Get started with Cloud Volumes ONTAP in the AWS C2S environment

Cloud Manager

Ben Cammett
June 11, 2021

Table of Contents

Get started with Cloud Volumes ONTAP in the AWS C2S environment

Similar to a standard AWS region, you can use Cloud Manager in the AWS Commercial Cloud Services (C2S) environment to deploy Cloud Volumes ONTAP, which provides enterprise-class features for your cloud storage. AWS C2S is a closed region specific to the U.S. Intelligence Community; the instructions on this page only apply to AWS C2S region users.

Supported features in C2S

The following features are available from Cloud Manager in the C2S environment:

- Cloud Volumes ONTAP
- Data replication
- A timeline for auditing

For Cloud Volumes ONTAP, you can create a single node system or an HA pair. Both licensing options are available: pay-as-you-go and bring your own license (BYOL).

Data tiering to S3 is also supported with Cloud Volumes ONTAP in C2S.

Limitations

None of NetApp's cloud services are available from Cloud Manager.

Because there's no internet access in the C2S environment, the following features aren't available either:

- Integration with NetApp Cloud Central
- Automated software upgrades from Cloud Manager
- NetApp AutoSupport
- AWS cost information for Cloud Volumes ONTAP resources

Deployment overview

Getting started with Cloud Volumes ONTAP in C2S includes a few steps.

1. Preparing your AWS environment.

   This includes setting up networking, subscribing to Cloud Volumes ONTAP, setting up permissions, and optionally setting up the AWS KMS.

2. Installing the Connector and setting up Cloud Manager.

   Before you can start using Cloud Manager to deploy Cloud Volumes ONTAP, you'll need to create a *Connector*. The Connector enables Cloud Manager to manage resources and processes within your public cloud environment (this includes Cloud Volumes ONTAP).

You'll log in to Cloud Manager from the software that gets installed on the Connector instance.

3. Launching Cloud Volumes ONTAP from Cloud Manager.

Each of these steps are described below.

Prepare your AWS environment

Your AWS environment must meet a few requirements.

Set up your networking

Set up your AWS networking so Cloud Volumes ONTAP can operate properly.

Steps

1. Choose the VPC and subnets in which you want to launch the Connector instance and Cloud Volumes ONTAP instances.
2. Ensure that your VPC and subnets will support connectivity between the Connector and Cloud Volumes ONTAP.
3. Set up a VPC endpoint to the S3 service.

   A VPC endpoint is required if you want to tier cold data from Cloud Volumes ONTAP to low-cost object storage.

Subscribe to Cloud Volumes ONTAP

A Marketplace subscription is required to deploy Cloud Volumes ONTAP from Cloud Manager.

Steps

1. Go to the AWS Intelligence Community Marketplace and search for Cloud Volumes ONTAP.
2. Select the offering that you plan to deploy.
3. Review the terms and click **Accept**.
4. Repeat these steps for the other offerings, if you plan to deploy them.

   You must use Cloud Manager to launch Cloud Volumes ONTAP instances. You must not launch Cloud Volumes ONTAP instances from the EC2 console.

Set up permissions

Set up IAM policies and roles that provide Cloud Manager and Cloud Volumes ONTAP with the permissions that they need to perform actions in the AWS Commercial Cloud Services environment.

You need an IAM policy and IAM role for each of the following:

- The Connector instance
- Cloud Volumes ONTAP instances
- The Cloud Volumes ONTAP HA mediator instance (if you want to deploy HA pairs)

Steps

1. Go to the AWS IAM console and click **Policies**.
2. Create a policy for the Connector instance.

```
{
    "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. Create a policy for Cloud Volumes ONTAP.

