



# **Enterprise Databases**

NetApp Solutions

NetApp  
June 07, 2022

This PDF was generated from <https://docs.netapp.com/us-en/netapp-solutionshttps://www.netapp.com/pdf.html?item=/media/25782-nva-1155.pdf> on June 07, 2022. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Table of Contents

NetApp Enterprise Database Solutions .....	1
Oracle Database .....	1
Microsoft SQL Server .....	45
Hybrid Cloud Database Solutions with SnapCenter .....	58

# NetApp Enterprise Database Solutions

## Oracle Database

### Deploying Oracle Database

#### Solution Overview

##### Automated Deployment of Oracle19c for ONTAP on NFS

Organizations are automating their environments to gain efficiencies, accelerate deployments, and reduce manual effort. Configuration management tools like Ansible are being used to streamline enterprise database operations. In this solution, we demonstrate how you can use Ansible to automate the provisioning and configuration of Oracle 19c with NetApp ONTAP. By enabling storage administrators, systems administrators, and DBAs to consistently and rapidly deploy new storage, configure database servers, and install Oracle 19c software, you achieve the following benefits:

- Eliminate design complexities and human errors, and implement a repeatable consistent deployment and best practices
- Decrease time for provisioning of storage, configuration of DB hosts, and Oracle installation
- Increase database administrators, systems and storage administrators productivity
- Enable scaling of storage and databases with ease

NetApp provides customers with validated Ansible modules and roles to accelerate deployment, configuration, and lifecycle management of your Oracle database environment. This solution provides instruction and Ansible playbook code, to help you:

- Create and configure ONTAP NFS storage for Oracle Database
- Install Oracle 19c on RedHat Enterprise Linux 7/8 or Oracle Linux 7/8
- Configure Oracle 19c on ONTAP NFS storage

For more details or to begin, please see the overview videos below.

#### AWX/Tower Deployments

- Part 1: Getting Started, Requirements, Automation Details and Initial AWX/Tower Configuration
- [https://docs.netapp.com/us-en/netapp-solutions/media/oracle\\_deployment\\_auto\\_v1.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/oracle_deployment_auto_v1.mp4) (video)
- Part 2: Variables and Running the Playbook
- [https://docs.netapp.com/us-en/netapp-solutions/media/oracle\\_deployment\\_auto\\_v2.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/oracle_deployment_auto_v2.mp4) (video)

#### CLI Deployment

- Part 1: Getting Started, Requirements, Automation Details and Ansible Control Host Setup
- [https://docs.netapp.com/us-en/netapp-solutions/media/oracle\\_deployment\\_auto\\_v4.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/oracle_deployment_auto_v4.mp4) (video)
- Part 2: Variables and Running the Playbook

► <https://docs.netapp.com/us-en/netapp-solutions/media/oracle3.mp4> (video)

## Getting started

This solution has been designed to be run in an AWX/Tower environment or by CLI on an Ansible control host.

## AWX/Tower

For AWX/Tower environments, you are guided through creating an inventory of your ONTAP cluster management and Oracle server (IPs and hostnames), creating credentials, configuring a project that pulls the Ansible code from NetApp Automation Github, and the Job Template that launches the automation.

1. Fill out the variables specific to your environment, and copy and paste them into the Extra Vars fields in your job template.
2. After the extra vars have been added to your job template, you can launch the automation.
3. The job template is run in three phases by specifying tags for `ontap_config`, `linux_config`, and `oracle_config`.

## CLI via the Ansible control host

1. To configure the Linux host so that it can be used as an Ansible control host  
[click here for RHEL 7/8 or CentOS 7/8](#), or  
[here for Ubuntu/Debian](#)
2. After the Ansible control host is configured, you can git clone the Ansible Automation repository.
3. Edit the hosts file with the IPs and/or hostnames of your ONTAP cluster management and Oracle server's management IPs.
4. Fill out the variables specific to your environment, and copy and paste them into the `vars.yml` file.
5. Each Oracle host has a variable file identified by its hostname that contains host-specific variables.
6. After all variable files have been completed, you can run the playbook in three phases by specifying tags for `ontap_config`, `linux_config`, and `oracle_config`.

## Requirements

Environment	Requirements
<b>Ansible environment</b>	AWX/Tower or Linux host to be the Ansible control host Ansible v.2.10 and higher Python 3 Python libraries - <code>netapp-lib</code> - <code>xmldict</code> - <code>jmespath</code>
<b>ONTAP</b>	ONTAP version 9.3 - 9.7 Two data aggregates NFS vlan and ifgrp created

Environment	Requirements
Oracle server(s)	RHEL 7/8
	Oracle Linux 7/8
	Network interfaces for NFS, public, and optional mgmt
	Oracle installation files on Oracle servers

## Automation Details

This automated deployment is designed with a single Ansible playbook that consists of three separate roles. The roles are for ONTAP, Linux, and Oracle configurations.

The following table describes which tasks are being automated.

Role	Tasks
ontap_config	Pre-check of the ONTAP environment
	Creation of NFS based SVM for Oracle
	Creation of export policy
	Creation of volumes for Oracle
	Creation of NFS LIFs
linux_config	Create mount points and mount NFS volumes
	Verify NFS mounts
	OS specific configuration
	Create Oracle directories
	Configure hugepages
	Disable SELinux and firewall daemon
	Enable and start chronyd service
oracle_config	increase file descriptor hard limit
	Create pam.d session file
	Oracle software installation
	Create Oracle listener
	Create Oracle databases
	Oracle environment configuration
	Save PDB state
	Enable instance archive mode
	Enable DNFS client
	Enable database auto startup and shutdown between OS reboots

## Default parameters

To simplify automation, we have preset many required Oracle deployment parameters with default values. It is generally not necessary to change the default parameters for most deployments. A more advanced user can make changes to the default parameters with caution. The default parameters are located in each role folder under defaults directory.

## Deployment instructions

Before starting, download the following Oracle installation and patch files and place them in the /tmp/archive directory with read, write, and execute access for all users on each DB server to be deployed. The automation tasks look for the named installation files in that particular directory for Oracle installation and configuration.

```
LINUX.X64_193000_db_home.zip -- 19.3 base installer  
p31281355_190000_Linux-x86-64.zip -- 19.8 RU patch  
p6880880_190000_Linux-x86-64.zip -- opatch version 12.2.0.1.23
```

## License

You should read license information as stated in the Github repository. By accessing, downloading, installing, or using the content in this repository, you agree the terms of the license laid out [here](#).

Note that there are certain restrictions around producing and/or sharing any derivative works with the content in this repository. Please make sure you read the terms of the [License](#) before using the content. If you do not agree to all of the terms, do not access, download, or use the content in this repository.

After you are ready, click [here for detailed AWX/Tower deployment procedures](#) or [here for CLI deployment](#).

## Step-by-step deployment procedure

### AWX/Tower deployment Oracle 19c Database

#### 1. Create the inventory, group, hosts, and credentials for your environment

This section describes the setup of inventory, groups, hosts, and access credentials in AWX/Ansible Tower that prepare the environment for consuming NetApp automated solutions.

1. Configure the inventory.
  - a. Navigate to Resources → Inventories → Add, and click Add Inventory.
  - b. Provide the name and organization details, and click Save.
  - c. On the Inventories page, click the inventory created.
  - d. If there are any inventory variables, paste them in the variables field.
  - e. Navigate to the Groups sub-menu and click Add.
  - f. Provide the name of the group for ONTAP, paste the group variables (if any) and click Save.
  - g. Repeat the process for another group for Oracle.
  - h. Select the ONTAP group created, go to the Hosts sub-menu and click Add New Host.
  - i. Provide the IP address of the ONTAP cluster management IP, paste the host variables (if any), and

click Save.

- j. This process must be repeated for the Oracle group and Oracle host(s) management IP/hostname.
- 2. Create credential types. For solutions involving ONTAP, you must configure the credential type to match username and password entries.
  - a. Navigate to Administration → Credential Types, and click Add.
  - b. Provide the name and description.
  - c. Paste the following content in Input Configuration:

```
fields:

- id: username
- type: string
- label: Username
- id: password
- type: string
- label: Password
- secret: true
- id: vsadmin_password
- type: string
- label: vsadmin_password
- secret: true

```

- d. Paste the following content into Injector Configuration:

```
extra_vars:

- password: '{{ password }}'
- username: '{{ username }}'
- vsadmin_password: '{{ vsadmin_password }}'

```

- 3. Configure the credentials.
  - a. Navigate to Resources → Credentials, and click Add.
  - b. Enter the name and organization details for ONTAP.
  - c. Select the custom Credential Type you created for ONTAP.
  - d. Under Type Details, enter the username, password, and vsadmin\_password.
  - e. Click Back to Credential and click Add.
  - f. Enter the name and organization details for Oracle.
  - g. Select the Machine credential type.
  - h. Under Type Details, enter the Username and Password for the Oracle hosts.
  - i. Select the correct Privilege Escalation Method, and enter the username and password.

## 2. Create a project

- 1. Go to Resources → Projects, and click Add.

- a. Enter the name and organization details.
- b. Select Git in the Source Control Credential Type field.
- c. enter [https://github.com/NetApp-Automation/na\\_oracle19c\\_deploy.git](https://github.com/NetApp-Automation/na_oracle19c_deploy.git) as the source control URL.
- d. Click Save.
- e. The project might need to sync occasionally when the source code changes.

### 3. Configure Oracle host\_vars

The variables defined in this section are applied to each individual Oracle server and database.

1. Input your environment-specific parameters in the following embedded Oracle hosts variables or host\_vars form.



The items in blue must be changed to match your environment.

#### Host VARS Config

```
<style>
div {
position: relative;
}
div button {
position: absolute;
top: 0;
right: 0;
}
button {
transition-duration: 0.4s;
background-color: white;
color: #1563a3;
border: 2px solid #1563a3;
}
button:hover {
background-color: #1563a3;
color: white;
}
#more_datastores_nfs {
display: block;
}
#more_datastores_nfs_button {
display: none;
}
</style>
<div class="listingblock"><div class="content"><div><button id="copy-
button1" onclick="CopyClassText1()">Copy</button></div><pre><code><div
class="CopyMeClass1" id="CopyMeID1">
```

```

#####
#####          Host Variables Configuration          #####
#####

# Add your Oracle Host
ansible_host: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>10.61.180.15</i></span>

# Oracle db log archive mode: true - ARCHIVELOG or false - NOARCHIVELOG
log_archive_mode: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>true</i></span>

# Number of pluggable databases per container instance identified by sid.
Pdb_name specifies the prefix for container database naming in this case
cdb2_pdb1, cdb2_pdb2, cdb2_pdb3
oracle_sid: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>cdb2</i></span>
pdb_num: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>3</i></span>
pdb_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>"{{ oracle_sid }}_pdb"</i></span>

# CDB listener port, use different listener port for additional CDB on same host
listener_port: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>1523</i></span>

# CDB is created with SGA at 75% of memory_limit, MB. Consider how many databases to be hosted on the node and how much ram to be allocated to each DB. The grand total SGA should not exceed 75% available RAM on node.
memory_limit: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>5464</i></span>

# Set "em_configuration: DBEXPRESS" to install enterprise manager express and choose a unique port from 5500 to 5599 for each sid on the host.
# Leave them black if em express is not installed.
em_configuration: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>DBEXPRESS</i></span>
```

```

em_express_port: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;" /><i>5501</i></span>

# "{{groups.oracle[0]}}" represents first Oracle DB server as defined in Oracle hosts group [oracle]. For concurrent multiple Oracle DB servers deployment, [0] will be incremented for each additional DB server. For example, "{{groups.oracle[1]}}" represents DB server 2, "{{groups.oracle[2]}}" represents DB server 3 ... As a good practice and the default, minimum three volumes is allocated to a DB server with corresponding /u01, /u02, /u03 mount points, which store oracle binary, oracle data, and oracle recovery files respectively. Additional volumes can be added by click on "More NFS volumes" but the number of volumes allocated to a DB server must match with what is defined in global vars file by volumes_nfs parameter, which dictates how many volumes are to be created for each DB server.

host_datastores_nfs:
  - {vol_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;' /><i>{{groups.oracle[0]}}_u01</i></span>", aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>aggr01_node01</i></span>, lif: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>172.21.94.200</i></span>, size: <span <div contenteditable="true"/><i>25</i></span>}
  - {vol_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;' /><i>{{groups.oracle[0]}}_u02</i></span>", aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>aggr01_node01</i></span>, lif: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>172.21.94.200</i></span>, size: <span <div contenteditable="true"/><i>25</i></span>}
  - {vol_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;' /><i>{{groups.oracle[0]}}_u03</i></span>", aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>aggr01_node01</i></span>, lif: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>172.21.94.200</i></span>, size: <span <div contenteditable="true"/><i>25</i></span>}
<a id="more_datastores_nfs" href="javascript:datastoredropdown();">More NFS volumes</a><div id="select_more_datastores_nfs"></div><a

```

```

id="more_datastores_nfs_button"
href="javascript:adddatastorevolumes();">Enter NFS volumes'
details</a><div id="extra_datastores_nfs"></div>
</div></code></pre></div></div>
<script>
function CopyClassText1() {
    var textToCopy = document.getElementById("CopyMeID1");
    var currentRange;
    if(document.getSelection().rangeCount > 0)
    {
        currentRange = document.getSelection().getRangeAt(0);
        window.getSelection().removeRange(currentRange);
    }
    else
    {
        currentRange = false;
    }
    var CopyRange = document.createRange();
    CopyRange.selectNode(textToCopy);
    window.getSelection().addRange(CopyRange);
    document.getElementById("more_datastores_nfs").style.display = "none";
    var command = document.execCommand("copy");
    if (command)
    {
        document.getElementById("copy-button1").innerHTML = "Copied!";
        setTimeout(revert_copy, 3000);
    }
    window.getSelection().removeRange(CopyRange);
    if(currentRange)
    {
        window.getSelection().addRange(currentRange);
    }
}
function revert_copy() {
    document.getElementById("copy-button1").innerHTML = "Copy";
    document.getElementById("more_datastores_nfs").style.display =
"block";
}

function datastoredropdown() {
    document.getElementById("more_datastores_nfs").style.display = "none";
    document.getElementById("more_datastores_nfs_button").style.display =
"block";
    var x=1;
    var myHTML = '';
    var buildup = '';

```

```

var wrapper = document.getElementById("select_more_datastores_nfs");
while (x < 100) {
    buildup += '<option value="' + x + '">' + x + '</option>';
    x++;
}
myHTML += '<a id="more_datastores_nfs">How many extra NFS volumes do
you wish to add?</a><select name="number_of_extra_datastores_nfs"
id="number_of_extra_datastores_nfs">' + buildup + '</select>';
wrapper.innerHTML = myHTML;
}

function adddatastorevolumes() {
    var y =
document.getElementById("number_of_extra_datastores_nfs").value;
    var j=0;
    var myHTML = '';
    var wrapper = document.getElementById("extra_datastores_nfs");
    while (j < y) {
        j++;
        myHTML += ' - {vol_name: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"><i>{{groups.oracle[0]}}_u01</i></span>,
aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"><i>aggr01_node02</i></span>, lif: <span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>172.21.94.201</i></span>,
size: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"><i>25</i></span>}<br>';
    }
    wrapper.innerHTML = myHTML;
    document.getElementById("select_more_datastores_nfs").style.display =
"none";
    document.getElementById("more_datastores_nfs_button").style.display =
"none";
}

</script>

```

- Fill in all variables in the blue fields.
- After completing variables input, click the Copy button on the form to copy all variables to be transferred to AWX or Tower.
- Navigate back to AWX or Tower and go to Resources → Hosts, and select and open the Oracle server configuration page.
- Under the Details tab, click edit and paste the copied variables from step 1 to the Variables field under the YAML tab.

- e. Click Save.
- f. Repeat this process for any additional Oracle servers in the system.

#### 4. Configure global variables

Variables defined in this section apply to all Oracle hosts, databases, and the ONTAP cluster.

1. Input your environment-specific parameters in following embedded global variables or vars form.



The items in blue must be changed to match your environment.

##### VARS

```
<style>
div {
position: relative;
}
div button {
position: absolute;
top: 0;
right: 0;
}
button {
transition-duration: 0.4s;
background-color: white;
color: #1563a3;
border: 2px solid #1563a3;
}
button:hover {
background-color: #1563a3;
color: white;
}
#more_storage_vlans {
display: block;
}
#more_storage_vlans_button {
display: none;
}
#more_nfs_volumes {
display: block;
}
#more_nfs_volumes_button {
display: none;
}
</style>
<div class="listingblock"><div class="content"><div><button id="copy-
```

```

button" onclick="CopyClassText()">Copy</button></div><pre><code><div
class="CopyMeClass" id="CopyMeID">
#####
##### Oracle 19c deployment global user configuration variables #####
#####
##### Consolidate all variables from ontap, linux and oracle #####
#####

#####
### Ontap env specific config variables ##
#####

#Inventory group name
#Default inventory group name - 'ontap'
#Change only if you are changing the group name either in inventory/hosts
file or in inventory groups in case of AWX/Tower
hosts_group: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"><i>ontap</i></span>

#CA_signed_certificates (ONLY CHANGE to 'true' IF YOU ARE USING CA SIGNED
CERTIFICATES)
ca_signed_certs: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>false</i></span>

#Names of the Nodes in the ONTAP Cluster
nodes:
- <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline;"><i>AFF-
01</i></span>
- <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline;"><i>AFF-
02</i></span>

#Storage VLANs
#Add additional rows for vlans as necessary
storage_vlans:
- {vlan_id: "<span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"><i>203</i></span>", name: "<span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>infra_NFS</i></span>", protocol: "<span <div
contenteditable="true"/><i>NFS</i></span>"}
<a id="more_storage_vlans" href="javascript:storagevlandropdown();">More

```

```

Storage VLANs</a><div id="select_more_storage_vlans"></div><a id="more_storage_vlans_button" href="javascript:addstoragevlans();">Enter Storage VLANs details</a><div id="extra_storage_vlans"></div>

#Details of the Data Aggregates that need to be created
#If Aggregate creation takes longer, subsequent tasks of creating volumes may fail.
#There should be enough disks already zeroed in the cluster, otherwise aggregate create will zero the disks and will take long time
data_aggregates:
  - {aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>aggr01_node01</i></span>}
  - {aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>aggr01_node02</i></span>}

#SVM name
svm_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>ora_svm</i></span>

# SVM Management LIF Details
svm_mgmt_details:
  - {address: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>172.21.91.100</i></span>, netmask: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>255.255.255.0</i></span>, home_port: <span <div contenteditable="true"/><i>e0M</i></span>}

# NFS storage parameters when data_protocol set to NFS. Volume named after Oracle hosts name identified by mount point as follow for oracle DB server 1. Each mount point dedicated to a particular Oracle files: u01 - Oracle binary, u02 - Oracle data, u03 - Oracle redo. Add additional volumes by click on "More NFS volumes" and also add the volumes list to corresponding host_vars as host_datastores_nfs variable. For multiple DB server deployment, additional volumes sets needs to be added for additional DB server. Input variable "{{groups.oracle[1]}}_u01", "{{groups.oracle[1]}}_u02", and "{{groups.oracle[1]}}_u03" as vol_name for second DB server. Place volumes for multiple DB servers alternatingly between controllers for balanced IO performance, e.g. DB server 1 on controller node1, DB server 2 on controller node2 etc. Make sure match lif address with controller node.
volumes_nfs:

