Launching Cloud Volumes ONTAP in AWS

Cloud Manager 3.5

Ben Cammett
November 01, 2018

NetApp®

Table of Contents

Launching Cloud Volumes ONTAP in AWS 1
Launching a single Cloud Volumes ONTAP system in AWS 1
Launching a Cloud Volumes ONTAP HA pair in AWS 6

Launching Cloud Volumes ONTAP in AWS

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

Launching a single Cloud Volumes ONTAP system in AWS

If you want to launch Cloud Volumes ONTAP in AWS, you need to create a new 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 Cloud Volumes ONTAP configuration.
- If you want to launch a BYOL system, 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 Networking requirements for Cloud Volumes ONTAP in AWS.

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 Cloud Volumes ONTAP 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 Working Environment**.
2. Under Create, select **Cloud Volumes ONTAP**.
3. On the Details and Credentials page, optionally change the AWS account, enter a working environment name, add tags if needed, and then enter a password.

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

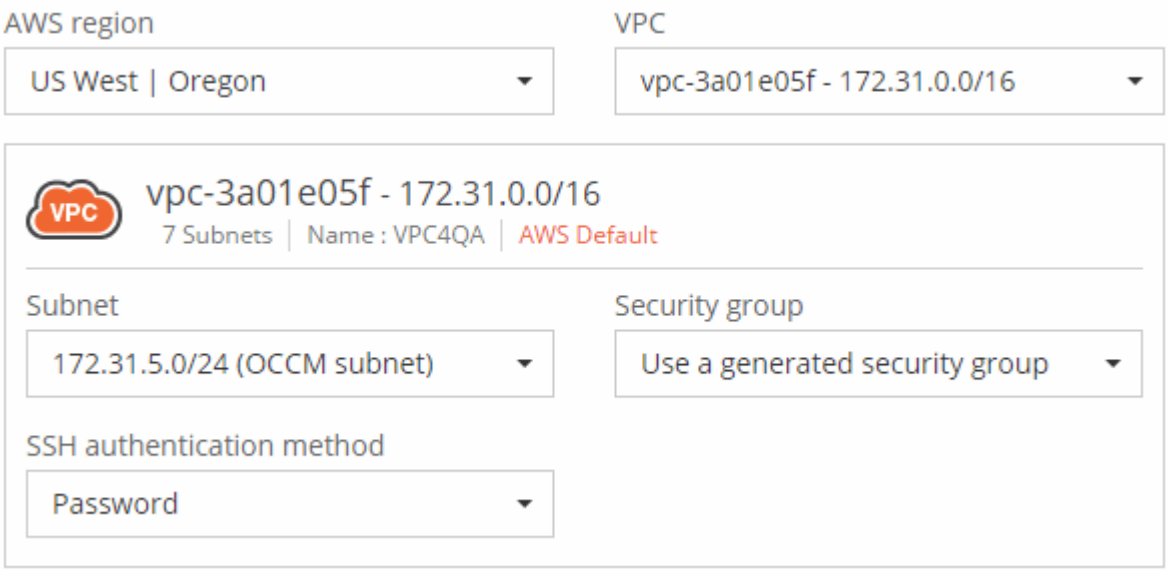
Field	Description
AWS Account	If you want to deploy Cloud Volumes ONTAP in other AWS accounts, then you must delegate access across accounts using an IAM role. For instructions, see Adding additional AWS accounts to Cloud Manager.

Field	Description
Working Environment Name	Cloud Manager uses the working environment name to name both the Cloud Volumes ONTAP system and the Amazon EC2 instance. It also uses the name as the prefix for the predefined security group, if you select that option.
Add tags	AWS tags are metadata for your AWS resources. Cloud Manager adds the tags to the Cloud Volumes ONTAP instance and each AWS resource associated with the instance. You can add up to four tags from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four tags when creating a working environment. For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources.
Credentials	These are the credentials for the Cloud Volumes ONTAP cluster admin account. You can use these credentials to connect to Cloud Volumes ONTAP through OnCommand System Manager or its CLI.

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 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.

6. On the BYOL License page, specify whether you have a license for this Cloud Volumes ONTAP system.

   To understand how licenses work, see Licensing.

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

8. 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 Cloud Volumes ONTAP nodes.

9. On the Licensing page, change the Cloud Volumes ONTAP 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 Cloud Volumes ONTAP 9.4 RC1 and 9.4 GA is available. The update does not occur from one release to another—for example, from 9.3 to 9.4.

10. 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.

11. On the Underlying Storage Resources page, choose a storage type and a disk size for all disks in the initial aggregate.

    You can choose a different disk type for subsequent volumes. For help choosing a disk type, see Choosing an AWS disk type.

For help choosing a disk size, see Choosing a disk size.

12. On the Write Speed & WORM page, choose **Normal** or **High** write speed, and activate write once, read many (WORM) storage, if desired.

    Learn more about write speed.

    Learn more about WORM storage.