```
{
    "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. If you plan to deploy a Cloud Volumes ONTAP HA pair, create a policy for the HA mediator.

```
{
    "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. Create IAM roles with the role type Amazon EC2 and attach the policies that you created in the previous steps.

   Similar to the policies, you should have one IAM role for the Connector, one for the Cloud Volumes ONTAP nodes, and one for the HA mediator (if you want to deploy HA pairs).

   You must select the Connector IAM role when you launch the Connector instance.

   You can select the IAM roles for Cloud Volumes ONTAP and the HA mediator when you create a Cloud Volumes ONTAP working environment from Cloud Manager.

Set up the AWS KMS

If you want to use Amazon encryption with Cloud Volumes ONTAP, ensure that requirements are met for the AWS Key Management Service.

Steps

1. Ensure that an active Customer Master Key (CMK) exists in your account or in another AWS account.

   The CMK can be an AWS-managed CMK or a customer-managed CMK.

2. If the CMK is in an AWS account separate from the account where you plan to deploy Cloud Volumes ONTAP, then you need to obtain the ARN of that key.

   You'll need to provide the ARN to Cloud Manager when you create the Cloud Volumes ONTAP system.

3. Add the IAM role for the Cloud Manager instance to the list of key users for a CMK.

   This gives Cloud Manager permissions to use the CMK with Cloud Volumes ONTAP.

Install and set up Cloud Manager

Before you can launch Cloud Volumes ONTAP systems in AWS, you must first launch the Connector instance from the AWS Marketplace and then log in and set up Cloud Manager.

Steps

1. Obtain a root certificate signed by a certificate authority (CA) in the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format. Consult your organization's policies and procedures for obtaining the certificate.

   You'll need to upload the certificate during the setup process. Cloud Manager uses the trusted certificate when sending requests to AWS over HTTPS.

2. Launch the Connector instance:
   a. Go to the AWS Intelligence Community Marketplace page for Cloud Manager.
   b. On the Custom Launch tab, choose the option to launch the instance from the EC2 console.
   c. Follow the prompts to configure the instance.

      Note the following as you configure the instance:

      - We recommend t3.xlarge.
      - You must choose the IAM role that you created when preparing your AWS environment.

        - You should keep the default storage options.
        - The required connection methods for the Connector are as follows: SSH, HTTP, and HTTPS.
3. Set up Cloud Manager from a host that has a connection to the Connector instance:
    a. Open a web browser and enter the following URL: http://ipaddress:80
    b. Specify a proxy server for connectivity to AWS services.
    c. Upload the certificate that you obtained in step 1.
    d. Complete the steps in the Setup wizard to set up Cloud Manager.
        - **System Details**: Enter a name for this instance of Cloud Manager and provide your company name.
        - **Create User**: Create the Admin user that you'll use to administer Cloud Manager.
        - **Review**: Review the details and approve the end user license agreement.
    e. To complete installation of the CA-signed certificate, restart the Connector instance from the EC2 console.
4. After the Connector restarts, log in using the administrator user account that you created in the Setup wizard.

Launch Cloud Volumes ONTAP

You can launch Cloud Volumes ONTAP instances in the AWS Commercial Cloud Services environment by creating new working environments in Cloud Manager.

What you'll need

- If you purchased a license, you must have the license file that you received from NetApp. The license file is a .NLF file in JSON format.
- A key pair is required to enable key-based SSH authentication to the HA mediator.

Steps

1. On the Working Environments page, click **Add Working Environment**.
2. Under Create, select Cloud Volumes ONTAP or Cloud Volumes ONTAP HA.
3. Complete the steps in the wizard to launch the Cloud Volumes ONTAP system.

    Note the following as you complete the wizard:

    - If you want to deploy Cloud Volumes ONTAP HA in multiple Availability Zones, deploy the configuration as follows because only two AZs were available in the AWS Commercial Cloud Services environment at the time of publication:
        - Node 1: Availability Zone A
        - Node 2: Availability Zone B
        - Mediator: Availability Zone A or B
    - You should leave the default option to use a generated security group.

