



Reference

Cloud Manager 3.5

NetApp
December 17, 2020

Table of Contents

- Reference 1
 - Frequently asked questions: Integrating Cloud Manager with NetApp Cloud Central 1
 - Supported regions 2
 - Security group rules for AWS 4
 - Security group rules for Azure 11
 - Cloud Manager REST APIs 15
 - AWS and Azure permissions for Cloud Manager 16
 - Default configurations 20
 - User roles 22
 - Where to get help and find more information 23

Reference

Frequently asked questions: Integrating Cloud Manager with NetApp Cloud Central

When upgrading to Cloud Manager 3.5, NetApp will choose specific Cloud Manager systems to integrate with NetApp Cloud Central, if they are not already integrated. This FAQ can answer questions that you might have about the process.

What is NetApp Cloud Central?

NetApp Cloud Central provides a centralized location to access and manage NetApp cloud data services. These services enable you to run critical applications in the cloud, create automated DR sites, back up your SaaS data, and effectively migrate and control data across multiple clouds.

Why is NetApp integrating my Cloud Manager system with Cloud Central?

Cloud Manager's integration with NetApp Cloud Central provides several benefits, including a simplified deployment experience, a single location to view and manage multiple Cloud Manager systems, and centralized user authentication.

What happens during the integration process?

NetApp migrates all local user accounts in your Cloud Manager system to the centralized user authentication available in Cloud Central.

How does centralized user authentication work?

With centralized user authentication, you can use the same set of credentials across Cloud Manager systems and between Cloud Manager and other data services, such as Cloud Sync. It's also easy to reset your password if you forget it.

Do I need to sign up for a Cloud Central user account?

NetApp will create a Cloud Central user account for you when we integrate your Cloud Manager system with Cloud Central. You simply need to reset your password to complete the registration process.

What if I already have a Cloud Central user account?

If the email address that you use to log in to Cloud Manager matches the email address for a Cloud Central user account, then you can log right in to your Cloud Manager system.

What if my Cloud Manager system has multiple user accounts?

NetApp migrates all local user accounts to Cloud Central user accounts. Every user needs to reset his or her password.

What if I have a user account that uses the same email address across multiple Cloud Manager systems?

You just need to reset your password once and then you can use the same Cloud Central user account to log in to each Cloud Manager system.

What if my local user account uses an invalid email address?

Resetting your password requires a valid email address. Contact us through the chat icon that is available in the lower right of the Cloud Manager interface.

What if I have automation scripts for Cloud Manager APIs?

All APIs are backwards compatible. You will need to update scripts that use passwords, if you change your password when you reset it.

What if my Cloud Manager system uses LDAP?

If your system uses LDAP, NetApp cannot automatically integrate the system with Cloud Central. You need to manually perform the following steps:

1. Deploy a new Cloud Manager system from [NetApp Cloud Central](#).
2. [Set up LDAP with the new system](#).
3. [Discover existing Cloud Volumes ONTAP systems](#) from the new Cloud Manager system.
4. Delete the old Cloud Manager system.

Does it matter where I installed my Cloud Manager system?

No. NetApp will integrate systems with Cloud Central no matter where they reside, whether that's in AWS, Azure, or on your premises.



The only exception is the AWS Commercial Cloud Services Environment.

Supported regions

Cloud Manager and Cloud Volumes ONTAP are supported in a number of AWS regions and Microsoft Azure regions.

Supported AWS regions

You can deploy Cloud Manager and Cloud Volumes ONTAP in the following AWS regions.

Asia Pacific

- Mumbai
- Seoul
- Singapore
- Sydney

- Tokyo

EU

- Frankfurt
- Ireland
- London
- Paris

North America

- Canada (Central)
- GovCloud (US)
- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)

South America

- Sao Paulo

Supported Azure regions

You can deploy Cloud Manager and Cloud Volumes ONTAP in the following Azure regions.

Asia Pacific

- Australia East
- Australia Southeast
- Central India
- East Asia
- Japan East
- Japan West
- Korea Central
- Korea South
- South India
- Southeast Asia
- West India

EU

- Germany Central
- Germany Northeast

- North Europe
- UK South
- UK West
- West Europe

North America

- Canada Central
- Canada East
- Central US
- East US
- East US 2
- North Central US
- South Central US
- US Gov Arizona
- US Gov Texas
- US Gov Virginia
- West US
- West US 2
- West Central US

South America

- Brazil South

Security group rules for AWS

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

Rules for Cloud Manager

The security group for Cloud Manager requires both inbound and outbound rules.

