Deploying ONTAP Cloud

Cloud Manager 3.4

NetApp
June 06, 2022

Table of Contents

Deploying ONTAP Cloud

Before you create ONTAP Cloud systems

Before you use Cloud Manager to create and manage ONTAP Cloud systems, your Cloud Manager administrator should have prepared networking and installed and set up Cloud Manager.

The following conditions should exist before you get started:

- AWS and Azure networking requirements were met for Cloud Manager and ONTAP Cloud.
- Cloud Manager has permissions to perform operations in AWS and Azure on your behalf.
- Each ONTAP Cloud product that users will deploy was subscribed to from the AWS Marketplace.
- Cloud Manager was installed.
- (Optional) Additional tenants were defined.
- (Optional) Additional user accounts were created, which can include Tenant Admins and Working Environment Admins.
- (Optional) If users want to enable ONTAP Cloud encryption in AWS, a key management infrastructure was set up and Cloud Manager encryption settings were defined.

Logging in to Cloud Manager

You can log in to Cloud Manager from any web browser that has a connection to the Cloud Manager system. For new Cloud Manager 3.4 systems and later, you must have a NetApp Cloud Central user account to log in.

Steps

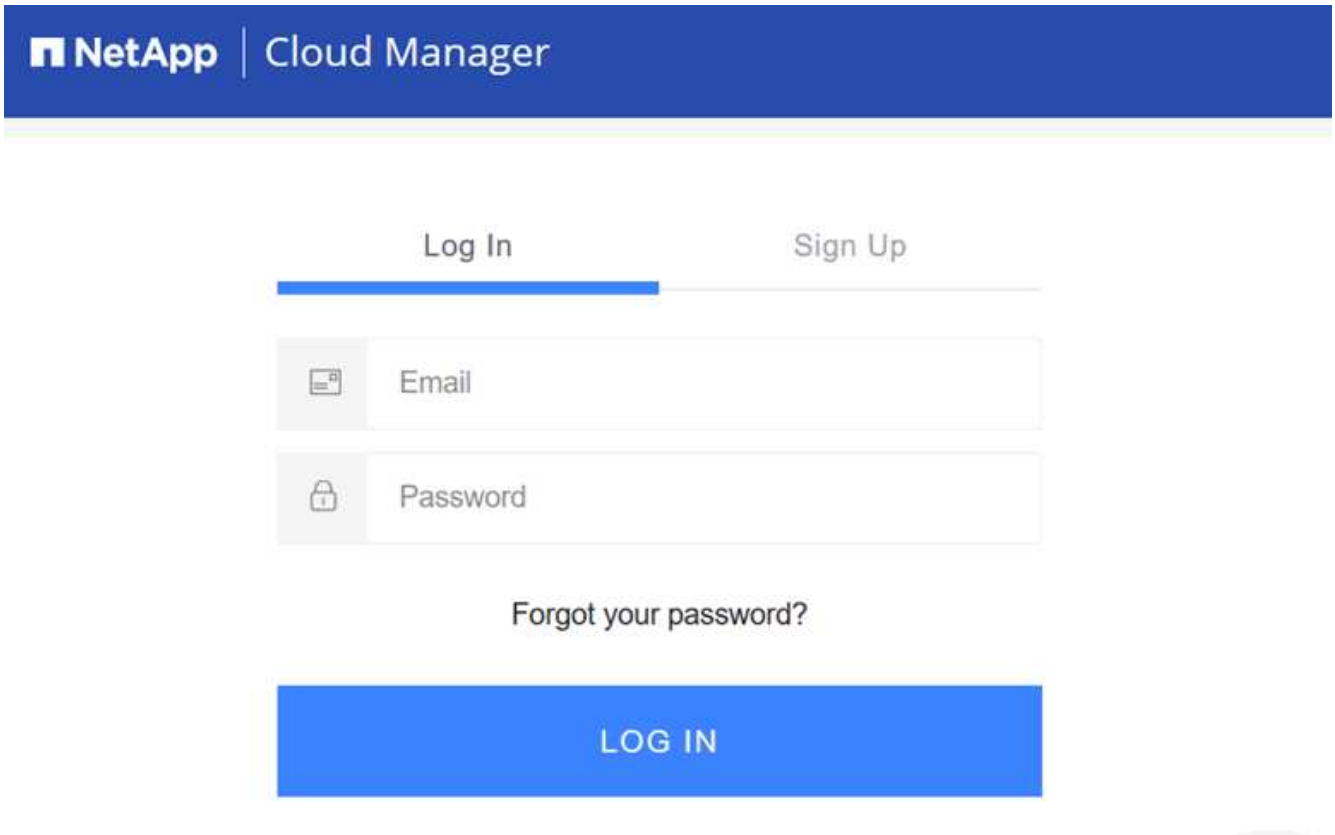
1. Open a web browser and enter the following URL:

   https://*ipaddress*:*port*

   ipaddress can be localhost, a private IP address, or a public IP address, depending on the configuration of the Cloud Manager host. For example, if Cloud Manager is in the public cloud without a public IP address, you must enter a private IP address from a host that has a connection to the Cloud Manager host.

   port is required if you changed the default HTTP (80) or HTTPS (443) ports. For example, if the HTTPS port was changed to 8443, you would enter https://ipaddress:8443

   After you enter the URL, the Cloud Manager log in screen appears. The following image shows the log in screen for new Cloud Manager 3.4 systems and later.



2. If you do not have a NetApp Cloud Central user account, you must sign up for one and then the Cloud Manager administrator must add your account to the system before you can log in.

Planning your ONTAP Cloud configuration

When you deploy ONTAP Cloud systems, you can choose a preconfigured system that matches your workload requirements, or you can create your own configuration. If you choose your own configuration, you should understand the options available to you.

Choosing a license type

ONTAP Cloud is available in AWS and Azure in two pricing options: pay-as-you-go and Bring Your Own License (BYOL). For pay-as-you-go, you can choose from three configurations: Explore, Standard, or Premium.

ONTAP Cloud for AWS

In AWS, you can deploy ONTAP Cloud as a single system or an HA pair.

