コネクタをセットアップします

Cloud Manager

NetApp
June 04, 2021

目次

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 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 の次の機能を使用するには、コネクタが必要です。

- Cloud Volumes ONTAP
- オンプレミスの ONTAP クラスタ
- クラウドコンプライアンス
- Kubernetes
- クラウドバックアップ
- 監視
- オンプレミスでの階層化
- グローバルファイルキャッシュ
- Amazon S3 バケットの検出

Azure NetApp Files 、 Cloud Volumes Service 、または Cloud Sync には、コネクタは * _ 必要ではありません。

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 Cloud Compliance を使用する場合はコネクタが必要になります。

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

Google Cloud で Cloud Volumes ONTAP システムを作成する場合は、 Google Cloud でもコネクタを実行する必要があります。別の場所で実行されているコネクタは使用できません。

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"
- "AWS Marketplace から入手できます"
- "Azure Marketplace から入手できます"
- "既存の Linux にソフトウェアをダウンロードしてインストールする ホスト"

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

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"。

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、ある Cloud Central 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いずれかのビジネスユニットの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
   - "Cloud Manager に既存の Cloud Volumes ONTAP システムを追加"
   - "ONTAP クラスタの検出"
3. を設定します "Capacity Management Mode （容量管理モード）" 追加のコネクタで * Manual * に接続します。

   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、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）

"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要件

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。

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

ネットワークのサブネットが 172 範囲に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。 "この問題の詳細については、こちらをご覧ください"。

アウトバウンドインターネットアクセス

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。アウトバウンドのインターネットアクセスは、コネクタを Linux ホストに手動でインストールする場合や、コネクタで実行されているローカル UI にアクセスする場合にも必要です。

次のセクションでは、特定のエンドポイントについて説明します。

AWS でリソースを管理するエンドポイント

コネクタは、 AWS でリソースを管理する際に次のエンドポイントに接続します。

VPC がネットワークアクセス制御リスト（ ACL ）を使用してトラフィックをフィルタリングする場合は、アウトバウンドとインバウンドの両方のトラフィックに対してこれらのエンドポイントを有効にしてください。

エンドポイント	目的
AWS サービス（ amazonaws.com ）： • クラウド形成 • 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 ） 正確なエンドポイントは、 Cloud Volumes ONTAP を導入する地域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。"	AWS に Cloud Volumes ONTAP を導入して管理できるようにします。
\ https://api.services.cloud.netapp.com:443	NetApp Cloud Central への API 要求。
\ https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	ソフトウェアイメージ、マニフェスト、およびテンプレートにアクセスできます。
¥ https://cognito-idp.us-east-1.amazonaws.com ¥ https://cognito-identity.us-east-1.amazonaws.com ¥ https://sts.amazonaws.com ¥ https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	コネクタがマニフェスト、テンプレート、および Cloud Volumes ONTAP アップグレードイメージにアクセスしてダウンロードできるようにします。
\ https://cloudmanagerinfraprod.azurecr.io	Docker を実行しているインフラのコンテナコンポーネントのソフトウェアイメージにアクセスでき、 Cloud Manager とのサービス統合のためのソリューションを提供します。
\ https://kinesis.us-east-1.amazonaws.com	ネットアップが監査レコードからデータをストリーミングできるようにします。
\ https://cloudmanager.cloud.netapp.com	Cloud Central アカウントを含む Cloud Manager サービスとの通信。
https://netapp-cloud-account.auth0.com	NetApp Cloud Central との通信により、ユーザ認証を一元的に行うことができます。
support.netapp.com:443 https://mysupport.netapp.com	ネットアップ AutoSupport との通信：コネクタは support.netapp.com:443 と通信し、 https://mysupport.netapp.com にリダイレクトされます。
¥ https://support.netapp.com/svcgw ¥ https://support.netapp.com/ServiceGW/entitlement ¥ https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com ¥ https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	システムライセンスとサポート登録を行うためのネットアップとの通信