Inbound rules for Cloud Manager

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

| Protocol | Port | Purpose |
|----------|------|--|
| SSH | 22 | Provides SSH access to the Cloud Manager host |
| HTTP | 80 | Provides HTTP access from client web browsers to the Cloud Manager web console |

| Protocol | Port | Purpose |
|----------|------|---|
| HTTPS | 443 | Provides HTTPS access from client web browsers to the Cloud Manager web console |

Outbound rules for Cloud Manager

The predefined security group for Cloud Manager opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

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

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

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by Cloud Manager.



The source IP address is the Cloud Manager host.

| Service | Protocol | Port | Destination | Purpose |
|---------------------------|----------|------|--|--|
| Active Directory | TCP | 88 | Active Directory forest | Kerberos V authentication |
| | TCP | 139 | Active Directory forest | NetBIOS service session |
| | TCP | 389 | Active Directory forest | LDAP |
| | TCP | 445 | Active Directory forest | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| | TCP | 464 | Active Directory forest | Kerberos V change & set password (SET_CHANGE) |
| | TCP | 749 | Active Directory forest | Active Directory Kerberos V change & set password (RPCSEC_GSS) |
| | UDP | 137 | Active Directory forest | NetBIOS name service |
| | UDP | 138 | Active Directory forest | NetBIOS datagram service |
| | UDP | 464 | Active Directory forest | Kerberos key administration |
| API calls and AutoSupport | HTTPS | 443 | Outbound internet and ONTAP cluster management LIF | API calls to AWS and ONTAP, and sending AutoSupport messages to NetApp |
| API calls | TCP | 3000 | ONTAP cluster management LIF | API calls to ONTAP |
| DNS | UDP | 53 | DNS | Used for DNS resolve by Cloud Manager |

Rules for Cloud Volumes ONTAP

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

Inbound rules for Cloud Volumes ONTAP

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 for Cloud Volumes ONTAP

The predefined security group for Cloud Volumes ONTAP opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic 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 |

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by Cloud Volumes ONTAP.



The source is the interface (IP address) on the Cloud Volumes ONTAP system.

| Service | Protocol | Port | Source | Destination | Purpose |
|------------------|----------|------|----------------------|-------------------------|--|
| Active Directory | TCP | 88 | Node management LIF | Active Directory forest | Kerberos V authentication |
| | UDP | 137 | Node management LIF | Active Directory forest | NetBIOS name service |
| | UDP | 138 | Node management LIF | Active Directory forest | NetBIOS datagram service |
| | TCP | 139 | Node management LIF | Active Directory forest | NetBIOS service session |
| | TCP | 389 | Node management LIF | Active Directory forest | LDAP |
| | TCP | 445 | Node management LIF | Active Directory forest | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| | TCP | 464 | Node management LIF | Active Directory forest | Kerberos V change & set password (SET_CHANGE) |
| | UDP | 464 | Node management LIF | Active Directory forest | Kerberos key administration |
| | TCP | 749 | Node management LIF | Active Directory forest | Kerberos V change & set Password (RPCSEC_GSS) |
| | TCP | 88 | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos V authentication |
| | UDP | 137 | Data LIF (NFS, CIFS) | Active Directory forest | NetBIOS name service |
| | UDP | 138 | Data LIF (NFS, CIFS) | Active Directory forest | NetBIOS datagram service |
| | TCP | 139 | Data LIF (NFS, CIFS) | Active Directory forest | NetBIOS service session |
| | TCP | 389 | Data LIF (NFS, CIFS) | Active Directory forest | LDAP |
| | TCP | 445 | Data LIF (NFS, CIFS) | Active Directory forest | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| | TCP | 464 | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos V change & set password (SET_CHANGE) |
| | UDP | 464 | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos key administration |
| | TCP | 749 | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos V change & set password (RPCSEC_GSS) |

