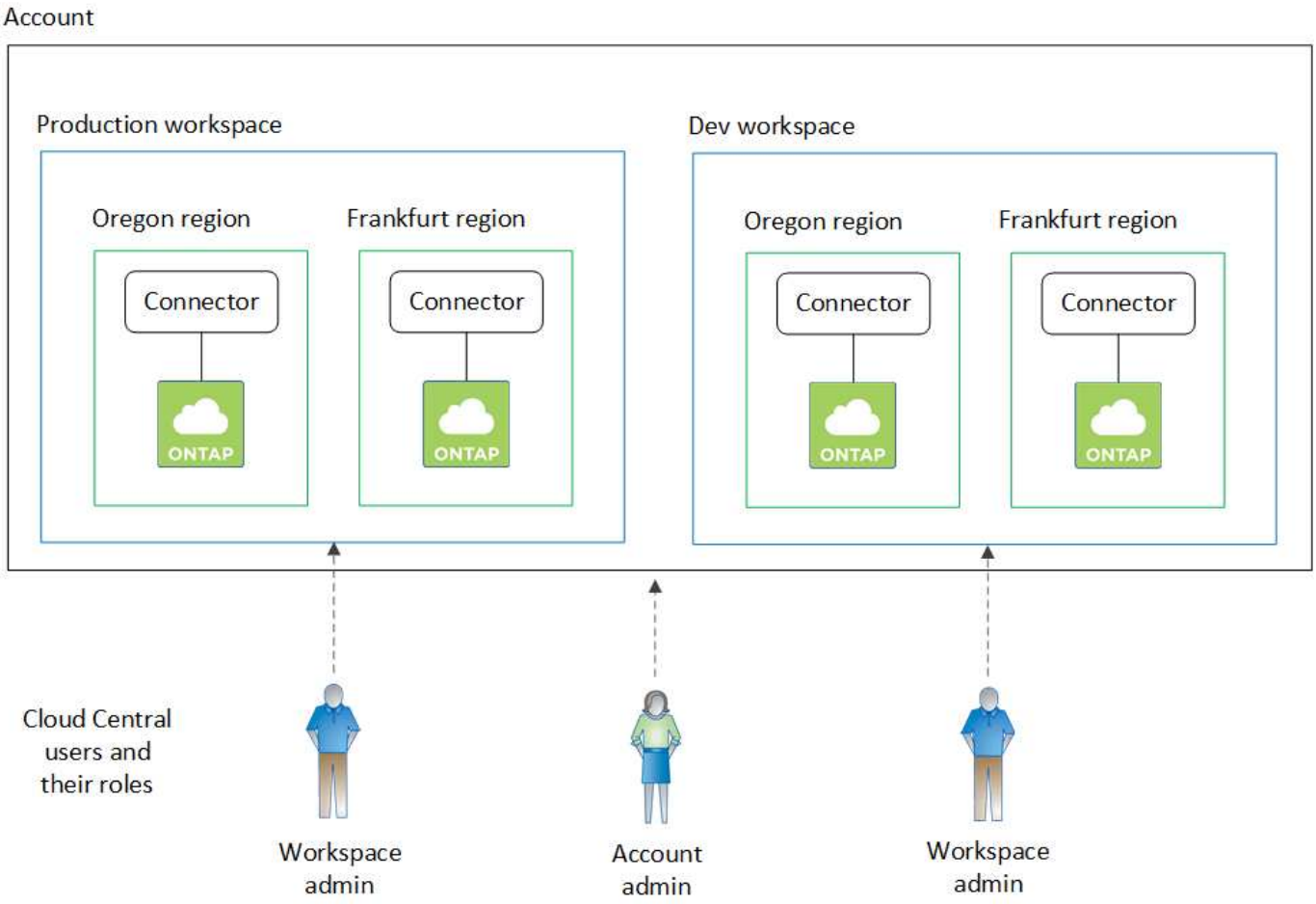
例

次の例は、アカウントの設定方法を示しています。

次のどちらの例のイメージも、コネクタと Cloud Volumes ONTAP システムは、実際にはクラウドプロバイダで実行されている *in* ネットアップアカウントには存在しません。これは、各コンポーネント間の関係の概念図です。

例 **1.**

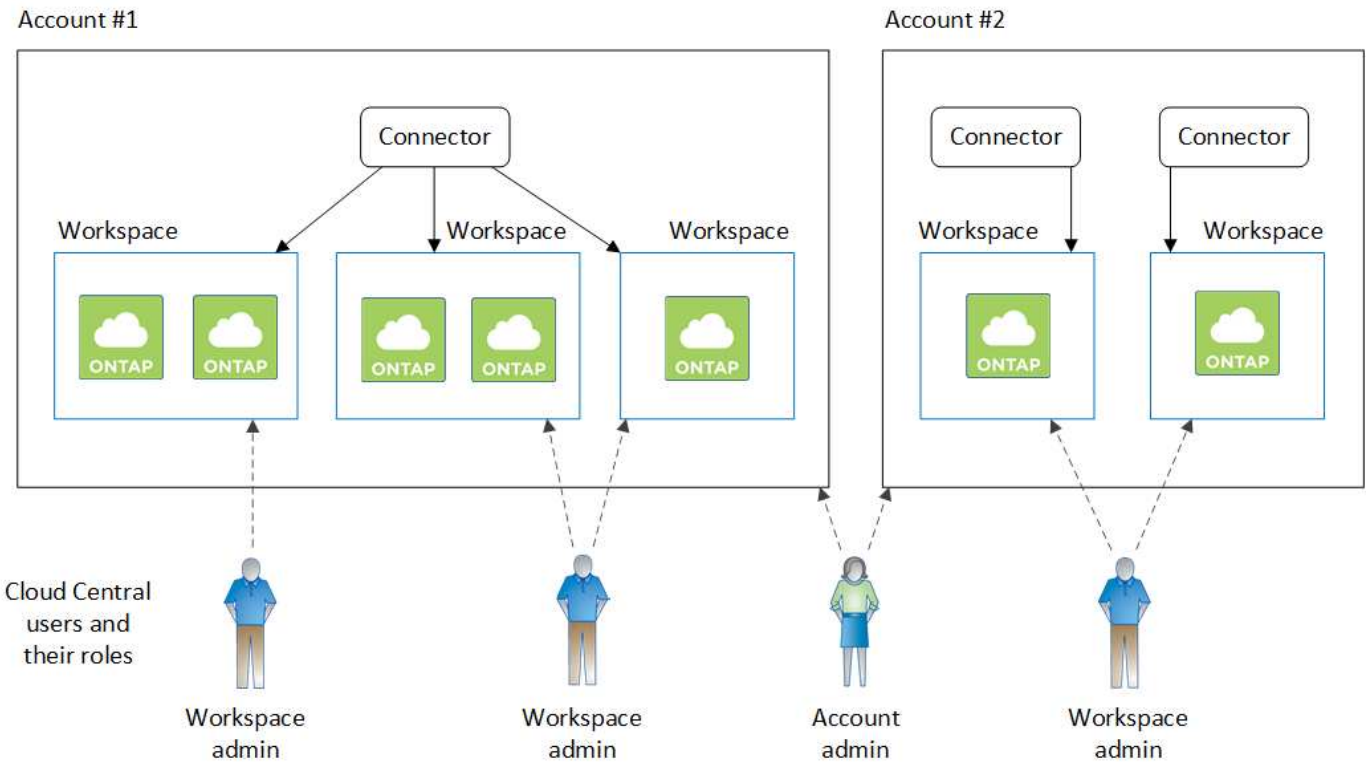
次の例は、 2 つのワークスペースを使用して分離された環境を作成するアカウントを示しています。1 つ目のワークスペースは本番環境用で、 2 つ目のワークスペースは開発環境用です。



例 **2**

次に、 2 つの異なるネットアップアカウントを使用した場合の、最も高度なマルチテナンシーの例を示します。たとえば、サービスプロバイダは、あるアカウントで Cloud Manager を使用して顧客にサービスを提供しながら、別のアカウントを使用して事業部門の 1 つにディザスタリカバリを提供することができます。

アカウント 2 には 2 つのコネクタがあります。これは、システムが別々の地域にある場合や、別々のクラウドプロバイダにある場合に発生することがあります。



ネットアップアカウントでワークスペースとユーザをセットアップ

Cloud Manager に初めてログインするときは、 _netapp アカウント _ を作成するように求められます。このアカウントはマルチテナンシーを提供し、分離されたワークスペース内でユーザとリソースを整理することができます。

"ネットアップアカウントの仕組みをご覧ください"。

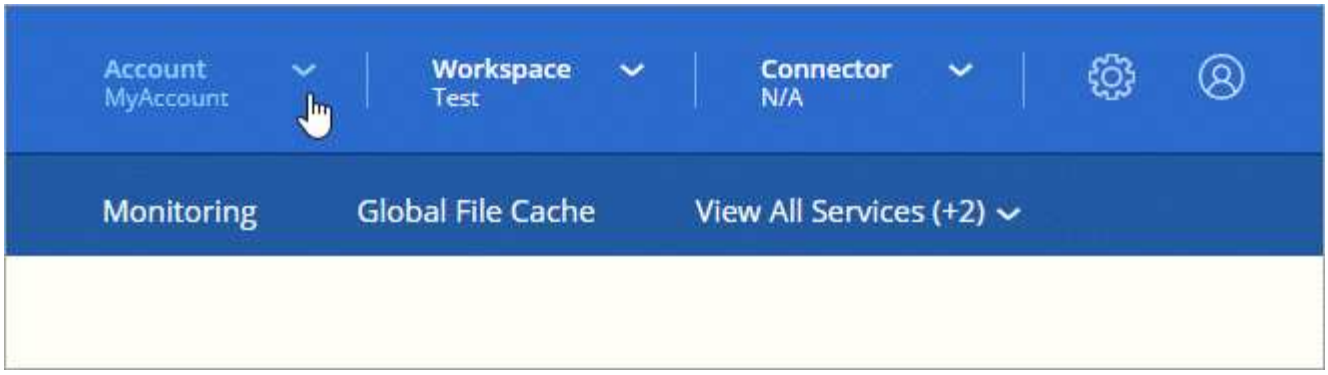
ユーザが Cloud Manager にアクセスしてワークスペース内の作業環境にアクセスできるように、ネットアップアカウントをセットアップします。1 人のユーザを追加するか、複数のユーザとワークスペースを追加するだけです。

ワークスペースを追加します

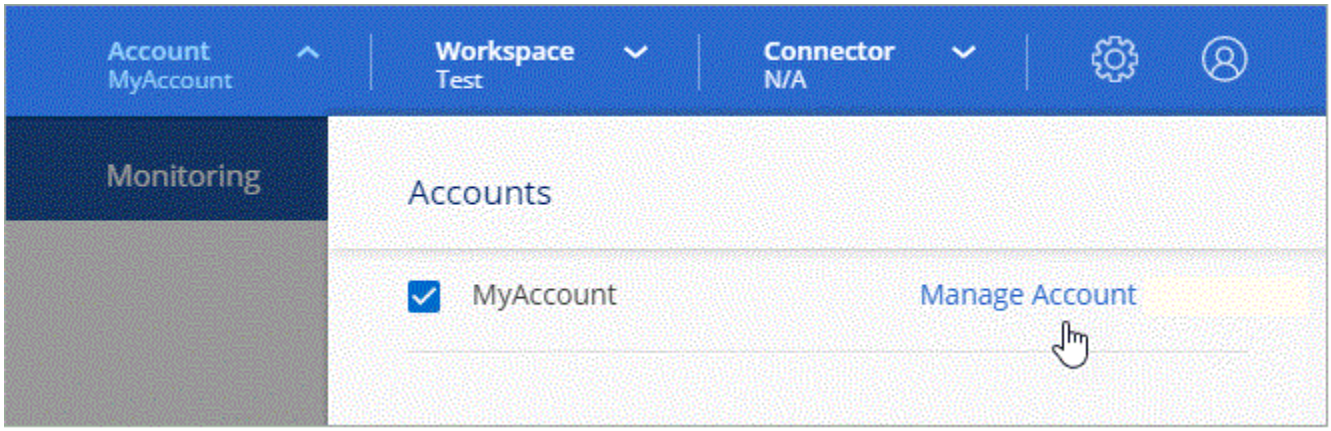
Cloud Manager のワークスペースを使用すると、作業環境のセットを他の作業環境や他のユーザから分離できます。たとえば、 2 つのワークスペースを作成し、各ワークスペースに別々のユーザーを関連付けることができます。

手順

1. の上部から "クラウドマネージャ"をクリックし、 [**Account**] ドロップダウンをクリックします。



2. 現在選択されているアカウントの横にある ［ * アカウントの管理 * ］ をクリックします。



3. [* ワークスペース *] をクリックします。
4. [新規ワークスペースの追加] をクリックします。
5. ワークスペースの名前を入力し、 * 追加 * をクリックします。

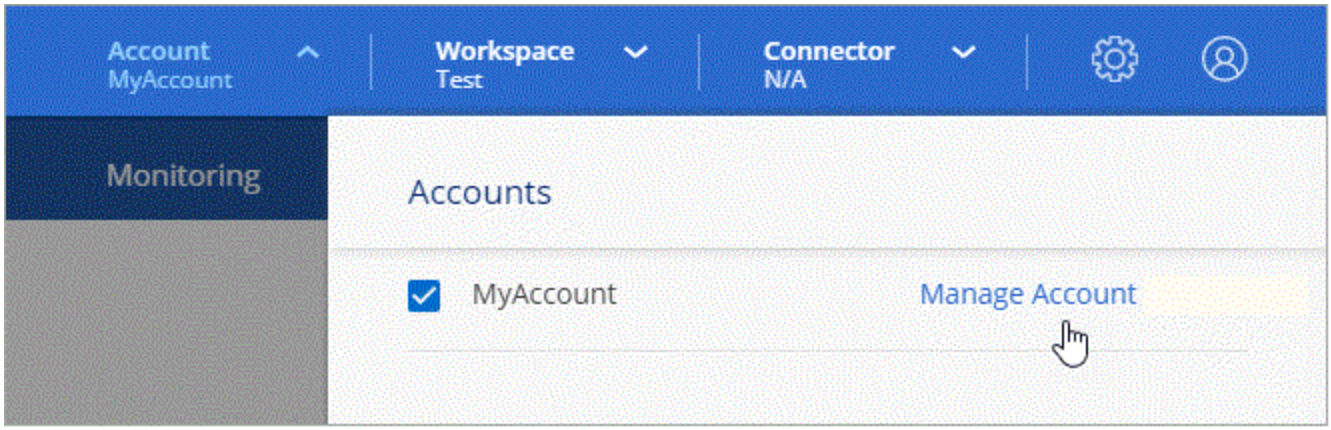
ワークスペース管理者がこのワークスペースにアクセスする必要がある場合は、ユーザーを関連付ける必要があります。また、ワークスペース管理者がコネクタを使用できるように、コネクタをワークスペースに関連付ける必要があります。

ユーザを追加します

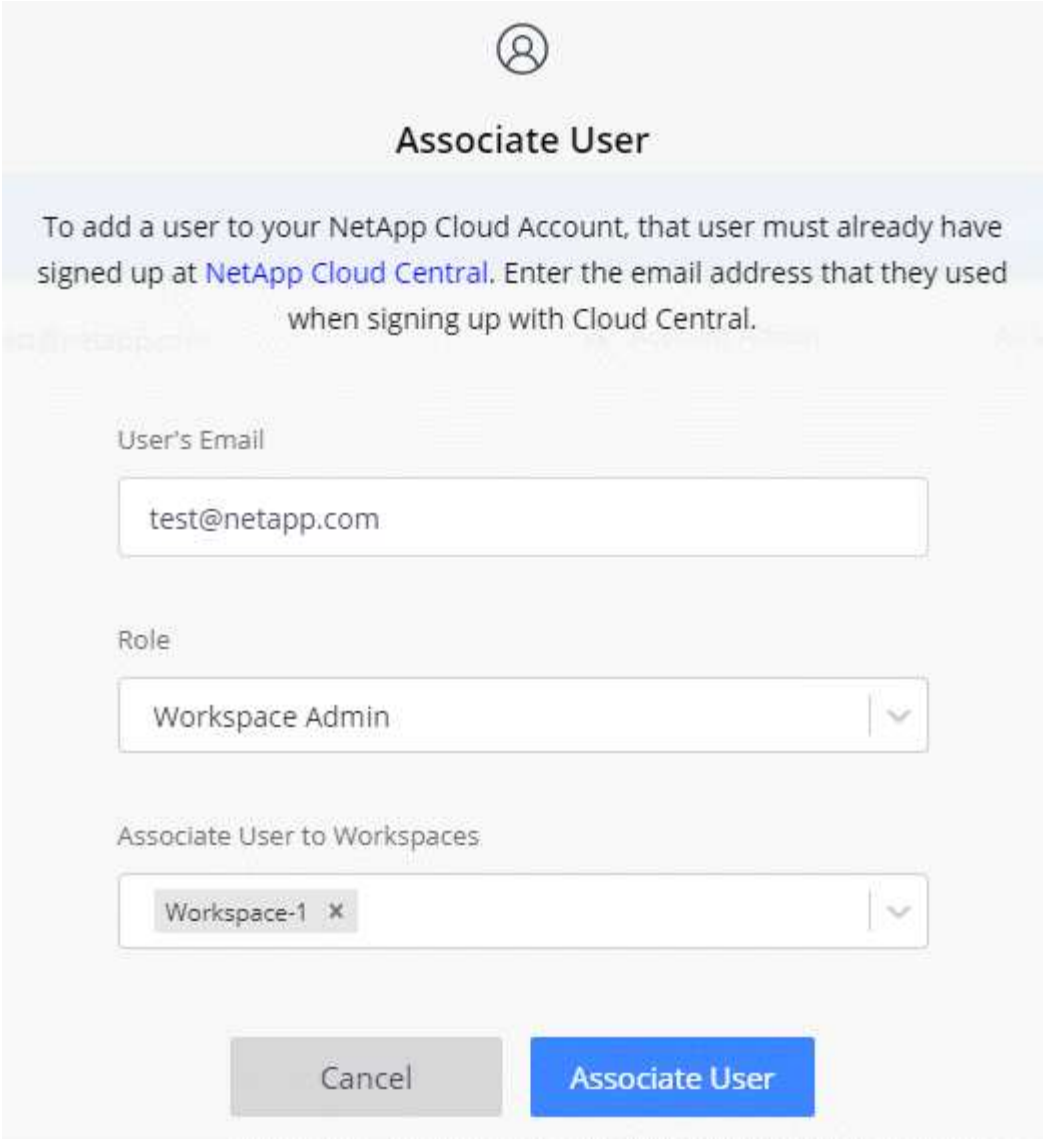
Cloud Central ユーザをネットアップアカウントに関連付けて、これらのユーザが Cloud Manager で作業環境を作成および管理できるようにします。

手順

1. ユーザーがまだ行っていない場合は、にアクセスするようにユーザーに依頼します "NetApp Cloud Central" 登録してください。
2. の上部から "クラウドマネージャ"をクリックし、 [**Account**] ドロップダウンをクリックして、 [**Manage Account**] をクリックします。



3. メンバータブで、 * ユーザーを関連付け * をクリックします。
4. ユーザの E メールアドレスを入力し、ユーザのロールを選択します。
   - * アカウント管理者 * ： Cloud Manager で任意の操作を実行できます。
   - * ワークスペース管理者 * ：割り当てられたワークスペースでリソースを作成および管理できます。
   - * Compliance Viewer * ：クラウドデータセンスガバナンスおよびコンプライアンス情報のみを表示し、アクセス権のあるワークスペースのレポートを生成できます。
   - * SnapCenter Admin* ： SnapCenter サービスを使用して、アプリケーションと整合性のあるバックアップを作成し、それらのバックアップを使用してデータをリストアできます。このサービスは現在ベータ版です。
5. Account Admin 以外のアカウントを選択した場合は、そのユーザに関連付けるワークスペースを 1 つ以上選択します。



6. [関連付け（ Associate ）] をクリックします。

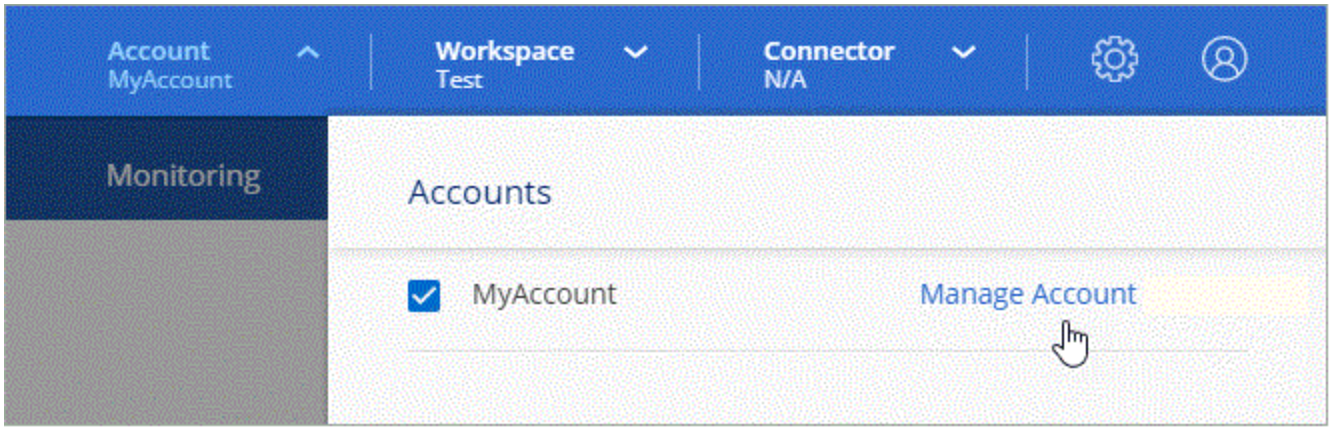
ユーザには、 NetApp Cloud Central の「 Account Association 」というタイトルの E メールが送信されます。 E メールには、 Cloud Manager にアクセスするために必要な情報が記載されています。

ワークスペース管理者をワークスペースに関連付けます

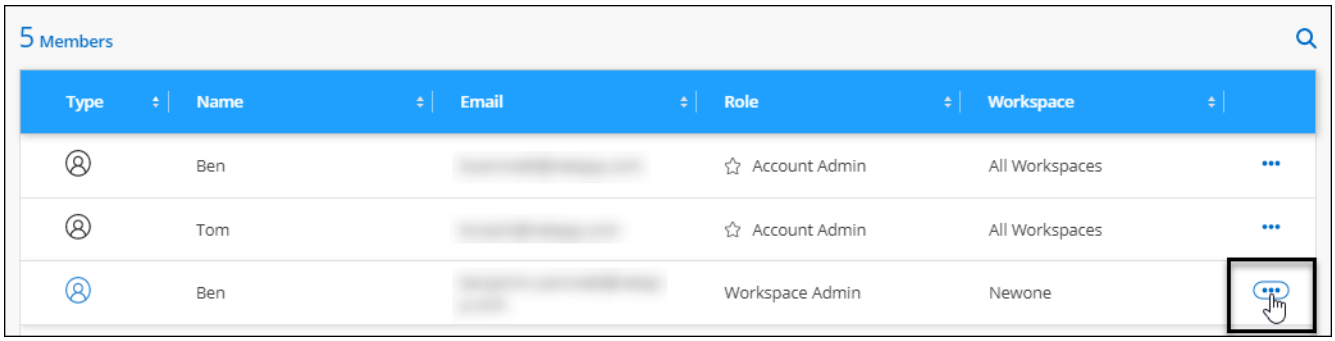
ワークスペース管理者は、いつでも追加のワークスペースに関連付けることができます。ユーザーを関連付けると、ワークスペース内の作業環境を作成して表示できます。

手順

1. Cloud Manager の上部で、 * Account * ドロップダウンをクリックし、 * Manage Account * をクリックします。



2. メンバー (Members) タブで ' ユーザーに対応する行のアクションメニューをクリックします



3. * ワークスペースの管理 * をクリックします。
4. 1 つ以上のワークスペースを選択し、 * 適用 * をクリックします。

コネクタがワークスペースにも関連付けられていれば、ユーザは Cloud Manager からこれらのワークスペースにアクセスできるようになりました。

コネクタをワークスペースに関連付けます

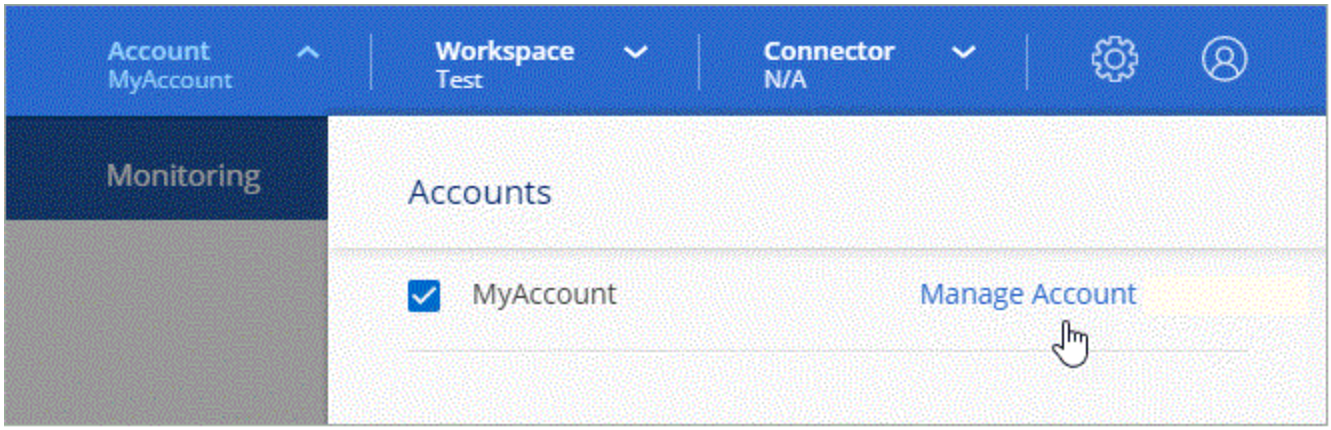
ワークスペース管理者がコネクタを使用して Cloud Volumes ONTAP システムを作成できるように、コネクタをワークスペースに関連付ける必要があります。

アカウント管理者のみがいる場合は、コネクタをワークスペースに関連付ける必要はありません。アカウント管理者は、デフォルトで Cloud Manager のすべてのワークスペースにアクセスできます。

"ユーザー、ワークスペース、コネクターの詳細をご覧ください"。

手順

1. Cloud Manager の上部で、 * Account * ドロップダウンをクリックし、 * Manage Account * をクリックします。



2. コネクター（ * Connector ）をクリックします。
3. 関連付けるコネクタの * ワークスペースの管理 * をクリックします。
4. 1 つ以上のワークスペースを選択し、 * 適用 * をクリックします。

ワークスペース管理者は、これらのコネクタを使用して Cloud Volumes ONTAP システムを作成できるようになりました。

次の手順

アカウントの設定が完了したので、ユーザーの削除、ワークスペース、コネクタ、およびサブスクリプションの管理によって、いつでもアカウントを管理できます。 "アカウントの管理方法について説明します"。

コネクタをセットアップします

コネクタについて説明します

ほとんどの場合、アカウント管理者は _ コネクタ _ をクラウドまたはオンプレミスネットワークに導入する必要があります。Connector は、 Cloud Manager を日常的に使用するための重要なコンポーネントです。Connector を使用すると、 Cloud Manager 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できます。

コネクタが必要な場合

Cloud Manager の多くの機能やサービスを使用するには、コネクタが必要です。

サービス

- ONTAP 管理機能用の Amazon FSX
- Amazon S3 バケットの検出
- クラウドバックアップ
- クラウドデータの意味
- クラウド階層化
- Cloud Volumes ONTAP

- グローバルファイルキャッシュ
- Kubernetes クラスタ
- 監視
- オンプレミスの ONTAP クラスタ

次のサービスには、コネクタが * _ ではありません _ * 。

- Active IQ デジタルアドバイザ
- 作業環境の作成にはコネクタは必要ありませんが、 ONTAP FSX for ONTAP を作成して管理し、データをレプリケートし、データセンスや Cloud Sync などの クラウド サービス と FSX for を統合する必要があります。
- Azure NetApp Files の特長

  Azure NetApp Files のセットアップと管理にコネクタは必要ありませんが、 Azure NetApp Files データのスキャンにクラウドデータセンスを使用する場合はコネクタが必要です。
- Cloud Volumes Service for Google Cloud
- Cloud Sync

デジタルウォレット

ほとんどの場合、コネクタなしでデジタルウォレットにライセンスを追加できます。

デジタルウォレットにライセンスを追加するためにコネクタが必要なのは、 Cloud Volumes ONTAP ノードベースのライセンスのみです。この場合、 Cloud Volumes ONTAP システムにインストールされているライセンスのデータを使用するため、コネクタが必要です。

サポートされている場所

コネクタは次の場所でサポートされています。

- Amazon Web Services の
- Microsoft Azure
- Google Cloud
- オンプレミス
- インターネットに接続できない、オンプレミス

Azure の導入についての注意

Azure でコネクタを導入する場合は、コネクタを管理する Cloud Volumes ONTAP システムと同じ Azure リージョンまたはに導入する必要があります "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 での Azure プライベートリンクの使用方法をご確認ください"。

Google Cloud の導入についての注意

Google Cloud で Cloud Volumes ONTAP システムを作成する場合は、 Google Cloud でも実行されているコネ

クタが必要です。AWS 、 Azure 、オンプレミスで実行されているコネクタは使用できません。

共有 Linux ホストはサポートされません

コネクタは、他のアプリケーションと共有されている VM ではサポートされません。VM は、コネクタソフトウェア専用にする必要があります。

サードパーティのエージェントと内線番号

Connector VM では、サードパーティのエージェントや VM 拡張機能はサポートされません。

コネクタは動作したままにしてください

コネクタは常時稼働している必要があります。有効にするサービスの継続的な健常性と運用性にとって重要です。

たとえば、 Cloud Volumes ONTAP PAYGO システムの正常性と運用においては、コネクタが重要な要素です。コネクタの電源がオフの場合、 Cloud Volumes ONTAP PAYGO システムは、コネクタとの通信を 14 日以上失った後にシャットダウンします。

コネクタを作成する方法

Workspace 管理者が Cloud Volumes ONTAP 作業環境を作成し、上記の他の機能を使用するには、アカウント管理者がコネクタを作成する必要があります。

アカウント管理者は、さまざまな方法でコネクタを作成できます。

- Cloud Manager から直接（推奨）
  - "AWS でを作成します"
  - "Azure で作成します"
  - "GCP で作成します"
- ソフトウェアを手動で独自の Linux ホストにインストールする
  - "インターネットにアクセスできるホスト"
  - "インターネットにアクセスできないオンプレミスのホスト"
- クラウドプロバイダのマーケットプレイスから
  - "AWS Marketplace"
  - "Azure Marketplace で入手できます"

操作を完了するためにコネクタが必要な場合は、 Cloud Manager からコネクタの作成を求められます。

権限

コネクタを作成するには特定の権限が必要であり、コネクタインスタンス自体に別の権限セットが必要です。

コネクタを作成する権限

Cloud Manager からコネクタを作成するユーザには、任意のクラウドプロバイダにインスタンスを導入するための特定の権限が必要です。Connector を作成するときは、 Cloud Manager に権限の要件が通知されま

す。

"各クラウドプロバイダのポリシーを表示します"。

コネクタインスタンスの権限

Connector で処理を実行するには、特定のクラウドプロバイダの権限が必要です。たとえば、 Cloud Volumes ONTAP を導入して管理するには、のように指定します。

Cloud Manager から直接コネクタを作成すると、必要な権限を持つコネクタが Cloud Manager によって作成されます。必要なことは何もありません。

コネクタを AWS Marketplace 、 Azure Marketplace 、またはソフトウェアを手動でインストールして作成する場合は、適切な権限が設定されていることを確認する必要があります。

"各クラウドプロバイダのポリシーを表示します"

コネクタごとの作業環境数

1 つのコネクタで複数の作業環境を Cloud Manager で管理できます。1 つのコネクタで管理できる作業環境の最大数は、環境によって異なります。管理対象は、作業環境の種類、ボリュームの数、管理対象の容量、ユーザの数によって異なります。

大規模な導入の場合は、ネットアップの担当者にご相談のうえ、環境のサイジングを行ってください。途中で問題が発生した場合は、製品内のチャットでお問い合わせください。

複数のコネクタを使用する場合

コネクタが 1 つしか必要ない場合もありますが、 2 つ以上のコネクタが必要な場合もあります。

次にいくつかの例を示します。

- マルチクラウド環境（ AWS と Azure ）を使用しているため、 AWS と Azure のコネクタが 1 つずつ必要です。各で、それらの環境で実行される Cloud Volumes ONTAP システムを管理します。
- サービスプロバイダは、 1 つのネットアップアカウントを使用してお客様にサービスを提供しながら、別のアカウントを使用してお客様のビジネスユニット 1 つにディザスタリカバリを提供することができます。アカウントごとに個別のコネクタがあります。

同じ作業環境で複数のコネクタを使用する

ディザスタリカバリ目的で、複数のコネクタを備えた作業環境を同時に管理できます。一方のコネクタが停止した場合は、もう一方のコネクタに切り替えて、作業環境をただちに管理できます。

この構成をセットアップするには：

1. "別のコネクタに切り替えます"
2. 既存の作業環境を検出
   - "既存の Cloud Volumes ONTAP システムを Cloud Manager に追加"
   - "ONTAP クラスタを検出"
3. を設定します "Capacity Management Mode （容量管理モード）"

メインコネクターのみ * オートマチックモード * に設定する必要があります。DR 目的で別のコネクタに切り替える場合は、必要に応じて容量管理モードを変更できます。

コネクタを切り替えるタイミング

最初のコネクタを作成すると、新しく作成する作業環境ごとに、そのコネクタが Cloud Manager によって自動的に使用されます。コネクタを追加で作成したら、コネクタを切り替えることで各コネクタに固有の作業環境を確認する必要があります。

"コネクタを切り替える方法について説明します"。

ローカルユーザインターフェイス

ではほぼすべてのタスクを実行する必要がありますが "SaaS ユーザインターフェイス"では、ローカルユーザーインターフェースは引き続きコネクターで使用できます。このインターフェイスは、インターネットにアクセスできない環境に Connector をインストールする場合や、 SaaS インターフェイスではなくコネクタ自体から実行する必要があるいくつかのタスクの場合に必要になります。

- "プロキシサーバを設定しています"
- パッチをインストールしています （通常はネットアップの担当者と協力してパッチをインストールします）
- AutoSupport メッセージをダウンロードしています （通常は問題が発生したときにネットアップの担当者が指示）

"ローカル UI へのアクセス方法について説明します"。

コネクタのアップグレード

Connector は、ソフトウェアが最新バージョンである限り、自動的にソフトウェアを更新します "アウトバウンドインターネットアクセス" をクリックしてソフトウェアアップデートを入手します。

コネクタのネットワークを設定します

コネクタがパブリッククラウド環境内のリソースや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。最も重要なステップは、さまざま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を確保することです。

このページの情報は、コネクタがアウトバウンドインターネットアクセスを持つ一般的な配置用です。

ネットワークでインターネットへのすべての通信にプロキシサーバを使用している場合は、 [設定] ページでプロキシサーバを指定できます。を参照してください "プロキシサーバを使用するようにコネクタを設定します"。

ターゲットネットワークへの接続

コネクタには、作成する作業環境の種類と、有効にする予定のサービスへのネットワーク接続が必要です。

たとえば、企業ネットワークにコネクタを設置する場合は、 Cloud Volumes ONTAP を起動する VPC または VNet への VPN 接続を設定する必要があります。

172 の範囲の **IP** アドレスと競合する可能性があります

Cloud Manager は、 172.17.0.0/16 と 172.18.0.0/16 の範囲に IP アドレスを持つ 2 つのインターフェイスを使用してコネクタを展開します。

これらの範囲のいずれかでネットワークのサブネットが設定されている場合、 Cloud Manager から接続エラーが発生することがあります。たとえば、 Cloud Manager でオンプレミスの ONTAP クラスタを検出すると失敗することがあります。

回避策は、コネクタのインターフェイスの IP アドレスを変更します。ネットアップサポートにお問い合わせください。

アウトバウンドインターネットアクセス

コネクタからのアウトバウンドインターネットアクセスが必要です。

パブリッククラウド環境内のリソースを管理するためのエンドポイント

Connector では、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アウトバウンドインターネットアクセスが必要です。

エンドポイント	目的
\ https://support.netapp.com	ライセンス情報を取得し、ネットアップサポートに AutoSupport メッセージを送信するため。
\ https://*.cloudmanager.cloud.netapp.com	Cloud Manager 内で SaaS の機能やサービスを提供できます。
¥ https://cloudmanagerinfraprod.azurecr.io ¥ https://*.blob.core.windows.net	をクリックして、 Connector と Docker コンポーネントをアップグレードします。

Linux ホストにコネクタをインストールするエンドポイント

Connector ソフトウェアは、手動でインストールすることもできます。その場合、 Connector のインストーラは、インストールプロセス中に次の URL にアクセスする必要があります。

- https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
- https://s3.amazonaws.com/aws-cli/awscli-bundle.zip
- ¥ https://*.blob.core.windows.net または ¥ https://hub.docker.com

ホストは、インストール中にオペレーティングシステムパッケージの更新を試みる可能性があります。ホストは、これらの OS パッケージの別のミラーリングサイトにアクセスできます。

ポートおよびセキュリティグループ

コネクタへの着信トラフィックは、開始しない限りありません。へのアクセスは、 HTTP および HTTPS を使用して提供されます "ローカル UI"は、まれな状況で使用します。SSH が必要になるのは、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のみです。

AWS のコネクタのルール

コネクタのセキュリティグループには、インバウンドとアウトバウンドの両方のルールが必要です。

インバウンドルール

プロトコル	ポート	目的
SSH	22	コネクタホストへの SSH アクセスを提供します
HTTP	80	クライアント Web ブラウザからローカルユーザインターフェイスへの HTTP アクセス、および Cloud Data Sense からの接続を提供します
HTTPS	443	クライアント Web ブラウザからローカルへの HTTPS アクセスを提供します ユーザインターフェイス
TCP	3128	AWS ネットワークで NAT やプロキシを使用していない場合に、 Cloud Data Sense インスタンスにインターネットアクセスを提供します
TCP	9060	Cloud Data Sense を有効にして使用できる（ GovCloud 環境の場合のみ必要）

アウトバウンドルール

コネクタの事前定義されたセキュリティグループは、すべての発信トラフィックを開きます。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

コネクタの事前定義されたセキュリティグループには、次のアウトバウンドルールが含まれています。

プロトコル	ポート	目的
すべての TCP	すべて	すべての発信トラフィック
すべての UDP	すべて	すべての発信トラフィック

高度なアウトバウンドルール

発信トラフィックに固定ルールが必要な場合は、次の情報を使用して、コネクタによる発信通信に必要なポートだけを開くことができます。

送信元 IP アドレスは、コネクタホストです。

サービス	プロトコル	ポート	宛先	目的
Active Directory	TCP	88	Active Directory フォレスト	Kerberos V 認証
	TCP	139	Active Directory フォレスト	NetBIOS サービスセッション
	TCP	389	Active Directory フォレスト	LDAP
	TCP	445	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	TCP	464	Active Directory フォレスト	Kerberos V パスワードの変更と設定（ SET_CHANGE ）
	TCP	749	Active Directory フォレスト	Active Directory Kerberos v の変更とパスワードの設定（ RPCSEC_GSS ）
	UDP	137	Active Directory フォレスト	NetBIOS ネームサービス
	UDP	138	Active Directory フォレスト	NetBIOS データグラムサービス
	UDP	464	Active Directory フォレスト	Kerberos キー管理
API コールと AutoSupport	HTTPS	443	アウトバウンドインターネットおよび ONTAP クラスタ管理 LIF	AWS および ONTAP への API コール、およびネットアップへの AutoSupport メッセージの送信
API コール	TCP	3000	ONTAP HA メディエーター	ONTAP HA メディエーターとの通信
	TCP	8088	S3 へのバックアップ	S3 へのバックアップを API で呼び出します
DNS	UDP	53	DNS	Cloud Manager による DNS 解決に使用されます
クラウドデータの意味	HTTP	80	Cloud Data Sense インスタンス	Cloud Volumes ONTAP に最適なクラウドデータ

Azure のコネクタのルール

コネクタのセキュリティグループには、インバウンドとアウトバウンドの両方のルールが必要です。

インバウンドルール

ポート	プロトコル	目的
22	SSH	コネクタホストへの SSH アクセスを提供します
80	HTTP	クライアント Web ブラウザからローカルへの HTTP アクセスを提供します ユーザインターフェイス
443	HTTPS	クライアント Web ブラウザからローカルへの HTTPS アクセスを提供します ユーザインターフェイス

アウトバウンドルール

コネクタの事前定義されたセキュリティグループは、すべての発信トラフィックを開きます。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

コネクタの事前定義されたセキュリティグループには、次のアウトバウンドルールが含まれています。

ポート	プロトコル	目的
すべて	すべての TCP	すべての発信トラフィック
すべて	すべての UDP	すべての発信トラフィック

高度なアウトバウンドルール

発信トラフィックに固定ルールが必要な場合は、次の情報を使用して、コネクタによる発信通信に必要なポートだけを開くことができます。

送信元 IP アドレスは、コネクタホストです。

サービス	ポート	プロトコル	宛先	目的
Active Directory	88	TCP	Active Directory フォレスト	Kerberos V 認証
	139	TCP	Active Directory フォレスト	NetBIOS サービスセッション
	389	TCP	Active Directory フォレスト	LDAP
	445	TCP	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	464	TCP	Active Directory フォレスト	Kerberos V パスワードの変更と設定（ SET_CHANGE ）
	749	TCP	Active Directory フォレスト	Active Directory Kerberos v の変更とパスワードの設定（ RPCSEC_GSS ）
	137	UDP	Active Directory フォレスト	NetBIOS ネームサービス
	138	UDP	Active Directory フォレスト	NetBIOS データグラムサービス
	464	UDP	Active Directory フォレスト	Kerberos キー管理
API コールと AutoSupport	443	HTTPS	アウトバウンドインターネットおよび ONTAP クラスタ管理 LIF	AWS および ONTAP への API コール、およびネットアップへの AutoSupport メッセージの送信
DNS	53	UDP	DNS	Cloud Manager による DNS 解決に使用されます

GCP のコネクターのルール

コネクタのファイアウォールルールには、インバウンドとアウトバウンドの両方のルールが必要です。

インバウンドルール

プロトコル	ポート	目的
SSH	22	コネクタホストへの SSH アクセスを提供します
HTTP	80	クライアント Web ブラウザからローカルへの HTTP アクセスを提供します ユーザインターフェイス

プロトコル	ポート	目的
HTTPS	443	クライアント Web ブラウザからローカルへの HTTPS アクセスを提供します ユーザインターフェイス

アウトバウンドルール

コネクタの定義済みファイアウォールルールによって、すべてのアウトバウンドトラフィックが開かれます。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

コネクタの定義済みファイアウォールルールには、次のアウトバウンドルールが含まれています。

プロトコル	ポート	目的
すべての TCP	すべて	すべての発信トラフィック
すべての UDP	すべて	すべての発信トラフィック

高度なアウトバウンドルール

発信トラフィックに固定ルールが必要な場合は、次の情報を使用して、コネクタによる発信通信に必要なポートだけを開くことができます。

送信元 IP アドレスは、コネクタホストです。

サービス	プロトコル	ポート	宛先	目的
Active Directory	TCP	88	Active Directory フォレスト	Kerberos V 認証
	TCP	139	Active Directory フォレスト	NetBIOS サービスセッション
	TCP	389	Active Directory フォレスト	LDAP
	TCP	445	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	TCP	464	Active Directory フォレスト	Kerberos V パスワードの変更と設定（ SET_CHANGE ）
	TCP	749	Active Directory フォレスト	Active Directory Kerberos v の変更とパスワードの設定（ RPCSEC_GSS ）
	UDP	137	Active Directory フォレスト	NetBIOS ネームサービス
	UDP	138	Active Directory フォレスト	NetBIOS データグラムサービス
	UDP	464	Active Directory フォレスト	Kerberos キー管理
API コールと AutoSupport	HTTPS	443	アウトバウンドインターネットおよび ONTAP クラスタ管理 LIF	GCP および ONTAP への API コール、およびネットアップへの AutoSupport メッセージの送信
DNS	UDP	53	DNS	Cloud Manager による DNS 解決に使用されます

