



Getting Started with AWS public cloud

NetApp Solutions

NetApp
October 15, 2021

This PDF was generated from https://docs.netapp.com/us-en/netapp-solutions/ent-apps-db/hybrid_dbops_snapcenter_getting_started_aws.html on October 21, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Getting Started with AWS public cloud	1
AWS public cloud	1

Getting Started with AWS public cloud

Previous: [Getting started on-premises.](#)

AWS public cloud



To make things easier to follow, we have created this document based on a deployment in AWS. However, the process is very similar for Azure and GCP.

1. Pre-flight check

Before deployment, make sure that the infrastructure is in place to allow for the deployment in the next stage. This includes the following:

- AWS account
- VPC in your region of choice
- Subnet with access to the public internet
- Permissions to add IAM roles into your AWS account
- A secret key and access key for your AWS user

2. Steps to deploy Cloud Manager and Cloud Volumes ONTAP in AWS



There are many methods for deploying Cloud Manager and Cloud Volumes ONTAP; this method is the simplest but requires the most permissions. If this method is not appropriate for your AWS environment, please consult the [NetApp Cloud Documentation](#).

Deploy the Cloud Manager connector

1. Navigate to [NetApp Cloud Central](#) and log in or sign up.



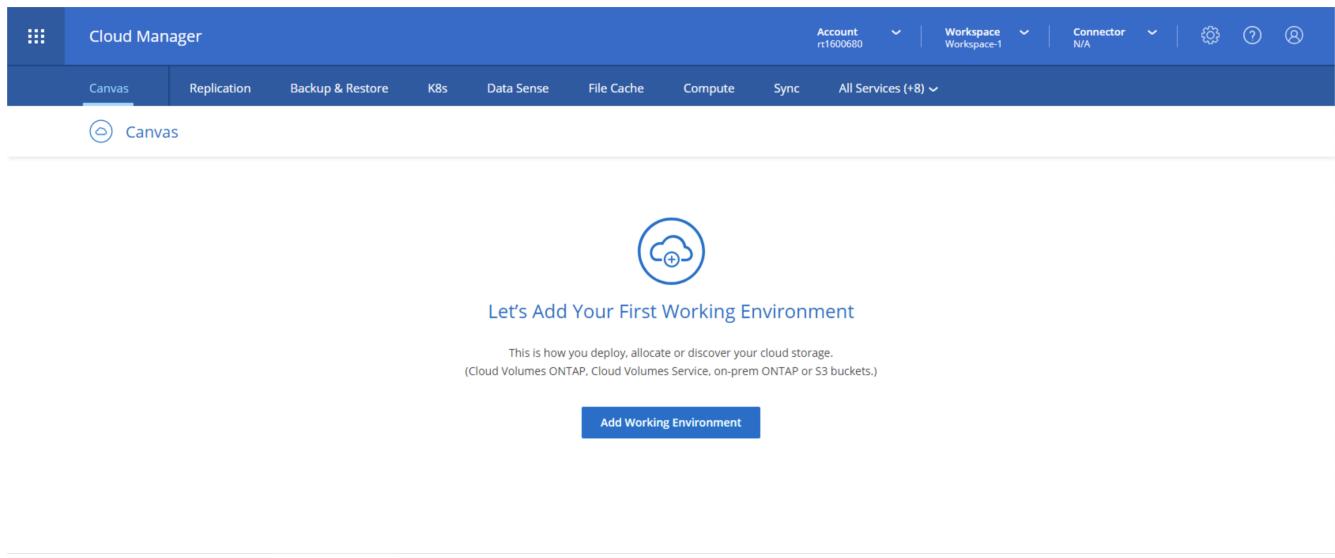
[Continue to Cloud Manager](#)

Log In to NetApp Cloud Central

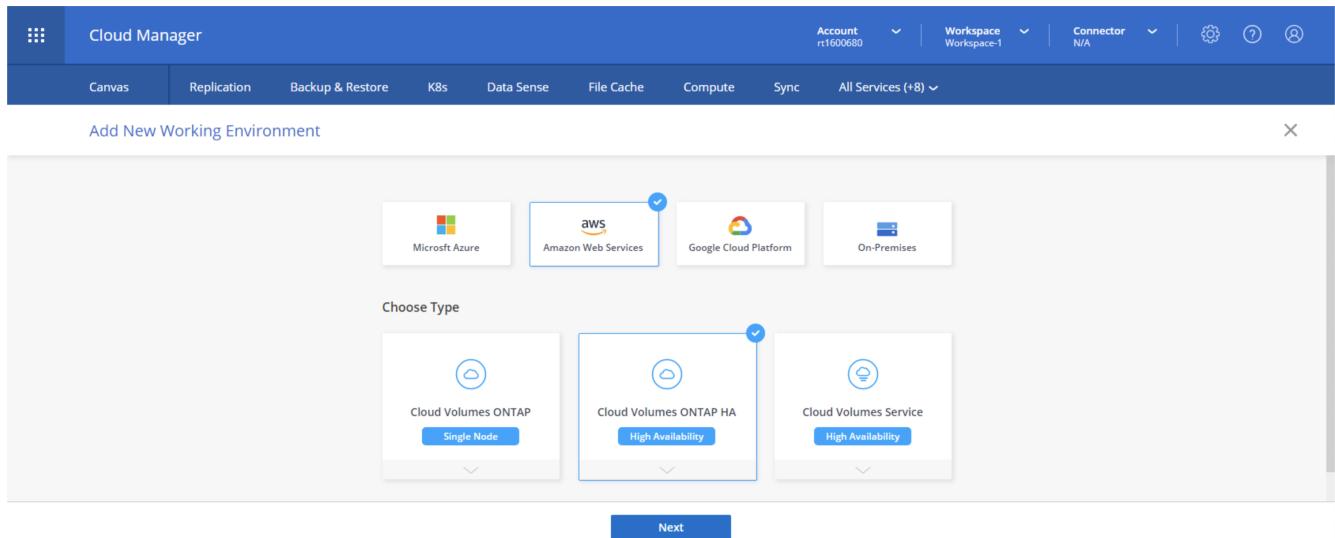
Don't have an account yet? [Sign Up](#)

[Forgot your password?](#)

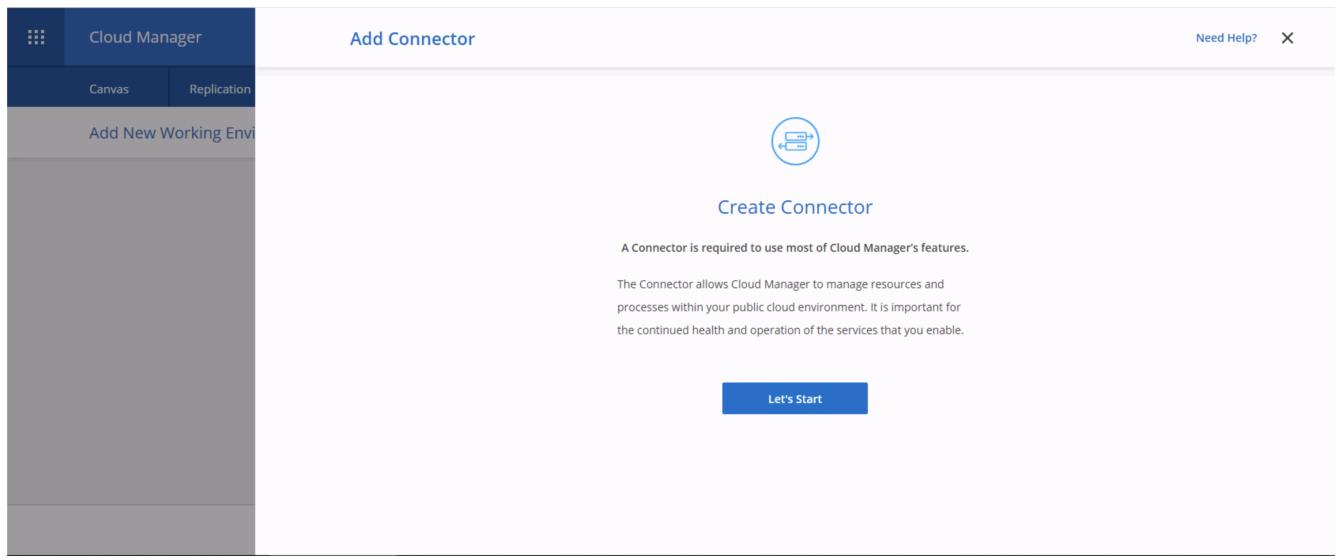
2. After you log in, you should be taken to the Canvas.



