



OnCommand® Cloud Manager 3.6.4

Quick Start Guide

For the AWS Commercial Cloud Services Environment

2 May 2019
doccomments@netapp.com



Cloud Manager and Cloud Volumes ONTAP in the 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. Most features that are available in a standard AWS region are also available in the Commercial Cloud Services environment.

The following limitations apply to the AWS Commercial Cloud Services environment:

- At the time of publication, the environment includes only two Availability Zones.
If you deploy Cloud Volumes ONTAP HA in multiple Availability Zones, the mediator must be in the same Availability Zone as one of the Cloud Volumes ONTAP HA nodes.
- Data tiering to S3 is not supported.
- The sync to S3 feature using the NetApp Cloud Sync service is not supported.
- The Volume View in Cloud Manager is not supported.
- Because there is no internet access in the C2S environment, the following features are not supported:
 - Integration with NetApp Cloud Central
 - Automated software upgrades from Cloud Manager
 - NetApp AutoSupport
 - AWS cost information for Cloud Volumes ONTAP resources

Preparing your AWS environment

Your AWS environment must meet a few requirements so that Cloud Manager and Cloud Volumes ONTAP operate correctly in the AWS Commercial Cloud Services environment.

Steps

1. Choose the VPC and subnets in which you want to launch the Cloud Manager instance and Cloud Volumes ONTAP instances.

If you plan to launch the Cloud Manager instance in a different location than Cloud Volumes ONTAP instances, then the Cloud Manager instance must have a network connection to that location.

2. Subscribe to Cloud Volumes ONTAP in AWS:
 - a. Go to the AWS Intelligence Community Marketplace and search for Cloud Volumes ONTAP.
 - b. Select the offering that you plan to deploy.
 - c. Review the terms and click **Accept**.
 - d. Repeat these steps for the other offerings, if you plan to deploy them.

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

3. Provide Cloud Manager and Cloud Volumes ONTAP with the permissions needed to perform actions in AWS by setting up IAM policies and roles for the instances:
 - a. From the AWS IAM console, create your own policies by copying and pasting the required permissions.

See [IAM policy requirements](#) on page 5.

Create Your Own Policy

Use the policy editor to type or paste in your own policy.



You should have one IAM policy for Cloud Manager, one for the Cloud Volumes ONTAP nodes, and one for the HA mediator (if you want to deploy HA pairs).

- b. Create IAM roles with the role type Amazon EC2 and attach the policies that you created in the previous step.

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

The following example shows the review page for the Cloud Manager policy.

Review

Review the following role information. To edit the role, click an edit link, or click **Create Role** to finish.

Role Name	Cloud_Manager	Edit Role Name
Role ARN	arn:aws:iam::642991768967:role/Cloud_Manager	
Trusted Entities	The identity provider(s) ec2.amazonaws.com	
Policies	arn:aws:iam::642991768967:policy/Cloud_Manager	Change Policies

You must select the Cloud Manager IAM role when you launch the Cloud Manager 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.

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

IAM policy requirements

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

Policy for the Cloud Manager 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",
        "iam>ListInstanceProfiles",
        "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/*"
    ]
  }
]
}

```

Policy for Cloud Volumes ONTAP instances

```

{
  "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"
  }
]}
}

```

Policy for the Cloud Volumes ONTAP HA mediator instance

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:AssignPrivateIpAddresses",

```

8 | Quick Start Guide for the AWS Commercial Cloud Services Environment

```
        "ec2:CreateRoute",
        "ec2>DeleteRoute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:ReplaceRoute",
        "ec2:UnassignPrivateIpAddresses"
    ],
    "Resource": "*"
}
]
```


Installing and setting up Cloud Manager

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

Steps

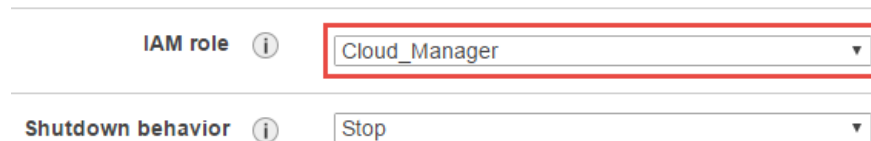
1. Obtain a root certificate signed by a certificate authority (CA) in the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format. Consult your organization's policies and procedures for obtaining the certificate.

You'll need to upload the certificate to AWS in step 4 after you complete the Setup wizard. Cloud Manager uses the trusted certificate when sending requests to AWS over HTTPS.

2. Launch the Cloud Manager instance:
 - a. Go to the AWS Intelligence Community Marketplace page for OnCommand 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:

- The t2.medium instance type is supported.
- You must choose the IAM role that you created when preparing your AWS environment.



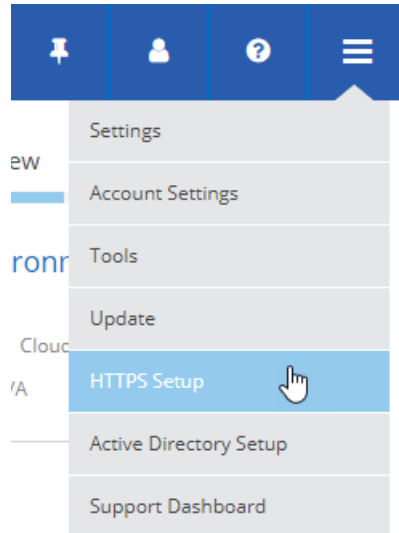
The image shows a configuration interface with two dropdown menus. The first dropdown is labeled 'IAM role' and has an information icon to its right. The selected value in this dropdown is 'Cloud_Manager', which is enclosed in a red rectangular box. The second dropdown is labeled 'Shutdown behavior' and also has an information icon to its right. The selected value in this dropdown is 'Stop'.

