AWS C2S で Cloud Volumes ONTAP を使用する方法を確認します 環境

Cloud Manager

Ben Cammett
March 15, 2021

目次

AWS C2S で Cloud Volumes ONTAP を使用する方法を確認します 環境

標準の AWS リージョンと同様に、 AWS Commercial クラウドサービス（ C2S ）環境で Cloud Manager を使用して Cloud Volumes ONTAP を導入できます。 C2S はクラウドストレージにエンタープライズクラスの機能を提供します。

C2S でサポートされている機能

C2S 環境の Cloud Manager から使用可能な機能は次のとおりです。

- Cloud Volumes ONTAP
- データレプリケーション
- 監査のスケジュール

Cloud Volumes ONTAP の場合は、シングルノードシステムまたは HA ペアを作成できます。どちらのライセンスオプションも使用できます。従量課金制とお客様所有のライセンス（ BYOL ）です。

S3 へのデータ階層化は、 C2S の Cloud Volumes ONTAP でもサポートされています。

制限

ネットアップのどのクラウドサービスも Cloud Manager からは使用できません。

C2S 環境ではインターネットにアクセスできないため、次の機能も使用できません。

- NetApp Cloud Central との統合
- Cloud Manager からのソフトウェアの自動アップグレード
- NetApp AutoSupport
- AWS の Cloud Volumes ONTAP リソースのコスト情報

導入の概要

C2S で Cloud Volumes ONTAP を使用するにはいくつかの手順を実行します。

1. AWS 環境の準備

   これには、ネットワークの設定、 Cloud Volumes ONTAP への登録、権限の設定、および必要に応じて AWS KMS のセットアップが含まれます。

2. Connector のインストールと Cloud Manager のセットアップ

   Cloud Manager を使用して Cloud Volumes ONTAP を導入するには、コネクタを作成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（ Cloud Volumes ONTAP を含む）を管理できます。

Connector インスタンスにインストールされているソフトウェアから Cloud Manager にログインします。

3. Cloud Manager から Cloud Volumes ONTAP を起動しています。

以下に、各手順について説明します。

AWS 環境を準備

AWS 環境はいくつかの要件を満たす必要があります。

ネットワークをセットアップします

Cloud Volumes ONTAP が適切に動作するように AWS ネットワークをセットアップします。

手順

1. コネクタインスタンスと Cloud Volumes ONTAP インスタンスを起動する VPC とサブネットを選択します。
2. VPC とサブネットがコネクタと Cloud Volumes ONTAP 間の接続をサポートしていることを確認します。
3. S3 サービスへの vPC エンドポイントをセットアップします。

   Cloud Volumes ONTAP から低コストのオブジェクトストレージにコールドデータを階層化する場合は、VPC エンドポイントが必要です。

Cloud Volumes ONTAP に登録します

Cloud Manager から Cloud Volumes ONTAP を導入するには、 Marketplace サブスクリプションが必要です。

手順

1. AWS Intelligence Community Marketplace にアクセスして、 Cloud Volumes ONTAP を検索します。
2. 導入を計画しているサービスを選択します。
3. 条件を確認し、 [**Accept**](同意する) をクリックします。
4. 導入を計画している場合は、他のサービスについても同じ手順を繰り返します。

   Cloud Volumes ONTAP インスタンスを起動するには、 Cloud Manager を使用する必要があります。Cloud Volumes ONTAP インスタンスを EC2 コンソールから起動しないでください。

権限を設定します

AWS Commercial クラウドサービス環境でアクションを実行するために必要な権限を Cloud Manager と Cloud Volumes ONTAP に提供する IAM ポリシーとロールを設定する。

次の項目について、 IAM ポリシーと IAM ロールを 1 つずつ用意する必要があります。

- コネクタインスタンス
- Cloud Volumes ONTAP インスタンス
- Cloud Volumes ONTAP HA メディエーターインスタンス （ HA ペアを導入する場合）

手順

1. AWS IAM コンソールに移動し、 * Policies * をクリックします。
2. コネクタインスタンスのポリシーを作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
```

```
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
```

```
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

3. Cloud Volumes ONTAP のポリシーを作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

4. Cloud Volumes ONTAP HA ペアを導入する場合は、 HA メディエーターのポリシーを作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

5. 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関連付けます。

   ポリシーと同様に、コネクタ用の IAM ロールが 1 つ、 Cloud Volumes ONTAP ノード用の IAM ロールが 1 つ、 HA メディエーター用の IAM ロールが 1 つ（ HA ペアを導入する場合）必要です。