```

```

    - {vol_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>{{groups.oracle[0]}}_u01</i></span>", aggr_name: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>aggr01_node01</i></span>, lif: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>172.21.94.200</i></span>, size: <span <div contenteditable='true'" /><i>25</i></span>}
    - {vol_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>{{groups.oracle[0]}}_u02</i></span>", aggr_name: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>aggr01_node01</i></span>, lif: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>172.21.94.200</i></span>, size: <span <div contenteditable='true'" /><i>25</i></span>}
    - {vol_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>{{groups.oracle[0]}}_u03</i></span>", aggr_name: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>aggr01_node01</i></span>, lif: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>172.21.94.200</i></span>, size: <span <div contenteditable='true'" /><i>25</i></span>}
<a id="more_nfs_volumes" href="javascript:nfsvolumesdropdown();">More NFS volumes</a><div id="select_more_nfs_volumes"></div><a id="more_nfs_volumes_button" href="javascript:addnfsvolumes();">Enter NFS volumes' details</a><div id="extra_nfs_volumes"></div>

#NFS LIFs IP address and netmask
nfs_lifs_details:
    - address: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>172.21.94.200</i></span> #for node-1
        netmask: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>255.255.255.0</i></span>
    - address: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>172.21.94.201</i></span> #for node-2
        netmask: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>255.255.255.0</i></span>

```

```

#NFS client match
client_match: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;" /><i>172.21.94.0/24</i></span>

#####
### Linux env specific config variables #####
#####

#NFS Mount points for Oracle DB volumes
mount_points:
  - <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;" /><i>/u01</i></span>
  - <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;" /><i>/u02</i></span>
  - <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;" /><i>/u03</i></span>

# Up to 75% of node memory size divided by 2mb. Consider how many
databases to be hosted on the node and how much ram to be allocated to
each DB.
# Leave it blank if hugepage is not configured on the host.
hugepages_nr: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;" /><i>1234</i></span>

# RedHat subscription username and password
redhat_sub_username: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;" /><i>xxx</i></span>
redhat_sub_password: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;" /><i>xxx</i></span>

#####
### DB env specific install and config variables #####
#####

db_domain: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;" /><i>your.domain.com</i></span>

```

```

# Set initial password for all required Oracle passwords. Change them
after installation.

initial_pwd_all: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"/><i>netapp123</i></span>

</div></code></pre></div></div>
<script>
function CopyClassText () {
    var textToCopy = document.getElementById("CopyMeID");
    var currentRange;
    if(document.getSelection().rangeCount > 0)
    {
        currentRange = document.getSelection().getRangeAt(0);
        window.getSelection().removeRange(currentRange);
    }
    else
    {
        currentRange = false;
    }
    var CopyRange = document.createRange();
    CopyRange.selectNode(textToCopy);
    window.getSelection().addRange(CopyRange);
    document.getElementById("more_storage_vlans").style.display = "none";
    document.getElementById("more_nfs_volumes").style.display = "none";
    var command = document.execCommand("copy");
    if (command)
    {
        document.getElementById("copy-button").innerHTML = "Copied!";
        setTimeout(revert_copy, 3000);
    }
    window.getSelection().removeRange(CopyRange);
    if(currentRange)
    {
        window.getSelection().addRange(currentRange);
    }
}
function revert_copy() {
    document.getElementById("copy-button").innerHTML = "Copy";
    document.getElementById("more_storage_vlans").style.display =
"block";
    document.getElementById("more_nfs_volumes").style.display = "block";
}
function storagevlandropdown() {
    document.getElementById("more_storage_vlans").style.display = "none";
    document.getElementById("more_storage_vlans_button").style.display =

```

```

"block";
    var x=1;
    var myHTML = '';
    var buildup = '';
    var wrapper = document.getElementById("select_more_storage_vlans");
    while (x < 10) {
        buildup += '<option value="' + x + '">' + x + '</option>';
        x++;
    }
    myHTML += '<a id="more_storage_vlans_info">How many extra VLANs do you
wish to add?</a><select name="number_of_extra_storage_vlans"
id="number_of_extra_storage_vlans">' + buildup + '</select>';
    wrapper.innerHTML = myHTML;
}
function addstoragevlans() {
    var y =
document.getElementById("number_of_extra_storage_vlans").value;
    var j=0;
    var myHTML = '';
    var wrapper = document.getElementById("extra_storage_vlans");
    while (j < y) {
        j++;
        myHTML += ' - {vlan_id: ""<span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"><i>203</i></span>", name: ""<span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>infra_NFS</i></span>",
protocol: ""<span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"><i>NFS</i></span>"}<br>';
    }
    wrapper.innerHTML = myHTML;
    document.getElementById("select_more_storage_vlans").style.display =
"none";
    document.getElementById("more_storage_vlans_button").style.display =
"none";
}
function nfsvolumesdropdown() {
    document.getElementById("more_nfs_volumes").style.display = "none";
    document.getElementById("more_nfs_volumes_button").style.display =
"block";
    var x=1;
    var myHTML = '';
    var buildup = '';
    var wrapper = document.getElementById("select_more_nfs_volumes");
    while (x < 100) {

```

```

        buildup += '<option value="' + x + '">' + x + '</option>';
        x++;
    }
    myHTML += '<a id="more_nfs_volumes_info">How many extra NFS volumes do
you wish to add?</a><select name="number_of_extra_nfs_volumes"
id="number_of_extra_nfs_volumes">' + buildup + '</select>';
    wrapper.innerHTML = myHTML;
}

function addnfsvolumes() {
    var y = document.getElementById("number_of_extra_nfs_volumes").value;
    var j=0;
    var myHTML = '';
    var wrapper = document.getElementById("extra_nfs_volumes");
    while (j < y) {
        j++;
        myHTML += ' - {vol_name: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"><i>rtpora04_u01</i></span>, aggr_name: <span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>aggr01_node02</i></span>,
lif: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"><i>172.21.94.201</i></span>, size: <span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>25</i></span>}<br>';
    }
    wrapper.innerHTML = myHTML;
    document.getElementById("select_more_nfs_volumes").style.display =
"none";
    document.getElementById("more_nfs_volumes_button").style.display =
"none";
}

</script>

```

1. Fill in all variables in blue fields.
2. After completing variables input, click the Copy button on the form to copy all variables to be transferred to AWX or Tower into the following job template.

## 5. Configure and launch the job template.

1. Create the job template.
  - a. Navigate to Resources → Templates → Add and click Add Job Template.
  - b. Enter the name and description
  - c. Select the Job type; Run configures the system based on a playbook, and Check performs a dry run of a playbook without actually configuring the system.

- d. Select the corresponding inventory, project, playbook, and credentials for the playbook.
  - e. Select the all\_playbook.yml as the default playbook to be executed.
  - f. Paste global variables copied from step 4 into the Template Variables field under the YAML tab.
  - g. Check the box Prompt on Launch in the Job Tags field.
  - h. Click Save.
2. Launch the job template.
- a. Navigate to Resources → Templates.
  - b. Click the desired template and then click Launch.
  - c. When prompted on launch for Job Tags, type in requirements\_config. You might need to click the Create Job Tag line below requirements\_config to enter the job tag.
-  requirements\_config ensures that you have the correct libraries to run the other roles.
- d. Click Next and then Launch to start the job.
  - e. Click View → Jobs to monitor the job output and progress.
  - f. When prompted on launch for Job Tags, type in ontap\_config. You might need to click the Create "Job Tag" line right below ontap\_config to enter the job tag.
  - g. Click Next and then Launch to start the job.
  - h. Click View → Jobs to monitor the job output and progress
  - i. After the ontap\_config role has completed, run the process again for linux\_config.
  - j. Navigate to Resources → Templates.
  - k. Select the desired template and then click Launch.
  - l. When prompted on launch for the Job Tags type in linux\_config, you might need to select the Create "job tag" line right below linux\_config to enter the job tag.
  - m. Click Next and then Launch to start the job.
  - n. Select View → Jobs to monitor the job output and progress.
  - o. After the linux\_config role has completed, run the process again for oracle\_config.
  - p. Go to Resources → Templates.
  - q. Select the desired template and then click Launch.
  - r. When prompted on launch for Job Tags, type oracle\_config. You might need to select the Create "Job Tag" line right below oracle\_config to enter the job tag.
  - s. Click Next and then Launch to start the job.
  - t. Select View → Jobs to monitor the job output and progress.

## 6. Deploy additional database on same Oracle host

The Oracle portion of the playbook creates a single Oracle container database on an Oracle server per execution. To create additional container databases on the same server, complete the following steps.

1. Revise host\_vars variables.
  - a. Go back to step 2 - Configure Oracle host\_vars.
  - b. Change the Oracle SID to a different naming string.

- c. Change the listener port to different number.
  - d. Change the EM Express port to a different number if you are installing EM Express.
  - e. Copy and paste the revised host variables to the Oracle Host Variables field in the Host Configuration Detail tab.
2. Launch the deployment job template with only the oracle\_config tag.

## Validate Oracle installation

1. Log in to Oracle server as oracle user and execute the following commands:

```
ps -ef | grep ora
```



This will list oracle processes if installation completed as expected and oracle DB started

2. Log in to the database to check the db configuration settings and the PDBs created with the following command sets.

```
sqlplus / as sysdba
```

```
[oracle@localhost ~]$ sqlplus / as sysdba
```

```
SQL*Plus: Release 19.0.0.0.0 - Production on Thu May 6 12:52:51 2021
Version 19.8.0.0.0
```

```
Copyright (c) 1982, 2019, Oracle. All rights reserved.
```

```
Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.8.0.0.0
```

```
SQL>
```

```
select name, log_mode from v$database;
```

```
SQL> select name, log_mode from v$database;
NAME LOG_MODE
-----
```

```
CDB2 ARCHIVELOG
```

```
show pdbs;
```

```
SQL> show pdbs
```

CON_ID	CON_NAME	OPEN	MODE	RESTRICTED
2	PDB\$SEED	READ ONLY	NO	
3	CDB2_PDB1	READ WRITE	NO	
4	CDB2_PDB2	READ WRITE	NO	
5	CDB2_PDB3	READ WRITE	NO	

```
col svrname form a30
col dirname form a30
select svrname, dirname, nfsversion from v$dnfs_servers;
```

```
SQL> col svrname form a30
SQL> col dirname form a30
SQL> select svrname, dirname, nfsversion from v$dnfs_servers;
```

SVRNAME DIRNAME NFSVERSION

```
-----  
172.21.126.200 /rhelora03_u02 NFSv3.0  
172.21.126.200 /rhelora03_u03 NFSv3.0  
172.21.126.200 /rhelora03_u01 NFSv3.0
```

This confirms that dNFS is working properly.

3. Connect to database via listener to check the Oracle listener configuration with the following command. Change to the appropriate listener port and database service name.

```
sqlplus system@//localhost:1523/cdb2_pdb1.cie.netapp.com
```

```
[oracle@localhost ~]$ sqlplus system@//localhost:1523/cdb2_pdb1.cie.netapp.com
```

```
SQL*Plus: Release 19.0.0.0.0 - Production on Thu May 6 13:19:57 2021
Version 19.8.0.0.0
```

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Enter password:

Last Successful login time: Wed May 05 2021 17:11:11 -04:00

Connected to:

Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.8.0.0.0

```
SQL> show user
USER is "SYSTEM"
SQL> show con_name
CON_NAME
CDB2_PDB1
```

This confirms that Oracle listener is working properly.

## Where to go for help?

If you need help with the toolkit, please join the [NetApp Solution Automation community support slack channel](#) and look for the solution-automation channel to post your questions or inquires.

### Step-by-step deployment procedure

#### CLI deployment Oracle 19c Database

This section covers the steps required to prepare and deploy Oracle19c Database with the CLI. Make sure that you have reviewed the [Getting Started and Requirements section](#) and prepared your environment accordingly.

#### Download Oracle19c repo

1. From your ansible controller, run the following command:

```
git clone https://github.com/NetApp-Automation/na_oracle19c_deploy.git
```

2. After downloading the repository, change directories to na\_oracle19c\_deploy <cd na\_oracle19c\_deploy>.

#### Edit the hosts file

Complete the following before deployment:

1. Edit your hosts file na\_oracle19c\_deploy directory.
2. Under [ontap], change the IP address to your cluster management IP.
3. Under the [oracle] group, add the oracle hosts names. The host name must be resolved to its IP address either through DNS or the hosts file, or it must be specified in the host.
4. After you have completed these steps, save any changes.

The following example depicts a host file:

```
#ONTAP Host<div>
[ontap]
<div>
<span <div contenteditable="false" style="color:#7EAF97
; font-weight:bold; font-style:italic; text-
decoration:;"/>10.61.184.183<i></i></span>
</div>
#Oracle hosts<div>
<div>
[oracle]<div>
<span <div contenteditable="false" style="color:#7EAF97
; font-weight:bold; font-style:italic; text-
decoration:;"/>rtpora01<i></i></span>
<div>
<span <div contenteditable="false" style="color:#7EAF97
; font-weight:bold; font-style:italic; text-
decoration:;"/>rtpora02<i></i></span>
</div>
```

This example executes the playbook and deploys oracle 19c on two oracle DB servers concurrently. You can also test with just one DB server. In that case, you only need to configure one host variable file.



The playbook executes the same way regardless of how many Oracle hosts and databases you deploy.

### Edit the host\_name.yml file under host\_vars

Each Oracle host has its host variable file identified by its host name that contains host-specific variables. You can specify any name for your host. Edit and copy the host\_vars from the Host VARS Config section and paste it into your desired host\_name.yml file.



The items in blue must be changed to match your environment.

### Host VARS Config

```
<style>
div {
position: relative;
}
div button {
position: absolute;
top: 0;
right: 0;
}
button {
```

```

transition-duration: 0.4s;
background-color: white;
color: #1563a3;
border: 2px solid #1563a3;
}
button:hover {
background-color: #1563a3;
color: white;
}
#more_datastores_nfs {
display: block;
}
#more_datastores_nfs_button {
display: none;
}
</style>
<div class="listingblock"><div class="content"><div><button id="copy-
button1" onclick="CopyClassText1()">Copy</button></div><pre><code><div
class="CopyMeClass1" id="CopyMeID1">
#####
#####          Host Variables Configuration          #####
#####
# Add your Oracle Host
ansible_host: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>10.61.180.15</i></span>

# Oracle db log archive mode: true - ARCHIVELOG or false - NOARCHIVELOG
log_archive_mode: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>true</i></span>

# Number of pluggable databases per container instance identified by sid.
Pdb_name specifies the prefix for container database naming in this case
cdb2_pdb1, cdb2_pdb2, cdb2_pdb3
oracle_sid: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>cdb2</i></span>
pdb_num: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>3</i></span>
pdb_name: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>"{{ oracle_sid }}_pdb"</i></span>

```

```

# CDB listener port, use different listener port for additional CDB on
same host
listener_port: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>1523</i></span>

# CDB is created with SGA at 75% of memory_limit, MB. Consider how many
databases to be hosted on the node and how much ram to be allocated to
each DB. The grand total SGA should not exceed 75% available RAM on node.
memory_limit: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>5464</i></span>

# Set "em_configuration: DBEXPRESS" to install enterprise manager express
and choose a unique port from 5500 to 5599 for each sid on the host.
# Leave them black if em express is not installed.
em_configuration: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>DBEXPRESS</i></span>
em_express_port: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>5501</i></span>

# "{{groups.oracle[0]}}" represents first Oracle DB server as defined in
Oracle hosts group [oracle]. For concurrent multiple Oracle DB servers
deployment, [0] will be incremented for each additional DB server. For
example, "{{groups.oracle[1]}}" represents DB server 2,
"{{groups.oracle[2]}}" represents DB server 3 ... As a good practice and
the default, minimum three volumes is allocated to a DB server with
corresponding /u01, /u02, /u03 mount points, which store oracle binary,
oracle data, and oracle recovery files respectively. Additional volumes
can be added by click on "More NFS volumes" but the number of volumes
allocated to a DB server must match with what is defined in global vars
file by volumes_nfs parameter, which dictates how many volumes are to be
created for each DB server.
host_datastores_nfs:
  - {vol_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>{{groups.oracle[0]}}_u01</i></span>",
    aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"><i>aggr01_node01</i></span>, lif: <span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>172.21.94.200</i></span>,
    size: <span <div contenteditable="true"/><i>25</i></span>}
  - {vol_name: ""<span <div contenteditable="true"

```

```

style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>{{groups.oracle[0]}}_u02</i></span>", aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>aggr01_node01</i></span>, lif: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>172.21.94.200</i></span>, size: <span <div contenteditable="true"/><i>25</i></span>
- {vol_name: "<span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>{{groups.oracle[0]}}_u03</i></span>", aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>aggr01_node01</i></span>, lif: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>172.21.94.200</i></span>, size: <span <div contenteditable="true"/><i>25</i></span>}
<a id="more_datastores_nfs" href="javascript:datastoredropdown();">More NFS volumes</a><div id="select_more_datastores_nfs"></div><a id="more_datastores_nfs_button" href="javascript:adddatastorevolumes();">Enter NFS volumes' details</a><div id="extra_datastores_nfs"></div>
</div></code></pre></div>
<script>
function CopyClassText1() {
    var textToCopy = document.getElementById("CopyMeID1");
    var currentRange;
    if(document.getSelection().rangeCount > 0)
    {
        currentRange = document.getSelection().getRangeAt(0);
        window.getSelection().removeRange(currentRange);
    }
    else
    {
        currentRange = false;
    }
    var CopyRange = document.createRange();
    CopyRange.selectNode(textToCopy);
    window.getSelection().addRange(CopyRange);
    document.getElementById("more_datastores_nfs").style.display = "none";
    var command = document.execCommand("copy");
    if (command)
    {
        document.getElementById("copy-button1").innerHTML = "Copied!";
        setTimeout(revert_copy, 3000);
    }
}

```

```

        window.getSelection().removeRange(CopyRange);
        if(currentRange)
        {
            window.getSelection().addRange(currentRange);
        }
    }

function revert_copy() {
    document.getElementById("copy-button1").innerHTML = "Copy";
    document.getElementById("more_datastores_nfs").style.display =
"block";
}

function datastoredropdown() {
    document.getElementById("more_datastores_nfs").style.display = "none";
    document.getElementById("more_datastores_nfs_button").style.display =
"block";
    var x=1;
    var myHTML = '';
    var buildup = '';
    var wrapper = document.getElementById("select_more_datastores_nfs");
    while (x < 100) {
        buildup += '<option value="' + x + '">' + x + '</option>';
        x++;
    }
    myHTML += '<a id="more_datastores_nfs">How many extra NFS volumes do
you wish to add?</a><select name="number_of_extra_datastores_nfs"
id="number_of_extra_datastores_nfs">' + buildup + '</select>';
    wrapper.innerHTML = myHTML;
}

function adddatastorevolumes() {
    var y =
document.getElementById("number_of_extra_datastores_nfs").value;
    var j=0;
    var myHTML = '';
    var wrapper = document.getElementById("extra_datastores_nfs");
    while (j < y) {
        j++;
        myHTML += ' - {vol_name: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"><i>{{groups.oracle[0]}}_u01</i></span>,
aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline;"><i>aggr01_node02</i></span>, lif: <span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>172.21.94.201</i></span>,
size: <span <div contenteditable="true" style="color:#004EFF; font-

```

```

        weight:bold; font-style:italic; text-
        decoration:underline;"/><i>25</i></span>}<br>';
    }
    wrapper.innerHTML = myHTML;
    document.getElementById("select_more_datastores_nfs").style.display =
    "none";
    document.getElementById("more_datastores_nfs_button").style.display =
    "none";
}

</script>

```

## Edit the vars.yml file

The `vars.yml` file consolidates all environment-specific variables (ONTAP, Linux, or Oracle) for Oracle deployment.

- Edit and copy the variables from the VARS section and paste these variables into your `vars.yml` file.