	Explore	Standard	Premium	BYOL
EC2 instance types	m4.xlarge	• m4.2xlarge • r4.xlarge	• c4.4xlarge • c4.8xlarge • m4.4xlarge • r4.2xlarge	• c4.4xlarge • c4.8xlarge • m4.xlarge • m4.2xlarge • m4.4xlarge • r4.xlarge • r4.2xlarge
EBS raw capacity limit	2 TB	10 TB	• 368 TB for single node systems • 360 TB per node in an HA pair	
Term	Hourly			6 or 12 months

Notes:

1. Pay-as-you-go configurations are not supported in GovCloud (US).
2. When you choose an EC2 instance type, you can specify whether it is a shared instance or a dedicated instance.
3. Enhanced write performance is supported when using EBS SSDs with ONTAP Cloud Standard, Premium, and BYOL.
4. Tiered storage configurations are supported with ONTAP Cloud Standard, Premium, and BYOL.
5. For AWS region support, see Supported AWS regions.

ONTAP Cloud for Azure

In Azure, you can deploy ONTAP Cloud as a single node system.

	Explore	Standard	Premium	BYOL
Virtual machine types	DS3_v2	• DS4_v2 • DS13_v2	• DS5_v2 • DS14_v2	• DS3_v2 • DS4_v2 • DS5_v2 • DS13_v2 • DS14_v2
Raw capacity limit	2 TB	10 TB	252 TB	
Term	Hourly			12 months

Notes:

1. The actual maximum capacity may be less because of virtual machine limits: 60 TB for DS3, 124 TB for DS4 and DS13, and 252 TB for DS5 and DS14.
2. For Azure region support, see Supported Azure regions.

Understanding storage limits

The raw capacity limit for an ONTAP Cloud system is tied to the license. Additional limits impact the size of aggregates and volumes. You should be aware of these limits as you plan your configuration.

You can find storage limits in the ONTAP Cloud Release Notes.

ONTAP Cloud 9.3 for AWS Release Notes
ONTAP Cloud 9.3 for Azure Release Notes

Choosing an AWS disk type

When you create volumes for ONTAP Cloud systems, you need to choose the underlying EBS volume type (which ONTAP Cloud sees as a *disk*). You should choose the configuration that meets your requirements for performance and cost.

The underlying AWS disk type for ONTAP Cloud can be a single EBS disk type or a tiered storage configuration that uses EBS as a performance tier and S3 as a capacity tier. For an overview of data tiering, see Storage. For requirements, see Tiering data in AWS.

Supported EBS disk types

At a high level, the differences between EBS disk types are as follows:

- *General Purpose SSD* disks balance cost and performance for a broad range of workloads. Performance is defined in terms of IOPS.
- *Provisioned IOPS SSD* disks are for critical applications that require the highest performance at a higher cost.
- *Throughput Optimized HDD* disks are for frequently accessed workloads that require fast and consistent throughput at a lower price.
- *Cold HDD* disks are meant for backups, or infrequently accessed data, because the performance is very low. Like Throughput Optimized HDD disks, performance is defined in terms of throughput.

Cold HDD disks are not supported with ONTAP Cloud HA configurations.

For additional details about the use cases for these disks, refer to AWS Documentation: EBS Volume Types.

Choosing an Azure disk type

When you create volumes for ONTAP Cloud systems, you need to choose the underlying Azure disk type. Each disk type is designed for different workloads. You should choose the disk that meets your requirements for both performance and cost.

The underlying disk type for Azure can be Premium Storage or Standard Storage:

- *Premium Storage* disks store data on solid state drives (SSDs). The SSD disks provide high performance for I/O-intensive workloads at a higher cost.
- If you do not need high IOPS, you can reduce your costs by using *Standard Storage* disks which are backed by hard disk drives (HDD).

For additional details about the use cases for these disks, see Microsoft Azure Documentation: Introduction to Microsoft Azure Storage.

Choosing a disk size

You can choose from several disk sizes when you launch ONTAP Cloud systems and when you use the advanced allocation option. You should consider the disk size carefully because it impacts cost, performance, and total volume and system capacity.

When you launch ONTAP Cloud instances, you must choose the default disk size for aggregates. Cloud Manager uses this disk size for the initial aggregate, and for any additional aggregates that it creates when you use the simple provisioning option. You can create aggregates that use a disk size different from the default by using the advanced allocation option.

In AWS, Cloud Manager gradually increases the size of disks as a system grows. For details, see Disk size selection for aggregates in AWS.

When choosing disk size, you should take several factors into consideration. The disk size impacts how much you pay for storage, the size of volumes that you can create in an aggregate, the total capacity available to an ONTAP Cloud system, and storage performance.

Different disk sizes are available for each disk type. Note that all disks in an aggregate must be the same size.

How disk size relates to performance in AWS

The performance of EBS disks is tied to disk size. The size determines the baseline IOPS and maximum burst duration for SSD disks and the baseline and burst throughput for HDD disks.

Larger disks have a higher baseline and burst performance, so you should always consider performance along with cost. Ultimately, you should choose the disk size that gives you the *sustained performance* that you need.

For example, when using General Purpose SSD disks, you might choose the following disk sizes:

- 100 GB because you want to start out with something small or because you have low performance requirements
- 500 GB because you want to get the best price to performance ratio
- 4 TB because you need very high sustained IOPS performance

Even if you do choose larger disks (for example, six 4 TB disks), you might not get all of the IOPS because the EC2 instance can reach its bandwidth limit.

For more details about the relationship between disk size and performance, refer to AWS Documentation: EBS Volume Types.

How disk size relates to performance in Azure

The performance of Azure Premium Storage is tied to the disk size. Larger disks provide higher IOPS and throughput. For example, choosing 1 TB disks can provide better performance than 500 GB disks, at a higher cost.

When sizing for performance, you should also be aware of performance limits tied to Azure virtual machine types. For details, refer to the following:

- Microsoft Azure Documentation: High-performance Premium Storage and managed disks for VMs
- Microsoft Azure Documentation: Sizes for Linux virtual machines in Azure

There are no performance differences between disk sizes for Standard Storage. You should choose disk size based on the capacity that you need.

Choosing a write speed

Cloud Manager enables you to choose a write speed setting for single node ONTAP Cloud systems. Before you choose a write speed, you should understand the differences between the normal and high settings and risks and recommendations when using high write speed.

Difference between normal write speed and high write speed

When you choose normal write speed, data is written directly to disk, thereby reducing the likelihood of data loss in the event of an unplanned system outage.

