クラウドプロバイダをセットアップします

Astra Control Service

NetApp
June 04, 2024

目次

クラウドプロバイダをセットアップします

Amazon Web Servicesをセットアップする

Amazon Elastic Kubernetes Service（EKS）クラスタをAstra Control Serviceで管理するには、Amazon Web Servicesプロジェクトを準備する手順がいくつか必要です。

Amazon Web Servicesのセットアップをすぐに開始できます

これらの手順を実行してすぐに作業を開始するか、残りのセクションまでスクロールして詳細を確認してください。

[1つ] Amazon Web ServicesのAstra Control Serviceの要件を確認

クラスタが正常に機能しており、サポートされているバージョンのKubernetesを実行していること、ワーカーノードがオンラインでLinuxやWindowsなどを実行していることを確認します。 このステップの詳細をご覧ください。

[2 つ] Amazonアカウントを作成します

Amazonアカウントをまだ作成していない場合は、EKSを使用できるように作成する必要があります。 このステップの詳細をご覧ください。

[3つ] Amazon Web Services CLIをインストールします

コマンドラインからAWSを管理できるように、AWS CLIをインストールします。 ステップバイステップの手順に従います。

[4.] オプション：**IAM**ユーザを作成します

Amazon Identity and Access Management（IAM）ユーザを作成します。また、この手順をスキップし、既存のIAMユーザをAstra Control Serviceで使用することもできます。

詳細な手順を参照してください。

[5 つ] 権限ポリシーを作成して適用します

Astra Control ServiceがAWSアカウントとやり取りするために必要な権限を持つポリシーを作成します。

詳細な手順を参照してください。

[6] IAMユーザのクレデンシャルを保存します

からAstra Control Serviceにクレデンシャルをインポートできるように、IAMユーザのクレデンシャルを保存します。

詳細な手順を参照してください。

EKSクラスタ要件

Kubernetes クラスタを Astra Control Service から検出して管理できるようにするには、 Kubernetes クラスタが次の要件を満たしている必要があります。

Kubernetes のバージョン

クラスタで1.25~1.28の範囲のKubernetesバージョンが実行されている必要があります。

イメージタイプ

各ワーカーノードのイメージタイプはLinuxである必要があります。

クラスタの状態

クラスタが正常な状態で稼働し、少なくとも 1 つのオンラインワーカーノードがあり、ワーカーノードが障害状態でない必要があります。

Astra Controlプロビジョニングツール

ストレージバックエンドを使用するには、Astra Control Provisionerと外部のSnapshotコントローラが必要です。これらの処理を有効にするには、次の手順を実行します。

1. "スナップショットCRDとスナップショットコントローラをインストールします"。
2. "Astra Control Provisionerを有効にする"。
3. "VolumeSnapshotClassを作成します"。

Amazon Elastic Block Store（**EBS**）向け**CSI**ドライバ

Amazon EBSストレージバックエンドを使用する場合は、EBS用のContainer Storage Interface（CSI）ドライバをインストールする必要があります（自動ではインストールされません）。

CSIドライバのインストール手順については、手順を参照してください。

外部**Snapshot**データをインストールします

まだ行っていない場合は、 "スナップショットCRDとスナップショットコントローラをインストールします"。

CSIドライバを**Amazon EKS**アドオンとしてインストールします

1. サービスアカウント用のAmazon EBS CSIドライバIAMロールを作成します。指示に従います "Amazonのドキュメントを参照してください"の手順に記載されたAWS CLIコマンドを使用します。
2. 次のAWS CLIコマンドを使用してAmazon EBS CSIアドオンを追加します。括弧<>内の情報は、環境に固有の値に置き換えてください。<driver_role>を、前の手順で作成したEBS CSIドライバロールの名前に置き換えます。

```
aws eks create-addon \
  --cluster-name <CLUSTER_NAME> \
  --addon-name aws-ebs-csi-driver \
  --service-account-role-arn
arn:aws:iam::<ACCOUNT_ID>:role/<DRIVER_ROLE>
```

EBSストレージクラスを設定します

1. Amazon EBS CSIドライバGitHubリポジトリをシステムにクローニングします。

```
git clone https://github.com/kubernetes-sigs/aws-ebs-csi-
driver.git
```

2. dynamicprovisioning exampleディレクトリに移動します。

```
cd aws-ebs-csi-driver/examples/kubernetes/dynamic-provisioning/
```

3. マニフェストディレクトリからEBS SCストレージクラスとEBS要求の永続的ボリューム要求を導入します。

```
kubectl apply -f manifests/storageclass.yaml
kubectl apply -f manifests/claim.yaml
```

4. EBS SCストレージクラスの説明

```
kubectl describe storageclass ebs-sc
```

ストレージクラスの属性を説明する出力が表示されます。

Amazonアカウントを作成します

Amazonアカウントをまだお持ちでない場合は、Amazon EKSに対する請求を有効にするためにアカウントを作成する必要があります。

手順

1. にアクセスします "Amazonホームページ" をクリックし、右上の「サインイン」を選択して、「ここから開始」を選択します。
2. プロンプトに従ってアカウントを作成します。