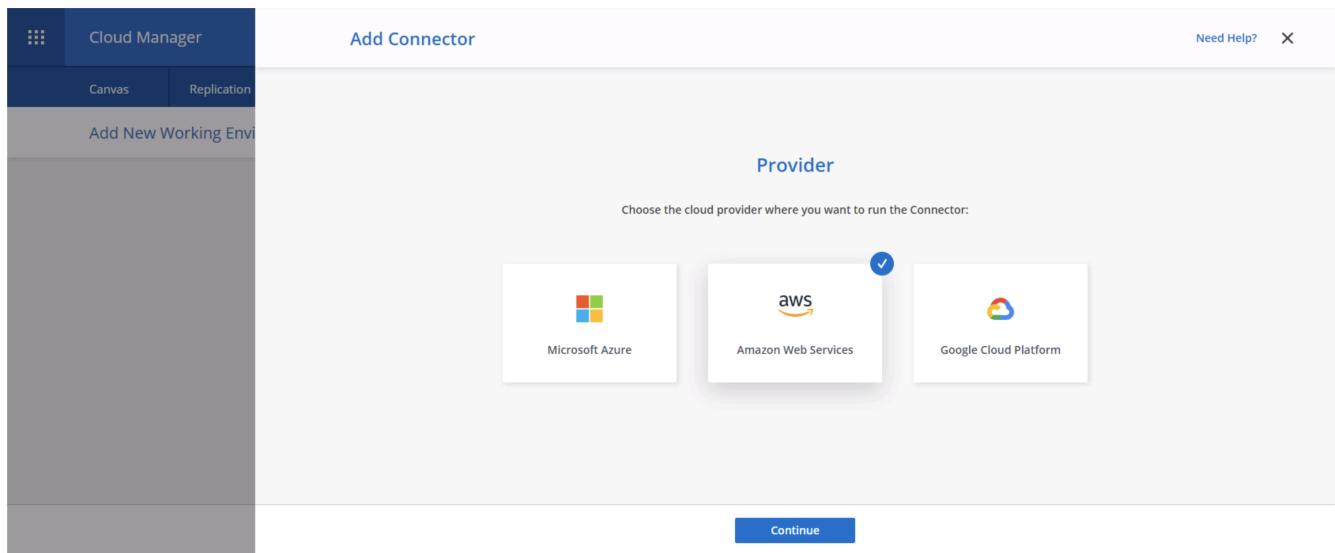
3. Click "Add Working Environment" and choose Cloud Volumes ONTAP in AWS. Here, you also choose whether you want to deploy a single node system or a high availability pair. I have chosen to deploy a high availability pair.



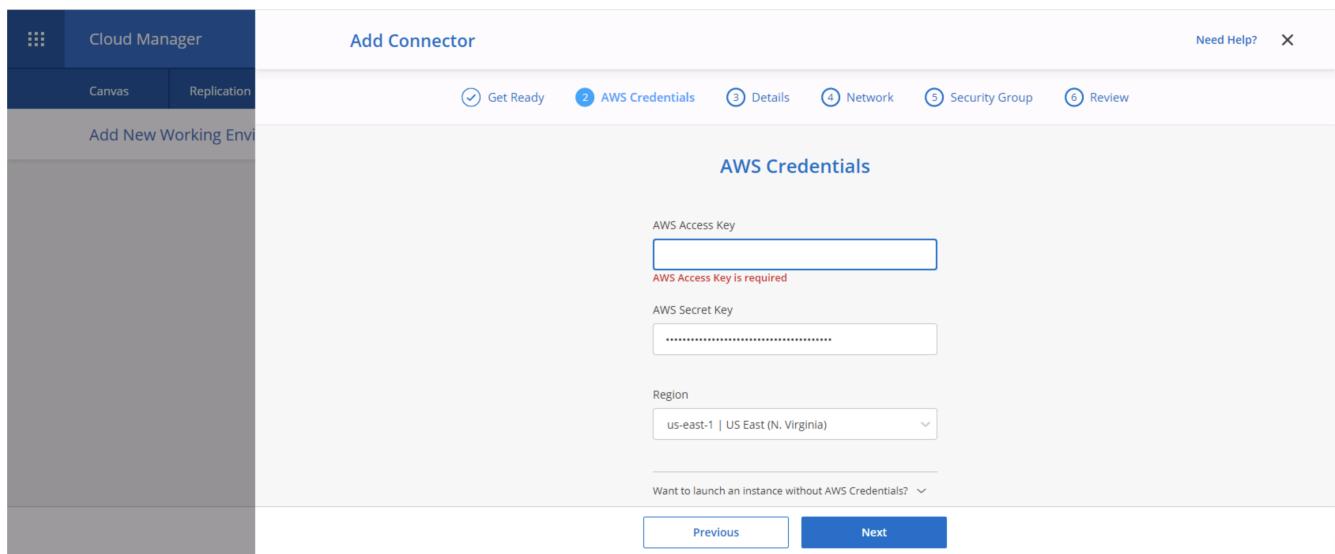
4. If no connector has been created, a pop-up appears asking you to create a connector.



5. Click Lets Start, and then choose AWS.



6. Enter your secret key and access key. Make sure that your user has the correct permissions outlined on the [NetApp policies page](#).



7. Give the connector a name and either use a predefined role as described on the [NetApp policies page](#) or ask Cloud Manager to create the role for you.

Cloud Manager

Add Connector

Get Ready AWS Credentials Details Network Security Group Review

Connector Instance Name: awscloudmanager

Connector Role:

- Create Role
- Select an existing Role

Role Name: Cloud-Manager-Operator-IBNt24

Add Tags to Connector Instance

Previous Next

8. Give the networking information needed to deploy the connector. Verify that outbound internet access is enabled by:
- Giving the connector a public IP address
 - Giving the connector a proxy to work through
 - Giving the connector a route to the public internet through an Internet Gateway

Cloud Manager

Add Connector

Get Ready AWS Credentials Details Network Security Group Review

Connectivity

VPC: vpc-083fcbd79f75dfb6e - 10.221.0.0/16

Subnet: 10.221.4.0/24 | publicSN_us-east-1a_rt1600...

Proxy Configuration (Optional)