| Service | Protocol | Port | Source | Destination | Purpose |
|------------|-------------|---------------------|--|----------------------------|--|
| Cluster | All traffic | All traffic | All LIFs on one node | All LIFs on the other node | Intercluster communications (Cloud Volumes ONTAP HA only) |
| | TCP | 3000 | Node management LIF | HA mediator | ZAPI calls (Cloud Volumes ONTAP HA only) |
| | ICMP | 1 | Node management LIF | HA mediator | Keep alive (Cloud Volumes ONTAP HA only) |
| DHCP | UDP | 68 | Node management LIF | DHCP | DHCP client for first-time setup |
| DHCPS | UDP | 67 | Node management LIF | DHCP | DHCP server |
| DNS | UDP | 53 | Node management LIF and data LIF (NFS, CIFS) | DNS | DNS |
| NDMP | TCP | 1860 0–18 699 | Node management LIF | Destination servers | NDMP copy |
| SMTP | TCP | 25 | Node management LIF | Mail server | SMTP alerts, can be used for AutoSupport |
| SNMP | TCP | 161 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | UDP | 161 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | TCP | 162 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | UDP | 162 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| SnapMirror | TCP | 1110 4 | Intercluster LIF | ONTAP intercluster LIFs | Management of intercluster communication sessions for SnapMirror |
| | TCP | 1110 5 | Intercluster LIF | ONTAP intercluster LIFs | SnapMirror data transfer |
| Syslog | UDP | 514 | Node management LIF | Syslog server | Syslog forward messages |

Rules for the HA mediator external security group

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 0.0.0.0/0.

| Protocol | Port | Purpose |
|----------|------|---------------------------------------|
| SSH | 22 | SSH connections to the HA mediator |
| TCP | 3000 | RESTful API access from Cloud Manager |

Outbound rules

The predefined security group for the HA mediator opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic 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 |

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by the HA mediator.

| Service | Protocol | Port | Destination | Purpose |
|---------|----------|------|------------------|------------------------------|
| API | HTTP S | 443 | AWS API services | Assist with storage failover |
| API | UDP | 53 | AWS API services | Assist with storage failover |



Rather than open these two ports, you can use a private endpoint instead.

Rules for the HA mediator internal security group

The predefined internal security group for the Cloud Volumes ONTAP HA mediator includes the following rules. Cloud Manager always creates this security group. You do not 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 |

Security group rules for Azure

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

Rules for Cloud Manager

The security group for Cloud Manager requires both inbound and outbound rules.

Inbound rules for Cloud Manager

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

| Protocol | Port | Purpose |
|----------|------|---|
| SSH | 22 | Provides SSH access to the Cloud Manager host |
| HTTP | 80 | Provides HTTP access from client web browsers to the Cloud Manager web console |
| HTTPS | 443 | Provides HTTPS access from client web browsers to the Cloud Manager web console |

Outbound rules for Cloud Manager

The predefined security group for Cloud Manager opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

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

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

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by Cloud Manager.



The source IP address is the Cloud Manager host.

| Service | Protocol | Port | Destination | Purpose |
|---------------------------|----------|------|--|--|
| Active Directory | TCP | 88 | Active Directory forest | Kerberos V authentication |
| | TCP | 139 | Active Directory forest | NetBIOS service session |
| | TCP | 389 | Active Directory forest | LDAP |
| | TCP | 445 | Active Directory forest | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| | TCP | 464 | Active Directory forest | Kerberos V change & set password (SET_CHANGE) |
| | TCP | 749 | Active Directory forest | Active Directory Kerberos V change & set password (RPCSEC_GSS) |
| | UDP | 137 | Active Directory forest | NetBIOS name service |
| | UDP | 138 | Active Directory forest | NetBIOS datagram service |
| | UDP | 464 | Active Directory forest | Kerberos key administration |
| API calls and AutoSupport | HTTPS | 443 | Outbound internet and ONTAP cluster management LIF | API calls to AWS and ONTAP, and sending AutoSupport messages to NetApp |
| API calls | TCP | 3000 | ONTAP cluster management LIF | API calls to ONTAP |
| DNS | UDP | 53 | DNS | Used for DNS resolve by Cloud Manager |

Rules for Cloud Volumes ONTAP

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

Inbound rules for Cloud Volumes ONTAP

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 |

| Protocol | Port | Purpose |
|----------|---------|--|
| 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 for Cloud Volumes ONTAP

The predefined security group for Cloud Volumes ONTAP opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic 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 |

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by Cloud Volumes ONTAP.