## VARS

```

<style>
div {
position: relative;
}
div button {
position: absolute;
top: 0;
right: 0;
}
button {
transition-duration: 0.4s;
background-color: white;
color: #1563a3;
border: 2px solid #1563a3;
}
button:hover {
background-color: #1563a3;
color: white;
}
#more_storage_vlans {
display: block;
}
#more_storage_vlans_button {
display: none;
}

```

```

#more_nfs_volumes {
    display: block;
}
#more_nfs_volumes_button {
    display: none;
}
</style>
<div class="listingblock"><div class="content"><div><button id="copy-
button" onclick="CopyClassText()">Copy</button></div><pre><code><div
class="CopyMeClass" id="CopyMeID">
#####
##### Oracle 19c deployment global user configuration variables #####
##### Consolidate all variables from ontap, linux and oracle #####
#####

#####
### Ontap env specific config variables ###
#####

#Inventory group name
#Default inventory group name - 'ontap'
#Change only if you are changing the group name either in inventory/hosts
file or in inventory groups in case of AWX/Tower
hosts_group: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"><i>ontap</i></span>

#CA_signed_certificates (ONLY CHANGE to 'true' IF YOU ARE USING CA SIGNED
CERTIFICATES)
ca_signed_certs: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>false</i></span>

#Names of the Nodes in the ONTAP Cluster
nodes:
    - <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline;"><i>AFF-
01</i></span>
    - <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline;"><i>AFF-
02</i></span>

#Storage VLANs
#Add additional rows for vlans as necessary
storage_vlans:

```

```

    - {vlan_id: ""<span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"/><i>203</i></span>", name: ""<span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"/><i>infra_NFS</i></span>",
protocol: ""<span <div
contenteditable="true""/><i>NFS</i></span>"}
<a id="more_storage_vlans" href="javascript:storagevlandropdown();">More
Storage VLANs</a><div id="select_more_storage_vlans"></div><a
id="more_storage_vlans_button" href="javascript:addstoragevlans();">Enter
Storage VLANs details</a><div id="extra_storage_vlans"></div>

#Details of the Data Aggregates that need to be created
#If Aggregate creation takes longer, subsequent tasks of creating volumes
may fail.
#There should be enough disks already zeroed in the cluster, otherwise
aggregate create will zero the disks and will take long time
data_aggregates:
    - {aggr_name: "<span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"/><i>aggr01_node01</i></span>"}
    - {aggr_name: "<span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"/><i>aggr01_node02</i></span>"}

#SVM name
svm_name: "<span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"/><i>ora_svm</i></span>

# SVM Management LIF Details
svm_mgmt_details:
    - {address: "<span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"/><i>172.21.91.100</i></span>, netmask: "<span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"/><i>255.255.255.0</i></span>,
home_port: "<span <div contenteditable="true""/><i>e0M</i></span>"}

# NFS storage parameters when data_protocol set to NFS. Volume named after
Oracle hosts name identified by mount point as follow for oracle DB server
1. Each mount point dedicated to a particular Oracle files: u01 - Oracle
binary, u02 - Oracle data, u03 - Oracle redo. Add additional volumes by
click on "More NFS volumes" and also add the volumes list to corresponding
host_vars as host_datastores_nfs variable. For multiple DB server

```

deployment, additional volumes sets needs to be added for additional DB server. Input variable "{{groups.oracle[1]}}\_u01", "{{groups.oracle[1]}}\_u02", and "{{groups.oracle[1]}}\_u03" as vol\_name for second DB server. Place volumes for multiple DB servers alternatingly between controllers for balanced IO performance, e.g. DB server 1 on controller node1, DB server 2 on controller node2 etc. Make sure match lif address with controller node.

volumes\_nfs:

- {vol\_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>{{groups.oracle[0]}}\_u01</i></span>", aggr\_name: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>aggr01\_node01</i></span>, lif: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>172.21.94.200</i></span>, size: <span <div contenteditable='true'><i>25</i></span>}"}
- {vol\_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>{{groups.oracle[0]}}\_u02</i></span>", aggr\_name: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>aggr01\_node01</i></span>, lif: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>172.21.94.200</i></span>, size: <span <div contenteditable='true'><i>25</i></span>}"}
- {vol\_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>{{groups.oracle[0]}}\_u03</i></span>", aggr\_name: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>aggr01\_node01</i></span>, lif: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>172.21.94.200</i></span>, size: <span <div contenteditable='true'><i>25</i></span>}"}

<a id="more\_nfs\_volumes" href="javascript:nfsvolumesdropdown();">More NFS volumes</a><div id="select\_more\_nfs\_volumes"></div><a id="more\_nfs\_volumes\_button" href="javascript:addnfsvolumes();">Enter NFS volumes' details</a><div id="extra\_nfs\_volumes"></div>

#NFS LIFs IP address and netmask

nfs\_lifs\_details:

- address: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>172.21.94.200</i></span> #for node-1
- netmask: <span <div contenteditable='true' style='color:#004EFF; font-

```

weight:bold; font-style:italic; text-
decoration:underline;"/><i>255.255.255.0</i></span>
- address: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"/><i>172.21.94.201</i></span> #for node-2
    netmask: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"/><i>255.255.255.0</i></span>

#NFS client match
client_match: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"/><i>172.21.94.0/24</i></span>

#####
### Linux env specific config variables ###
#####

#NFS Mount points for Oracle DB volumes
mount_points:
- <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"/><i>/u01</i></span>
- <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"/><i>/u02</i></span>
- <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"/><i>/u03</i></span>

# Up to 75% of node memory size divided by 2mb. Consider how many
databases to be hosted on the node and how much ram to be allocated to
each DB.
# Leave it blank if hugepage is not configured on the host.
hugepages_nr: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"/><i>1234</i></span>

# RedHat subscription username and password
redhat_sub_username: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"/><i>xxx</i></span>
redhat_sub_password: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"/><i>xxx</i></span>

```

```

#####
### DB env specific install and config variables #####
#####

db_domain: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>your.domain.com</i></span>

# Set initial password for all required Oracle passwords. Change them after installation.
initial_pwd_all: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>netapp123</i></span>

</div></code></pre></div></div>
<script>
function CopyClassText() {
    var textToCopy = document.getElementById("CopyMeID");
    var currentRange;
    if(document.getSelection().rangeCount > 0)
    {
        currentRange = document.getSelection().getRangeAt(0);
        window.getSelection().removeRange(currentRange);
    }
    else
    {
        currentRange = false;
    }
    var CopyRange = document.createRange();
    CopyRange.selectNode(textToCopy);
    window.getSelection().addRange(CopyRange);
    document.getElementById("more_storage_vlans").style.display = "none";
    document.getElementById("more_nfs_volumes").style.display = "none";
    var command = document.execCommand("copy");
    if (command)
    {
        document.getElementById("copy-button").innerHTML = "Copied!";
        setTimeout(revert_copy, 3000);
    }
    window.getSelection().removeRange(CopyRange);
    if(currentRange)
    {
        window.getSelection().addRange(currentRange);
    }
}
function revert_copy() {

```

```

        document.getElementById("copy-button").innerHTML = "Copy";
        document.getElementById("more_storage_vlans").style.display =
"block";
        document.getElementById("more_nfs_volumes").style.display = "block";
    }
    function storagevlandropdown() {
        document.getElementById("more_storage_vlans").style.display = "none";
        document.getElementById("more_storage_vlans_button").style.display =
"block";
        var x=1;
        var myHTML = '';
        var buildup = '';
        var wrapper = document.getElementById("select_more_storage_vlans");
        while (x < 10) {
            buildup += '<option value="' + x + '">' + x + '</option>';
            x++;
        }
        myHTML += '<a id="more_storage_vlans_info">How many extra VLANs do you
wish to add?</a><select name="number_of_extra_storage_vlans"
id="number_of_extra_storage_vlans">' + buildup + '</select>';
        wrapper.innerHTML = myHTML;
    }
    function addstoragevlans() {
        var y =
document.getElementById("number_of_extra_storage_vlans").value;
        var j=0;
        var myHTML = '';
        var wrapper = document.getElementById("extra_storage_vlans");
        while (j < y) {
            j++;
            myHTML += ' - {vlan_id: ""<span contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"><i>203</i></span>", name: ""<span contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>infra_NFS</i></span>", protocol:
"&quot;<span contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"><i>NFS</i></span>&quot;}<br>';
        }
        wrapper.innerHTML = myHTML;
        document.getElementById("select_more_storage_vlans").style.display =
"none";
        document.getElementById("more_storage_vlans_button").style.display =
"none";
    }
    function nfsvolumesdropdown() {

```

```

document.getElementById("more_nfs_volumes").style.display = "none";
document.getElementById("more_nfs_volumes_button").style.display =
"block";
var x=1;
var myHTML = '';
var buildup = '';
var wrapper = document.getElementById("select_more_nfs_volumes");
while (x < 100) {
    buildup += '<option value="' + x + '">' + x + '</option>';
    x++;
}
myHTML += '<a id="more_nfs_volumes_info">How many extra NFS volumes do
you wish to add?</a><select name="number_of_extra_nfs_volumes"
id="number_of_extra_nfs_volumes">' + buildup + '</select>';
wrapper.innerHTML = myHTML;
}

function addnfsvolumes() {
var y = document.getElementById("number_of_extra_nfs_volumes").value;
var j=0;
var myHTML = '';
var wrapper = document.getElementById("extra_nfs_volumes");
while (j < y) {
    j++;
    myHTML += ' - {vol_name: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"><i>rtpora04_u01</i></span>, aggr_name: <span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>aggr01_node02</i></span>,
lif: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"><i>172.21.94.201</i></span>, size: <span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>25</i></span>}<br>';
}
wrapper.innerHTML = myHTML;
document.getElementById("select_more_nfs_volumes").style.display =
"none";
document.getElementById("more_nfs_volumes_button").style.display =
"none";
}

</script>

```

## Run the playbook

After completing the required environment prerequisites and copying the variables into `vars.yml` and

`your_host.yml`, you are now ready to deploy the playbooks.



<username> must be changed to match your environment.

1. Run the ONTAP playbook by passing the correct tags and ONTAP cluster username. Fill the password for ONTAP cluster, and vsadmin when prompted.

```
ansible-playbook -i hosts all_playbook.yml -u username -k -K -t  
ontap_config -e @vars/vars.yml
```

2. Run the Linux playbook to execute Linux portion of deployment. Input for admin ssh password as well as sudo password.

```
ansible-playbook -i hosts all_playbook.yml -u username -k -K -t  
linux_config -e @vars/vars.yml
```

3. Run the Oracle playbook to execute Oracle portion of deployment. Input for admin ssh password as well as sudo password.

```
ansible-playbook -i hosts all_playbook.yml -u username -k -K -t  
oracle_config -e @vars/vars.yml
```

## Deploy Additional Database on Same Oracle Host

The Oracle portion of the playbook creates a single Oracle container database on an Oracle server per execution. To create additional container database on the same server, complete the following steps:

1. Revise the `host_vars` variables.
  - a. Go back to step 3 - Edit the `host_name.yml` file under `host_vars`.
  - b. Change the Oracle SID to a different naming string.
  - c. Change the listener port to different number.
  - d. Change the EM Express port to a different number if you have installed EM Express.
  - e. Copy and paste the revised host variables to the Oracle host variable file under `host_vars`.
2. Execute the playbook with the `oracle_config` tag as shown above in [Run the playbook](#).

## Validate Oracle installation

1. Log in to Oracle server as oracle user and execute the following commands:

```
ps -ef | grep ora
```



This will list oracle processes if installation completed as expected and oracle DB started

2. Log in to the database to check the db configuration settings and the PDBs created with the following command sets.

```
sqlplus / as sysdba
```

```
[oracle@localhost ~]$ sqlplus / as sysdba
```

```
SQL*Plus: Release 19.0.0.0.0 - Production on Thu May 6 12:52:51 2021
Version 19.8.0.0.0
```

```
Copyright (c) 1982, 2019, Oracle. All rights reserved.
```

```
Connected to:
```

```
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.8.0.0.0
```

```
SQL>
```

```
select name, log_mode from v$database;
```

```
SQL> select name, log_mode from v$database;
```

```
NAME LOG_MODE
```

```
-----
```

```
CDB2 ARCHIVELOG
```

```
show pdbs;
```

```
SQL> show pdbs
```

CON_ID	CON_NAME	OPEN	MODE	RESTRICTED
2	PDB\$SEED	READ	ONLY	NO
3	CDB2_PDB1	READ	WRITE	NO
4	CDB2_PDB2	READ	WRITE	NO
5	CDB2_PDB3	READ	WRITE	NO

```
col svrname form a30
col dirname form a30
select svrname, dirname, nfsversion from v$dnfs_servers;
```

SQL> col svrname form a30  
SQL> col dirname form a30  
SQL> select svrname, dirname, nfsversion from v\$dnfs\_servers;

SVRNAME DIRNAME NFSVERSION

```
-----  

172.21.126.200 /rhelora03_u02 NFSv3.0  

172.21.126.200 /rhelora03_u03 NFSv3.0  

172.21.126.200 /rhelora03_u01 NFSv3.0
```

This confirms that dNFS is working properly.

3. Connect to database via listener to check the Oracle listener configuration with the following command. Change to the appropriate listener port and database service name.

```
sqlplus system@//localhost:1523/cdb2_pdb1.cie.netapp.com
```

[oracle@localhost ~]\$ sqlplus system@//localhost:1523/cdb2\_pdb1.cie.netapp.com

SQL\*Plus: Release 19.0.0.0.0 - Production on Thu May 6 13:19:57 2021  
Version 19.8.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Enter password:  
Last Successful login time: Wed May 05 2021 17:11:11 -04:00

Connected to:  
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production  
Version 19.8.0.0.0

SQL> show user

```
USER is "SYSTEM"
SQL> show con_name
CON_NAME
CDB2_PDB1
```

This confirms that Oracle listener is working properly.

## Where to go for help?

If you need help with the toolkit, please join the [NetApp Solution Automation community support slack channel](#) and look for the solution-automation channel to post your questions or inquiries.

# Oracle Database Data Protection

## Solution Overview

### Automated Data Protection for Oracle Databases

Organizations are automating their environments to gain efficiencies, accelerate deployments, and reduce manual effort. Configuration management tools like Ansible are being used to streamline enterprise database operations. In this solution, we demonstrate how you can use Ansible to automate the data protection of Oracle with NetApp ONTAP. By enabling storage administrators, systems administrators, and DBAs to consistently and rapidly setup data replication to an offsite data center or to public cloud, you achieve the following benefits:

- Eliminate design complexities and human errors, and implement a repeatable consistent deployment and best practices
- Decrease time for configuration of Intercluster replication, CVO instantiation, and recovery of Oracle databases
- Increase database administrators, systems and storage administrators productivity
- Provides database recovery workflow for ease of testing a DR scenario.

NetApp provides customers with validated Ansible modules and roles to accelerate deployment, configuration, and lifecycle management of your Oracle database environment. This solution provides instruction and Ansible playbook code, to help you:

### On Prem to on prem replication

- Create intercluster lifs on source and destination
- Establish cluster and vserver peering
- Create and initialize SnapMirror of Oracle volumes
- Create a replication schedule through AWX/Tower for Oracle binaries, databases, and logs
- Restore Oracle DB on the destination, and bring database online

### On Prem to CVO in AWS

- Create AWS connector
- Create CVO instance in AWS
- Add On-Prem cluster to Cloud Manager

- Create intercluster lifs on source
- Establish cluster and vserver peering
- Create and initialize SnapMirror of Oracle volumes
- Create a replication schedule through AWX/Tower for Oracle binaries, databases, and logs
- Restore Oracle DB on the destination, and bring database online

For more details or to begin, please see the overview videos below.

## AWX/Tower Deployments

- Part 1: TBD

**video**

- Part 2: TBD

**video**

After you are ready, click [here](#) for getting started with the solution.

## Getting started

This solution has been designed to be run in an AWX/Tower environment.

## AWX/Tower

For AWX/Tower environments, you are guided through creating an inventory of your ONTAP cluster management and Oracle server (IPs and hostnames), creating credentials, configuring a project that pulls the Ansible code from NetApp Automation Github, and the Job Template that launches the automation.

1. The solution has been designed to run in a private cloud scenario (on-premise to on-premise), and hybrid cloud (on-premise to public cloud Cloud Volumes ONTAP [CVO])
2. Fill out the variables specific to your environment, and copy and paste them into the Extra Vars fields in your job template.
3. After the extra vars have been added to your job template, you can launch the automation.
4. The automation is set to be ran three phases (Setup, Replication Schedule for Oracle Binaries, Database, Logs, and Replication Schedule just for Logs), and a forth phase to recovering the database at a DR site.
5. For detailed instructions for obtaining the keys and tokens necessary for the CVO Data Protection visit [Gather Pre-requisites For CVO and Connector Deployments](#)

## Requirements

## On-Prem |

Environment	Requirements
<b>Ansible environment</b>	AWX/Tower Ansible v.2.10 and higher Python 3 Python libraries - netapp-lib - xmltodict - jmespath
<b>ONTAP</b>	ONTAP version 9.8 + Two data aggregates NFS vlan and ifgrp created
<b>Oracle server(s)</b>	RHEL 7/8 Oracle Linux 7/8 Network interfaces for NFS, public, and optional mgmt Existing Oracle environment on source, and the equivalent Linux operating system at the destination (DR Site or Public Cloud)

## CVO

Environment	Requirements
<b>Ansible environment</b>	AWX/Tower Ansible v.2.10 and higher Python 3 Python libraries - netapp-lib - xmltodict - jmespath
<b>ONTAP</b>	ONTAP version 9.8 + Two data aggregates NFS vlan and ifgrp created
<b>Oracle server(s)</b>	RHEL 7/8 Oracle Linux 7/8 Network interfaces for NFS, public, and optional mgmt Existing Oracle environment on source, and the equivalent Linux operating system at the destination (DR Site or Public Cloud) Set appropriate swap space on the Oracle EC2 instance, by default some EC2 instances are deployed with 0 swap

Environment	Requirements
Cloud Manager/AWS	AWS Access/Secret Key
	NetApp Cloud Manager Account
	NetApp Cloud Manager Refresh Token

## Automation Details

## On-Prem |

This automated deployment is designed with a single Ansible playbook that consists of three separate roles. The roles are for ONTAP, Linux, and Oracle configurations. The following table describes which tasks are being automated.

Playbook	Tasks
ontap_setup	Pre-check of the ONTAP environment
	Creation of Intercluster LIFs on source cluster (OPTIONAL)
	Creation of Intercluster LIFs on destination cluster (OPTIONAL)
	Creation of Cluster and SVM Peering
	Creation of destination SnapMirror and Initialization of designated Oracle volumes
ora_replication_cg	Enable backup mode for each database in /etc/oratab
	Snapshot taken of Oracle Binary and Database volumes
	Snapmirror Updated
	Turn off backup mode for each database in /etc/oratab
ora_replication_log	Switch current log for each database in /etc/oratab
	Snapshot taken of Oracle Log volume
	Snapmirror Updated
ora_recovery	Break SnapMirror
	Enable NFS and create junction path for Oracle volumes on the destination
	Configure DR Oracle Host
	Mount and verify Oracle volumes
	Recover and start Oracle database

## CVO

This automated deployment is designed with a single Ansible playbook that consists of three separate roles. The roles are for ONTAP, Linux, and Oracle configurations. The following table describes which tasks are being automated.