HTTP Proxy: Example: http://172.16.254.1:8080

Define Credentials for this Proxy

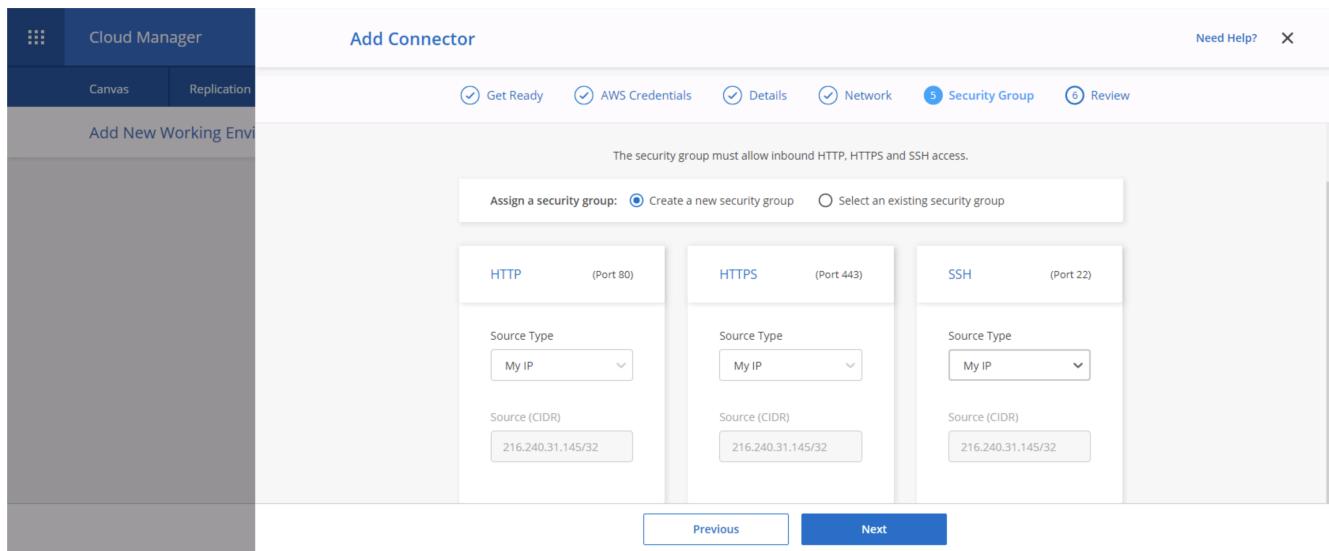
Upload a root certificate

Key Pair: rt1600680

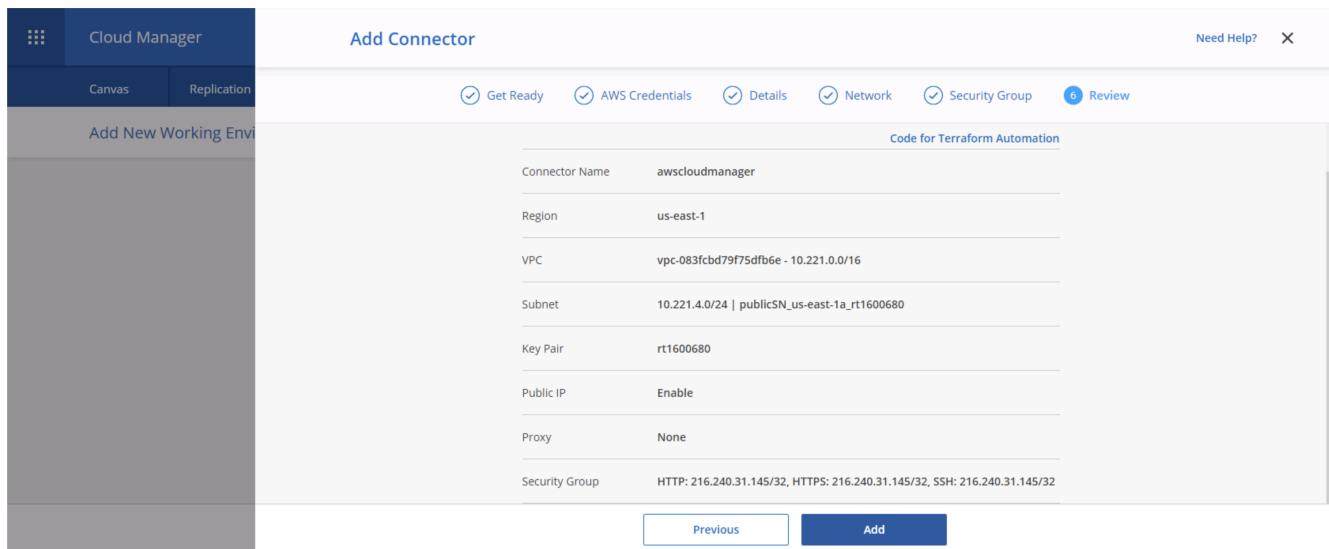
Public IP: Enable

Previous Next

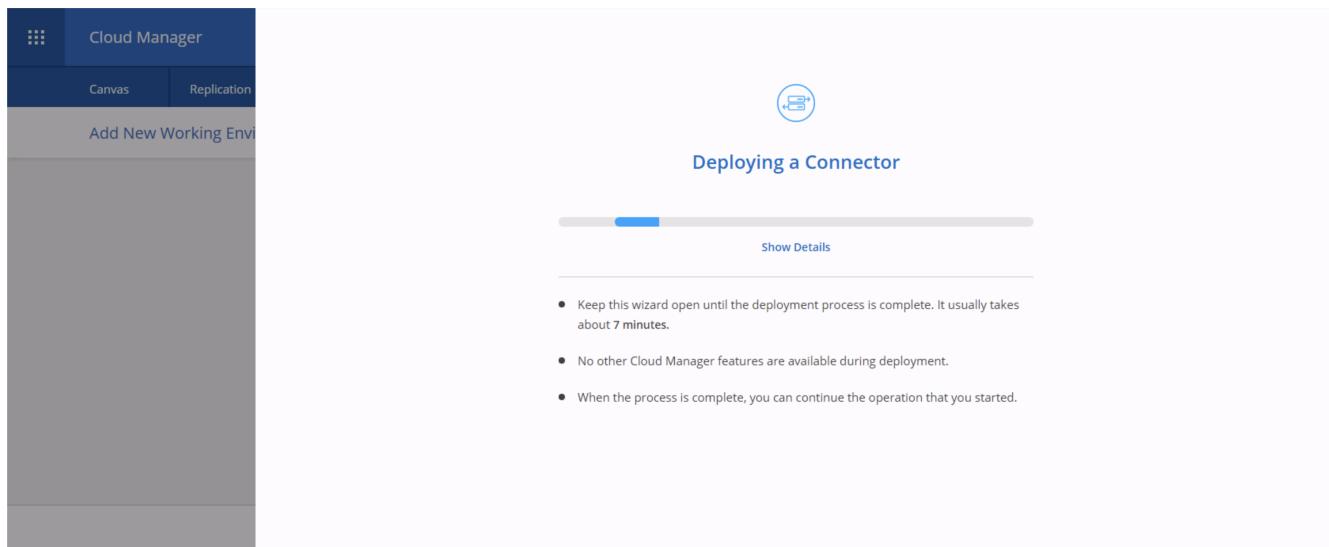
9. Provide communication with the connector via SSH, HTTP, and HTTPS by either providing a security group or creating a new security group. I have enabled access to the connector from my IP address only.



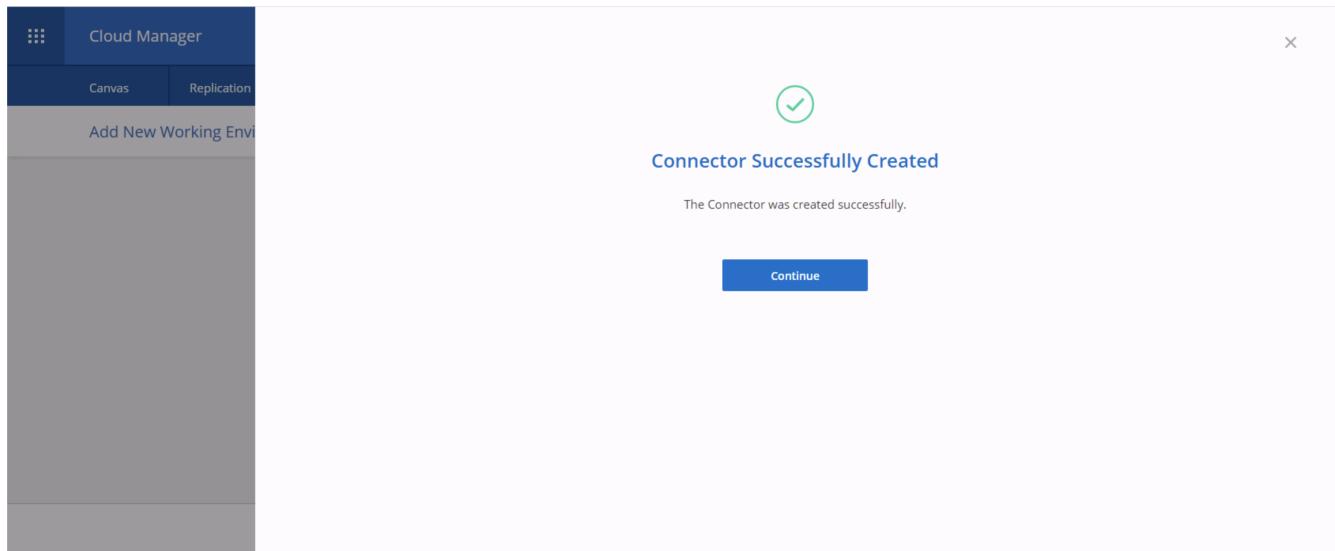
10. Review the information on the summary page and click Add to deploy the connector.



11. The connector now deploys using a cloud formation stack. You can monitor its progress from Cloud Manager or through AWS.