The source is the interface (IP address) on the Cloud Volumes ONTAP system.

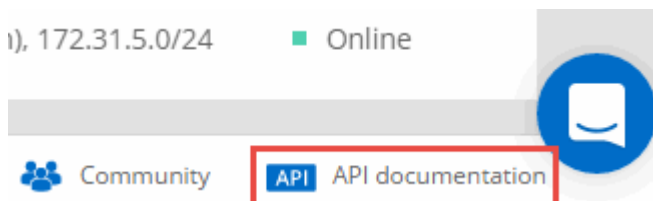
| Service | Protocol | Port | Source | Destination | Purpose |
|------------------|----------|------|----------------------|-------------------------|--|
| Active Directory | TCP | 88 | Node management LIF | Active Directory forest | Kerberos V authentication |
| | UDP | 137 | Node management LIF | Active Directory forest | NetBIOS name service |
| | UDP | 138 | Node management LIF | Active Directory forest | NetBIOS datagram service |
| | TCP | 139 | Node management LIF | Active Directory forest | NetBIOS service session |
| | TCP | 389 | Node management LIF | Active Directory forest | LDAP |
| | TCP | 445 | Node management LIF | Active Directory forest | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| | TCP | 464 | Node management LIF | Active Directory forest | Kerberos V change & set password (SET_CHANGE) |
| | UDP | 464 | Node management LIF | Active Directory forest | Kerberos key administration |
| | TCP | 749 | Node management LIF | Active Directory forest | Kerberos V change & set Password (RPCSEC_GSS) |
| | TCP | 88 | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos V authentication |
| | UDP | 137 | Data LIF (NFS, CIFS) | Active Directory forest | NetBIOS name service |
| | UDP | 138 | Data LIF (NFS, CIFS) | Active Directory forest | NetBIOS datagram service |
| | TCP | 139 | Data LIF (NFS, CIFS) | Active Directory forest | NetBIOS service session |
| | TCP | 389 | Data LIF (NFS, CIFS) | Active Directory forest | LDAP |
| | TCP | 445 | Data LIF (NFS, CIFS) | Active Directory forest | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| | TCP | 464 | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos V change & set password (SET_CHANGE) |
| | UDP | 464 | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos key administration |
| | TCP | 749 | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos V change & set password (RPCSEC_GSS) |
| DHCP | UDP | 68 | Node management LIF | DHCP | DHCP client for first-time setup |
| DHCPS | UDP | 67 | Node management LIF | DHCP | DHCP server |

| Service | Protocol | Port | Source | Destination | Purpose |
|------------|----------|---------------------|--|-------------------------|--|
| DNS | UDP | 53 | Node management LIF and data LIF (NFS, CIFS) | DNS | DNS |
| NDMP | TCP | 1860 0–18 699 | Node management LIF | Destination servers | NDMP copy |
| SMTP | TCP | 25 | Node management LIF | Mail server | SMTP alerts, can be used for AutoSupport |
| SNMP | TCP | 161 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | UDP | 161 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | TCP | 162 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | UDP | 162 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| SnapMirror | TCP | 1110 4 | Intercluster LIF | ONTAP intercluster LIFs | Management of intercluster communication sessions for SnapMirror |
| | TCP | 1110 5 | Intercluster LIF | ONTAP intercluster LIFs | SnapMirror data transfer |
| Syslog | UDP | 514 | Node management LIF | Syslog server | Syslog forward messages |

Cloud Manager REST APIs

Cloud Manager includes REST APIs that enable software developers to automate the management of NetApp storage in the cloud. There is an API for every action that is available from the user interface.

Cloud Manager provides interactive API documentation using the Swagger interface. A link to the API documentation is available in the lower-right corner of the console:



You can also find an overview, examples, and an API reference in the [OnCommand Cloud Manager API Developer Guide](#).

AWS and Azure permissions for Cloud Manager

Cloud Manager requires permissions to perform actions in AWS and Azure on your behalf. These permissions are included in [the policies provided by NetApp](#). You might want to understand what Cloud Manager does with these permissions.