Playbook	Tasks
cvo_setup	Pre-check of the environment AWS Configure/AWS Access Key ID/Secret Key/Default Region Creation of AWS Role Creation of NetApp Cloud Manager Connector instance in AWS Creation of Cloud Volumes ONTAP (CVO) instance in AWS Add On-Prem Source ONTAP Cluster to NetApp Cloud Manager Creation of destination SnapMirror and Initialization of designated Oracle volumes
ora_replication_cg	Enable backup mode for each database in /etc/oratab Snapshot taken of Oracle Binary and Database volumes Snapmirror Updated Turn off backup mode for each database in /etc/oratab
ora_replication_log	Switch current log for each database in /etc/oratab Snapshot taken of Oracle Log volume Snapmirror Updated
ora_recovery	Break SnapMirror Enable NFS and create junction path for Oracle volumes on the destination CVO Configure DR Oracle Host Mount and verify Oracle volumes Recover and start Oracle database

## Default parameters

To simplify automation, we have preset many required Oracle parameters with default values. It is generally not necessary to change the default parameters for most deployments. A more advanced user can make changes to the default parameters with caution. The default parameters are located in each role folder under defaults directory.

## License

You should read license information as stated in the Github repository. By accessing, downloading, installing, or using the content in this repository, you agree the terms of the license laid out [here](#).

Note that there are certain restrictions around producing and/or sharing any derivative works with the content in this repository. Please make sure you read the terms of the [License](#) before using the content. If you do not agree to all of the terms, do not access, download, or use the content in this repository.

After you are ready, click [here for detailed AWX/Tower procedures](#).

# Microsoft SQL Server

## TR-4897: SQL Server on Azure NetApp Files - Real Deployment View

Niyaz Mohamed, NetApp

IT organizations face constant change. Gartner reports nearly 75% of all databases will require cloud-based storage by 2022. As a leading relational database management system (RDBMS), Microsoft SQL Server is the go-to choice for Windows platform-designed applications and organizations that rely on SQL Server for everything from enterprise resource planning (ERP) to analytics to content management. SQL Server has helped to revolutionize the way enterprises manage massive data sets and power their applications to meet the schema and query performance demands.

Most IT organizations follow a cloud-first approach. Customers in a transformation phase evaluate their current IT landscape and then migrate their database workloads to the cloud based on an assessment and discovery exercise. Some factors driving customers toward cloud migration include elasticity/burst, data center exit, data center consolidation, end-of-life scenarios, mergers, acquisitions, and so on. The reason for migration can vary based on each organization and their respective business priorities. When moving to the cloud, choosing the right cloud storage is very important in order to unleash the power of SQL Server database cloud deployment.

### Use case

Moving the SQL Server estate to Azure and integrating SQL Server with Azure's vast array of platform-as-a-service (PaaS) features such as Azure Data Factory, Azure IoT Hub, and Azure Machine Learning creates tremendous business value to support digital transformation. Adopting the cloud also enables the respective business unit to focus on productivity and delivering new features and enhancements faster (Dev/Test use case) than relying on the CAPEX model or traditional private cloud models. This document covers a real-time deployment of SQL Server Always On availability group (AOAG) on Azure NetApp Files leveraging Azure Virtual Machines.

Azure NetApp Files provides enterprise-grade storage with continuously available file shares. Continuously available shares are required by SQL Server production databases on SMB file share to make sure that the node always has access to the database storage, including during disruptive scenarios such as controller upgrades or failures. Continuously available file shares eliminate the need to replicate data between storage nodes. Azure NetApp Files uses SMB 3.0 scale-out, persistent handles, and transparent failover to support nondisruptive operations (NDOs) for planned and unplanned downtime events, including many administrative tasks.

When planning cloud migrations, you should always evaluate the best approach to use. The most common and easiest approach for application migration is rehosting (also known as lift and shift). The example scenario provided in this document uses the rehosting method. SQL Server on Azure virtual machines with Azure NetApp Files allows you to use full versions of SQL Server in the cloud without having to manage on-premises hardware. SQL Server virtual machines (VMs) also simplify licensing costs when you pay as you go and provides elasticity and bursting capabilities for development, test, and estate refresh scenarios.

### Factors to consider

#### VM performance

Selecting the right VM size is important for optimal performance of a relational database in a public cloud. Microsoft recommends that you continue using the same database performance-tuning options that are applicable to SQL Server in on-premises server environments. Use [memory-optimized](#) VM sizes for the best performance of SQL Server workloads. Collect the performance data of existing deployment to identify the RAM and CPU utilization while choosing the right instances. Most deployments choose between the D, E, or M

series.

## Notes:

- For the best performance of SQL Server workloads, use memory-optimized VM sizes.
- NetApp and Microsoft recommend that you identify the storage performance requirements before choosing the instance type with the appropriate memory-to-vCore ratio. This also helps select a lower-instance type with the right network bandwidth to overcome storage throughput limits of the VM.

## VM redundancy

To increase redundancy and high availability, SQL Server VMs should either be in the same [availability set](#) or different [availability zones](#). When creating Azure VMs, you must choose between configuring availability sets versus availability zones; an Azure VM cannot participate in both.

## High availability

For high availability, configuring SQL Server AOAG or Always On Failover Cluster Instance (FCI) is the best option. For AOAG, this involves multiple instances of SQL Server on Azure Virtual Machines in a virtual network. If high availability is required at the database level, consider configuring SQL Server availability groups.

## Storage configuration

Microsoft SQL Server can be deployed with an SMB file share as the storage option. Starting with SQL Server 2012, system databases (master, model, msdb, or tempdb), and user databases can be installed with Server Message Block (SMB) file server as a storage option. This applies to both SQL Server stand-alone and SQL Server FCI.



File share storage for SQL Server databases should support continuously available property. This provides uninterrupted access to the file-share data.

Azure NetApp Files provides high performing file storage to meet any demanding workload, and it reduces SQL Server TCO as compared to block storage solutions. With block storage, VMs have imposed limits on I/O and bandwidth for disk operations; network bandwidth limits alone are applied against Azure NetApp Files. In other words, no VM-level I/O limits are applied to Azure NetApp Files. Without these I/O limits, SQL Server running on smaller VMs connected to Azure NetApp Files can perform as well as SQL Server running on much larger VMs. Azure NetApp Files reduce SQL Server deployment costs by reducing compute and software licensing costs. For detailed cost analysis and performance benefits of using Azure NetApp Files for SQL Server deployment, see the [Benefits of using Azure NetApp Files for SQL Server deployment](#).

## Benefits

The benefits of using Azure NetApp Files for SQL Server include the following:

- Using Azure NetApp Files allows you to use smaller instances, thus reducing compute cost.
- Azure NetApp Files also reduces software licensing costs, which reduce the overall TCO.
- Volume reshaping and dynamic service level capability optimizes cost by sizing for steady-state workloads and avoiding overprovisioning.

## Notes:

- To increase redundancy and high availability, SQL Server VMs should either be in the same [availability set](#)

or in different [availability zones](#). Consider file path requirements if user-defined data files are required; in which case, select SQL FCI over SQL AOAG.

- The following UNC path is supported: `\ANFSMB-b4ca.anf.test\SQLDB` and `\ANFSMB-b4ca.anf.test\SQLDB\`.
- The loopback UNC path is not supported.
- For sizing, use historic data from your on-premises environment. For OLTP workloads, match the target IOPS with performance requirements using workloads at average and peak times along with the disk reads/sec and disk writes/sec performance counters. For data warehouse and reporting workloads, match the target throughput using workloads at average and peak times and the disk read bytes/sec and disk write bytes/sec. Average values can be used in conjunction with volume reshaping capabilities.

#### Create continuously available shares

Create continuously available shares with the Azure portal or Azure CLI. In the portal, select the Enable Continuous Availability property option. for the Azure CLI, specify the share as a continuously available share by using the `az netappfiles volume create` with the `smb-continuously-avl` option set to `$True`. To learn more about creating a new, continuous availability-enabled volume, see [Creating a Continuously Available Share](#).

#### Notes:

- Enable continuous availability for the SMB volume as shown in the following image.
- If a non-administrator domain account is used, make sure the account has the required security privilege assigned.
- Set the appropriate permissions at the share level and proper file-level permissions.
- A continuously available property cannot be enabled on existing SMB volumes. To convert an existing volume to use a continuously available share, use NetApp Snapshot technology. For more information, see [Convert existing SMB volumes to use Continuous Availability](#).

# Create a volume

X

Basics    **Protocol**    Tags    Review + create

Configure access to your volume.

## Access

Protocol type  NFS  SMB  Dual-protocol (NFSv3 and SMB)

## Configuration

Active Directory * <small>(i)</small>	<input type="text" value="10.0.0.100 - anf.test/join"/> <small>▼</small>
Share name * <small>(i)</small>	<input type="text" value="SQLDB"/>
Enable Continuous Availability <small>(i)</small>	<input checked="" type="checkbox"/>

**Review + create**

< Previous

Next : Tags >

## Performance

Azure NetApp Files supports three service levels: Standard (16MBps per terabyte), Premium (64MBps per terabyte), and Ultra (128MBps per terabyte). Provisioning the right volume size is important for optimal performance of the database workload. With Azure NetApp Files, volume performance and the throughput limit are based on a combination of the following factors:

- The service level of the capacity pool to which the volume belongs
- The quota assigned to the volume
- The quality of service (QoS) type (auto or manual) of the capacity pool

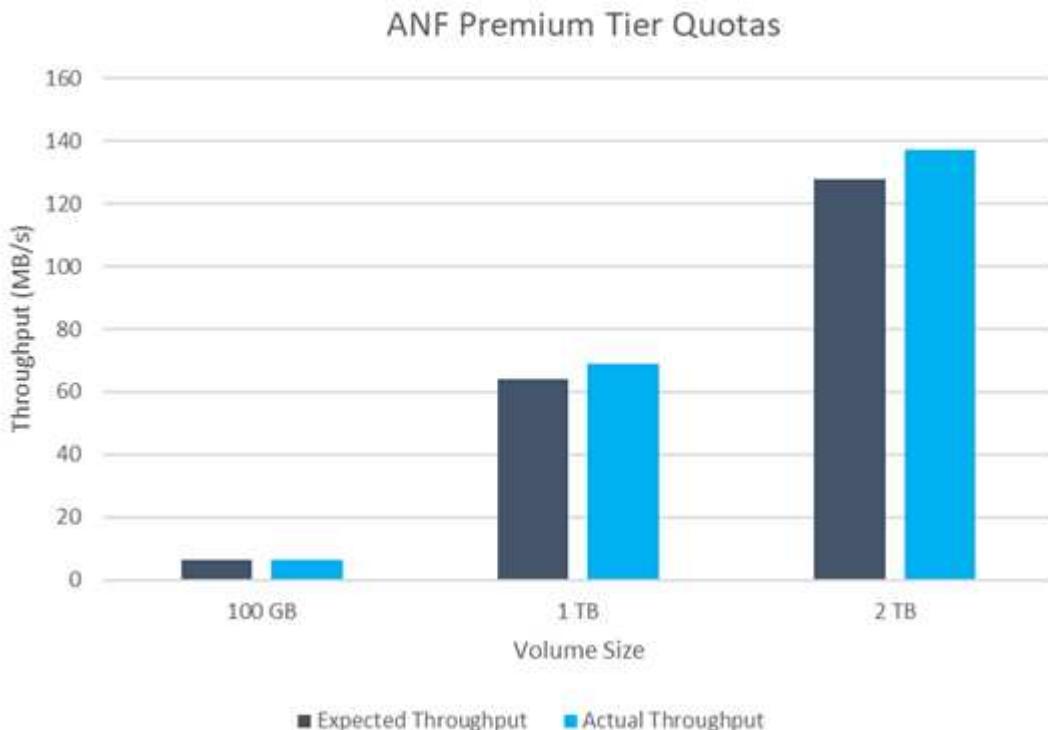
For more information, see [Service levels for Azure NetApp Files](#).

Service Level	Throughput		
Ultra	128MiB/s per 1TiB quota		
Premium	64MiB/s per 1TiB quota		
Standard	16MiB/s per 1TiB quota		
E.g. 1	Premium Tier (64MiB/s per 1TiB quota)	2TiB Volume Quota	Up to 128MiB/s gross throughput
E.g. 2	Premium Tier (64MiB/s per 1TiB quota)	100 GiB Volume Quota	Up to 6.25MiB/s gross throughput

### Performance validation

As with any deployment, testing the VM and storage is critical. For storage validation, tools such as HammerDB, Apploader, the [SQL Server storage benchmark \(SB\) tool](#), or any custom script or FIO with the appropriate read/write mix should be used. Keep in mind however that most SQL Server workloads, even busy OLTP workloads, are closer to 80%–90% read and 10%–20% write.

To showcase performance, a quick test was performed against a volume using premium service levels. In this test, the volume size was increased from 100GB to 2TB on the fly without any disruption to application access and zero data migration.



Here is another example of real time performance testing with HammerDB performed for the deployment covered in this paper. For this testing, we used a small instance with eight vCPUs, a 500GB Premium SSD, and a 500GB SMB Azure NetApp Files volume. HammerDB was configured with 80 warehouses and eight

users.

The following chart shows that Azure NetApp Files was able to deliver 2.6x the number of transactions per minute at 4x lower latency when using a comparable sized volume (500GB).

An additional test was performed by resizing to a larger instance with 32x vCPUs and a 16TB Azure NetApp Files volume. There was a significant increase in transactions per minute with consistent 1ms latency. HammerDB was configured with 80 warehouses and 64 users for this test.



### Cost optimization

Azure NetApp Files allows nondisruptive, transparent volume resizing and the ability to change the service levels with zero downtime and no effect on applications. This is a unique capability allowing dynamic cost management that avoids the need to perform database sizing with peak metrics. Rather, you can use steady state workloads, which avoids upfront costs. The volume reshaping and dynamic service-level change allows you to adjust the bandwidth and service level of Azure NetApp Files volumes on demand almost instantaneously without pausing I/O, while retaining data access.

Azure PaaS offerings such as LogicApp or Functions can be used to easily resize the volume based on a specific webhook or alert rule trigger to meet the workload demands while dynamically handling the cost.

For example, consider a database that needs 250MBps for steady state operation; however, it also requires a peak throughput of 400MBps. In this case, the deployment should be performed with a 4TB volume within the Premium service level to meet the steady-state performance requirements. To handle the peak workload, increase the volume size using Azure functions to 7TB for that specific period, and then downsize the volume to make the deployment cost effective. This configuration avoids overprovisioning of the storage.

### Real-time, high-level reference design

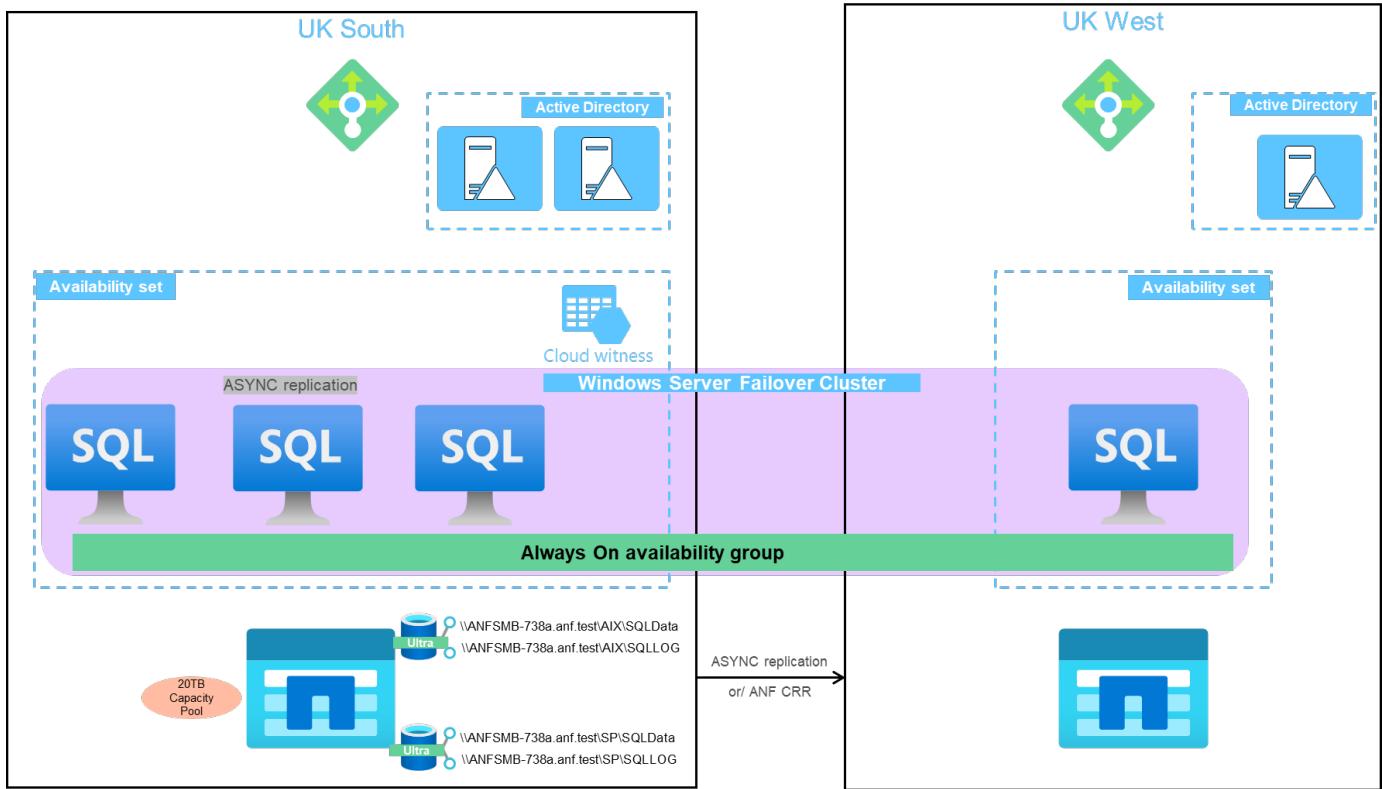
This section covers a real-time deployment of a SQL database estate in an AOAG configuration using an Azure NetApp Files SMB volume.