オンプレミスコネクタ用のポート

コネクタは、オンプレミスの Linux ホストに手動でインストールする場合、下記の _ インバウンド _ ポートを使用します。

これらのインバウンドルールは、オンプレミスコネクタの両方の配置モデルに適用されます。つまり、インターネットアクセスがインストールされているか、インターネットアクセスがないかです。

プロトコル	ポート	目的
HTTP	80	クライアント Web ブラウザからローカルへの HTTP アクセスを提供します ユーザインターフェイス

プロトコル	ポート	目的
HTTPS	443	クライアント Web ブラウザからローカルへの HTTPS アクセスを提供します ユーザインターフェイス

Cloud Manager から AWS にコネクタを作成します

Cloud Manager のほとんどの機能を使用するには、 Account Admin が _ Connector を導入する必要があります。 "コネクタが必要になるタイミングを学習します"。Connector を使用すると、 Cloud Manager 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できます。

このページでは、 Cloud Manager から AWS でコネクタを直接作成する方法について説明します。 "コネクタを配置するその他の方法について説明します"。

これらの手順は、 Account Admin ロールを持つユーザが実行する必要があります。ワークスペース管理者はコネクタを作成できません。

最初の Cloud Volumes ONTAP 作業環境を作成する際、まだコネクタがない場合は、 Cloud Manager からコネクタの作成を求められます。

AWS 認証をセットアップする

Cloud Manager で VPC にコネクタインスタンスを導入するには、 AWS で認証する必要があります。次のいずれかの認証方式を選択できます。

- Cloud Manager に IAM ロールを割り当てます
- IAM ユーザの AWS アクセスキーとシークレットキーを指定します

使用する認証方式に、 Connector インスタンスを AWS に導入するための必要な権限がある必要があります。

IAM ロールを設定する

Cloud Manager で Connector を AWS に導入するために想定できる IAM ロールを設定します。

手順

1. からコネクタ IAM ポリシーをダウンロードします "Cloud Manager Policies ページ"。

   このポリシーには、 AWS でコネクタを作成するために必要な権限が含まれています。Cloud Manager は、作成時にコネクタインスタンスに新しい権限セットを適用します。

2. ターゲットアカウントの AWS IAM コンソールに移動します。
3. [アクセス管理] で、 [役割] 、 [役割の作成 *] の順にクリックし、手順に従って役割を作成します。

   必ず次の手順を実行してください。

   - 信頼されるエンティティのタイプ * 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、 Cloud Manager SaaS アカウントの ID として「 952013314444 」

を入力してください

- 以前にダウンロードしたコネクタ IAM ポリシーに表示されている権限を含むポリシーを作成します。

4. IAM ロールのロール ARN をコピーして、コネクタの作成時に Cloud Manager に貼り付けることができるようにします。

IAM ロールに必要な権限が割り当てられます。

IAM ユーザの権限を設定します

コネクタを作成するときに、 Connector インスタンスの導入に必要な権限を持つ IAM ユーザに AWS アクセスキーとシークレットキーを指定できます。

手順

1. から Connector 展開ポリシーをダウンロードします "Cloud Manager Policies ページ"。

   この IAM ポリシーには、 AWS でコネクタを作成するために必要な権限が含まれています。Cloud Manager は、作成時にコネクタインスタンスに新しい権限セットを適用します。

2. AWS IAM コンソールで、コネクタ IAM ポリシーからコピーしたテキストを貼り付けて独自のポリシーを作成します。
3. 前の手順で作成したポリシーを、 Cloud Manager からコネクタを作成する IAM ユーザに関連付けます。
4. IAM ユーザのアクセスキーとシークレットキーにアクセスできることを確認します。

AWS ユーザに、 Cloud Manager からコネクタを作成するために必要な権限が付与されました。Cloud Manager からプロンプトが表示されたら、このユーザの AWS アクセスキーを指定する必要があります。

コネクタを作成します

Cloud Manager では、ユーザインターフェイスから AWS に直接コネクタを作成できます。

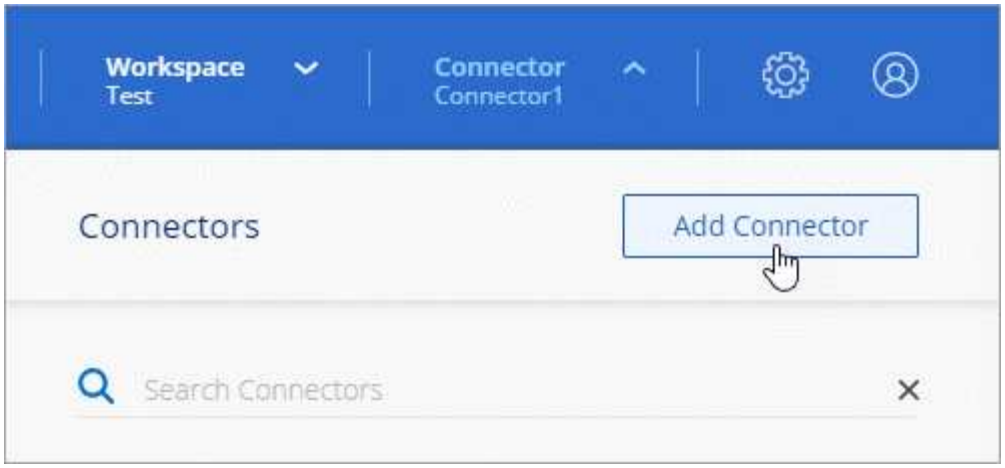
必要なもの

- AWS 認証方式： Cloud Manager が権限を持つ IAM ロールの ARN 、または IAM ユーザの AWS アクセスキーとシークレットキーのいずれかです。
- 選択した AWS リージョン内の VPC 、サブネット、キーペア。
- Cloud Manager でコネクタ用の IAM ロールが自動的に作成されないようにするには、専用のを作成する必要があります "使用するポリシー"。

  これらは、 Connector がパブリッククラウド環境内のリソースを管理するために必要な権限です。これは、コネクタインスタンスの作成時に指定したアクセス許可とは異なります。

手順

1. 最初の作業環境を作成する場合は、 * 作業環境の追加 * をクリックし、プロンプトに従います。それ以外の場合は、 [**connector**] ドロップダウンをクリックし、 [**Add connector**] を選択します。



2. クラウドプロバイダとして「 * Amazon Web Services * 」を選択し、「 * Continue * 」をクリックします。

   Connector は、作成する作業環境の種類や有効にするサービスへのネットワーク接続を確立する必要があることに注意してください。

   "Connector のネットワーク要件の詳細については、こちらをご覧ください"。

3. ウィザードの手順に従って、コネクタを作成します。
   - * 準備をしてください * ：必要なものを確認してください。
   - * AWS クレデンシャル * ： AWS リージョンを指定してから認証方式を選択します。認証方式は、 Cloud Manager が引き受けることができる IAM ロールか、 AWS のアクセスキーとシークレットキーのどちらかです。

     [*Assume Role] を選択した場合は、 Connector 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。クレデンシャルの追加のセットは、 [Credentials] ページから作成する必要があります。ウィザードのドロップダウンリストから使用できるようになります。 "クレデンシャルを追加する方法について説明します"。

   - * 詳細 * ：コネクタの詳細を入力します。
     - インスタンスの名前を入力します。
     - カスタムタグ（メタデータ）をインスタンスに追加します。
     - 必要な権限を含む新しいロールを Cloud Manager で作成するか、またはを使用して設定した既存のロールを選択するかを選択します "必要な権限"。
     - コネクタの 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ことも、カスタムキーを使用することもできます。
   - * ネットワーク * ：インスタンスに 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。
   - * セキュリティグループ * ：新しいセキュリティグループを作成するか、インバウンド HTTP 、 HTTPS 、 SSH アクセス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。

コネクタへの着信トラフィックは、開始しない限りありません。へのアクセスは、HTTP および HTTPS を使用して提供されます "ローカル UI"は、まれな状況で使用します。SSH が必要になるのは、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のみです。

◦ * 復習 * ：選択内容を確認して、設定が正しいことを確認してください。

4. [追加（ Add ）] をクリックします。

インスタンスの準備が完了するまでに約 7 分かかります。処理が完了するまで、ページには表示されたままにしておいてください。

ワークスペース管理者がコネクタを使用して Cloud Volumes ONTAP システムを作成できるように、コネクタをワークスペースに関連付ける必要があります。アカウント管理者のみがいる場合は、コネクタをワークスペースに関連付ける必要はありません。アカウント管理者は、デフォルトで Cloud Manager のすべてのワークスペースにアクセスできます。 "詳細はこちら。"。

Cloud Manager から Azure にコネクタを作成します

Cloud Manager のほとんどの機能を使用するには、 Account Admin が _ Connector を導入する必要があります。Connector を使用すると、 Cloud Manager 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できます。 "コネクタが必要になるタイミングを学習します"。

このページでは、 Cloud Manager から直接 Azure でコネクタを作成する方法について説明します。 "コネクタを配置するその他の方法について説明します"。

これらの手順は、 Account Admin ロールを持つユーザが実行する必要があります。ワークスペース管理者はコネクタを作成できません。

最初の Cloud Volumes ONTAP 作業環境を作成する際、まだコネクタがない場合は、 Cloud Manager からコネクタの作成を求められます。

概要

Connector を導入するには、 Azure で Connector VM を作成するために必要な権限を持つログインを Cloud Manager に付与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、 Microsoft アカウントでサインインします。このアカウントには Azure 固有の権限が必要です。これがデフォルトのオプションです。

   次の手順に従って、作業を開始してください。

2. Azure AD サービスプリンシパルの詳細を指定します。このサービスプリンシパルには、特定の権限も必要です。

   次の手順に従って、作業を開始してください。

Azure のリージョンに関する注意

コネクタは、管理対象の Cloud Volumes ONTAP システムまたはにある Azure リージョンと同じ Azure リージョンに導入する必要があります "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 での Azure プライベートリンクの使用方法をご確認ください"。

Azure アカウントを使用してコネクタを作成します

Azure でコネクタを作成するデフォルトの方法は、プロンプトが表示されたら Azure アカウントでログインすることです。ログインフォームは、 Microsoft が所有およびホストしています。クレデンシャルがネットアップに提供されていません。

Azure アカウントの権限を設定します

Cloud Manager からコネクタを導入する前に、 Azure アカウントが正しい権限を持っていることを確認する必要があります。

手順

1. をダウンロードします "コネクタの Azure ポリシー"。

   リンクを右クリックし、 [名前を付けてリンクを保存 ...] をクリックしてファイルをダウンロードする。

2. JSON ファイルを変更して、割り当て可能な範囲に Azure サブスクリプション ID を追加します。

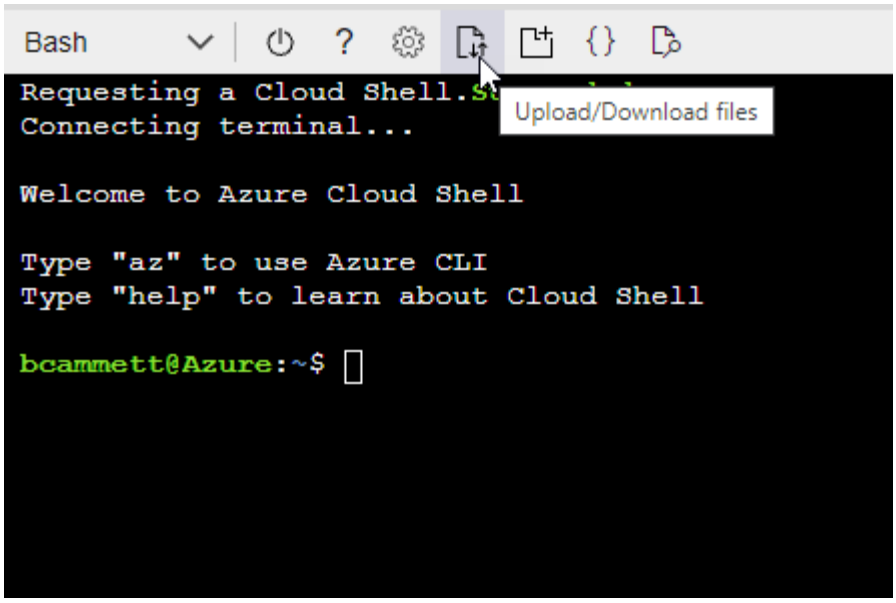
   ◦ 例 *

```
"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。

   次の手順は、 Azure Cloud Shell で Bash を使用してロールを作成する方法を示しています。

   a. 開始 "Azure Cloud Shell の略" 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 で次の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。

4. Cloud Manager からコネクタを導入するユーザにロールを割り当てます。
   a. [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。
   b. 「 * アクセスコントロール（ IAM ） * 」をクリックします。
   c. [* 追加 > 役割の割り当ての追加 *] をクリックして、権限を追加します。
      - Azure SetupAsService * ロールを選択し、 * 次へ * をクリックします。

        Azure SetupAsService は、で指定されているデフォルトの名前です "Azure の Connector 導入ポリシー"。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。

      - [* 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。
      - [* メンバーの選択 *] 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。
      - 「 * 次へ * 」をクリックします。
      - [レビュー + 割り当て（ Review + Assign ）] をクリックします。

Azure ユーザに、 Cloud Manager から Connector を導入するために必要な権限が付与されるようになりました。

Azure アカウントでログインしてコネクタを作成します

Cloud Manager では、ユーザインターフェイスから直接 Azure にコネクタを作成できます。

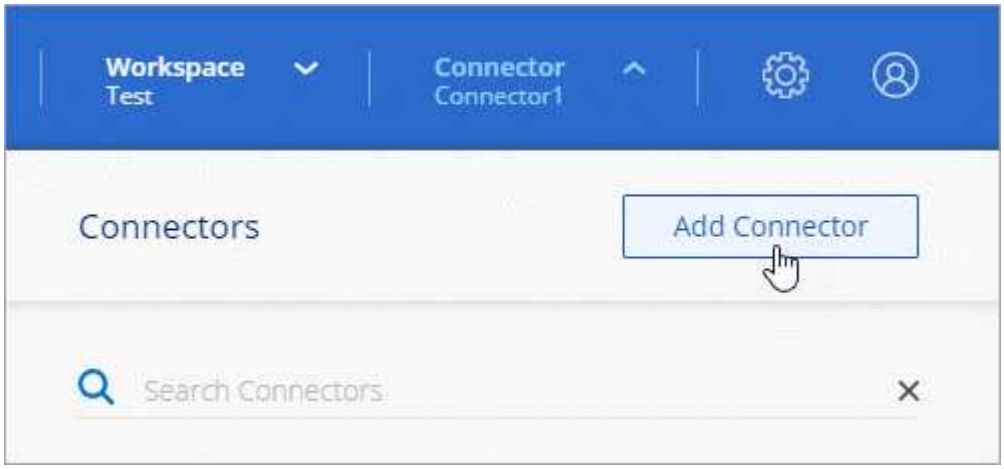
必要なもの

- Azure サブスクリプション。
- 選択した Azure リージョン内の VNet およびサブネット
- Cloud Manager で Connector 用の Azure ロールが自動的に作成されないようにするには、独自のを作成する必要があります "使用するポリシー"。

  これらの権限はコネクタインスタンス自体に適用されます。これは、以前にコネクタを展開するように設定したアクセス権とは異なります。

手順

1. 最初の作業環境を作成する場合は、 * 作業環境の追加 * をクリックし、プロンプトに従います。それ以外の場合は、 [**connector**] ドロップダウンをクリックし、 [**Add connector**] を選択します。



2. クラウドプロバイダとして「 * Microsoft Azure * 」を選択します。

   Connector は、作成する作業環境の種類や有効にするサービスへのネットワーク接続を確立する必要があることに注意してください。

   "Connector のネットワーク要件の詳細については、こちらをご覧ください"。

3. ウィザードの手順に従って、コネクタを作成します。

   ◦ * 準備完了 * ：必要なものを確認して、 * 次へ * をクリックしてください。

   ◦ プロンプトが表示されたら、 Microsoft アカウントにログインします。このアカウントには、仮想マシンの作成に必要な権限が付与されている必要があります。

   このフォームは、 Microsoft が所有およびホストしています。クレデンシャルがネットアップ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、そのアカウントは Cloud Manager によって自動的に使用されます。アカウントが複数ある場合は、適切なアカウントを使用するために、最初にログアウトする必要があります。

   ◦ * VM 認証 * ： 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、認証方法を選択します。

- * 詳細 * ：インスタンスの名前を入力し、タグを指定し、必要な権限を持つ新しいロールを Cloud Manager で作成するか、で設定した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ているサブスクリプションを選択できます。選択した各サブスクリプションには、 Cloud Volumes ONTAP をこれらのサブスクリプションに導入するための権限が Connector に付与されます。

- * ネットワーク * ： 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、および必要に応じてプロキシ設定を指定します。
- * セキュリティグループ * ：新しいセキュリティグループを作成するか、インバウンド HTTP 、 HTTPS 、 SSH アクセス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。

  コネクタへの着信トラフィックは、開始しない限りありません。へのアクセスは、 HTTP および HTTPS を使用して提供されます "ローカル UI"は、まれな状況で使用します。SSH が必要になるのは、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のみです。

- * 復習 * ：選択内容を確認して、設定が正しいことを確認してください。

4. [追加（ Add ）] をクリックします。

   仮想マシンの準備が完了するまでに約 7 分かかります。処理が完了するまで、ページには表示されたままにしておいてください。

ワークスペース管理者がコネクタを使用して Cloud Volumes ONTAP システムを作成できるように、コネクタをワークスペースに関連付ける必要があります。アカウント管理者のみがいる場合は、コネクタをワークスペースに関連付ける必要はありません。アカウント管理者は、デフォルトで Cloud Manager のすべてのワークスペースにアクセスできます。 "詳細はこちら。"。

サービスプリンシパルを使用してコネクタを作成します

Azure アカウントでログインする代わりに、必要な権限がある Azure サービスプリンシパルのクレデンシャルを Cloud Manager に入力することもできます。

サービスプリンシパルを使用した **Azure** 権限の付与

Azure Active Directory でサービスプリンシパルを作成およびセットアップし、 Cloud Manager で必要な Azure クレデンシャルを取得して、 Azure に Connector を導入するために必要な権限を付与します。

手順

1. [Create an Azure Active Directory application]。
2. [Assign the application to a role]。
3. [Add Windows Azure Service Management API permissions]。
4. [Get the application ID and directory ID]。
5. [Create a client secret]。

Azure Active Directory アプリケーションを作成します

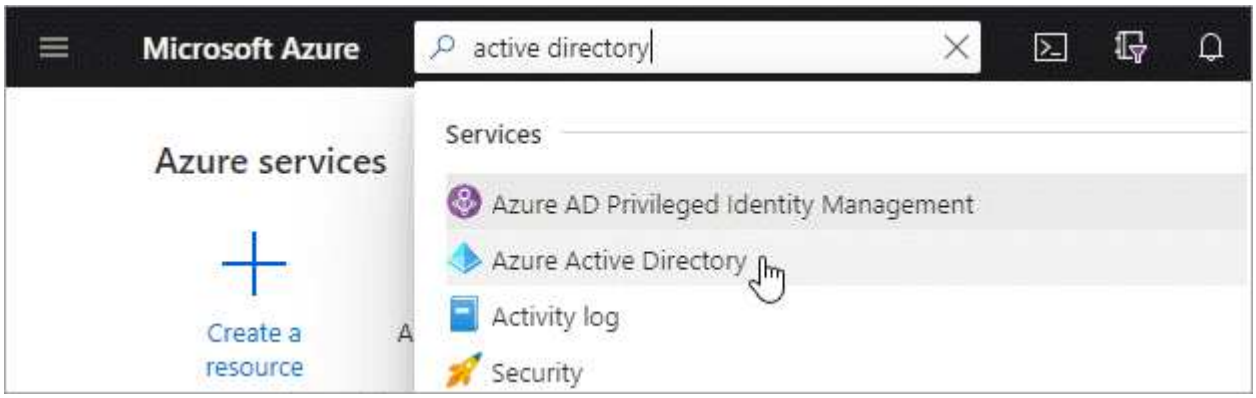
Cloud Manager でコネクタの導入に使用する Azure Active Directory （ AD ）アプリケーションとサービスプ

リンシパルを作成します。

Azure で Active Directory アプリケーションを作成してロールに割り当てるための適切な権限が必要です。詳細については、を参照してください "Microsoft Azure のドキュメント：「 Required permissions"。

手順

1. Azure ポータルで、 * Azure Active Directory * サービスを開きます。



2. メニューで、 * アプリ登録 * をクリックします。
3. [新規登録] をクリックします。
4. 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（ Cloud Manager 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できます。
5. [*Register] をクリックします。

AD アプリケーションとサービスプリンシパルを作成しておきます。

アプリケーションをロールに割り当てます

コネクタを導入する Azure サブスクリプションにサービスプリンシパルをバインドし、カスタムの「 Azure SetupAsService 」ロールを割り当てる必要があります。

手順

1. をダウンロードします "Azure の Connector 導入ポリシー"。

   リンクを右クリックし、 [名前を付けてリンクを保存 ...] をクリックしてファイルをダウンロードする。

2. JSON ファイルを変更して、割り当て可能な範囲に Azure サブスクリプション ID を追加します。
   - 例 *

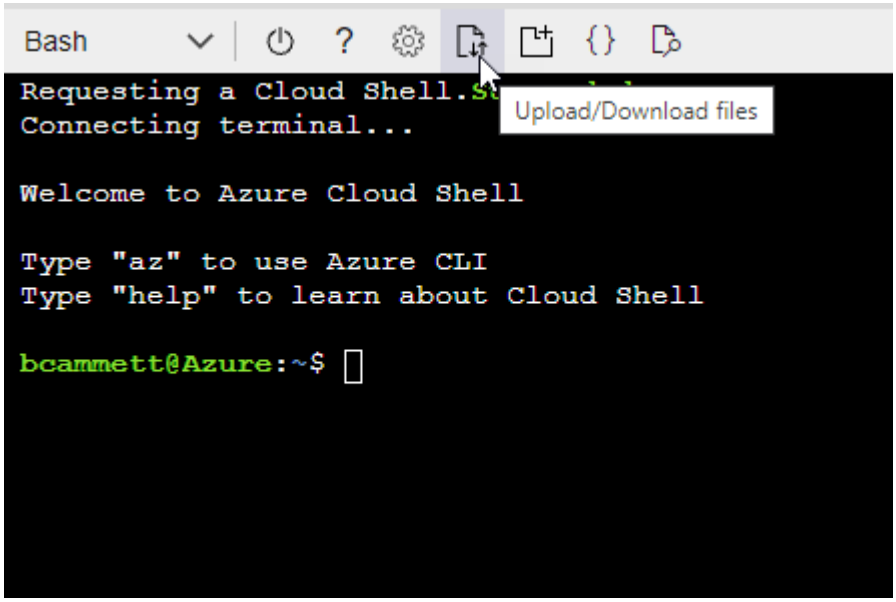
```
"AssignableScopes": [
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

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。

   次の手順は、 Azure Cloud Shell で Bash を使用してロールを作成する方法を示しています。

   a. 開始 "Azure Cloud Shell の略" 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 で次の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。

4. ロールにアプリケーションを割り当てます。

   a. Azure ポータルで、 * Subscriptions * サービスを開きます。

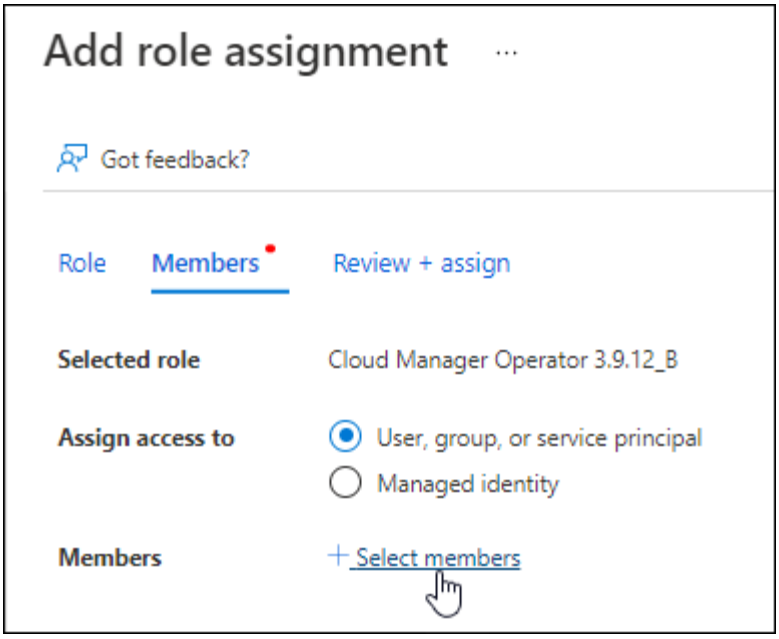
   b. サブスクリプションを選択します。

   c. [* アクセス制御 (IAM)] 、 [追加] 、 [役割の割り当ての追加 *] の順にクリックします。

   d. [* 役割（ * Role ）] タブで、 * Azure SetupAsService * 役割を選択し、 * 次へ * をクリックします。

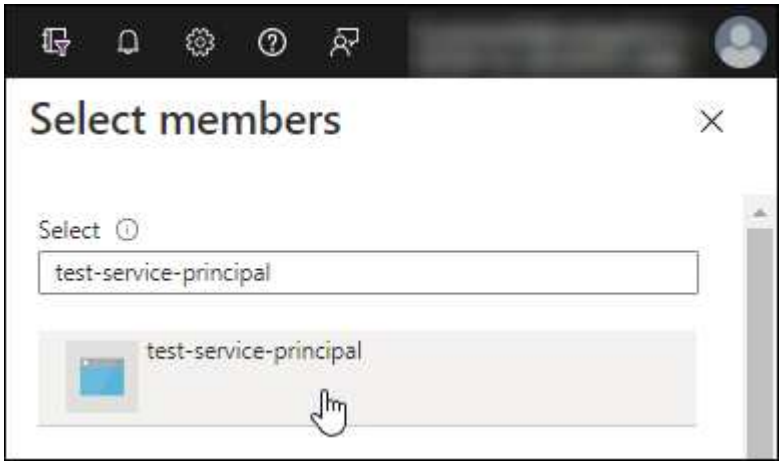
   e. [* Members* （メンバー * ）] タブで、次の手順を実行します。

      - [* 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。
      - [メンバーの選択] をクリックします。



- 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、 * Select * をクリックします。
  - 「 * 次へ * 」をクリックします。

    a. [レビュー + 割り当て（ Review + Assign ）] をクリックします。

    サービスプリンシパルに、 Connector の導入に必要な Azure 権限が付与されるようになりました。

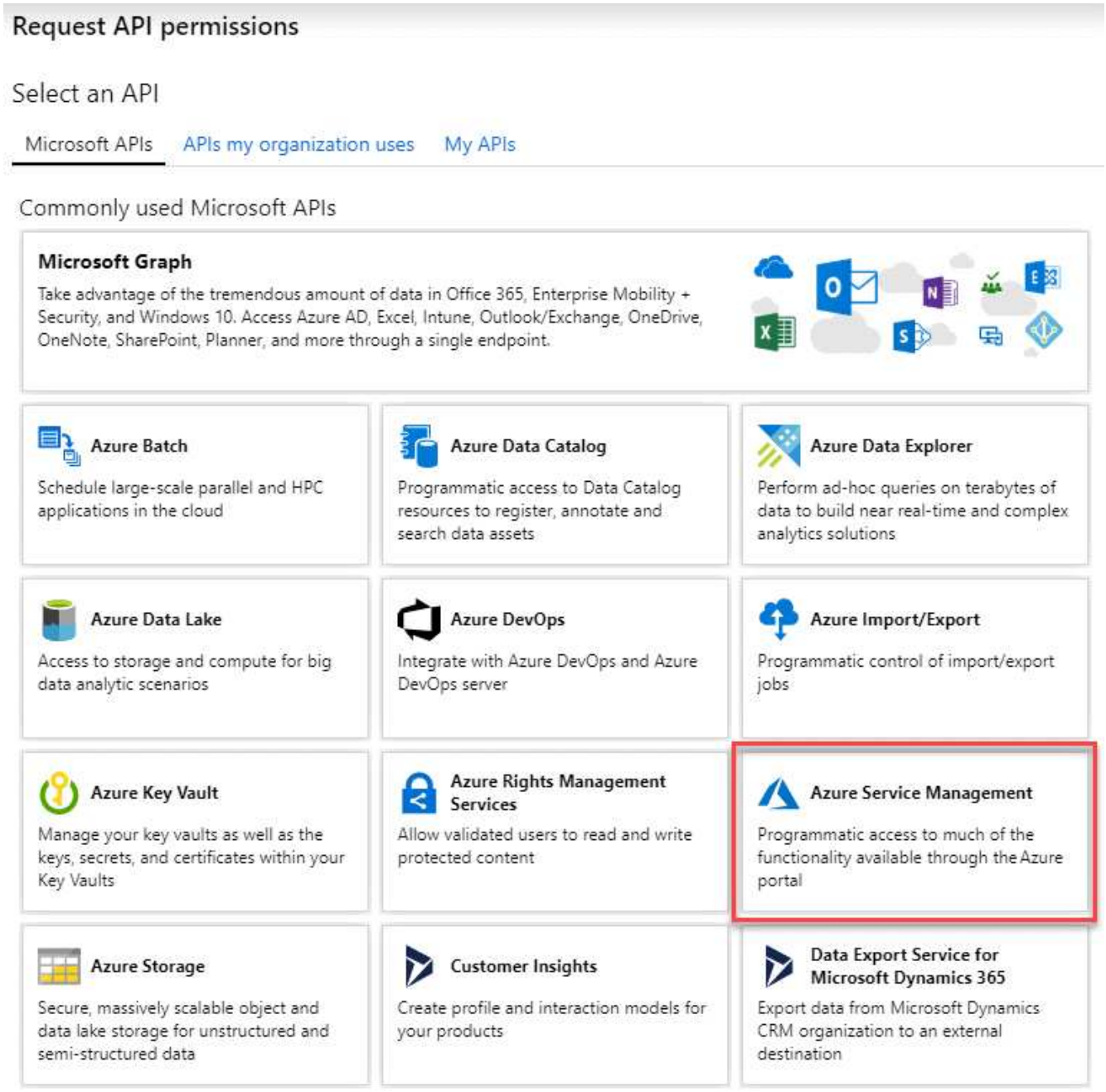
Windows Azure Service Management API 権限を追加します

サービスプリンシパルに「 Windows Azure Service Management API 」の権限が必要です。

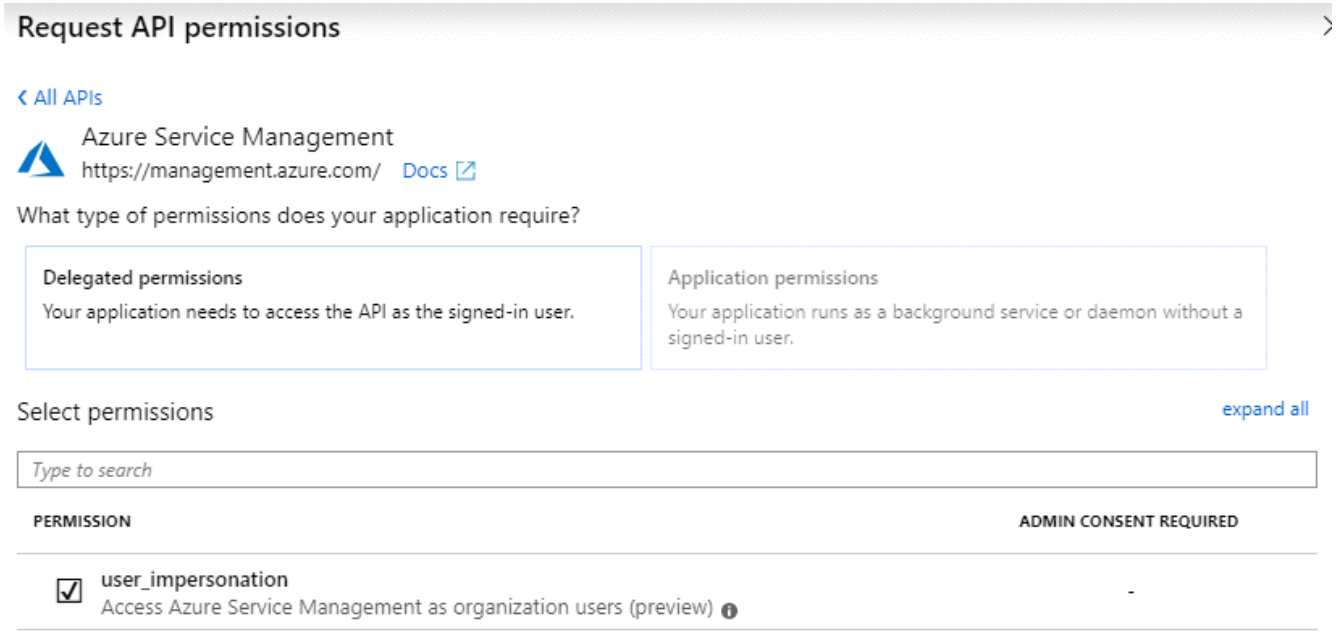
手順

1. Azure Active Directory * サービスで、 * アプリ登録 * をクリックしてアプリケーションを選択します。

2. [API アクセス許可] 、 [アクセス許可の追加] の順にクリックします。
3. Microsoft API* 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 *] をクリックし、 [* 権限の追加 *] をクリックします。

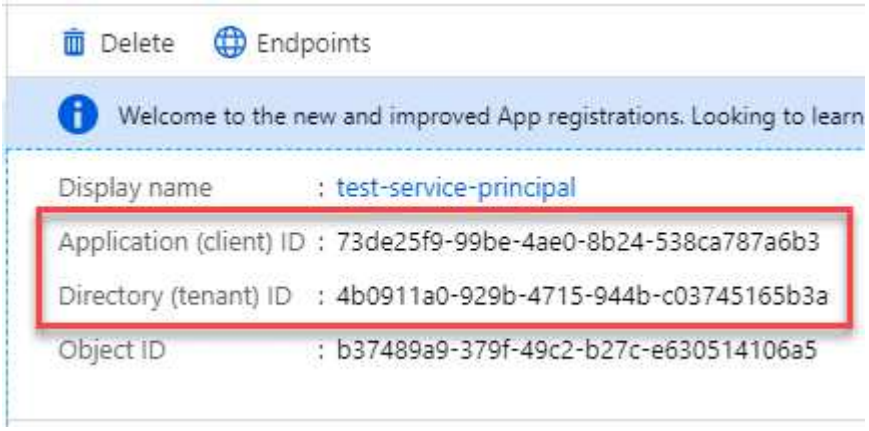


アプリケーション **ID** とディレクトリ **ID** を取得します

Cloud Manager でコネクタを作成するときは、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。Cloud Manager は、この ID を使用してプログラムによってサインインします。

手順

1. Azure Active Directory * サービスで、 * アプリ登録 * をクリックして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。



クライアントシークレットを作成します

Cloud Manager がクライアントシークレットを使用して Azure AD で認証できるようにするには、クライアントシークレットを作成し、そのシークレットの値を Cloud Manager に指定する必要があります。

手順

1. Azure Active Directory * サービスを開きます。

2. [* アプリ登録 *] をクリックして、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 * ］ をクリックします。
4. シークレットと期間の説明を入力します。
5. [追加（ Add ）] をクリックします。
6. クライアントシークレットの値をコピーします。

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をコピーしました。この情報は、コネクタを作成するときに Cloud Manager で入力する必要があります。

サービスプリンシパルでログインしてコネクタを作成します

Cloud Manager では、ユーザインターフェイスから直接 Azure にコネクタを作成できます。

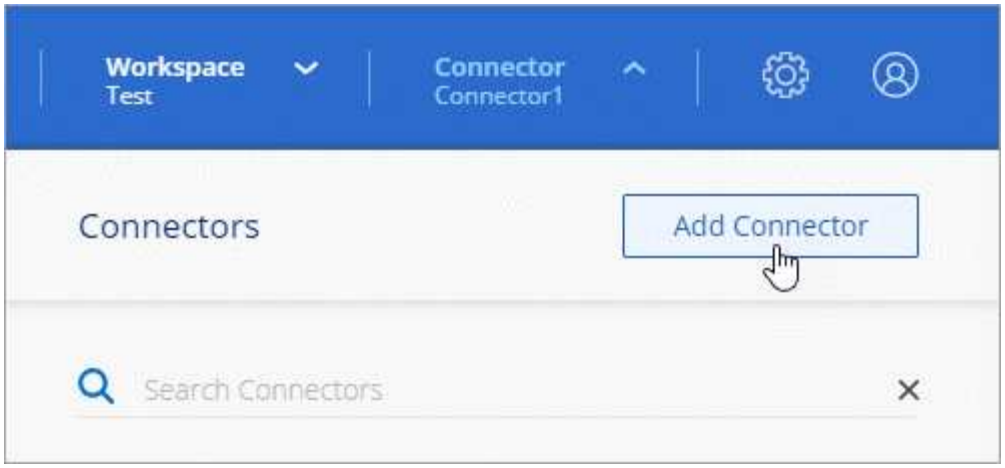
必要なもの

- Azure サブスクリプション。
- 選択した Azure リージョン内の VNet およびサブネット
- Cloud Manager で Connector 用の Azure ロールが自動的に作成されないようにするには、独自のを作成する必要があります "使用するポリシー"。

  これらの権限はコネクタインスタンス自体に適用されます。これは、以前にコネクタを展開するように設定したアクセス権とは異なります。

手順

1. 最初の作業環境を作成する場合は、 * 作業環境の追加 * をクリックし、プロンプトに従います。それ以外の場合は、 [**connector**] ドロップダウンをクリックし、 [**Add connector**] を選択します。



2. クラウドプロバイダとして「 * Microsoft Azure * 」を選択します。

   Connector は、作成する作業環境の種類や有効にするサービスへのネットワーク接続を確立する必要があることに注意してください。

   "Connector のネットワーク要件の詳細については、こちらをご覧ください"。

3. ウィザードの手順に従って、コネクタを作成します。

   - * Get Ready * ： * Azure AD サービスプリンシパル * をクリックし、必要な権限を付与する Azure Active Directory 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 ：を参照してください [Get the application ID and directory ID]。
   - ディレクトリ（テナント） ID ：を参照してください [Get the application ID and directory ID]。
   - クライアントシークレット：を参照してください [Create a client secret]。
   - * VM 認証 * ： 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、認証方法を選択します。
   - * 詳細 * ：インスタンスの名前を入力し、タグを指定し、必要な権限を持つ新しいロールを Cloud Manager で作成するか、で設定した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ているサブスクリプションを選択できます。選択した各サブスクリプションには、 Cloud Volumes ONTAP をこれらのサブスクリプションに導入するための権限が Connector に付与されます。

   - * ネットワーク * ： 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、および必要に応じてプロキシ設定を指定します。
   - * セキュリティグループ * ：新しいセキュリティグループを作成するか、インバウンド HTTP 、 HTTPS 、 SSH アクセス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。

     コネクタへの着信トラフィックは、開始しない限りありません。へのアクセスは、 HTTP および HTTPS を使用して提供されます "ローカル UI"は、まれな状況で使用します。SSH が必要になるのは、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のみです。

   - * 復習 * ：選択内容を確認して、設定が正しいことを確認してください。

4. [追加（ Add ）] をクリックします。

   仮想マシンの準備が完了するまでに約 7 分かかります。処理が完了するまで、ページには表示されたままにしておいてください。

ワークスペース管理者がコネクタを使用して Cloud Volumes ONTAP システムを作成できるように、コネクタをワークスペースに関連付ける必要があります。アカウント管理者のみがいる場合は、コネクタをワークスペースに関連付ける必要はありません。アカウント管理者は、デフォルトで Cloud Manager のすべてのワークスペースにアクセスできます。 "詳細はこちら。"。

Cloud Manager から Google Cloud でコネクタを作成します

Cloud Manager のほとんどの機能を使用するには、 Account Admin が _ Connector を導入する必要があります。 "コネクタが必要になるタイミングを学習します"。Connector を使用すると、 Cloud Manager 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できます。

このページでは、 Cloud Manager から GCP でコネクタを直接作成する方法について説明します。 "コネクタを配置するその他の方法について説明します"。

これらの手順は、 Account Admin ロールを持つユーザが実行する必要があります。ワークスペース管理者はコネクタを作成できません。

最初の Cloud Volumes ONTAP 作業環境を作成する際、まだコネクタがない場合は、 Cloud Manager からコネクタの作成を求められます。

権限を設定しています

Connector を展開する前に、 GCP アカウントに正しい権限があること、および Connector VM のサービスアカウントが設定されていることを確認する必要があります。

手順

1. コネクタを展開する GCP ユーザーが、で権限を持っていることを確認します "GCP の Connector 展開ポリシー"。

   "YAML ファイルを使用してカスタムロールを作成できます" ユーザーに添付します。gcloud コマンドラインを使用して、ロールを作成する必要があります。

2. プロジェクトで Cloud Volumes ONTAP システムを作成および管理するために Cloud Manager に必要な権限を持つサービスアカウントをセットアップします。

   このサービスアカウントは、作成時に Connector VM に関連付けます。

   a. "GCP で役割を作成します" で定義した権限を含むポリシーを作成します "GCP 向け Cloud Manager ポリシー"。ここでも gcloud コマンドラインを使用する必要があります。

      この YAML ファイルに含まれる権限は、手順 1 の権限とは異なります。

   b. "GCP サービスアカウントを作成し、カスタムロールを適用します を作成しました"。

   c. Cloud Volumes ONTAP を他のプロジェクトに導入する場合は、 "クラウドでサービスアカウントを追

加してアクセスを許可します そのプロジェクトに対するマネージャの役割"。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。

これで、 GCP ユーザーはコネクタの作成に必要な権限を持ち、 Connector VM のサービスアカウントが設定されました。

共有 VPC の権限

共有 VPC を使用してリソースをサービスプロジェクトに導入する場合は、次の権限が必要です。IAM の設定が完了したら、この表を参考にして権限の表を環境に反映させる必要があります。

サービスアカウント	作成者	でホストされています	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
Cloud Manager サービスアカウント	カスタム	サービスプロジェクト	• "この .yaml ファイルで見つかった権限"	• compute.networkUser • deploymentmanager. editor	サービスプロジェクトへの Cloud Volumes ONTAP とサービスの導入と保守
Cloud Volumes ONTAP サービスアカウント	カスタム	サービスプロジェクト	• storagec.admin • メンバー： Cloud Manager サービスアカウント。 serviceAccount. user	該当なし	（オプション）データ階層化と Cloud Backup に使用できます
Google API サービスエージェント	GCP	サービスプロジェクト	• （デフォルト） Editor	• compute.networkUser	導入に代わって GCP API とやり取りします。Cloud Manager で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	GCP	サービスプロジェクト	• （デフォルト） Editor	• compute.networkUser	導入に代わって GCP インスタンスとコンピューティングインフラを導入します。Cloud Manager で共有ネットワークを使用できるようにします。