When you choose high write speed, data is buffered in memory before it is written to disk, which provides faster write performance. Due to this caching, there is the potential for data loss if an unplanned system outage occurs.

The amount of data that can be lost in the event of an unplanned system outage is the span of the last two consistency points. A consistency point is the act of writing buffered data to disk. A consistency point occurs when the write log is full or after 10 seconds (whichever comes first). However, AWS EBS volume performance can affect consistency point processing time.

When to use high write speed

High write speed is a good choice if fast write performance is required for your workload and you can withstand the risk of data loss in the event of an unplanned system outage.

Recommendations when using high write speed

If you enable high write speed, you should ensure write protection at the application layer.

Choosing a volume usage profile

ONTAP includes several storage efficiency features that can reduce the total amount of storage that you need. When you create a volume in Cloud Manager, you can choose a profile that enables these features or a profile that disables them. You should learn more about these features to help you decide which profile to use.

NetApp storage efficiency features provide the following benefits:

Thin provisioning

Presents more logical storage to hosts or users than you actually have in your physical storage pool. Instead of preallocating storage space, storage space is allocated dynamically to each volume as data is written.

Deduplication

Improves efficiency by locating identical blocks of data and replacing them with references to a single shared block. This technique reduces storage capacity requirements by eliminating redundant blocks of data that reside in the same volume.

Compression

Reduces the physical capacity required to store data by compressing data within a volume on primary, secondary, and archive storage.

AWS network information worksheet

When you launch ONTAP Cloud in AWS, you need to specify details about your VPC network. You can use a worksheet to collect the information from your administrator.

Network information for ONTAP Cloud

AWS information	Your value
Region	
VPC	
Subnet	
Security group (if using your own)	

Network information for an ONTAP Cloud HA pair in multiple AZs

AWS information	Your value
Region	
VPC	
Security group (if using your own)	
Node 1 availability zone	
Node 1 subnet	
Node 2 availability zone	
Node 2 subnet	
Mediator availability zone	
Mediator subnet	
Key pair for the mediator	
Floating IP address for cluster management port	
Floating IP address for data on node 1	
Floating IP address for data on node 2	
Route tables for floating IP addresses	

Azure network information worksheet

When you deploy ONTAP Cloud in Azure, you need to specify details about your virtual network. You can use a worksheet to collect the information from your administrator.

Azure information	Your value
Region	
Virtual network (VNet)	
Subnet	
Network security group (if using your own)	

Launching ONTAP Cloud in AWS

You can launch ONTAP Cloud in a single-system configuration or as an HA pair in AWS.

Launching a single ONTAP Cloud system in AWS

If you want to launch an ONTAP Cloud instance in AWS, you need to create an ONTAP Cloud working environment in Cloud Manager.

Before you begin

- You should have prepared by choosing a configuration and by obtaining AWS networking information from your administrator. For details, see Planning your ONTAP Cloud configuration.
- If you want to launch an ONTAP Cloud BYOL instance, you must have the 20-digit serial number (license key) and you must have credentials for a NetApp Support Site account, if the tenant is not already linked with an account.
- If you want to use CIFS, you must have set up DNS and Active Directory. For details, see AWS networking requirements.

About this task

Immediately after you create the working environment, Cloud Manager launches a test instance in the specified VPC to verify connectivity. If successful, Cloud Manager immediately terminates the instance and then starts deploying the ONTAP Cloud system. If Cloud Manager cannot verify connectivity, creation of the working environment fails. The test instance is either a t2.nano (for default VPC tenancy) or m3.medium (for dedicated VPC tenancy).

Steps

1. On the Working Environments page, click **Add environment**.
2. Under Create, select **ONTAP Cloud**.
3. On the Details and Credentials page, enter a name for the working environment, add AWS tags if needed, enter a password, and then click **Continue**.

   Some of the fields in this page are self-explanatory. The following table describes fields for which you might need guidance:

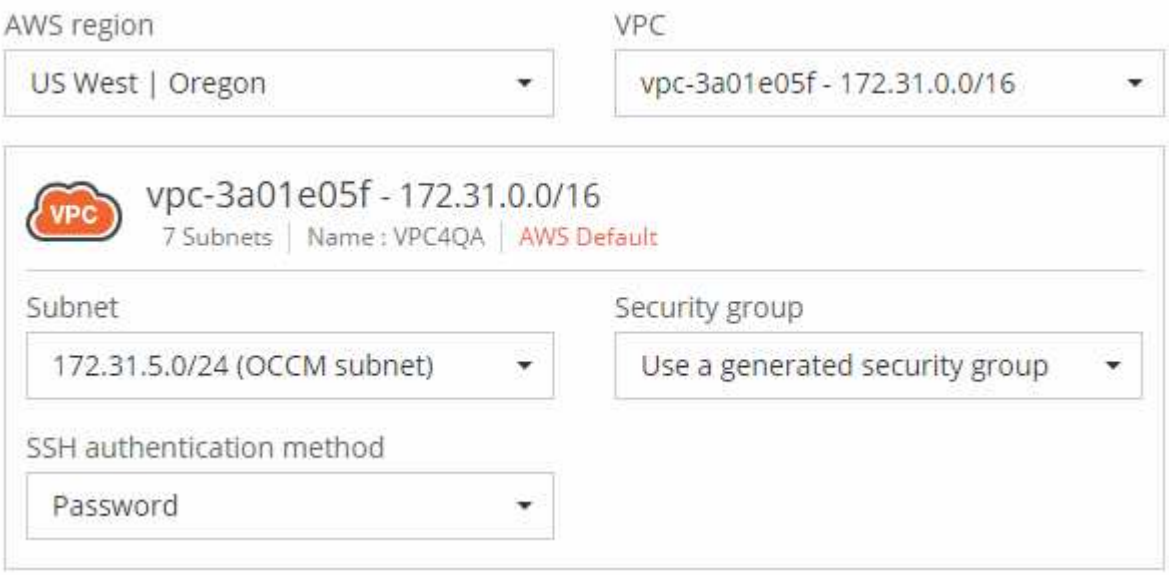
Field	Description
Credentials	These are the credentials for the ONTAP Cloud cluster admin account. You can use these credentials to connect to ONTAP Cloud through OnCommand System Manager or its CLI.