- Number of nodes: 4
- Number of databases: 21
- Number of availability groups: 4

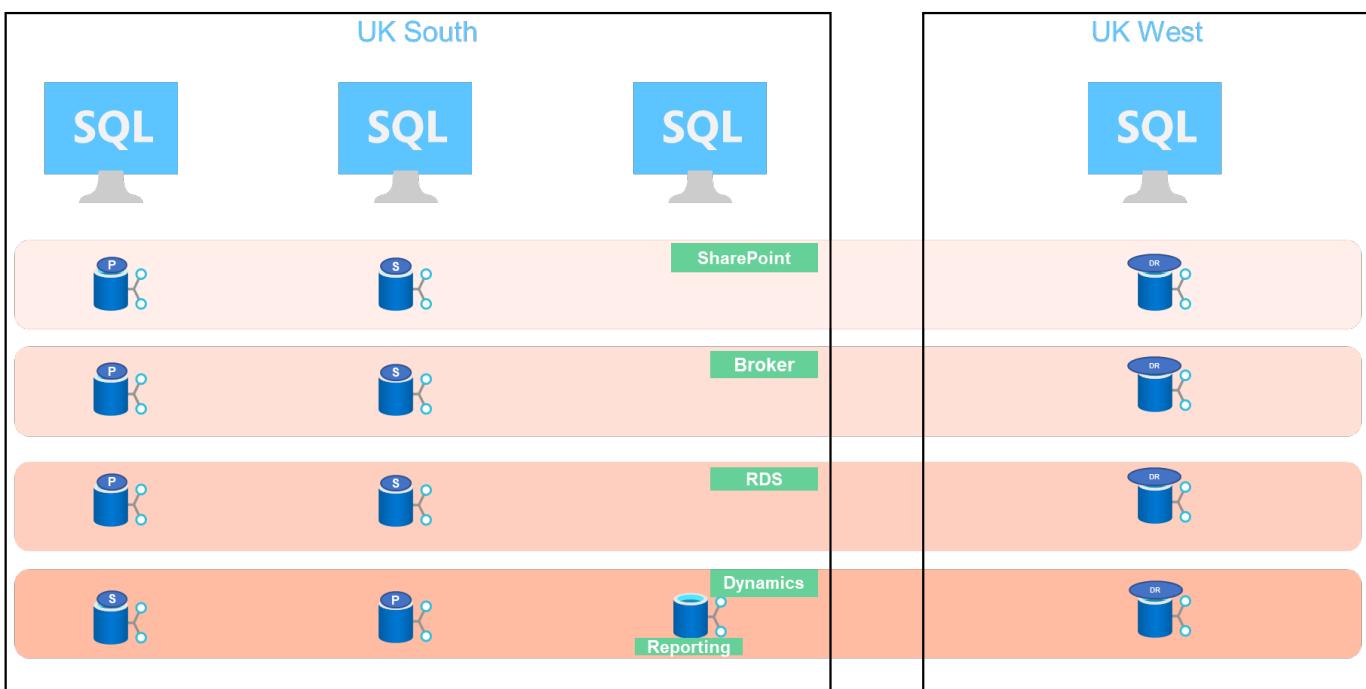
- Backup retention: 7 days
- Backup archive: 365 days



Deploying FCI with SQL Server on Azure virtual machines with an Azure NetApp Files share provides a cost-efficient model with a single copy of the data. This solution can prevent add-file operation issues if the file path differs from the secondary replica.



The following image shows the databases within AOAG spread across the nodes.



### Data layout

The user database files (.mdf) and user database transaction log files (.ldf) along with tempDB are stored on the same volume. The service level is Ultra.

The configuration consists of four nodes and four AGs. All 21 databases (part of Dynamic AX, SharePoint, RDS connection broker, and indexing services) are stored on the Azure NetApp Files volumes. The databases are balanced between the AOAG nodes to use the resources on the nodes effectively. Four D32 v3 instances are added in the WSFC, which participates in the AOAG configuration. These four nodes are provisioned in the Azure virtual network and are not migrated from on-premises.

### Notes:

- If the logs require more performance and throughput depending on the nature of the application and the queries executed, the database files can be placed on the Premium service level, and the logs can be stored at the Ultra service level.
- If the tempdb files have been placed on Azure NetApp Files, then the Azure NetApp Files volume should be separated from the user database files. Here is an example distribution of the database files in AOAG.

### Notes:

- To retain the benefits of Snapshot copy-based data protection, NetApp recommends not combining data and log data into the same volume.
- An add-file operation performed on the primary replica might fail on the secondary databases if the file path of a secondary database differs from the path of the corresponding primary database. This can happen if the share path is different on primary and secondary nodes (due to different computer accounts). This failure could cause the secondary databases to be suspended. If the growth or performance pattern cannot be predicted and the plan is to add files later, a SQL Server failover cluster with Azure NetApp Files is an acceptable solution. For most deployments, Azure NetApp Files meets the performance requirements.

## Migration

There are several ways to migrate an on-premises SQL Server user database to SQL Server in an Azure virtual machine. The migration can be either online or offline. The options chosen depend on the SQL Server version, business requirements, and the SLAs defined within the organization. To minimize downtime during the database migration process, NetApp recommends using either the AlwaysOn option or the transactional replication option. If it is not possible to use these methods, you can migrate the database manually.

The simplest and most thoroughly tested approach for moving databases across machines is backup and restore. Typically, you can start with a database backup followed by a copy of the database backup into Azure. You can then restore the database. For the best data transfer performance, migrate the database files into the Azure VM using a compressed backup file. The high-level design referenced in this document uses the backup approach to Azure file storage with Azure file sync and then restore to Azure NetApp files.



Azure Migrate can be used to discover, assess, and migrate SQL Server workloads.

To perform a migration, complete the following high-level steps:

1. Based on your requirements, set up connectivity.
2. Perform a full database backup to an on-premises file-share location.
3. Copy the backup files to an Azure file share with Azure file sync.
4. Provision the VM with the desired version of SQL Server.
5. Copy the backup files to the VM by using the `copy` command from a command prompt.
6. Restore the full databases to SQL Server on Azure virtual machines.



To restore 21 databases, it took approximately nine hours. This approach is specific to this scenario. However, other migration techniques listed below can be used based on your situation and requirements.

Other migration options to move data from an on-premises SQL Server to Azure NetApp Files include the following:

- Detach the data and log files, copy them to Azure Blob storage, and then attach them to SQL Server in the Azure VM with an ANF file share mounted from the URL.
- If you are using Always On availability group deployment on-premises, use the [Add Azure Replica Wizard](#) to create a replica in Azure and then perform failover.
- Use SQL Server [transactional replication](#) to configure the Azure SQL Server instance as a subscriber, disable replication, and point users to the Azure database instance.
- Ship the hard drive using the Windows Import/Export Service.

## Backup and recovery

Backup and recovery are an important aspect of any SQL Server deployment. It is mandatory to have the appropriate safety net to quickly recover from various data failure and loss scenarios in conjunction with high availability solutions such as AOAG. SQL Server Database Quiesce Tool, Azure Backup (streaming), or any third-party backup tool such as Commvault can be used to perform an application-consistent backup of the databases,

Azure NetApp Files Snapshot technology allows you to easily create a point-in-time (PiT) copy of the user databases without affecting performance or network utilization. This technology also allows you to restore a

Snapshot copy to a new volume or quickly revert the affected volume to the state it was in when that Snapshot copy was created by using the revert volume function. The Azure NetApp Files snapshot process is very quick and efficient, which allows for multiple daily backups, unlike the streaming backup offered by Azure backup. With multiple Snapshot copies possible in a given day, the RPO and RTO times can be significantly reduced. To add application consistency so that data is intact and properly flushed to the disk before the Snapshot copy is taken, use the SQL Server database quiesce tool ([SCSQLAPI tool](#); access to this link requires NetApp SSO login credentials). This tool can be executed from within PowerShell, which quiesces the SQL Server database and in turn can take the application-consistent storage Snapshot copy for backups.

\*Notes: \*

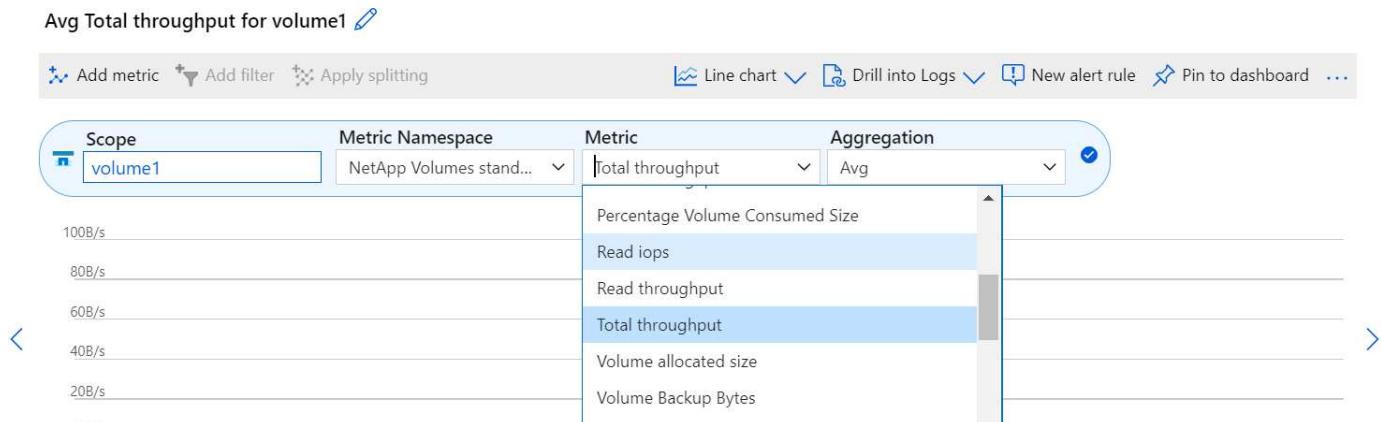
- The SCSSQLAPI tool only supports the 2016 and 2017 versions of SQL Server.
- The SCSSQLAPI tool only works with one database at a time.
- Isolate the files from each database by placing them onto a separate Azure NetApp Files volume.

Because of SCSSQL API's vast limitations, [Azure Backup](#) was used for data protection in order to meet the SLA requirements. It offers a stream-based backup of SQL Server running in Azure Virtual Machines and Azure NetApp Files. Azure Backup allows a 15-minute RPO with frequent log backups and PiT recovery up to one second.

## Monitoring

Azure NetApp Files is integrated with Azure Monitor for the time series data and provides metrics on allocated storage, actual storage usage, volume IOPS, throughput, disk read bytes/sec, disk write bytes/sec, disk reads/sec and disk writes/sec, and associated latency. This data can be used to identify bottlenecks with alerting and to perform health checks to verify that your SQL Server deployment is running in an optimal configuration.

In this HLD, ScienceLogic is used to monitor Azure NetApp Files by exposing the metrics using the appropriate service principal. The following image is an example of the Azure NetApp Files Metric option.



## Dev/Test using thick clones

With Azure NetApp Files, you can create instantaneous copies of databases to test functionality that should be implemented by using the current database structure and content during the application development cycles, to use the data extraction and manipulation tools when populating data warehouses, or to even recover data that was mistakenly deleted or changed. This process does not involve copying data from Azure Blob containers, which makes it very efficient. After the volume is restored, it can be used for read/write operations, which significantly reduces validation and time to market. This needs to be used in conjunction with SCSSQLAPI for application consistency. This approach provides yet another continuous cost optimization technique along with

Azure NetApp Files leveraging the Restore to New volume option.

#### Notes:

- The volume created from the Snapshot copy using the Restore New Volume option consumes capacity from the capacity pool.
- You can delete the cloned volumes by using REST or Azure CLI to avoid additional costs (in case the capacity pool must be increased).

#### Hybrid storage options

Although NetApp recommends using the same storage for all the nodes in SQL Server availability groups, there are scenarios in which multiple storage options can be used. This scenario is possible for Azure NetApp Files in which a node in AOAG is connected with an Azure NetApp Files SMB file share and the second node is connected with an Azure Premium disk. In these instances, make sure that the Azure NetApp Files SMB share is holding the primary copy of the user databases and the Premium disk is used as the secondary copy.

#### Notes:

- In such deployments, to avoid any failover issues, make sure that continuous availability is enabled on the SMB volume. With no continuously available attribute, the database can fail if there is any background maintenance at the storage layer.
- Keep the primary copy of the database on the Azure NetApp Files SMB file share.

#### Business continuity

Disaster recovery is generally an afterthought in any deployment. However, disaster recovery must be addressed during the initial design and deployment phase to avoid any impact to your business. With Azure NetApp Files, the cross-region replication (CRR) functionality can be used to replicate the volume data at the block level to the paired region to handle any unexpected regional outage. The CRR-enabled destination volume can be used for read operations, which makes it an ideal candidate for disaster recovery simulations. In addition, the CRR destination can be assigned with the lowest service level (for instance, Standard) to reduce the overall TCO. In the event of a failover, replication can be broken, which makes the respective volume read/write capable. Also, the service level of the volume can be changed by using the dynamic service level functionality to significantly reduce disaster recovery cost. This is another unique feature of Azure NetApp Files with block replication within Azure.

#### Long-term Snapshot copy archive

Many organizations must perform long-term retention of snapshot data from database files as a mandatory compliance requirement. Although this process is not used in this HLD, it can be easily accomplished by using a simple batch script using [AzCopy](#) to copy the snapshot directory to the Azure Blob container. The batch script can be triggered based on a specific schedule by using scheduled tasks. The process is straightforward—it includes the following steps:

1. Download the AzCopy V10 executable file. There is nothing to install because it is an exe file.
2. Authorize AzCopy by using a SAS token at the container level with the appropriate permissions.
3. After AzCopy is authorized, the data transfer begins.

#### Notes:

- In batch files, make sure to escape the % characters that appear in SAS tokens. This can be done by adding an additional % character next to existing % characters in the SAS token string.

- The **Secure Transfer Required** setting of a storage account determines whether the connection to a storage account is secured with Transport Layer Security (TLS). This setting is enabled by default. The following batch script example recursively copies data from the Snapshot copy directory to a designated Blob container:

```
SET source="Z:\~snapshot"
echo %source%
SET
dest="https://testanfacct.blob.core.windows.net/azcopts?sp=racwdl&st=2020
-10-21T18:41:35Z&se=2021-10-22T18:41:00Z&sv=2019-12
-12&sr=c&sig=ZxRUJwF1LXgHS8As7HzXJOaDXXVJ7PxxIX3ACpx56XY%%3D"
echo %dest%
```

The following example cmd is executed in PowerShell:

```
-recursive
```

```
INFO: Scanning...
INFO: Any empty folders will not be processed, because source and/or
destination doesn't have full folder support
Job b3731dd8-da61-9441-7281-17a4db09ce30 has started
Log file is located at: C:\Users\niyaz\.azcopy\b3731dd8-da61-9441-7281-
17a4db09ce30.log
0.0 %, 0 Done, 0 Failed, 2 Pending, 0 Skipped, 2 Total,
INFO: azcopy.exe: A newer version 10.10.0 is available to download
0.0 %, 0 Done, 0 Failed, 2 Pending, 0 Skipped, 2 Total,
Job b3731dd8-da61-9441-7281-17a4db09ce30 summary
Elapsed Time (Minutes): 0.0333
Number of File Transfers: 2
Number of Folder Property Transfers: 0
Total Number of Transfers: 2
Number of Transfers Completed: 2
Number of Transfers Failed: 0
Number of Transfers Skipped: 0
TotalBytesTransferred: 5
Final Job Status: Completed
```

## Notes:

- A similar backup feature for long-term retention will soon be available in Azure NetApp Files.
- The batch script can be used in any scenario that requires data to be copied to Blob container of any region.

## **Cost optimization**

With volume reshaping and dynamic service level change, which is completely transparent to the database, Azure NetApp Files allows continuous cost optimizations in Azure. This capability is used in this HLD extensively to avoid overprovisioning of additional storage to handle workload spikes.

Resizing the volume can be easily accomplished by creating an Azure function in conjunction with the Azure alert logs.

## **Conclusion**

Whether you are targeting an all-cloud or hybrid cloud with stretch databases, Azure NetApp Files provides excellent options to deploy and manage the database workloads while reducing your TCO by making data requirements seamless to the application layer.

This document covers recommendations for planning, designing, optimizing, and scaling Microsoft SQL Server deployments with Azure NetApp Files, which can vary greatly between implementations. The right solution depends on both the technical details of the implementation and the business requirements driving the project.

## **Takeaways**

The key points of this document include:

- You can now use Azure NetApp Files to host the database and file share witness for SQL Server cluster.
- You can boost the application response times and deliver 99.9999% availability to provide access to SQL Server data when and where it is needed.
- You can simplify the overall complexity of the SQL Server deployment and ongoing management, such as raid striping, with simple and instant resizing.
- You can rely on intelligent operations features to help you deploy SQL Server databases in minutes and speed development cycles.
- If Azure Cloud is the destination, Azure NetApp Files is the right storage solution for optimized deployment.

## **Where to find additional information**

To learn more about the information described in this document, refer to the following website links:

- Solution architectures using Azure NetApp Files

<https://docs.microsoft.com/en-us/azure/azure-netapp-files/azure-netapp-files-solution-architectures>

- Benefits of using Azure NetApp Files for SQL Server deployment

<https://docs.microsoft.com/en-us/azure/azure-netapp-files/solutions-benefits-azure-netapp-files-sql-server>

- SQL Server on Azure Deployment Guide Using Azure NetApp Files

<https://www.netapp.com/pdf.html?item=/media/27154-tr-4888.pdf>

- Fault tolerance, high availability, and resilience with Azure NetApp Files

<https://cloud.netapp.com/blog/azure-anf-blr-fault-tolerance-high-availability-and-resilience-with-azure-netapp-files>

# Hybrid Cloud Database Solutions with SnapCenter

## TR-4908: Hybrid Cloud Database Solutions with SnapCenter Overview

Alan Cao, Felix Melligan, NetApp

This solution provides NetApp field and customers with instructions and guidance for configuring, operating, and migrating databases to a hybrid cloud environment using the NetApp SnapCenter GUI-based tool and the NetApp storage service CVO in public clouds for the following use cases:

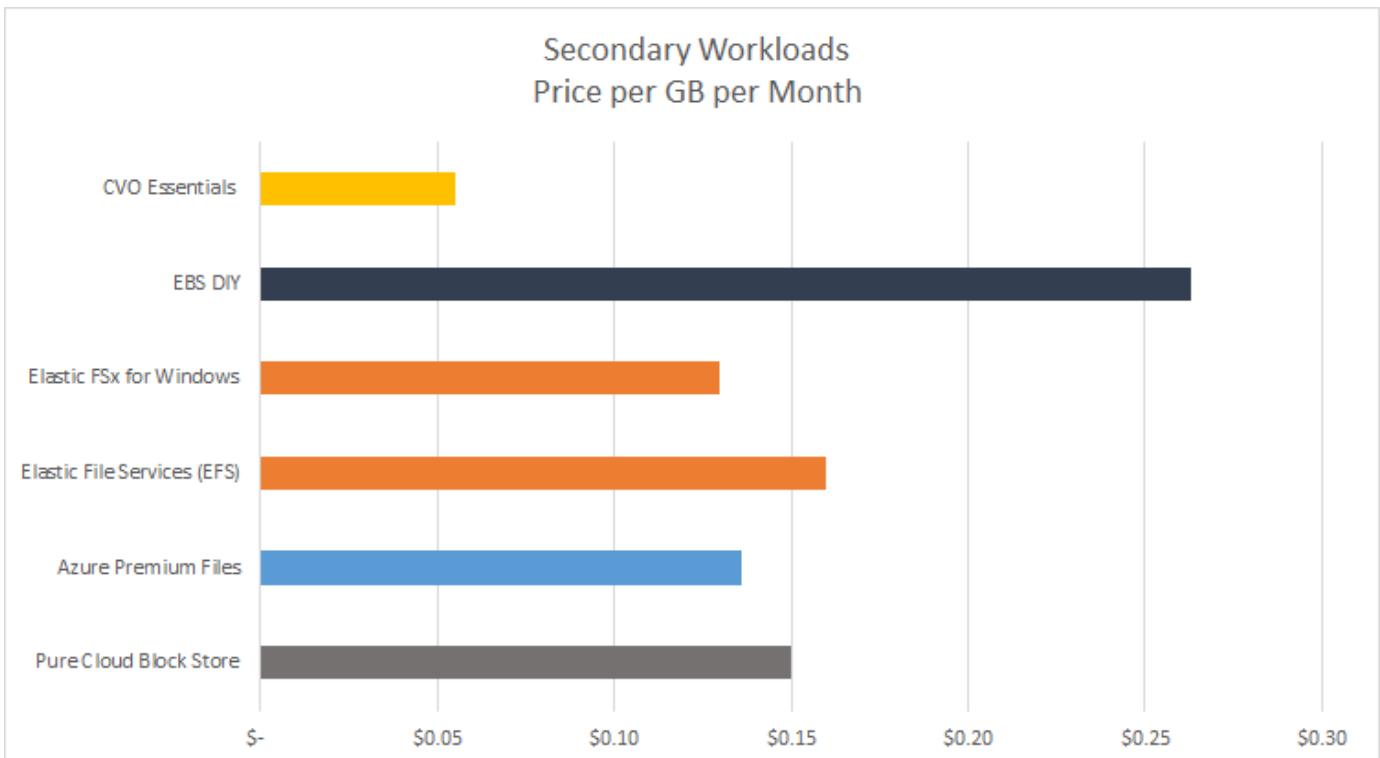
- Database dev/test operations in the hybrid cloud
- Database disaster recovery in the hybrid cloud

Today, many enterprise databases still reside in private corporate data centers for performance, security, and/or other reasons. This hybrid cloud database solution enables enterprises to operate their primary databases on site while using a public cloud for dev/test database operations as well as for disaster recovery to reduce licensing and operational costs.