注：

1. deploymentmanager. editor は、ファイアウォールルールを導入環境に渡しておらず、 Cloud Manager に作成を許可することを選択している場合にのみホストプロジェクトで必要です。ルールを指定しない場合、 Cloud Manager はホストプロジェクトに導入を作成し、 VPC0 ファイアウォールルールを適用します。
2. Firewall.create および firewall.delete が必要となるのは、ファイアウォールルールを導入環境に渡しず、 Cloud Manager で作成することを選択している場合だけです。これらの権限は、 Cloud Manager サービスアカウントの .yaml ファイルに格納されています。共有 VPC を使用して HA ペアを導入する場合は、これらの権限を使用して VPC1 、 2 、および 3 のファイアウォールルールが作成されます。他のすべて

の展開では、これらの権限は VPC0 のルールの作成にも使用されます。

3. データ階層化の場合、階層化サービスアカウントは、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して serviceAccount.user ロールを持つ必要があります。現在、プロジェクトレベルで serviceAccount.user を割り当てている場合、 getIAMPolicy でサービスアカウントを照会しても権限は表示されません。

Google Cloud API の有効化

Connector と Cloud Volumes ONTAP を導入するには、いくつかの API が必要です。

ステップ

1. "プロジェクトで次の Google Cloud API を有効にします"。
    - Cloud Deployment Manager V2 API
    - クラウドロギング API
    - Cloud Resource Manager API の略
    - Compute Engine API
    - ID およびアクセス管理（ IAM ） API

GCP でコネクタを作成する

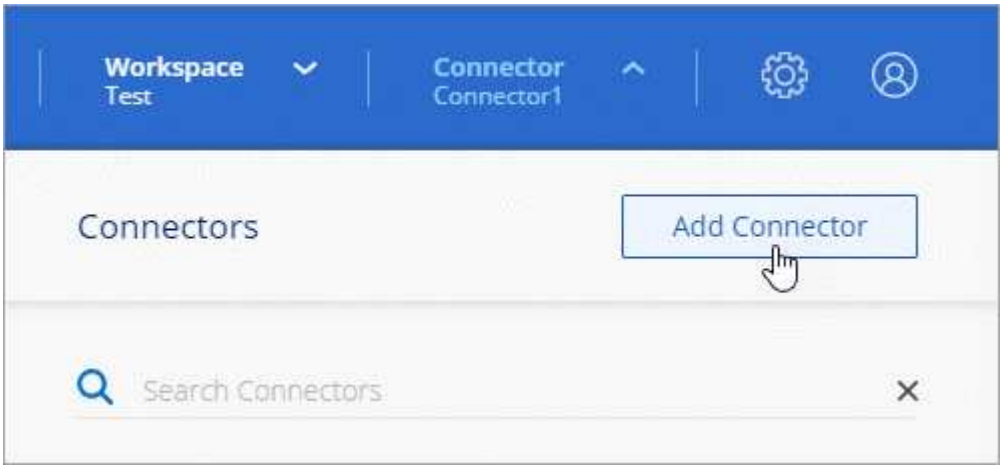
Cloud Manager ユーザインターフェイスから直接、または gcloud を使用して、 Google Cloud でコネクタを作成する。

必要なもの

- 。 "必要な権限" Google Cloud アカウントの場合は、このページの最初のセクションで説明します。
- Google Cloud プロジェクト。
- このページの最初のセクションで説明するように、 Cloud Volumes ONTAP の作成と管理に必要な権限を持つサービスアカウント。
- Google Cloud リージョン内の VPC とサブネット。

クラウドマネージャ

1. 最初の作業環境を作成する場合は、 * 作業環境の追加 * をクリックし、プロンプトに従います。それ以外の場合は、 [**connector**] ドロップダウンをクリックし、 [**Add connector**] を選択します。



2. クラウドプロバイダとして * Google Cloud Platform * を選択します。

   Connector は、作成する作業環境の種類や有効にするサービスへのネットワーク接続を確立する必要があることに注意してください。

   "Connector のネットワーク要件の詳細については、こちらをご覧ください"。

3. ウィザードの手順に従って、コネクタを作成します。
   - * 準備をしてください * ：必要なものを確認してください。
   - プロンプトが表示されたら、 Google アカウントにログインします。このアカウントには、仮想マシンインスタンスを作成するために必要な権限が付与されている必要があります。

     このフォームは Google が所有およびホストしています。クレデンシャルがネットアップに提供されていません。

   - * 基本設定 * ：仮想マシンインスタンスの名前を入力し、タグを指定し、プロジェクトを選択してから、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 、および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、必要に応じてプロキシ設定を指定します。
   - * 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、インバウンド HTTP 、 HTTPS 、 SSH アクセス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。

     コネクタへの着信トラフィックは、開始しない限りありません。へのアクセスは、 HTTP および HTTPS を使用して提供されます "ローカル UI"は、まれな状況で使用します。SSH が必要になるのは、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のみです。

◦ * 復習 * ：選択内容を確認して、設定が正しいことを確認してください。

4. [追加（ Add ）] をクリックします。

   インスタンスの準備が完了するまでに約 7 分かかります。処理が完了するまで、ページには表示されたままにしておいてください。

gcloud

1. ご希望の方法で gcloud 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ますが、 GCP コンソールで Google Cloud Shell を使用できます。

   Google Cloud SDK の詳細については、を参照してください "Google Cloud SDK ドキュメントページ"。

2. 上のセクションで定義した必要な権限を持つユーザ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。ここで、 * user account はログインに使用するユーザアカウントです。

   ```
   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. gcloud compute instances create コマンドを実行します。

```
gcloud compute instances create <instance-name>
  --machine-type=n1-standard-4
  --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 インスタンスに必要なインスタンス名。

プロジェクト
: （オプション） VM を導入するプロジェクト。

service-account のことです
: 手順 2 の出力で指定したサービスアカウント。

ゾーン
: VM を導入するゾーン

no-address
: （オプション）外部 IP アドレスは使用されません（パブリックインターネットにトラフィックを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）タグを使用してファイアウォールルールをコネクタインスタンスにリンクするには、ネットワークタグを追加します

network-path
: （オプション）コネクタを配置するネットワークの名前を追加します（共有 VPC の場合は完全パスが必要です）。

subnet-path 」を指定します
: （オプション）コネクタを導入するサブネットの名前を追加します（共有 VPC の場合は完全パスが必要です）。

kms -key-path
: （オプション） KMS キーを追加してコネクタのディスクを暗号化する（ IAM 権限も適用する必要があります）

これらの旗についてのより多くの情報のために、訪問しなさい "Google Cloud Compute SDK ドキュメン

ト"。

+
コマンドを実行すると、ネットアップのゴールデンイメージを使用してコネクタが導入されます。コネクタインスタンスとソフトウェアは、約 5 分後に実行される必要があります。

1. コネクタインスタンスに接続されているホストから Web ブラウザを開き、次の URL を入力します。

   http://*ipaddress*:80[]

2. ログイン後、コネクタを設定します。
   a. コネクタに関連付けるネットアップアカウントを指定します。

      "ネットアップアカウントについて"。

   b. システムの名前を入力します。

これで、 Connector のインストールとセットアップが完了しました。Cloud Manager は、新しい作業環境の作成時にこのコネクタを自動的に使用します。ただし、コネクタが複数ある場合は、が必要です "スイッチを切り替えます"。

次の手順

Cloud Manager にログインしてセットアップしたので、ユーザは作業環境の作成と検出を開始できます。

- "Cloud Volumes ONTAP for AWS の利用を開始しましょう"
- "Cloud Volumes ONTAP for Azure の利用を開始しましょう"
- "Cloud Volumes ONTAP for Google Cloud の利用を開始しましょう"
- "Azure NetApp Files をセットアップする"
- "ONTAP 用に Amazon FSX をセットアップします"
- "Cloud Volumes Service for AWS をセットアップする"
- "オンプレミスの ONTAP クラスタを検出"
- "Amazon S3 バケットを検出します"

Cloud Manager の管理

ネットアップアカウント

ネットアップアカウントの管理

"初期セットアップを実行したあと"では、後でユーザー、サービスアカウント、ワークスペース、コネクタ、およびサブスクリプションを管理することで、アカウント設定を管理できます。

"ネットアップアカウントの仕組みをご覧ください"。

テナンシー **API** を使用してアカウントを管理します

API 要求を送信してアカウント設定を管理する場合は、 _Tenancy _API を使用する必要があります。この API は、 Cloud Volumes ONTAP の作業環境の作成と管理に使用する Cloud Manager API とは異なります。

"テナンシー API のエンドポイントを表示します"

ユーザの作成と管理

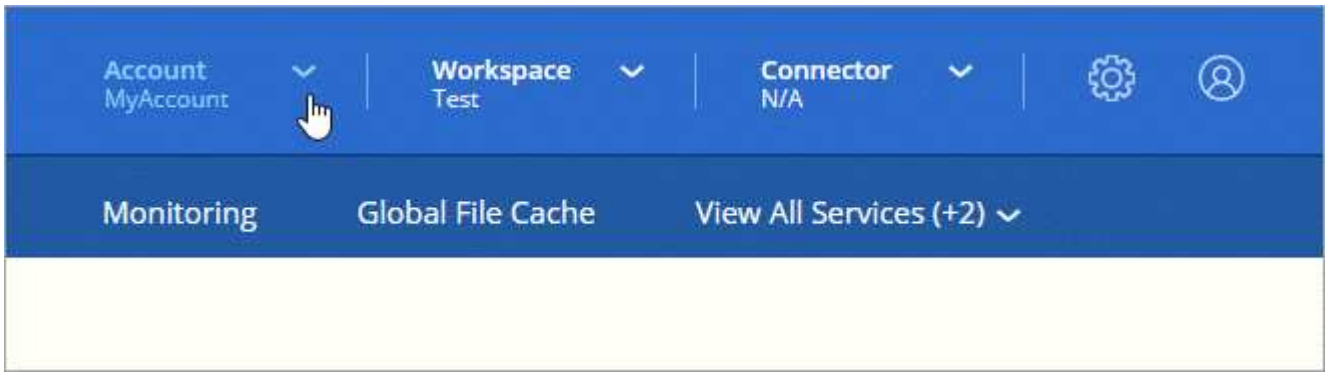
アカウント内のユーザーは、アカウントのワークスペース内のリソースを管理するためにアクセスできます。

ユーザを追加する

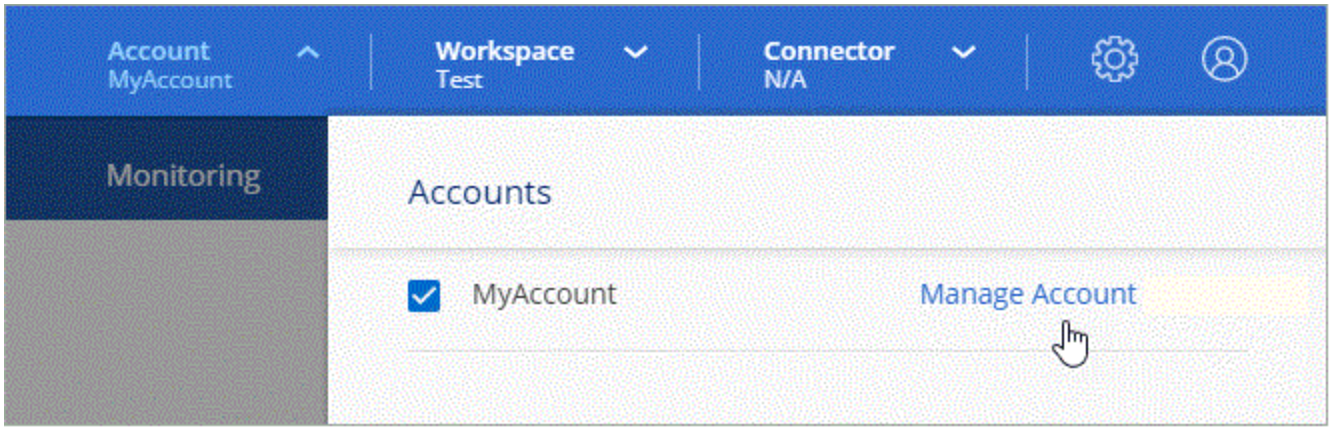
Cloud Central ユーザをネットアップアカウントに関連付けて、これらのユーザが Cloud Manager で作業環境を作成および管理できるようにします。

手順

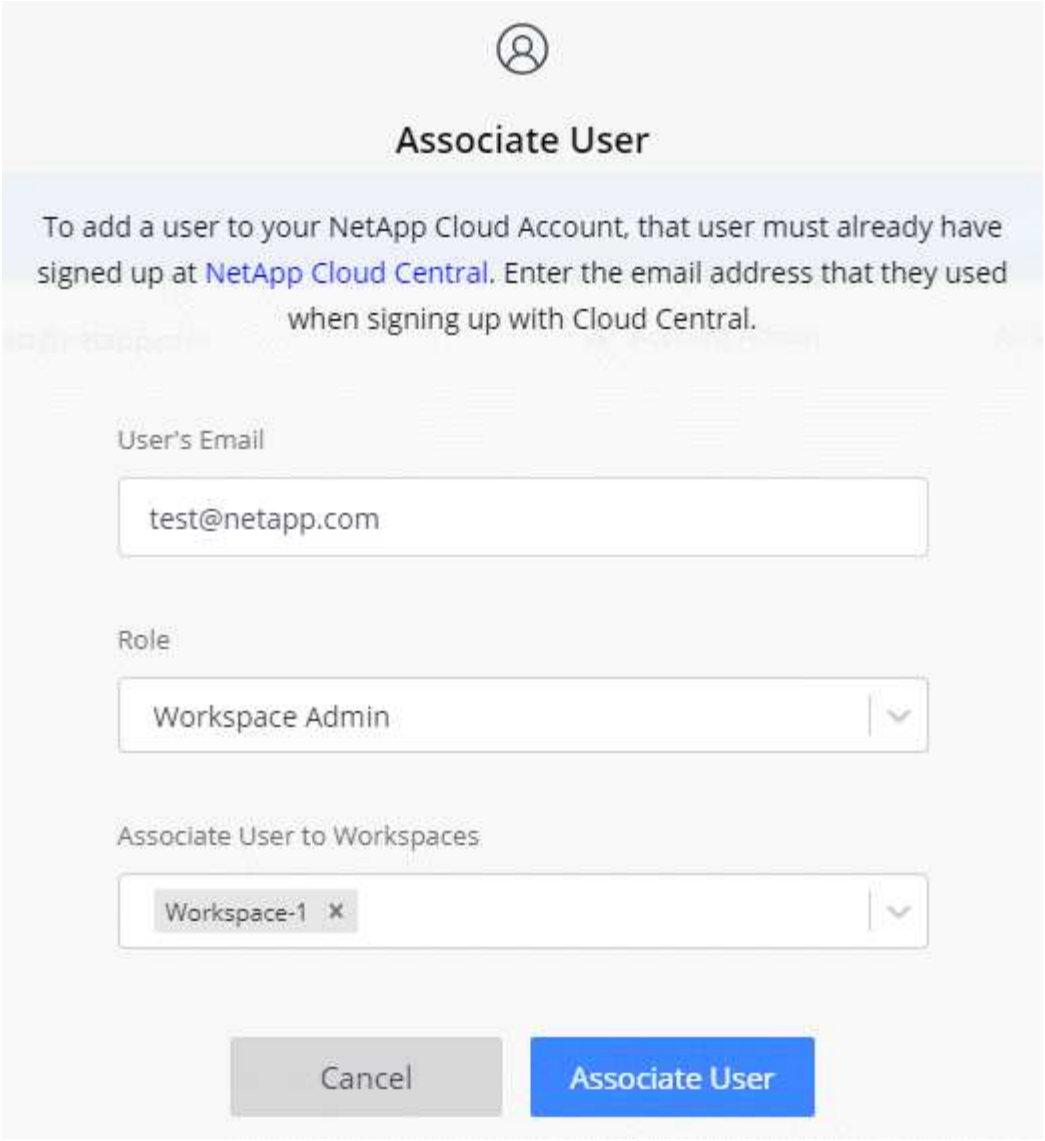
1. ユーザーがまだ行っていない場合は、にアクセスするようにユーザーに依頼します "NetApp Cloud Central" 登録してください。
2. Cloud Manager の上部で、 * Account * ドロップダウンをクリックします。



3. 現在選択されているアカウントの横にある ［ * アカウントの管理 * ］ をクリックします。



4. メンバータブで、 * ユーザーを関連付け * をクリックします。
5. ユーザの E メールアドレスを入力し、ユーザのロールを選択します。
   - * アカウント管理者 * ： Cloud Manager で任意の操作を実行できます。
   - * ワークスペース管理者 * ：割り当てられたワークスペースでリソースを作成および管理できます。
   - * Compliance Viewer * ：クラウドデータセンスのコンプライアンス情報のみを表示し、アクセス権限のあるワークスペースのレポートを生成できます。
   - * SnapCenter Admin* ： SnapCenter サービスを使用して、アプリケーションと整合性のあるバックアップを作成し、それらのバックアップを使用してデータをリストアできます。_ このサービスは現在ベータ版です。 _
6. Workspace Admin または Compliance Viewer を選択した場合は、 1 つ以上のワークスペースを選択してそのユーザーに関連付けます。



7. [関連付け（ Associate ）] をクリックします。

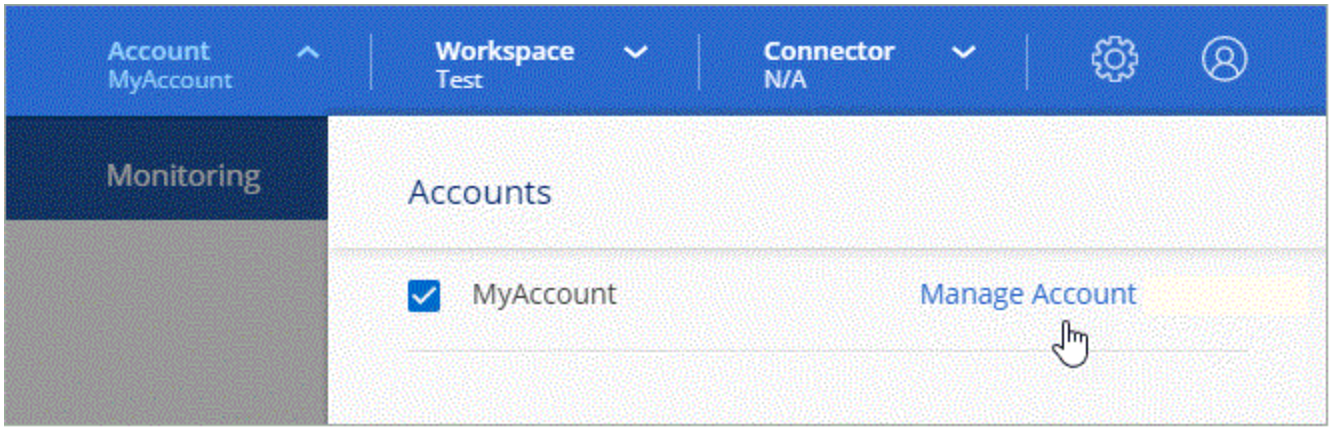
ユーザには、 NetApp Cloud Central の「 Account Association 」というタイトルの E メールが送信されます。 E メールには、 Cloud Manager にアクセスするために必要な情報が記載されています。

ユーザの削除

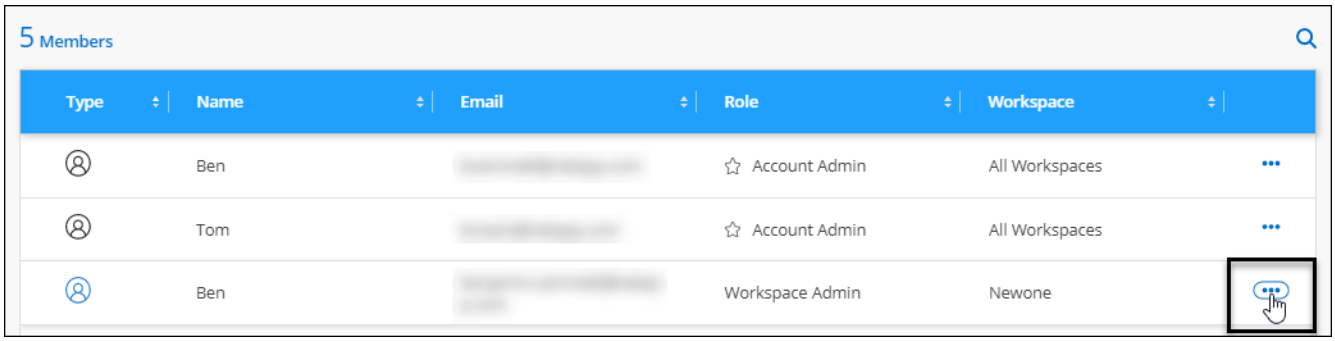
ユーザが割り当てを解除すると、ネットアップアカウントのリソースにアクセスできなくなります。

手順

1. Cloud Manager の上部で、 * Account * ドロップダウンをクリックし、 * Manage Account * をクリックします。



2. メンバー (Members) タブで ' ユーザーに対応する行のアクションメニューをクリックします



3. [ユーザーの関連付けを解除（ Disassociate User ）] をクリックし、 [関連付けを解除（ Disassociate ）] をクリックして

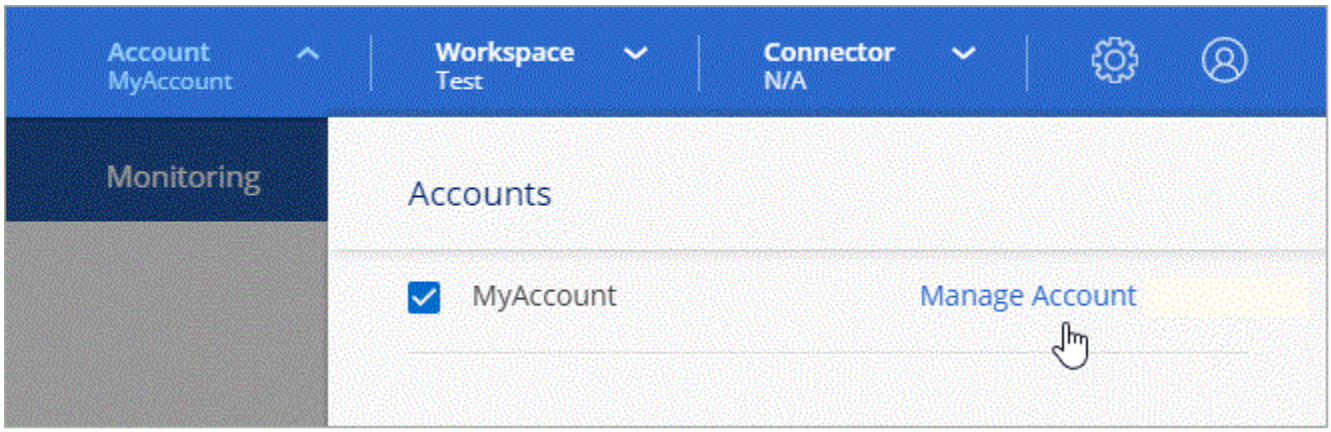
ユーザはこのネットアップアカウントのリソースにアクセスできなくなります。

ワークスペース管理者のワークスペースの管理

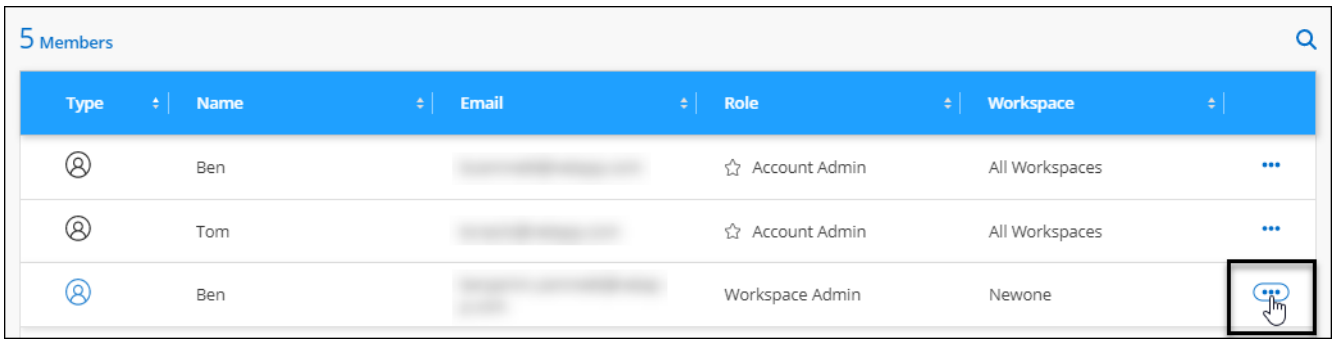
ワークスペース管理者は、いつでもワークスペースに関連付けたり、ワークスペースと関連付けを解除したりできます。ユーザーを関連付けると、ワークスペース内の作業環境を作成して表示できます。

手順

1. Cloud Manager の上部で、 * Account * ドロップダウンをクリックし、 * Manage Account * をクリックします。



2. メンバー (Members) タブで ' ユーザーに対応する行のアクションメニューをクリックします



3. * ワークスペースの管理 * をクリックします。
4. ユーザーに関連付けるワークスペースを選択し、 * 適用 * をクリックします。

コネクタがワークスペースにも関連付けられていれば、ユーザは Cloud Manager からこれらのワークスペースにアクセスできるようになりました。

サービスアカウントの作成と管理

サービスアカウントは「ユーザ」の役割を果たし、 Cloud Manager に対して自動化のための許可された API 呼び出しを実行できます。これにより、自動化スクリプトを作成する必要がなくなります。自動化スクリプトは、会社を離れることができる実際のユーザアカウントに基づいて作成する必要がなくなります。フェデレーションを使用している場合は、クラウドから更新トークンを生成することなくトークンを作成できます。

サービスアカウントには、他の Cloud Manager ユーザと同様にロールを割り当てることで権限を付与します。サービスアカウントを特定のワークスペースに関連付けることで、サービスがアクセスできる作業環境（リソース）を制御することもできます。

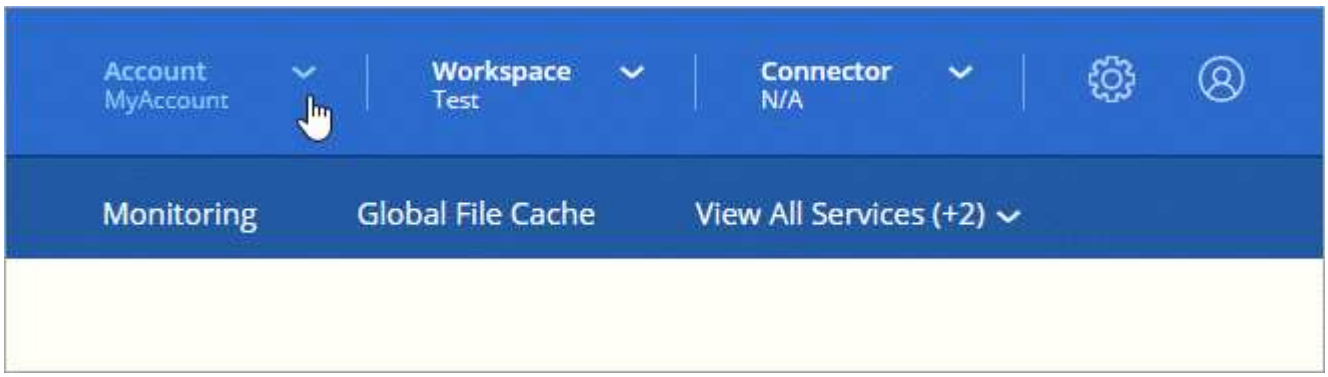
サービスアカウントを作成すると、 Cloud Manager でサービスアカウントのクライアント ID とクライアントシークレットをコピーまたはダウンロードできます。このキーペアは、 Cloud Manager との認証に使用されます。

サービスアカウントの作成

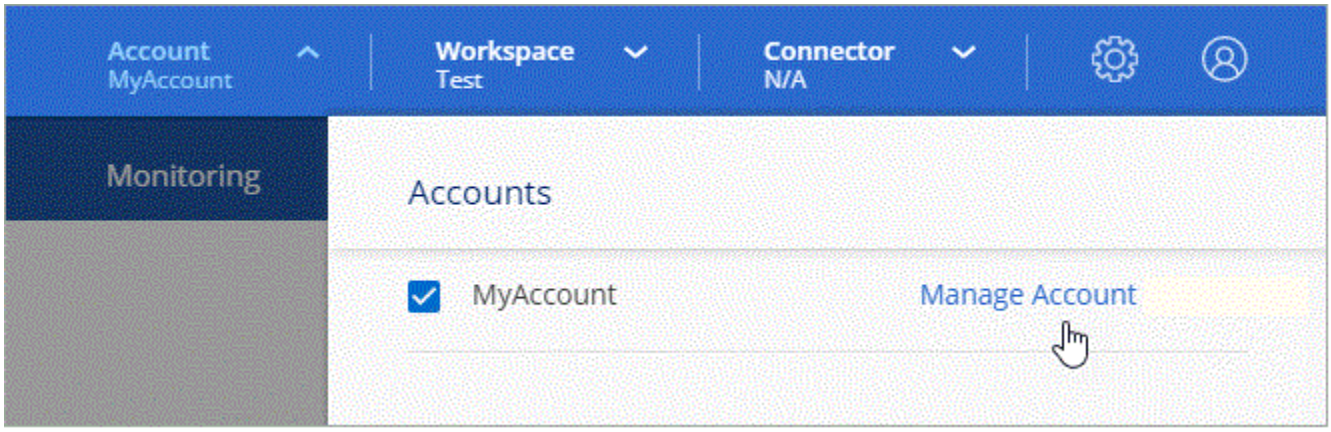
作業環境でリソースを管理するために必要な数のサービスアカウントを作成します。

手順

1. Cloud Manager の上部で、 * Account * ドロップダウンをクリックします。



2. 現在選択されているアカウントの横にある ［ * アカウントの管理 * ］ をクリックします。



3. メンバータブで、 * サービスアカウントの作成 * をクリックします。
4. 名前を入力し、ロールを選択します。Account Admin 以外のロールを選択した場合は、このサービスアカウントに関連付けるワークスペースを選択します。
5. [作成（ Create ）] をクリックします。
6. クライアント ID とクライアントシークレットをコピーまたはダウンロードします。

   クライアントシークレットは 1 回だけ表示され、 Cloud Manager ではどこにも保存されません。シークレットをコピーまたはダウンロードして安全に保管します。

7. [* 閉じる *] をクリックします。

サービスアカウントのベアラトークンを取得する

への API 呼び出しを実行するため "テナンシー API"サービスアカウントのベアラートークンを取得する必要があります。

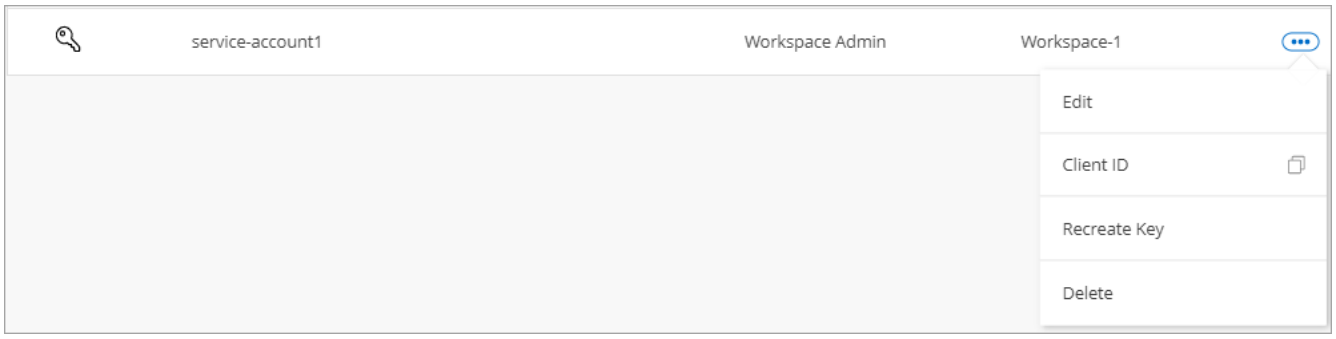
```
curl --location --request POST 'https://netapp-cloud-
account.auth0.com/oauth/token' \
--header 'Content-Type: application/json' \
--data-raw '{
    "grant_type": "client_credentials",
    "client_secret": "<client secret>",
    "audience": "https://api.cloud.netapp.com",
    "client_id": "<client id>"
}'
```

クライアント **ID** をコピーしています

サービスアカウントのクライアント ID はいつでもコピーできます。

手順

1. [メンバー] タブで、サービスアカウントに対応する行のアクションメニューをクリックします。



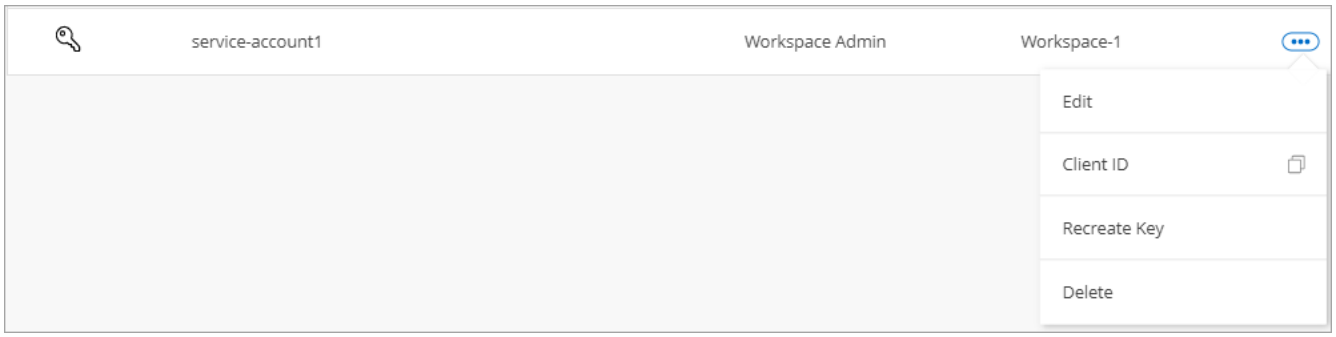
2. [クライアント ID] をクリックします。
3. ID がクリップボードにコピーされます。

キーの再作成中です

キーを再作成すると、このサービスアカウントの既存のキーが削除され、新しいキーが作成されます。前のキーを使用することはできません。

手順

1. [メンバー] タブで、サービスアカウントに対応する行のアクションメニューをクリックします。



2. [キーの再作成 *] をクリックします。
3. 再作成 * をクリックして確定します。
4. クライアント ID とクライアントシークレットをコピーまたはダウンロードします。

   クライアントシークレットは 1 回だけ表示され、 Cloud Manager ではどこにも保存されません。シークレットをコピーまたはダウンロードして安全に保管します。

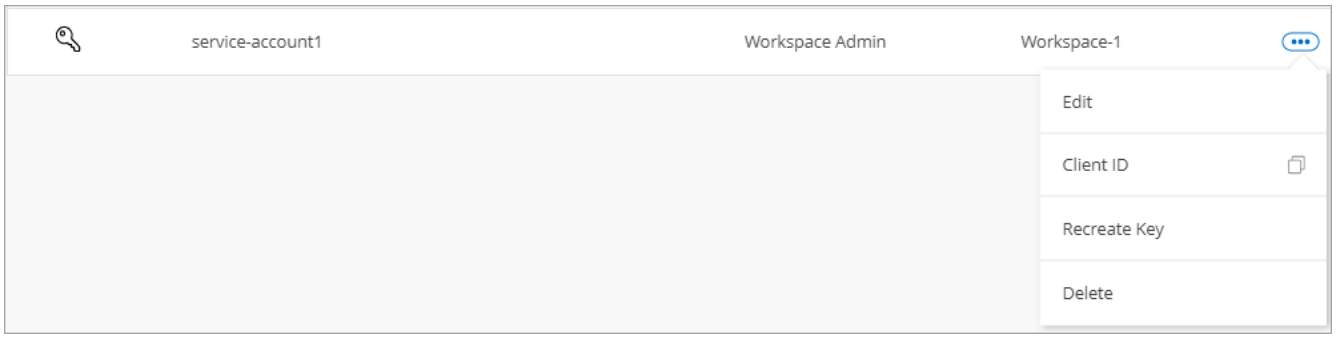
5. [* 閉じる *] をクリックします。

サービスアカウントを削除する

不要になったサービスアカウントを削除します。

手順

1. [メンバー] タブで、サービスアカウントに対応する行のアクションメニューをクリックします。



2. [削除（ Delete ）] をクリックします。
3. 再度 * Delete * をクリックして確定します。

ワークスペースの管理

ワークスペースの作成、名前の変更、および削除により、ワークスペースを管理します。ワークスペースにリソースが含まれている場合、ワークスペースは削除できません。空である必要があります。

手順

1. Cloud Manager の上部で、 * Account * ドロップダウンをクリックし、 * Manage Account * をクリックします。
2. [* ワークスペース *] をクリックします。
3. 次のいずれかのオプションを選択します。
   - 新しいワークスペースを作成するには、 * 新しいワークスペースを追加 * をクリックします。
   - * 名前変更 * をクリックして、ワークスペースの名前を変更します。
   - ワークスペースを削除するには、 * 削除 * をクリックします。

コネクタのワークスペースを管理する

ワークスペース管理者が Cloud Manager からワークスペースにアクセスできるように、コネクタをワークスペースに関連付ける必要があります。

アカウント管理者のみがいる場合は、コネクタをワークスペースに関連付ける必要はありません。アカウント管理者は、デフォルトで Cloud Manager のすべてのワークスペースにアクセスできます。

"ユーザー、ワークスペース、コネクターの詳細をご覧ください"。

手順

1. Cloud Manager の上部で、 * Account * ドロップダウンをクリックし、 * Manage Account * をクリックします。
2. コネクター（ * Connector ）をクリックします。
3. 関連付けるコネクタの * ワークスペースの管理 * をクリックします。
4. コネクタに関連付けるワークスペースを選択し、 * 適用 * をクリックします。

サブスクリプションの管理

クラウドプロバイダのマーケットプレイスからサブスクライブすると、各サブスクリプションはアカウント設定ウィジェットから利用できます。サブスクリプションの名前を変更したり、 1 つまたは複数のアカウントからサブスクリプションの関連付けを解除したりすることができます。

たとえば、 2 つのアカウントがあり、それぞれが別々のサブスクリプションで課金されるとします。いずれかのアカウントとサブスクリプションの関連付けを解除することで、 Cloud Volume ONTAP 作業環境の作成時にそのアカウントのユーザが誤って誤ったサブスクリプションを選択しないようにすることができます。

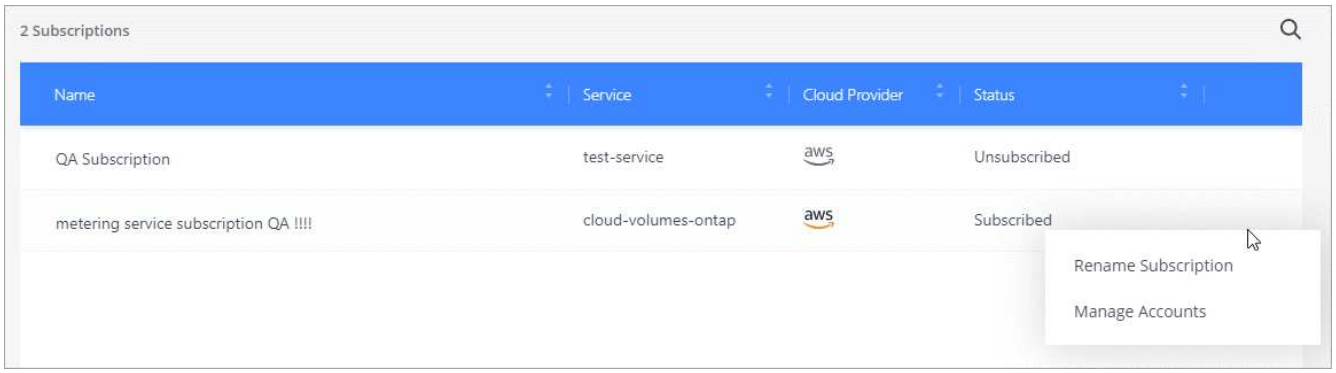
"サブスクリプションの詳細については、こちらをご覧ください"。

手順

1. Cloud Manager の上部で、 * Account * ドロップダウンをクリックし、 * Manage Account * をクリックします。
2. [サブスクリプション] をクリックします。

   現在表示しているアカウントに関連付けられている月額プランのみが表示されます。

3. 管理するサブスクリプションに対応する行のアクションメニューをクリックします。



4. サブスクリプションの名前を変更するか、サブスクリプションに関連付けられているアカウントを管理するかを選択します。

アカウント名を変更する

アカウント名はいつでも変更して、わかりやすい名前に変更してください。

手順

1. Cloud Manager の上部で、 * Account * ドロップダウンをクリックし、 * Manage Account * をクリックします。
2. 「 * 概要 * 」タブで、アカウント名の横にある編集アイコンをクリックします。
3. 新しいアカウント名を入力し、 * 保存 * をクリックします。

プライベートプレビューを許可します

アカウントでプライベートプレビューを有効にすると、 Cloud Manager でプレビュー版として提供される新しい NetApp クラウドサービスにアクセスできるようになります。

プライベートプレビューのサービスは、期待どおりに動作することが保証されておらず、サービスが停止したり、機能しなくなったりする可能性があります。

手順

1. Cloud Manager の上部で、 * Account * ドロップダウンをクリックし、 * Manage Account * をクリックします。
2. [* 概要 *] タブで、 [* プライベートプレビューを許可する *] 設定を有効にします。

サードパーティサービスを許可しています

アカウント内のサードパーティサービスが、 Cloud Manager で使用可能なサードパーティサービスにアクセスできるようにします。サードパーティのサービスはクラウドサービスとネットアップが提供するサービスに似ていますが、サードパーティが管理とサポートを行っています。

手順

1. Cloud Manager の上部で、 * Account * ドロップダウンをクリックし、 * Manage Account * をクリックします。
2. [* 概要 *] タブで、 [* サードパーティサービスを許可する *] 設定を有効にします。

SaaS プラットフォームを無効にする

会社のセキュリティポリシーに準拠するために必要な場合を除き、 SaaS プラットフォームを無効にすることはお勧めしません。SaaS プラットフォームを無効にすると、ネットアップの統合クラウドサービスを使用できなくなります。

SaaS プラットフォームを無効にすると、 Cloud Manager から次のサービスを使用できなくなります。

- クラウドデータの意味
- Kubernetes
- クラウド階層化
- グローバルファイルキャッシュ

SaaS プラットフォームを無効にする場合は、からすべてのタスクを実行する必要があります "コネクタで使用可能なローカルユーザインターフェイス"。

これは元に戻すことができない操作であり、 Cloud Manager SaaS プラットフォームを使用できなくなります。ローカルコネクターからアクションを実行する必要があります。ネットアップの統合クラウドサービスの多くを利用することはできません。また、 SaaS プラットフォームを再度有効にするには、ネットアップのサポートが必要になります。

手順

1. Cloud Manager の上部で、 * Account * ドロップダウンをクリックし、 * Manage Account * をクリックします。
2. ［概要］ タブで、 SaaS プラットフォームの使用を無効にするオプションを切り替えます。

アカウントでの操作の監視

Cloud Manager で実行されている処理のステータスを監視して、対処が必要な問題がな

いかどうかを確認できます。ステータスは、通知センターまたはタイムラインで表示できます。

次の表は、通知センターとタイムラインの比較を示しています。これにより、それぞれの機能を理解することができます。

通知センター	タイムライン
イベントとアクションのステータスの概要が表示されます	各イベントまたはアクションの詳細を表示し、詳細な調査を行います
現在のログインセッションのステータスを表示します。ログオフすると、通知センターに情報が表示されなくなります	過去 1 カ月までステータスを保持します
ユーザインターフェイ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 からのすべての操作が表示されます
ユーザが開始した操作を表示します	ユーザが開始したアクションとシステムが開始したアクションの両方が表示されます
結果を重要度でフィルタリングします	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します