Field	Description
Name	Cloud Manager uses the working environment name to name both the ONTAP Cloud system and the Amazon EC2 instance. It also uses the name as the prefix for the predefined security group, if you select that option.
AWS tags	AWS tags are metadata for your AWS resources. Cloud Manager adds the tags to the ONTAP Cloud instance and each AWS resource associated with the instance. For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources.

If AWS keys were not specified for your Cloud Manager account, you are prompted to enter them after you click Continue. You need to enter them before you can proceed.

4. On the Location page, enter the network information that you recorded in the AWS worksheet and then click **Continue**.

   The following image shows the Location page filled out:



5. On the Data Encryption page, choose no data encryption, ONTAP Cloud-managed encryption, or AWS-managed encryption.

   To better understand these options, see Data encryption in AWS.

   For AWS-managed encryption, you can choose a different master key if more than one key is available in your account.

If Cloud Manager was not set up for encryption, the Cloud Manager Admin must set it up. See Setting up ONTAP Cloud encryption.

6. If you chose ONTAP Cloud encryption, select one to four key managers, select the certificate of the CA that signed the server certificate for each key manager, and then click **Continue**.

The key manager CA certificate is for all selected key managers, which means the same certificate authority (CA) must have signed the server certificate for each key manager.

7. On the ONTAP Cloud BYOL License page, specify whether you want to enter a license for this ONTAP Cloud system.

   To understand how licenses work, see Licensing.

8. On the Preconfigured Packages page, select one of the packages to quickly launch an ONTAP Cloud system, or click **Create my own configuration**.

   If you choose one of the packages, you only need to specify a volume and then review and approve the configuration.

9. On the IAM Role page, you should keep the default option to let Cloud Manager create the role for you.

   If you prefer to use your own policy, it must meet policy requirements for ONTAP Cloud nodes.

10. On the Licensing page, change the ONTAP Cloud version as needed, select a license, an instance type, the instance tenancy, and then click **Continue**.

    If your needs change after you launch the instance, you can modify the license or instance type later.

    If a newer Release Candidate, General Availability, or patch release is available for the selected version, then Cloud Manager updates the system to that version when creating the working environment. For example, the update occurs if you select ONTAP Cloud 9.3 RC1 and ONTAP Cloud 9.3 GA is available. The update does not occur from one release to another—for example, from 9.2 to 9.3.

11. If the NetApp Support Site credentials page is displayed, enter your NetApp Support Site credentials.

    Credentials are required for BYOL instances. For details, see Why you should link a tenant to your NetApp Support Site account.

12. On the Underlying storage resources page, choose a single storage type or data tiering.

    The underlying AWS disk type is for the initial volume. You can choose a different disk type for subsequent volumes. For help choosing a disk type, see Choosing an AWS disk type.

13. On the Disk Size page, select the default disk size for all disks in the initial aggregate.

    For help choosing a size, see Choosing disk size.

14. On the Write Speed page, choose **Normal** or **High**.

    For help choosing between the options, see Choosing a write speed.

15. On the Create Volume page, enter details for the new volume, and then click **Continue**.

    You might skip this step if you want to create a volume for iSCSI. Cloud Manager sets up volumes for NFS and CIFS only.

    Some of the fields in this page are self-explanatory. The following table describes fields for which you might need guidance:

Field	Description
Size	The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.
Access control (for NFS only)	An export policy defines the clients in the subnet that can access the volume. By default, Cloud Manager enters a value that provides access to all instances in the subnet.
Permissions and Users / Groups (for CIFS only)	These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.
Volume Protection	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.
Usage Profile	Usage profiles define the NetApp storage efficiency features that are enabled for a volume. For more information, see Understanding volume usage profiles.

The following image shows the Volume page filled out for the CIFS protocol:

16. If you chose the CIFS protocol, set up a CIFS server on the ONTAP Cloud CIFS Setup page:

Field	Description
DNS Primary and Secondary IP Address	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.

Field	Description
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.
DNS Domain	The DNS domain for the ONTAP Cloud storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.

17. On the Review & Approve page, review and confirm your selections:
    a. Review details about the configuration.
    b. Click **More information** to review details about support and the AWS resources that Cloud Manager will purchase.
    c. Select the **I understand…** check boxes.
    d. Click **Go**.

Result

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

If you experience any issues launching the ONTAP Cloud instance, review the failure message. You can also select the working environment and click Re-create environment.

For additional help, go to NetApp ONTAP Cloud Support.

After you finish

- If you launched an ONTAP Cloud pay-as-you-go instance and the tenant is not linked to a NetApp Support Site account, manually register the instance with NetApp to enable support. For instructions, see Registering ONTAP Cloud instances.

  Support from NetApp is included with your ONTAP Cloud instance. To activate support, you must first register the instance with NetApp.

- If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.
- If you want to apply quotas to volumes, use System Manager or the CLI.

  Quotas enable you to restrict or track the disk space and number of files used by a user, group, or qtree.

- If this is the first ONTAP Cloud instance launched in AWS, remind your administrator to finish setting up AWS billing and cost management for Cloud Manager by enabling the WorkingEnvironmentId tag. This tag is not available in AWS until after you create your first ONTAP Cloud working environment under the AWS payer account.

Launching an ONTAP Cloud HA pair in AWS

If you want to launch an ONTAP Cloud HA pair in AWS, you need to create an ONTAP Cloud HA working environment in Cloud Manager.

Before you begin

- You should have prepared by choosing a configuration and by obtaining AWS networking information from your administrator. For details, see Planning your ONTAP Cloud configuration.
- If you purchased ONTAP Cloud BYOL licenses, you must have a 20-digit serial number (license key) for each node, and you must have credentials for a NetApp Support Site account if the tenant is not already associated with an account.
- If you want to use CIFS, you must have set up DNS and Active Directory. For details, see AWS networking requirements.

About this task

Immediately after you create the working environment, Cloud Manager launches a test instance in the specified VPC to verify connectivity. If successful, Cloud Manager immediately terminates the instance and then starts deploying the ONTAP Cloud system. If Cloud Manager cannot verify connectivity, creation of the working environment fails. The test instance is either a t2.nano (for default VPC tenancy) or m3.medium (for dedicated VPC tenancy).

Steps

1. On the Working Environments page, click **Add environment**.
2. Under Create, select **ONTAP Cloud HA**.
3. On the Details and Credentials page, enter a name for the working environment, add AWS tags if required, enter a password, and then click **Continue**.