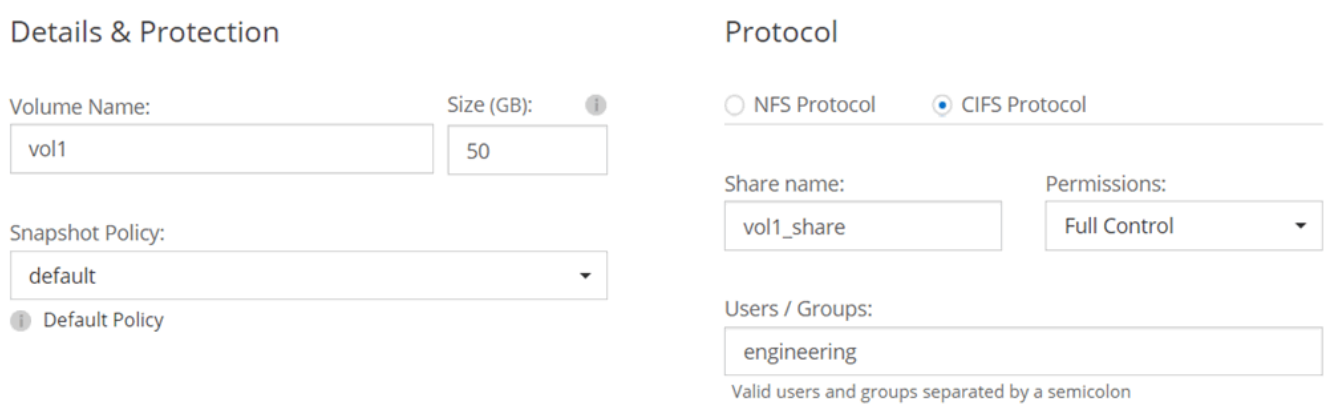
13. On the Create Volume page, enter details for the new volume, and then click **Continue**.

    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.
Snapshot Policy	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.

    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 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.
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 Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.

15. On the Usage Profile, Disk Type, and Tiering Policy page, choose whether you want to enable storage efficiency features and edit the S3 tiering policy, if needed.

    For more information, see Understanding volume usage profiles and Data tiering overview.

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

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

For additional help, go to NetApp Cloud Volumes ONTAP Support.

After you finish

- If you launched a 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 Cloud Volumes ONTAP.

  Support from NetApp is included with your Cloud Volumes ONTAP system. 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 Cloud Volumes ONTAP 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 Cloud Volumes ONTAP working environment under the AWS payer account.

Launching a Cloud Volumes ONTAP HA pair in AWS

If you want to launch a Cloud Volumes ONTAP HA pair in AWS, you need to create an 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 Cloud Volumes ONTAP configuration.
- If you purchased 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 Networking requirements for Cloud Volumes ONTAP in AWS.

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 Cloud Volumes ONTAP 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 Working Environment**.
2. Under Create, select **Cloud Volumes ONTAP HA**.
3. On the Details and Credentials page, optionally change the AWS account, enter a working environment name, add tags if needed, and then enter a password.

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

Field	Description
AWS Account	If you want to deploy Cloud Volumes ONTAP in other AWS accounts, then you must delegate access across accounts using an IAM role. For instructions, see Adding additional AWS accounts to Cloud Manager.
Working Environment Name	Cloud Manager uses the working environment name to name both the Cloud Volumes ONTAP system and the Amazon EC2 instance. It also uses the name as the prefix for the predefined security group, if you select that option.
Add tags	AWS tags are metadata for your AWS resources. Cloud Manager adds the tags to the Cloud Volumes ONTAP instance and each AWS resource associated with the instance. For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources.
Credentials	These are the credentials for the Cloud Volumes ONTAP cluster admin account. You can use these credentials to connect to Cloud Volumes ONTAP through OnCommand System Manager or its CLI.

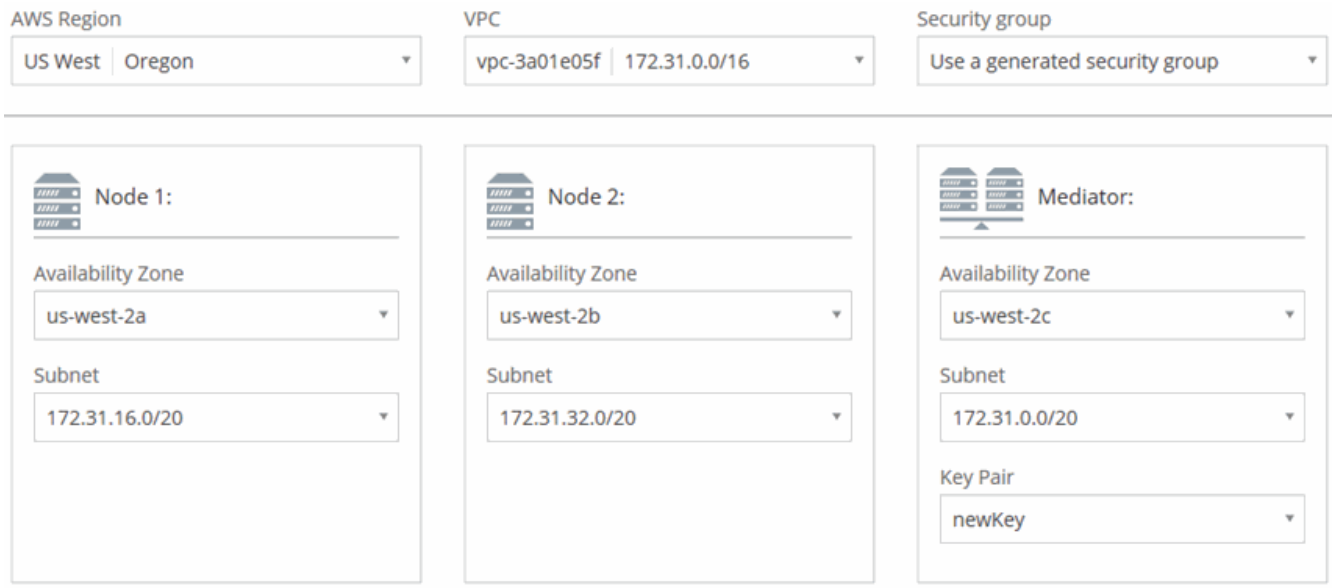
If AWS keys were not specified for your Cloud Manager account, you are prompted to enter them after you click Continue. You must enter the AWS keys before you proceed.