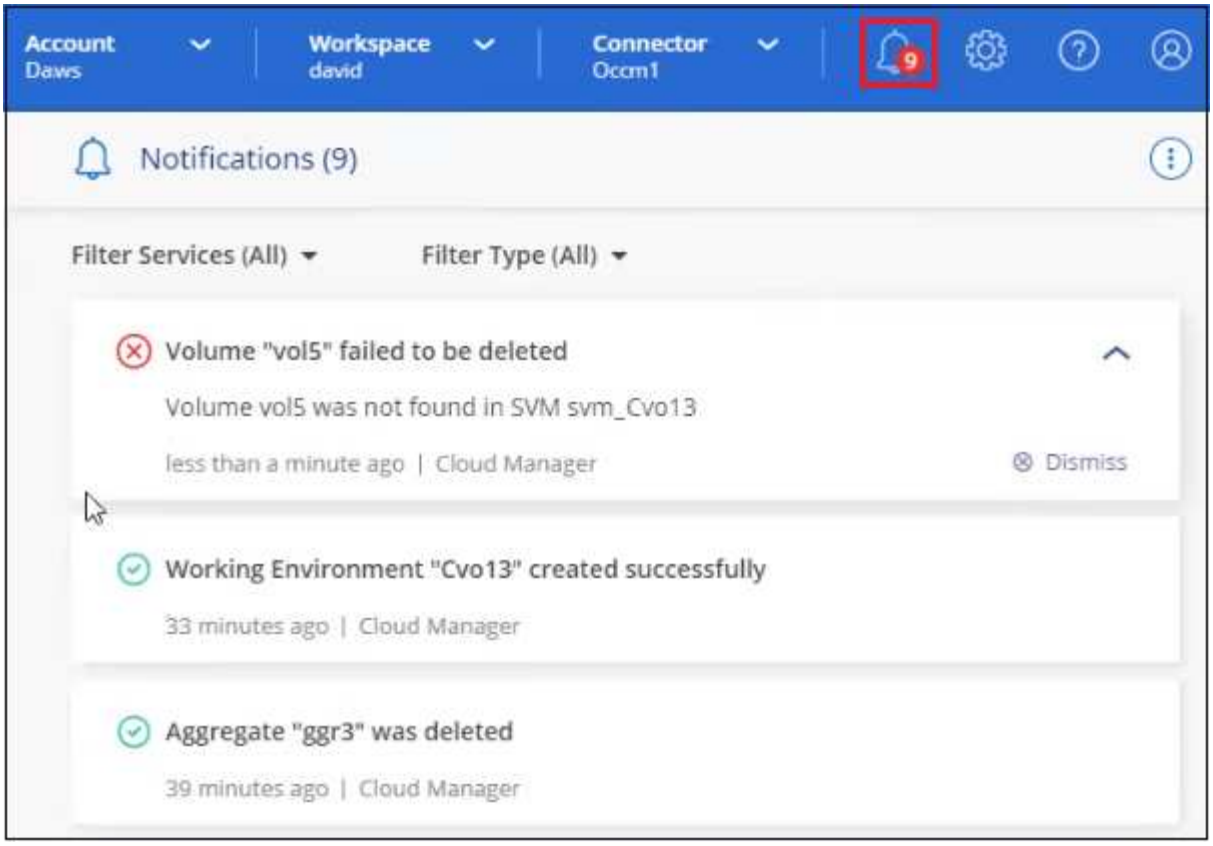
通知センターを使用した動作ステータスの監視

通知は、 Cloud Manager で開始した処理の進捗状況を追跡するイベントのようなもので、処理が成功したかどうか、失敗したかどうかを確認できます。現在のログインセッションで開始した Cloud Manager の処理（および今後のクラウドサービス処理）のステータスを表示できます。

現時点では、次の Cloud Volumes ONTAP オブジェクトの作成および削除に関する通知のみがサポートされています。

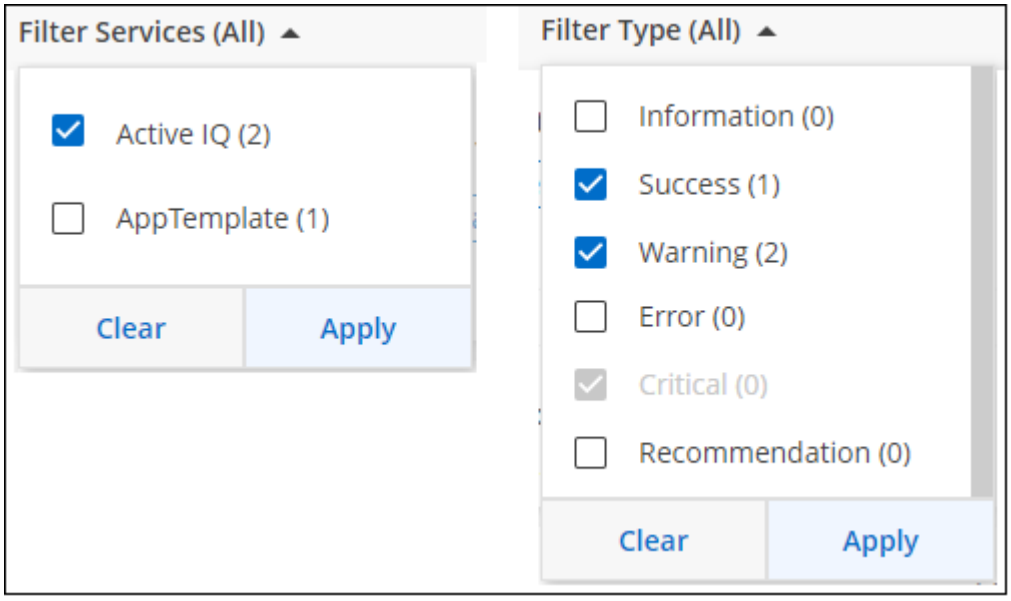
- 作業環境
- アグリゲート
- 個のボリューム

通知を表示するには、通知ベル（  ）をクリックします。ベルの小さなバブルの色は、アクティブな最上位レベルの重大度通知を示します。赤いバブルが表示されている場合は、重要な通知があることを意味します。



通知のフィルタリング

デフォルトでは、すべての通知が表示されます。通知センターに表示される通知をフィルタリングして、重要な通知のみを表示できます。Cloud Manager の「サービス」および通知の「タイプ」でフィルタできます。



たとえば、 Cloud Manager の処理に対する「エラー」通知と「警告」通知のみを表示する場合は、それらのエントリを選択します。表示される通知のタイプはでのみです。

通知が不要になった場合は、ページから削除できます。すべての通知を一度に却下することも、個々の通知を却下することもできます。

すべての通知を却下するには、通知センターでをクリックします ⋮ をクリックして、 [すべてを却下] を選択します。

個々の通知を却下するには、通知の上にカーソルを置き、 * Dismiss * をクリックします。

アカウント内のユーザアクティビティを監査する

Cloud Manager のタイムラインには、アカウントの管理用にユーザが完了した操作が表示されます。これには、ユーザの関連付け、ワークスペースの作成、コネクタの作成などの管理操作が含まれます。

タイムラインのチェックは、特定のアクションを実行したユーザーを特定する必要がある場合や、アクションのステータスを特定する必要がある場合に役立ちます。

手順

1. [* すべてのサービス > タイムライン *] をクリックします。
2. [フィルタ] で、 [サービス *] 、 [テナント *] の順にクリックし、 [適用 *] をクリックします。

タイムラインが更新され、アカウント管理アクションが表示されます。

ロール

アカウント管理者、ワークスペース管理者、コンプライアンスビューア、および SnapCenter 管理者の各ロールは、ユーザーに特定の権限を提供します。

Compliance Viewer ロールは、読み取り専用の Cloud Data Sense アクセス用です。

タスク	アカウント管理者	ワークスペース管理者	**Compliance Viewer**（コンプライアンスビューア）	**SnapCenter** 管理者
作業環境の管理	はい。	はい。	いいえ	いいえ
作業環境でサービスを有効にします	はい。	はい。	いいえ	いいえ

タスク	アカウント管理者	ワークスペース管理者	**Compliance Viewer**（コンプライアンスビューア）	**SnapCenter** 管理者
データ複製ステータスを表示します	はい。	はい。	いいえ	いいえ
タイムラインを表示します	はい。	はい。	いいえ	いいえ
ワークスペースを切り替えます	はい。	はい。	はい。	いいえ
データセンススキャンの結果を表示します	はい。	はい。	はい。	いいえ
作業環境を削除します	はい。	いいえ	いいえ	いいえ
Kubernetes クラスタを作業環境に接続	はい。	いいえ	いいえ	いいえ
Cloud Volumes ONTAP レポートを受信します	はい。	いいえ	いいえ	いいえ
コネクタを作成します	はい。	いいえ	いいえ	いいえ
ネットアップアカウントを管理	はい。	いいえ	いいえ	いいえ
クレデンシャルを管理する	はい。	いいえ	いいえ	いいえ
Cloud Manager の設定を変更	はい。	いいえ	いいえ	いいえ
サポートダッシュボードを表示および管理します	はい。	いいえ	いいえ	いいえ
Cloud Manager から作業環境を削除します	はい。	いいえ	いいえ	いいえ
HTTPS 証明書をインストールします	はい。	いいえ	いいえ	いいえ
SnapCenter サービスを使用します	はい。	はい。	いいえ	はい。

関連リンク

- "ネットアップアカウントでワークスペースとユーザをセットアップ"
- "ネットアップアカウントでのワークスペースとユーザの管理"

コネクタ

高度な導入

AWS Marketplace からコネクタを作成します

Cloud Manager からコネクタを直接作成することを推奨します。 AWS アクセスキーを指定しない場合は、 AWS Marketplace からコネクタを起動できます。Connector の作成とセットアップが完了すると、新しい作業環境を作成するときに、 Cloud Manager によって自動的に Connector が使用されます。

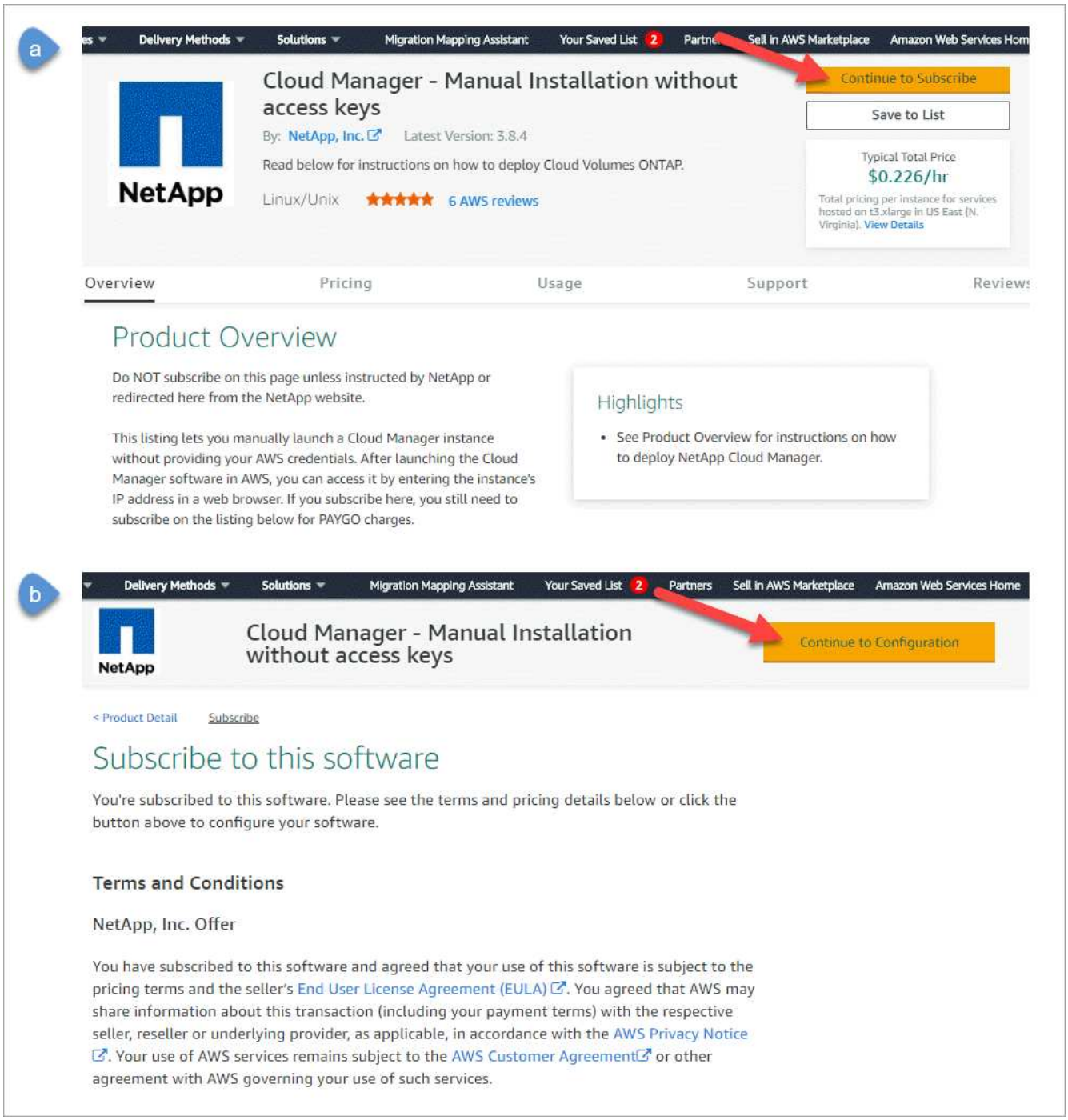
手順

1. EC2 インスタンス用の IAM ポリシーとロールを作成します。
   a. 次のサイトから Cloud Manager IAM ポリシーをダウンロードします。

      "NetApp Cloud Manager ： AWS 、 Azure 、 GCP ポリシー"

   b. IAM コンソールから、 Cloud Manager IAM ポリシーからテキストをコピーアンドペーストして、独自のポリシーを作成します。
   c. ロールタイプが Amazon EC2 の IAM ロールを作成し、前の手順で作成したポリシーをロールに付加します。
2. 次に、に進みます "AWS Marketplace の Cloud Manager のページ" AMI から Cloud Manager を導入

   IAM ユーザがサブスクライブとサブスクライブ解除を行うには、 AWS Marketplace の権限が必要です。
3. [Marketplace] ページで [* Continue to Subscribe*] をクリックし、 [* Continue to Configuration*] をクリックします。



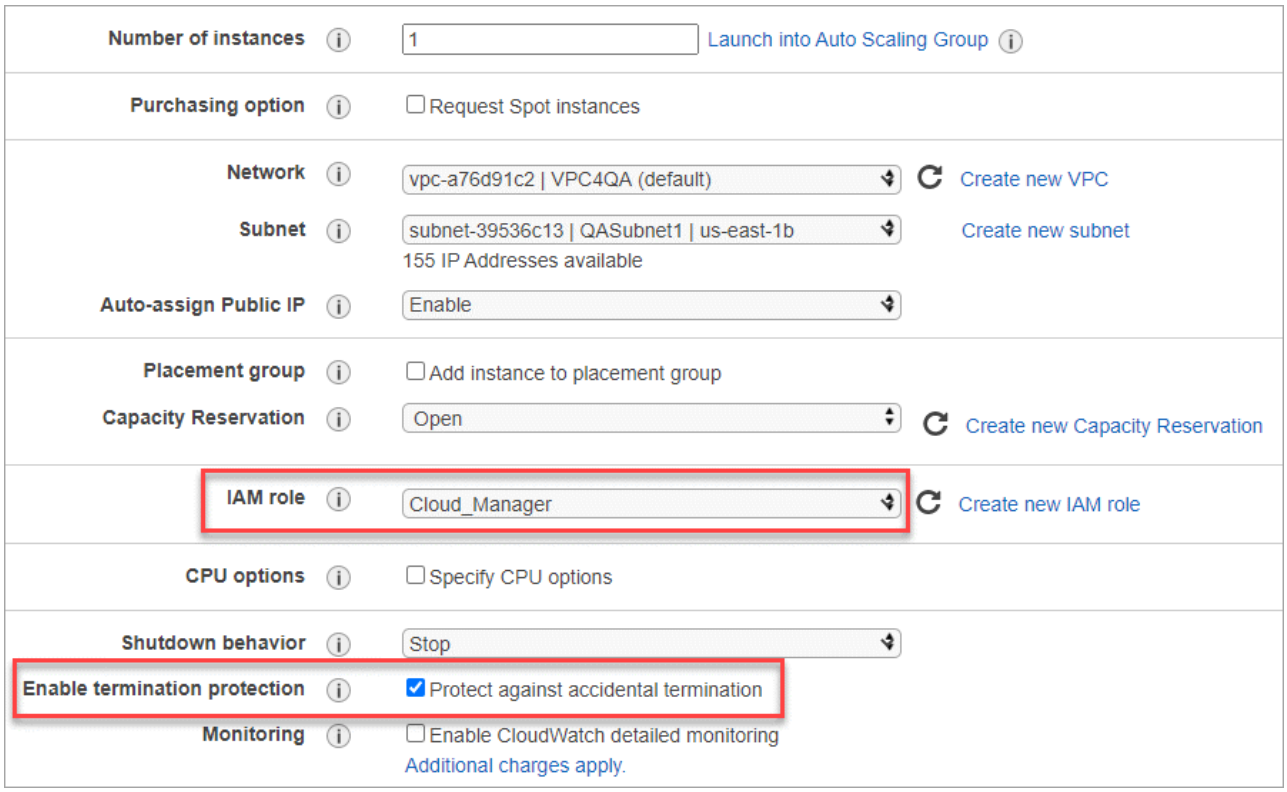
4. デフォルトのオプションを変更し、 [* Continue to Launch] をクリックします。
5. [アクションの選択] で [EC2 で起動] を選択し、 [* 起動 *] をクリックします。

   以下の手順では、 EC2 コンソールからインスタンスを起動する方法について説明します。このコンソールでは、 IAM ロールを Cloud Manager インスタンスに関連付けることができます。これは、 * ウェブサイトからの起動 * アクションを使用しては実行できません。

6. プロンプトに従って、インスタンスを設定および導入します。
   - * 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（ t3.xlarge を推奨）のいずれかを選択します。

     "インスタンスの要件を確認します"。

- * Configure Instance * ： VPC とサブネットを選択し、手順 1 で作成した IAM ロールを選択して、終了保護を有効にし（推奨）、要件を満たす他の設定オプションを選択します。



- * Add Storage* ：デフォルトのストレージ・オプションをそのまま使用します。
- * Add Tags* ：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設定 * ：コネクタインスタンスに必要な接続方法（ SSH 、 HTTP 、 HTTPS ）を指定します。
- * 復習 * ：選択内容を確認して、 * 起動 * をクリックします。

  AWS は、指定した設定でソフトウェアを起動します。コネクタインスタンスとソフトウェアは、約 5 分後に実行される必要があります。

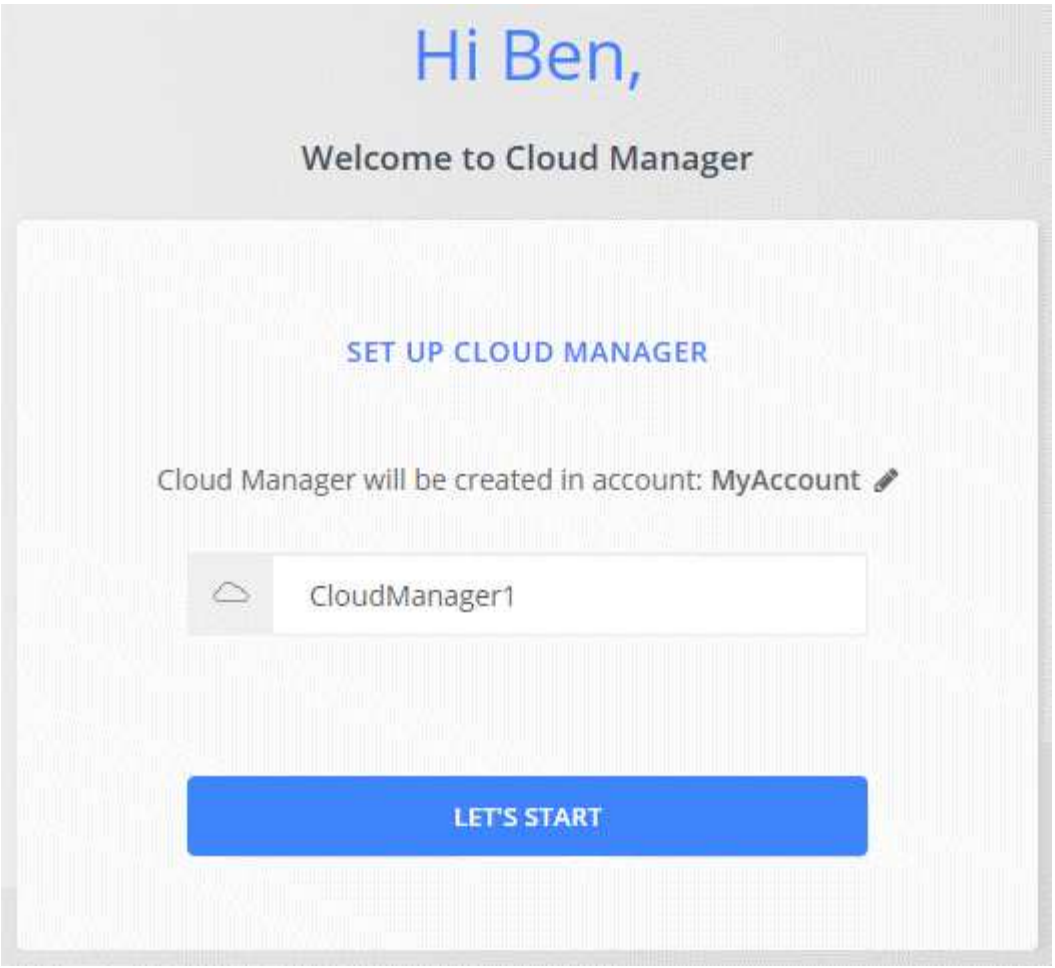
7. コネクタインスタンスに接続されているホストから Web ブラウザを開き、次の URL を入力します。

   http://*ipaddress*:80[]

8. ログイン後、コネクタを設定します。
   a. コネクタに関連付けるネットアップアカウントを指定します。

      "ネットアップアカウントについて"。

   b. システムの名前を入力します。



これで、 Connector のインストールとセットアップが完了しました。Cloud Manager は、新しい作業環境の作成時にこのコネクタを自動的に使用します。ただし、コネクタが複数ある場合は、が必要です "スイッチを切り替えます"。

Azure Marketplace からコネクタを作成します

Cloud Manager からコネクタを直接作成することを推奨しますが、必要に応じて Azure Marketplace からコネクタを起動できます。Connector の作成とセットアップが完了すると、新しい作業環境を作成するときに、 Cloud Manager によって自動的に Connector が使用されます。

Azure でコネクタを作成する

Azure Marketplace のイメージを使用して Azure に Connector を導入し、コネクタにログインしてネットアップアカウントを指定します。

手順

1. "Azure Marketplace の NetApp Connector VM のページに移動します"
2. [* Get it Now* (今すぐ取得)] をクリックし、 [* Continue * (続行)] をクリックします。
3. Azure ポータルで、 * Create * をクリックし、手順に従って仮想マシンを設定します。

   VM を設定する際には、次の点に注意してください。

- Cloud Manager は、 HDD または SSD ディスクのいずれかで最適なパフォーマンスを実現できます。
- CPU と RAM の要件を満たす VM サイズを選択します。DS3 v2 を推奨します。

  "VM の要件を確認します"。

- ネットワークセキュリティグループの場合、コネクタには、 SSH 、 HTTP 、および HTTPS を使用したインバウンド接続が必要です。

  "コネクタのセキュリティグループルールの詳細については、こちらを参照してください"。

- [* 管理（ * Management ）] で、 [* オン * （ * on * ）] を選択して、コネクターに割り当てられた管理 ID * を有効にします。

  管理対象の ID を使用すると、 Connector 仮想マシンはクレデンシャルを指定せずに自身を Azure Active Directory に識別できるため、この設定は重要です。 "Azure リソース用の管理対象 ID の詳細については、こちらをご覧ください"。

4. [* Review + create *（レビュー + 作成）] ページで選択内容を確認し、 [* Create *（作成）] をクリックして展開を開始します。

   指定した設定で仮想マシンが展開されます。仮想マシンと Connector ソフトウェアが起動するまでの所要時間は約 5 分です。

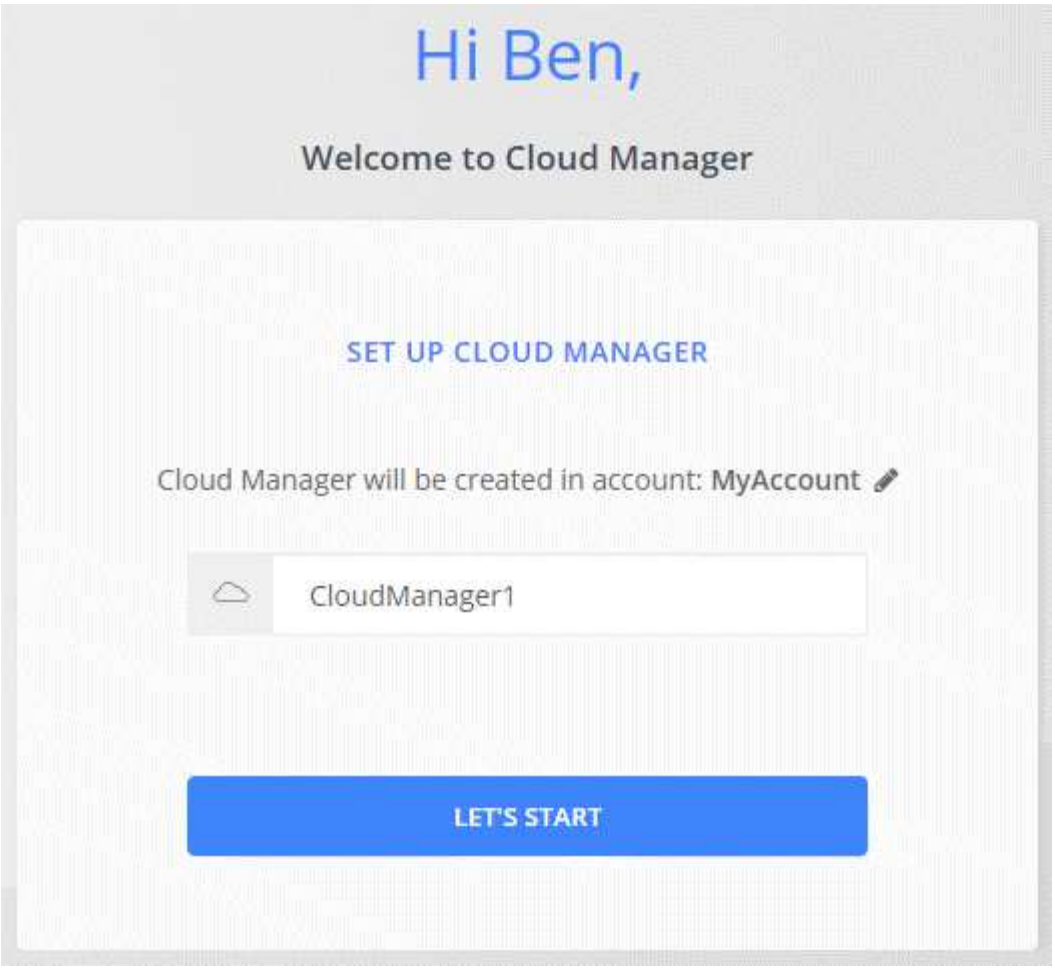
5. Connector 仮想マシンに接続されているホストから Web ブラウザを開き、次の URL を入力します。

   http://*ipaddress*:80[]

6. ログイン後、コネクタを設定します。
   a. コネクタに関連付けるネットアップアカウントを指定します。

      "ネットアップアカウントについて"。

   b. システムの名前を入力します。



これでコネクタがインストールされ、セットアップされました。Cloud Volumes ONTAP を Azure に導入するには、 Azure の権限を付与する必要があります。

Azure 権限を付与しています

Azure にコネクタを導入したら、を有効にしておく必要があります "システムによって割り当てられた管理 ID"。カスタムロールを作成し、そのロールを Connector 仮想マシンに割り当てて、 1 つ以上のサブスクリプションに必要な Azure 権限を付与する必要があります。

手順

1. Cloud Manager ポリシーを使用してカスタムロールを作成します。

   a. をダウンロードします "Cloud Manager Azure ポリシー"。

   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。

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

      - 例 *

      「譲渡対象」：「 / 契約 / D333AF45-0D07-4154-943D-C25FBZZZZ 」、「 / 契約 / 契約 /54B91999-B3E6-4599-908E-416E0ZZZZ 」、「 / 契約 /E471C-3B42-4AE7-9B59-CE5BBZZZZ 」

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。

次の例は、 Azure CLI 2.0 を使用してカスタムロールを作成する方法を示しています。

「 AZ role definition create — role-definition C ： \Policy_for _cloud_Manager_azure_3.9.8.json

これで、 Connector 仮想マシンに割り当てることができる Cloud Manager Operator というカスタムロールが作成されます。

2. 1 つ以上のサブスクリプションのロールを Connector 仮想マシンに割り当てます。

a. [サブスクリプション] サービスを開き、 Cloud Volumes ONTAP システムを展開するサブスクリプションを選択します。

b. * アクセス制御（ IAM ） * > * 追加 * > * 役割の割り当ての追加 * をクリックします。

c. [* 役割] タブで、 * Cloud Manager Operator * 役割を選択し、 * Next * をクリックします。

Cloud Manager Operator は、で指定されたデフォルトの名前です "Cloud Manager ポリシー"。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。

d. [* Members* （メンバー * ）] タブで、次の手順を実行します。

- * 管理対象 ID * へのアクセス権を割り当てます。
- [* メンバーの選択 *] をクリックし、 Connector 仮想マシンが作成されたサブスクリプションを選択し、 [* 仮想マシン *] を選択してから、 Connector 仮想マシンを選択します。
- [* 選択 *] をクリックします。
- 「 * 次へ * 」をクリックします。

e. [レビュー + 割り当て（ Review + Assign ）] をクリックします。

f. 追加のサブスクリプションから Cloud Volumes ONTAP を導入する場合は、そのサブスクリプションに切り替えてから、これらの手順を繰り返します。

Connector には、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が付与されました。Cloud Manager は、新しい作業環境の作成時にこのコネクタを自動的に使用します。ただし、コネクタが複数ある場合は、が必要です "スイッチを切り替えます"。

インターネットにアクセスできる既存の **Linux** ホストにコネクタをインストールします

コネクタを作成する最も一般的な方法は、 Cloud Manager から直接、またはクラウドプロバイダのマーケットプレイスから直接行う方法です。ただし、ネットワークまたはクラウドにある既存の Linux ホストに Connector ソフトウェアをダウンロードしてインストールすることもできます。以下の手順は、インターネットにアクセスできるホストに固有の手順です。

"コネクタを配置するその他の方法について説明します"。

Google Cloud で Cloud Volumes ONTAP システムを作成する場合は、 Google Cloud でも実行されているコネクタが必要です。AWS 、 Azure 、オンプレミスで実行されているコネクタは使用できません。

コネクタソフトウェアは、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で実行する必要があります。

専用のホストが必要です

他のアプリケーションと共有しているホストでは、このコネクタはサポートされていません。専用のホストである必要があります。

CPU

4 コアまたは 4 個の vCPU

RAM

16 GB

AWS EC2 インスタンスタイプ

上記の CPU と RAM の要件を満たすインスタンスタイプ。コネクタを Cloud Manager から直接導入する場合は、 t3.xlarge を使用してインスタンスタイプを指定することを推奨します。

Azure VM サイズ

上記の CPU と RAM の要件を満たすインスタンスタイプ。Cloud Manager からコネクタを直接導入する場合は、 DS3 v2 を推奨し、この VM サイズを使用します。

GCP マシンタイプ

上記の CPU と RAM の要件を満たすインスタンスタイプ。Cloud Manager からコネクタを直接導入する場合は、 n1-standard-4 を使用することを推奨します。

サポートされているオペレーティングシステム

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9

  Red Hat Enterprise Linux システムは、 Red Hat サブスクリプション管理に登録する必要があります。登録されていない場合、 Connector 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のリポジトリにアクセスできません。

  Connector は、これらのオペレーティングシステムの英語版でサポートされています。

ハイパーバイザー

認定済みのベアメタルハイパーバイザーまたはホスト型ハイパーバイザー CentOS または Red Hat Enterprise Linux を実行しますhttps://access.redhat.com/certified-hypervisors["Red Hat ソリューション：「 Which hypervisors are certified to run Red Hat Enterprise Linux ？」"^]

/opt のディスクスペース

100GiB のスペースが使用可能である必要があります

/var のディスク領域

20GiB のスペースが必要です

アウトバウンドインターネットアクセス

コネクターをインストールし、パブリッククラウド環境内でリソースとプロセスを管理するには、アウトバウンドインターネットアクセスが必要です。エンドポイントのリストについては、を参照してください "コネクタのネットワーク要件"。

コネクタを取り付ける

サポートされている Linux ホストがあることを確認したら、コネクタソフトウェアを取得してインストールできます。

コネクタをインストールするには root 権限が必要です。

このタスクについて

- インストールを実行すると、ネットアップサポートからのリカバリ手順用に AWS コマンドラインツール（ awscli ）がインストールされます。

  AWSCLI のインストールに失敗したというメッセージが表示された場合は、このメッセージを無視しても問題ありません。コネクタは、工具なしで正常に作動する。

- ネットアップサポートサイトで入手できるインストーラは、それよりも古いバージョンの場合があります。インストール後、新しいバージョンが利用可能になると、コネクタは自動的に更新されます。

手順

1. から Cloud Manager ソフトウェアをダウンロードします "ネットアップサポートサイト"をクリックし、Linux ホストにコピーします。

   AWS の EC2 インスタンスに接続してファイルをコピーする方法については、を参照してください "AWS ドキュメント：「 Connecting to Your Linux Instance Using SSH"。

2. スクリプトを実行する権限を割り当てます。

   ```
   chmod +x OnCommandCloudManager-V3.9.16.sh
   ```

3. インストールスクリプトを実行します。

   プロキシサーバを使用している場合は、次のようにコマンドパラメータを入力する必要があります。プロキシに関する情報の入力を求めるプロンプトは表示されません。

   ```
    ./OnCommandCloudManager-V3.9.16.sh [silent] [proxy=ipaddress]
   [proxyport=port] [proxyuser=user_name] [proxypwd=password]
   ```

   silent 情報の入力を求めずにインストールを実行します。

プロキシサーバの背後にホストがある場合は、 _proxy_is が必要です。

proxyport_ は、プロキシサーバのポートです。

proxyUser は、ベーシック認証が必要な場合に、プロキシサーバのユーザ名です。

_proxypwd_は 、指定したユーザー名のパスワードです。

4. silent パラメータを指定しなかった場合は、「 * Y * 」と入力してインストールを続行します。

   Cloud Manager がインストールされました。プロキシサーバを指定した場合、インストールの最後に Cloud Manager Service （ OCCM ）が 2 回再起動します。

5. Web ブラウザを開き、次の URL を入力します。

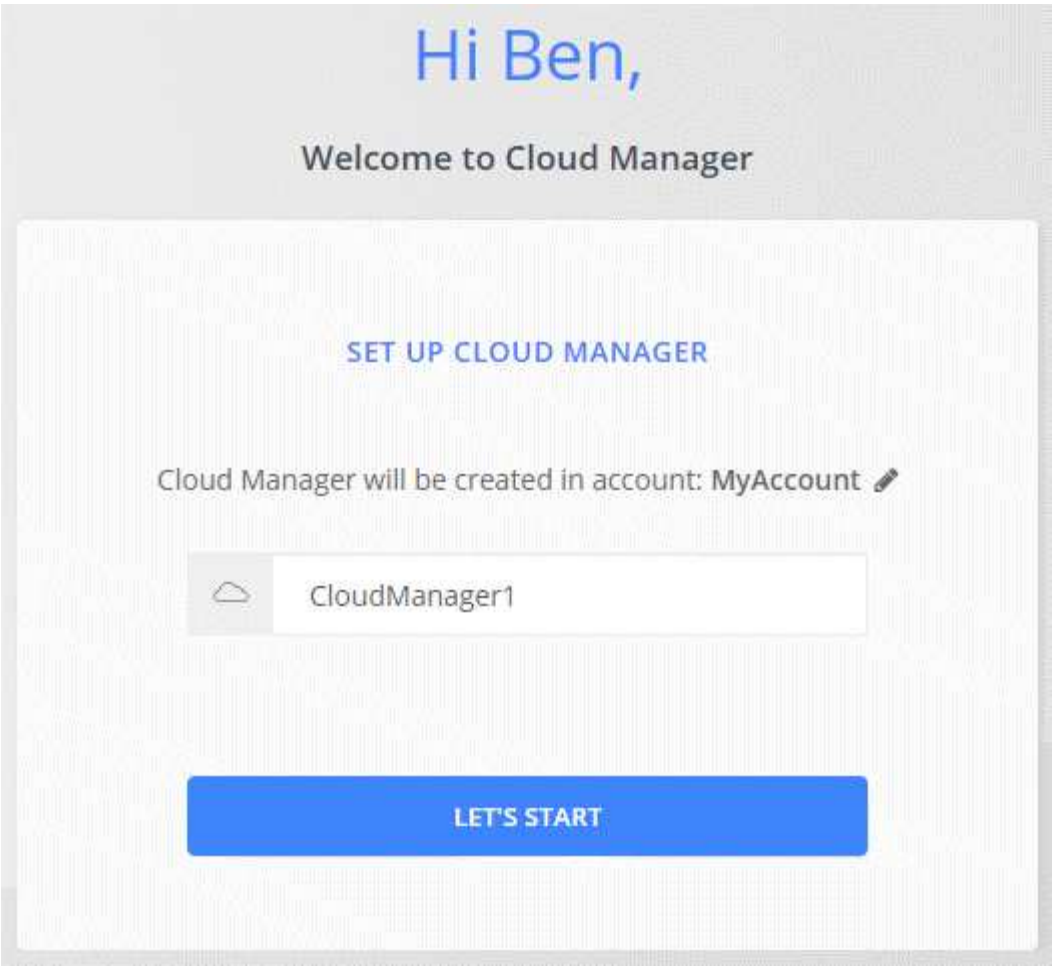
   https://*ipaddress*[]

   _ipaddress _ には、ホストの設定に応じて、 localhost 、プライベート IP アドレス、またはパブリック IP アドレスを指定できます。たとえば、パブリック IP アドレスのないパブリッククラウドにコネクタがある場合は、コネクタホストに接続されているホストからプライベート IP アドレスを入力する必要があります。

6. NetApp Cloud Central に登録するか、ログインします。
7. Connector を Google Cloud にインストールした場合は、 Cloud Manager がプロジェクトで Cloud Volumes ONTAP システムを作成および管理するために必要な権限を持つサービスアカウントをセットアップします。
   a. "GCP で役割を作成します" で定義した権限を含むポリシーを作成します "GCP 向け Cloud Manager ポリシー"。
   b. "GCP サービスアカウントを作成し、カスタムロールを適用します を作成しました"。
   c. "このサービスアカウントを Connector VM に関連付けます"。
   d. Cloud Volumes ONTAP を他のプロジェクトに導入する場合は、 "クラウドでサービスアカウントを追加してアクセスを許可します そのプロジェクトに対するマネージャの役割"。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。
8. ログインしたら、 Cloud Manager をセットアップします。
   a. コネクタに関連付けるネットアップアカウントを指定します。

      "ネットアップアカウントについて"。

   b. システムの名前を入力します。



これで、 Connector のインストールとセットアップが完了しました。Cloud Manager は、新しい作業環境の作成時にこのコネクタを自動的に使用します。

Cloud Manager がパブリッククラウド環境内のリソースやプロセスを管理できるように、権限を設定します。

- AWS "AWS アカウントをセットアップして、に追加します Cloud Manager の略"
- Azure "Azure アカウントをセットアップして、に追加します Cloud Manager の略"
- Google Cloud ：上記の手順 7 を参照してください

インターネットにアクセスせずにオンプレミスにコネクタをインストールします

インターネットにアクセスできないオンプレミスの Linux ホストにコネクタをインストールできます。オンプレミスの ONTAP クラスタを検出し、クラスタ間でデータをレプリケートして、クラウドデータを検出してデータをスキャンできます。

ここで説明するインストール手順は、前述の使用事例を対象としています。 "コネクタを配置するその他の方法について説明します"。

ホストの要件を確認

コネクタソフトウェアは、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で実行する必要があります。

専用のホストが必要です

他のアプリケーションと共有しているホストでは、このコネクタはサポートされていません。専用のホストである必要があります。

CPU

4 コアまたは 4 個の vCPU

RAM

16 GB

サポートされているオペレーティングシステム

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9

Red Hat Enterprise Linux システムは、 Red Hat サブスクリプション管理に登録する必要があります。登録されていない場合、 Connector 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のリポジトリにアクセスできません。

Connector は、これらのオペレーティングシステムの英語版でサポートされています。

ハイパーバイザー

認定済みのベアメタルハイパーバイザーまたはホスト型ハイパーバイザー CentOS または Red Hat Enterprise Linux を実行しますhttps://access.redhat.com/certified-hypervisors["Red Hat ソリューション：「 Which hypervisors are certified to run Red Hat Enterprise Linux ？」"^]

ディスクタイプ

SSD が必要です

/opt のディスクスペース

100GiB のスペースが使用可能である必要があります

/var のディスク領域

20GiB のスペースが必要です

Docker Engine の略

Connector をインストールする前に、ホストに Docker Engine バージョン 19 以降が必要です。 "インストール手順を確認します"。

コネクタを取り付ける

サポートされている Linux ホストがあることを確認したら、コネクタソフトウェアを取得してインストールで

きます。

コネクタをインストールするには root 権限が必要です。

手順

1. Docker が有効で実行されていることを確認します。

```
sudo sysctl enable docker && sudo sysctl start docker
```

2. から Cloud Manager ソフトウェアをダウンロードします "ネットアップサポートサイト"。
3. インストーラを Linux ホストにコピーします。
4. スクリプトを実行する権限を割り当てます。

```
chmod +x /path/cloud-manager-connector-offline-v3.9.16
```

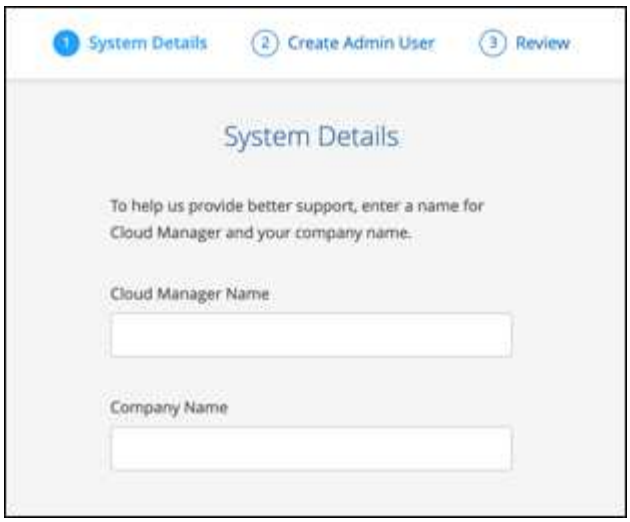
5. インストールスクリプトを実行します。

```
sudo /path/cloud-manager-connector-offline-v3.9.16
```