   Some of the fields in this page are self-explanatory. The following table describes fields for which you might need guidance:

Field	Description
Credentials	These are the credentials for the ONTAP Cloud cluster admin account. You can use these credentials to connect to ONTAP Cloud through OnCommand System Manager or its CLI.
Name	Cloud Manager uses the working environment name to name the ONTAP Cloud cluster and the Amazon EC2 instances. It also uses the name as the prefix for the predefined security group, if you select that option.
AWS tags	AWS tags are metadata for your AWS resources. Cloud Manager adds the tags to the ONTAP Cloud instances and each AWS resource associated with the instances. For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources.

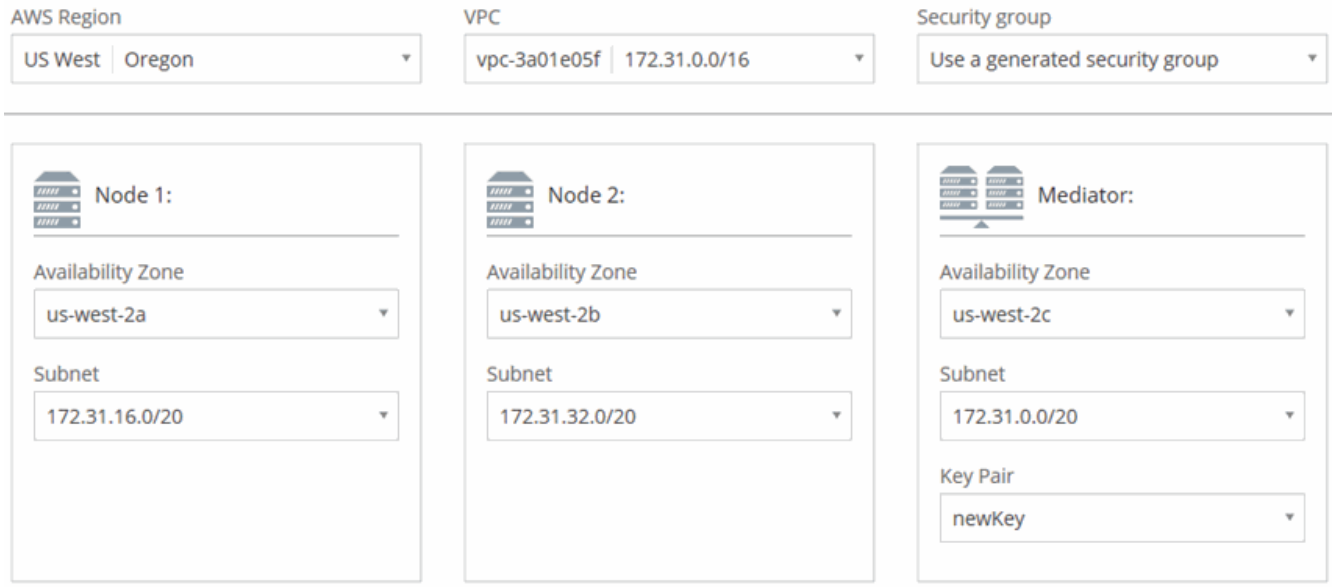
   If AWS keys were not specified for your Cloud Manager account, you are prompted to enter them after you click Continue. You must enter the AWS keys before you proceed.

4. On the HA Deployment Models page, choose an HA configuration.

   For an overview of the deployment models, see ONTAP Cloud HA for AWS.

5. On the Location page, enter the network information that you recorded in the AWS worksheet and then click **Continue**.

   The following image shows the Location page filled out for a multiple AZ configuration:



6. On the Connectivity and SSH Authentication page, choose connection methods for the HA pair and the mediator.
7. If you chose multiple AZs, specify the floating IP addresses for the cluster management interface port and the two NFS/CIFS data ports and then click **Continue**.

   The IP addresses must be outside of the CIDR block for all VPCs in the region. For additional details, see AWS networking requirements for ONTAP Cloud HA in multiple AZs.

8. If you chose multiple AZs, select the route tables that should include routes to the floating IP addresses and then click **Continue**.

   If you have more than one route table, it is very important to select the correct route tables. Otherwise, some clients might not have access to the ONTAP Cloud HA pair. For more information about route tables, refer to AWS Documentation: Route Tables.

9. On the Data Encryption page, choose no data encryption, ONTAP Cloud-managed encryption, or AWS-managed encryption.

   To better understand these options, see Data encryption in AWS.

   For AWS-managed encryption, you can choose a different master key if more than one key is available in your account.

   If Cloud Manager was not set up for encryption, the Cloud Manager Admin must set it up. See Setting up ONTAP Cloud encryption.

10. If you selected ONTAP Cloud encryption, select one to four key managers, select the certificate of the CA that signed the server certificate for each key manager, and then click **Continue**.

    The key manager CA certificate is for all selected key managers, which means the same certificate authority (CA) must have signed the server certificate for each key manager.

11. On the ONTAP Cloud BYOL License page, specify whether you want to enter a license for this ONTAP Cloud system.

To understand how licenses work, see Licensing.

12. On the Preconfigured Packages page, select one of the packages to quickly launch an ONTAP Cloud system, or click **Create my own configuration**.

    If you choose one of the packages, you only need to specify a volume and then review and approve the configuration.

13. On the IAM Role page, you should keep the default option to let Cloud Manager create the roles for you.

    If you prefer to use your own policy, it must meet policy requirements for ONTAP Cloud nodes.

14. On the Licensing page, change the ONTAP Cloud version as needed, select a license, an instance type, the instance tenancy, and then click **Continue**.

    If your needs change after you launch the instances, you can modify the license or instance type later.

    > If a newer Release Candidate, General Availability, or patch release is available for the selected version, then Cloud Manager updates the system to that version when creating the working environment. For example, the update occurs if you select ONTAP Cloud 9.3 RC1 and ONTAP Cloud 9.3 GA is available. The update does not occur from one release to another—for example, from 9.2 to 9.3.

15. If the NetApp Support Site credentials page is displayed, enter your NetApp Support Site credentials.

    Credentials are required for BYOL instances. For details, see Why you should link a tenant to your NetApp Support Site account.

16. On the Underlying storage resources page, choose a single storage type or data tiering.

    The underlying AWS disk type is for the initial volume. You can choose a different disk type for subsequent volumes. For help choosing a disk type, see Choosing an AWS disk type.