- You should keep the default storage options.
 - The required connection methods for the Cloud Manager instance are as follows: SSH, HTTP, and HTTPS.
3. Set up Cloud Manager from a host that has a connection to the Cloud Manager instance:
 - a. Open a web browser and enter the following URL:
`http://ipaddress:80`
 - b. Complete the steps in the Setup wizard to set up a new Cloud Manager instance.
Note the following as you set up Cloud Manager:
 - AutoSupport is not enabled by default in the Commercial Cloud Services environment.
 - The option to automatically update Cloud Manager to the newest version is not available in the Commercial Cloud Services environment because there is no internet connection.
 4. After you finish the **Setup** wizard, Cloud Manager prompts you for the certificate that you obtained in step 1:
 - a. Click **Load File** and select the certificate.
 - b. Click **Install and Restart** to install the certificate and restart Cloud Manager.
 5. After Cloud Manager restarts, log in using the administrator user account that you created in the **Setup** wizard.

- Optional: If you don't want to use a self-signed certificate for HTTPS access to the Cloud Manager console, install a certificate signed by a CA:

Note: This certificate is used when accessing the Cloud Manager console over HTTPS. The certificate that you provided in step 4 was required for communication with AWS services.

- In the upper right of the Cloud Manager console, click the task drop-down list, and then select **HTTPS Setup**.



- In the **HTTPS Setup** page, install a certificate by first generating a certificate signing request (CSR) or by installing your own CA-signed certificate.

The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.

After you install the certificate, Cloud Manager uses the certificate when you can access the console using HTTPS (port 443).

- If needed, click **Tenants** and create additional tenants.
- If multiple people need to use Cloud Manager, click the user icon, select **Users**, and add additional user accounts.

Note: A Cloud Manager Admin has access to all tenants and working environments, a Tenant Admin can administer the working environments in a single tenant, and a Working Environment Admin can administer one or more working environments in a tenant.

Result

Cloud Manager is now installed and set up so users can launch Cloud Volumes ONTAP instances.

Launching Cloud Volumes ONTAP instances

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

Before you begin

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.

Steps

1. On the **Working Environments** page, click **Create**.
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.
[Security group rules](#) on page 13
- A key pair is required to enable key-based SSH authentication to Cloud Volumes ONTAP.
- 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.
Note: 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.

The following image shows the Review & Approve page for a new system:

Review & Approve

HApair1

us-west-2 | HA | AWS

- I understand that in order to activate support, I must first register Cloud Volumes ONTAP with NetApp. [More information >](#)
- I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements. [More information >](#)

Overview

Networking

Storage

Storage System:	Cloud Volumes ONTAP HA	HA Deployment Model:	Multiple Availability Zones
License Type:	Cloud Volumes ONTAP Standard	Encryption:	AWS Managed
Capacity Limit:	10TB	Customer Master Key:	aws/ebs
Software Version:	ONTAP-9.5P2X2	Nodes Role:	HARole
Cloud Volumes ONTAP runs on:	m5.2xlarge	Mediator Role:	Mediator_OK
Instance Tenancy:	Shared	Account ID:	████████████████████

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 rules for Cloud Manager

Inbound rules

Note: The source for inbound rules is 0.0.0.0/0.

Type	Port range	Used for
SSH	22	SSH connections to Cloud Manager
HTTP	80	Accessing the Cloud Manager console
HTTPS	443	Accessing the Cloud Manager console

Outbound rules

Type	Port range	Used for
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

Security group rules for Cloud Volumes ONTAP

Inbound rules

Note: The source for inbound rules is 0.0.0.0/0.

Type	Port range	Used for
All ICMP	All	Pinging the instance
Custom TCP Rule	111	Portmapper
Custom TCP Rule	139	NetBIOS
Custom TCP Rule	161-162	SNMP
Custom TCP Rule	445	Microsoft SMB
Custom TCP Rule	635	NFS mount
Custom TCP Rule	749	Kerberos
Custom TCP Rule	2049	NFS
Custom TCP Rule	3260	iSCSI
Custom TCP Rule	4045-4046	NFS mountd
Custom TCP Rule	10000	NDMP
Custom TCP Rule	11104-11105	Intercluster management and data

Type	Port range	Used for
Custom UDP Rule	111	Portmapper
Custom UDP Rule	161-162	SNMP
Custom UDP Rule	635	NFS mount
Custom UDP Rule	2049	NFS
Custom UDP Rule	4045-4046	NFS mountd
Custom UDP Rule	4049	NFS rquotad protocol
HTTP	80	ONTAP System Manager access
HTTPS	443	ONTAP System Manager access
SSH	22	SSH to the CLI

Outbound rules

Type	Port range	Used for
All ICMP	All	All outbound traffic (SnapMirror and SnapVault)
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

External security group rules for the HA mediator

Inbound rules

Note: The source for inbound rules is 0.0.0.0/0.

Type	Port range	Used for
SSH	22	SSH connections to the HA mediator
TCP	3000	RESTful API access from Cloud Manager

Outbound rules

Type	Port range	Used for
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

Internal security group rules for the HA mediator

Note: Cloud Manager always creates this security group. You do not have the option to use your own security group.

Inbound rules

Type	Port range	Used for
All traffic	All	Communication between the HA mediator and Cloud Volumes ONTAP HA nodes only

Outbound rules

Type	Port range	Used for
All traffic	All	Communication between the HA mediator and Cloud Volumes ONTAP HA nodes only

Where to get help and find more information

You can get help and find more information about Cloud Manager and Cloud Volumes ONTAP by going to <https://docs.netapp.com/us-en/occm> from a system that has internet access.

Copyright

Copyright © 2019 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

Trademark

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

[*doccomments@netapp.com*](mailto:doccomments@netapp.com)

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277