6. Web ブラウザを開き、と入力します https://*ipaddress*[] ここで、 *ipaddress* は Linux ホストの IP アドレスです。

   次の画面が表示されます。

7. Set Up New Cloud Manager * をクリックし、プロンプトに従ってシステムをセットアップします。
   - * System Details * ： Cloud Manager システムの名前と会社名を入力します。



◦ * 管理者ユーザーの作成 * ：システムの管理者ユーザーを作成します。

このユーザアカウントはシステム上でローカルに実行されます。NetApp Cloud Central への接続はありません。

◦ * 復習 * ：詳細を確認し、ライセンス契約に同意して、 * セットアップ * をクリックします。

8. 作成した管理者ユーザを使用して Cloud Manager にログインします。

これでコネクタがインストールされ、ダークサイト環境で使用できる Cloud Manager の機能の使用を開始できるようになります。

次の内容

- "オンプレミスの ONTAP クラスタを検出"
- "オンプレミスの ONTAP クラスタ間でデータをレプリケート"
- "Cloud Data Sense を使用してボリュームデータをスキャンする"

新しいバージョンの Connector ソフトウェアが利用可能になると、ソフトウェアはネットアップサポートサイトにアップロードされます。 "コネクタをアップグレードする方法について説明します"。

コネクタのシステム ID の確認

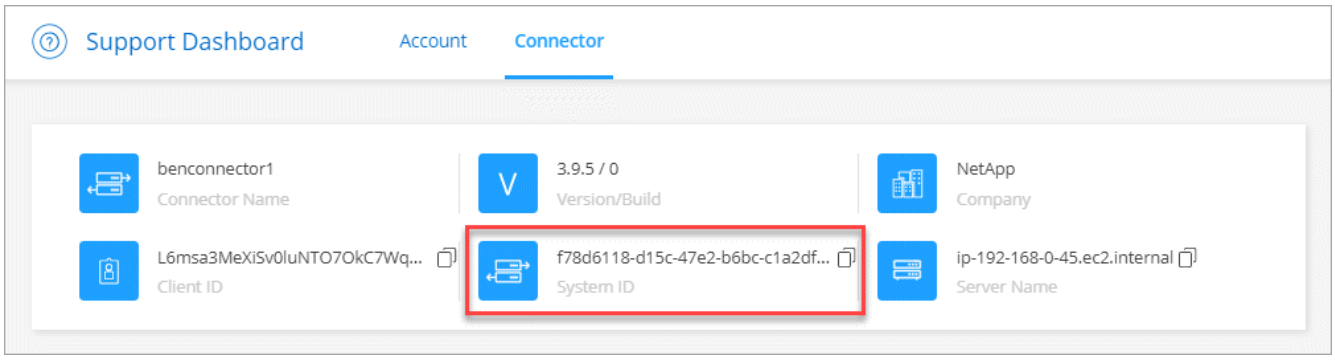
作業を開始する際に、ネットアップの担当者からコネクタのシステム ID を尋ねられることがあります。この ID は通常、ライセンスの取得やトラブルシューティングの目的で使用されます。

手順

1. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックします。
2. [サポート（ Support ）] > [コネクター（ Connector ）] をクリック

システム ID が一番上に表示されます。

◦ 例 *



既存のコネクタの管理

1 つ以上のコネクタを作成した後、コネクタを切り替えたり、コネクタで実行されているローカルユーザーインタフェースに接続したりすることで、コネクタを管理できます。

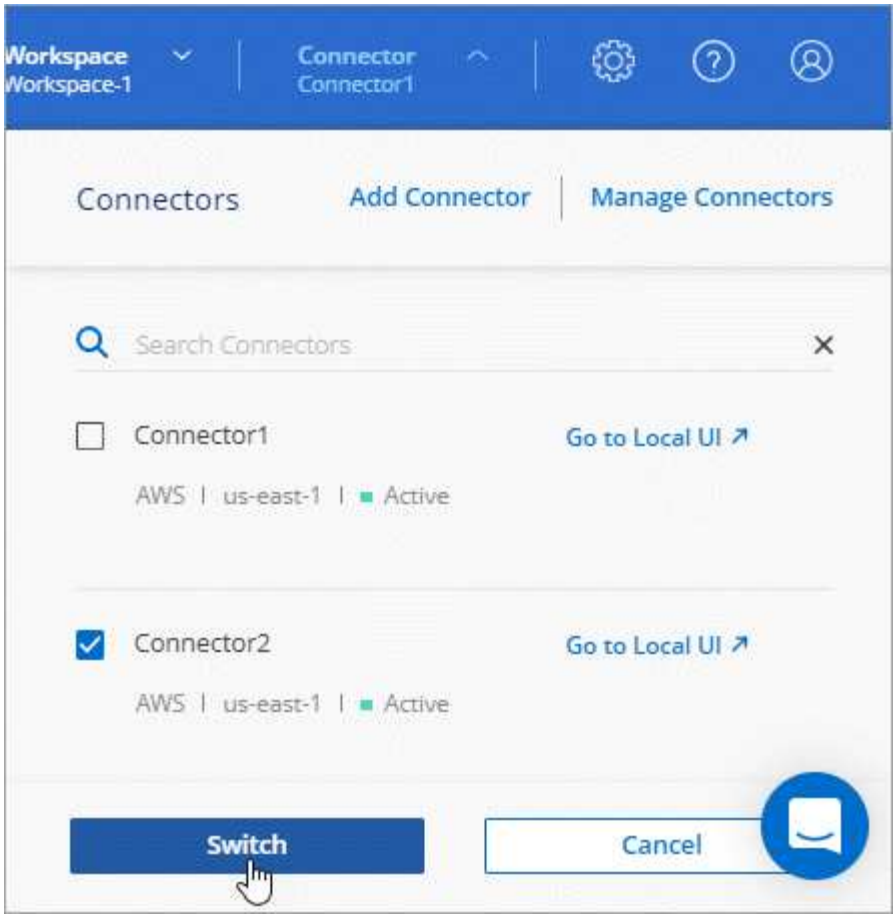
コネクタを切り替えます

複数のコネクタがある場合は、コネクタを切り替えることで特定のコネクタに関連付けられている作業環境を確認できます。

たとえば、マルチクラウド環境で作業しているとします。AWS にコネクタが 1 つ、 Google Cloud にコネクタが 1 つあるとします。これらのクラウドで実行されている Cloud Volumes ONTAP システムを管理するには、これらのコネクタを切り替える必要があります。

ステップ

1. [* コネクタ] ドロップダウンをクリックし、別のコネクタを選択して、 [スイッチ *] をクリックします。



Cloud Manager が更新され、選択したコネクタに関連付けられている作業環境が表示されます。

ローカル **UI** にアクセスします

SaaS ユーザインターフェイスからほとんどのタスクを実行する必要がありますが、ローカルユーザインターフェイスは引き続きコネクタで使用できます。このインターフェイスは、コネクタ自体から実行する必要があるいくつかのタスクに必要です。

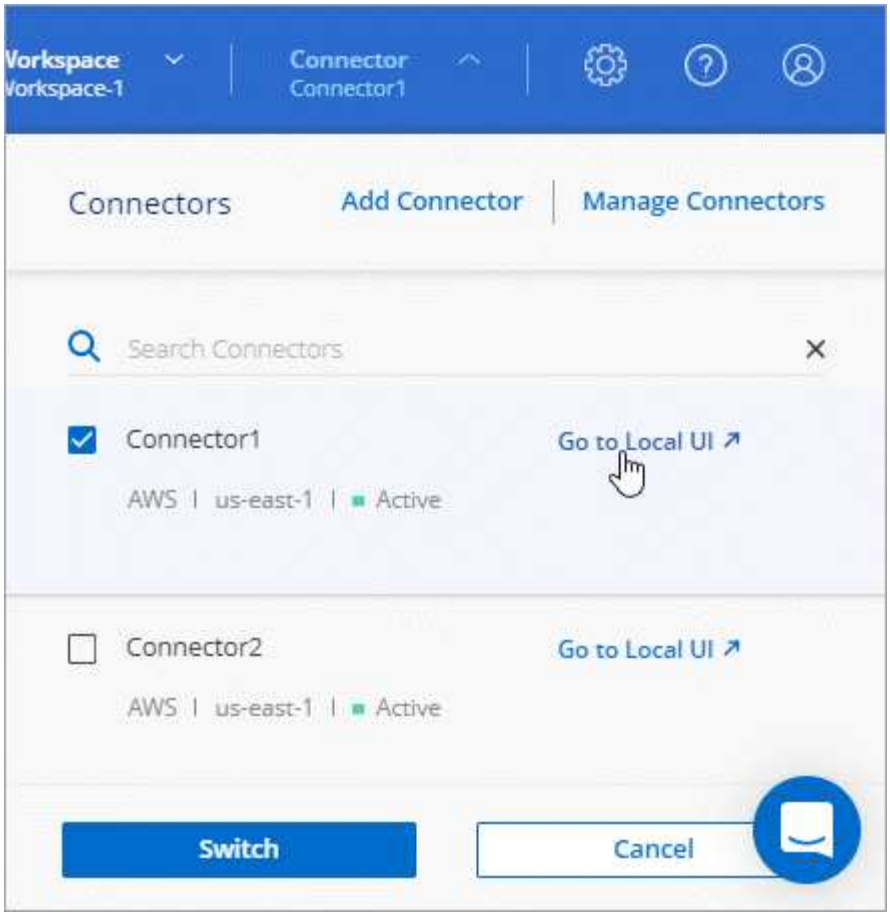
- "プロキシサーバを設定しています"
- パッチをインストールしています （通常はネットアップの担当者と協力してパッチをインストールします）
- AutoSupport メッセージをダウンロードしています （通常は問題が発生したときにネットアップの担当者が指示）

手順

1. "Cloud Manager SaaS インターフェイスにログインします" コネクターインスタンスへのネットワーク接続を持つマシンから。

   コネクタにパブリック IP アドレスがない場合は、 VPN 接続が必要です。そうでない場合は、コネクタと同じネットワークにあるジャンプホストから接続する必要があります。

2. [* Connector* （コネクタ * ）] ドロップダウンをクリックし、 [* ローカル UI へ移動 * （ Go to Local UI * ）] をクリックします。



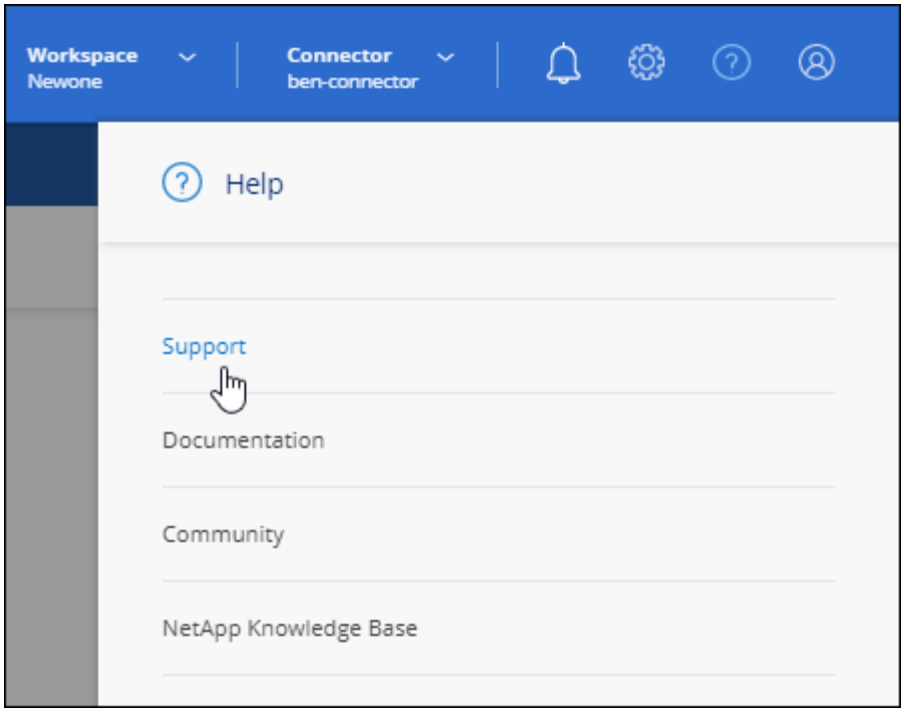
コネクタで実行されている Cloud Manager インターフェイスが新しいブラウザタブに表示されます。

AutoSupport メッセージをダウンロードまたは送信します

問題が発生した場合、ネットアップの担当者から、トラブルシューティングの目的で AutoSupport メッセージをネットアップサポートに送信するように依頼されることがあります。

手順

1. 上のセクションの説明に従って、コネクタローカル UI に接続します。
2. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックし、 * Support * を選択します。

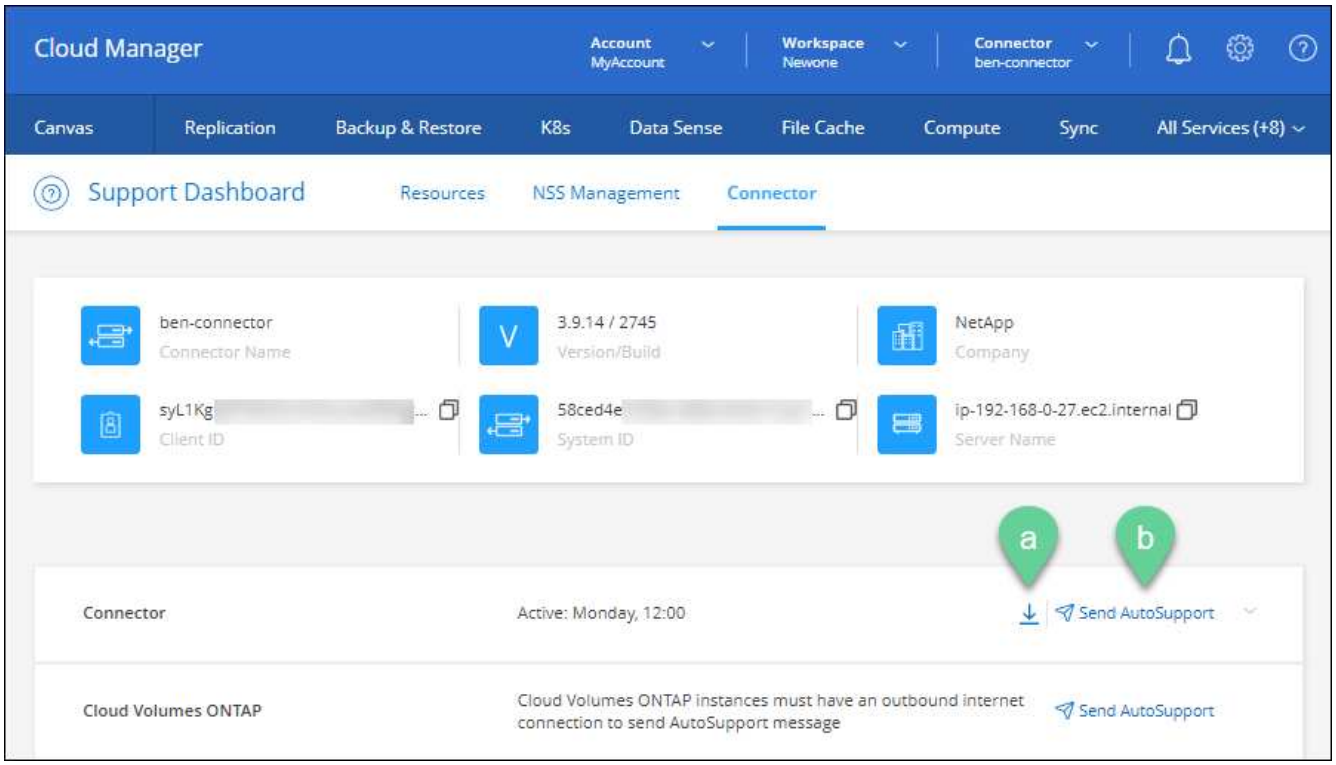


メニューのスクリーンショット。サポートは最初に表示されるオプションです"]

3. コネクター（ * Connector ）をクリックします。
4. ネットアップサポートへの情報の送信方法に応じて、次のいずれかを実行します。

   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。登録したら、任意の方法でネットアップサポートに送信できます。

   b. 「 * Send AutoSupport * 」をクリックして、メッセージをネットアップサポートに直接送信します。



Linux VM に接続します

コネクタが実行されている Linux VM に接続する必要がある場合は、クラウドプロバイダから提供されている接続オプションを使用できます。

AWS

AWS でコネクタインスタンスを作成する際に、 AWS のアクセスキーとシークレットキーを指定しました。このキーペアを使用して、 SSH でインスタンスに接続できます。

"AWS Docs ： Linux インスタンスに接続します"

Azure

Azure で Connector VM を作成する際に、パスワードまたは SSH 公開鍵を使用して認証するように選択します。選択した認証方式を使用して VM に接続します。

"Azure Docs ： SSH を使用して VM を接続します"

Google Cloud

Google Cloud でコネクタを作成するときに認証方法を指定することはできません。ただし、 Google Cloud Console または Google Cloud CLI （ gcloud ）を使用して Linux VM インスタンスに接続することができます。

"Google Cloud Docs ： Linux VM に接続します"

セキュリティ更新プログラムを適用する

コネクタのオペレーティングシステムをアップデートして、最新のセキュリティアップデートでパッチが適用されていることを確認します。

手順

1. コネクタホストの CLI シェルにアクセスします。
2. 管理者権限で次のコマンドを実行します。

```
sudo -s
service service-manager stop
yum -y update --security
service service-manager start
```

コネクタの URI を編集します

コネクタの URI を追加および削除します。

手順

1. Cloud Manager ヘッダーの * Connector * ドロップダウンをクリックします。
2. [* コネクターの管理 *] をクリックします。

3. コネクターのアクションメニューをクリックし、 * URI を編集 * をクリックする。
4. URI を追加して削除し、 * 適用 * をクリックします。

Google Cloud NAT ゲートウェイを使用しているときのダウンロードエラーを修正します

コネクタは、 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。設定で Google Cloud NAT ゲートウェイを使用している場合、ダウンロードが失敗することがあります。この問題を修正するには、ソフトウェアイメージを分割するパーツの数を制限します。この手順は、 Cloud Manager API を使用して実行する必要があります。

ステップ

1. 次の JSON を本文として /occm/config に PUT 要求を送信します。

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

maxDownloadSessions の値は 1 または 1 より大きい任意の整数です。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 は値の例です。使用する値は、 NAT の設定と同時に使用できるセッションの数によって異なります。

"/occm/config API 呼び出しの詳細を確認してください"。

インターネットにアクセスせずにオンプレミスのコネクタをアップグレードします

あなたの場合 "インターネットにアクセスできないオンプレミスホストにコネクタをインストール"では、ネットアップサポートサイトで新しいバージョンを利用できる場合にコネクタをアップグレードできます。

アップグレードプロセス中にコネクタを再起動する必要があるため、アップグレード中はユーザインターフェイスを使用できなくなります。

手順

1. から Cloud Manager ソフトウェアをダウンロードします "ネットアップサポートサイト"。
2. インストーラを Linux ホストにコピーします。
3. スクリプトを実行する権限を割り当てます。

```
chmod +x /path/cloud-manager-connector-offline-v3.9.14
```

4. インストールスクリプトを実行します。

```
sudo /path/cloud-manager-connector-offline-v3.9.14
```

5. アップグレードが完了したら、 * Help > Support > Connector * を選択してコネクタのバージョンを確認できます。

インターネットにアクセスできるホスト上のソフトウェアアップグレードについてはどうでしょうか。

Connector は、ソフトウェアが最新バージョンである限り、自動的にソフトウェアを更新します "アウトバウンドインターネットアクセス" をクリックしてソフトウェアアップデートを入手します。

Cloud Manager からコネクタを削除します

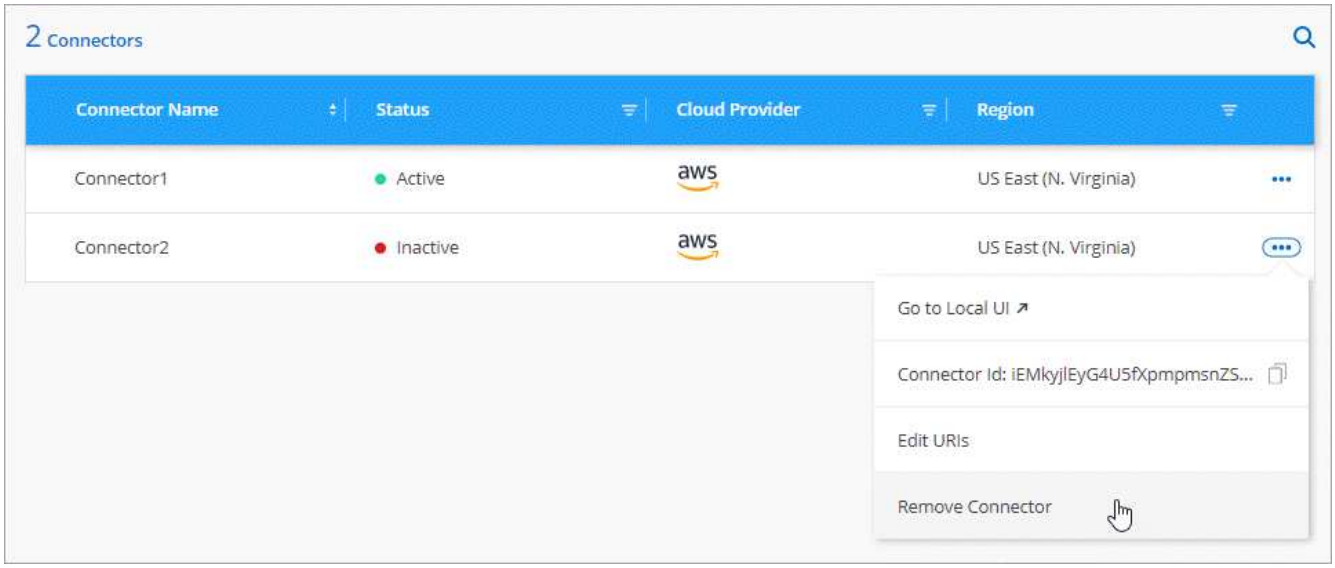
非アクティブなコネクタは、 Cloud Manager のコネクタのリストから削除できます。この処理は、 Connector 仮想マシンを削除した場合や Connector ソフトウェアをアンインストールした場合に実行できます。

コネクタの取り外しについては、次の点に注意してください。

- この操作で仮想マシンが削除されることはありません。
- この操作は元に戻せません — Cloud Manager からコネクタを削除すると、再度 Cloud Manager に追加することはできません。

手順

1. Cloud Manager ヘッダーの * Connector * ドロップダウンをクリックします。
2. [* コネクターの管理 *] をクリックします。
3. 非アクティブなコネクターのアクションメニューをクリックし、 * コネクターを除去 * をクリックする。



4. 確認するコネクタの名前を入力し、 [削除] をクリックします。

Cloud Manager によってレコードからコネクタが削除されます。

Connector ソフトウェアをアンインストールします

問題のトラブルシューティングを行う場合や、ソフトウェアをホストから完全に削除する場合は、コネクタソフトウェアをアンインストールします。使用する必要がある手順は、インターネットにアクセスできるホストにコネクタをインストールしたか、インターネットにアクセスできない制限されたネットワーク内のホストに

インストールしたかによって異なります。

インターネットにアクセスできるホストからをアンインストールします

Online Connector には、ソフトウェアのアンインストールに使用できるアンインストールスクリプトが含まれています。

ステップ

1. 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/cloudmanager/bin/uninstall.sh [サイレント] *

   silent_ 確認を求めずにスクリプトを実行します。

インターネットにアクセスできないホストからをアンインストールします

ネットアップサポートサイトからコネクタソフトウェアをダウンロードし、インターネットにアクセスできない制限されたネットワークにインストールした場合は、ここに示すコマンドを使用します。

ステップ

1. Linux ホストから、次のコマンドを実行します。

```
docker-compose -f /opt/application/netapp/ds/docker-compose.yml down -v
rm -rf /opt/application/netapp/ds
```

セキュアなアクセスのための **HTTPS** 証明書の管理

デフォルトでは、 Cloud Manager は Web コンソールへの HTTPS アクセスに自己署名証明書を使用します。認証局（ 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。

始める前に

Cloud Manager の設定を変更する前に、コネクタを作成する必要があります。 "詳細をご確認ください"。

HTTPS 証明書のインストール

セキュアなアクセスのために、 CA によって署名された証明書をインストールします。

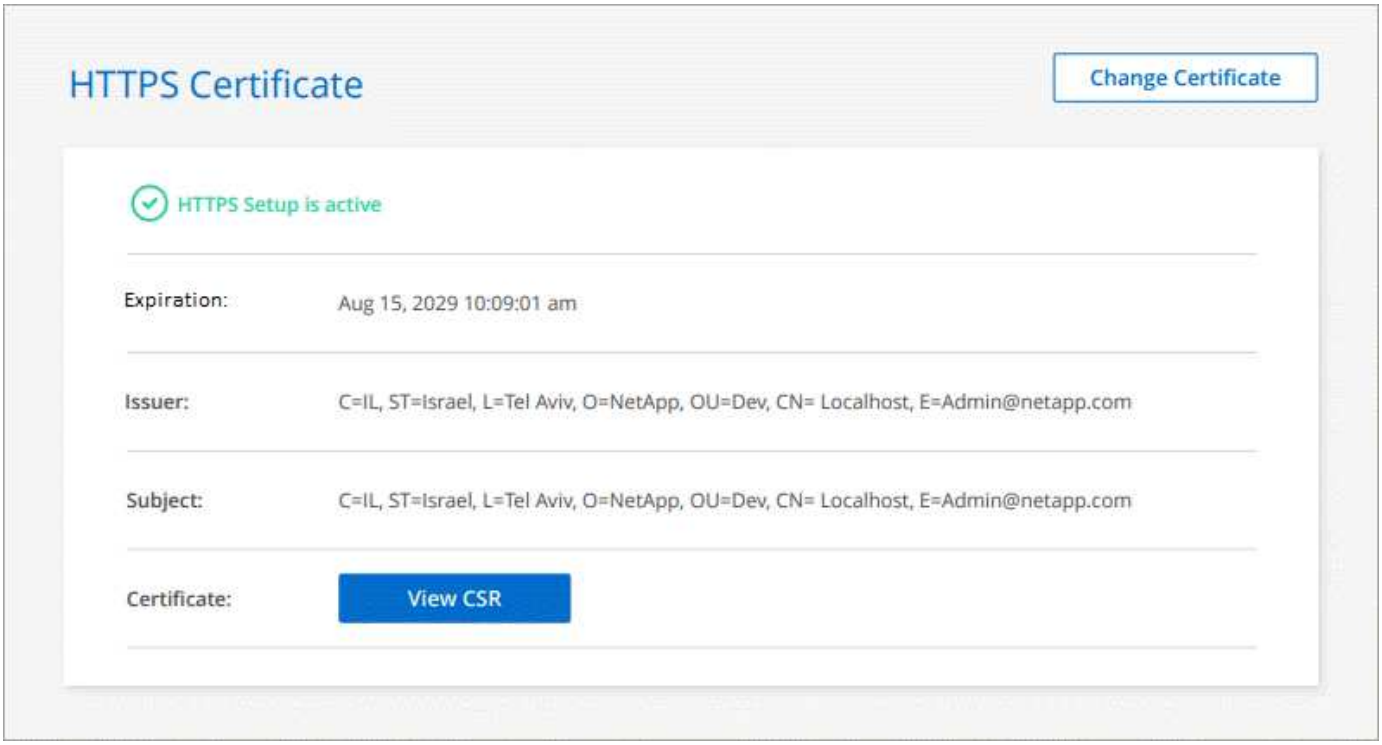
手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * HTTPS セットアップ * を選択します。

2. [HTTPS Setup] ページで、証明書署名要求（ CSR ）を生成するか、独自の CA 署名付き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 を生成します	a. コネクターホストのホスト名または DNS （共通名）を入力し、 * CSR の生成 * をクリックします。 証明書署名要求が表示されます。 b. CSR を使用して、 SSL 証明書要求を CA に送信します。 証明書では、 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。 c. 証明書ファイルをアップロードし、 * Install * をクリックします。
独自の CA 署名付き証明書をインストールします	a. 「 CA 署名証明書のインストール」を選択します。 b. 証明書ファイルと秘密鍵の両方をロードし、 * Install * をクリックします。 証明書では、 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。

Cloud Manager は、 CA 署名付き証明書を使用して、セキュアな HTTPS アクセスを提供するようになりました。次の図は、セキュアアクセス用に設定された Cloud Manager システムを示しています。



Cloud Manager の HTTPS 証明書を更新します

Cloud Manager Web コンソールへの安全なアクセスを確保するために、 Cloud Manager HTTPS 証明書は有効期限が切れ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証明書を更新しないと、ユーザが 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. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * HTTPS セットアップ * を選択します。

   Cloud Manager 証明書の詳細が表示されます。有効期限も表示されます。

2. [証明書の変更] をクリックし、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。

Cloud Manager は新しい CA 署名付き証明書を使用して、セキュアな HTTPS アクセスを提供します。

HTTP プロキシサーバを使用するためのコネクタの設定

社内ポリシーで、インターネットへのすべての HTTP 通信にプロキシサーバを使用する必要がある場合は、その HTTP プロキシサーバを使用するようにコネクタを設定する必要があります。プロキシサーバは、クラウドまたはネットワークに配置できます。

Cloud Manager では、コネクタでの HTTPS プロキシの使用はサポートされていません。

コネクタでプロキシを有効にします

プロキシサーバ、そのコネクタ、および管理対象の Cloud Volumes ONTAP システム（ HA メディエーターを含む）を使用するようにコネクタを設定すると、すべてのでプロキシサーバが使用されます。

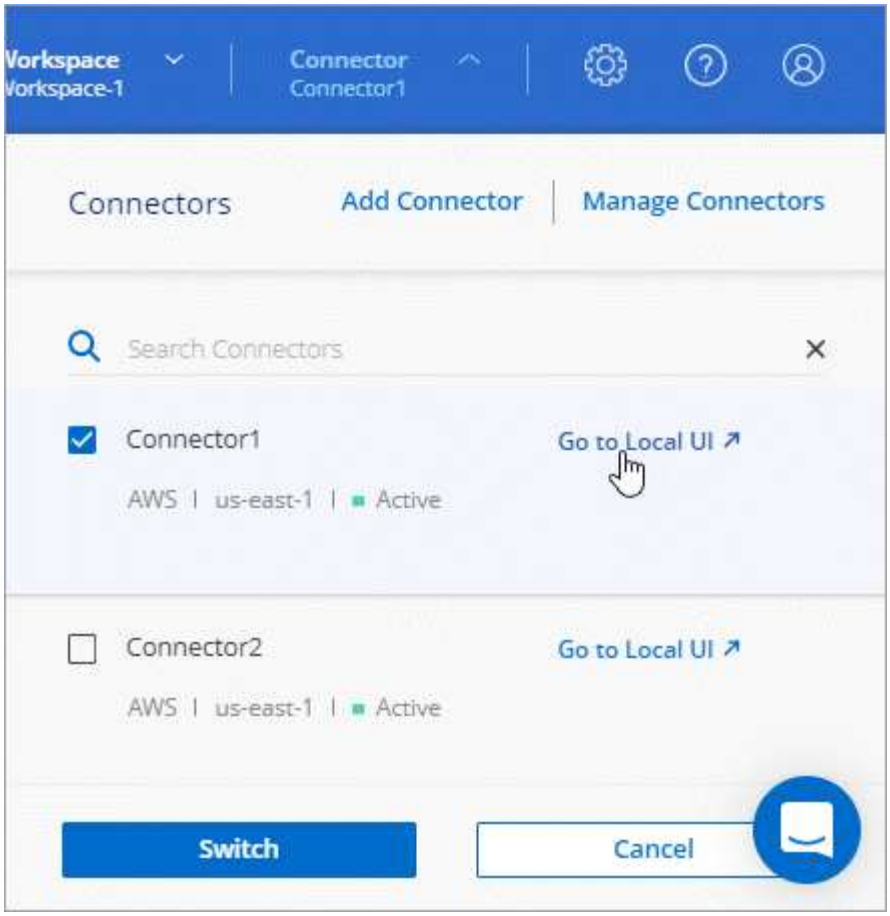
この操作により、コネクタが再起動されます。続行する前に、コネクタが操作を実行していないことを確認してください。

手順

1. "Cloud Manager SaaS インターフェイスにログインします" コネクターインスタンスへのネットワーク接続を持つマシンから。

   コネクタにパブリック IP アドレスがない場合は、 VPN 接続が必要です。そうでない場合は、コネクタと同じネットワークにあるジャンプホストから接続する必要があります。

2. [* コネクタ * （ Connector * ）] ドロップダウンをクリックし、特定のコネクターの [ローカル UI へ移動（ * Go to local UI * ）] をクリックする。



コネクタで実行されている Cloud Manager インターフェイスが新しいブラウザタブに表示されます。

3. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * コネクタ設定 * を選択します。

4. [**General**] で、 **[*HTTP Proxy Configuration**] をクリックします。
5. プロキシを設定します。
   a. [プロキシを有効にする *] をクリックします
   b. 構文を使用してサーバを指定します http://*address:port*[]
   c. ベーシック認証の場合は、ユーザ名とパスワードを指定します サーバに必要です
   d. [保存（ Save ）] をクリックします。

   Cloud Manager では、 @ 文字を含むパスワードはサポートされていません。

プロキシサーバを指定すると、 AutoSupport メッセージの送信時にプロキシサーバを使用するように、新しい Cloud Volumes ONTAP システムが自動的に設定されます。ユーザが Cloud Volumes ONTAP システムを作成する前にプロキシサーバを指定しなかった場合は、 System Manager を使用して、各システムの AutoSupport オプションでプロキシサーバを手動で設定する必要があります。

API の直接トラフィックを有効にします

プロキシサーバを設定している場合は、プロキシを経由せずに Cloud Manager に API 呼び出しを直接送信できます。このオプションは、 AWS 、 Azure 、または Google Cloud で実行されているコネクタでサポートされます。

手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * コネクタ設定 * を選択します。

2. **[General]** で、 **[** Support Direct API traffic*] をクリックします。
3. チェックボックスをクリックしてオプションを有効にし、 * 保存 * をクリックします。

コネクタのデフォルト設定

コネクタのトラブルシューティングが必要な場合は、コネクタの設定を理解すると役立つことがあります。

インターネットアクセスを使用するデフォルト設定

- Cloud Manager から（またはクラウドプロバイダのマーケットプレイスから直接） Connector を導入した場合は、次の点に注意してください。
  - AWS では、 EC2 Linux インスタンスのユーザ名は EC2-user です。
  - イメージのオペレーティングシステムは次のとおりです。
    - AWS ： Red Hat Enterprise Linux 7.6 （ HVM ）
    - Azure ： CentOS 7.6
    - GCP ： CentOS 7.9

      オペレーティングシステムには GUI は含まれていません。システムにアクセスするには、端末を使用する必要があります。
- Cloud Manager から導入した場合、デフォルトのシステムディスクは次のようになります。
  - AWS ： 50GiB の gp2 ディスクです
  - Azure ： 100GiB の Premium SSD ディスク
  - Google Cloud ： 100GiB の SSD 永続ディスク
- Connector インストールフォルダは、次の場所にあります。

  /opt/application/netapp/cloudmanager です
- ログファイルは次のフォルダに格納されます。
  - /opt/application/netapp/cloudmanager/log を選択します

このフォルダのログには、 Connector イメージと Docker イメージの詳細が記録されます。

- /opt/application/NetApp/cloudmanager/docx_occm/data/log

  このフォルダには、コネクタで実行されているクラウドサービスと Cloud Manager サービスの詳細が記録されます。

- Cloud Manager サービスの名前は occm です。
- OCCM サービスは MySQL サービスに依存します。

  MySQL サービスがダウンしている場合は、 OCCM サービスもダウンしています。

- 次のパッケージがまだインストールされていない場合は、 Cloud Manager によって Linux ホストにインストールされます。
  - 7 郵便番号
  - AWSCLI
  - Docker です
  - Java
  - Kubectl のように入力する
  - MySQL
  - Tridentctl
  - プル
  - 取得
- このコネクタは Linux ホストで次のポートを使用します。
  - HTTP アクセスの場合は 80
  - 443 ： HTTPS アクセス用
  - 3306 （ Cloud Manager データベース用
  - クラウドマネージャ API プロキシの場合は 8080
  - Service Manager API の場合は 8666
  - 8777 （ Health-Checker コンテナサービス API の場合）

インターネットアクセスを使用しないデフォルトの設定

インターネットにアクセスできないオンプレミスの Linux ホストにコネクタを手動でインストールした場合、次の構成が適用されます。 "このインストールオプションの詳細については、こちらをご覧ください"。

- Connector インストールフォルダは、次の場所にあります。

  /opt/application/NetApp/DS

- ログファイルは次のフォルダに格納されます。

  /var/lib/docker /volumes /DS_occmdata/_data/log

このフォルダのログには、 Connector イメージと Docker イメージの詳細が記録されます。

- すべてのサービスが Docker コンテナ内で実行されています

  サービスは、実行されている Docker ランタイムサービスに依存します

- このコネクタは Linux ホストで次のポートを使用します。
  - HTTP アクセスの場合は 80
  - 443 ： HTTPS アクセス用

AWS クレデンシャル

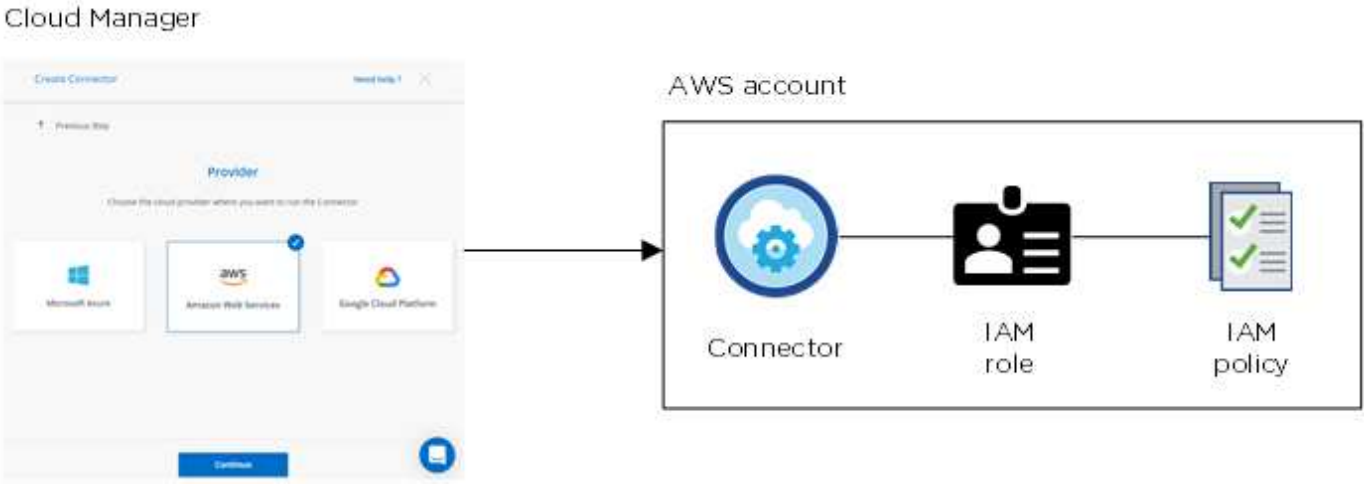
AWS のクレデンシャルと権限

Cloud Manager では、 Cloud Volumes ONTAP の導入時に使用する AWS クレデンシャルを選択できます。すべての Cloud Volumes ONTAP システムは、初期の AWS クレデンシャルを使用して導入することも、クレデンシャルを追加することもできます。

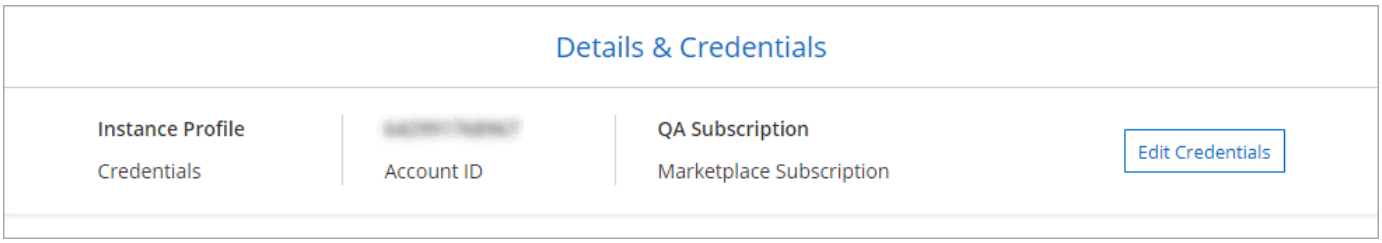
AWS の初期クレデンシャル

Cloud Manager からコネクタを導入する場合は、 IAM ロールの ARN または IAM ユーザのアクセスキーを指定する必要があります。使用する認証方式に、 Connector インスタンスを AWS に導入するための必要な権限がある必要があります。必要な権限は、に表示されます "AWS 用のコネクタ導入ポリシー"。

Cloud Manager が AWS でコネクタインスタンスを起動すると、インスタンス用の IAM ロールとインスタンスプロファイルが作成されます。また、ポリシーを適用して、指定した AWS アカウント内のリソースやプロセスを管理する権限を Connector に提供します。 "Cloud Manager での権限の使用方法を確認します。"。



Cloud Volumes ONTAP の新しい作業環境を作成すると、 Cloud Manager で選択される AWS クレデンシャルにはデフォルトで次のものがあります。

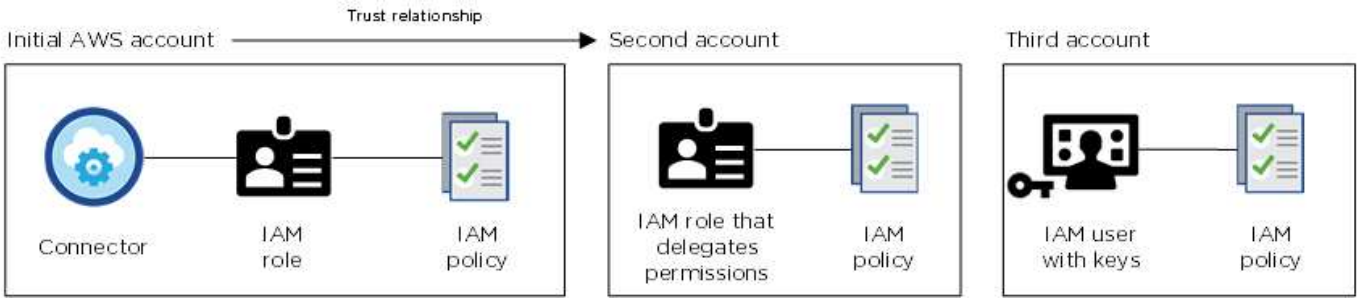


追加の **AWS** クレデンシャル

AWS クレデンシャルを追加する方法は 2 種類あります。

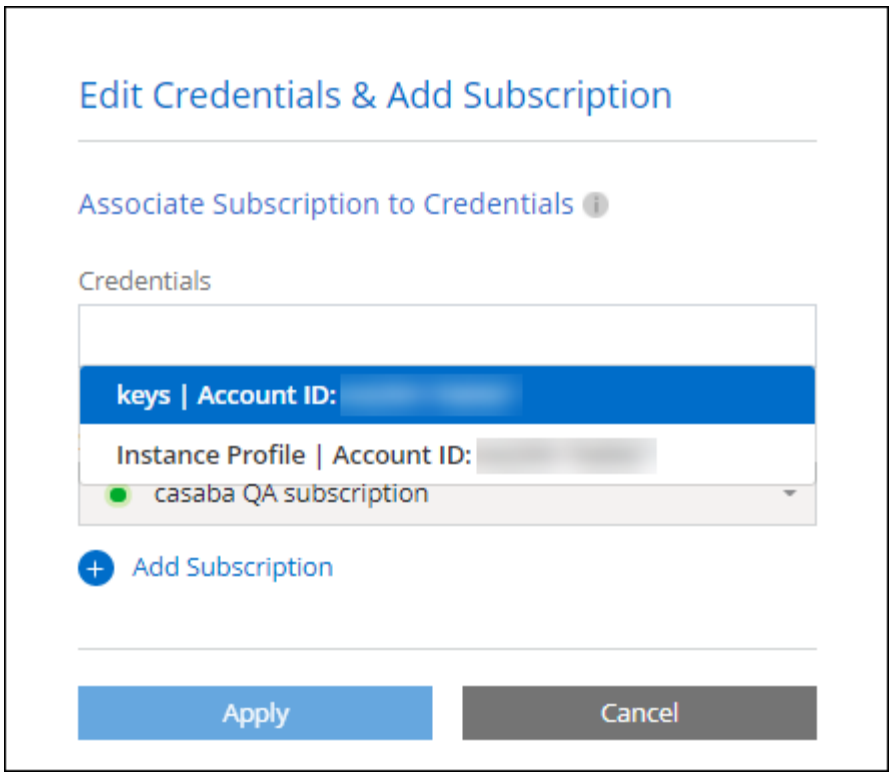
AWS クレデンシャルを既存のコネクタに追加する

別々の AWS アカウントで Cloud Volumes ONTAP を起動する場合は、どちらかを実行します "IAM ユーザまたは ARN に AWS キーを指定します 信頼できるアカウントのロール"。次の図は、 2 つの追加アカウントを示しています。 1 つは、信頼されたアカウントの IAM ロールを介してアクセス許可を提供し、もう 1 つは IAM ユーザの AWS キーを使用してアクセス許可を提供します。