Many enterprise databases, such as Oracle, SQL Server, SAP HANA, and so on, carry high licensing and operational costs. Many customers pay a one-time license fee as well as annual support costs based on the number of compute cores in their database environment, whether the cores are used for development, testing, production, or disaster recovery. Many of those environments might not be fully utilized throughout the application lifecycle.

The solutions provide an option for customers to potentially reduce their licensable cores count by moving their database environments devoted to development, testing, or disaster recovery to the cloud. By using public-cloud scale, redundancy, high availability, and a consumption-based billing model, the cost saving for licensing and operation can be substantial, while not sacrificing any application usability or availability.

Beyond potential database license-cost savings, the NetApp capacity-based CVO license model allows customers to save storage costs on a per-GB basis while empowering them with high level of database manageability that is not available from competing storage services. The following chart shows a storage cost comparison of popular storage services available in the public cloud.



This solution demonstrates that, by using the SnapCenter GUI-based software tool and NetApp SnapMirror technology, hybrid cloud database operations can be easily setup, implemented, and operated.

The following videos demonstrate SnapCenter in action:

- [Backup of an Oracle database across a Hybrid Cloud using SnapCenter](#)
- [SnapCenter- Clone DEV/TEST to AWS Cloud for an Oracle database](#)

Notably, although the illustrations throughout this document show CVO as a target storage instance in the public cloud, the solution is also fully validated for the new release of the FSx ONTAP storage engine for AWS.

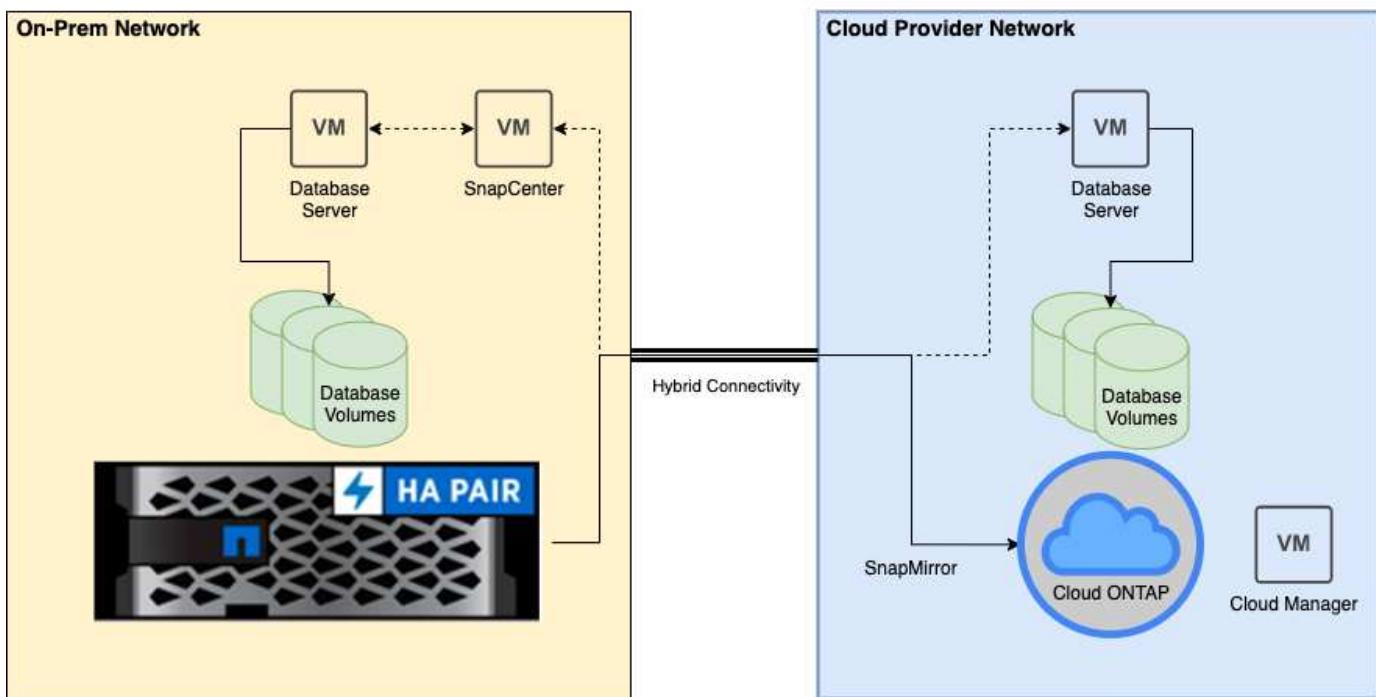
To test drive the solution and use cases for yourself, a NetApp Lab-on-Demand SL10680 can be requested at following xref:[./databases/ TL\\_AWS\\_004 HCoD: AWS - NW,SnapCenter\(OnPrem\)](#).

[Next: Solutions architecture.](#)

## Solution Architecture

[Previous: Introduction.](#)

The following architecture diagram illustrates a typical implementation of enterprise database operation in a hybrid cloud for dev/test and disaster recovery operations.



In normal business operations, synchronized database volumes in the cloud can be cloned and mounted to dev/test database instances for applications development or testing. In the event of a failure, the synchronized database volumes in the cloud can then be activated for disaster recovery.

[Next: Solutions requirements.](#)

## SnapCenter Requirements

[Previous: Solutions architecture.](#)

This solution is designed in a hybrid cloud setting to support on-premises production databases that can burst to all of the popular public clouds for dev/test and disaster recovery operations.

This solution supports all databases that are currently supported by SnapCenter, although only Oracle and SQL Server databases are demonstrated here. This solution is validated with virtualized database workloads, although bare-metal workloads are also supported.

We assume that production database servers are hosted on-premises with DB volumes presented to DB hosts from a ONTAP storage cluster. SnapCenter software is installed on-premises for database backup and data replication to the cloud. An Ansible controller is recommended but not required for database deployment automation or OS kernel and DB configuration syncing with a standby DR instance or dev/test instances in the public cloud.

## Requirements

Environment	Requirements
<b>On-premises</b>	Any databases and versions supported by SnapCenter SnapCenter v4.4 or higher Ansible v2.09 or higher ONTAP cluster 9.x Intercluster LIFs configured Connectivity from on-premises to a cloud VPC (VPN, interconnect, and so on) Networking ports open - ssh 22 - tcp 8145, 8146, 10000, 11104, 11105
<b>Cloud - AWS</b>	<a href="#">Cloud Manager Connector</a> <a href="#">Cloud Volumes ONTAP</a> Matching DB OS EC2 instances to On-prem
<b>Cloud - Azure</b>	<a href="#">Cloud Manager Connector</a> <a href="#">Cloud Volumes ONTAP</a> Matching DB OS Azure Virtual Machines to On-prem
<b>Cloud - GCP</b>	<a href="#">Cloud Manager Connector</a> <a href="#">Cloud Volumes ONTAP</a> Matching DB OS Google Compute Engine instances to on-premises

[Next: Prerequisites configuration.](#)

## Prerequisites configuration

[Previous: Solutions requirements.](#)

Certain prerequisites must be configured both on-premises and in the cloud before the execution of hybrid cloud database workloads. The following section provides a high-level summary of this process, and the following links provide further information about necessary system configuration.

### On premises

- SnapCenter installation and configuration
- On-premises database server storage configuration
- Licensing requirements
- Networking and security
- Automation

### Public cloud

- A NetApp Cloud Central login
- Network access from a web browser to several endpoints

- A network location for a connector
- Cloud provider permissions
- Networking for individual services

Important considerations:

1. Where to deploy the Cloud Manager Connector?
2. Cloud Volume ONTAP sizing and architecture
3. Single node or high availability?

The following links provide further details:

[On Premises](#)

[Public Cloud](#)

[Next: Prerequisites on-premises.](#)

### Prerequisites on-premises

[Previous: Prerequisites configuration.](#)

The following tasks must be completed on-premises to prepare the SnapCenter hybrid-cloud database workload environment.

#### SnapCenter installation and configuration

The NetApp SnapCenter tool is a Windows-based application that typically runs in a Windows domain environment, although workgroup deployment is also possible. It is based on a multitiered architecture that includes a centralized management server (the SnapCenter server) and a SnapCenter plug-in on the database server hosts for database workloads. Here are a few key considerations for hybrid-cloud deployment.

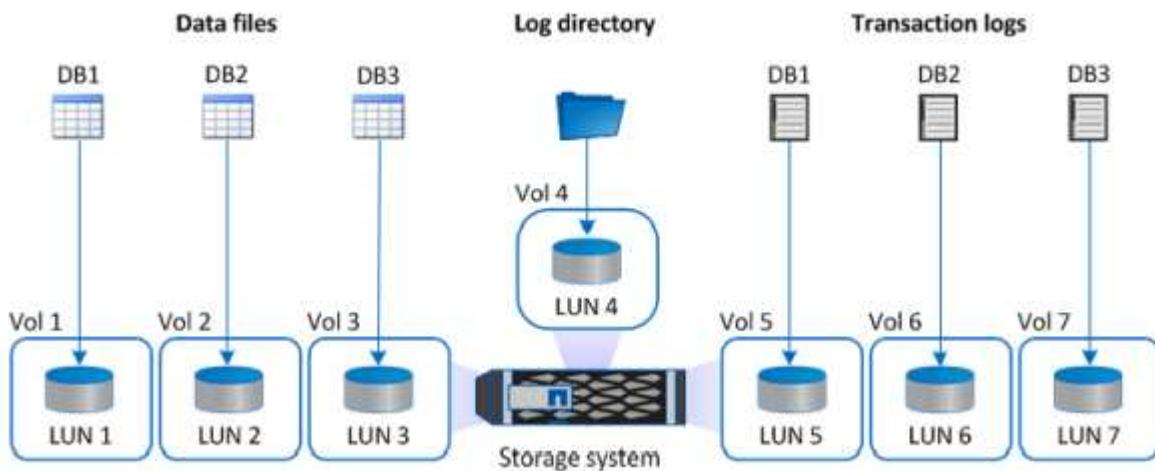
- **Single instance or HA deployment.** HA deployment provides redundancy in the case of a single SnapCenter instance server failure.
- **Name resolution.** DNS must be configured on the SnapCenter server to resolve all database hosts as well as on the storage SVM for forward and reverse lookup. DNS must also be configured on database servers to resolve the SnapCenter server and the storage SVM for both forward and reverse lookup.
- **Role-based access control (RBAC) configuration.** For mixed database workloads, you might want to use RBAC to segregate management responsibility for different DB platform such as an admin for Oracle database or an admin for SQL Server. Necessary permissions must be granted for the DB admin user.
- **Enable policy-based backup strategy.** To enforce backup consistency and reliability.
- **Open necessary network ports on the firewall.** For the on-premises SnapCenter server to communicate with agents installed in the cloud DB host.
- **Ports must be open to allow SnapMirror traffic between on-prem and public cloud.** The SnapCenter server relies on ONTAP SnapMirror to replicate onsite Snapshot backups to cloud CVO storage SVMs.

After careful pre-installation planning and consideration, click this [SnapCenter installation workflow](#) for details of SnapCenter installation and configuration.

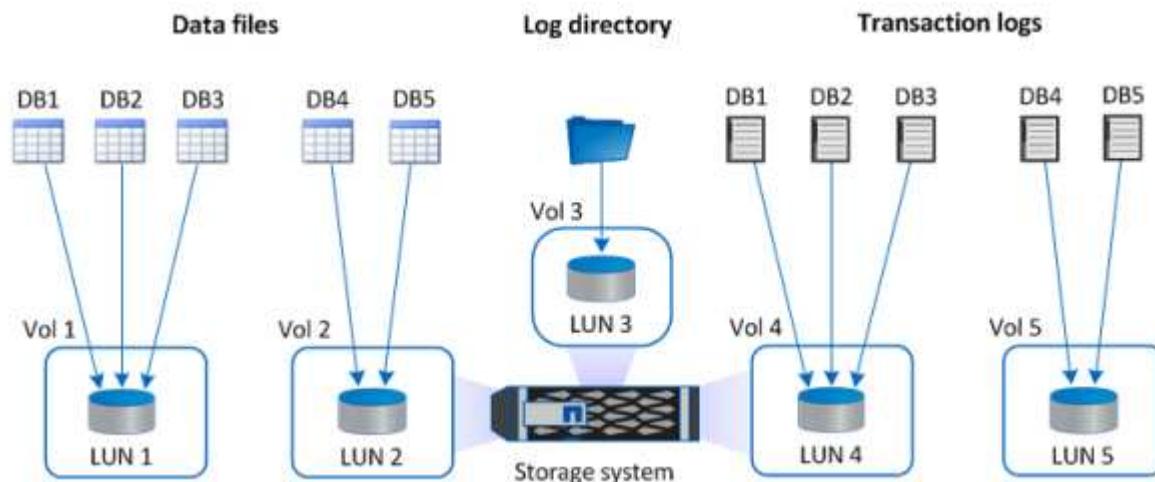
## On-premises database server storage configuration

Storage performance plays an important role in the overall performance of databases and applications. A well-designed storage layout can not only improve DB performance but also make it easy to manage database backup and recovery. Several factors should be considered when defining your storage layout, including the size of the database, the rate of expected data change for the database, and the frequency with which you perform backups.

Directly attaching storage LUNs to the guest VM by either NFS or iSCSI for virtualized database workloads generally provides better performance than storage allocated via VMDK. NetApp recommends the storage layout for a large SQL Server database on LUNs depicted in the following figure.



The following figure shows the NetApp recommended storage layout for small or medium SQL Server database on LUNs.



The Log directory is dedicated to SnapCenter to perform transaction log rollup for database recovery. For an extra large database, multiple LUNs can be allocated to a volume for better performance.

For Oracle database workloads, SnapCenter supports database environments backed by ONTAP storage that are mounted to the host as either physical or virtual devices. You can host the entire database on a single or multiple storage devices based on the criticality of the environment. Typically, customers isolate data files on dedicated storage from all other files such as control files, redo files, and archive log files. This helps administrators to quickly restore (ONTAP single-file SnapRestore) or clone a large critical database (petabyte

scale) using Snapshot technology within few seconds to minutes.



For mission critical workloads that are sensitive to latency, a dedicated storage volume should be deployed to different types of Oracle files to achieve the best latency possible. For a large database, multiple LUNs (NetApp recommends up to eight) per volume should be allocated to data files.



For smaller Oracle databases, SnapCenter supports shared storage layouts in which you can host multiple databases or part of a database on the same storage volume or LUN. As an example of this layout, you can host data files for all the databases on a +DATA ASM disk group or a volume group. The remainder of the files (redo, archive log, and control files) can be hosted on another dedicated disk group or volume group (LVM). Such a deployment scenario is illustrated below.



To facilitate the relocation of Oracle databases, the Oracle binary should be installed on a separate LUN that is included in the regular backup policy. This ensures that in the case of database relocation to a new server host, the Oracle stack can be started for recovery without any potential issues due to an out-of-sync Oracle binary.

#### Licensing requirements

SnapCenter is licensed software from NetApp. It is generally included in an on-premises ONTAP license. However, for hybrid cloud deployment, a cloud license for SnapCenter is also required to add CVO to SnapCenter as a target data replication destination. Please review following links for SnapCenter standard capacity-based license for details:

#### [SnapCenter standard capacity-based licenses](#)

#### Networking and security

In a hybrid database operation that requires an on-premises production database that is burstable to cloud for dev/test and disaster recovery, networking and security is important factor to consider when setting up the

environment and connecting to the public cloud from an on-premises data center.

Public clouds typically use a virtual private cloud (VPC) to isolate different users within a public-cloud platform. Within an individual VPC, security is controlled using measures such as security groups that are configurable based on user needs for the lockdown of a VPC.

The connectivity from the on-premises data center to the VPC can be secured through a VPN tunnel. On the VPN gateway, security can be hardened using NAT and firewall rules that block attempts to establish network connections from hosts on the internet to hosts inside the corporate data center.

For networking and security considerations, review the relevant inbound and outbound CVO rules for your public cloud of choice:

- [Security group rules for CVO - AWS](#)
- [Security group rules for CVO - Azure](#)
- [Firewall rules for CVO - GCP](#)

#### **Using Ansible automation to sync DB instances between on-premises and the cloud - optional**

To simplify management of a hybrid-cloud database environment, NetApp highly recommends but does not require that you deploy an Ansible controller to automate some management tasks, such as keeping compute instances on-premises and in the cloud in sync. This is particular important because an out-of-sync compute instance in the cloud might render the recovered database in the cloud error prone because of missing kernel packages and other issues.

The automation capability of an Ansible controller can also be used to augment SnapCenter for certain tasks, such as breaking up the SnapMirror instance to activate the DR data copy for production.

Follow these instruction to set up your Ansible control node for RedHat or CentOS machines: [RedHat/CentOS Ansible Controller Setup](#).

Follow these instruction to set up your Ansible control node for Ubuntu or Debian machines: [Ubuntu/Debian Ansible Controller Setup](#).

[Next: Public cloud.](#)

#### **Prerequisites for the public cloud**

[Previous: Prerequisites on-premises.](#)

Before we install the Cloud Manager connector and Cloud Volumes ONTAP and configure SnapMirror, we must perform some preparation for our cloud environment. This page describes the work that needs to be done as well as the considerations when deploying Cloud Volumes ONTAP.

#### **Cloud Manager and Cloud Volumes ONTAP deployment prerequisites checklist**

- A NetApp Cloud Central login
- Network access from a web browser to several endpoints
- A network location for a Connector
- Cloud provider permissions
- Networking for individual services

For more information about what you need to get started, visit our [cloud documentation](#).

## Considerations

### 1. What is a Cloud Manager connector?

In most cases, a Cloud Central account admin must deploy a connector in your cloud or on-premises network. The connector enables Cloud Manager to manage resources and processes within your public cloud environment.

For more information about Connectors, visit our [cloud documentation](#).

### 2. Cloud Volumes ONTAP sizing and architecture

When deploying Cloud Volumes ONTAP, you are given the choice of either a predefined package or the creation of your own configuration. Although many of these values can be changed later on nondisruptively, there are some key decisions that need to be made before deployment based on the workloads to be deployed in the cloud.

Each cloud provider has different options for deployment and almost every workload has its own unique properties. NetApp has a [CVO sizing tool](#) that can help size deployments correctly based on capacity and performance, but it has been built around some basic concepts which are worth considering:

- Capacity required
- Network capability of the cloud virtual machine
- Performance characteristics of cloud storage

The key is to plan for a configuration that not only satisfies the current capacity and performance requirements, but also looks at future growth. This is generally known as capacity headroom and performance headroom.

If you would like further information, read the documentation about planning correctly for [AWS](#), [Azure](#), and [GCP](#).

### 3. Single node or high availability?

In all clouds, there is the option to deploy CVO in either a single node or in a clustered high availability pair with two nodes. Depending on the use case, you might wish to deploy a single node to save costs or an HA pair to provide further availability and redundancy.