Amazon Web Services CLIをインストールします

コマンドラインからAWSリソースを管理できるように、AWS CLIをインストールします。

ステップ

1. に進みます "AWS CLIの使用を開始する" および手順に従ってCLIをインストールします。

オプション：IAMユーザを作成します

IAMユーザを作成し、セキュリティを強化しながらAWSのサービスとリソースを使用、管理できるようにします。また、この手順をスキップし、既存のIAMユーザをAstra Control Serviceで使用することもできます。

ステップ

1. に進みます "IAMユーザを作成する" および手順に従ってIAMユーザを作成します。

権限ポリシーを作成して適用します

Astra Control ServiceがAWSアカウントとやり取りするために必要な権限を持つポリシーを作成します。

手順

1. 「policy.json」という名前の新しいファイルを作成します。
2. 次のJSONコンテンツをファイルにコピーします。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData",
                "fsx:DescribeVolumes",
                "ec2:DescribeRegions",
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:GetObject",
                "iam:SimulatePrincipalPolicy",
                "s3:ListAllMyBuckets",
                "eks:DescribeCluster",
                "eks:ListNodegroups",
                "eks:DescribeNodegroup",
                "eks:ListClusters",
                "iam:GetUser",
                "s3:DeleteObject",
                "s3:DeleteBucket",
                "autoscaling:DescribeAutoScalingGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

3. ポリシーを作成します。

```
POLICY_ARN=$(aws iam create-policy  --policy-name <policy-name> --policy
-document file://policy.json  --query='Policy.Arn' --output=text)
```

4. IAM ユーザにポリシーを付加します。「<iam-user-name>」を、作成したIAMユーザのユーザ名または既存のIAMユーザの名前に置き換えます。

```
aws iam attach-user-policy --user-name <IAM-USER-NAME> --policy-arn
=$POLICY_ARN
```

IAMユーザのクレデンシャルを保存します

ユーザをAstra Control Serviceで認識できるように、IAMユーザのクレデンシャルを保存します。

手順

1. クレデンシャルをダウンロードします。「<iam-user-name>」を、使用するIAMユーザのユーザ名に置き換えます。

```
aws iam create-access-key --user-name <IAM-USER-NAME> --output json >
credential.json
```

結果

「credential.json」ファイルが作成され、Astra Control Serviceにそのクレデンシャルをインポートできます。

Google Cloud をセットアップします

Astra Control Service を使用して Google Kubernetes Engine クラスタを管理するには、Google Cloud プロジェクトを準備するための手順がいくつか必要です。

Google Cloud Volumes Service for Google Cloud をストレージバックエンドとして使用せず、あとで使用する予定の場合は、 Google Cloud Volumes Service for Google Cloud を今すぐ設定するために必要な手順を実行する必要があります。サービスアカウントをあとで作成すると、既存のストレージバケットへのアクセスが失われる可能性があります。

Google Cloud のセットアップをすぐに開始できます

これらの手順を実行してすぐに作業を開始するか、残りのセクションまでスクロールして詳細を確認してください。

[1つ] Google Kubernetes Engine の Astra Control Service の要件を確認

クラスタが正常で、サポートされているKubernetesバージョンが実行されていること、ワーカーノードがオンラインでサポートされているイメージタイプが実行されていることなどを確認します。 このステップの詳細をご覧ください。

[2 つ]（オプション）： Cloud Volumes Service for Google Cloud を購入します

ストレージバックエンドとして Cloud Volumes Service for Google Cloud を使用する場合は、 Google Cloud Marketplace の NetApp Cloud Volumes Service ページに移動して、「購入」を選択します。 このステップの詳細をご覧ください。

[3つ] Google Cloud プロジェクトで API を有効にします

次の Google Cloud API を有効にします。

- Google Kubernetes Engine の略
- クラウドストレージ

- Cloud Storage JSON API
- サービス利用
- Cloud Resource Manager API の略
- NetApp Cloud Volumes Service の略
  - Cloud Volumes Service for Google Cloud で必要です
  - Google Persistent Disk の場合はオプション（ただし推奨
- Service Consumer Management API の略
- サービスネットワーク API
- Service Management API の略

ステップバイステップの手順に従います。

[4.] 必要な権限を持つサービスアカウントを作成します

次の権限を持つ Google Cloud サービスアカウントを作成します。

- Kubernetes Engine Admin の略
- NetApp Cloud Volumes Admin の権限が必要です
  - Cloud Volumes Service for Google Cloud で必要です
  - Google Persistent Disk の場合はオプション（ただし推奨
- ストレージ管理者
- Service Usage Viewer （サービス使用状況ビューア
- ネットワークビューアを計算します

詳細な手順を参照してください。

[5 つ**]** サービスアカウントキーを作成します

サービスアカウントのキーを作成し、そのキーファイルを安全な場所に保存します。 ステップバイステップの手順に従います。

[6] （オプション）： **VPC** のネットワークピアリングを設定します

Cloud Volumes Service for Google Cloud をストレージバックエンドとして使用する場合は、 VPC から Cloud Volumes Service for Google Cloud へのネットワークピアリングを設定します。 ステップバイステップの手順に従います。

GKE クラスタの要件

Kubernetes クラスタを Astra Control Service から検出して管理できるようにするには、 Kubernetes クラスタが次の要件を満たしている必要があります。これらの要件の一部は、 Cloud Volumes Service for Google Cloud をストレージバックエンドとして使用する場合にのみ適用されます。