What Cloud Manager does with AWS permissions

Cloud Manager uses an AWS account to make API calls to several AWS services, including EC2, S3, CloudFormation, IAM, the Security Token Service (STS), and the Key Management Service (KMS).

| Actions | Purpose |
|---|--|
| "ec2:StartInstances", "ec2:StopInstances", "ec2:DescribeInstances", "ec2:DescribeInstanceStatus", "ec2:RunInstances", "ec2:TerminateInstances", "ec2:ModifyInstanceAttribute", | Launches a Cloud Volumes ONTAP instance and stops, starts, and monitors the instance. |
| "ec2:DescribeInstanceAttribute", | Verifies that enhanced networking is enabled for supported instance types. |
| "ec2:DescribeRouteTables", "ec2:DescribeImages", | Launches a Cloud Volumes ONTAP HA configuration. |
| "ec2:CreateTags", | Tags every resource that Cloud Manager creates with the "WorkingEnvironment" and "WorkingEnvironmentId" tags. Cloud Manager uses these tags for maintenance and cost allocation. |
| "ec2:CreateVolume", "ec2:DescribeVolumes", "ec2:ModifyVolumeAttribute", "ec2:AttachVolume", "ec2:DeleteVolume", "ec2:DetachVolume", | Manages the EBS volumes that Cloud Volumes ONTAP uses as back-end storage. |
| "ec2:CreateSecurityGroup", "ec2>DeleteSecurityGroup", "ec2:DescribeSecurityGroups", "ec2:RevokeSecurityGroupEgress", "ec2:AuthorizeSecurityGroupEgress", "ec2:AuthorizeSecurityGroupIngress", "ec2:RevokeSecurityGroupIngress", | Creates predefined security groups for Cloud Volumes ONTAP. |
| "ec2:CreateNetworkInterface", "ec2:DescribeNetworkInterfaces", "ec2>DeleteNetworkInterface", "ec2:ModifyNetworkInterfaceAttribute", | Creates and manages network interfaces for Cloud Volumes ONTAP in the target subnet. |
| "ec2:DescribeSubnets", "ec2:DescribeVpcs", | Gets the list of destination subnets and security groups, which is needed when creating a new working environment for Cloud Volumes ONTAP. |


| Actions | Purpose |
|---|---|
| "ec2:DescribeDhcpOptions", | Determines DNS servers and the default domain name when launching Cloud Volumes ONTAP instances. |
| "ec2:CreateSnapshot", "ec2:DeleteSnapshot", "ec2:DescribeSnapshots", | Takes snapshots of EBS volumes during initial setup and whenever a Cloud Volumes ONTAP instance is stopped. |
| "ec2:GetConsoleOutput", | Captures the Cloud Volumes ONTAP console, which is attached to AutoSupport messages. |
| "ec2:DescribeKeyPairs", | Obtains the list of available key pairs when launching instances. |
| "ec2:DescribeRegions", | Gets a list of available AWS regions. |
| "ec2:DeleteTags", "ec2:DescribeTags", | Manages tags for resources associated with Cloud Volumes ONTAP instances. |
| "cloudformation:CreateStack", "cloudformation:DeleteStack", "cloudformation:DescribeStacks", "cloudformation:DescribeStackEvents", "cloudformation:ValidateTemplate", | Launches Cloud Volumes ONTAP instances. |
| "iam:PassRole", "iam:CreateRole", "iam:DeleteRole", "iam:PutRolePolicy", "iam:CreateInstanceProfile", "iam:DeleteRolePolicy", "iam:AddRoleToInstanceProfile", "iam:RemoveRoleFromInstanceProfile", "iam:DeleteInstanceProfile", | Launches a Cloud Volumes ONTAP HA configuration. |
| "iam:ListInstanceProfiles", "sts:DecodeAuthorizationMessage", "ec2:AssociateIamInstanceProfile", "ec2:DescribeIamInstanceProfileAssociations", "ec2:DisassociateIamInstanceProfile", | Manages instance profiles for Cloud Volumes ONTAP instances. |
| "s3:GetObject", "s3:ListBucket" | Obtains AWS cost data for Cloud Volumes ONTAP. |
| "s3:GetBucketTagging", "s3:GetBucketLocation", "s3:ListAllMyBuckets", | Obtains information about AWS S3 buckets so Cloud Manager can integrate with the NetApp Data Fabric Cloud Sync service. |
| "s3:CreateBucket", "s3:DeleteBucket", "s3:GetLifecycleConfiguration", "s3:PutLifecycleConfiguration", "s3:PutBucketTagging", "s3:ListBucketVersions", | Manages the S3 bucket that a Cloud Volumes ONTAP system uses as a capacity tier. |