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

   For an overview of the deployment models, see Cloud Volumes ONTAP 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 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 Cloud Volumes ONTAP 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 Cloud Volumes ONTAP HA pair. For more information about route tables, refer to AWS Documentation: Route Tables.

9. On the Data Encryption page, choose no data 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.

10. On the BYOL License page, specify whether you have a license for this Cloud Volumes ONTAP system.

    To understand how licenses work, see Licensing.

11. On the Preconfigured Packages page, select one of the packages to quickly launch a Cloud Volumes ONTAP 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.

12. 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 Cloud Volumes ONTAP nodes and the HA mediator.

13. On the Licensing page, change the Cloud Volumes ONTAP 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 Cloud Volumes ONTAP 9.4 RC1 and 9.4 GA is available. The update does not occur from one release to another—for example, from 9.3 to 9.4.

14. 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.

15. On the Underlying Storage Resources page, choose a storage type and a disk size for all disks in the initial aggregate.

    You can choose a different disk type for subsequent volumes. For help choosing a disk type, see Choosing an AWS disk type.

    For help choosing a disk size, see Choosing a disk size.

16. On the WORM page, activate write once, read many (WORM) storage, if desired.

    Learn more about WORM storage.

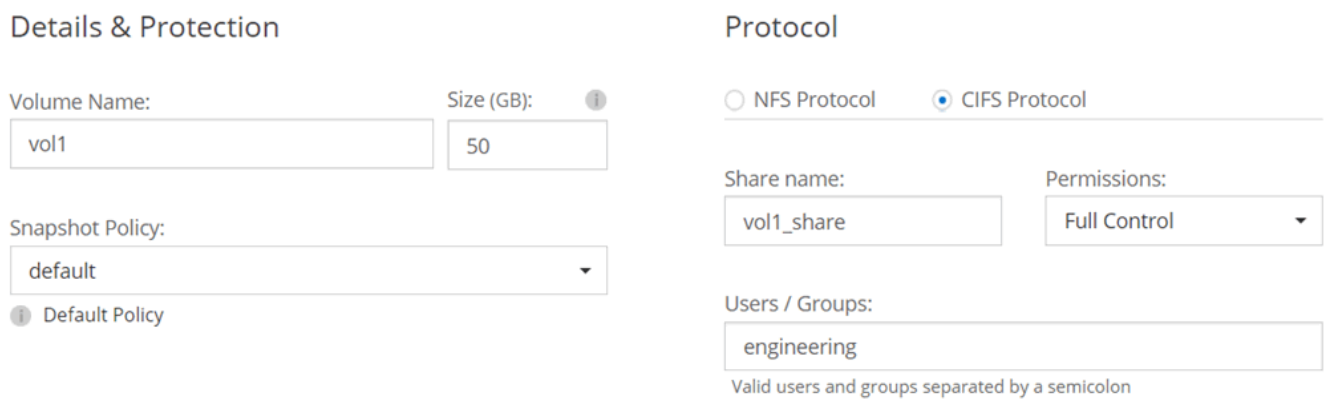
17. On the Create Volume page, enter details for the new volume, and then click **Continue**.

    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.
Snapshot Policy	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.

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



18. If you selected the CIFS protocol, set up a CIFS server on the 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.

Field	Description
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 Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.

19. On the Usage Profile, Disk Type, and Tiering Policy page, choose whether you want to enable storage efficiency features and edit the S3 tiering policy, if needed.

    For more information, see Understanding volume usage profiles and Data tiering overview.

20. 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 Cloud Volumes ONTAP 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 Cloud Volumes ONTAP Support.

After you finish

- If you launched a 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 Cloud Volumes ONTAP.

  Support from NetApp is included with your Cloud Volumes ONTAP system. 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 Cloud Volumes ONTAP 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 Cloud Volumes ONTAP working environment under the AWS payer account.