エンドポイント	目的
¥ https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com ¥ https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com ¥ https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	ネットアップがサポートの問題のトラブルシューティングに必要な情報を収集できるようにします。
\ https://ipa-signer.cloudmanager.netapp.com	Cloud Manager でライセンスを生成できます（ Cloud Volumes ONTAP 用の FlexCache ライセンスなど）。
次のようなさまざまなサードパーティの場所があります。 • https://repo1.maven.org/maven2 です • https://oss.sonType.org/content/repository を参照してください • \ https://repo.typesafe.com サードパーティの所在地は変更される可能性があります。	アップグレード時に、 Cloud Manager はサードパーティの依存関係に対応する最新のパッケージをダウンロードします。

Azure でリソースを管理するエンドポイント

コネクタは、 Azure でリソースを管理する際に次のエンドポイントに接続します。

エンドポイント	目的
https://management.azure.com https://login.microsoftonline.com	Cloud Manager では、ほとんどの Azure リージョンに Cloud Volumes ONTAP を導入して管理できます。
https://management.microSoftazure.de https://login.microsoftonline.de	Cloud Manager は、 Azure Germany リージョンに Cloud Volumes ONTAP を導入して管理できます。
https://management.usgovcloudapi.net/ https://login.microsoftonline.com	Cloud Manager は、 Azure US GOV リージョンに Cloud Volumes ONTAP を導入して管理できます。
\ https://api.services.cloud.netapp.com:443	NetApp Cloud Central への API 要求。
\ https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	ソフトウェアイメージ、マニフェスト、およびテンプレートにアクセスできます。
¥ https://cognito-idp.us-east-1.amazonaws.com ¥ https://cognito-identity.us-east-1.amazonaws.com ¥ https://sts.amazonaws.com ¥ https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	コネクタがマニフェスト、テンプレート、および Cloud Volumes ONTAP アップグレードイメージにアクセスしてダウンロードできるようにします。
\ https://cloudmanagerinfraprod.azurecr.io	Docker を実行しているインフラのコンテナコンポーネントのソフトウェアイメージにアクセスでき、 Cloud Manager とのサービス統合のためのソリューションを提供します。
\ https://kinesis.us-east-1.amazonaws.com	ネットアップが監査レコードからデータをストリーミングできるようにします。

エンドポイント	目的
\ https://cloudmanager.cloud.netapp.com	Cloud Central アカウントを含む Cloud Manager サービスとの通信。
https://netapp-cloud-account.auth0.com	NetApp Cloud Central との通信により、ユーザ認証を一元的に行うことができます。
support.netapp.com:443 https://mysupport.netapp.com	ネットアップ AutoSupport との通信：コネクタは support.netapp.com:443 と通信し、https://mysupport.netapp.com にリダイレクトされます。
¥ https://support.netapp.com/svcgw ¥ https://support.netapp.com/ServiceGW/entitlement ¥ https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com ¥ https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	システムライセンスとサポート登録を行うためのネットアップとの通信
¥ https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com ¥ https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com ¥ https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	ネットアップがサポートの問題のトラブルシューティングに必要な情報を収集できるようにします。
\ https://ipa-signer.cloudmanager.netapp.com	Cloud Manager でライセンスを生成できます（ Cloud Volumes ONTAP 用の FlexCache ライセンスなど）。
* .blob.core.windows.net	プロキシを使用する場合は HA ペアに必要です。
次のようなさまざまなサードパーティの場所があります。 • https://repo1.maven.org/maven2 です • https://oss.sonType.org/content/repository を参照してください • \ https://repo.typesafe.com サードパーティの所在地は変更される可能性があります。	アップグレード時に、 Cloud Manager はサードパーティの依存関係に対応する最新のパッケージをダウンロードします。

GCP でリソースを管理するためのエンドポイント

コネクタは、 GCP でリソースを管理する際に次のエンドポイントに接続します。

エンドポイント	目的
\ https://www.googleapis.com	GCP で Cloud Volumes ONTAP を導入および管理するために、 Connector から Google API に接続できるようにします。
\ https://api.services.cloud.netapp.com:443	NetApp Cloud Central への API 要求。
\ https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	ソフトウェアイメージ、マニフェスト、およびテンプレートにアクセスできます。