| Actions | Purpose |
|--------------------------------|---|
| "kms:List*", "kms:Describe" | Obtains information about keys from the AWS Key Management Service. |

What Cloud Manager does with Azure permissions

The Cloud Manager Azure policy includes the permissions that Cloud Manager needs to deploy and manage Cloud Volumes ONTAP in Azure.

| Actions | Purpose |
|---|---|
| "Microsoft.Compute/locations/operations/read", "Microsoft.Compute/locations/vmSizes/read", "Microsoft.Compute/operations/read", "Microsoft.Compute/virtualMachines/instanceView/read", "Microsoft.Compute/virtualMachines/powerOff/action", "Microsoft.Compute/virtualMachines/read", "Microsoft.Compute/virtualMachines/restart/action", "Microsoft.Compute/virtualMachines/start/action", "Microsoft.Compute/virtualMachines/deallocate/action", "Microsoft.Compute/virtualMachines/vmSizes/read", "Microsoft.Compute/virtualMachines/write", | Creates Cloud Volumes ONTAP and stops, starts, deletes, and obtains the status of the system. |
| "Microsoft.Compute/images/write", "Microsoft.Compute/images/read", | Enables Cloud Volumes ONTAP deployment from a VHD. |
| "Microsoft.Compute/disks/delete", "Microsoft.Compute/disks/read", "Microsoft.Compute/disks/write", "Microsoft.Storage/checknameavailability/read", "Microsoft.Storage/operations/read", "Microsoft.Storage/storageAccounts/listkeys/action", "Microsoft.Storage/storageAccounts/read", "Microsoft.Storage/storageAccounts/regeneratekey/action", "Microsoft.Storage/storageAccounts/write" | Manages Azure storage accounts and disks, and attaches the disks to Cloud Volumes ONTAP. |
| "Microsoft.Network/networkInterfaces/read", "Microsoft.Network/networkInterfaces/write", "Microsoft.Network/networkInterfaces/join/action", | Creates and manages network interfaces for Cloud Volumes ONTAP in the target subnet. |
| "Microsoft.Network/networkSecurityGroups/read", "Microsoft.Network/networkSecurityGroups/write", "Microsoft.Network/networkSecurityGroups/join/action", | Creates predefined network security groups for Cloud Volumes ONTAP. |

| Actions | Purpose |
|---|--|
| "Microsoft.Resources/subscriptions/locations/read", "Microsoft.Network/locations/operationResults/read", "Microsoft.Network/locations/operations/read", "Microsoft.Network/virtualNetworks/read", "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read", "Microsoft.Network/virtualNetworks/subnets/read", "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read", "Microsoft.Network/virtualNetworks/virtualMachines/read", "Microsoft.Network/virtualNetworks/subnets/join/action", | Gets network information about regions, the target VNet and subnet, and adds Cloud Volumes ONTAP to VNets. |
| <div data-bbox="183 774 246 837"></div> <div data-bbox="323 705 773 905"> <p>If your network configuration uses route tables, then Cloud Manager also requires the following permission:</p> <p>Microsoft.Network/routeTables/join/action</p> </div> | Enables VNet service endpoints for data tiering. |
| "Microsoft.Resources/deployments/operations/read", "Microsoft.Resources/deployments/read", "Microsoft.Resources/deployments/write", | Deploys Cloud Volumes ONTAP from a template. |
| "Microsoft.Resources/deployments/operations/read", "Microsoft.Resources/deployments/read", "Microsoft.Resources/deployments/write", "Microsoft.Resources/resources/read", "Microsoft.Resources/subscriptions/operationresults/read", "Microsoft.Resources/subscriptions/resourceGroups/delete", "Microsoft.Resources/subscriptions/resourceGroups/read", "Microsoft.Resources/subscriptions/resourcegroups/resources/read", "Microsoft.Resources/subscriptions/resourceGroups/write", | Creates and manages resource groups for Cloud Volumes ONTAP. |
| "Microsoft.Compute/snapshots/write", "Microsoft.Compute/snapshots/read", "Microsoft.Compute/disks/beginGetAccess/action" | Creates and manages Azure managed snapshots. |
| "Microsoft.Compute/availabilitySets/write", "Microsoft.Compute/availabilitySets/read", | Creates and manages availability sets for Cloud Volumes ONTAP. |
| "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read", "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write" | Enables programmatic deployments from the Azure Marketplace. |