そのあとで "Cloud Manager にアカウントのクレデンシャルを追加します" IAM ロールの Amazon リソース名（ ARN ）、または IAM ユーザの AWS キーを指定します。

クレデンシャルを追加したら、新しい作業環境を作成するときにクレデンシャルに切り替えることができます。



ページで [アカウントの切り替え] をクリックした後に、クラウドプロバイダアカウントを選択する方法を示すスクリーンショット。"]

AWS クレデンシャルを **Cloud Manager** に直接追加

Cloud Manager に新しい AWS クレデンシャルを追加すると、 ONTAP 作業環境の FSX の作成と管理、またはコネクタの作成に必要な権限が Cloud Manager に付与されます。

市場への導入とオンプレミスの導入についてはどうでしょうか。

上記の各セクションでは、 Cloud Manager のコネクタで推奨される導入方法について説明します。から AWS に Connector を導入することもできます "AWS Marketplace" また、次のことも可能です "コネクタをオンプレミスにインストールします"。

Marketplace を使用する場合も、アクセス許可は同じ方法で提供されます。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済みます。

オンプレミス環境では、 Cloud Manager システム用の IAM ロールを設定することはできませんが、追加の AWS アカウントの場合と同様に権限を付与することはできます。

AWS クレデンシャル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。

前述したように、 Cloud Manager では、いくつかの方法で AWS クレデンシャルを提供できます。信頼されたアカウントで IAM ロールを割り当てるか、 AWS アクセスキーを指定することで、コネクタインスタンスに関連付けられた IAM ロールを指定できます。

最初の 2 つのオプションでは、 Cloud Manager は AWS Security Token Service を使用して、継続的にローテーションする一時的なクレデンシャルを取得します。このプロセスはベストプラクティスであり、自動的に実行され、セキュリティが確保されています。

Cloud Manager に AWS アクセスキーを指定する場合は、 Cloud Manager でキーを一定の間隔で更新して、キーをローテーションする必要があります。これは完全に手動で行います。

Cloud Manager の AWS クレデンシャルとサブスクリプションを管理します

AWS クレデンシャルを追加および管理して、 Cloud Manager が AWS アカウントでクラウドリソースを導入および管理するために必要な権限を付与されるようにします。複数の AWS サブスクリプションを管理する場合は、それぞれのサブスクリプションをのクレデンシャルページから別々の AWS クレデンシャルに割り当てることができます。

概要

AWS クレデンシャルは、既存のコネクタに追加するか、 Cloud Manager に直接追加できます。

- AWS クレデンシャルを既存のコネクタに追加する

  既存のコネクタに新しい AWS クレデンシャルを追加すると、同じコネクタを使用して別の AWS アカウントに Cloud Volumes ONTAP を導入できるようになります。 AWS クレデンシャルをコネクタに追加する方法について説明します。

- AWS クレデンシャルを Cloud Manager に直接追加

  Cloud Manager に新しい AWS クレデンシャルを追加すると、 ONTAP 作業環境の FSX の作成と管理、またはコネクタの作成に必要な権限が Cloud Manager に付与されます。 Cloud Manager に AWS クレデンシャルを追加する方法について説明します。

クレデンシャルのローテーション方法

Cloud Manager では、いくつかの方法で AWS クレデンシャルを指定できます。信頼されたアカウントで IAM ロールを割り当てるか、 AWS アクセスキーを指定することで、コネクタインスタンスに関連付けられた IAM ロールを指定します。 "AWS のクレデンシャルと権限に関する詳細情報"。

最初の 2 つのオプションでは、 Cloud Manager は AWS Security Token Service を使用して、継続的にローテーションする一時的なクレデンシャルを取得します。このプロセスは自動でセキュアであるため、ベストプラクティスです。

Cloud Manager に AWS アクセスキーを指定する場合は、 Cloud Manager でキーを一定の間隔で更新して、キーをローテーションする必要があります。これは完全に手動で行います。

コネクタにクレデンシャルを追加します

他の AWS アカウントで Cloud Volumes ONTAP を導入して管理できるように、 AWS クレデンシャルをコネクタに追加します。別のアカウントの IAM ロールの ARN を指定するか、 AWS アクセスキーを指定できます。

権限を付与します

Connector に AWS クレデンシャルを追加する前に、必要な権限を指定する必要があります。この権限を付与することで、 Cloud Manager からその AWS アカウント内のリソースやプロセスを管理できるようになります。権限の指定方法は、 Cloud Manager に信頼されたアカウントまたは AWS キーのロールの ARN を提供するかどうかによって異なります。

Cloud Manager からコネクタを導入すると、 Cloud Manager はコネクタを導入したアカウントの AWS クレデンシャルを自動的に追加しました。既存のシステムに Connector ソフトウェアを手動でインストールした場合、この初期アカウントは追加されません。 "AWS のクレデンシャルと権限について説明します"。

- 選択肢 *
- [Grant permissions by assuming an IAM role in another account]
- [Grant permissions by providing AWS keys]

別のアカウントで **IAM** ロールを想定して権限を付与します

IAM ロールを使用して、コネクタインスタンスを導入したソース 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。その後、 Cloud Manager に信頼されたアカウントの IAM ロールの ARN を提供します。

手順

1. Cloud Volumes ONTAP を導入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、 [役割] 、 [役割の作成 *] の順にクリックし、手順に従って役割を作成します。

   必ず次の手順を実行してください。

   - 信頼されるエンティティのタイプ * 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、コネクタインスタンスが存在するアカウントの ID を入力します。
   - から入手できる Cloud Manager IAM ポリシーを使用してポリシーを作成します "Cloud Manager Policies ページ"。
3. 後日 Cloud Manager に貼り付けることができるように、 IAM ロールの ARN をコピーします。

これで、アカウントに必要な権限が付与されました。 これで、クレデンシャルをコネクタに追加できるようになりました。

AWS キーを指定して権限を付与します

Cloud Manager に IAM ユーザの AWS キーを提供する場合は、必要な権限をそのユーザに付与する必要があります。Cloud Manager IAM ポリシーは、 Cloud Manager が使用できる AWS アクションとリソースを定義します。

手順

1. から Cloud Manager IAM ポリシーをダウンロードします "Cloud Manager Policies ページ"。
2. IAM コンソールから、 Cloud Manager IAM ポリシーからテキストをコピーアンドペーストして、独自のポリシーを作成します。

   "AWS のドキュメント：「 Creating IAM Policies"

3. IAM ロールまたは IAM ユーザにポリシーを関連付けます。
   - "AWS のドキュメント：「 Creating IAM Roles"
   - "AWS のドキュメント：「 Adding and Removing IAM Policies"

これで、アカウントに必要な権限が付与されました。 これで、クレデンシャルをコネクタに追加できるようになりました。

クレデンシャルを追加します

必要な権限を AWS アカウントに付与したら、そのアカウントのクレデンシャルを既存のコネクタに追加できます。これにより、同じコネクタを使用してアカウントの Cloud Volumes ONTAP システムを起動できます。

作成したクレデンシャルをクラウドプロバイダで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。Cloud Manager にクレデンシャルを追加するまで数分待ってから、

手順

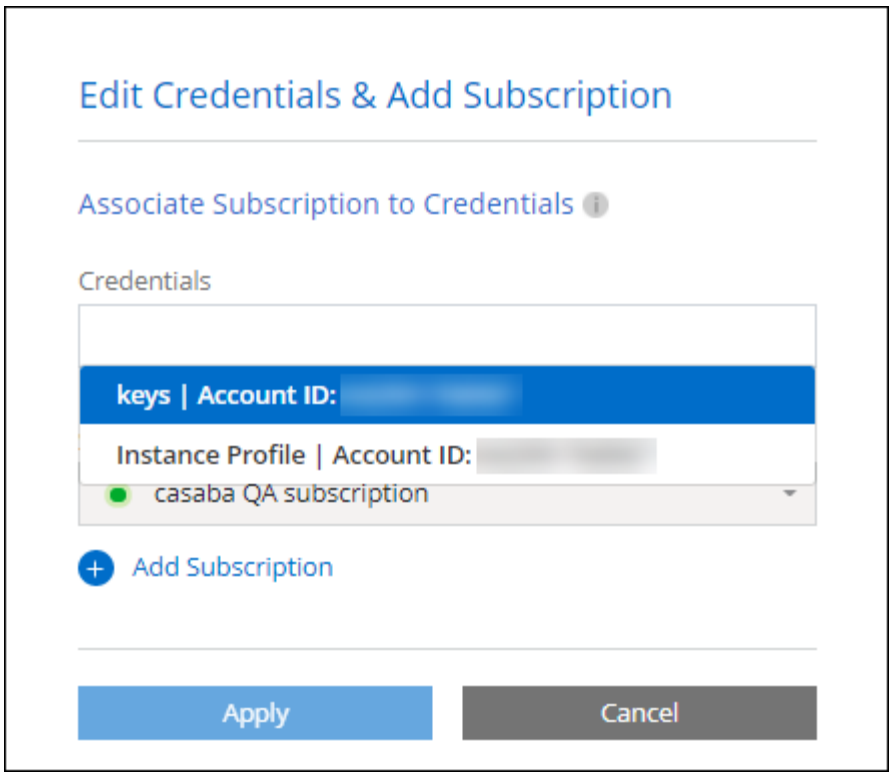
1. Cloud Manager で正しいコネクタが選択されていることを確認します。
2. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * クレデンシャル * を選択します。

3. [Add Credentials] をクリックし、ウィザードの手順に従います。
   a. * 資格情報の場所 * ：「 * Amazon Web Services > Connector * 」を選択します。
   b. * クレデンシャルの定義 * ：信頼された 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. * Marketplace サブスクリプション *: 今すぐ登録するか、既存のサブスクリプションを選択して、 Marketplace 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。

      Cloud Volumes ONTAP の料金を 1 時間単位で支払う（ PAYGO ）場合や 1 年単位で支払う場合は、 AWS のクレデンシャルを AWS Marketplace から Cloud Volumes ONTAP への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 * ：新しいクレデンシャルの詳細を確認し、 * 追加 * をクリックします。

新しい作業環境を作成するときに、 [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。



ページで [アカウントの切り替え] をクリックした後に、クラウドプロバイダアカウントを選択する方法を示すスクリーンショット。"]

Cloud Manager にクレデンシャルを追加します

Cloud Manager に AWS クレデンシャルを追加するには、 IAM ロールの ARN を指定します。このロールにより、 ONTAP 作業環境で FSX を作成したり、コネクタを作成したりするために必要な権限が Cloud Manager に付与されます。

ONTAP 作業環境で FSX を作成する場合、または新しいコネクタを作成する場合に、資格情報を使用できます。

IAM ロールを設定します

Cloud Manager SaaS で役割を引き受けることを可能にする 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、 [役割] 、 [役割の作成 *] の順にクリックし、手順に従って役割を作成します。

   必ず次の手順を実行してください。

   - 信頼されるエンティティのタイプ * 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、 Cloud Manager SaaS の ID として 952013314444 を入力してください
   - ONTAP 作業環境の FSX を作成するため、またはコネクタ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。
     - "ONTAP の FSX に必要な権限を表示します"
     - から Connector 展開ポリシーを表示します "Cloud Manager Policies ページ"

3. IAM ロールのロール ARN をコピーして、次の手順で Cloud Manager に貼り付けることができます。

IAM ロールに必要な権限が割り当てられます。 これで、 Cloud Manager に追加できます。

クレデンシャルを追加します

IAM ロールに必要な権限を付与したら、 Cloud Manager に ARN ロールを追加します。

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数分かかることがあります。Cloud Manager にクレデンシャルを追加するまで数分待ってから、

手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * クレデンシャル * を選択します。

2. [Add Credentials] をクリックし、ウィザードの手順に従います。
   a. * クレデンシャルの場所 * ：「 * Amazon Web Services > Cloud Manager * 」を選択します。
   b. * クレデンシャルの定義 * ： IAM ロールの ARN （ Amazon リソース名）を指定します。
   c. * 確認 * ：新しいクレデンシャルの詳細を確認し、 * 追加 * をクリックします。

FSX for ONTAP 作業環境を作成するとき、または新しいコネクタを作成するときに、資格情報を使用できるようになりました。

AWS サブスクリプションを関連付ける

Cloud Manager に AWS のクレデンシャルを追加したら、 AWS Marketplace のサブスクリプションをそれらのクレデンシャル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、 Cloud Volumes ONTAP の料金を時間単位で支払う（ PAYGO ）と年単位の契約を使用する、および他の NetApp クラウドサービスを使用することができます。

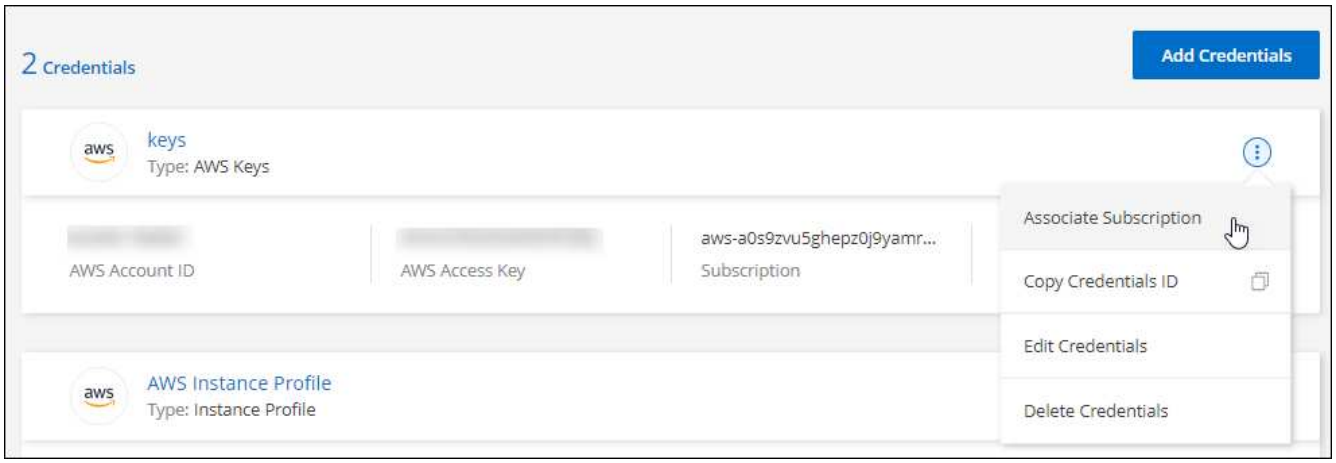
Cloud Manager にクレデンシャルを追加したあとに、 AWS Marketplace サブスクリプションを関連付けるシナリオは 2 つあります。

- Cloud Manager にクレデンシャルを最初に追加したときに、サブスクリプションを関連付けていません。
- 既存の AWS Marketplace 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場合。

Cloud Manager の設定を変更する前に、コネクタを作成する必要があります。 "コネクタの作成方法を説明します"。

手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * クレデンシャル * を選択します。
2. 一連の資格情報のアクションメニューをクリックし、 * 契約の関連付け * を選択します。



3. ダウンリストから既存のサブスクリプションを選択するか、 * サブスクリプションの追加 * をクリックして、新しいサブスクリプションを作成する手順を実行します。

   ▶ https://docs.netapp.com/ja-jp/cloud-manager-setup-admin//media/video_subscribing_aws.mp4 *(video)*

クレデンシャルを編集する

Cloud Manager で AWS クレデンシャルを編集するには、アカウントタイプ（ AWS キーまたは想定ロール）を変更するか、名前を編集するか、クレデンシャル自体（キーまたはロール ARN ）を更新します。

コネクタ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クレデンシャルは編集できません。

手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * クレデンシャル * を選択します。
2. 一連の資格情報のアクションメニューをクリックし、 * 資格情報の編集 * を選択します。
3. 必要な変更を行い、 * 適用 * をクリックします。

クレデンシャルを削除し

クレデンシャルが不要になった場合は、 Cloud Manager から削除できます。削除できるのは、作業環境に関連付けられていないクレデンシャルのみです。

コネクタ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クレデンシャルは削除できません。

手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * クレデンシャル * を選択します。
2. 一連の資格情報のアクションメニューをクリックし、 * 資格情報の削除 * を選択します。
3. 削除を確定するには、 * 削除 * をクリックします。

Azure のクレデンシャル

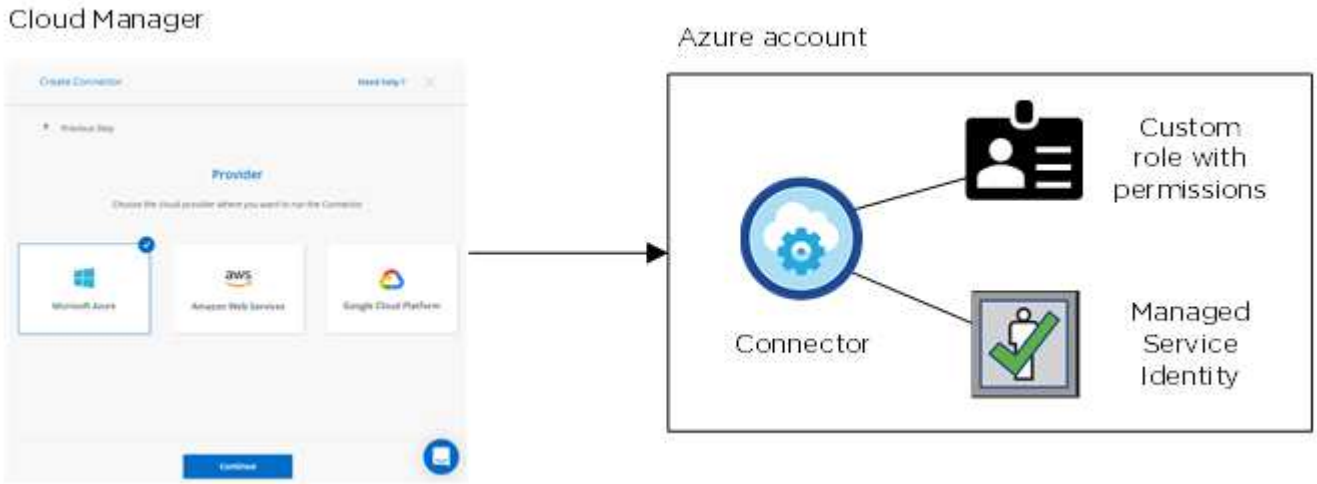
Azure のクレデンシャルと権限

Cloud Manager では、 Cloud Volumes ONTAP の導入時に使用する Azure クレデンシャルを選択できます。すべての Cloud Volumes ONTAP システムは、初期の Azure クレデンシャルを使用して導入することも、クレデンシャルを追加することもできます。

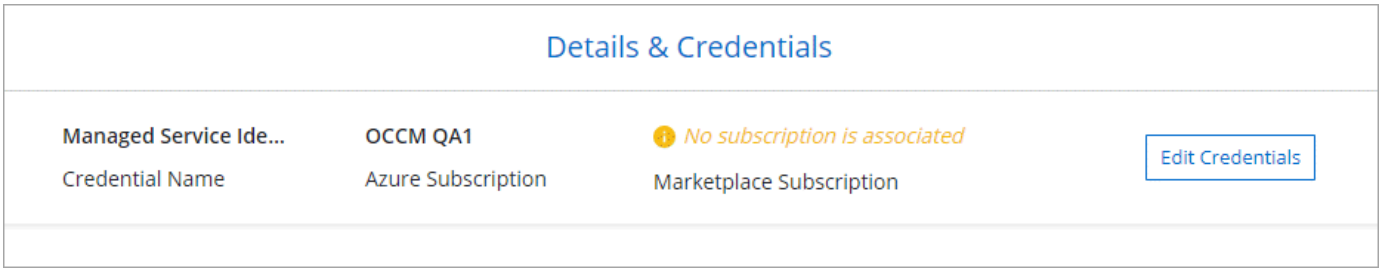
Azure の初期クレデンシャル

Cloud Manager から Connector を導入する場合は、 Connector 仮想マシンを導入する権限を持つ 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、に表示されます "Azure の Connector 導入ポリシー"。

Cloud Manager が Azure に Connector 仮想マシンを導入すると、が有効になります "システムによって割り当てられた管理 ID" 仮想マシンで、カスタムロールを作成して仮想マシンに割り当てます。Cloud Manager に、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権限が付与されます。 "Cloud Manager での権限の使用方法を確認します。"。



Cloud Volumes ONTAP 用の新しい作業環境を作成すると、 Cloud Manager でデフォルトで次の Azure クレデンシャルが選択されます。

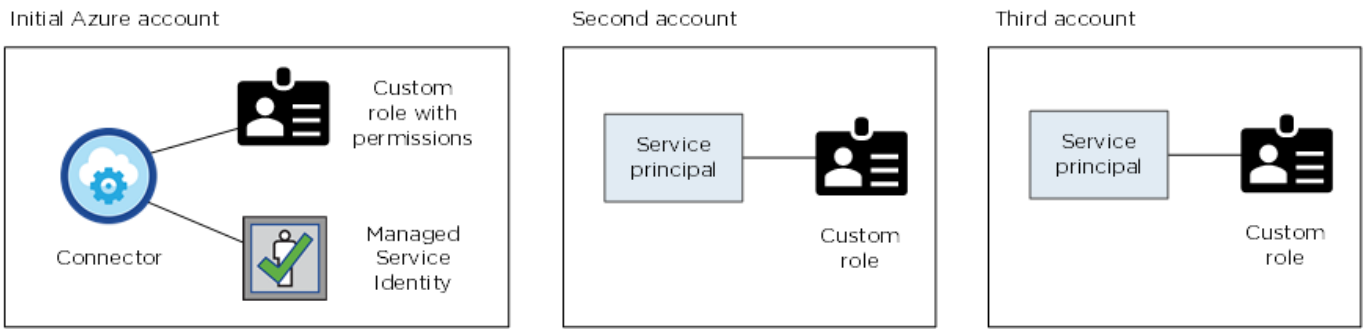


マネージド ID 向けの Azure サブスクリプションが追加されました

管理対象 ID は、 Connector を起動したサブスクリプションに関連付けられます。別の Azure サブスクリプションを選択する場合は、が必要です "管理対象 ID をこれらのサブスクリプションに関連付けます"。

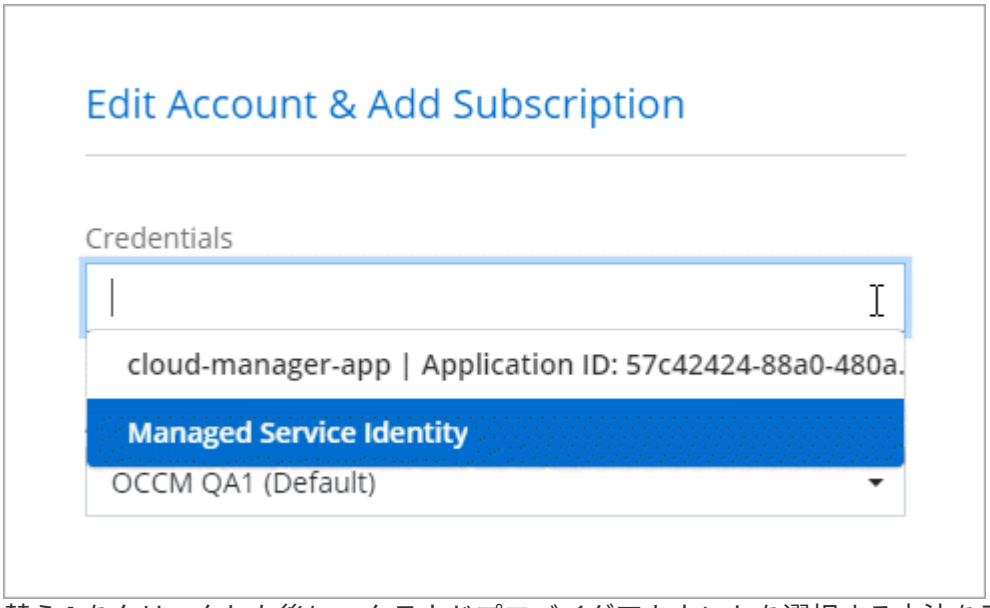
Azure の追加クレデンシャル

別の Azure クレデンシャルを使用して Cloud Volumes ONTAP を導入する場合は、必要な権限をに付与する必要があります "Azure Active でサービスプリンシパルを作成およびセットアップする ディレクトリ" を Azure アカウントごとに用意します。次の図は、 2 つの追加アカウントを示しています。各アカウントには、権限を提供するサービスプリンシパルとカスタムロールが設定されています。



そのあとで "Cloud Manager にアカウントのクレデンシャルを追加します" AD サービスプリンシパルの詳細を指定します。

クレデンシャルを追加したら、新しい作業環境を作成するときにクレデンシャルに切り替えることができます。



ページで [アカウントの切り替え] をクリックした後に、クラウドプロバイダアカウントを選択する方法を示すスクリーンショット。"]

市場への導入とオンプレミスの導入についてはどうでしょうか。

上記のセクションでは、 NetApp Cloud Central のコネクタで推奨される導入方法について説明します。から Azure に Connector を導入することもできます "Azure Marketplace で入手できます"を使用できます "コネクタをオンプレミスにインストールします"。

Marketplace を使用する場合も、アクセス許可は同じ方法で提供されます。コネクタの管理 ID を手動で作成してセットアップし、追加のアカウントに権限を付与するだけで済みます。

オンプレミス環境では、 Connector の管理対象 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追加のアカウントの場合と同様に権限を設定できます。

Cloud Manager の Azure クレデンシャルとサブスクリプションの管理

Cloud Volumes ONTAP システムを作成するときに、そのシステムで使用する Azure クレデンシャルを選択する必要があります。従量課金制のライセンスを使用している場合は、 Marketplace サブスクリプションも選択する必要があります。複数の Azure クレデンシャルを使用する場合や、複数の Azure Marketplace サブスクリプションを Cloud Volumes ONTAP に使用する場合は、このページの手順に従います。

Cloud Manager で Azure サブスクリプションとクレデンシャルを追加するには、 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 管理 ID に関連付けます。
2. 別の Azure クレデンシャルを使用して Cloud Volumes ONTAP を導入する場合は、サービスプリンシパルを使用して Azure 権限を付与し、そのクレデンシャルを Cloud Manager に追加します。

追加の Azure サブスクリプションを管理対象 ID に関連付ける

Cloud Manager では、 Cloud Volumes ONTAP を導入する Azure クレデンシャルと Azure サブスクリプションを選択できます。管理対象に別の Azure サブスクリプションを選択することはできません を関連付けない限り、アイデンティティプロファイルを作成します "管理された ID" それらの登録と。

管理対象 ID はです "最初の Azure アカウント" Cloud Manager からコネクタを導入する場合。コネクタを導入すると、 Cloud Manager Operator ロールが作成され、 Connector 仮想マシンに割り当てられます。

手順

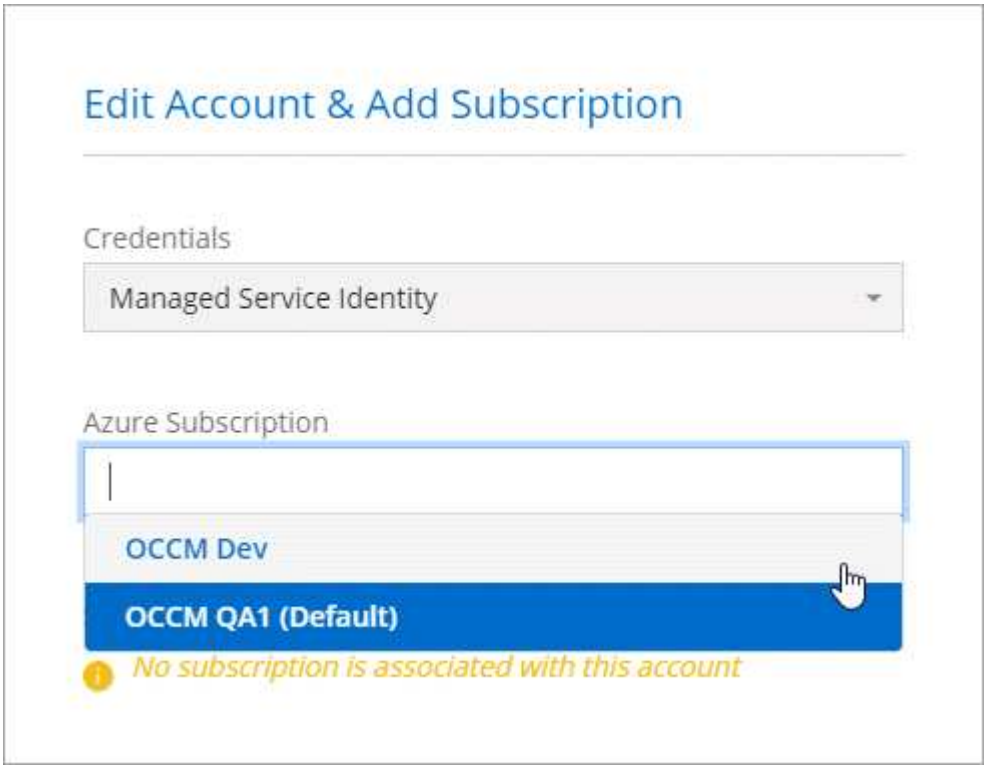
1. Azure ポータルにログインします。
2. [サブスクリプション] サービスを開き、 Cloud Volumes ONTAP を展開するサブスクリプションを選択します。
3. 「 * アクセスコントロール（ IAM ） * 」をクリックします。
   a. [* 追加 > 役割の割り当ての追加 *] をクリックして、権限を追加します。
      - Cloud Manager Operator * ロールを選択します。

      Cloud Manager Operator は、で指定されたデフォルトの名前です "Cloud Manager ポリシー"。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。
- Connector 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。
- Connector 仮想マシンを選択します。
- [保存（ Save ）] をクリックします。

4. 追加のサブスクリプションについても、この手順を繰り返します。

新しい作業環境を作成するときに、管理対象 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。



Cloud Manager に **Azure** クレデンシャルを追加しておきます

Cloud Manager からコネクタを導入すると、必要な権限が割り当てられた仮想マシンで、 Cloud Manager によってシステムによって割り当てられた管理対象 ID を使用できるようになります。Cloud Volumes ONTAP 用の新しい作業環境を作成すると、 Cloud Manager でデフォルトで次の Azure クレデンシャルが選択されます。

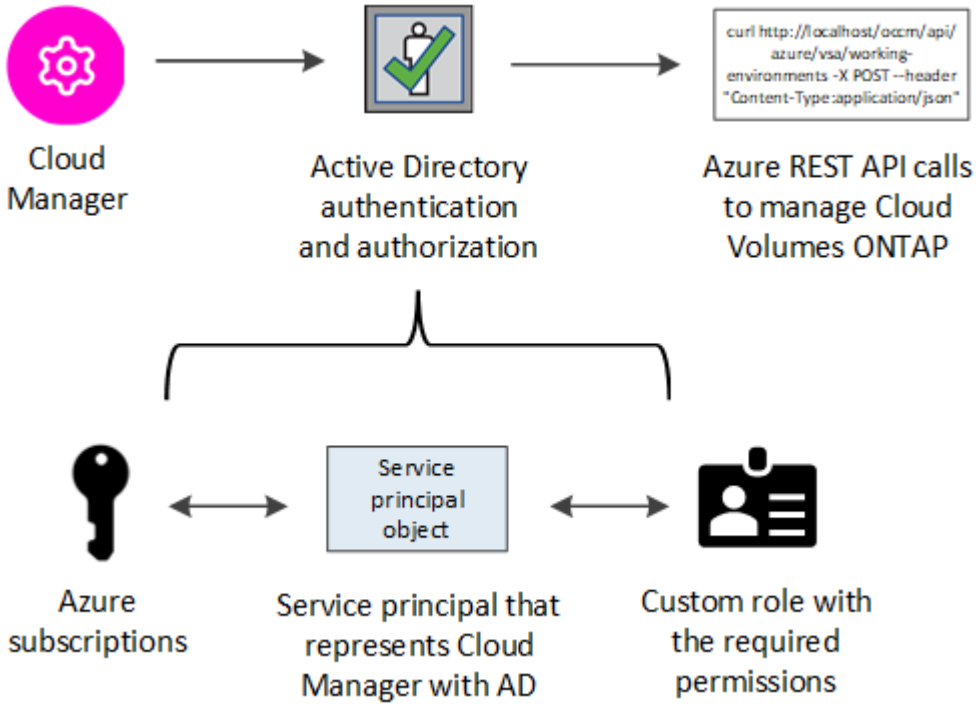
既存のシステムに Connector ソフトウェアを手動でインストールした場合、初期クレデンシャルは追加されません。 "Azure のクレデンシャルと権限について説明します"。

異なる Azure クレデンシャルを使用して Cloud Volumes ONTAP を導入する場合は、 Azure Active Directory 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、 Cloud Manager に新しいクレデンシャルを追加できます。

サービスプリンシパルを使用した **Azure** 権限の付与

Cloud Manager には、 Azure でアクションを実行するための権限が必要です。Azure アカウントに必要な権限を付与するには、 Azure Active Directory でサービスプリンシパルを作成して設定し、 Cloud Manager で必要な Azure クレデンシャルを取得します。

次の図は、 Cloud Manager 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、 Azure Active Directory の Cloud Manager を表し、必要な権限を許可するカスタムロールに割り当てられます。



手順

1. Azure Active Directory アプリケーションを作成します。
2. アプリケーションをロールに割り当てます。
3. Windows Azure Service Management API 権限を追加します。
4. アプリケーション ID とディレクトリ ID を取得します。
5. クライアントシークレットを作成します。

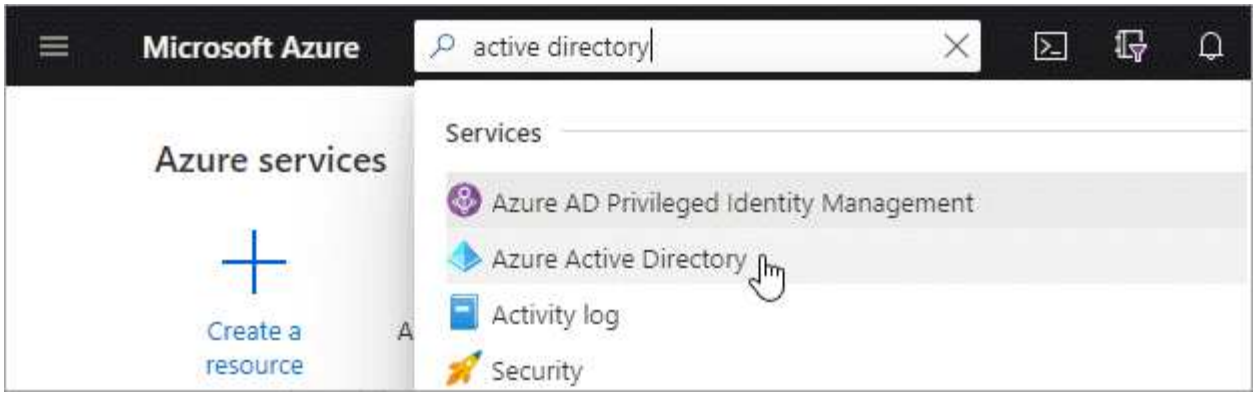
Azure Active Directory アプリケーションの作成

Cloud Manager でロールベースアクセス制御に使用できる Azure Active Directory （ 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す。

Azure で Active Directory アプリケーションを作成してロールに割り当てるための適切な権限が必要です。詳細については、を参照してください "Microsoft Azure のドキュメント：「 Required permissions"。

手順

1. Azure ポータルで、 * Azure Active Directory * サービスを開きます。



2. メニューで、 * アプリ登録 * をクリックします。
3. [新規登録] をクリックします。
4. 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（ Cloud Manager 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できます。
5. [*Register] をクリックします。

AD アプリケーションとサービスプリンシパルを作成しておきます。

アプリケーションをロールに割り当てます

Azure で Cloud Manager に権限を付与するには、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「 OnCommand Cloud Manager Operator 」ロールを割り当てる必要があります。

手順

1. をダウンロードします "Cloud Manager Azure ポリシー"。

   リンクを右クリックし、 [名前を付けてリンクを保存 ...] をクリックしてファイルをダウンロードする。

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 ファイルを変更します。

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

   - 例 *

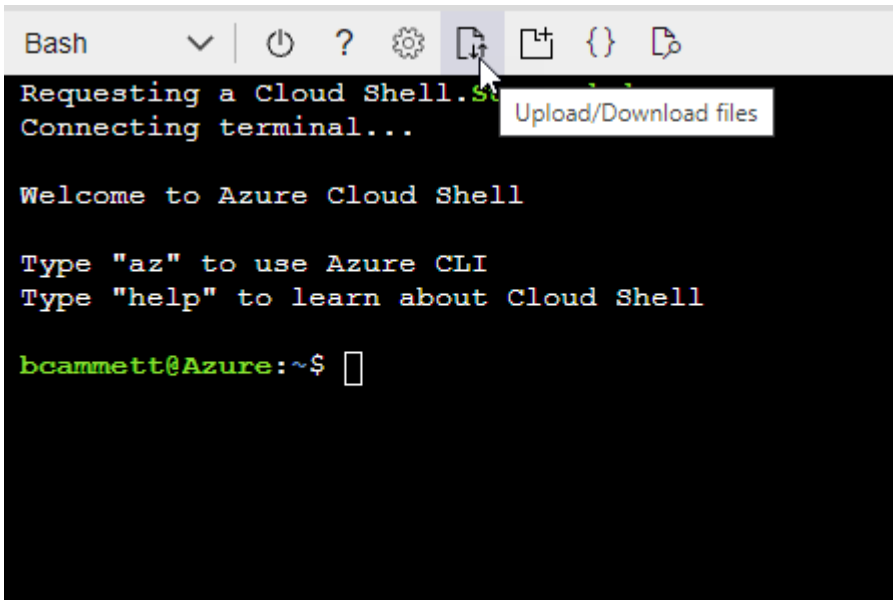
```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

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。

次の手順は、 Azure Cloud Shell で Bash を使用してロールを作成する方法を示しています。

a. 開始 "Azure Cloud Shell の略" 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 で次のコマンドを入力します。