Kubernetes のバージョン

クラスタで1.26~1.28の範囲のKubernetesバージョンが実行されている必要があります。

イメージタイプ

各ワーカーノードのイメージタイプはである必要があります `COS_CONTAINERD`。

クラスタの状態

クラスタが正常な状態で稼働し、少なくとも 1 つのオンラインワーカーノードがあり、ワーカーノードが障害状態でない必要があります。

Google Cloud リージョン

Cloud Volumes Service for Google Cloud をストレージバックエンドとして使用する場合は、クラスタがで実行されている必要があります "Cloud Volumes Service for Google Cloud がサポートされている Google Cloud リージョン。" Astra Control Service は、 CVS と CVS パフォーマンスの両方のサービスタイプをサポートします。Cloud Volumes Service for Google Cloud をサポートするリージョンは、たとえストレージバックエンドとして使用していない場合でも選択することを推奨します。これにより、パフォーマンス要件が変化した場合に、 Cloud Volumes Service for Google Cloud をストレージバックエンドとして簡単に使用できるようになります。

ネットワーキング

Cloud Volumes Service for Google Cloud をストレージバックエンドとして使用する場合は、 Cloud Volumes Service for Google Cloud とピア関係にある VPC 内にクラスタを配置する必要があります。 この手順については、以下で説明します。

プライベートクラスタ

クラスタがプライベートの場合は、を参照してください "許可されたネットワーク" Astra Control Service の IP アドレスを許可する必要があります。

52.188.218.166-32

GKE クラスタの動作モード

標準モードのオペレーションを使用する必要があります。自動操舵モードは、現時点ではテストされていません。 "操作モードの詳細を確認してください"。

ストレージプール

NetApp Cloud Volumes ServiceをCVSサービスタイプのストレージバックエンドとして使用する場合は、ボリュームをプロビジョニングする前にストレージプールを設定する必要があります。を参照してください "GKE クラスタのサービスタイプ、ストレージクラス、 PV サイズ" を参照してください。

オプション：**Cloud Volumes Service for Google Cloud**を購入

Astra Control Service では、永続的ボリュームのストレージバックエンドとして Cloud Volumes Service for Google Cloud を使用できます。このサービスを使用する場合は、 Google Cloud Marketplace で Cloud Volumes Service for Google Cloud を購入して、永続的ボリュームに対する請求を有効にする必要があります。

ステップ

1. にアクセスします "NetApp Cloud Volumes Service のページ" Google Cloud Marketplace で「 * Purchase * 」を選択し、画面の指示に従います。

"Google Cloud のドキュメントに記載されているステップバイステップの手順に従って、サービスを購入して有効にします"。

プロジェクトで API を有効にします

特定の Google Cloud API にアクセスするには、プロジェクトに権限が必要です。API は、 Google Kubernetes Engine （ GKE ）クラスタや NetApp Cloud Volumes Service ストレージなどの Google Cloud リソースとのやり取りに使用されます。

ステップ

1. "Google Cloud コンソールまたは gcloud CLI を使用して、次の API を有効にする"：
    - Google Kubernetes Engine の略
    - クラウドストレージ
    - Cloud Storage JSON API
    - サービス利用
    - Cloud Resource Manager API の略
    - NetApp Cloud Volumes Service （ Cloud Volumes Service for Google Cloud に必要）
    - Service Consumer Management API の略
    - サービスネットワーク API
    - Service Management API の略

次のビデオでは、 Google Cloud コンソールから API を有効にする方法を紹介します。

► https://docs.netapp.com/ja-jp/astra-control-service/media/get-started/video-enable-gcp-apis.mp4 *(video)*

サービスアカウントを作成します

Astra Control Service は、 Google Cloud サービスアカウントを使用して、 Kubernetes アプリケーションデータ管理をお客様に代わって容易にします。

手順

1. Google Cloud およびにアクセスします "コンソール、 gcloud コマンド、またはその他の推奨される方法を使用して、サービスアカウントを作成します"。
2. サービスアカウントに次のロールを付与します。
    - * Kubernetes Engine Admin * - クラスタの一覧表示とアプリ管理のための管理アクセスの作成に使用します。
    - * NetApp Cloud Volume Admin * - アプリケーション用の永続的ストレージの管理に使用します。
    - * ストレージ管理者 * - アプリのバックアップ用のバケットとオブジェクトを管理するために使用します。
    - * Service Usage Viewer * - 必要な Cloud Volumes Service for Google Cloud API が有効になっているかどうかを確認するために使用します。
    - * Compute Network Viewer * - Kubernetes VPC で Google Cloud の Cloud Volumes Service にアクセスできるかどうかを確認するために使用します。

gcloud を使用したい場合は、 Astra Control インターフェイス内から手順を実行できます。[**Account] > [Credentials] > [Add Credentials]** を選択し、 **[*Instructions**] を選択します。

Google Cloud コンソールを使用する場合は、次のビデオで、コンソールからサービスアカウントを作成する方法を紹介します。

► https://docs.netapp.com/ja-jp/astra-control-service/media/get-started/video-create-gcp-service-account.mp4

(video)

共有 **VPC** のサービスアカウントを設定します

1 つのプロジェクトに存在する GKE クラスタを管理し、別のプロジェクト（共有 VPC ）から VPC を使用するには、「 * Compute Network Viewer * 」ロールを持つホストプロジェクトのメンバーとして Astra サービスアカウントを指定する必要があります。