17. On the Disk Size page, select the default disk size for all disks in the initial aggregate.

    For help choosing a size, see Choosing disk size.

18. On the Write Speed page, choose **Normal** or **High**.

    For help choosing between the options, see Choosing a write speed.

19. On the Create Volume page, enter details for the new volume, and then click **Continue**.

    You might skip this step if you want to create a volume for iSCSI. Cloud Manager sets up volumes for NFS and CIFS only.

    Some of the fields in this page are self-explanatory. The following table describes fields for which you might need guidance:

Field	Description
Size	The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.

Field	Description
Access control (for NFS only)	An export policy defines the clients in the subnet that can access the volume. By default, Cloud Manager enters a value that provides access to all instances in the subnet.
Permissions and Users / Groups (for CIFS only)	These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.
Volume Protection	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.
Usage Profile	Usage profiles define the NetApp storage efficiency features that are enabled for a volume. Understanding volume usage profiles

The following image shows the Volume page filled out for the CIFS protocol:

20. If you selected the CIFS protocol, set up a CIFS server on the ONTAP Cloud CIFS Setup page:

Field	Description
DNS Primary and Secondary IP Address	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.

Field	Description
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.
DNS Domain	The DNS domain for the ONTAP Cloud storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.

21. On the Review & Approve page, review and confirm your selections:
    a. Review details about the configuration.
    b. Click **More information** to review details about support and the AWS resources that Cloud Manager will purchase.
    c. Select the **I understand…** check boxes.
    d. Click **Go**.

Result

Cloud Manager launches the ONTAP Cloud HA pair. You can track the progress in the timeline.

If you experience any issues launching the HA pair, review the failure message. You can also select the working environment and click Re-create environment.

For additional help, go to NetApp ONTAP Cloud Support.

After you finish

- If you launched an ONTAP Cloud pay-as-you-go instance and the tenant is not linked to a NetApp Support Site account, manually register the instance with NetApp to enable support. For instructions, see Registering ONTAP Cloud instances.

  Support from NetApp is included with your ONTAP Cloud instance. To activate support, you must first register the instance with NetApp.

- If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.
- If you want to apply quotas to volumes, use System Manager or the CLI.

  Quotas enable you to restrict or track the disk space and number of files used by a user, group, or qtree.

- If this is the first ONTAP Cloud instance launched in AWS, remind your administrator to finish setting up AWS billing and cost management for Cloud Manager by enabling the WorkingEnvironmentId tag. This tag is not available in AWS until after you create your first ONTAP Cloud working environment under the AWS payer account.

Launching ONTAP Cloud in Azure

You can launch a single ONTAP Cloud system in Azure by creating an ONTAP Cloud working environment in Cloud Manager.

Before you begin

- You should have prepared by choosing a configuration and by obtaining Azure networking information from your administrator. For details, see Planning your ONTAP Cloud configuration.
- If you want to launch an ONTAP Cloud BYOL instance, you must have the 20-digit serial number (license key) and you must have credentials for a NetApp Support Site account, if the tenant is not already linked with an account.

About this task

When Cloud Manager creates an ONTAP Cloud system in Azure, it creates a resource group that includes the security group, network interfaces, and two storage accounts: one for Azure Standard Storage and one for Premium Storage.

Steps

1. On the Working Environments page, click **Add environment**.
2. Under Create, select **ONTAP Cloud**.
3. On the Details and Credentials page, optionally change the Azure subscription, specify a cluster name and resource group name, add tags if needed, and then specify credentials.

   The following table describes fields for which you might need guidance:

Field	Description
Azure Subscription	If the Azure service principal is bound to multiple Azure subscriptions, select the current subscription and then choose another subscription. For instructions about binding the service principal, see Granting Azure Permissions to Cloud Manager.
Working Environment Name	Cloud Manager uses the working environment name to name both the ONTAP Cloud system and the Azure virtual machine. It also uses the name as the prefix for the predefined security group, if you select that option.
Resource Group Name	If you uncheck **Use Default**, you can type the name of an existing resource group or a new resource group.
Tags	Tags are metadata for your Azure resources. Cloud Manager adds the tags to the ONTAP Cloud system and each Azure resource associated with the system. For information about tags, refer to Microsoft Azure Documentation: Using tags to organize your Azure resources.
Credentials	These are the credentials for the ONTAP Cloud cluster admin account. You can use these credentials to connect to ONTAP Cloud through OnCommand System Manager or its CLI.

   If Azure credentials were not specified for your Cloud Manager account, you are prompted to enter them after you click Continue. You need to enter them before you can proceed.

4. On the Location page, enter the network information that you recorded in the worksheet, select the checkbox to confirm network connectivity, and then click **Continue**.
5. On the ONTAP Cloud BYOL License page, specify whether you want to enter a license for this ONTAP Cloud system.

   To understand how licenses work, see Licensing.

6. On the Preconfigured Packages page, select one of the packages to quickly launch an ONTAP Cloud

system, or click **Create my own configuration**.

If you choose one of the packages, you only need to specify a volume and then review and approve the configuration.

7. On the Licensing page, change the ONTAP Cloud version as needed, select a license and a virtual machine type, and then click **Continue**.

   If your needs change after you launch the system, you can modify the license or virtual machine type later.

   > If a newer Release Candidate, General Availability, or patch release is available for the selected version, then Cloud Manager updates the system to that version when creating the working environment. For example, the update occurs if you select ONTAP Cloud 9.3 RC1 and ONTAP Cloud 9.3 GA is available. The update does not occur from one release to another—for example, from 9.2 to 9.3.

8. On the Azure Marketplace page, follow the steps if Cloud Manager could not enable programmatic deployments of ONTAP Cloud.
9. If the NetApp Support Site credentials page is displayed, enter your NetApp Support Site credentials.

   Credentials are required for BYOL instances. For details, see Why you should link a tenant to your NetApp Support Site account.

10. On the Underlying storage resources page, choose either **Premium Storage** or **Standard Storage**.

    The disk type is for the initial volume. You can choose a different disk type for subsequent volumes. For help choosing a disk type, see Choosing an Azure disk type.

11. On the Disk Size page, select the default disk size for all disks in the initial aggregate and for any additional aggregates that Cloud Manager creates when you use the simple provisioning option.

    You can create aggregates that use a different disk size by using the advanced allocation option.