```
az role definition create --role-definition
Policy_for_cloud_Manager_Azure_3.9.8.json
```

これで、 _Cloud Manager Operator _ という名前のカスタムロールが作成されます。

4. ロールにアプリケーションを割り当てます。

a. Azure ポータルで、 * Subscriptions * サービスを開きます。

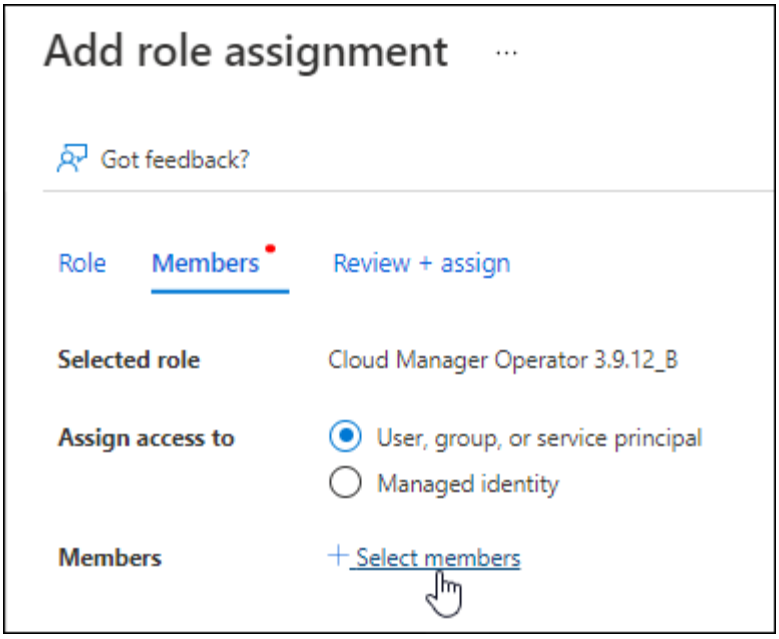
b. サブスクリプションを選択します。

c. [* アクセス制御 (IAM)] 、 [追加] 、 [役割の割り当ての追加 *] の順にクリックします。

d. [* 役割] タブで、 * Cloud Manager Operator * 役割を選択し、 * Next * をクリックします。

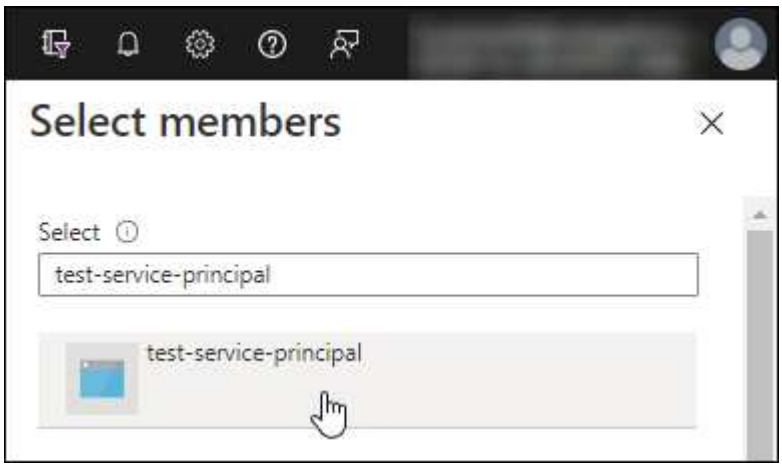
e. [* Members* （メンバー * ）] タブで、次の手順を実行します。

- [* 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。
- [メンバーの選択] をクリックします。



- 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、 * Select * をクリックします。
- 「 * 次へ * 」をクリックします。

f. [レビュー + 割り当て（ Review + Assign ）] をクリックします。

サービスプリンシパルに、 Connector の導入に必要な Azure 権限が付与されるようになりました。

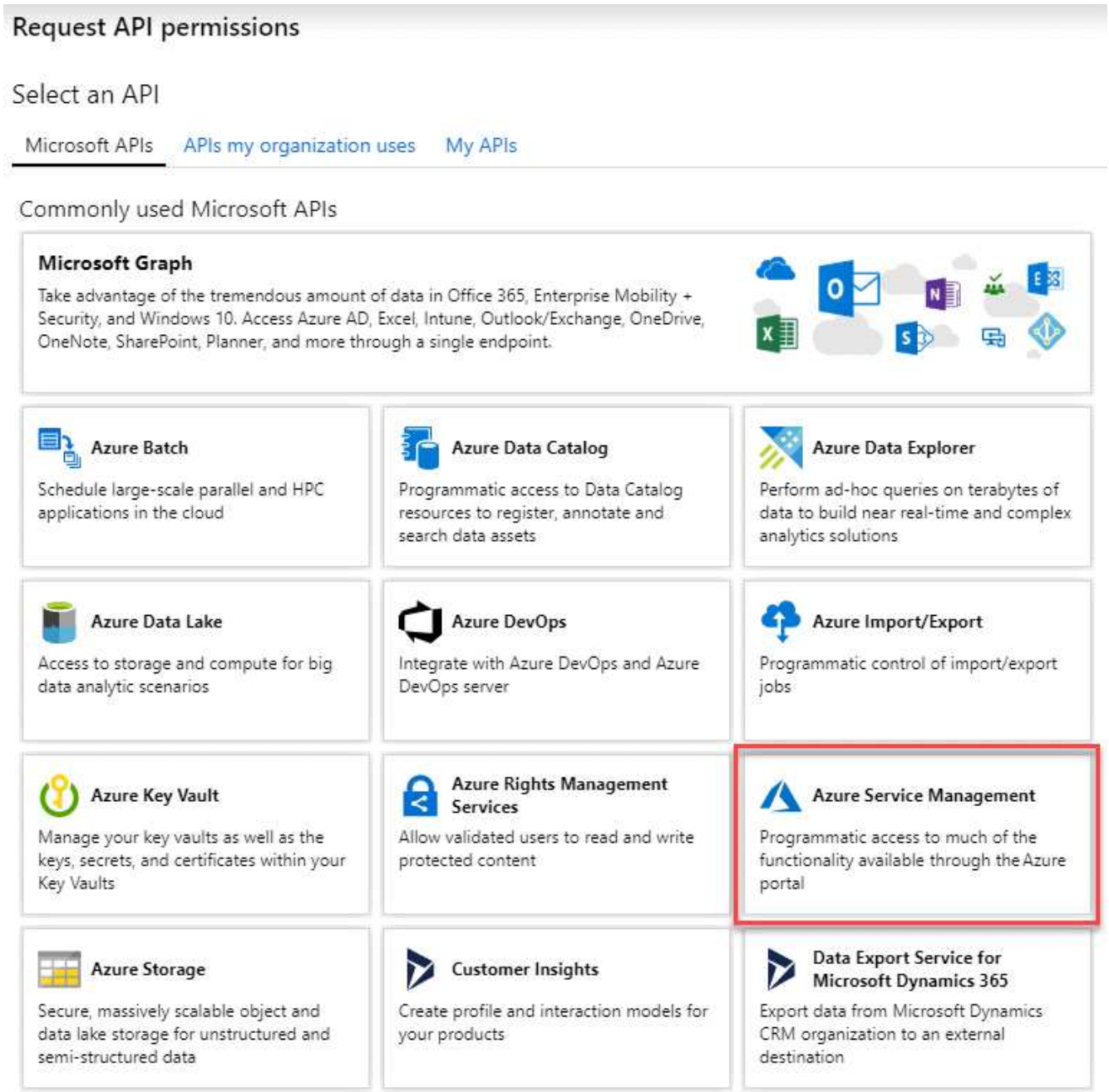
Cloud Volumes ONTAP を複数の Azure サブスクリプションから導入する場合は、サービスプリンシパルを各サブスクリプションにバインドする必要があります。Cloud Manager では、 Cloud Volumes ONTAP の導入時に使用するサブスクリプションを選択できます。

Windows Azure Service Management API 権限を追加しています

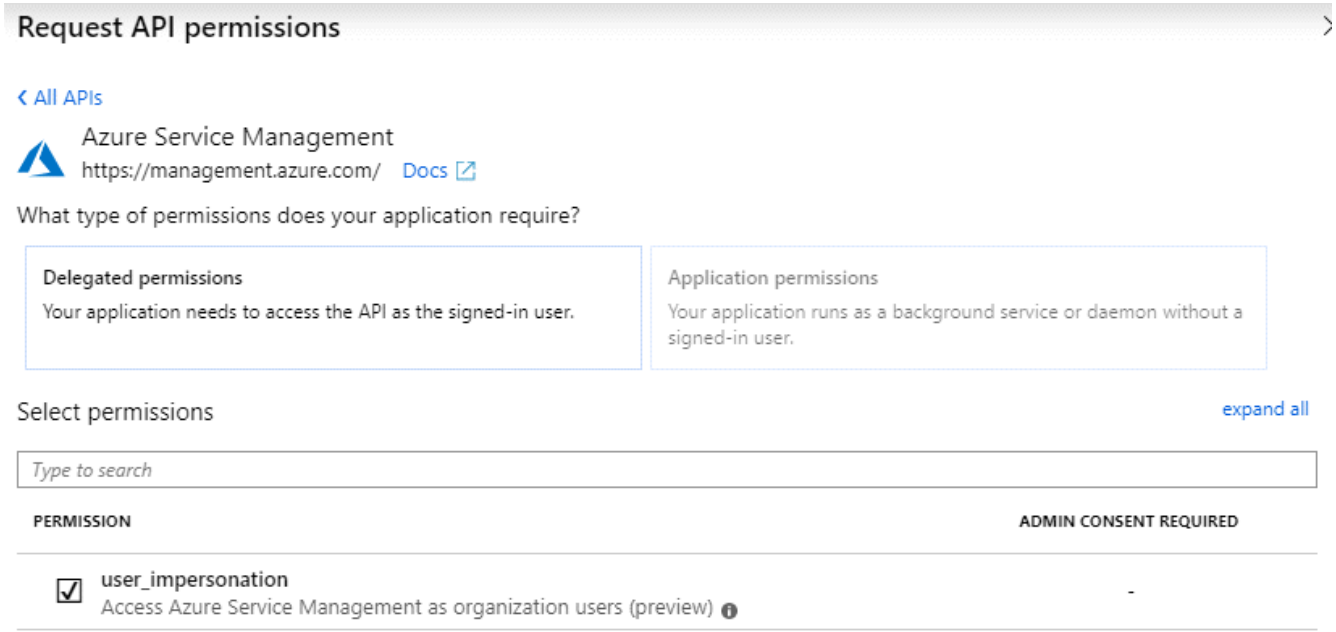
サービスプリンシパルに「 Windows Azure Service Management API 」の権限が必要です。

手順

1. Azure Active Directory * サービスで、 * アプリ登録 * をクリックしてアプリケーションを選択します。
2. [API アクセス許可] 、 [アクセス許可の追加] の順にクリックします。
3. Microsoft API* 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 *] をクリックし、 [* 権限の追加 *] をクリックします。

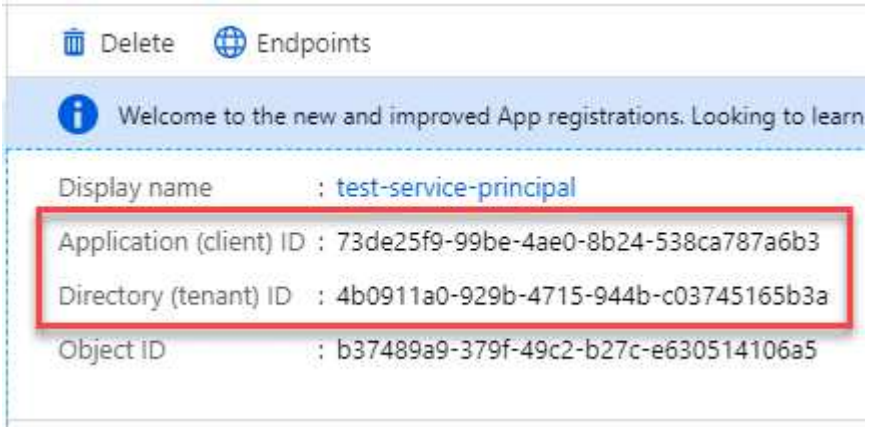


アプリケーション **ID** とディレクトリ **ID** を取得しています

Cloud Manager に Azure アカウントを追加するときは、アプリケーション（クライアント）の 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。Cloud Manager は、この ID を使用してプログラムによってサインインします。

手順

1. Azure Active Directory * サービスで、 * アプリ登録 * をクリックして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。



クライアントシークレットの作成

Cloud Manager がクライアントシークレットを使用して Azure AD で認証できるようにするには、クライアントシークレットを作成し、そのシークレットの値を Cloud Manager に指定する必要があります。

手順

1. Azure Active Directory * サービスを開きます。

2. [* アプリ登録 *] をクリックして、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 * ］ をクリックします。
4. シークレットと期間の説明を入力します。
5. [追加（ Add ）] をクリックします。
6. クライアントシークレットの値をコピーします。

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をコピーしました。この情報は、 Cloud Manager で Azure アカウントを追加するときに入力する必要があります。

Cloud Manager にクレデンシャルを追加してください

必要な権限を Azure アカウントに付与したら、そのアカウントのクレデンシャルを Cloud Manager に追加できます。この手順を完了すると、複数の Azure クレデンシャルを使用して Cloud Volumes ONTAP を起動できます。

作成したクレデンシャルをクラウドプロバイダで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。Cloud Manager にクレデンシャルを追加するまで数分待ってから、

Cloud Manager の設定を変更する前に、コネクタを作成する必要があります。 "詳細をご確認ください"。

手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * クレデンシャル * を選択します。

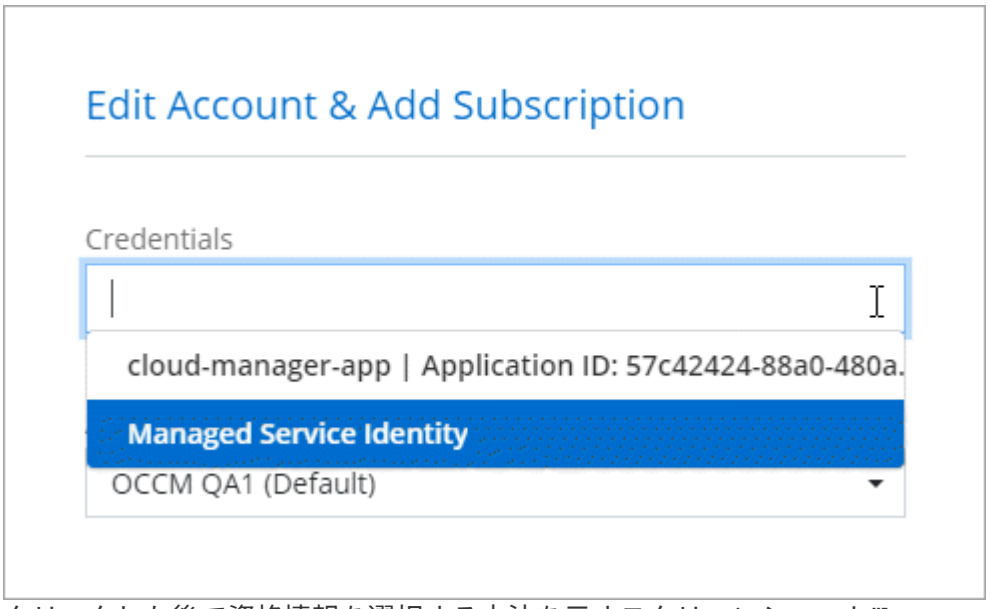
2. [Add Credentials] をクリックし、ウィザードの手順に従います。
   a. * 資格情報の場所 * ： Microsoft Azure > Connector * を選択します。
   b. * クレデンシャルの定義 * ：必要な権限を付与する Azure Active Directory サービスプリンシパルに関する情報を入力します。
      - アプリケーション（クライアント） ID ：を参照してください [Getting the application ID and directory ID]。
      - ディレクトリ（テナント） ID ：を参照してください [Getting the application ID and directory ID]。
      - クライアントシークレット：を参照してください [Creating a client secret]。

c. * Marketplace サブスクリプション *: 今すぐ登録するか、既存のサブスクリプションを選択して、 Marketplace 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。

   Cloud Volumes ONTAP の料金を時間単位で支払う（ PAYGO ）には、 Azure のクレデンシャルが Azure Marketplace からのサブスクリプションに関連付けられている必要があります。

d. * 確認 * ：新しいクレデンシャルの詳細を確認し、 * 追加 * をクリックします。

これで、から別のクレデンシャルセットに切り替えることができます [詳細と資格情報] ページ "新しい作業環境を作成する場合"



ページで [資格情報の編集] をクリックした後で資格情報を選択する方法を示すスクリーンショット"]

既存のクレデンシャルを管理する

Cloud Manager にすでに追加した Azure クレデンシャルの管理では、 Marketplace でのサブスクリプションの関連付け、クレデンシャルの編集、および削除を行います。

Azure Marketplace サブスクリプションをクレデンシャルに関連付ける

Cloud Manager に Azure のクレデンシャルを追加したら、 Azure Marketplace サブスクリプションをそれらのクレデンシャル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、他のネットアップクラウドサービスを使用できます。

Cloud Manager にクレデンシャルを追加したあとに、 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。

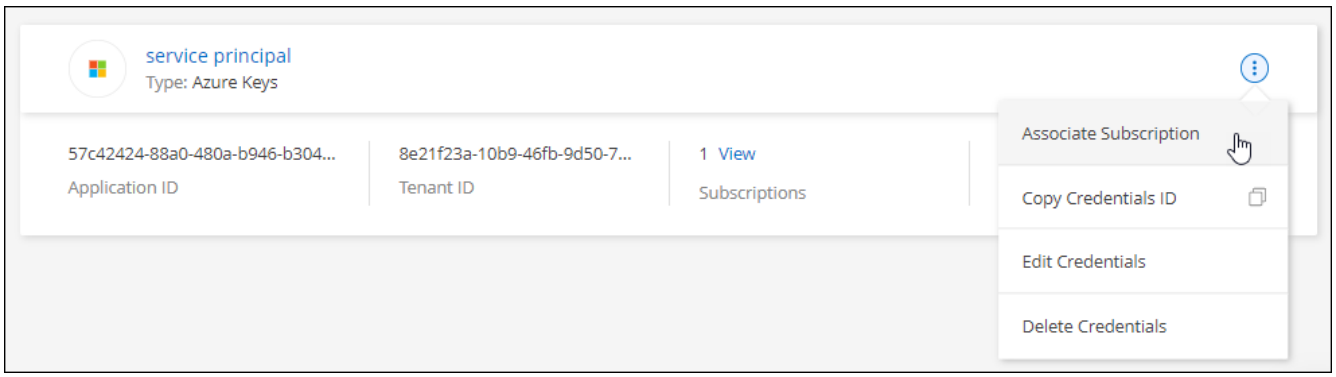
- Cloud Manager にクレデンシャルを最初に追加したときに、サブスクリプションを関連付けていません。
- 既存の Azure Marketplace サブスクリプションを新しいサブスクリプションに置き換える場合。

Cloud Manager の設定を変更する前に、コネクタを作成する必要があります。 "詳細をご確認ください"。

手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * クレデンシャル * を選択します。

2. 一連の資格情報のアクションメニューをクリックし、 * 契約の関連付け * を選択します。



3. ダウンリストからサブスクリプションを選択するか、 * サブスクリプションの追加 * をクリックして、手順に従って新しいサブスクリプションを作成します。

   次のビデオは、作業環境ウィザードのコンテキストから開始しますが、 [サブスクリプションの追加] をクリックした後も同じワークフローが表示されます。

   ▶ https://docs.netapp.com/ja-jp/cloud-manager-setup-admin//media/video_subscribing_azure.mp4 *(video)*

クレデンシャルの編集

Azure サービスクレデンシャルの詳細を変更して、 Cloud Manager で Azure クレデンシャルを編集します。たとえば、サービスプリンシパルアプリケーション用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の更新が必要になることがあります。

手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * クレデンシャル * を選択します。
2. 一連の資格情報のアクションメニューをクリックし、 * 資格情報の編集 * を選択します。
3. 必要な変更を行い、 * 適用 * をクリックします。

クレデンシャルを削除し

クレデンシャルが不要になった場合は、 Cloud Manager から削除できます。削除できるのは、作業環境に関連付けられていないクレデンシャルのみです。

手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * クレデンシャル * を選択します。
2. 一連の資格情報のアクションメニューをクリックし、 * 資格情報の削除 * を選択します。
3. 削除を確定するには、 * 削除 * をクリックします。

Google Cloud のクレデンシャル

Google Cloud のプロジェクト、権限、アカウント

サービスアカウントを使用すると、 Cloud Manager に対し、 Connector と同じプロジェクトまたは異なるプロジェクトにある Cloud Volumes ONTAP システムを導入および管

理する権限が付与されます。

Cloud Manager のプロジェクトと権限

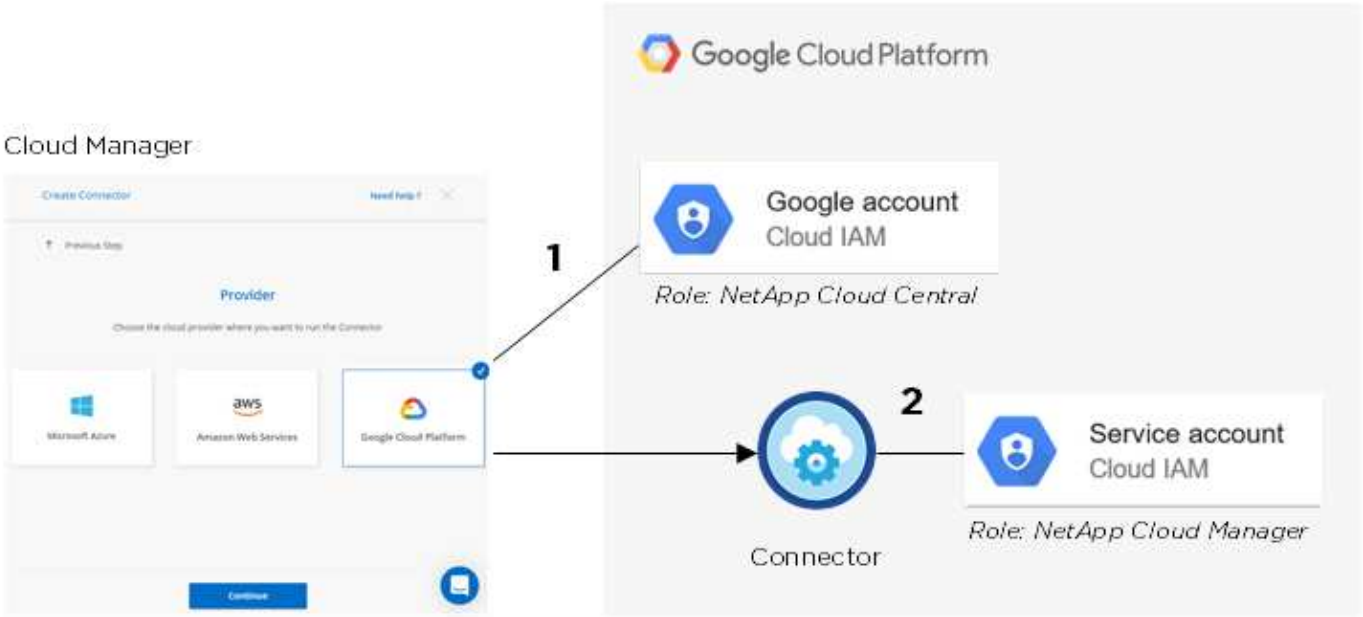
Google Cloud に Cloud Volumes ONTAP を導入する前に、まず Google Cloud プロジェクトに Connector を導入する必要があります。Connector は、オンプレミスでも別のクラウドプロバイダでも実行できません。

Cloud Manager からコネクタを直接導入するには、次の 2 組の権限が必要です。

1. Cloud Manager から Connector VM インスタンスを起動する権限がある Google アカウントを使用して Connector を導入する必要があります。
2. コネクタを配置するときに、を選択するよう求められます "サービスアカウント" VM インスタンスの場合です。Cloud Manager は、サービスアカウントから権限を取得して、 Cloud Volumes ONTAP システムを代わりに作成および管理します。権限は、サービスアカウントにカスタムロールを割り当てることによって提供されます。

ユーザとサービスアカウントに必要な権限を含む YAML ファイルを 2 つ設定しました。 "YAML ファイルを使用して設定する方法を学習します 権限"。

次の図は、上記の番号 1 と 2 で説明した権限の要件を示しています。



Project for Cloud Volumes ONTAP の略

Cloud Volumes ONTAP は、コネクタ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配置するには、まずコネクタサービスアカウントとその役割をそのプロジェクトに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について説明します"
- "GCP とで Cloud Volumes ONTAP を導入する方法について説明します プロジェクトを選択します"

Cloud Manager の GCP クレデンシャルとサブスクリプションの管理

Connector VM インスタンスに関連付けられているクレデンシャルを管理できます。

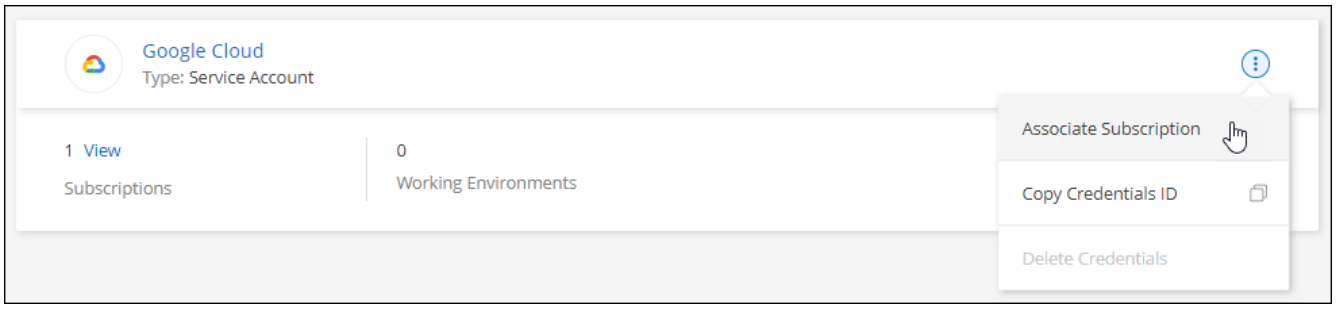
Marketplace サブスクリプションと GCP クレデンシャルの関連付け

GCP に Connector を導入すると、 Cloud Manager は Connector VM インスタンスに関連付けられたデフォルトのクレデンシャルセットを作成します。Cloud Manager で Cloud Volumes ONTAP の導入に使用するクレデンシャルを指定します。

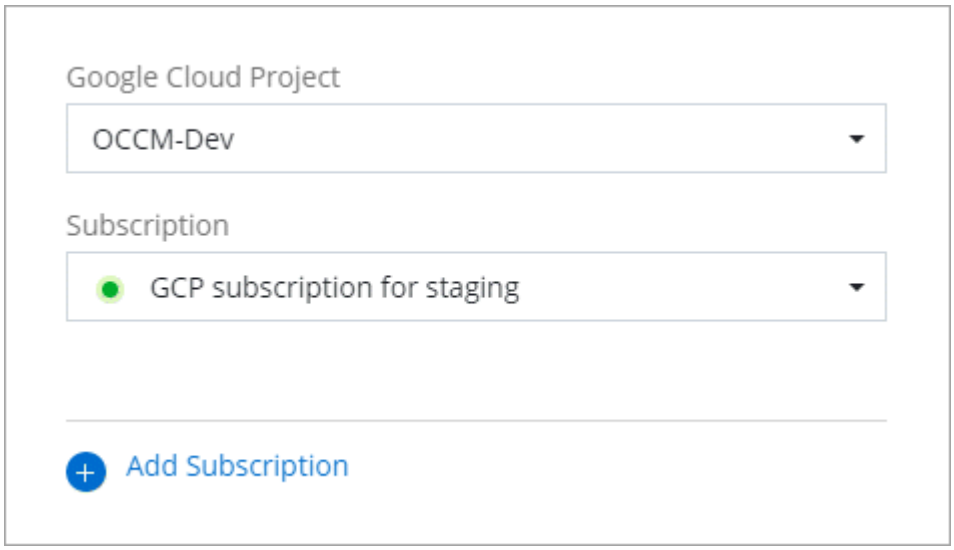
これらの資格情報に関連付けられている Marketplace サブスクリプションは、いつでも変更できます。サブスクリプションを使用すると、従量課金制の Cloud Volumes ONTAP システムを作成し、他のネットアップクラウドサービスを使用できます。

手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * クレデンシャル * を選択します。
2. 一連の資格情報のアクションメニューをクリックし、 * 契約の関連付け * を選択します。



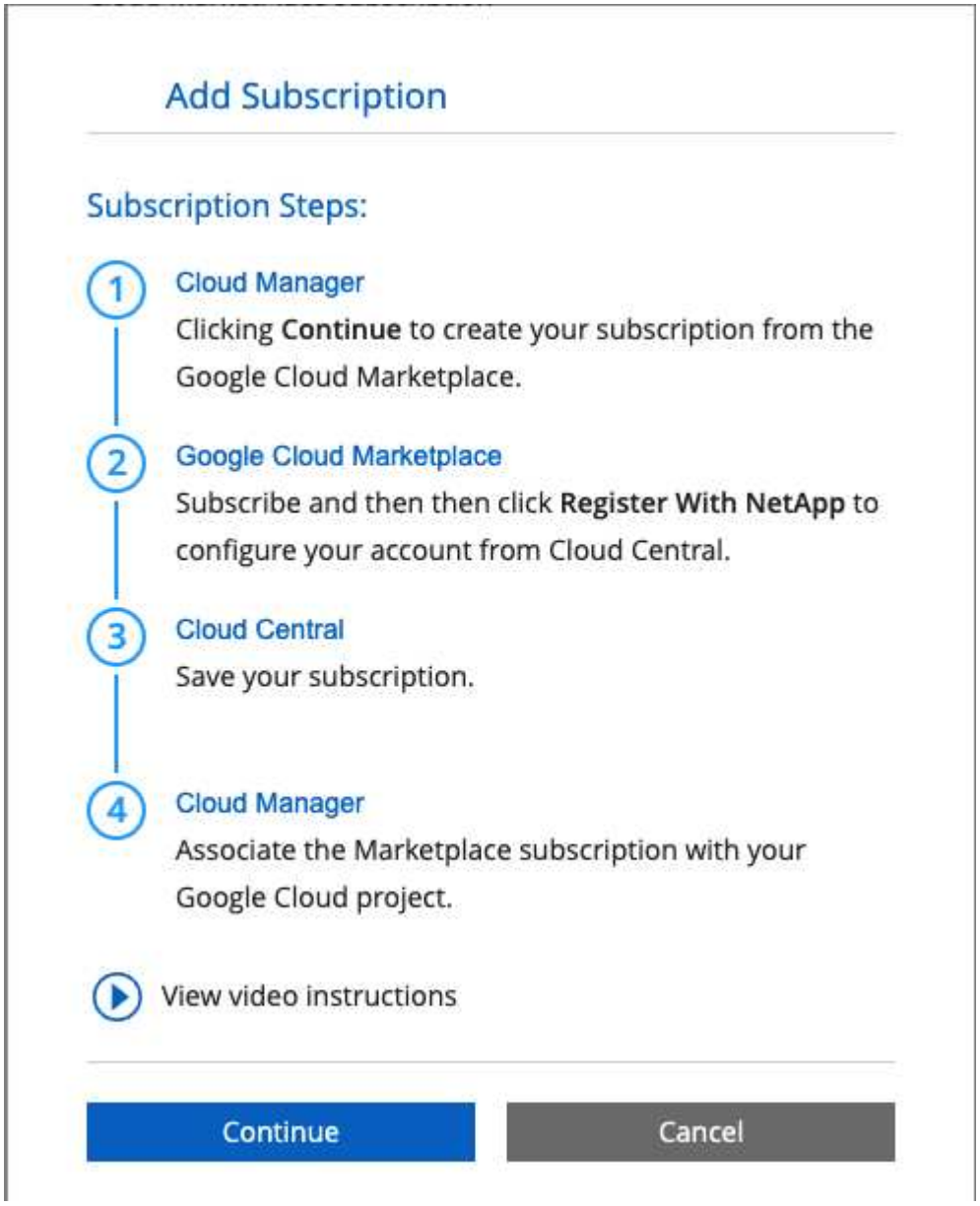
3. ダウンリストから Google Cloud プロジェクトとサブスクリプションを選択します。



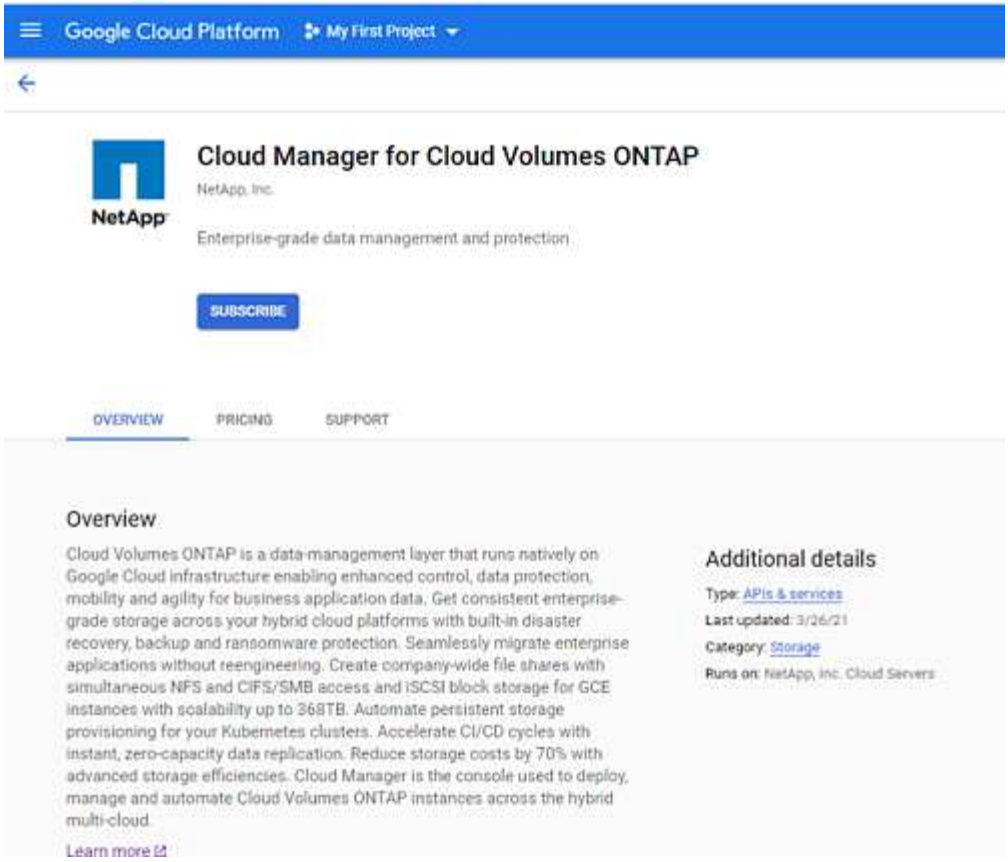
4. [関連付け（ Associate ）] をクリックします。
5. サブスクリプションをまだお持ちでない場合は、 [サブスクリプションの追加] をクリックし、以下の手順に従って新しいサブスクリプションを作成します。

次の手順を実行する前に、 Google Cloud アカウントと NetApp Cloud Central へのログインの両方に課金管理者権限があることを確認してください。

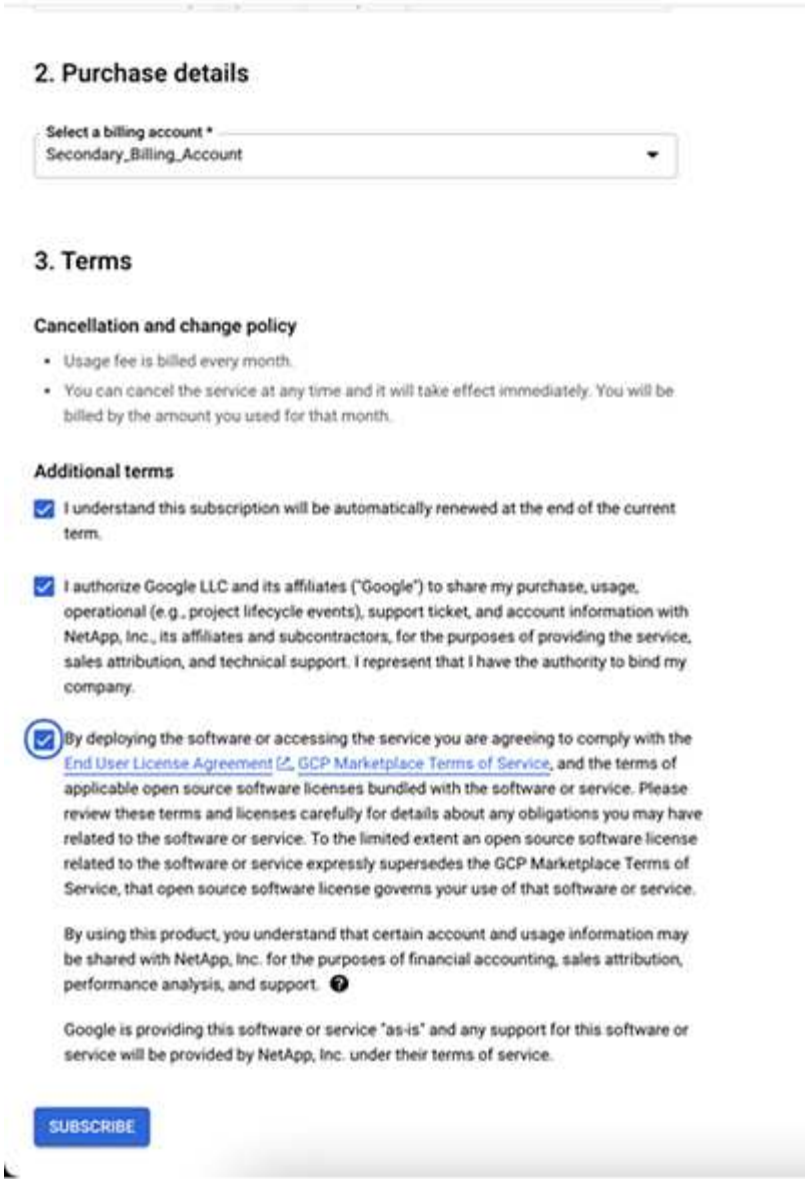
6. サブスクリプションの手順をもう一度表示し、 [* Continue （続行）] をクリックします。



7. にリダイレクトされたら "Google Cloud Marketplace の NetApp Cloud Manager のページ"をクリックし、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。



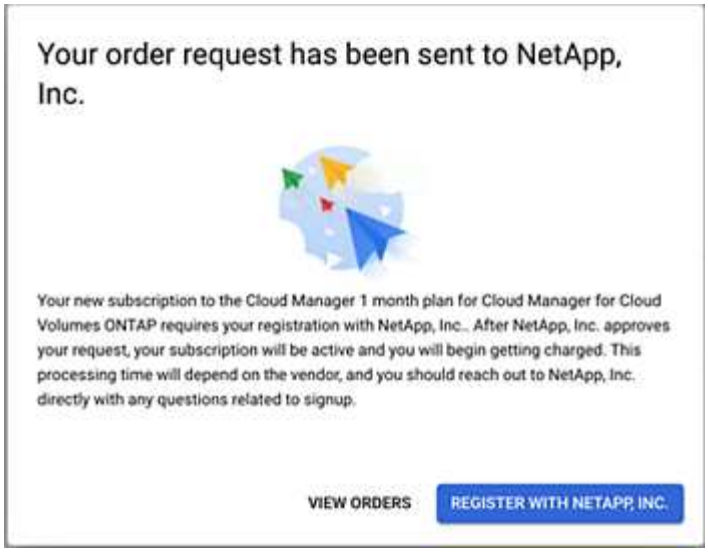
8. [**Subscribe**] をクリックします
9. 適切な請求先アカウントを選択し、条件に同意します。



10. [**Subscribe**] をクリックします

    転送要求がネットアップに送信されます。

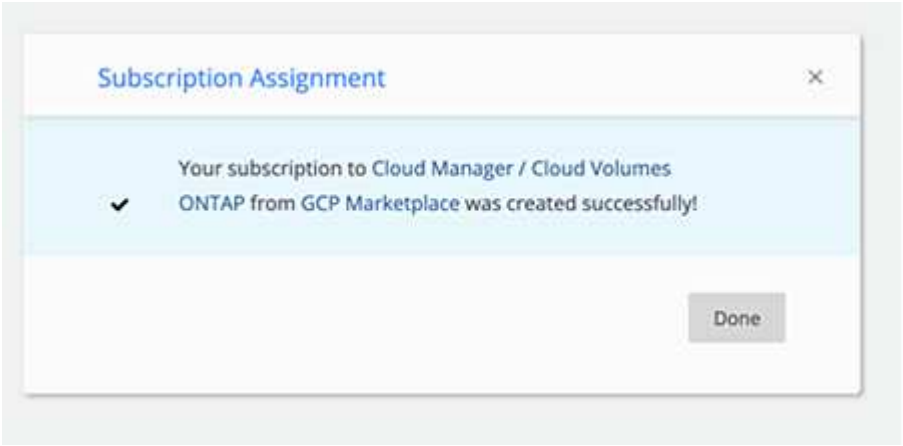
11. ポップアップダイアログボックスで、 NetApp Cloud Central にリダイレクトされる * Register with NetApp 、 Inc. * をクリックします。



GCP サブスクリプションをネットアップ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て NetApp Cloud Central 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ていません。

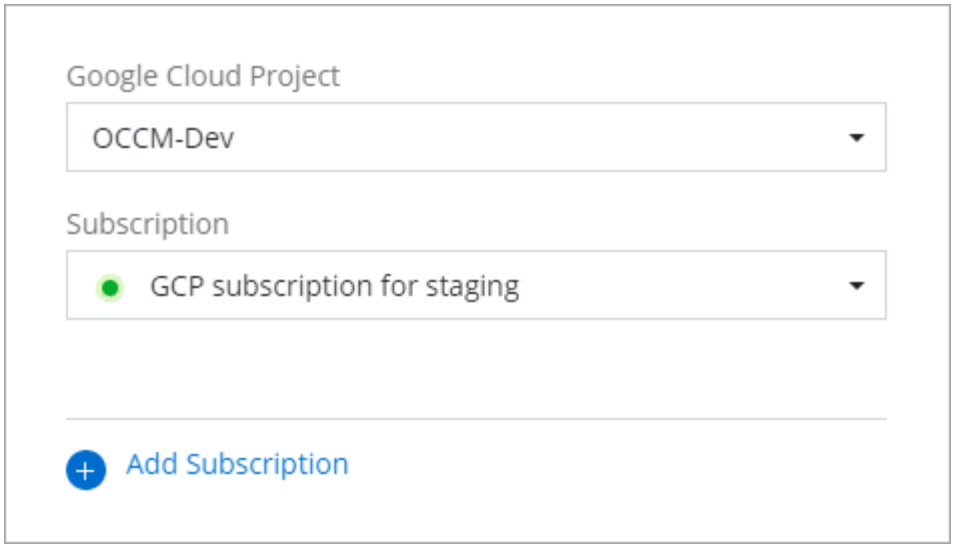
12. Cloud Central にリダイレクトされたら、 NetApp Cloud Central にログインするか、サインアップして * Done * をクリックして続行します。

    GCP サブスクリプションは、ユーザログインが関連付けられているすべてのネットアップアカウントにリンクされます。



組織のユーザが請求用アカウントから NetApp Cloud Manager サブスクリプションにすでに登録している場合は、にリダイレクトされます "NetApp Cloud Central の Cloud Volumes ONTAP ページ" 代わりに、予想外の場合は、ネットアップの営業チームにお問い合わせください。Google では、 1 つの Google 請求アカウントにつき 1 つのサブスクリプションのみが有効です。

13. このプロセスが完了したら、 Cloud Manager のクレデンシャルページに戻り、この新しいサブスクリプションを選択します。

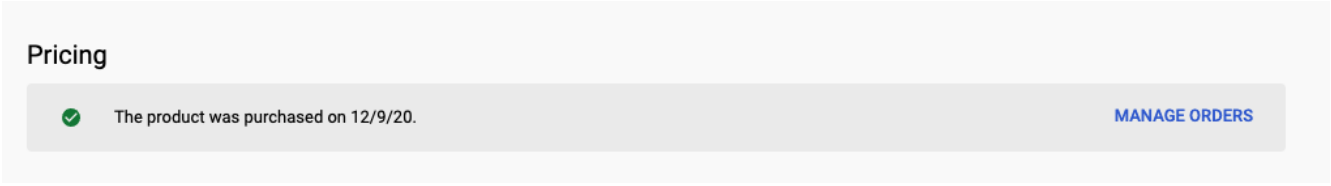


Marketplace サブスクリプションプロセスのトラブルシューティング

Google Cloud Marketplace から Cloud Volumes ONTAP にサブスクライブすると、権限が正しくないために断片化されたり、 NetApp Cloud Central へのリダイレクトに誤って追随したりしない場合があります。この場合は、次の手順に従ってサブスクリプションプロセスを完了してください。

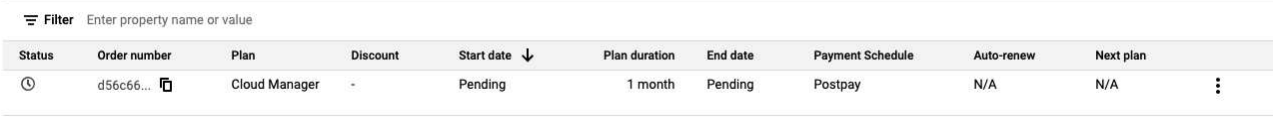
手順

1. に移動します "Google Cloud Marketplace の NetApp Cloud Manager のページ" 注文の状態を確認します。ページに「 * プロバイダで管理」と表示されている場合は、下にスクロールして「 * 注文の管理 * 」をクリックします。



   a. 注文に緑のチェックマークが表示されていて、これが予期しない場合は、同じ請求アカウントを使用している組織の他の人がすでに登録されている可能性があります。想定外のサポートやサブスクリプションの詳細が必要な場合は、ネットアップの営業チームにお問い合わせください。

   b. 注文に時計と * 保留中 * のステータスが表示されている場合は、マーケットプレイスのページに戻り、 * プロバイダで管理 * を選択して、上記の手順を完了します。



Cloud Manager でネットアップサポートサイトのアカウントを追加および管理します

ネットアップサポートサイト（ NSS ）アカウントのクレデンシャルを入力して、 Cloud Volumes ONTAP の主要なワークフローを有効にし、 Active IQ による予測分析とプロアクティブなサポートを有効にします。

概要

次のタスクを実行するには、 Cloud Manager にネットアップサポートサイトのアカウントを追加する必要があります。

- お客様所有のライセンスを使用（ BYOL ）した場合に Cloud Volumes ONTAP を導入するには

  Cloud Manager で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 アカウントを指定する必要があります。これには、期間の更新の自動更新も含まれます。

- 従量課金制の Cloud Volumes ONTAP システムを登録できます

  お使いのシステムのサポートを有効にし、ネットアップのテクニカルサポートリソースにアクセスするには、 NSS アカウントを用意する必要があります。

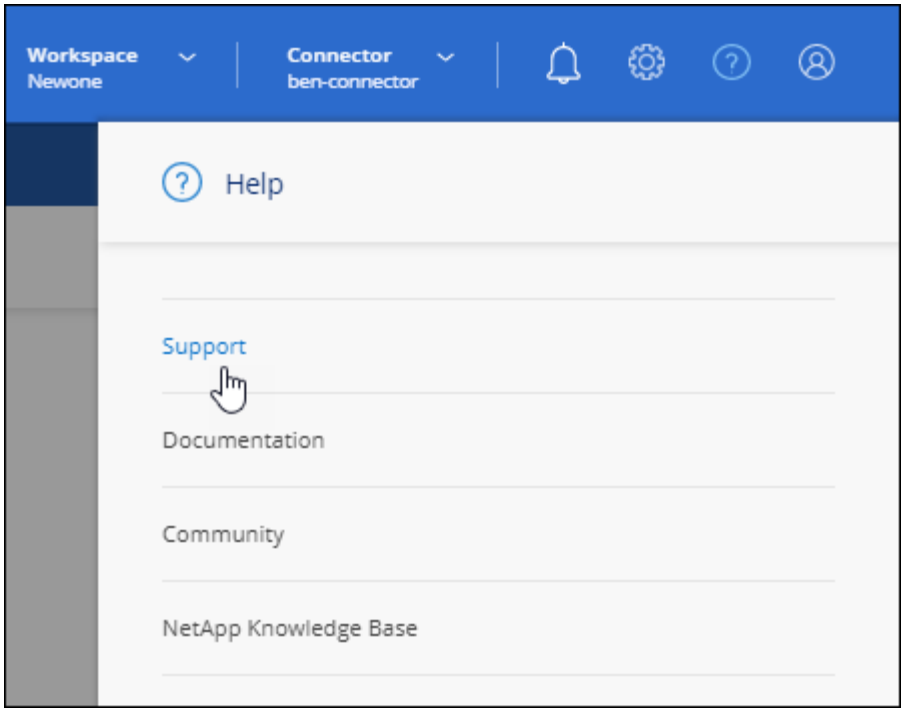
- をクリックして、 Cloud Volumes ONTAP ソフトウェアを最新リリースにアップグレードします
- から Active IQ デジタルアドバイザを使用します

NSS アカウントを追加します

サポートダッシュボードを使用すると、すべてのネットアップサポートサイトのアカウントを 1 箇所から追加および管理できます。

手順

1. ネットアップサポートサイトのアカウントがない場合は、 "1 名で登録します"。
2. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックし、 * Support * を選択します。



メニューのスクリーンショット。サポートは最初に表示されるオプションです"]

3. **[NSS Management] > [Add NSS Account]** をクリックします。
4. メッセージが表示されたら、 [* Continue （続行）] をクリックして Microsoft ログインページにリダイレクトします。

   ネットアップは、サポートとライセンスに固有の認証サービスのアイデンティティプロバイダとして Microsoft Azure Active Directory を使用しています。

5. ログインページで、ネットアップサポートサイトの登録 E メールアドレスとパスワードを入力して認証プロセスを実行します。

   Cloud Manager で NSS アカウントを使用することができます。

   アカウントに関する次の要件に注意してください。

   - お客様レベルのアカウントである必要があります（ゲストや一時アカウントは使用できません）。
   - ノードベースの BYOL システムを導入する場合は、次の点に注意してください。
     - BYOL システムのシリアル番号にアクセスする権限がアカウントに必要です。
     - セキュアな BYOL サブスクリプションを購入した場合は、セキュアな NSS アカウントが必要です。

新しい Cloud Volumes ONTAP システムの作成時、既存の Cloud Volumes ONTAP システムの登録時、および Active IQ でデータを表示するときに、アカウントを選択できるようになりました。

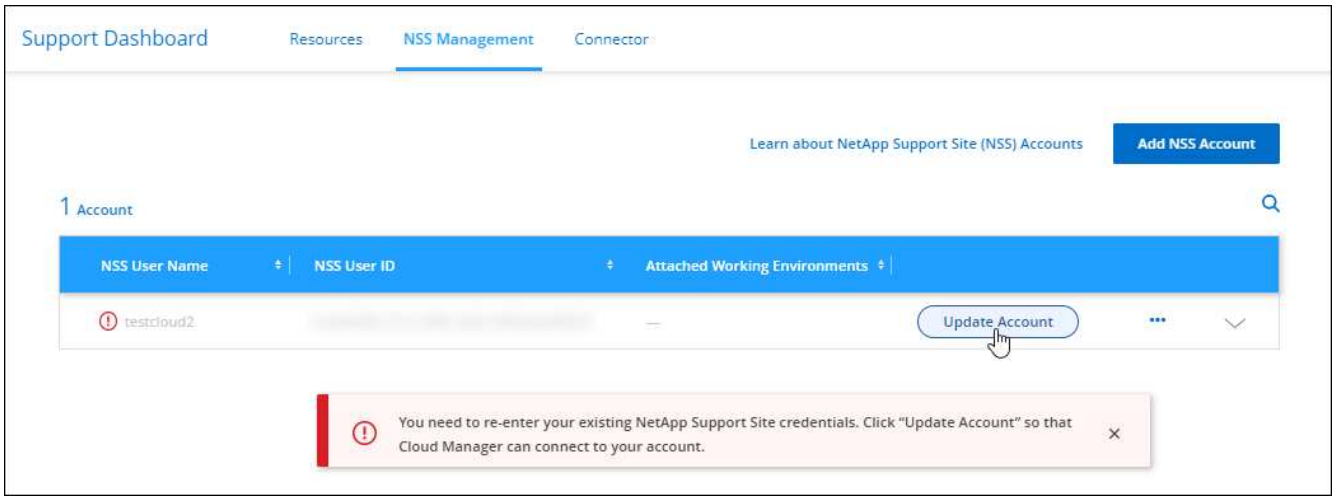
- "AWS での Cloud Volumes ONTAP の起動"
- "Azure で Cloud Volumes ONTAP を起動します"
- "GCP での Cloud Volumes ONTAP の起動"
- "従量課金制システムの登録"

NSS アカウントを更新して新しい認証方法を適用します

2021 年 11 月以降、ネットアップはサポートとライセンスに固有の認証サービスのアイデンティティプロバイダとして Microsoft Azure Active Directory を使用します。この更新によって、 Cloud Manager は、以前に追加した既存のアカウントのクレデンシャルの更新を求めます。

手順

1. まだ行っていない場合は、 "現在のネットアップアカウントにリンクする Microsoft Azure Active Directory B2C アカウントを作成します"。
2. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックし、 * Support * を選択します。
3. [*NSS 管理 *] をクリックします。
4. アップデートする NSS アカウントの場合は、 * アカウントの更新 * をクリックします。



5. メッセージが表示されたら、 [* Continue （続行）] をクリックして Microsoft ログインページにリダイレクトします。

   ネットアップは、サポートとライセンスに固有の認証サービスのアイデンティティプロバイダとして Microsoft Azure Active Directory を使用しています。

6. ログインページで、ネットアップサポートサイトの登録 E メールアドレスとパスワードを入力して認証プロセスを実行します。

   処理が完了したら、更新したアカウントが表に _new_account として表示されるようになります。古いバージョンのアカウントは ' 既存の作業環境の関連付けとともにテーブルに表示されます

7. 既存の Cloud Volumes ONTAP 作業環境が古いバージョンのアカウントに接続されている場合は、次の手順に従ってください それらの作業環境を別の NSS アカウントに接続します。
8. 古いバージョンの NSS アカウントに移動し、をクリックします ••• 次に、 * Delete * を選択します。

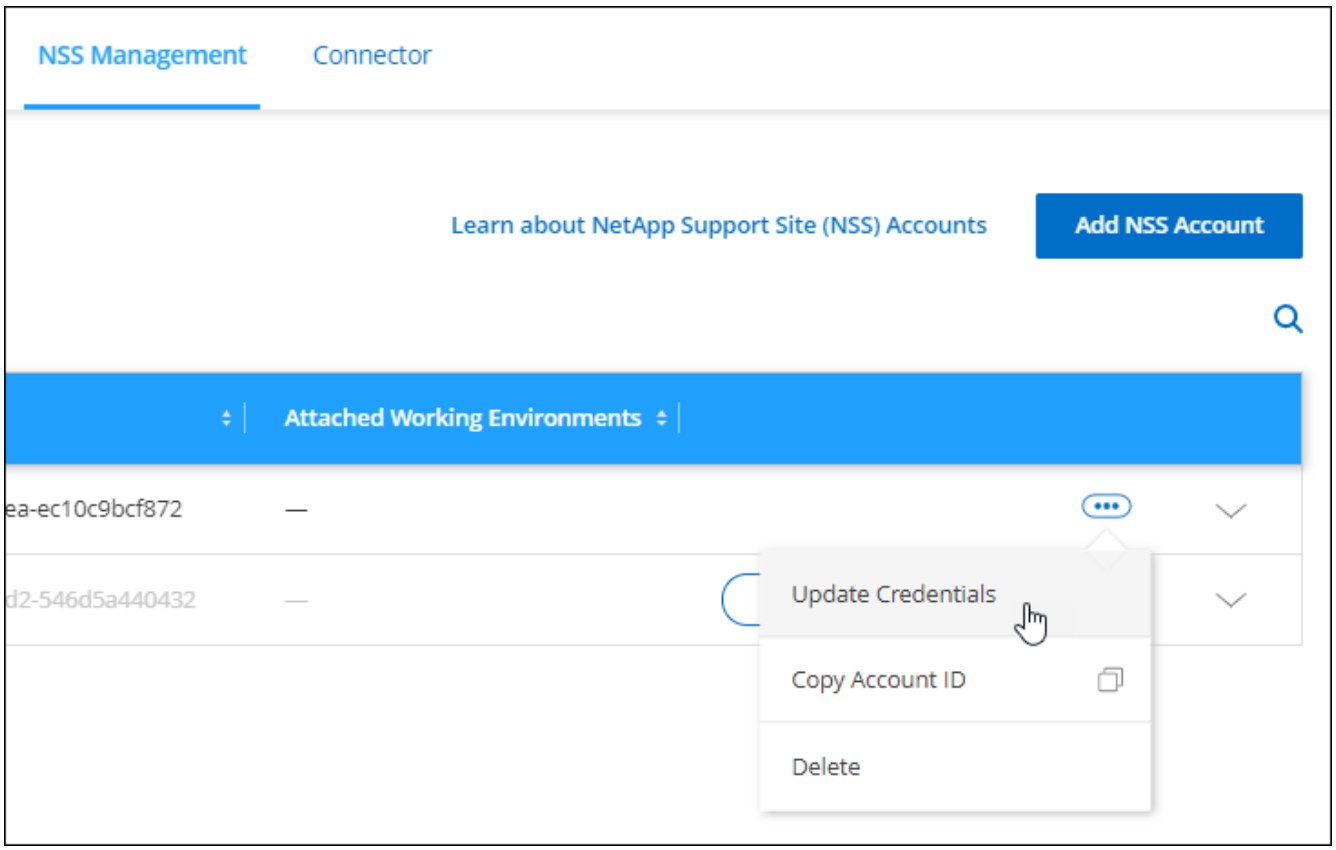
NSS クレデンシャルを更新します

NSS アカウントのクレデンシャルを変更するたびに、 Cloud Manager で更新する必要があります。

手順

1. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックし、 * Support * を選択します。

2. [*NSS 管理 *] をクリックします。
3. アップデートする NSS アカウントのをクリックします ••• 次に、 [資格情報の更新] を選択します。



4. メッセージが表示されたら、 [* Continue （続行）] をクリックして Microsoft ログインページにリダイレクトします。

   ネットアップは、サポートとライセンスに固有の認証サービスのアイデンティティプロバイダとして Microsoft Azure Active Directory を使用しています。

5. ログインページで、ネットアップサポートサイトの登録 E メールアドレスとパスワードを入力して認証プロセスを実行します。

作業環境を別の NSS アカウントに接続します

組織に複数のネットアップサポートサイトのアカウントがある場合、 Cloud Volumes ONTAP システムに関連付けられているアカウントを変更することができます。

この機能は、ネットアップがアイデンティティ管理に導入した Microsoft Azure AD を使用するように設定された NSS アカウントでのみサポートされます。この機能を使用する前に、「 * NSS アカウントを追加 * 」または「 * アカウントを更新 * 」をクリックする必要があります。

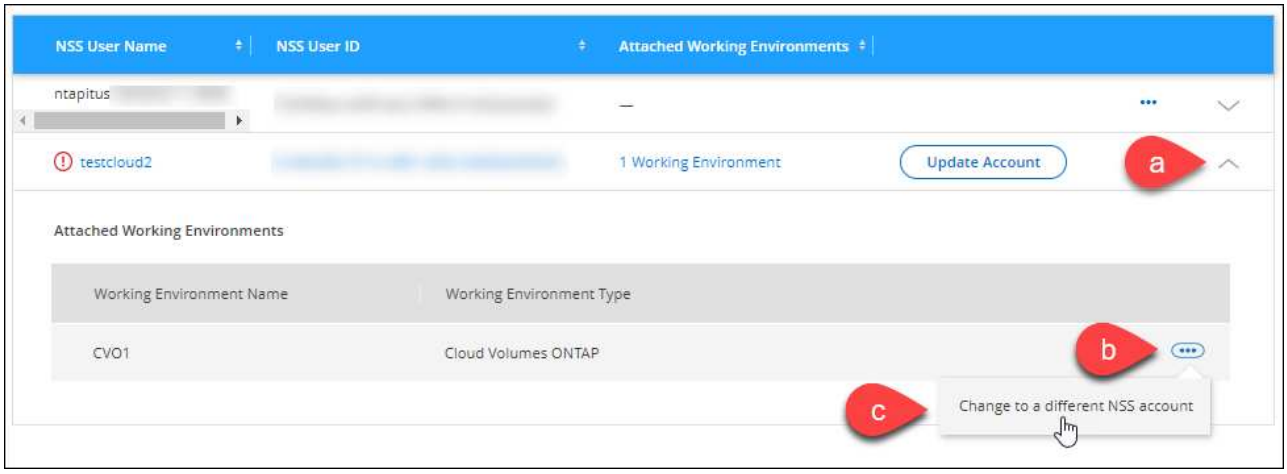
手順

1. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックし、 * Support * を選択します。
2. [*NSS 管理 *] をクリックします。
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. 作業環境が現在関連付けられているネットアップサポートサイトのアカウントの行を展開します。

b. 関連付けを変更する作業環境で、をクリックします ...

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 * をクリックします。

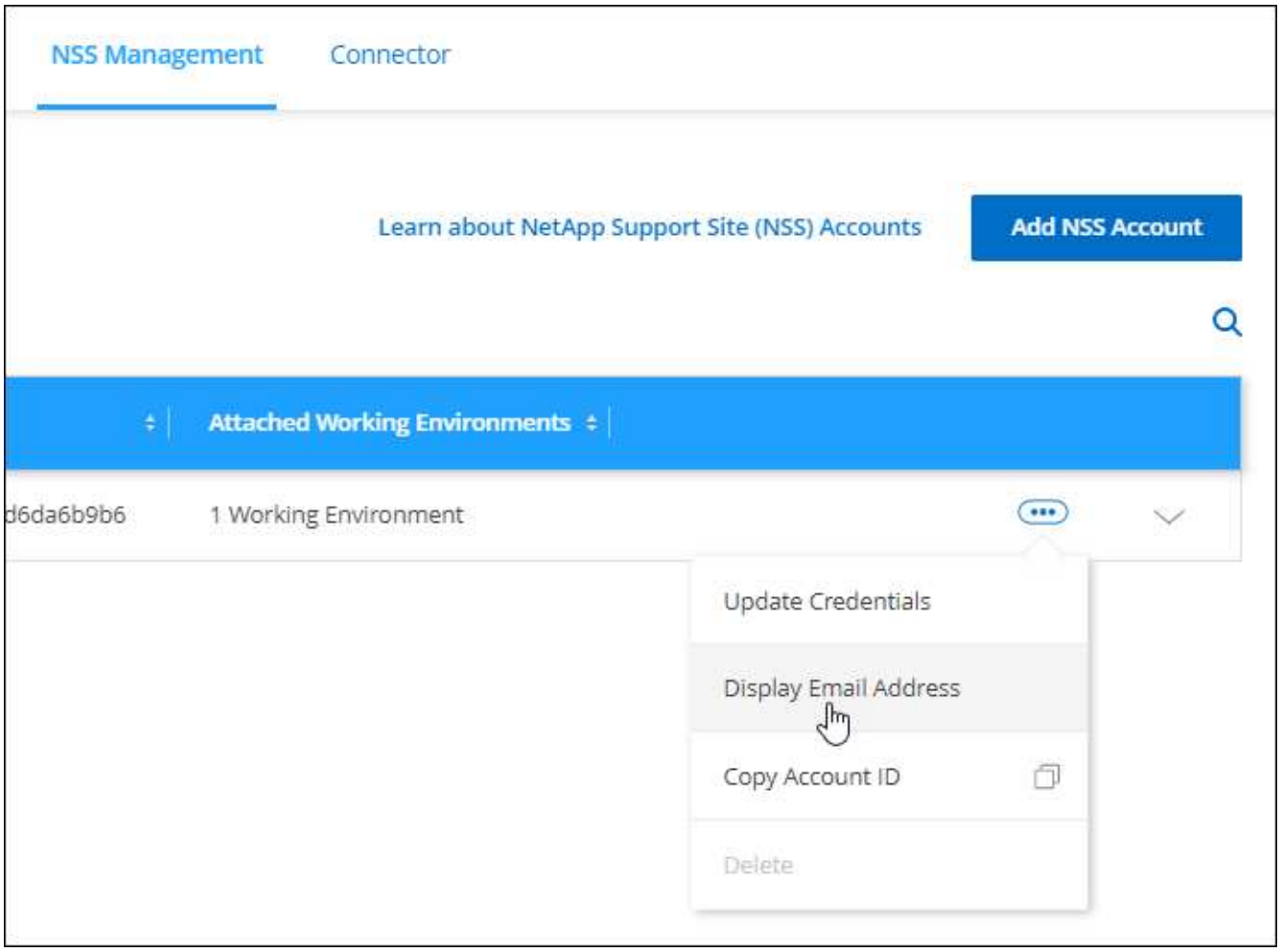
NSS アカウントの E メールアドレスを表示します

ネットアップサポートサイトのアカウントで認証サービスに Microsoft Azure Active Directory が使用されているため、 Cloud Manager に表示される NSS ユーザ名は通常、 Azure AD で生成された識別子です。そのため、そのアカウントに関連付けられている E メールアドレスがすぐにわからない場合があります。Cloud Manager には、関連付けられている E メールアドレスを表示するオプションがあります。

NSS の管理ページに移動すると、 Cloud Manager のテーブル内のアカウントごとにトークンが生成されます。このトークンには、関連付けられた E メールアドレスに関する情報が含まれます。その後、ページから移動するとトークンが削除されます。この情報はキャッシュされないため、プライバシーを保護できます。

手順

1. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックし、 * Support * を選択します。
2. [*NSS 管理 *] をクリックします。
3. アップデートする NSS アカウントのをクリックします ... 次に、 [電子メールアドレスの表示 *] を選択します。



Cloud Manager に、ネットアップサポートサイトのユーザ名と関連付けられている E メールアドレスが表示されます。コピーボタンを使用して、電子メールアドレスをコピーできます。

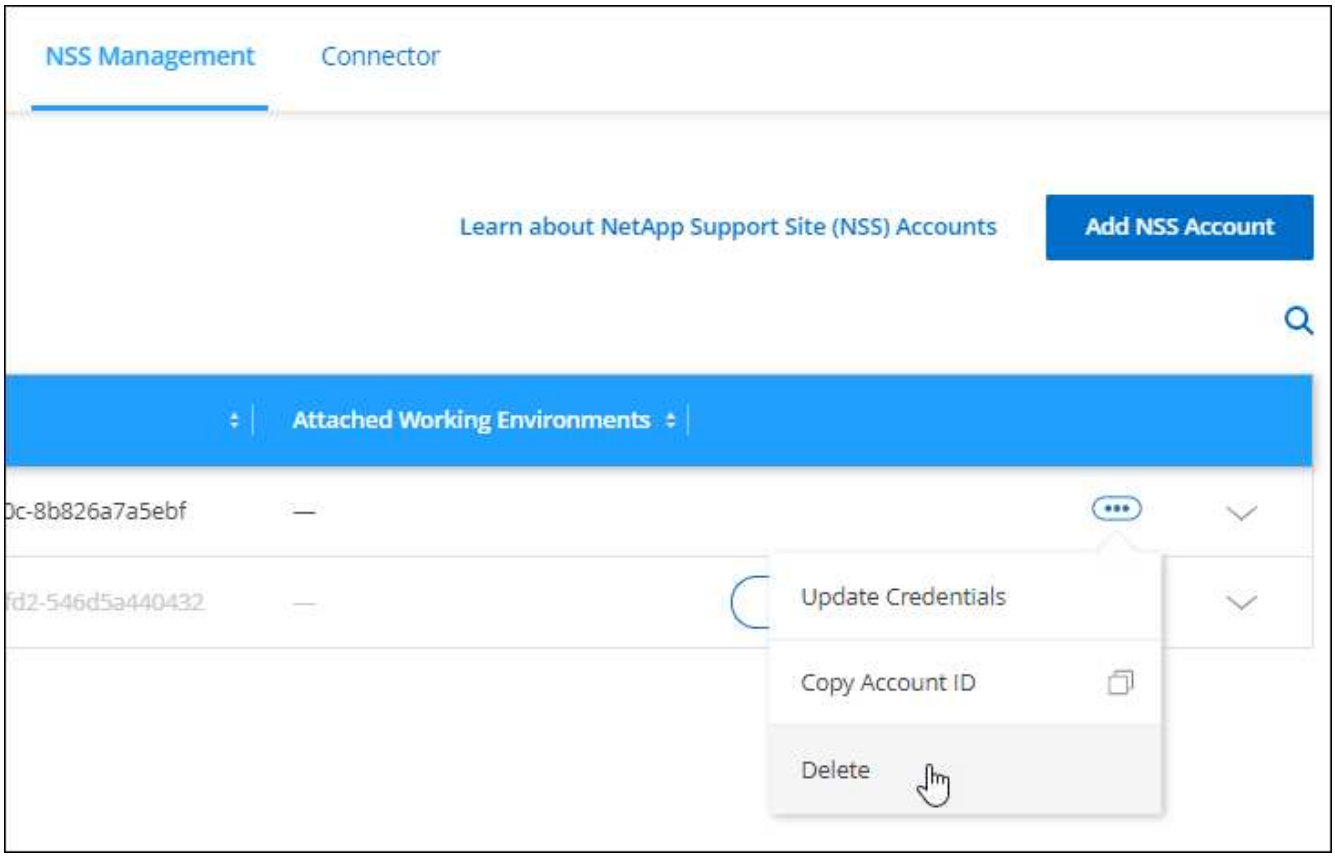
NSS アカウントを削除します

Cloud Manager で使用しない NSS アカウントを削除します。

Cloud Volumes ONTAP 作業環境に現在関連付けられているアカウントは削除できません。最初にが必要です それらの作業環境を別の NSS アカウントに接続します。

手順

1. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックし、 * Support * を選択します。
2. [*NSS 管理 *] をクリックします。
3. 削除する NSS アカウントのをクリックします ••• 次に、 * Delete * を選択します。



4. 削除を確定するには、 * 削除 * をクリックします。

参照

AWS でコネクタに必要な権限

Cloud Manager からクラウドプロバイダの処理を実行するには権限が必要です。これらの権限はに含まれています "ネットアップが提供するポリシー"。このような権限を持つ Cloud Manager の機能を理解しておく必要があるかもしれません。

Cloud Manager は AWS アカウントを使用して、 EC2 、 S3 、 CloudFormation 、 IAM 、 Security Token Service （ STS ）、 Key Management Service （ KMS ）などの複数の AWS サービスへの API コールを行います。

アクション	目的
"EC2:StartInstances" 、 "EC2:StopInstances" 、 "EC2:DescribeInstances" 、 "EC2:DescribeInstanceStatus" 、 "EC2:RunInstances" 、 "EC2:TerminateInstances" 、 "EC2:ModifyInstanceAttribute" 、	Cloud Volumes ONTAP インスタンスを起動し、インスタンスを停止、開始、監視します。
"EC2: DescribeInstanceAttribute" 、	サポートされているインスタンスタイプで Enhanced Networking が有効になっていることを確認します。
「 EC2 ：説明文」、「 EC2 ：説明文」、	Cloud Volumes ONTAP HA 構成を起動します。
EC2 ： createTags 、	Cloud Manager が作成するすべてのリソースに「 workingEnvironment 」タグと「 workingEnvironmId 」タグを付けます。Cloud Manager では、これらのタグを使用してメンテナンスとコスト割り当てを行います。