      The predefined security group includes the rules that Cloud Volumes ONTAP needs to operate successfully. If you have a requirement to use your own, you can refer to the security group section below.

- You must choose the IAM role that you created when preparing your AWS environment.
- The underlying AWS disk type is for the initial Cloud Volumes ONTAP volume.

  You can choose a different disk type for subsequent volumes.

- The performance of AWS disks is tied to disk size.

  You should choose the disk size that gives you the sustained performance that you need. Refer to AWS documentation for more details about EBS performance.

- The disk size is the default size for all disks on the system.

  

  If you need a different size later, you can use the Advanced allocation option to create an aggregate that uses disks of a specific size.

- Storage efficiency features can improve storage utilization and reduce the total amount of storage that you need.

Result

Cloud Manager launches the Cloud Volumes ONTAP instance. You can track the progress in the timeline.

Security group rules

Cloud Manager creates security groups that include the inbound and outbound rules that Cloud Manager and Cloud Volumes ONTAP need to operate successfully in the cloud. You might want to refer to the ports for testing purposes or if you prefer to use your own security groups.

Security group for the Connector

The security group for the Connector requires both inbound and outbound rules.

Inbound rules

Protocol	Port	Purpose
SSH	22	Provides SSH access to the Connector host
HTTP	80	Provides HTTP access from client web browsers to the local user interface
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface

Outbound rules

The predefined security group for the Connector includes the following outbound rules.

Protocol	Port	Purpose
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

Security group for Cloud Volumes ONTAP

The security group for Cloud Volumes ONTAP nodes requires both inbound and outbound rules.

Inbound rules

The source for inbound rules in the predefined security group is 0.0.0.0/0.

Protocol	Port	Purpose
All ICMP	All	Pinging the instance
HTTP	80	HTTP access to the System Manager web console using the IP address of the cluster management LIF
HTTPS	443	HTTPS access to the System Manager web console using the IP address of the cluster management LIF
SSH	22	SSH access to the IP address of the cluster management LIF or a node management LIF
TCP	111	Remote procedure call for NFS
TCP	139	NetBIOS service session for CIFS
TCP	161-162	Simple network management protocol
TCP	445	Microsoft SMB/CIFS over TCP with NetBIOS framing
TCP	635	NFS mount
TCP	749	Kerberos
TCP	2049	NFS server daemon
TCP	3260	iSCSI access through the iSCSI data LIF
TCP	4045	NFS lock daemon
TCP	4046	Network status monitor for NFS
TCP	10000	Backup using NDMP
TCP	11104	Management of intercluster communication sessions for SnapMirror
TCP	11105	SnapMirror data transfer using intercluster LIFs
UDP	111	Remote procedure call for NFS
UDP	161-162	Simple network management protocol
UDP	635	NFS mount
UDP	2049	NFS server daemon
UDP	4045	NFS lock daemon
UDP	4046	Network status monitor for NFS
UDP	4049	NFS rquotad protocol

Outbound rules

The predefined security group for Cloud Volumes ONTAP includes the following outbound rules.

Protocol	Port	Purpose
All ICMP	All	All outbound traffic
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

External security group for the HA mediator

The predefined external security group for the Cloud Volumes ONTAP HA mediator includes the following inbound and outbound rules.

Inbound rules

The source for inbound rules is traffic from the VPC where the Connector resides.

Protocol	Port	Purpose
SSH	22	SSH connections to the HA mediator
TCP	3000	RESTful API access from the Connector

Outbound rules

The predefined security group for the HA mediator includes the following outbound rules.

Protocol	Port	Purpose
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

Internal security group for the HA mediator

The predefined internal security group for the Cloud Volumes ONTAP HA mediator includes the following rules. Cloud Manager always creates this security group. You don’t have the option to use your own.

Inbound rules

The predefined security group includes the following inbound rules.

Protocol	Port	Purpose
All traffic	All	Communication between the HA mediator and HA nodes

Outbound rules

The predefined security group includes the following outbound rules.

Protocol	Port	Purpose
All traffic	All	Communication between the HA mediator and HA nodes