    For help choosing a size, see Choosing disk size.

12. On the Write Speed page, choose **Normal** or **High**.

    For help choosing between the options, see Choosing a write speed.

13. On the Create Volume page, enter details for the new volume, and then click **Continue**.

    You should skip this step if you want to use iSCSI. Cloud Manager enables you to create volumes for NFS and CIFS only.

    Some of the fields in this page are self-explanatory. The following table describes fields for which you might need guidance:

Field	Description
Size	The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.

Field	Description
Access control (for NFS only)	An export policy defines the clients in the subnet that can access the volume. By default, Cloud Manager enters a value that provides access to all instances in the subnet.
Permissions and Users / Groups (for CIFS only)	These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.
Volume Protection	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.
Usage Profile	Usage profiles define the NetApp storage efficiency features that are enabled for a volume. Understanding volume usage profiles

The following image shows the Volume page filled out for the CIFS protocol:

14. If you chose the CIFS protocol, set up a CIFS server on the ONTAP Cloud CIFS Setup page:

Field	Description
DNS Primary and Secondary IP Address	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.

Field	Description
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.
DNS Domain	The DNS domain for the ONTAP Cloud storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.

15. On the Review & Approve page, review and confirm your selections:
    a. Review details about the configuration.
    b. Click **More information** to review details about support and the Azure resources that Cloud Manager will purchase.
    c. Select the **I understand…** check boxes.
    d. Click **Go**.

Result

Cloud Manager deploys the ONTAP Cloud system. You can track the progress in the timeline.

If you experience any issues deploying the ONTAP Cloud system, review the failure message. You can also select the working environment and click Re-create environment.

For additional help, go to NetApp ONTAP Cloud Support.

After you finish

- If you deployed an ONTAP Cloud pay-as-you-go system and the tenant is not linked to a NetApp Support Site account, manually register the system with NetApp to enable support. For instructions, see Registering ONTAP Cloud instances.

  Support from NetApp is included with your ONTAP Cloud system. To activate support, you must first register the system with NetApp.

- If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.
- If you want to apply quotas to volumes, use System Manager or the CLI.

  Quotas enable you to restrict or track the disk space and number of files used by a user, group, or qtree.

Registering pay-as-you-go systems

Support from NetApp is included with ONTAP Cloud Explore, Standard, and Premium systems, but you must first activate support by registering the systems with NetApp, if you have not set up automatic registration.

Before you begin

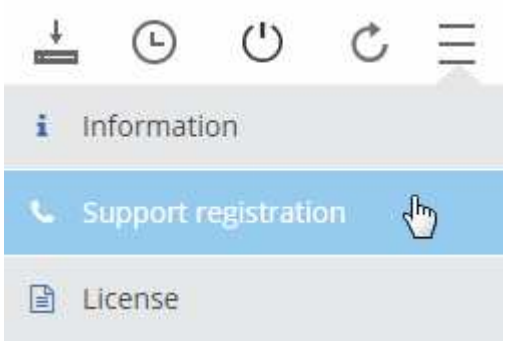
The host from which you are logged in to Cloud Manager must have internet access. If it does not, you can register from another location by going to NetApp ONTAP Cloud Registration.

About this task

If a tenant is linked to a NetApp Support Site account, Cloud Manager automatically registers the system with that account. However, if the tenant is not linked to an account, then you should register systems with NetApp after you launch them.

Steps

1. On the Working Environments page, double-click the name of the system that you want to register.
2. Click the menu icon and then click **Support registration**:



   The information that you need to register an instance is displayed:

   - Instance ID
   - Serial number
   - Account ID

3. To automatically register future instances in the tenant, click the link to enter your NetApp Support Site credentials.
4. To register this instance with NetApp support, click the link and then click **Register to NetApp support**.

   Following this link automatically completes the instance ID, serial number, and account ID in the registration form.

5. Follow the instructions to register your ONTAP Cloud instance.

Setting up ONTAP Cloud

After you deploy ONTAP Cloud, you can set it up by synchronizing the system time using NTP and by performing a few optional tasks from either System Manager or the CLI.

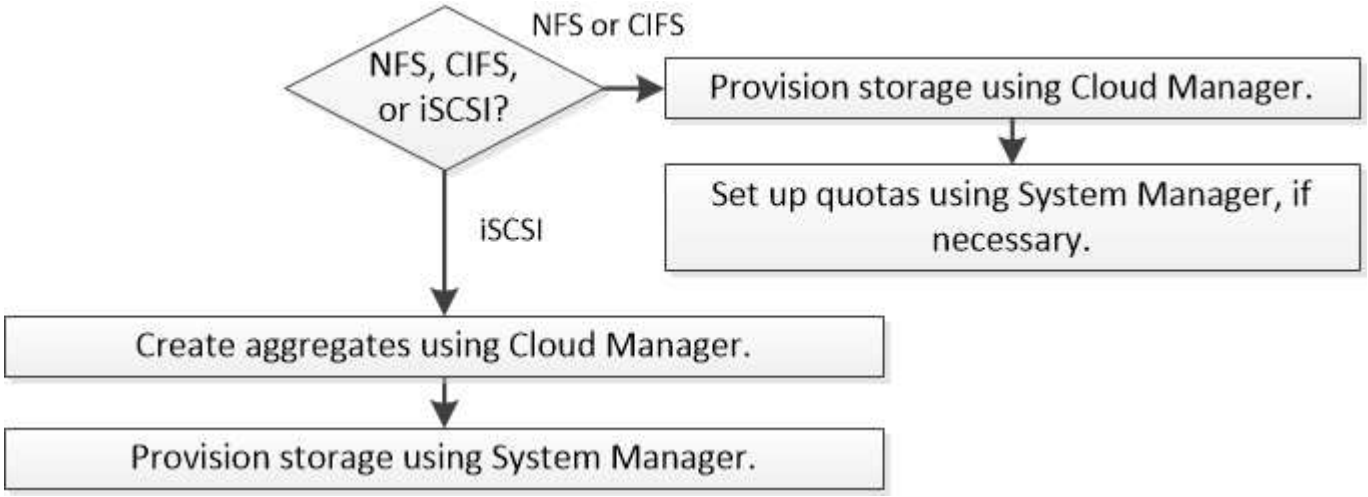
Task	Description
Synchronize the system time using NTP	ONTAP Cloud needs a Network Time Protocol (NTP) server to synchronize the time with clients and peered clusters. Problems can occur when the time is inaccurate. You can configure the NTP server using System Manager or the CLI. For instructions, see the System Manager Help or the ONTAP 9 System Administration Reference.