   コネクタインスタンスを起動するときに、コネクタ IAM ロールを選択する必要があります。

   Cloud Volumes ONTAP の IAM ロールと HA メディエーターは、 Cloud Manager から Cloud Volumes ONTAP の作業環境を作成するときに選択できます。

AWS KMS を設定します

Cloud Volumes ONTAP で Amazon 暗号化を使用する場合は、 AWS Key Management Service の要件を満たしていることを確認します。

手順

1. アクティブな Customer Master Key （ CMK ；カスタマーマスターキー）がアカウントまたは別の AWS アカウントに存在することを確認します。

   CMK は、 AWS 管理の CMK または顧客管理の CMK にすることができます。

2. Cloud Volumes ONTAP を導入するアカウントとは別の AWS アカウントに CMK を配置する場合は、そのキーの ARN を取得する必要があります。

   Cloud Volumes ONTAP システムの作成時には、 Cloud Manager への ARN の提供が必要になります。

3. Cloud Manager インスタンス用の IAM ロールを CMK のキーユーザのリストに追加します。

   これにより、 Cloud Manager には、 Cloud Volumes ONTAP で CMK を使用する権限が与えられます。

Cloud Manager をインストールしてセットアップする

AWS で Cloud Volumes ONTAP システムを起動するには、まず AWS Marketplace から Connector インスタンスを起動してから、ログインして Cloud Manager をセットアップする必要があります。

手順

1. Privacy Enhanced Mail （ PEM ） Base-64 でエンコードされた X.509 形式の認証局（ CA ）が署名したルート証明書を取得する証明書を入手するには、組織のポリシーと手順を参照してください。

   セットアッププロセス中に証明書をアップロードする必要があります。Cloud Manager は、 HTTPS 経由で AWS に要求を送信する際に信頼された証明書を使用します。

2. コネクタインスタンスを起動します。
   a. AWS Intelligence Community Marketplace の Cloud Manager のページに移動します。
   b. Custom Launch タブで、 EC2 コンソールからインスタンスを起動するオプションを選択します。
   c. プロンプトに従って、インスタンスを設定します。

      インスタンスを設定する際には、次の点に注意してください。

- t3.xlarge をお勧めします。
- AWS 環境の準備の際に作成した IAM ロールを選択する必要があります。
- デフォルトのストレージオプションはそのままにしておく必要があります。
- コネクタに必要な接続方法は、 SSH 、 HTTP 、 HTTPS です。

3. コネクタインスタンスに接続されているホストから Cloud Manager をセットアップします。
   a. Web ブラウザを開き、次の URL を入力します。 ""
   b. AWS サービスに接続するためのプロキシサーバを指定します。
   c. 手順 1 で取得した証明書をアップロードします。
   d. セットアップウィザードの手順に従って、 Cloud Manager をセットアップします。
      - * System Details * ： Cloud Manager インスタンスの名前を入力し、会社名を入力します。
      - * ユーザの作成 * ： Cloud Manager の管理に使用する管理者ユーザを作成します。
      - * レビュー * ：詳細を確認し、エンドユーザーライセンス契約を承認します。
   e. CA 署名証明書のインストールを完了するには、 EC2 コンソールからコネクタインスタンスを再起動します。
4. コネクタが再起動したら、セットアップウィザードで作成した管理者ユーザアカウントを使用してログインします。

Cloud Volumes ONTAP を起動します

Cloud Manager で新しい作業環境を作成することで、 AWS Commercial クラウドサービス環境で Cloud Volumes ONTAP インスタンスを起動できます。

必要なもの

- ライセンスを購入した場合は、ネットアップから受け取ったライセンスファイルが必要です。ライセンスファイルは JSON 形式の .NLF ファイルです。
- HA メディエーターへのキーベースの SSH 認証を有効にするには、キーペアが必要です。

手順

1. 作業環境ページで、 * 作業環境の追加 * をクリックします。
2. 作成（ Create ）で、 Cloud Volumes ONTAP または Cloud Volumes ONTAP HA を選択します。
3. ウィザードの手順に従って、 Cloud Volumes ONTAP システムを起動します。

   ウィザードを完了する際には、次の点に注意してください。

   - 複数のアベイラビリティゾーンに Cloud Volumes ONTAP HA を導入する場合は、公開時点で AWS Commercial クラウドサービス環境で使用可能な AZ は 2 つだけだったため、次のように構成を導入します。
     - ノード 1 ：アベイラビリティゾーン A
     - ノード 2 ：アベイラビリティゾーン B
     - メディエーター：アベイラビリティゾーン A または B
   - 生成されたセキュリティグループを使用するには、デフォルトのオプションをそのままにしておく必