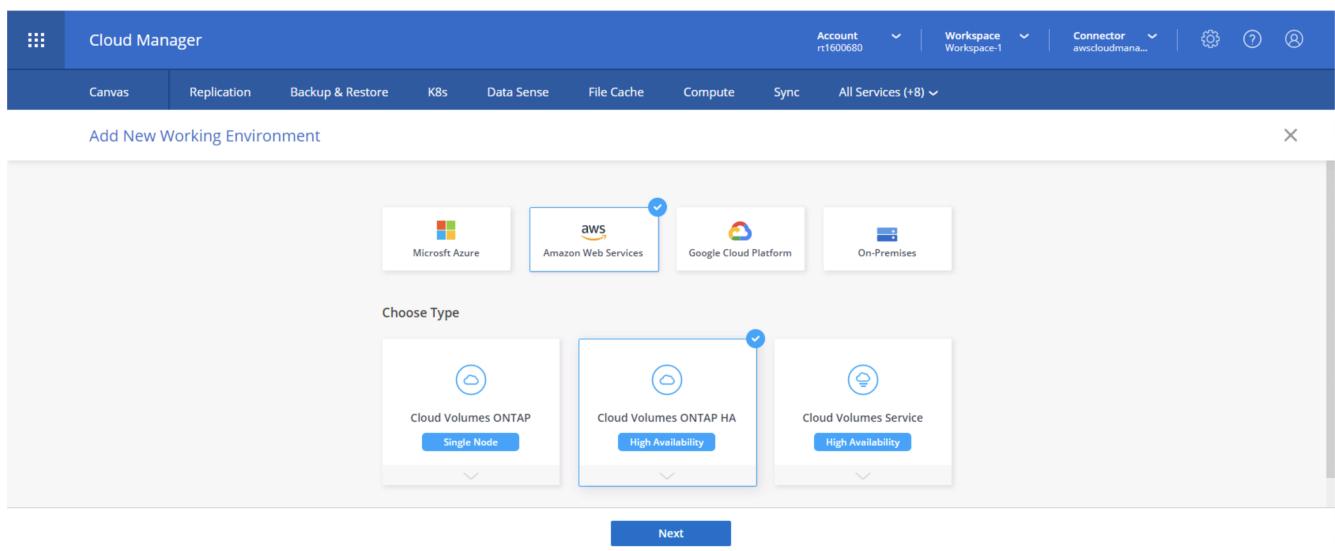


12. When the deployment is complete, a success page appears.



Deploy Cloud Volumes ONTAP

1. Select AWS and the type of deployment based on your requirements.



2. If no subscription has been assigned and you wish to purchase with PAYGO, choose Edit Credentials.

The screenshot shows the 'Create a New Working Environment' wizard, Step 2: Details and Credentials. The top bar includes account (rt1600680), workspace (Workspace-1), connector (awscloudman...), and navigation icons. The main area has tabs for 'Previous Step' (highlighted), 'Instance Profile' (322944748816), 'Credential Name' (Account ID), and 'Marketplace Subscription'. A note says 'No subscription is associated'. A 'Edit Credentials' button is visible. Below, 'Details' and 'Credentials' sections are shown, with 'Working Environment Name' set to 'Up to 40 characters' and 'User Name' set to 'admin'. A 'Continue' button is at the bottom.

3. Choose Add Subscription.

The screenshot shows the 'Edit Credentials & Add Subscription' step. It displays the 'Associate Subscription to Credentials' section with a dropdown for 'Credentials' (Instance Profile | Account ID: 322944748816) and a note 'No subscription is associated with this credential'. A '+ Add Subscription' button is present. The 'Apply' and 'Cancel' buttons are at the bottom.

4. Choose the type of contract that you wish to subscribe to. I chose Pay-as-you-go.

The screenshot shows the 'Edit Credentials & Add Subscription' step. It displays a note: 'Select a subscription option and click Continue. The AWS Marketplace enables you to view pricing details and then subscribe.' Two options are shown: 'Pay-Per-TiB - Annual Contract' (radio button) and 'Pay-as-you-go' (radio button, selected). Below, 'The next steps:' list: 1. AWS Marketplace (Subscribe and then click Set Up Your Account to configure your account.) and 2. Cloud Manager (Save your subscription and associate the Marketplace subscription with your AWS credentials.). 'Continue' and 'Cancel' buttons are at the bottom.

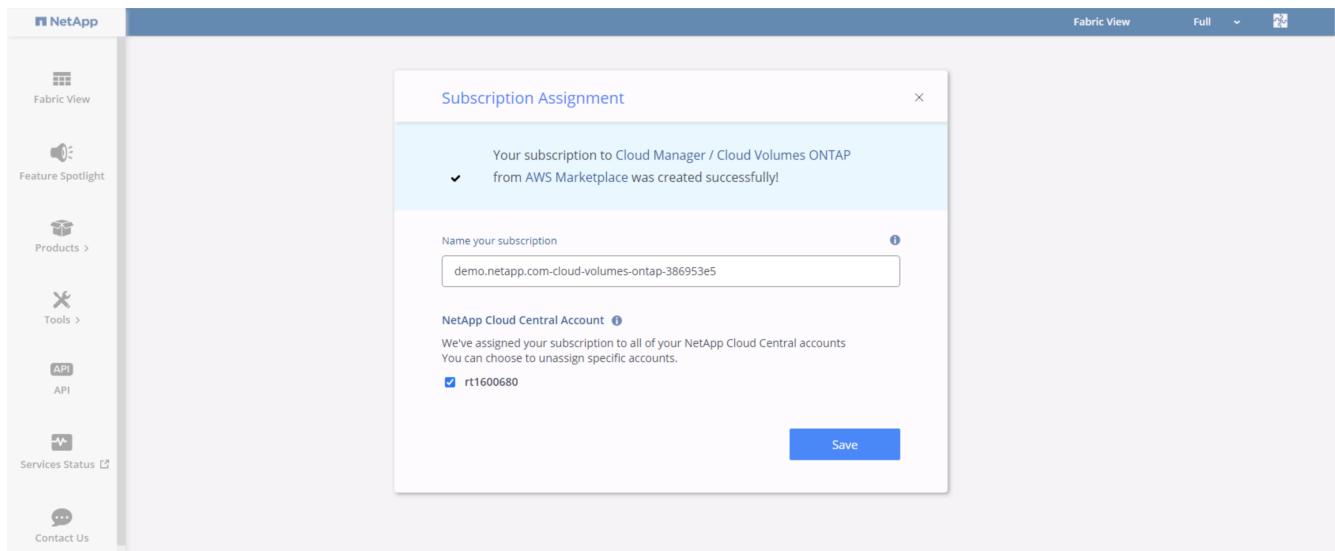
5. You are redirected to AWS; choose Continue to Subscribe.

The screenshot shows the AWS Marketplace interface. At the top, there's a navigation bar with links like 'About', 'Categories', 'Delivery Methods', 'Solutions', 'AWS IQ', 'Resources', and 'Your Saved List'. On the right, there are links for 'Partners', 'Sell in AWS Marketplace', 'Amazon Web Services Home', and 'Help'. A search bar is located at the top right. The main content area features a product card for 'Cloud Manager - Deploy & Manage NetApp Cloud Data Services' by NetApp, Inc. The card includes a brief description: 'Start here to deploy and manage Cloud Volumes ONTAP, Cloud Tiering, Cloud Data Sense, Cloud Backup and Cloud Volumes Service. Accelerate critical business apps with speed,' followed by a 'Show more' link. Below the card are tabs for 'Overview' (which is selected), 'Pricing', 'Usage', 'Support', and 'Reviews'. To the right of the card is a 'Highlights' section with a bulleted list: 'Streamline the deployment of all your NetApp Cloud Volumes ONTAP environments', 'Centrally manage your NetApp based storage and replicate across availability zones or to and from your data center', and 'Enable your IT administrators to audit and track your cloud storage resource spend'. At the bottom of the card, it says 'Cloud Manager eases the day-to-day requirements of operating your cloud storage environment including configuring, provisioning, and monitoring each of your active NetApp Cloud Data Services including their virtual and hardware storage nodes. It offers a'.