Task	Description
Optional: Configure AutoSupport	AutoSupport proactively monitors the health of your system and automatically sends messages to NetApp technical support by default. If the Cloud Manager Admin added a proxy server to Cloud Manager before you launched your instance, ONTAP Cloud is configured to use that proxy server for AutoSupport messages. You should test AutoSupport to ensure that it can send messages. For instructions, see the System Manager Help or the ONTAP 9 System Administration Reference.
Optional: Configure EMS	The Event Management System (EMS) collects and displays information about events that occur on ONTAP Cloud systems. To receive event notifications, you can set event destinations (email addresses, SNMP trap hosts, or syslog servers) and event routes for a particular event severity. You can configure EMS using the CLI. For instructions, see the ONTAP 9 EMS Configuration Express Guide.
Optional: Create an SVM management network interface (LIF)	If you want to use SnapDrive for Windows or SnapCenter with an ONTAP Cloud HA pair, you must create the storage virtual machine (SVM) management network interface (LIF) that SnapDrive and SnapCenter require. The SVM management LIF must use a floating IP address. You can create the LIF from System Manager or the CLI. The following example shows how to create the LIF from the CLI: `network interface create -vserver svm_cloud -lif svm_mgmt -role data -data-protocol none -home-node cloud-01 -home-port e0a -address 10.0.2.126 -netmask 255.255.255.0 -status-admin up -firewall -policy mgmt`
Optional: Change the backup location of configuration files	ONTAP Cloud automatically creates configuration backup files that contain information about the configurable options that it needs to operate properly. By default, ONTAP Cloud backs up the files to the Cloud Manager host every eight hours. If you want to send the backups to an alternate location, you can change the location to an FTP or HTTP server in your data center or in AWS. For example, you might already have a backup location for your FAS storage systems. You can change the backup location using the CLI. See the ONTAP 9 System Administration Reference.

Provisioning storage

You can provision additional NFS and CIFS storage for your ONTAP Cloud systems from Cloud Manager by managing volumes and aggregates. If you need to create iSCSI

storage, you should do so from System Manager.



Provisioning volumes

If you need more storage after you launch an ONTAP Cloud system, you can provision new NFS and CIFS volumes from Cloud Manager.

Before you begin

If you want to use CIFS in AWS, you must have set up DNS and Active Directory. For details, see AWS networking requirements.

Steps

1. On the Working Environments page, double-click the name of the ONTAP Cloud system on which you want to provision volumes.
2. Create a new volume on any aggregate or on a specific aggregate:

Action	Steps
Create a new volume and let Cloud Manager choose the containing aggregate	Click **Add New Volume**.
Create a new volume on a specific aggregate	a. Click the menu icon, and then click **Advanced > Advanced allocation**. b. Click the menu for an aggregate. c. Click **Create volume**.

3. Enter details for the new volume, and then click **Continue**.

   Some of the fields in this page are self-explanatory. The following table describes fields for which you might need guidance:

Field	Description
Size	The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.
Access control (for NFS only)	An export policy defines the clients in the subnet that can access the volume. By default, Cloud Manager enters a value that provides access to all instances in the subnet.
Permissions and Users / Groups (for CIFS only)	These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.
Volume Protection	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.

4. If you chose the CIFS protocol and the CIFS server has not been set up, specify details for the server in the Create a CIFS Server dialog box, and then click **Save and continue**:

Field	Description
DNS Primary and Secondary IP Address	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.
DNS Domain	The DNS domain for the ONTAP Cloud storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.

5. On the Usage Profile & Tiering page, choose a usage profile and disk type, and then click **Go**.

   For details about usage profiles, see Choosing a volume usage profile.

6. When prompted, click **Approve**.

Result

ONTAP Cloud provisions the volume.

After you finish

If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.

If you want to apply quotas to volumes, you must use System Manager or the CLI. Quotas enable you to restrict or track the disk space and number of files used by a user, group, or qtree.

Provisioning volumes on the second node in an HA configuration

By default, Cloud Manager creates volumes on the first node in an HA configuration. If you need an active-active configuration, in which both nodes serve data to clients, you must create aggregates and volumes on the second node.

Steps

1. On the Working Environments page, double-click the name of the ONTAP Cloud working environment on which you want to manage aggregates.
2. Click the menu icon and then click **Advanced > Advanced allocation**.
3. Click **Add Aggregate** and then create the aggregate.
4. For Home Node, choose the second node in the HA pair.
5. After Cloud Manager creates the aggregate, select it and then click **Create volume**.
6. Enter details for the new volume, and then click **Create**.

After you finish

You can create additional volumes on this aggregate if required.

When you mount the volume to clients, you must use the floating IP address of the node on which the volume resides.

Creating aggregates

You can create aggregates yourself or let Cloud Manager do it for you when it creates volumes. The benefit of creating aggregates yourself is that you can choose the underlying EBS disk size, which enables you to size your aggregate for the capacity or the performance that you need.

Steps

1. On the Working Environments page, double-click the name of the ONTAP Cloud instance on which you want to manage aggregates.
2. Click the menu icon, and then click **Advanced > Advanced allocation**.
3. Click **Add Aggregate** and then specify details for the aggregate.

   For help with disk type and disk size, see Planning your configuration.
4. Click **Go**, and then click **Approve and Purchase**.

Provisioning iSCSI LUNs

If you want to create iSCSI LUNs, you need to do so from System Manager.

Before you begin

- The Host Utilities must be installed and set up on the hosts that will connect to the LUN.
- You must have recorded the iSCSI initiator name from the host. You need to supply this name when you create an igroup for the LUN.
- Before you create volumes in System Manager, you must ensure that you have an aggregate with sufficient space. You need to create aggregates in Cloud Manager. For details, see Creating aggregates.

About this task

These steps describe how to use System Manager for ONTAP Cloud 9.3 and later.

Steps

1. Log in to System Manager.
2. Click **Storage > LUNs**.
3. Click **Create** and follow the prompts to create the LUN.
4. Connect to the LUN from your hosts.

   For instructions, see the Host Utilities documentation for your operating system.