要があります。

事前定義されたセキュリティグループには、 Cloud Volumes ONTAP が正常に動作するために必要なルールが含まれています。独自の要件がある場合は、下のセキュリティグループのセクションを参照してください。

- AWS 環境の準備の際に作成した IAM ロールを選択する必要があります。
- 基盤となる AWS ディスクタイプは Cloud Volumes ONTAP の初期ボリューム用です。

  以降のボリュームでは、別のディスクタイプを選択できます。

- AWS ディスクのパフォーマンスはディスクサイズに依存します。

  必要なパフォーマンスを継続的に提供するディスクサイズを選択する必要があります。EBS のパフォーマンスの詳細については、 AWS のドキュメントを参照してください。

- ディスクサイズは、システム上のすべてのディスクのデフォルトサイズです。

  

  あとでサイズを変更する必要がある場合は、 Advanced allocation オプションを使用して、特定のサイズのディスクを使用するアグリゲートを作成できます。

- Storage Efficiency 機能を使用すると、ストレージ利用率を高めて、必要なストレージの総容量を減らすことができます。

Cloud Manager が Cloud Volumes ONTAP インスタンスを起動します。タイムラインで進行状況を追跡できます。

セキュリティグループのルール

Cloud Manager で作成されるセキュリティグループには、 Cloud Manager と Cloud Volumes ONTAP がクラウドで正常に動作するために必要なインバウンドとアウトバウンドのルールが含まれています。テスト目的または独自のセキュリティグループを使用する場合は、ポートを参照してください。

コネクタのセキュリティグループ

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 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

Cloud Volumes ONTAP のセキュリティグループ

Cloud Volumes ONTAP ノード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

定義済みセキュリティグループのインバウンドルールの送信元は 0.0.0.0/0 です。

プロトコル	ポート	目的
すべての ICMP	すべて	インスタンスの ping を実行します
HTTP	80	クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTP アクセス
HTTPS	443	クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTPS アクセス
SSH	22	クラスタ管理 LIF またはノード管理 LIF の IP アドレスへの SSH アクセス
TCP	111	NFS のリモートプロシージャコール
TCP	139	CIFS の NetBIOS サービスセッション
TCP	161-162	簡易ネットワーク管理プロトコル
TCP	445	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
TCP	635	NFS マウント
TCP	749	Kerberos
TCP	2049	NFS サーバデーモン
TCP	3260	iSCSI データ LIF を介した iSCSI アクセス
TCP	4045	NFS ロックデーモン
TCP	4046	NFS のネットワークステータスモニタ
TCP	10000	NDMP を使用したバックアップ
TCP	11104	SnapMirror のクラスタ間通信セッションの管理
TCP	11105	クラスタ間 LIF を使用した SnapMirror データ転送
UDP	111	NFS のリモートプロシージャコール

プロトコル	ポート	目的
UDP	161-162	簡易ネットワーク管理プロトコル
UDP	635	NFS マウント
UDP	2049	NFS サーバデーモン
UDP	4045	NFS ロックデーモン
UDP	4046	NFS のネットワークステータスモニタ
UDP	4049	NFS rquotad プロトコル

アウトバウンドルール

Cloud Volumes ONTAP 用の定義済み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 ICMP	すべて	すべての発信トラフィック
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

HA メディエーターの外部セキュリティグループ

Cloud Volumes ONTAP HA Mediator 用に事前定義された外部セキュリティグループには、次のインバウンドルールとアウトバウンドルールが含まれています。

インバウンドルール

インバウンドルールのソースは、コネクタが存在する VPC からのトラフィックです。

プロトコル	ポート	目的
SSH	22	HA メディエータへの SSH 接続
TCP	3000	コネクタからの RESTful API アクセス

アウトバウンドルール

HA Mediator 用の定義済み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

HA メディエーターの内部セキュリティグループ

Cloud Volumes ONTAP HA Mediator 用に事前定義された内部セキュリティグループには、次のルールが含ま

れています。Cloud　Manager　は常にこのセキュリティグループを作成します。独自のオプションはありません。

インバウンドルール

事前定義されたセキュリティグループには、次の着信ルールが含まれています。

プロトコル	ポート	目的
すべてのトラフィック	すべて	HA メディエータと HA ノード間の通信

アウトバウンドルール

定義済みのセキュリティグループには、次の発信ルールが含まれます。

プロトコル	ポート	目的
すべてのトラフィック	すべて	HA メディエータと HA ノード間の通信