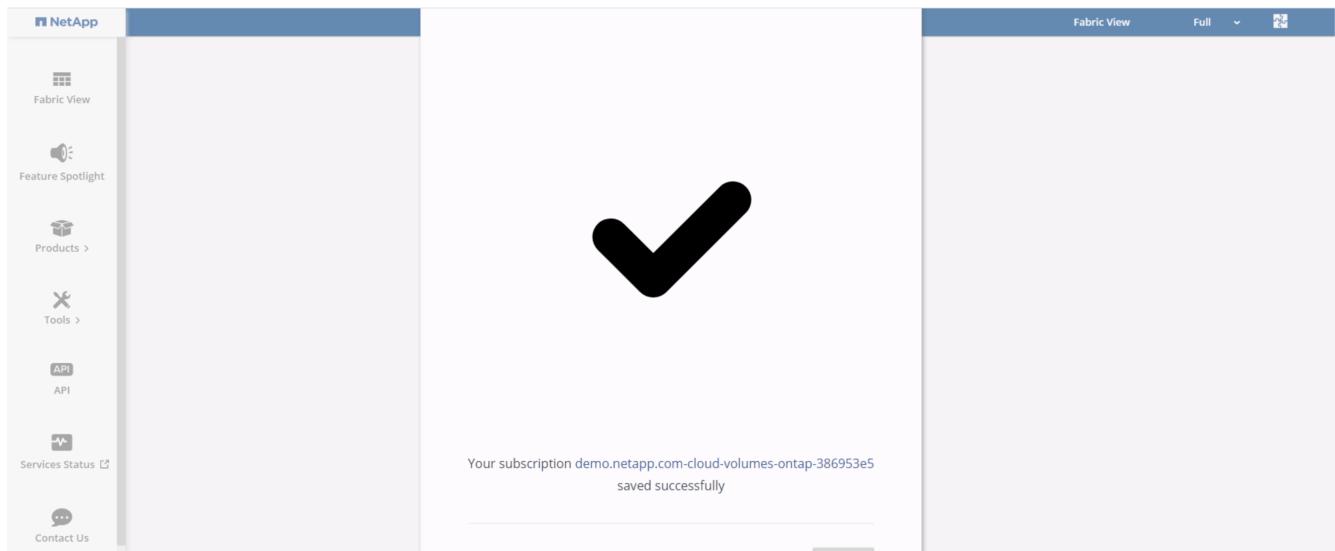
6. Subscribe and you are redirected back to NetApp Cloud Central. If you have already subscribed and don't get redirected, choose the "Click here" link.

The screenshot shows the AWS Marketplace subscription confirmation page. The top navigation bar and search bar are visible. The main content area displays a message: 'You are extended multiple offers! Select an offer first and review the pricing information and EULA.' Below this, there's a dropdown menu showing 'Offer name: NetApp, Inc. for SaaS 2020-07-20- Private Offer - current subscription'. To the right, there's a note: 'You are subscribed to this offer. By: NetApp, Inc. Offer ID: offer-hmolsqhv7ji This offer is going to expire on August 1, 2022 UTC'. Further down, a box contains a question mark icon and the text: 'Having issues signing up for your product? If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.' To the right, another box says 'You Have Subscribed to a Private Offer' with detailed information about the subscription. At the bottom, there's a 'Subscribe' button and a note: 'By subscribing to this software, you agree to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You also agree and acknowledge that AWS may share information about this transaction.'

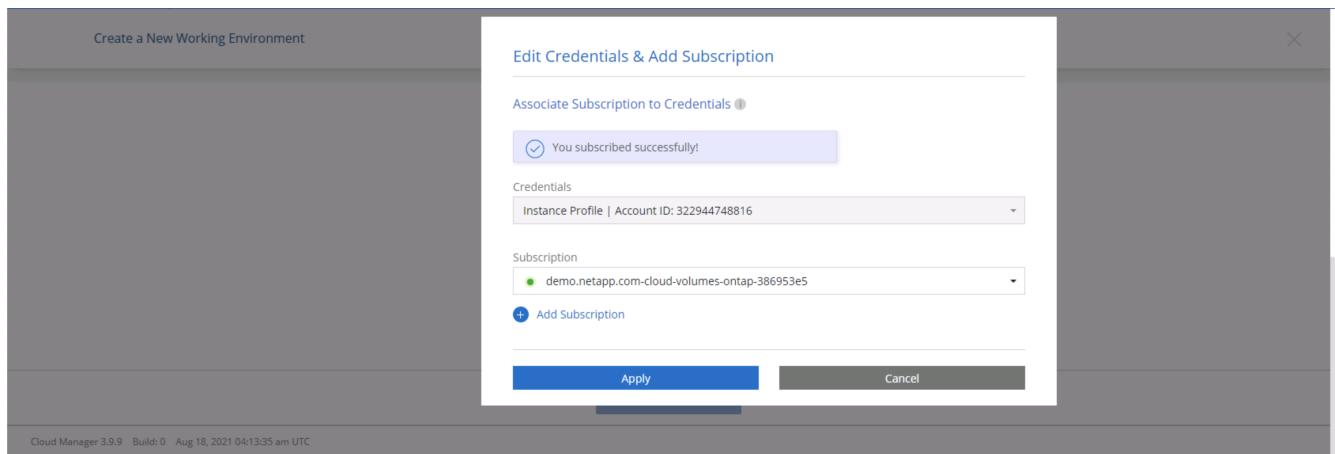
7. You are redirected to Cloud Central where you must name your subscription and assign it to your Cloud Central account.



- When successful, a check mark page appears. Navigate back to your Cloud Manager tab.



- The subscription now appears in Cloud Central. Click Apply to continue.



- Enter the working environment details such as:

- a. Cluster name

b. Cluster password

c. AWS tags (Optional)

The screenshot shows the 'Cloud Manager' interface with the title 'Create a New Working Environment'. The 'Details and Credentials' tab is selected. In the 'Details' section, the 'Working Environment Name (Cluster Name)' field contains 'hybridawscvo'. Below it, there is a link to 'Add Tags' and a note: 'Optional Field | Up to four tags'. In the 'Credentials' section, the 'User Name' field is set to 'admin', and the 'Password' and 'Confirm Password' fields both contain '*****'. A 'Continue' button is at the bottom.

11. Choose which additional services you would like to deploy. To discover more about these services, visit the [NetApp Cloud Homepage](#).

The screenshot shows the 'Cloud Manager' interface with the title 'Create a New Working Environment'. The 'Services' tab is selected. It lists three services with toggle switches: 'Data Sense & Compliance' (on), 'Backup to Cloud' (on), and 'Monitoring' (on). A 'Continue' button is at the bottom.

12. Choose whether to deploy in multiple availability zones (requires three subnets, each in a different AZ), or a single availability zone. I chose multiple AZs.

Cloud Manager

Account: rt1600680 | Workspace: Workspace-1 | Connector: awscloudman...

Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+8) ▾

Create a New Working Environment HA Deployment Models X

↑ Previous Step

Multiple Availability Zones

- Provides maximum protection against AZ failures.
- Enables selection of 3 availability zones.
- An HA node serves data if its partner goes offline.

Extended Info

Single Availability Zone

- Protects against failures within a single AZ.
- Single availability zone. HA nodes are in a placement group, spread across distinct underlying hardware.
- An HA node serves data if its partner goes offline.

Extended Info

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

13. Choose the region, VPC, and security group for the cluster to be deployed into. In this section, you also assign the availability zones per node (and mediator) as well as the subnets that they occupy.

Cloud Manager

Account: rt1600680 | Workspace: Workspace-1 | Connector: awscloudman...

Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+8) ▾

Create a New Working Environment Region & VPC X

↑ Previous Step

AWS Region: US East | N. Virginia

VPC: vpc-083fcbd79f75dfb6e - 10.221.0.0/16

Security group: Use a generated security group

Node 1:	Node 2:	Mediator:
Availability Zone: us-east-1a	Availability Zone: us-east-1b	Availability Zone: us-east-1c
Subnet: 10.221.1.0/24	Subnet: 10.221.2.0/24	Subnet: 10.221.3.0/24

Continue

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

14. Choose the connection methods for the nodes as well as the mediator.

Cloud Manager

Account: rt1600680 | Workspace: Workspace-1 | Connector: awscloudman...

Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+8) ▾

Create a New Working Environment Connectivity & SSH Authentication X

↑ Previous Step

Nodes	Mediator
SSH Authentication Method: Password	Security Group: Use a generated security group
	Key Pair Name: rt1600680
	Internet Connection Method: Public IP address

Continue

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC



The mediator requires communication with the AWS APIs. A public IP address is not required so long as the APIs are reachable after the mediator EC2 instance has been deployed.

1. Floating IP addresses are used to allow access to the various IP addresses that Cloud Volumes ONTAP uses, including cluster management and data serving IPs. These must be addresses that are not already routable within your network and are added to route tables in your AWS environment. These are required to enable consistent IP addresses for an HA pair during failover. More information about floating IP addresses can be found in the [NetApp Cloud Documentation](#).

The screenshot shows the 'Cloud Manager' interface with the 'Floating IPs' step selected. It includes fields for entering floating IP addresses for cluster management, NFS/CIFS data, and SVM management. A note explains that floating IPs can migrate between HA nodes if failures occur, and that an AWS transit gateway can be set up for external access. A 'Continue' button is at the bottom.

2. Select which route tables the floating IP addresses are added to. These route tables are used by clients to communicate with Cloud Volumes ONTAP.

The screenshot shows the 'Cloud Manager' interface with the 'Route Tables' step selected. It lists two route tables: 'private_rt_rt1600680' and 'public_rt_rt1600680'. Both are checked. A note states that selecting route tables enables client access to the HA pair. An 'Additional Information' link is present. A 'Continue' button is at the bottom.

3. Choose whether to enable AWS managed encryption or AWS KMS to encrypt the ONTAP root, boot, and data disks.

Cloud Manager

Account: rt1600680 | Workspace: Workspace-1 | Connector: awscloudman...

Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+8) ▾

Create a New Working Environment Data Encryption X

↑ Previous Step AWS Managed Encryption

AWS is responsible for data encryption and decryption operations. Key management is handled by AWS key management services.

Default Master Key: aws/ebs

Continue

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

4. Choose your licensing model. If you don't know which to choose, contact your NetApp representative.

Cloud Manager

Account: rt1600680 | Workspace: Workspace-1 | Connector: awscloudman...

Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+8) ▾

Create a New Working Environment Cloud Volumes ONTAP Charging Methods & NSS Account X

↑ Previous Step Cloud Volumes ONTAP Charging Methods

Learn more about our charging methods

Pay-As-You-Go by the hour

Bring your own license

Freemium (Up to 500GB)

NetApp Support Site Account (Optional)

Learn more about NetApp Support Site (NSS) accounts

To register this Cloud Volumes ONTAP to support, you should add NetApp Support Site Account.

Don't have a NetApp Support Site account? Select go to finish deploying this system. After it's created, use the Support Registration option to create an NSS account.

Add Netapp Support Site Account

Continue

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

5. Select which configuration best suits your use case. This is related to the sizing considerations covered in the prerequisites page.

Cloud Manager

Account: rt1600680 | Workspace: Workspace-1 | Connector: awscloudman...

Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+8) ▾

Create a New Working Environment Preconfigured Packages X

↑ Previous Step Select a preconfigured Cloud Volumes ONTAP system that best matches your needs, or create your own configuration. Preconfigured settings can be modified at a later time. Change Configuration

 POC and small workloads Up to 2TB of storage

 Database and application data production workloads Up to 10TB of storage

 Cost effective DR Up to 10TB of storage

 Highest performance production workloads Up to 368TB of storage

Continue

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

6. Optionally, create a volume. This is not required, because the next steps use SnapMirror, which creates the volumes for us.

Create a New Working Environment

Create Volume

↑ Previous Step

Details & Protection

Volume Name: Size (GB):

Snapshot Policy: Default Policy

Protocol

NFS CIFS iSCSI

Access Control:

Custom export policy

Advanced options

Continue Skip

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

7. Review the selections made and tick the boxes to verify that you understand that Cloud Manager deploys resources into your AWS environment. When ready, click Go.

Create a New Working Environment

Review & Approve

↑ Previous Step **hybridawscvo**

AWS | us-east-1 | HA

Show API request

I understand that in order to activate support, I must first register Cloud Volumes ONTAP with NetApp. [More information >](#)

I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements. [More information >](#)

Overview **Networking** **Storage**

Storage System:	Cloud Volumes ONTAP HA	HA Deployment Model:	Multiple Availability Zones
License Type:	Cloud Volumes ONTAP Standard	Encryption:	AWS Managed
Capacity Limit:	10TB	Customer Master Key:	aws/ebs

Go

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

8. Cloud Volumes ONTAP now starts its deployment process. Cloud Manager uses AWS APIs and cloud formation stacks to deploy Cloud Volumes ONTAP. It then configures the system to your specifications, giving you a ready-to-go system that can be instantly utilized. The timing for this process varies depending on the selections made.

The screenshot shows the Cloud Manager Canvas interface. At the top, there are tabs for Canvas, Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+8). The Canvas tab is selected. In the center, there's a cloud icon labeled "hybridawsco" containing "Cloud Volumes ONTAP" and "HA". Below it, a progress bar indicates "C Initializing". To the right, another cloud icon labeled "Amazon S3" shows "1 Buckets" and "1 Region". On the far right, a sidebar titled "Working environments" lists "1 Cloud Volumes ONTAP (High-Availability)" and "0 B Allocated Capacity", and "1 Amazon S3" with "0 Buckets". A "Go to Tabular View" link is at the top right.

9. You can monitor the progress by navigating to the Timeline.

The screenshot shows the Cloud Manager Timeline interface. The top navigation bar includes tabs for Canvas, Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+8). The Timeline tab is selected. The main area is divided into sections: "Resources" (Canvas, Digital Wallet, Timeline), "Services" (Replication, Backup & Restore, K8s, Data Sense, Compliance, Tiering, Monitoring, File Cache, Compute, Sync, SnapCenter, Active IQ), and a bottom section with a link to "https://cloudmanager.netapp.com/timeline".

10. The Timeline acts as an audit of all actions performed in Cloud Manager. You can view all of the API calls that are made by Cloud Manager during setup to both AWS as well as the ONTAP cluster. This can also be effectively used to troubleshoot any issues that you face.

The screenshot shows the Cloud Manager interface with the 'Timeline' tab selected. At the top, there are tabs for Canvas, Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+8). The Timeline section displays a table of deployment events:

Time	Action	Service	Agent	Resource	User	Status
Aug 18 2021, 9:42:32 pm	Check Connectivity	Cloud Manager	awscloudman...	hybridawscvo	Full Name	Success
Aug 18 2021, 9:42:00 pm	Create Aws Ha Working Environment	Cloud Manager	awscloudma...	hybridawscvo	Full Name	Pending
Aug 18 2021, 10:09:39 pm	Describe Operation Status					Success
Aug 19 2021, 10:00:20 pm	Describe Operation Status					Success

- After deployment is complete, the CVO cluster appears on the Canvas, which the current capacity. The ONTAP cluster in its current state is fully configured to allow a true, out-of-the-box experience.

The screenshot shows the Cloud Manager interface with the 'Canvas' tab selected. The main area displays two cloud icons representing deployed environments:

- Cloud Volumes ONTAP (High-Availability)**: Shows 1 GiB Allocated Capacity.
- Amazon S3**: Shows 2 Buckets and 1 Region.

To the right, a sidebar titled 'Working environments' lists the same resources with their details:

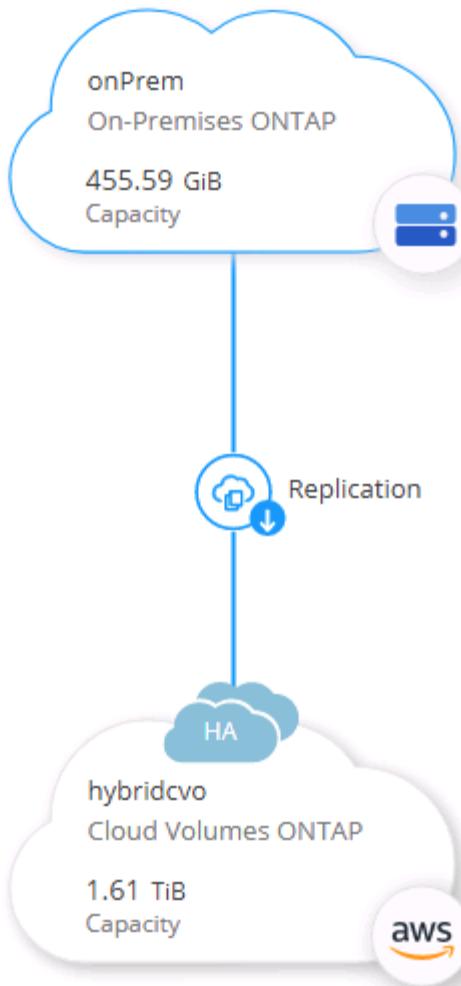
- 1 Cloud Volumes ONTAP (High-Availability)
1 GiB Allocated Capacity
- 1 Amazon S3
0 Buckets

Configure SnapMirror from on-premises to cloud

Now that you have a source ONTAP system and a destination ONTAP system deployed, you can replicate volumes containing database data into the cloud.