手順

1. Google Cloud コンソールから、 * iam & Admin* に移動し、 * サービスアカウント * を選択します。
2. Astra のサービスアカウントを見つけます "必要な権限" E メールアドレスをコピーします。
3. ホストプロジェクトに移動し、 * iam & Admin* > * iam * を選択します。
4. 「 * 追加」を選択し、サービスアカウントのエントリを追加します。
   a. * 新規メンバー * ：サービスアカウントのメールアドレスを入力します。
   b. * 役割 * ： [* コンピュート・ネットワーク・ビューア *] を選択します。
   c. [保存（ Save ）] を選択します。

結果

共有 VPC を使用して GKE クラスタを追加すると、 Astra で完全に機能します。

サービスアカウントキーを作成します

Astra Control Service にユーザ名とパスワードを入力する代わりに、最初のクラスタを追加するときにサービスアカウントキーを指定します。Astra Control Service は、サービスアカウントキーを使用して、設定したサービスアカウントの ID を確立します。

サービスアカウントキーは、 JavaScript Object Notation （ JSON ）形式で格納されたプレーンテキストです。ここには、アクセス権を持つ GCP リソースに関する情報が含まれています。

JSON ファイルは、キーの作成時にのみ表示またはダウンロードできます。ただし、新しいキーはいつでも作成できます。

手順

1. Google Cloud およびにアクセスします "コンソール、 gcloud コマンド、またはその他の推奨される方法を使用して、サービスアカウントキーを作成します"。
2. プロンプトが表示されたら、サービスアカウントキーファイルを安全な場所に保存します。

次のビデオは、 Google Cloud コンソールからサービスアカウントキーを作成する方法を示しています。

► https://docs.netapp.com/ja-jp/astra-control-service/media/get-started/video-create-gcp-service-account-

key.mp4 *(video)*

オプション：VPCのネットワークピアリングを設定します

Cloud Volumes Service for Google Cloud をストレージバックエンドサービスとして使用する場合は、 VPC から Cloud Volumes Service for Google Cloud へのネットワークピアリングを設定します。

ネットワークピアリングを設定する最も簡単な方法は、 gcloud コマンドを Cloud Volumes Service から直接取得することです。コマンドは、新しいファイルシステムを作成するときに Cloud Volumes Service から使用できます。

手順

1. "NetApp BlueXPグローバルリージョンマップにアクセス" をクリックし、クラスタが存在する Google Cloud リージョンで使用するサービスタイプを特定します。

   Cloud Volumes Service には、 CVS と CVS パフォーマンスの 2 つのサービスタイプがあります。 "これらのサービスタイプの詳細については、こちらをご覧ください"。

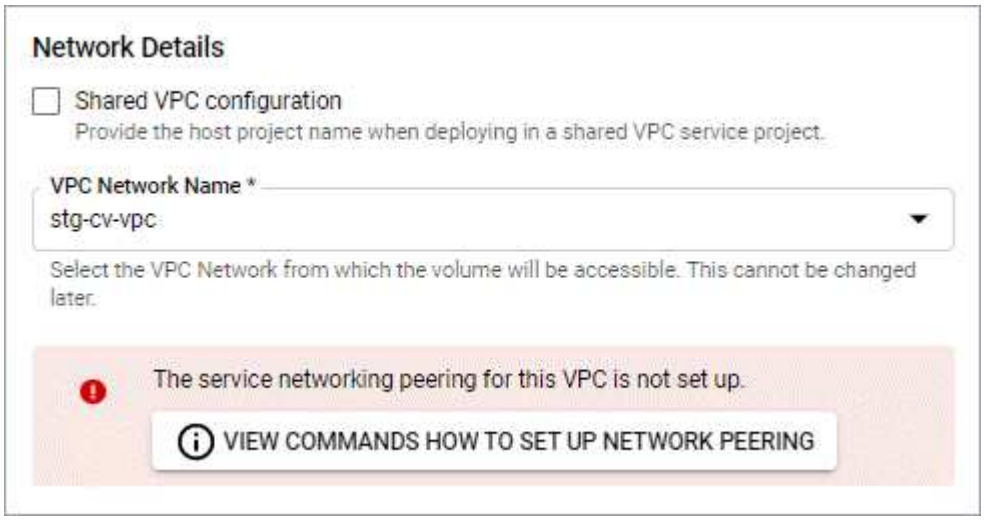
2. "Google Cloud Platform の Cloud Volume にアクセスします"。
3. [* Volumes （ボリューム）] ページで、 [* Create （作成）] を選択します。
4. サービスタイプ * で、 * CVS * または * CVS - パフォーマンス * のいずれかを選択します。

   Google Cloud リージョンに適したサービスタイプを選択する必要があります。これは、手順 1 で特定したサービスタイプです。サービスタイプを選択すると、ページ上のリージョンのリストが、そのサービスタイプがサポートされているリージョンで更新されます。