エンドポイント	目的
¥ https://cognito-idp.us-east-1.amazonaws.com ¥ https://cognito-identity.us-east-1.amazonaws.com ¥ https://sts.amazonaws.com ¥ https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	コネクタがマニフェスト、テンプレート、および Cloud Volumes ONTAP アップグレードイメージにアクセスしてダウンロードできるようにします。
\ https://cloudmanagerinfraprod.azurecr.io	Docker を実行しているインフラのコンテナコンポーネントのソフトウェアイメージにアクセスでき、 Cloud Manager とのサービス統合のためのソリューションを提供します。
\ https://kinesis.us-east-1.amazonaws.com	ネットアップが監査レコードからデータをストリーミングできるようにします。
\ https://cloudmanager.cloud.netapp.com	Cloud Central アカウントを含む Cloud Manager サービスとの通信。
https://netapp-cloud-account.auth0.com	NetApp Cloud Central との通信により、ユーザ認証を一元的に行うことができます。
support.netapp.com:443 https://mysupport.netapp.com	ネットアップ AutoSupport との通信：コネクタは support.netapp.com:443 と通信し、 https://mysupport.netapp.com にリダイレクトされます。
¥ https://support.netapp.com/svcgw ¥ https://support.netapp.com/ServiceGW/entitlement ¥ https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com ¥ https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	システムライセンスとサポート登録を行うためのネットアップとの通信
¥ https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com ¥ https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com ¥ https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	ネットアップがサポートの問題のトラブルシューティングに必要な情報を収集できるようにします。
\ https://ipa-signer.cloudmanager.netapp.com	Cloud Manager でライセンスを生成できます（ Cloud Volumes ONTAP 用の FlexCache ライセンスなど）。
次のようなさまざまなサードパーティの場所があります。 • https://repo1.maven.org/maven2 です • https://oss.sonType.org/content/repository を参照してください • \ https://repo.typesafe.com サードパーティの所在地は変更される可能性があります。	アップグレード時に、 Cloud Manager はサードパーティの依存関係に対応する最新のパッケージをダウンロードします。

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。

- http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm
- https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
- https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

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。

ローカルを使用するときに **Web** ブラウザからアクセスするエンドポイント **UI**

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。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
コネクタホスト	Cloud Manager コンソールをロードするには、 Web ブラウザでホストの 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 を使用できます。 • プライベート IP は、 VPN とがある場合に機能します 仮想ネットワークへの直接アクセス • 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の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する必要があります。
¥ https://auth0.com ¥ https://cdn.auth0.com ¥ https://netapp-cloud-account.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。

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への HTTP アクセスを提供します Cloud Compliance からのユーザインターフェイスと接続
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 Compliance インスタンスにインターネットアクセスを提供します

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 クラスタ管理 LIF	ONTAP への API コール
	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
クラウドコンプライアンス	HTTP	80	Cloud Compliance インスタンス	Cloud Volumes ONTAP 向けクラウドコンプライアンス

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
API コール	3000	TCP	ONTAP クラスタ管理 LIF	ONTAP への API コール
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

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
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
API コール	TCP	3000	ONTAP クラスタ管理 LIF	ONTAP への API コール
DNS	UDP	53	DNS	Cloud Manager による DNS 解決に使用されます

AWS で Cloud Manager からコネクタを作成する

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。オプションとして、を選択することもできます "AWS Marketplace からコネクタを作成します"またはをに設定します "ソフトウェアをダウンロードして、ご使用のホストにインストールします"。

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。

コネクタを作成するための AWS 権限を設定する

Cloud Manager からコネクタを導入する前に、 AWS 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. 次の場所からコネクタ 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"