For a DR use case or spinning up temporary storage for development and testing, single nodes are common since the impact of a sudden zonal or infrastructure outage is lower. However, for any production use case, when the data is in only a single location, or when the dataset must have more redundancy and availability, high availability is recommended.

For further information about the architecture of each cloud's version of high availability, visit the documentation for [AWS](#), [Azure](#) and [GCP](#).

[Next: Getting started overview](#).

## Getting started overview

[Previous: Prerequisites for the public cloud](#).

This section provides a summary of the tasks that must be completed to meet the prerequisite requirements as outlined in previous section. The following section provide a high level tasks list for both on-premises and public cloud operations. The detailed processes and procedures can be accessed by clicking on the relevant

links.

## On-premises

- Setup database admin user in SnapCenter
- SnapCenter plugin installation prerequisites
- SnapCenter host plugin installation
- DB resource discovery
- Setup storage cluster peering and DB volume replication
- Add CVO database storage SVM to SnapCenter
- Setup database backup policy in SnapCenter
- Implement backup policy to protect database
- Validate backup

## AWS public cloud

- Pre-flight check
- Steps to deploy Cloud Manager and Cloud Volumes ONTAP in AWS
- Deploy EC2 compute instance for database workload

Click the following links for details:

[On Premises, Public Cloud - AWS](#)

## Getting started on premises

[Previous: Getting started overview.](#)

### On Premises

#### 1. Setup database admin user in SnapCenter

The NetApp SnapCenter tool uses role-based access control (RBAC) to manage user resources access and permission grants, and SnapCenter installation creates prepopulated roles. You can also create custom roles based on your needs or applications. It makes sense to have a dedicated admin user ID for each database platform supported by SnapCenter for database backup, restoration, and/or disaster recovery. You can also use a single ID to manage all databases. In our test cases and demonstration, we created a dedicated admin user for both Oracle and SQL Server, respectively.

Certain SnapCenter resources can only be provisioned with the SnapCenterAdmin role. Resources can then be assigned to other user IDs for access.

In a pre-installed and configured on-premises SnapCenter environment, the following tasks might have already have been completed. If not, the following steps create a database admin user:

1. Add the admin user to Windows Active Directory.
2. Log into SnapCenter using an ID granted with the SnapCenterAdmin role.
3. Navigate to the Access tab under Settings and Users, and click Add to add a new user. The new user ID is linked to the admin user created in Windows Active Directory in step 1. . Assign the proper role to the user

as needed. Assign resources to the admin user as applicable.

Name	Type	Roles	Domain
administrator	User	SnapCenterAdmin	demo
oradba	User	App Backup and Clone Admin	demo
sqldba	User	App Backup and Clone Admin	demo

## 2. SnapCenter plugin installation prerequisites

SnapCenter performs backup, restore, clone, and other functions by using a plugin agent running on the DB hosts. It connects to the database host and database via credentials configured under the Setting and Credentials tab for plugin installation and other management functions. There are specific privilege requirements based on the target host type, such as Linux or Windows, as well as the type of database.

DB hosts credentials must be configured before SnapCenter plugin installation. Generally, you want to use an administrator user accounts on the DB host as your host connection credentials for plugin installation. You can also grant the same user ID for database access using OS-based authentication. On the other hand, you can also employ database authentication with different database user IDs for DB management access. If you decide to use OS-based authentication, the OS admin user ID must be granted DB access. For Windows domain-based SQL Server installation, a domain admin account can be used to manage all SQL Servers within the domain.

Windows host for SQL server:

1. If you are using Windows credentials for authentication, you must set up your credential before installing plugins.
2. If you are using a SQL Server instance for authentication, you must add the credentials after installing plugins.
3. If you have enabled SQL authentication while setting up the credentials, the discovered instance or database is shown with a red lock icon. If the lock icon appears, you must specify the instance or database credentials to successfully add the instance or database to a resource group.
4. You must assign the credential to a RBAC user without sysadmin access when the following conditions are met:
  - The credential is assigned to a SQL instance.
  - The SQL instance or host is assigned to an RBAC user.
  - The RBAC DB admin user must have both the resource group and backup privileges.

Unix host for Oracle:

1. You must have enabled the password-based SSH connection for the root or non-root user by editing sshd.conf and restarting the sshd service. Password-based SSH authentication on AWS instance is turned off by default.
2. Configure the sudo privileges for the non-root user to install and start the plugin process. After installing the plugin, the processes run as an effective root user.

3. Create credentials with the Linux authentication mode for the install user.
4. You must install Java 1.8.x (64-bit) on your Linux host.
5. Installation of the Oracle database plugin also installs the SnapCenter plugin for Unix.

### 3. SnapCenter host plugin installation



Before attempting to install SnapCenter plugins on cloud DB server instances, make sure that all configuration steps have been completed as listed in the relevant cloud section for compute instance deployment.

The following steps illustrate how a database host is added to SnapCenter while a SnapCenter plugin is installed on the host. The procedure applies to adding both on-premises hosts and cloud hosts. The following demonstration adds a Windows or a Linux host residing in AWS.

#### Configure SnapCenter VMware global settings

Navigate to Settings > Global Settings. Select "VMs have iSCSI direct attached disks or NFS for all the hosts" under Hypervisor Settings and click Update.

The screenshot shows the 'Global Settings' tab selected in the top navigation bar. On the left, there's a sidebar with icons for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings (which is selected), and Alerts. The main content area is titled 'Global Settings' and contains a 'Hypervisor Settings' section. Inside this section, there's a checkbox labeled 'VMs have iSCSI direct attached disks or NFS for all the hosts' which is checked, and a blue 'Update' button next to it. Below this are sections for 'Notification Server Settings', 'Configuration Settings', 'Purge Jobs Settings', 'Domain Settings', and 'CA Certificate Settings', each with a collapse/expand arrow.

#### Add Windows host and installation of plugin on the host

1. Log into SnapCenter with a user ID with SnapCenterAdmin privileges.
2. Click the Hosts tab from the left-hand menu, and then click Add to open the Add Host workflow.
3. Choose Windows for Host Type; the Host Name can be either a host name or an IP address. The host name must be resolved to the correct host IP address from the SnapCenter host. Choose the host credentials created in step 2. Choose Microsoft Windows and Microsoft SQL Server as the plugin packages to be installed.

The screenshot shows the 'Add Host' workflow. On the left, there's a sidebar with icons for Managed Hosts, Search by Name, and a list of existing hosts: 'rhe12.demo.netapp.com' and 'soft.demo.netapp.com'. The main area has a title 'Add Host' and a form with fields: 'Host Type' set to 'Windows', 'Host Name' set to 'sql-standby', and 'Credentials' set to 'Domain Admin'. Below the form is a section titled 'Select Plug-ins to Install' for 'SnapCenter Plug-ins Package 4.5 for Windows'. It contains checkboxes for 'Microsoft Windows' (checked), 'Microsoft SQL Server' (checked), 'Microsoft Exchange Server' (unchecked), and 'SAP HANA' (unchecked). At the bottom of this section are 'More Options...', 'Port, gMSA, Install Path, Custom Plug-ins...', 'Submit', and 'Cancel' buttons.

- After the plugin is installed on a Windows host, its Overall Status is shown as "Configure log directory."

Name	Type	System	Plug-in	Version	Overall Status
rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	<span style="color: green;">Running</span>
sql1_demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	<span style="color: green;">Running</span>
sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	<span style="color: orange;">Configure log directory</span>

- Click the Host Name to open the SQL Server log directory configuration.

Host Details

Host Name: sql-standby.demo.netapp.com  
Host IP: 10.221.2.56  
Overall Status: Configure log directory  
Host Type: Windows  
System: Stand-alone  
Credentials: Domain Admin  
Plug-ins: SnapCenter Plug-ins package 4.5.0.6123 for Windows  
✓ Microsoft Windows  
✓ Microsoft SQL Server [Remove](#) [Configure log directory](#)

Alerts: No Alerts

- Click "Configure log directory" to open "Configure Plug-in for SQL Server."

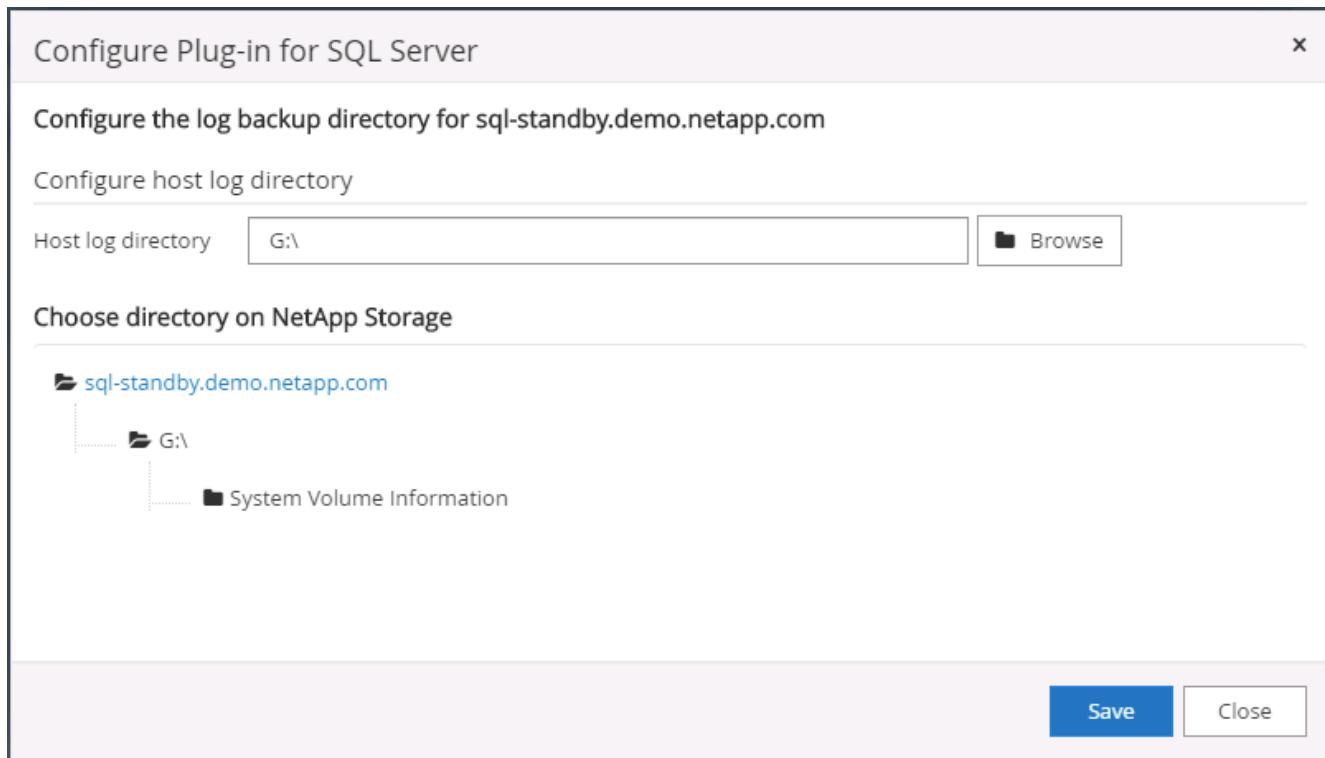
Configure Plug-in for SQL Server

Configure the log backup directory for sql-standby.demo.netapp.com

Configure host log directory

Host log directory: dedicated disk directory path

- Click Browse to discover NetApp storage so that a log directory can be set; SnapCenter uses this log directory to roll up the SQL server transaction log files. Then click Save.



For NetApp storage provisioned to a DB host to be discovered, the storage (on-prem or CVO) must be added to SnapCenter, as illustrated in step 6 for CVO as an example.

- After the log directory is configured, the Windows host plugin Overall Status is changed to Running.

Name	Type	System	Plug-in	Version	Overall Status
rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running
sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running
sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running

- To assign the host to the database management user ID, navigate to the Access tab under Settings and Users, click the database management user ID (in our case the sqldba that the host needs to be assigned to), and click Save to complete host resource assignment.

Name	Type	Roles	Domain
administrator	User	SnapCenterAdmin	demo
oradba	User	App Backup and Clone Admin	demo
sqldba	User	App Backup and Clone Admin	demo

Assign Assets

Asset Type: Host

search

<input type="checkbox"/>	Asset Name	
<input type="checkbox"/>	rhel2.demo.netapp.com	
<input type="checkbox"/>	sql1.demo.netapp.com	
<input checked="" type="checkbox"/>	sql-standby.demo.netapp.com	

**Save** **Close**

### Add Unix host and installation of plugin on the host

1. Log into SnapCenter with a user ID with SnapCenterAdmin privileges.
2. Click the Hosts tab from left-hand menu, and click Add to open the Add Host workflow.
3. Choose Linux as the Host Type. The Host Name can be either the host name or an IP address. However, the host name must be resolved to correct host IP address from SnapCenter host. Choose host credentials created in step 2. The host credentials require sudo privileges. Check Oracle Database as the plug-in to be installed, which installs both Oracle and Linux host plugins.

Add Host

Host Type: Linux

Host Name: ora-standby

Credentials: admin

Select Plug-ins to Install SnapCenter Plug-ins Package 4.5 for Linux

Oracle Database  
 SAP HANA

[More Options](#) : Port, Install Path, Custom Plug-ins...

**Submit** **Cancel**

4. Click More Options and select "Skip preinstall checks." You are prompted to confirm the skipping of the preinstall check. Click Yes and then Save.

More Options

Port	8145	<a href="#">i</a>
Installation Path	/opt/NetApp/snapcenter	<a href="#">i</a>
<input checked="" type="checkbox"/> Skip preinstall checks <input checked="" type="checkbox"/> Add all hosts in the oracle RAC		
Custom Plug-ins		
Choose a File <a href="#">Browse</a> <a href="#">Upload</a>		
No plug-ins found.		
<a href="#">Save</a> <a href="#">Cancel</a>		

5. Click Submit to start the plugin installation. You are prompted to Confirm Fingerprint as shown below.

Confirm Fingerprint

Authenticity of the host cannot be determined [i](#)

Host name	<a href="#">Edit</a>	Fingerprint	Valid
ora-standby.demo.netapp.com		ssh-rsa 3072 5C:02:EF:6B:63:54:59:10:84:DF:4D:6B:AB:FB:61:67	

[Confirm and Submit](#) [Close](#)

6. SnapCenter performs host validation and registration, and then the plugin is installed on the Linux host. The status is changed from Installing Plugin to Running.

Name	Type	System	Plug-in	Version	Overall Status
ora-standby.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running
rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running
sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running
sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running

7. Assign the newly added host to the proper database management user ID (in our case, oradba).

User Name: oradba  
Domain: demo  
Roles: App Backup and Clone Admin

Asset Name	Type	Asset Type
10.0.0.1	DataOntapCluster	Storage Connection
192.168.0.101	DataOntapCluster	Storage Connection
admin		Credentials
Linux Admin		Credentials
Oracle Archive Log Backup		Policy
Oracle Full Online Backup		Policy
rhel2.demo.netapp.com		host

Asset Type: Host

Asset Name
<input checked="" type="checkbox"/> ora-standby.demo.netapp.com
<input type="checkbox"/> rhel2.demo.netapp.com
<input type="checkbox"/> sql1.demo.netapp.com
<input type="checkbox"/> sql-standby.demo.netapp.com

Save Close

#### 4. Database resource discovery

With successful plugin installation, the database resources on the host can be immediately discovered. Click the Resources tab in the left-hand menu. Depending on the type of database platform, a number of views are available, such as the database, resources group, and so on. You might need to click the Refresh Resources tab if the resources on the host are not discovered and displayed.

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com				Not protected

When the database is initially discovered, the Overall Status is shown as "Not protected." The previous screenshot shows an Oracle database not protected yet by a backup policy.

When a backup configuration or policy is set up and a backup has been executed, the Overall Status for the database shows the backup status as "Backup succeeded" and the timestamp of the last backup. The following screenshot shows the backup status of a SQL Server user database.

Name	Instance	Host	Last Backup	Overall Status	Type
master	sql1	sql1.demo.netapp.com		Not available for backup	System database
model	sql1	sql1.demo.netapp.com		Not available for backup	System database
msdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tempdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tpcc	sql1	sql1.demo.netapp.com	09/14/2021 2:35:07 PM	Backup succeeded	User database

If database access credentials are not properly set up, a red lock button indicates that the database is not accessible. For example, if Windows credentials do not have sysadmin access to a database instance, then database credentials must be reconfigured to unlock the red lock.

Name	Host	Resource Groups	Policies	State	Type
sql-standby	sql-standby.demo.netapp.com			Running	Standalone ()
sql1	sql1.demo.netapp.com			Running	Standalone (15.0.2000)

The Microsoft SQL Server or Windows credentials are necessary to unlock the selected instance. Click Refresh Resources to run a discovery with the associated Auth.

Name	Host	Resource Groups	Policies	State	Type
sql-standby	sql-standby.demo.netapp.com	None	None	Not available for backup. DB is not on NetApp storage, auto-close is enabled or in recovery mode.	Standalone ()
sql1	sql1.demo.netapp.com				Standalone (15.0.2000)

After the appropriate credentials are configured either at the Windows level or the database level, the red lock disappears and SQL Server Type information is gathered and reviewed.

Name	Host	Resource Groups	Policies	State	Type
sql1	sql1.demo.netapp.com			Running	Standalone (15.0.2000)
sql-standby	sql-standby.demo.netapp.com			Running	Standalone (15.0.2000)

## 5. Setup storage cluster peering and DB volumes replication

To protect your on-premises database data using a public cloud as the target destination, on-premises ONTAP cluster database volumes are replicated to the cloud CVO using NetApp SnapMirror technology. The replicated target volumes can then be cloned for DEV/OPS or disaster recovery. The following high-level steps enable you to set up cluster peering and DB volumes replication.

1. Configure intercluster LIFs for cluster peering on both the on-premises cluster and the CVO cluster instance. This step can be performed with ONTAP System Manager. A default CVO deployment has inter-cluster LIFs configured automatically.

On-premises cluster:

The screenshot shows the ONTAP System Manager interface with the 'NETWORK' tab selected. In the 'IPspaces' section, there are two entries: 'Cluster' (Broadcast Domains Cluster) and 'Default' (Storage VMs, svm\_onPrem, Broadcast Domains Default). In the 'Broadcast Domains' section, there are two entries: 'Cluster' (9000 MTU, IPspace: Cluster) and 'Default' (1500 MTU, IPspace: Default, onPrem-01 e0a e0b e0c e0d e0e e0f e0g e0h e0g-100 e0e-200 e0f-201). The 'Network Interfaces' section lists three interfaces: 'onPrem-01\_IC' (Status: green, Storage VM: Default, Address: 192.168.0.113, Current Node: onPrem-01, Current Port: e0b, Type: Intercluster), 'onPrem-01\_mgmt1' (Status: green, Storage VM: Default, Address: 192.168.0.111, Current Node: onPrem-01, Current Port: e0c, Type: Cluster/Node Mgmt), and 'cluster\_mgmt' (Status: green, Storage VM: Default, Address: 192.168.0.101, Current Node: onPrem-01, Current Port: e0a, Type: Cluster/Node Mgmt).