   この手順の後、コマンドを取得するためにネットワーク情報を入力するだけで済みます。

5. [* Region* （ * 地域）] で、地域とゾーンを選択します。
6. [ネットワークの詳細 *] で VPC を選択します。

   ネットワークピアリングを設定していない場合は、次の通知が表示されます。



7. ボタンを選択して、ネットワークピアリングのセットアップコマンドを表示します。
8. コマンドをコピーし、 Cloud Shell で実行します。

これらのコマンドの使用方法の詳細については、を参照してください "Cloud Volumes Service for GCP のクイックスタート"。

"プライベートサービスアクセスの設定とネットワークピアリングの設定について詳しくは、こちらをご覧ください"。

9. 完了したら、 * ファイルシステムの作成 * ページでキャンセルを選択できます。

このボリュームの作成は、ネットワークピアリング用のコマンドを取得するためだけに開始しました。

Azure NetApp Files を使用して Microsoft Azure をセットアップする

Microsoft Azure サブスクリプションを準備してから、 Astra Control Service で Azure Kubernetes Service クラスタを管理するには、いくつかの手順を実行する必要があります。Azure NetApp Files をストレージバックエンドとして使用する場合は、次の手順に従います。

Azure のセットアップのクイックスタート

これらの手順を実行してすぐに作業を開始するか、残りのセクションまでスクロールして詳細を確認してください。

[1つ] Azure Kubernetes Service の **Astra Control Service** の要件を確認

クラスタが正常で、サポートされているバージョンのKubernetesを実行していること、ノードプールがオンラインでLinuxを実行していることなどを確認します。 このステップの詳細をご覧ください。

[2 つ] Microsoft Azure に登録

Microsoft Azure アカウントを作成します。 このステップの詳細をご覧ください。

[3つ] Azure NetApp Files に登録します

ネットアップリソースプロバイダを登録 このステップの詳細をご覧ください。

[4.] ネットアップアカウントを作成します

Azure ポータルで Azure NetApp Files にアクセスし、ネットアップアカウントを作成します。 このステップの詳細をご覧ください。

[5 つ] 容量プールを設定

永続ボリューム用に 1 つ以上の容量プールを設定します。 このステップの詳細をご覧ください。

[6] サブネットを **Azure NetApp Files** に委譲します

サブネットを Azure NetApp Files に委譲し、 Astra Control サービスがそのサブネット内に永続的ボリュームを作成できるようにします。 このステップの詳細をご覧ください。

[7] Azure サービスプリンシパルを作成します

Contributor ロールを持つ Azure サービスプリンシパルを作成します。 このステップの詳細をご覧ください。

[8] オプション：**Azure**バックアップバケットの冗長性を設定する

デフォルトでは、バケットAstra Control ServiceはAzure Kubernetes Serviceのバックアップを保存するためにを使用し、ローカルのRedundant Storage（LRS）冗長性オプションを使用します。オプションとして、Azureバケットに永続性レベルの冗長性を設定することができます。 このステップの詳細をご覧ください。

Azure Kubernetes Service クラスタの要件

Kubernetes クラスタを Astra Control Service から検出して管理できるようにするには、 Kubernetes クラスタが次の要件を満たしている必要があります。

Kubernetes のバージョン

クラスタでKubernetesバージョン1.26~1.28が実行されている必要があります。

イメージタイプ

すべてのノードプールのイメージタイプは Linux である必要があります。

クラスタの状態

クラスタが正常な状態で稼働し、少なくとも 1 つのオンラインワーカーノードがあり、ワーカーノードが障害状態でない必要があります。

Azure リージョン

クラスタは、 Azure NetApp Files が利用可能なリージョンに配置する必要があります。 "Azure 製品を地域別に表示します"。

サブスクリプション。

クラスタは、 Azure NetApp Files が有効になっているサブスクリプションに含まれている必要があります。サブスクリプションはいつでも選択できます Azure NetApp Files に登録します。

VNet

以下の VNet の要件を考慮してください。

- クラスタは、 Azure NetApp Files 委任サブネットに直接アクセスできる VNet 内に存在する必要があります。 委任されたサブネットを設定する方法について説明します。
- Kubernetes クラスタが別の VNet 内の Azure NetApp Files 委任サブネットにピアリングされている VNet 内にある場合は、ピアリング接続の両側をオンラインにする必要があります。
- Azure NetApp Files を使用した VNet （すぐにピア関係にある VNet を含む）で使用される IP 数のデフォルトの上限は 1 、 000 です。 "Azure NetApp Files のリソース制限を確認します"。

  限界に近づくと、次の 2 つのオプションがあります。

  - 可能です "制限の増加を要求します"。サポートが必要な場合は、ネットアップの担当者にお問い合わせください。
  - 新しい Amazon Kubernetes Service （ AKS ）クラスタを作成するときに、クラスタの新しいネットワークを指定します。新しいネットワークを作成したら、新しいサブネットをプロビジョニング

し、そのサブネットを Azure NetApp Files に委譲します。

Microsoft Azure に登録

Microsoft Azure アカウントをお持ちでない場合は、まず Microsoft Azure にサインアップします。

手順

1. にアクセスします "Azure サブスクリプションページ" をクリックして Azure サービスに登録してください。
2. プランを選択し、指示に従ってサブスクリプションを完了します。

Azure NetApp Files に登録します

ネットアップリソースプロバイダを登録すると、 Azure NetApp Files にアクセスできます。

手順

1. Azure ポータルにログインします。
2. "Azure NetApp Files のドキュメントに従って、ネットアップリソースプロバイダを登録してください"。

ネットアップアカウントを作成します

Azure NetApp Files でネットアップアカウントを作成します。

ステップ

1. "Azure NetApp Files のドキュメントに従って、 Azure ポータルからネットアップアカウントを作成します"。

容量プールをセットアップする

Astra Control Service が容量プールに永続的ボリュームをプロビジョニングできるようにするには、 1 つ以上の容量プールが必要です。Astra Control Service では、容量プールを作成しない。