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。

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。

AWS でコネクタを作成する

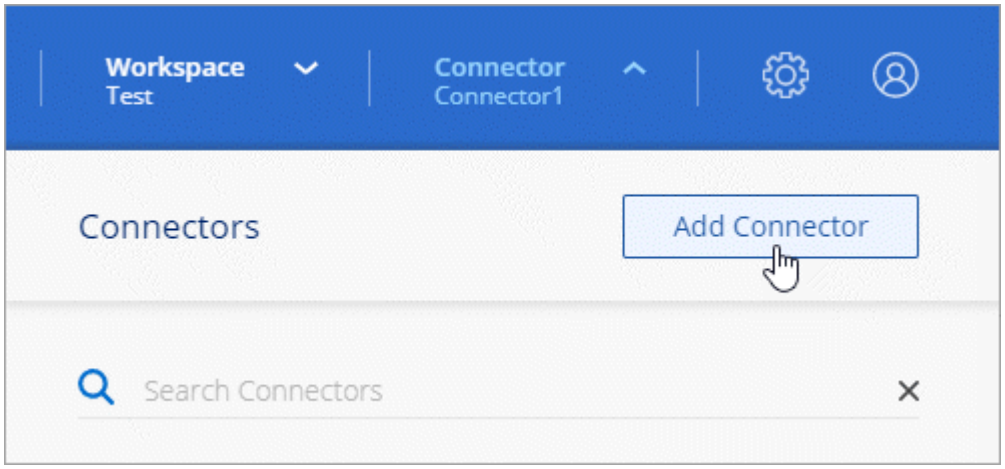
Cloud Manager では、ユーザインターフェイスから AWS に直接コネクタを作成できます。

必要なもの

- IAM 用の AWS アクセスキーとシークレットキー を持つユーザ "必要な権限"。
- 選択した AWS リージョン内の VPC 、サブネット、キーペア。

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. [* 開始しましょう *] をクリックします。
3. クラウドプロバイダとして「 * Amazon Web Services * 」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"。

4. 必要な情報を確認し、 [* Continue （続行）] をクリックします。
5. 必要な情報を入力します。
   - * AWS クレデンシャル * ：インスタンスの名前を入力し、権限の要件を満たす AWS アクセスキーとシークレットキーを指定します。
   - * 場所 * ：インスタンスの AWS リージョン、 VPC 、およびサブネットを指定します。
   - * ネットワーク * ：インスタンスで使用するキーペア、パブリック IP アドレスを有効にするかどうか、およびオプションで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。

6. [作成（ Create ）] 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 にコネクタを作成する

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 から直接 Azure でコネクタを作成する方法について説明します。オプションとして、を選択することもできます "Azure Marketplace からコネクタを作成します"またはをに設定します "ソフトウェアをダウンロードして、ご使用のホストにインストールします"。

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。

コネクタを作成するための **Azure** 権限を設定しています

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. コネクタの Azure 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 "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。