For a guide on compatible ONTAP versions for SnapMirror, see the [SnapMirror Compatibility Matrix](#).

- Click the source ONTAP system (on-premises) and either drag and drop it to the destination, select Replication > Enable, or select Replication > Menu > Replicate.



Select Enable.

SERVICES



Replication

■ Off

Enable



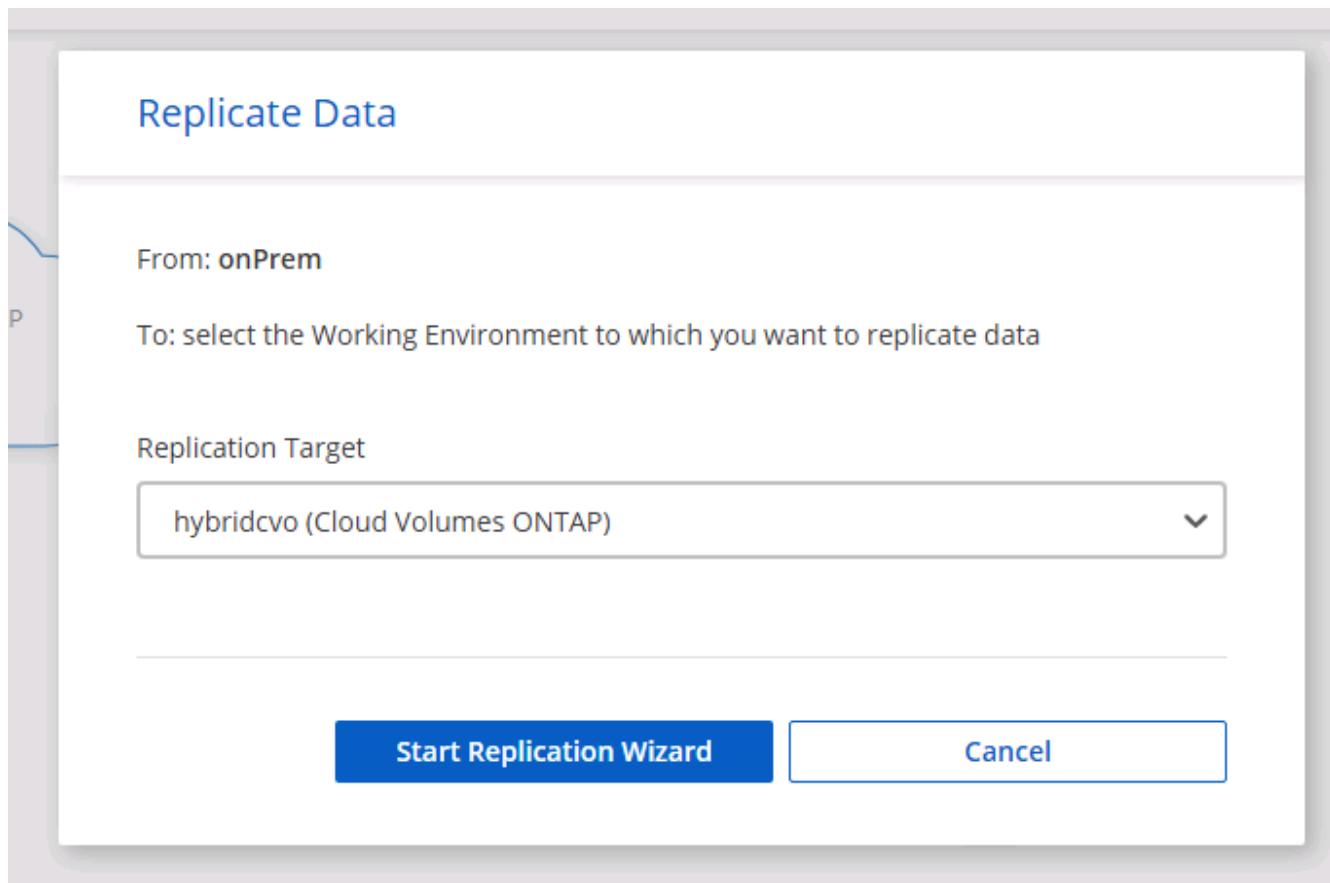
Or Options.

The screenshot shows the configuration for the 'onPrem' cluster. In the top left, there's a blue circular icon with two server racks labeled 'onPrem'. To its right, the status is shown as 'On'. On the far right are three small blue circles with icons: an info symbol, a vertical ellipsis, and a close/x symbol. Below this, under the heading 'DETAILS', it says 'On-PremisesONTAP'. Under the heading 'SERVICES', there's a section for 'Replication' with a cloud icon, labeled 'On' with a green square, and '1 Replication Target' with a blue circle containing a vertical ellipsis.

Replicate.

This screenshot is similar to the first one but includes a callout box pointing to the '1 Replication Target' entry in the 'Replication' section. The callout box contains two items: 'View Replications' with a list icon and 'Replicate' with a circular arrow icon. The rest of the interface elements are identical to the first screenshot.

2. If you did not drag and drop, choose the destination cluster to replicate to.



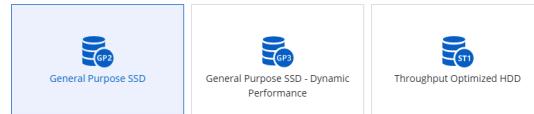
3. Choose the volume that you'd like to replicate. We replicated the data and all log volumes.

Replication Setup				Source Volume Selection			
rhel2_u03	■ ONLINE	rhel2_u0309232119421203118	■ ONLINE				
INFO		INFO					
Storage VM Name	svm_onPrem	Storage VM Name	svm_onPrem				
Tiering Policy	None	Tiering Policy	None				
Volume Type	RW	Volume Type	RW				
CAPACITY		CAPACITY					
100 GB Allocated	7.29 GB Disk Used	100 GB Allocated	35.83 MB Disk Used				
■ ONLINE	■ ONLINE	■ ONLINE	■ ONLINE				
sql1_log	■ ONLINE	sql1_snapctr	■ ONLINE				
INFO		INFO					
Storage VM Name	svm_onPrem	Storage VM Name	svm_onPrem				
Tiering Policy	None	Tiering Policy	None				
Volume Type	RW	Volume Type	RW				
CAPACITY		CAPACITY					
21.35 GB Allocated	18.16 GB Disk Used	24.87 GB Allocated	21.23 GB Disk Used				
■ ONLINE	■ ONLINE	■ ONLINE	■ ONLINE				
Cloud Manager 3.9.10 Build: 2 Sep 12, 2021 06:47:41 am UTC							

4. Choose the destination disk type and tiering policy. For disaster recovery, we recommend an SSD as the disk type and to maintain data tiering. Data tiering tiers the mirrored data into low-cost object storage and saves you money on local disks. When you break the relationship or clone the volume, the data uses the fast, local storage.

[↑ Previous Step](#)

Destination Disk Type



S3 Tiering

[What are storage tiers?](#) Enabled DisabledNote: If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.[Continue](#)

Cloud Manager 3.9.10 Build:2 Sep 12, 2021 06:47:41 am UTC

5. Select the destination volume name: we chose [source_volume_name]_dr.

Destination Volume Name

Destination Volume Name

sql1_data_dr

Destination Aggregate

Automatically select the best aggregate ▾

6. Select the maximum transfer rate for the replication. This enables you to save bandwidth if you have a low bandwidth connection to the cloud such as a VPN.

Max Transfer Rate

You should limit the transfer rate. An unlimited rate might negatively impact the performance of other applications and it might impact your Internet performance.