Kubernetes アプリケーション用の容量プールを設定する際には、次の点を考慮してください。

- 容量プールは、 AKS クラスタが Astra Control Service で管理される同じ Azure リージョンに作成する必要があります。
- 容量プールには、 Ultra 、 Premium 、または Standard のいずれかのサービスレベルを指定できます。これらのサービスレベルはそれぞれ、パフォーマンスのニーズに合わせて設計されています。Astra Control Service は、 3 つすべてをサポートします。

  Kubernetes クラスタで使用するサービスレベルごとに容量プールを設定する必要があります。

  "Azure NetApp Files のサービスレベルの詳細については、こちらをご覧ください"。

- Astra Control Service で保護するアプリケーションの容量プールを作成する前に、それらのアプリケーションに必要なパフォーマンスと容量を選択します。

  適切な容量をプロビジョニングすることで、ユーザは必要に応じて永続ボリュームを作成できるようになります。容量を使用できない場合は、永続ボリュームをプロビジョニングできません。

- Azure NetApp Files 容量プールでは、手動または自動の QoS タイプを使用できます。Astra Control Service は、自動 QoS 容量プールをサポートします。手動の QoS 容量プールはサポートされません。

ステップ

1. "Azure NetApp Files のドキュメントに従って、自動 QoS 容量プールを設定します"。

サブネットを **Azure NetApp Files** に委譲します

サブネットを Azure NetApp Files に委譲し、 Astra Control Service がそのサブネット内に永続的ボリュームを作成できるようにする必要があります。Azure NetApp Files を使用すると、 VNet 内の委譲されたサブネットを 1 つだけ設定できます。

ピア VNet を使用している場合は、ピアリング接続の両側がオンラインである必要があります。 Kubernetes クラスタが配置されている VNet と、 Azure NetApp Files 委任サブネットが設定された VNet です。

ステップ

1. "Azure NetApp Files のドキュメントに従って、サブネットを Azure NetApp Files に委譲します"。

完了したら

10 分ほど待ってから、委任されたサブネットで実行されているクラスタを検出します。

Azure サービスプリンシパルを作成します

Astra Control Service には、 Contributor ロールを割り当てられた Azure サービスプリンシパルが必要です。Astra Control Service では、このサービスプリンシパルを使用して、 Kubernetes アプリケーションデータの管理をお客様に代わって容易にします。

サービスプリンシパルは、アプリケーション、サービス、およびツールで使用するために特別に作成される ID です。サービスプリンシパルにロールを割り当てると、 Azure の特定のリソースへのアクセスが制限されます。

Azure CLI を使用してサービスプリンシパルを作成するには、次の手順に従います。出力は JSON ファイルに保存し、後で Astra Control Service に提供する必要があります。 "CLI の使用の詳細については、 Azure のドキュメントを参照してください"。

次の手順では、サービスプリンシパルを作成する権限があり、 Microsoft Azure SDK （ AZ コマンド）がマシンにインストールされていることを前提としています。

要件

- サービスプリンシパルは、通常の認証を使用する必要があります。証明書はサポートされていません。
- サービスプリンシパルに、 Azure サブスクリプションへの寄稿者または所有者のアクセス権が付与されている必要があります。
- スコープ用に選択するサブスクリプションまたはリソースグループには、 AKS クラスタと Azure NetApp Files アカウントが含まれている必要があります。

手順

1. AKS クラスタが存在するサブスクリプションとテナント ID を特定します（これは Astra Control Service で管理するクラスタです）。

```
az configure --list-defaults
az account list --output table
```

2. サブスクリプション全体を使用するかリソースグループを使用するかに応じて、次のいずれかの操作を行います。
   - サービスプリンシパルを作成し、 Contributor ロールを割り当て、クラスタが存在するサブスクリプション全体にスコープを指定します。

     ```
     az ad sp create-for-rbac --name service-principal-name --role
     contributor --scopes /subscriptions/SUBSCRIPTION-ID
     ```

   - サービスプリンシパルを作成し、 Contributor ロールを割り当て、クラスタが存在するリソースグループを指定します。

     ```
     az ad sp create-for-rbac --name service-principal-name --role
     contributor --scopes /subscriptions/SUBSCRIPTION-
     ID/resourceGroups/RESOURCE-GROUP-ID
     ```

3. 作成された Azure CLI 出力は JSON ファイルとして保存します。

   Astra Control Service が AKS クラスタを検出し、 Kubernetes のデータ管理処理を管理できるように、このファイルを指定する必要があります。 "Astra Control Service での資格情報の管理について説明します"。

4. オプション： JSON ファイルにサブスクリプション ID を追加し、ファイルを選択すると Astra Control Service によって自動的に ID が入力されるようにします。

   それ以外の場合は、表示されたときに Astra Control Service でサブスクリプション ID を入力する必要があります。

   - 例 *

```
{
  "appId": "0db3929a-bfb0-4c93-baee-aaf8",
  "displayName": "sp-example-dev-sandbox",
  "name": "http://sp-example-dev-sandbox",
  "password": "mypassword",
  "tenant": "011cdf6c-7512-4805-aaf8-7721afd8ca37",
  "subscriptionId": "99ce999a-8c99-99d9-a9d9-99cce99f99ad"
}
```