| Actions | Purpose |
|-----------------------------------|---|
| "Microsoft.Authorization/locks/*" | Enables management of locks on Azure disks. |

Default configurations

Details about how Cloud Manager and Cloud Volumes ONTAP are configured by default can help you administer the systems.

Default configuration for Cloud Manager on Linux

If you need to troubleshoot Cloud Manager or your Linux host, it might help to understand how Cloud Manager is configured.

- If you deployed Cloud Manager from NetApp Cloud Central (or directly from the AWS Marketplace or Azure Marketplace), note the following:
 - In AWS, the user name for the EC2 Linux instance is `ec2-user`.
 - For both AWS and Azure, the operating system for the Cloud Manager image is Red Hat Enterprise Linux 7.4 (HVM).

The operating system does not include a GUI. You must use a terminal to access the system.

- The Cloud Manager installation folder resides in the following location:

`/opt/application/netapp/cloudmanager`

- Log files are contained in the following folder:

`/opt/application/netapp/cloudmanager/log`

- The Cloud Manager service is named `occm`.
- The `occm` service is dependent on the MySQL service.

If the MySQL service is down, then the `occm` service is down too.

- Cloud Manager installs the following packages on the Linux host, if they are not already installed:
 - 7Zip
 - AWSCLI
 - Java
 - MySQL
 - Wget

Default configuration for Cloud Volumes ONTAP

Understanding how Cloud Volumes ONTAP is configured by default can help you set up and administer your systems, especially if you are familiar with ONTAP because the default setup for Cloud Volumes ONTAP is different than ONTAP.

- Cloud Volumes ONTAP is available as a single system in AWS and Microsoft Azure, and as an HA pair in AWS.


- Cloud Manager creates one data-serving SVM when it deploys Cloud Volumes ONTAP. While you can create another data-serving SVM from System Manager or the CLI, using multiple data-serving SVMs is not supported.
- Several network interfaces are created by default:
 - A cluster management LIF
 - An intercluster LIF
 - A node management LIF
 - An iSCSI data LIF
 - A CIFS and NFS data LIF



LIF failover is disabled by default for Cloud Volumes ONTAP due to EC2 requirements. Migrating a LIF to a different port breaks the external mapping between IP addresses and network interfaces on the instance, making the LIF inaccessible.

- Cloud Volumes ONTAP sends configuration backups to Cloud Manager using HTTPS.
- When logged in to Cloud Manager, the backups are accessible from <https://ipaddress/occm/offboxconfig/>
- Cloud Manager sets a few volume attributes differently than other management tools (System Manager or the CLI, for example).

The following table lists the volume attributes that Cloud Manager sets differently from the defaults:

| Attribute | Value set by Cloud Manager |
|-----------------------------|---|
| Autosize mode | grow |
| Maximum autosize | 1,000 percent <div>  <p>The Cloud Manager Admin can modify this value from the Settings page.</p> </div> |
| Security style | NTFS for CIFS volumes UNIX for NFS volumes |
| Space guarantee style | none |
| UNIX permissions (NFS only) | 777 |

See the *volume create* man page for information about these attributes.

Boot and root data for Cloud Volumes ONTAP

In addition to the storage for user data, Cloud Manager also purchases cloud storage for boot and root data on each Cloud Volumes ONTAP system.

AWS

- One Provisioned IOPS SSD disk for Cloud Volumes ONTAP boot data, which is approximately 45 GB and 1,250 PIOPS
- One General Purpose SSD disk for Cloud Volumes ONTAP root data, which is approximately 140 GB
- One EBS snapshot for each boot disk and root disk

In an HA pair, both Cloud Volumes ONTAP nodes replicate its root disk to the partner node.