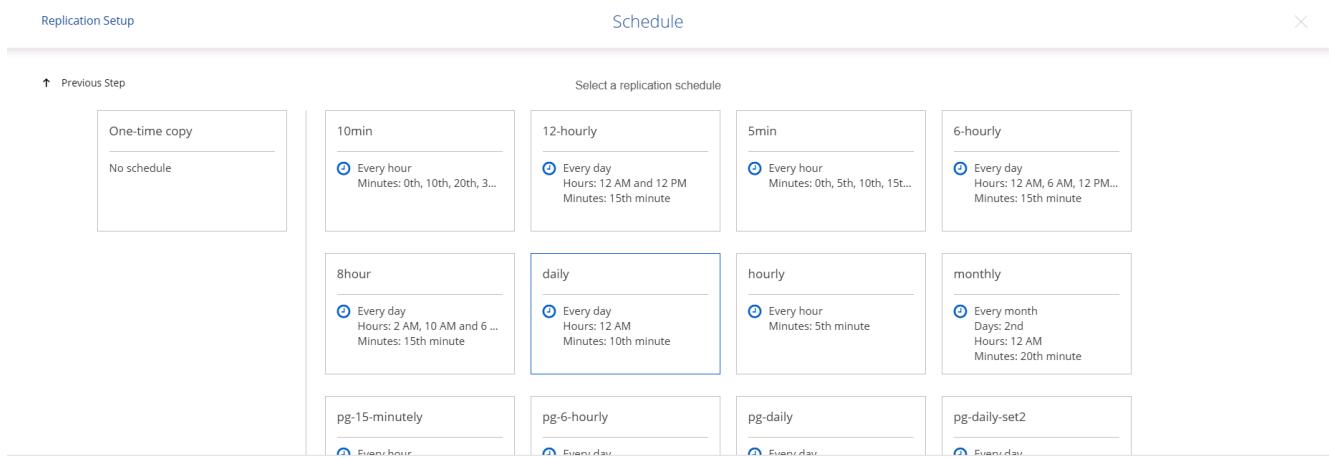
- Limited to: MB/s
- Unlimited (recommended for DR only machines)

7. Define the replication policy. We chose a Mirror, which takes the most recent dataset and replicates that into the destination volume. You could also choose a different policy based on your requirements.

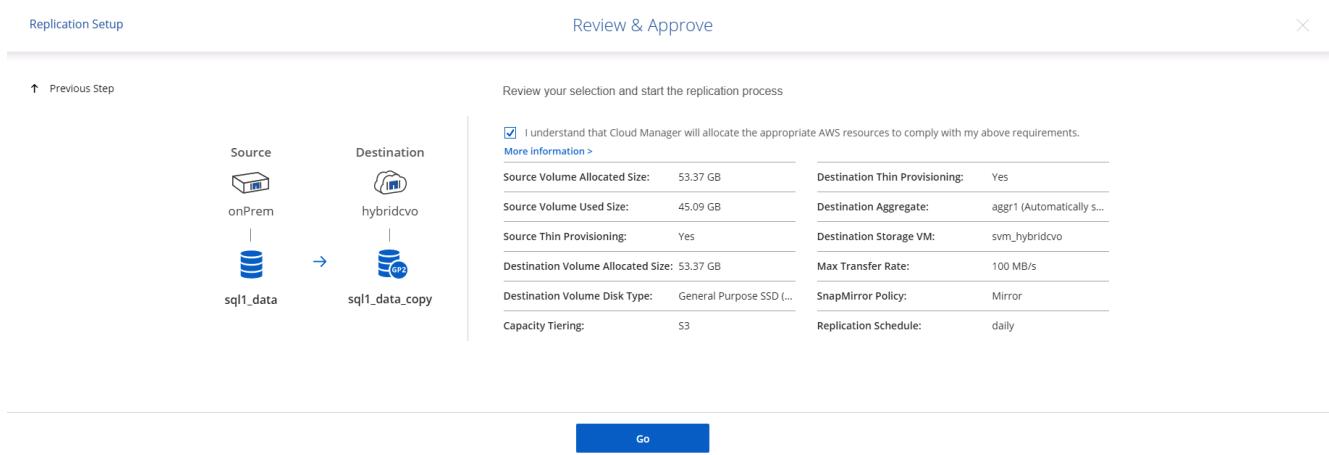
Replication Policy

Default Policies	Additional Policies
<p> Mirror</p> <p>Typically used for disaster recovery</p> <p>More info</p>	<p> Mirror and Backup (1 month retention)</p> <p>Configures disaster recovery and long-term retention of backups on the same destination volume</p> <p>More info</p>

8. Choose the schedule for triggering replication. NetApp recommends setting a "daily" schedule of for the data volume and an "hourly" schedule for the log volumes, although this can be changed based on requirements.



9. Review the information entered, click Go to trigger the cluster peer and SVM peer (if this is your first time replicating between the two clusters), and then implement and initialize the SnapMirror relationship.



10. Continue this process for data volumes and log volumes.

11. To check all of your relationships, navigate to the Replication tab inside Cloud Manager. Here you can manage your relationships and check on their status.

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
✓	rhel2_u01 onPrem	rhel2_u01_dr hybridcvo	43 minutes 43 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:50 AM 19.73 MiB
✓	rhel2_u02 onPrem	rhel2_u02_dr hybridcvo	1 hour 37 minutes 59 seconds	idle	snapmirrored	Sep 30, 2021, 2:37:08 PM 239.78 MiB
✓	rhel2_u03 onPrem	rhel2_u03_dr hybridcvo	16 hours 1 minute 9 seconds	idle	snapmirrored	Sep 30, 2021, 4:07:14 PM 225.37 KiB
✓	sql1_data onPrem	sql1_data_dr hybridcvo	1 hour 6 minutes 50 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:28 AM 24.56 KiB

12. After all the volumes have been replicated, you are in a steady state and ready to move on to the disaster recovery and dev/test workflows.

3. Deploy EC2 compute instance for database workload

AWS has preconfigured EC2 compute instances for various workloads. The choice of instance type determines the number of CPU cores, memory capacity, storage type and capacity, and network performance. For the use cases, with the exception of the OS partition, the main storage to run database workload is allocated from CVO or the FSx ONTAP storage engine. Therefore, the main factors to consider are the choice of CPU cores, memory, and network performance level. Typical AWS EC2 instance types can be found here: [EC2 Instance Type](#).

Sizing the compute instance

1. Select the right instance type based on the required workload. Factors to consider include the number of business transactions to be supported, the number of concurrent users, data set sizing, and so on.
2. EC2 instance deployment can be launched through the EC2 Dashboard. The exact deployment procedures are beyond the scope of this solution. See [Amazon EC2](#) for details.

Linux instance configuration for Oracle workload

This section contain additional configuration steps after an EC2 Linux instance is deployed.

1. Add an Oracle standby instance to the DNS server for name resolution within the SnapCenter management domain.
2. Add a Linux management user ID as the SnapCenter OS credentials with sudo permissions without a password. Enable the ID with SSH password authentication on the EC2 instance. (By default, SSH password authentication and passwordless sudo is turned off on EC2 instances.)
3. Configure Oracle installation to match with on-premises Oracle installation such as OS patches, Oracle versions and patches, and so on.
4. NetApp Ansible DB automation roles can be leveraged to configure EC2 instances for database dev/test and disaster recovery use cases. The automation code can be download from the NetApp public GitHub site: [Oracle 19c Automated Deployment](#). The goal is to install and configure a database software stack on an EC2 instance to match on-premises OS and database configurations.

Windows instance configuration for SQL Server workload

This section lists additional configuration steps after an EC2 Windows instance is initially deployed.

1. Retrieve the Windows administrator password to log in to an instance via RDP.
2. Disable the Windows firewall, join the host to Windows SnapCenter domain, and add the instance to the DNS server for name resolution.
3. Provision a SnapCenter log volume to store SQL Server log files.
4. Configure iSCSI on the Windows host to mount the volume and format the disk drive.
5. Again, many of the previous tasks can be automated with the NetApp automation solution for SQL Server. Check the NetApp automation public GitHub site for newly published roles and solutions: [NetApp Automation](#).

Next: [Workflow for dev/test bursting to cloud](#).

Copyright Information

Copyright © 2021 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.