"EC2:CreateVolume" 、 "EC2:DescribeVolumes" 、 "EC2:ModifyVolumeAttribute" 、 "EC2:AttachVolume" 、 "EC2:DeleteVolume" 、 "EC2:DetachVolume" 、	Cloud Volumes ONTAP がバックエンドストレージとして使用する EBS ボリュームを管理します。
"EC2:CreateSecurityGroup" 、 "EC2:DeleteSecurityGroup" 、 "EC2:RevokeSecurityGroupEgress " 、 "EC2:AuthorizeSecurityGroupEgress " 、 "EC2:RevokeSecurityGroupIngress " 、 "EC2:RevokeSecurityGroupIngress " 、	Cloud Volumes ONTAP 用の定義済みセキュリティグループを作成します。
"EC2:CreateNetworkInterface", "EC2:DescribeNetworkInterfaces ", "EC2:DeleteNetworkInterface", "EC2:ModifyNetworkInterfaceAttribute",	ターゲットサブネット内の Cloud Volumes ONTAP のネットワークインターフェイスを作成および管理します。
「 EC2 ：説明サブネット」、「 EC2 ：説明 VPC 」、	Cloud Volumes ONTAP 用の新しい作業環境を作成するときに必要な、デスティネーションサブネットとセキュリティグループのリストを取得します。
EC2 ： DescribeDHCPOptions	Cloud Volumes ONTAP インスタンスの起動時に DNS サーバとデフォルトのドメイン名を決定します。

アクション	目的
「 EC2 ： CreateSnapshot 」、「 EC2 ： DeleteSnapshot 」、「 EC2 ： DescribeSnapshot 」、	初期セットアップ時、および Cloud Volumes ONTAP インスタンスが停止したときに、 EBS ボリュームのスナップショットを作成します。
"EC2:GetConsoleOutput" 、	AutoSupport メッセージに添付された Cloud Volumes ONTAP コンソールをキャプチャします。
「 EC2 ：説明キーペア」、	インスタンスの起動時に使用可能なキーペアのリストを取得します。
「 EC2 ：説明論」、	使用可能な AWS リージョンのリストを取得します。
EC2 ： DeleteTags 、 EC2 ： DescribeTags 、	Cloud Volumes ONTAP インスタンスに関連付けられたリソースのタグを管理します。
CloudFormation ： CreateStack 」、「 CloudFormation ： DeleteStack 」、「 CloudFormation ： DescribeStack 」、「 CloudFormation ： DescribeStackEvents 」、「 CloudFormation ： ValidateTemplate 」、	Cloud Volumes ONTAP インスタンスを起動します。
"iam ： PassRole" 、 "iam ： CREATEROLE" 、 "iam ： PutRolePolicy " 、 "iam ： CreateInstanceProfile" 、 "iam ： DeleteRolePolicy " 、 "iam ： AddRoleToInstanceProfile" 、 "IAM ： RemoveRoleInstanceFromProfile" 、 "iam ： DeleteInstanceProfile" 、 "iam ： DeleteInstanceProfile	Cloud Volumes ONTAP HA 構成を起動します。
"IAM:ListInstanceProfiles" 、 "STS: DecodeAuthorizationMessage" 、 "EC2:AssociateIamInstanceProfile" 、 "EC2:DescribeIamInstanceProfileAssociations" 、 "EC2:DisassociateIamInstanceProfileProfile" 、	Cloud Volumes ONTAP インスタンスのインスタンスプロファイルを管理します。
「 s3 ： GetBucketTagging 」、「 s3 ： GetBucketLocation 」、「 s3 ： ListAllMyBuckets 」、「 s3 ： ListBucket 」	AWS S3 バケットに関する情報を取得して、 Cloud Manager を NetApp Data Fabric Cloud Sync サービスと統合できるようにします。
s3 ： CreateBucket 、 s3 ： DeleteBucket 、 s3 ： GetLifecycleConfiguration 、 s3 ： PutBucketTagging 、 s3 ： ListBucketVersions 、 s3 ： GetBucketPolicyStatus 、 s3 ： GetBucketPublicAccessBlock 、 s3 ： GetBucketAccessBlock 、 GetBucketAccessBlock	Cloud Volumes ONTAP システムでデータ階層として使用する S3 バケットを管理します。
"kms ：リスト * " 、 "kms ：再暗号化 * " 、 "kms ： DESCRIBE * " 、 "kms ： CreateGrant" 、	AWS Key Management Service （ KMS ；キー管理サービス）を使用した Cloud Volumes ONTAP のデータ暗号化を有効にします。
"CE:GetReservationUtilization" 、 "CE:GetDimensionValues" 、 "CE:GetCostAndUsage", "CE:GetTags"	Cloud Volumes ONTAP の AWS コストデータを取得します。

アクション	目的
"EC2:CreatePlacementGroup" 、 "EC2:DeletePlacementGroup"	単一の AWS アベイラビリティゾーンに HA 構成を導入すると、 Cloud Manager は 2 つの HA ノードと AWS 分散配置グループ内のメディエーターを起動します。
EC2: DescribeReservedInstancesOffers (英語)	Cloud Manager は、 Cloud Data Sense の導入の一環としてこの権限を使用して、使用するインスタンスタイプを選択します。
"EC2:CreateTags" 、 "EC2:DeleteTags" 、 "EC2:DescribeTags" 、 "tag:getResources" 、 "tag:getTagKeys" 、 "tag:getTagValues", "tag:TagResources", "tag:UntagResources"	Cloud Manager Tagging サービスを使用して、 AWS リソースのタグを管理できます。
「 s3 ： DeleteBucket 」、「 s3 ： GetLifecycleConfiguration 」、「 s3 ： PutBucketLifeConfiguration 」、「 s3 ： PutBucketTagging 」、「 s3 ： ListBucketVersions 」、「 s3 ： ListBucket 」、「 s3 ： ListAllMyBuckets 」、「 s3 ： GetBucketAccessBuckets3 ： GetBucketAccessBuckets3 、 GetBucketAccessBuckets3 ： GetBucketAccessBlock	Cloud Manager では、 S3 へのバックアップサービスを有効にする際にこれらの権限を使用します。
"EKS ： ListClusters" 、 "EKS ： DescribeCluster" 、 "IAM ： GetInstanceProfile"	Amazon EKS クラスタの検出を有効にします。

Azure の Connector に必要な権限

Cloud Manager からクラウドプロバイダの処理を実行するには権限が必要です。これらの権限はに含まれています "ネットアップが提供するポリシー"。このような権限を持つ Cloud Manager の機能を理解しておく必要があるかもしれません。

Cloud Manager Azure ポリシーには、 Cloud Manager が Azure で Cloud Volumes ONTAP を導入および管理するために必要な権限が含まれています。

アクション	目的
「 Microsoft.Compute/locations/operations/read" 」、「 Microsoft.Compute/locations/vmSizes/read" 」、「 Microsoft.Compute/operations/read" 」、「 Microsoft.Compute/virtualMachines/instanceView/read " 」、「 Microsoft.Compute/virtualMachines/powerOff/action" 」、「 Microsoft.Compute/virtualMachines/read" 」、「 Microsoft.Compute/virtualMachines/restart/action" 」、「 Microsoft.Compute/virtualMachines/start/action" 」、「 Microsoft.Compute/virtualMachines/deallocate/action" 」、「 Microsoft.Compute/virtualMachines/vmSizes/read" 」、「 Microsoft.Compute/virtualMachines/write" 」、	Cloud Volumes ONTAP を作成し、システムのステータスを停止、開始、削除、取得します。
「 microsoft.compute/images/write 」、「 microsoft.compute/images/read 」、	VHD から Cloud Volumes ONTAP を導入できます。
Microsoft.Compute/disks/delete" 、 Microsoft.Compute/disks/read" 、 Microsoft.Compute/disks/write" 、 "Microsoft.Storage/checknameavailability/read" 、 "Microsoft.Storage/operations/read" 、 "microsoft.StorageAccounts/listkeyss/action" 、 "microsoft.Storage/storageAccounts/read" 、 "microsoft.Storage/regenerateAccounts/action" 、 "Microsoft.Storage/storageAccounts/action" 、 "/writeStorageAccounts" 、 "/StorageAccounts/StorageAccounts/write/StorageAccounts" 、 ","Microsoft 。	Azure ストレージアカウントとディスクを管理し、ディスクを Cloud Volumes ONTAP に接続します。
"microsoft.StorageAccounts/blobServices/containers/read" 、 "microsoft.KeyVault/vaults/read" 、 "microsoft.KeyVault/vaults/accessPolicies/write"	Azure BLOB ストレージへのバックアップとストレージアカウントの暗号化を有効にします
「 microsoft.network/networkinterfaces/read 」、「 microsoft.network/networkinterfaces/write 」、「 microsoft.network/networkinterfaces/join/action 」、	ターゲットサブネット内の Cloud Volumes ONTAP のネットワークインターフェイスを作成および管理します。
「 microsoft.network/networksecuritygroups/read 」、「 microsoft.network/networksecuritygroups/write 」、「 microsoft.network/networksecuritygroups/join/action 」、	Cloud Volumes ONTAP 用の定義済みネットワークセキュリティグループを作成します。

アクション	目的
「 microsoft.Resources/Subscriptions /locations /read 」、「 Microsoft.Network/locations/operationResults/read" 」、「 Microsoft.Network/locations/operations/read" 」、「 Microsoft.Network/virtualNetworks/read" 」、「 Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read" 」、「 Microsoft.Network/virtualNetworks/subnets/read" 」、「 Microsoft.Network/virtualNetworks/subnets/virtualMachines/read" 」、「 Microsoft.Network/virtualNetworks/virtualMachines/read" 」、「 Microsoft.Network/virtualNetworks/subnets/join/action" 」、	リージョン、ターゲット VNet 、およびサブネットに関するネットワーク情報を取得し、 vnet に Cloud Volumes ONTAP を追加します。
「 Microsoft.Network/virtualNetworks/subnets/write" 」、 Microsoft.Network/routeTables/join/action" 、	データ階層化のための VNet サービスエンドポイントを有効にします。
「 Microsoft.Resources/Deployments/Operations/Read 」、「 Microsoft.Resources/Deployments/Read 」、「 Microsoft.Resources/Deployments/Write 」、	テンプレートから Cloud Volumes ONTAP を導入します。
"microsoft.Resources/Deployments/operations/read" 、 "microsoft.Resources/Deployments/read" 、 "microsoft.Resources/resources/read" 、 "microsoft.resources/resources/operationresults/read" 、 "microsoft.resources/Subscriptions /resourceGroups/delete" 、 "microsoft.resources/Subscriptions /resources/groups/resources/resources/reads/resources/resources/resources/resources/resources/resources/resources/reading" 、 ","","","resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/groups/	Cloud Volumes ONTAP のリソースグループを作成および管理します。
「 Microsoft.Compute/snapshots/write" 」、「 Microsoft.Compute/snapshots/read" 」、「 Microsoft.Compute/snapshots/delete" 」、「 Microsoft.Compute/disks/beginGetAccess/action" 」、	Azure マネージドスナップショットを作成および管理します。
"microsoft.compute/availabilitySets/write", "microsoft.compute/availabilitySets/read",	Cloud Volumes ONTAP の可用性セットを作成および管理します。
"Microsoft.MarketplaceOrdering/Offered Types/publishers/capers/plans/agreements/read" 、 "Microsoft.MarketplaceOrdering / offerTypes/publishers/capes/plans/agreements/write"	Azure Marketplace からのプログラムによる展開を可能にします。

アクション	目的
「 Microsoft.Network/loadBalancers/read" 」、「 Microsoft.Network/loadBalancers/write" 」、「 Microsoft.Network/loadBalancers/delete" 」、「 Microsoft.Network/loadBalancers/backendAddressPools/read" 」、「 Microsoft.Network/loadBalancers/backendAddressPools/join/action" 」、「 Microsoft.Network/loadBalancers/frontendIPConfigurations/read" 」、「 Microsoft.Network/loadBalancers/loadBalancingRules/read" 」、「 Microsoft.Network/loadBalancers/probes/read" 」、「 Microsoft.Network/loadBalancers/probes/join/action" 」	HA ペアの Azure ロードバランサを管理します。
"Microsoft 許可 / ロック /*"	Azure ディスクのロックの管理を有効にします。
"Microsoft.Authorization/roleDefinites/write" 、 "Microsoft.Authorization/rolrolわり あて /write" 、 "Microsoft.Web/sites/*"	HA ペアのフェイルオーバーを管理します。
「 Microsoft.Network/privateEndpoints/write" 」、「 Microsoft.StorageAccounts/PrivateEndpointConnectionsApproval/action 」、「 microsoft.Storage/storageAccounts/privateEndpointConnections/read 」、「 Microsoft.Network/privateEndpoints/read" 」、「 Microsoft.Network/privateDnsZones/write" 」、「 Microsoft.Network/privateDnsZones/virtualNetworkLinks/write" 」、「 Microsoft.Network/privateDnsZones/A/write" 」、「 Microsoft.Network/privateDnsZones/virtualNetworkLinks/read" 」、「 Microsoft.Network/privateDnsZones/read" 」、「 Microsoft.Network/virtualNetworks/join/action" 」、「 」、「 」、「 」	プライベートエンドポイントの管理をイネーブルにします。プライベートエンドポイントは、サブネットの外部への接続が提供されない場合に使用されます。Cloud Manager は、サブネット内で内部接続のみを使用して HA 用のストレージアカウントを作成します。
" Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete" 、	Azure NetApp Files のボリュームを Cloud Manager で削除できます。
"microsoft.Resources/Deployments/operationStatuses/read"	Azure では、一部の仮想マシン環境に対してこの権限が必要です（導入時に使用する基盤となる物理ハードウェアによって異なります）。

アクション	目的
"microsoft.Resources/Deployments/operationStatuses/read" 、 "microsoft.Insights / Metrics / Read" 、 "Microsoft.Compute/virtualMachines/extensions/write" 、 "Microsoft.Compute/virtualMachines/extensions/read" 、 "Microsoft.Compute/virtualMachines/extensions/delete" 、 "Microsoft.Compute/virtualMachines/delete" 、 "Microsoft.Network/networkInterfaces/delete" 、 "Microsoft.Network/networkSecurityGroups/delete" 、 "Microsoft.Resources/Deployments/delete" 、	グローバルファイルキャッシュを使用できます。
「 Microsoft.Network/privateEndpoints/delete" 」、 Microsoft.Compute/availabilitySets/delete" 、	導入の失敗や削除が発生した場合に、 Cloud Manager が Cloud Volumes ONTAP に属するリソースグループからリソースを削除できるようにします。
「 Microsoft.Compute/diskEncryptionSets/read" 」 Microsoft.Compute/diskEncryptionSets/write" 、 「 Microsoft.Compute/diskEncryptionSets/delete" 」 「 microsoft.KeyVaults/vaults/deploy/action 」、 「 microsoft.KeyVault/vaults/read 」、 「 microsoft.KeyVaults/accessPolicies/write 」、	Cloud Volumes ONTAP で、お客様が管理する暗号化キーの使用を有効にします。この機能は API を使用してサポートされます。
"microsoft.Resources/tags/read" 、 "microsoft.Resources/tags/write" 、 "microsoft.Resources/tags/delete"	Cloud Manager Tagging サービスを使用して、 Azure リソースのタグを管理できます。
「 Microsoft.Network/applicationSecurityGroups/write" 」、 「 Microsoft.Network/applicationSecurityGroups/read" 」、 「 Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action" 」、 「 Microsoft.Network/networkSecurityGroups/securityRules/write" 」、 「 Microsoft.Network/applicationSecurityGroups/delete" 」、 「 Microsoft.Network/networkSecurityGroups/securityRules/delete"	Cloud Manager で HA ペアのアプリケーションセキュリティグループを設定できるため、 HA インターコネクトとクラスタネットワークの NIC が分離されます。

Google Cloud の Connector に必要な権限です

Cloud Manager からクラウドプロバイダの処理を実行するには権限が必要です。これらの権限はに含まれています "ネットアップが提供するポリシー"。このような権限を持つ Cloud Manager の機能を理解しておく必要があるかもしれません。

GCP の Cloud Manager ポリシーには、 Cloud Volumes ONTAP の導入と管理に Cloud Manager が必要とする権限が含まれています。

アクション	目的
-compute.disks .create -computedisks .createsnapshot - compute.disks.delete -computedisks .get-compute.diskList - compute.disks.setLabels - compute.disks.us	Cloud Volumes ONTAP 用のディスクを作成および管理します。
-compute-firewalls .create - compute.firewalls.delete -comput領域 .firewalls .get-comput領域 .firewalls リスト	Cloud Volumes ONTAP のファイアウォールルールを作成します。
-computer.globalOperationsGet	処理のステータスを確認できます。
-compute.image.get-compute.image.getFromFamily -compute.image.list - compute.images.useReadOnly	VM インスタンスのイメージを取得します。
- compute.instances.attachDisk - compute.instances.detachDisk	ディスクを Cloud Volumes ONTAP に接続して接続解除します。
- compute.instances.create - compute.instances.delete	Cloud Volumes ONTAP VM インスタンスを作成および削除します。
- compute.instances.get	VM インスタンスを一覧表示します。
- compute.instances.getSerialPortOutput	をクリックしてコンソールログを取得してください
- compute.instances.list	ゾーン内のインスタンスのリストを取得します。
- compute.instances.setDeletionProtection	インスタンスに削除保護を設定します。
- compute.instances.setLabels	ラベルを追加します。
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	Cloud Volumes ONTAP のマシンタイプを変更します。
- compute.instances.setMetadata	をクリックしてください。
- compute.instances.setTags	ファイアウォールルールのタグを追加します。
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Cloud Volumes ONTAP を開始および停止します。
-computesCompute .machineTypes.get	コア数を取得して qoutas をチェックしてください。
- compute.projects.get	複数のプロジェクトをサポートするため。
-compute-snapshots-create - compute.snapshots.delete -compute-snapshots -getCompute-snapshots-list - compute.snapshots.setLabels	永続ディスクスナップショットを作成および管理するには、次の手順に従います。
- compute.networks.get - compute.networks.list - comput.regions.Get-comput領域 .list-comput領域 .subnetworks -compute.subnetworks .listCompute.zoneOperations-get-compute.zones .get-compute.zones リスト	新しい Cloud Volumes ONTAP 仮想マシンインスタンスの作成に必要なネットワーク情報を取得するため。

アクション	目的
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list -deploymentmanager. マニフェスト .get-deploymentmanager. マニフェスト .list-list-deploymentmanager. operations-get-deploymentmanager. operationlist -deploymentmanager. resources.get-deploymentmanager. resources.list-deploymentmanager. typeProviders.get-deploymentmanager. typeProviders.list-deploymentmanager. -deploymentmanager. types] リスト	Google Cloud Deployment Manager を使用して Cloud Volumes ONTAP 仮想マシンインスタンスを導入します。
-logging.logEntries.list-logging.privateLogEntries.list	スタックログドライブを取得する方法
- resourcemanager.projects.get	複数のプロジェクトをサポートするため。
-storagバケット 。 create - storage.buckets.delete -storagバケット .get-storagバケット .list-storagバケット .buckets-update	Google Cloud Storage バケットを作成して管理し、データを階層化します。
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms .cryptoKeys.get-cloudkms .cryptoKeys.list-cloudkm.keyringlist.list	Cloud Volumes ONTAP でクラウドキー管理サービスからお客様が管理する暗号化キーを使用するため。
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - storage.objects-get -storage.objectlist	Cloud Volumes ONTAP インスタンスにサービスアカウントを設定します。このサービスアカウントは、Google Cloud Storage バケットへのデータ階層化の権限を提供します。
-compute.address.listCompute.backendServices. create -compute.networks.updatePolicy -compute.regionBackendServices.create -compute.regionBackendServices.get -compute.regionBackendServices.list	をクリックしてください。
- compute.subnetworks.us e-compute.subnetworks.useExternalIp - compute.instances.addAccessConfig	クラウドデータの意味を有効にするため。
-container-type コンテナクラスタリスト	Google Kubernetes Engine で実行されている Kubernetes クラスタを検出する。

知識とサポート

サポートに登録します

""

ヘルプを表示します

""

法的通知

""

""

- "Cloud Manager 3.9 に関する注意事項"