5. オプション：サービスプリンシパルをテストします。サービスプリンシパルで使用するスコープに応じて、次のコマンド例を選択します。

サブスクリプションの範囲

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az group list --subscription SUBSCRIPTION-ID
az aks list --subscription SUBSCRIPTION-ID
az storage container list --account-name STORAGE-ACCOUNT-NAME
```

リソースグループのスコープ

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az aks list --subscription SUBSCRIPTION-ID --resource-group RESOURCE-
GROUP-ID
```

オプション：Azureバックアップバケットの冗長性を設定する

Azureバックアップバケットには、より永続性の高い冗長性レベルを設定できます。デフォルトでは、バケットAstra Control ServiceはAzure Kubernetes Serviceのバックアップを保存するためにを使用し、ローカルのRedundant Storage（LRS）冗長性オプションを使用します。Azureバケットでより永続性の高い冗長性オプションを使用するには、次の作業を行う必要があります。

手順

1. 使用する必要がある冗長性レベルを使用するAzureストレージアカウントを作成します "以下の手順を参照して"。
2. を使用して、新しいストレージアカウントにAzureコンテナを作成します "以下の手順を参照して"。
3. コンテナをバケットとしてAstra Control Serviceに追加します。を参照してください "追加のバケットを追加します"。
4. （オプション）新しく作成したバケットをAzureバックアップのデフォルトバケットとして使用するには、バケットをAzureのデフォルトバケットとして設定します。を参照してください "デフォルトバケットを変更する"。

Azure で管理されているディスクを使用して Microsoft Azure をセットアップする

Microsoft Azure サブスクリプションを準備してから、 Astra Control Service で Azure Kubernetes Service クラスタを管理するには、いくつかの手順を実行する必要があります。Azure で管理されているディスクをストレージバックエンドとして使用する場合は、次の手順に従います。

Azure のセットアップのクイックスタート

これらの手順を実行してすぐに作業を開始するか、残りのセクションまでスクロールして詳細を確認してください。

[1つ] Azure Kubernetes Service の Astra Control Service の要件を確認

クラスタが正常で、サポートされているバージョンのKubernetesを実行していること、ノードプールがオンラインでLinuxを実行していることなどを確認します。 このステップの詳細をご覧ください。

[2 つ] Microsoft Azure に登録

Microsoft Azure アカウントを作成します。 このステップの詳細をご覧ください。

[3つ] Azure サービスプリンシパルを作成します

Contributor ロールを持つ Azure サービスプリンシパルを作成します。 このステップの詳細をご覧ください。

[4.] CSI ドライバの詳細を設定します

CSI ドライバと連携するように Azure サブスクリプションとクラスタを設定する必要があります。 このステップの詳細をご覧ください。

[5 つ] オプション：Azureバックアップバケットの冗長性を設定する

デフォルトでは、バケットAstra Control ServiceはAzure Kubernetes Serviceのバックアップを保存するためにを使用し、ローカルのRedundant Storage（LRS）冗長性オプションを使用します。オプションとして、Azureバケットに永続性レベルの冗長性を設定することができます。 このステップの詳細をご覧ください。

Azure Kubernetes Service クラスタの要件

Kubernetes クラスタを Astra Control Service から検出して管理できるようにするには、 Kubernetes クラスタが次の要件を満たしている必要があります。

Kubernetes のバージョン
: クラスタでKubernetesバージョン1.26~1.28が実行されている必要があります。

イメージタイプ
: すべてのノードプールのイメージタイプは Linux である必要があります。

クラスタの状態
: クラスタが正常な状態で稼働し、少なくとも 1 つのオンラインワーカーノードがあり、ワーカーノードが障害状態でない必要があります。

Azure リージョン
: ベストプラクティスとして、 Azure NetApp Files をストレージバックエンドとして使用しない場合でも、そのリージョンを選択することを推奨します。これにより、パフォーマンス要件が変わった場合でも、 Azure NetApp Files をストレージバックエンドとして簡単に使用できるようになります。 "Azure 製品を地域別に表示します"。

CSI ドライバ
: クラスタには適切な CSI ドライバがインストールされている必要があります。

Microsoft Azure に登録

Microsoft Azure アカウントをお持ちでない場合は、まず Microsoft Azure にサインアップします。

手順

1. にアクセスします "Azure サブスクリプションページ" をクリックして Azure サービスに登録してください。
2. プランを選択し、指示に従ってサブスクリプションを完了します。

Azure サービスプリンシパルを作成します

Astra Control Service には、 Contributor ロールを割り当てられた Azure サービスプリンシパルが必要です。Astra Control Service では、このサービスプリンシパルを使用して、 Kubernetes アプリケーションデータの管理をお客様に代わって容易にします。

サービスプリンシパルは、アプリケーション、サービス、およびツールで使用するために特別に作成される ID です。サービスプリンシパルにロールを割り当てると、 Azure の特定のリソースへのアクセスが制限されます。

Azure CLI を使用してサービスプリンシパルを作成するには、次の手順に従います。出力は JSON ファイルに保存し、後で Astra Control Service に提供する必要があります。 "CLI の使用の詳細については、 Azure のドキュメントを参照してください"。