Azure

- One Premium Storage SSD disk for Cloud Volumes ONTAP boot data, which is approximately 73 GB
- One Premium Storage SSD disk for Cloud Volumes ONTAP root data, which is approximately 140 GB
- One Azure snapshot for each boot disk and root disk

Where the disks reside

Cloud Manager lays out the storage from AWS and Azure as follows:

- Boot data resides on a disk attached to the EC2 instance or Azure virtual machine.

This disk, which contains the boot image, is not available to Cloud Volumes ONTAP.

- Root data, which contains the system configuration and logs, resides in aggr0.
- The storage virtual machine (SVM) root volume resides in aggr1.
- Data volumes also reside in aggr1.

User roles

Each Cloud Manager user account is assigned a role that defines permissions.

| Task | Cloud Manager Admin | Tenant Admin | Working Environment Admin |
|---|---------------------|------------------------------|--|
| Manage tenants | Yes | No | No |
| Manage working environments | Yes | Yes, for the assigned tenant | Yes, for assigned working environments |
| Integrate a working environment with Cloud Sync | Yes | Yes | No |
| View data replication status | Yes | Yes, for the assigned tenant | Yes, for assigned working environments |
| View the timeline | Yes | Yes | Yes |
| Create and delete user accounts | Yes | Yes, for the assigned tenant | No |
| Modify user accounts | Yes | Yes, for the assigned tenant | Yes, for their own account |

| Task | Cloud Manager Admin | Tenant Admin | Working Environment Admin |
|--|---------------------|--------------|---------------------------|
| Switch between the Storage System View and the Volume View | Yes | No | No |
| Modify settings | Yes | No | No |
| View and manage the Support Dashboard | Yes | No | No |
| Back up and restore Cloud Manager | Yes | No | No |
| Remove a working environment | Yes | No | No |
| Update Cloud Manager | Yes | No | No |
| Install an HTTPS certificate | Yes | No | No |
| Set up Active Directory | Yes | No | No |
| Enable the Cloud Storage Automation Report | Yes | No | No |

Where to get help and find more information

You can get help and find more information about Cloud Manager and Cloud Volumes ONTAP through various resources, including videos, forums, and support.

- [Videos for Cloud Manager and Cloud Volumes ONTAP](#)

Watch videos that show you how to deploy and manage Cloud Volumes ONTAP in AWS and Azure and how to replicate data across your hybrid cloud.

- [Policies for Cloud Manager](#)

Download JSON files that include the permissions that Cloud Manager needs to perform actions in AWS and Azure.

- [Cloud Manager API Developer Guide](#)

Read an overview of the APIs, examples of how to use them, and an API reference.

- Technical reports
 - [NetApp Technical Report 4383: Performance Characterization of Cloud Volumes ONTAP in Amazon Web Services with Application Workloads](#)
 - [NetApp Technical Report 4671: Performance Characterization of Cloud Volumes ONTAP in Azure with Application Workloads](#)
- [Cloud Volumes ONTAP 9 SVM Disaster Recovery Preparation Express Guide](#)

Describes how to quickly configure a destination SVM in preparation for disaster recovery.

- [Cloud Volumes ONTAP 9 SVM Disaster Recovery Express Guide](#)

Describes how to quickly activate a destination SVM after a disaster, and then reactivate the source SVM.

- [ONTAP 9 Documentation Center](#)

Access product documentation for ONTAP, which can help you as you use Cloud Volumes ONTAP.

- [NetApp Cloud Volumes ONTAP Support](#)

Access support resources to get help and troubleshoot issues with Cloud Volumes ONTAP.

- [NetApp Community: Hybrid Cloud](#)

Connect with peers, ask questions, exchange ideas, find resources, and share best practices.

- [NetApp Cloud Central](#)

Find information about additional NetApp products and solutions for the cloud.

- [NetApp Product Documentation](#)

Search NetApp product documentation for instructions, resources, and answers.

- [Notice for Cloud Manager 3.5](#)

Provides information about third-party copyright and licenses.

Copyright Information

Copyright © 2020 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.