   b. 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"
],
```

   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 _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。

2. 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。

   - Azure AD のユーザ、グループ、アプリケーション * へのアクセスを割り当てます。
   - ユーザアカウントを選択します。
   - [保存（ Save ）] 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 でコネクタを作成する

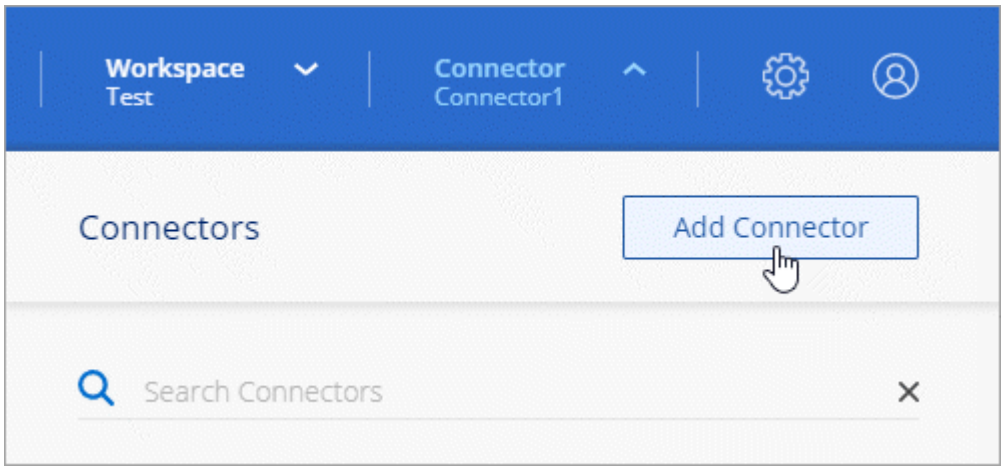
Cloud Manager では、ユーザインターフェイスから直接 Azure にコネクタを作成できます。

必要なもの

- 。 "必要な権限" 使用している Azure アカウントに対して。
- 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

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. [* 開始しましょう *] をクリックします。
3. 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"。

4. 必要な情報を確認し、 [* Continue （続行）] をクリックします。
5. 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。

6. 必要な情報を入力します。
   - * VM 認証 * ：仮想マシンの名前、ユーザ名、パスワード、または公開鍵を入力します。
   - * 基本設定 * ： Azure サブスクリプション、 Azure リージョン、および新しいリソースグループを作成するか既存のリソースグループを使用するかを選択します。
   - * 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。

7. [作成（ Create ）] 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 GCP でコネクタを作成する

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。オプションとして、を選択することもできます "ソフトウェアをダウンロードして、ご使用のホストにインストールします"。

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。

コネクタを作成するための GCP 権限の設定

Cloud Manager から Connector を導入する前に、 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. Cloud Manager を導入する GCP ユーザがであることを確認します NetApp Cloud Central には、にアクセス許可が含まれています "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、 Cloud Manager から作成するときに 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。

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、ホストプロジェクト内で Connector サービスアカウントに *compute.networkUser* ロールも必要です。 "このロールは、 Connector VM にを使用する権限を付与します 共有 VPC"。

GCP ユーザに Cloud Manager から Connector を作成するために必要な権限が付与され、 Connector VM のサービスアカウントが設定されます。

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 では、ユーザインターフェイスから直接 GCP でコネクタを作成できます。

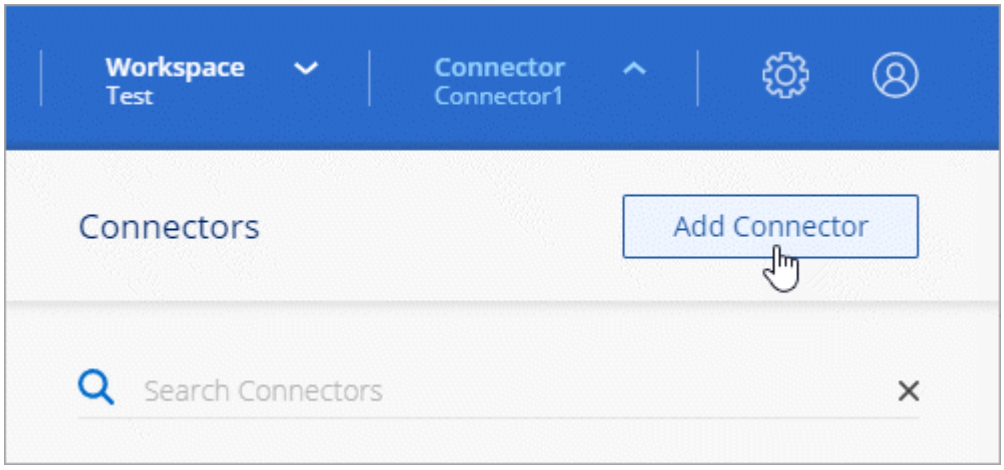
必要なもの

- 。 "必要な権限" をクリックしてください。

- Google Cloud プロジェクト。
- 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。

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. [* 開始しましょう *] をクリックします。
3. 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"。

4. 必要な情報を確認し、 [* Continue （続行）] をクリックします。
5. 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。

6. 必要な情報を入力します。
   - * 基本設定 * ：仮想マシンインスタンスの名前を入力し、必要な権限を持つプロジェクトおよびサービスアカウントを指定します。
   - * 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。

7. [作成（ Create ）] 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。"。