次の手順では、サービスプリンシパルを作成する権限があり、 Microsoft Azure SDK （ AZ コマンド）がマシンにインストールされていることを前提としています。

要件

- サービスプリンシパルは、通常の認証を使用する必要があります。証明書はサポートされていません。
- サービスプリンシパルに、 Azure サブスクリプションへの寄稿者または所有者のアクセス権が付与されている必要があります。
- スコープ用に選択するサブスクリプションまたはリソースグループには、 AKS クラスタと Azure NetApp Files アカウントが含まれている必要があります。

手順

1. AKS クラスタが存在するサブスクリプションとテナント ID を特定します（これは Astra Control Service で管理するクラスタです）。

```
az configure --list-defaults
az account list --output table
```

2. サブスクリプション全体を使用するかリソースグループを使用するかに応じて、次のいずれかの操作を行います。
    - サービスプリンシパルを作成し、 Contributor ロールを割り当て、クラスタが存在するサブスクリプション全体にスコープを指定します。

```
az ad sp create-for-rbac --name service-principal-name --role
contributor --scopes /subscriptions/SUBSCRIPTION-ID
```

- サービスプリンシパルを作成し、 Contributor ロールを割り当て、クラスタが存在するリソースグループを指定します。

```
az ad sp create-for-rbac --name service-principal-name --role
contributor --scopes /subscriptions/SUBSCRIPTION-
ID/resourceGroups/RESOURCE-GROUP-ID
```

3. 作成された Azure CLI 出力は JSON ファイルとして保存します。

   Astra Control Service が AKS クラスタを検出し、 Kubernetes のデータ管理処理を管理できるように、このファイルを指定する必要があります。 "Astra Control Service での資格情報の管理について説明します"。

4. オプション： JSON ファイルにサブスクリプション ID を追加し、ファイルを選択すると Astra Control Service によって自動的に ID が入力されるようにします。

   それ以外の場合は、表示されたときに Astra Control Service でサブスクリプション ID を入力する必要があります。

   - 例 *

```
{
  "appId": "0db3929a-bfb0-4c93-baee-aaf8",
  "displayName": "sp-example-dev-sandbox",
  "name": "http://sp-example-dev-sandbox",
  "password": "mypassword",
  "tenant": "011cdf6c-7512-4805-aaf8-7721afd8ca37",
  "subscriptionId": "99ce999a-8c99-99d9-a9d9-99cce99f99ad"
}
```

5. オプション：サービスプリンシパルをテストします。サービスプリンシパルで使用するスコープに応じて、次のコマンド例を選択します。

   サブスクリプションの範囲

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az group list --subscription SUBSCRIPTION-ID
az aks list --subscription SUBSCRIPTION-ID
az storage container list --account-name STORAGE-ACCOUNT-NAME
```

リソースグループのスコープ

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az aks list --subscription SUBSCRIPTION-ID --resource-group RESOURCE-
GROUP-ID
```

CSI ドライバの詳細を設定します

Azure管理ディスクをAstra Control Serviceとともに使用するには、必要なCSIドライバをインストールする必要があります。

Azure サブスクリプションで CSI ドライバ機能を有効にします

CSI ドライバをインストールする前に、 Azure サブスクリプションで CSI ドライバ機能を有効にする必要があります。

手順

1. Azure コマンドラインインターフェイスを開きます。
2. 次のコマンドを実行してドライバを登録します。

```
az feature register --namespace "Microsoft.ContainerService" --name
"EnableAzureDiskFileCSIDriver"
```

3. 次のコマンドを実行して、変更が伝播されることを確認します。

```
az provider register -n Microsoft.ContainerService
```

次のような出力が表示されます。

```
{
"id": "/subscriptions/b200155f-001a-43be-87be-
3edde83acef4/providers/Microsoft.Features/providers/Microsoft.ContainerSer
vice/features/EnableAzureDiskFileCSIDriver",
"name": "Microsoft.ContainerService/EnableAzureDiskFileCSIDriver",
"properties": {
   "state": "Registering"
},
"type": "Microsoft.Features/providers/features"
}
```

Azure 管理ディスク **CSI** ドライバを **Azure Kubernetes Service** クラスタにインストールします

Azure CSI ドライバをインストールして準備を完了できます。

ステップ

1. に進みます "Microsoft CSI ドライバのマニュアル"。
2. 指示に従って、必要な CSI ドライバをインストールします。

オプション：**Azure**バックアップバケットの冗長性を設定する

Azureバックアップバケットには、より永続性の高い冗長性レベルを設定できます。デフォルトでは、バケットAstra Control ServiceはAzure Kubernetes Serviceのバックアップを保存するためにを使用し、ローカルのRedundant Storage（LRS）冗長性オプションを使用します。Azureバケットでより永続性の高い冗長性オプションを使用するには、次の作業を行う必要があります。

手順

1. 使用する必要がある冗長性レベルを使用するAzureストレージアカウントを作成します "以下の手順を参照して"。
2. を使用して、新しいストレージアカウントにAzureコンテナを作成します "以下の手順を参照して"。
3. コンテナをバケットとしてAstra Control Serviceに追加します。を参照してください "追加のバケットを追加します"。
4. （オプション）新しく作成したバケットをAzureバックアップのデフォルトバケットとして使用するには、バケットをAzureのデフォルトバケットとして設定します。を参照してください "デフォルトバケットを変更する"。

著作権に関する情報

商標に関する情報