Target CVO cluster:

The screenshot shows the ONTAP System Manager interface with the 'NETWORK' tab selected. In the 'IPspaces' section, there are two entries: 'Cluster' (Broadcast Domains Cluster) and 'Default' (Storage VMs, svm\_hybridcvo, Broadcast Domains Default). In the 'Broadcast Domains' section, there are two entries: 'Cluster' (9000 MTU, IPspace: Cluster, hybridcvo-01 e0b, hybridcvo-02 e0b) and 'Default' (9001 MTU, IPspace: Default, hybridcvo-01 e0a, hybridcvo-02 e0a). The 'Network Interfaces' section lists five interfaces: 'hybridcvo-02\_mgmt1' (Status: green, Storage VM: Default, Address: 10.221.2.104, Current Node: hybridcvo-02, Current Port: e0a, Type: Cluster/Node Mgmt), 'inter\_1' (Status: green, Storage VM: Default, Address: 10.221.1.180, Current Node: hybridcvo-01, Current Port: e0a, Type: Intercluster, Cluster/Node Mgmt), 'inter\_2' (Status: green, Storage VM: Default, Address: 10.221.2.250, Current Node: hybridcvo-02, Current Port: e0a, Type: Intercluster, Cluster/Node Mgmt), 'iscsi\_1' (Status: green, Storage VM: svm\_hybridcvo, Address: 10.221.1.5, Current Node: hybridcvo-01, Current Port: e0a, Protocols: iSCSI, Type: Data), and 'iscsi\_2' (Status: green, Storage VM: svm\_hybridcvo, Address: 10.221.2.168, Current Node: hybridcvo-02, Current Port: e0a, Protocols: iSCSI, Type: Data). The 'inter\_1' and 'inter\_2' interfaces are highlighted with a red box.

2. With the intercluster LIFs configured, cluster peering and volume replication can be set up by using drag-and-drop in NetApp Cloud Manager. See "[Getting Started - AWS Public Cloud](#)" for details.

Alternatively, cluster peering and DB volume replication can be performed by using ONTAP System Manager as follows:

3. Log into ONTAP System Manager. Navigate to Cluster > Settings and click Peer Cluster to set up cluster peering with the CVO instance in the cloud.

The screenshot shows the ONTAP System Manager interface. The left sidebar is collapsed. The main area has a search bar at the top right. The left sidebar includes sections for Overview, Applications, Volumes, LUNs, NVMe Namespaces, Shares, Qtrees, Quotas, Storage VMs, Tiers, NETWORK, EVENTS & JOBS, PROTECTION, HOSTS, and CLUSTER. The CLUSTER section is expanded, showing Overview and Settings. The Settings link is highlighted with a blue background.

**UI Settings**

- LOG LEVEL: DEBUG
- INACTIVITY TIMEOUT: 30 minutes

**Intercluster Settings**

**Network Interfaces**

- IP ADDRESS: 192.168.0.113

**Cluster Peers**

- PEERED CLUSTER NAME: hybridcvo
- Peer Cluster (button highlighted with a red box)
- Generate Passphrase
- Manage Cluster Peers

**Storage VM Peers**

- PEERED STORAGE VMs: 1

4. Go to the Volumes tab. Select the database volume to be replicated and click Protect.

The screenshot shows the ONTAP System Manager interface with the VOLUMES tab selected in the left sidebar. The left sidebar is expanded, showing DASHBOARD, STORAGE, NETWORK, EVENTS & JOBS, and PROTECTION sections. The VOLUMES section is highlighted with a blue background.

**Volumes**

	Name
<input type="checkbox"/>	onPrem_data
<input type="checkbox"/>	rhel2_u01
<input type="checkbox"/>	rhel2_u02
<input checked="" type="checkbox"/>	rhel2_u03
<input type="checkbox"/>	rhel2_u030923211942120311
<input type="checkbox"/>	8
<input type="checkbox"/>	sql1_data
<input type="checkbox"/>	sql1_log
<input type="checkbox"/>	sql1_snapctr
<input type="checkbox"/>	svm_onPrem_root

**Protect** (button highlighted with a red box)

**rhel2\_u03 All Volumes**

**Overview** (selected tab)

**Snapshot Copies**

**Clone Hierarchy**

**SnapMirror (Local or Remote)**

**Capacity**

STATUS: Online

MOUNT PATH: /rhel2\_u03

STORAGE VM: svm\_onPrem

LOCAL TIER: onPrem\_01\_SSD\_1

SNAPSHOT POLICY: default

QUOTA: Off

TYPE: Read Write

SPACE RESERVATION

**Performance**

Hour (selected)

Day

Week

**Latency**

1.5

1

5. Set the protection policy to Asynchronous. Select the destination cluster and storage SVM.

The screenshot shows the 'Protect Volumes' dialog in the ONTAP System Manager. The 'PROTECTION POLICY' dropdown is set to 'Asynchronous'. Under 'Source', 'CLUSTER' is 'onPrem' and 'SELECTED VOLUMES' is 'rhel2\_u03'. Under 'Destination', 'CLUSTER' is 'hybridcvo' and 'STORAGE VM' is 'svm\_hybridcvo'. In the 'Destination Settings' section, there are two matching labels. The 'VOLUME NAME' field has a prefix 'vol\_' and a suffix '\_dest'. Under 'Configuration Details', the 'Initialize relationship' checkbox is checked, while 'Enable FabricPool' is unchecked.

- Validate that the volume is synced between the source and target and that the replication relationship is healthy.

Source	Destination	Protection Policy	Relationship Health	Relationship Status	Lag
svm_onPrem:rhel2_u03	svm_hybridcvo:rhel2_u03_dr	MirrorAllSnapshots	<span style="color: green;">Healthy</span>	<span style="color: green;">Mirrored</span>	12 seconds

## 6. Add CVO database storage SVM to SnapCenter

- Log into SnapCenter with a user ID with SnapCenterAdmin privileges.
- Click the Storage System tab from the menu, and then click New to add a CVO storage SVM that hosts replicated target database volumes to SnapCenter. Enter the cluster management IP in the Storage System field, and enter the appropriate username and password.

- Click More Options to open additional storage configuration options. In the Platform field, select Cloud Volumes ONTAP, check Secondary, and then click Save.

Platform	Cloud Volumes ON <sup>TM</sup>	<input checked="" type="checkbox"/> Secondary
Protocol	HTTPS	
Port	443	
Timeout	60	seconds
<input type="checkbox"/> Preferred IP		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

- Assign the storage systems to SnapCenter database management user IDs as shown in [3. SnapCenter host plugin installation](#).

Name	IP	Cluster Name	User Name	Platform	Controller License
svm_hybridcvo	10.0.0.1			CVO	<span style="color:red;">*</span>
svm_onPrem	192.168.0.101			CVO	<span style="color:green;">✓</span>

## 7. Setup database backup policy in SnapCenter

The following procedures demonstrates how to create a full database or log file backup policy. The policy can then be implemented to protect databases resources. The recovery point objective (RPO) or recovery time objective (RTO) dictates the frequency of database and/or log backups.

## Create a full database backup policy for Oracle

1. Log into SnapCenter as a database management user ID, click Settings, and then click Policies.

The screenshot shows the NetApp SnapCenter interface. The left sidebar has links for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings (which is selected), and Alerts. The main area is titled 'Policies' and shows 'Oracle Database'. A search bar says 'Search by Name'. Below is a table with columns: Name, Backup Type, Schedule Type, Replication, and Verification. Two policies are listed:

Name	Backup Type	Schedule Type	Replication	Verification
Oracle Archive Log Backup	LOG, ONLINE	Hourly	SnapMirror	
Oracle Full Online Backup	FULL, ONLINE	Daily	SnapMirror	

At the top right are buttons for New (+), Modify, Copy, Details, and Delete.

2. Click New to launch a new backup policy creation workflow or choose an existing policy for modification.

The dialog box is titled 'Modify Oracle Database Backup Policy' with a close button 'x' in the top right. On the left is a vertical navigation bar with steps 1 through 7: 1. Name, 2. Backup Type, 3. Retention, 4. Replication, 5. Script, 6. Verification, 7. Summary. Step 1 is highlighted in blue. The main area is titled 'Provide a policy name'. It contains two fields: 'Policy name' with the value 'Oracle Full Online Backup' and 'Details' with the value 'Backup all data and log files'. In the bottom right corner are 'Previous' and 'Next' buttons.

3. Select the backup type and schedule frequency.

Modify Oracle Database Backup Policy

**1 Name**

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Select Oracle database backup options

Choose backup type

Online backup

Datafiles, control files, and archive logs

Datafiles and control files

Archive logs

Offline backup i

Mount i

Shutdown

Save state of PDBs i

Choose schedule frequency

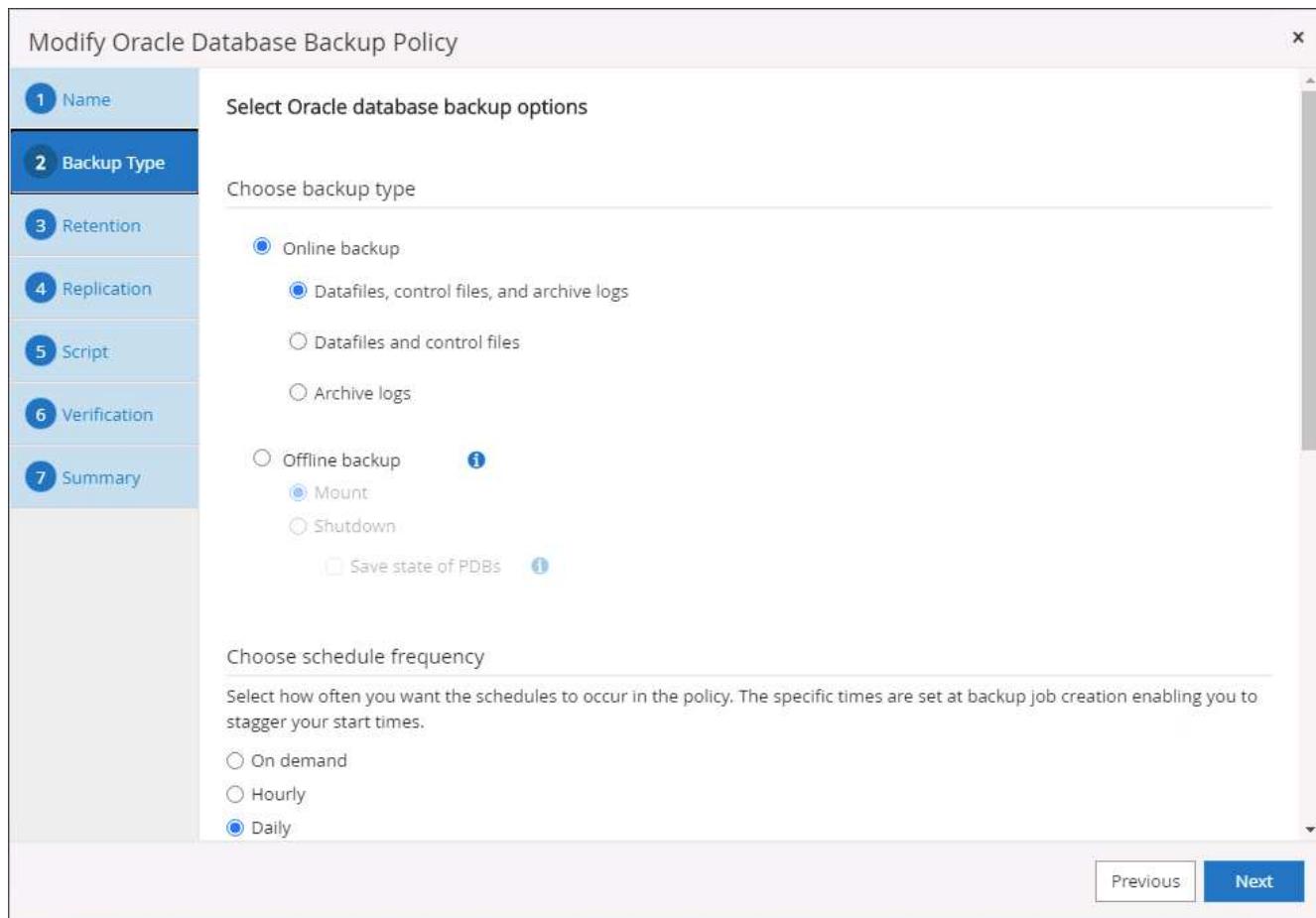
Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

On demand

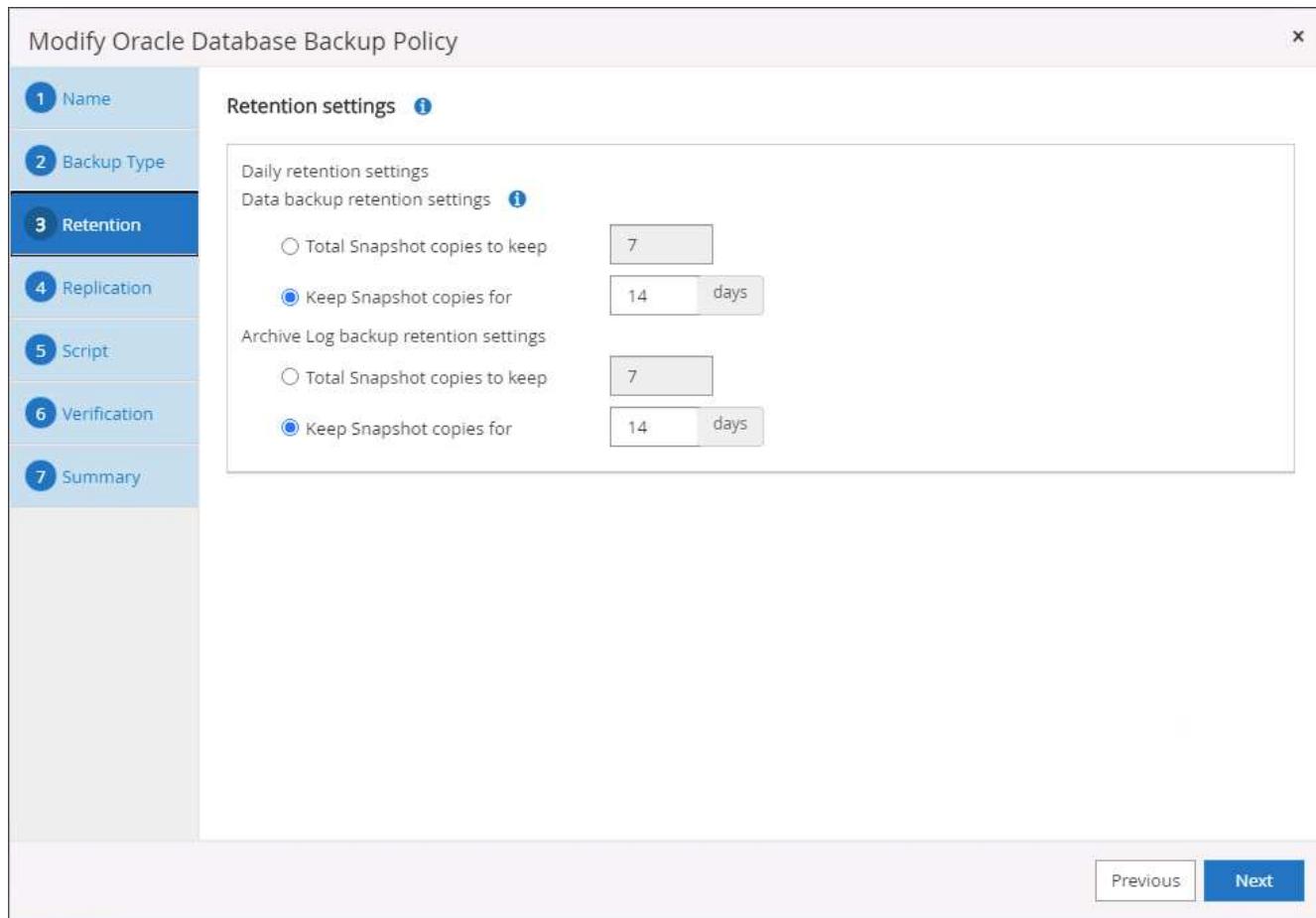
Hourly

Daily

Previous Next



4. Set the backup retention setting. This defines how many full database backup copies to keep.



5. Select the secondary replication options to push local primary snapshots backups to be replicated to a secondary location in cloud.

Modify Oracle Database Backup Policy x

**1 Name**

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Select secondary replication options i

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label Daily i

Error retry count 3 i

Previous Next

6. Specify any optional script to run before and after a backup run.

Modify Oracle Database Backup Policy X

Specify optional scripts to run before and after performing a backup job

1 Name	Prescript full path <input type="text" value="/var/opt/snapcenter/spl/scripts/"/> Enter Prescript path	
2 Backup Type	Prescript arguments <input type="text"/>	
3 Retention	Postscript full path <input type="text" value="/var/opt/snapcenter/spl/scripts/"/> Enter Postscript path	
4 Replication	Postscript arguments <input type="text"/>	
5 Script	Script timeout 60	secs
6 Verification		
7 Summary		

Previous **Next**

7. Run backup verification if desired.

Modify Oracle Database Backup Policy X

**1 Name** Select the options to run backup verification

**2 Backup Type** Run Verifications for following backup schedules

Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

Daily

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Verification script commands

Script timeout	60	secs
Prescript full path	/var/opt/snapcenter/spl/scripts/	Enter Prescript path
Prescript arguments	Choose optional arguments...	
Postscript full path	/var/opt/snapcenter/spl/scripts/	Enter Postscript path
Postscript arguments	Choose optional arguments...	

Previous Next

8. Summary.

Modify Oracle Database Backup Policy

Step	Setting	Description
1 Name	Summary	
2 Backup Type	Policy name	Oracle Full Online Backup
3 Retention	Details	Backup all data and log files
4 Replication	Backup type	Online backup
5 Script	Schedule type	Daily
6 Verification	RMAN catalog backup	Disabled
7 Summary	Archive log pruning	None
	On demand data backup retention	None
	On demand archive log backup retention	None
	Hourly data backup retention	None
	Hourly archive log backup retention	None
	Daily data backup retention	Delete Snapshot copies older than : 14 days
	Daily archive log backup retention	Delete Snapshot copies older than : 14 days
	Weekly data backup retention	None
	Weekly archive log backup retention	None
	Monthly data backup retention	None
	Monthly archive log backup retention	None
	Replication	SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3

[Previous](#) [Finish](#)

## Create a database log backup policy for Oracle

1. Log into SnapCenter with a database management user ID, click Settings, and then click Policies.
2. Click New to launch a new backup policy creation workflow, or choose an existing policy for modification.

New Oracle Database Backup Policy X

**1 Name**

Provide a policy name

Policy name  i

Details

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Previous Next

The screenshot shows the 'New Oracle Database Backup Policy' wizard. The 'Name' step is active, with the policy name set to 'Oracle Archive Log Backup' and details indicating it's for 'Backup Oracle archive logs'. The sidebar lists steps 2 through 7: Backup Type, Retention, Replication, Script, Verification, and Summary. At the bottom are 'Previous' and 'Next' buttons.

3. Select the backup type and schedule frequency.

New Oracle Database Backup Policy

**1 Name**

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Select Oracle database backup options

Choose backup type

Online backup

Datafiles, control files, and archive logs

Datafiles and control files

Archive logs

Offline backup i

Mount

Shutdown

Save state of PDBs i

Choose schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

On demand

Hourly

Daily

[Previous](#) [Next](#)

The screenshot shows the 'New Oracle Database Backup Policy' configuration interface. The left sidebar lists steps 1 through 7. Step 2, 'Backup Type', is currently active. Under 'Choose backup type', 'Archive logs' is selected. Under 'Choose schedule frequency', 'Hourly' is selected. At the bottom right, there are 'Previous' and 'Next' buttons.

4. Set the log retention period.

New Oracle Database Backup Policy

**1 Name**

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Retention settings i

Hourly retention settings

Data backup retention settings i

Total Snapshot copies to keep

Keep Snapshot copies for  days

Archive Log backup retention settings

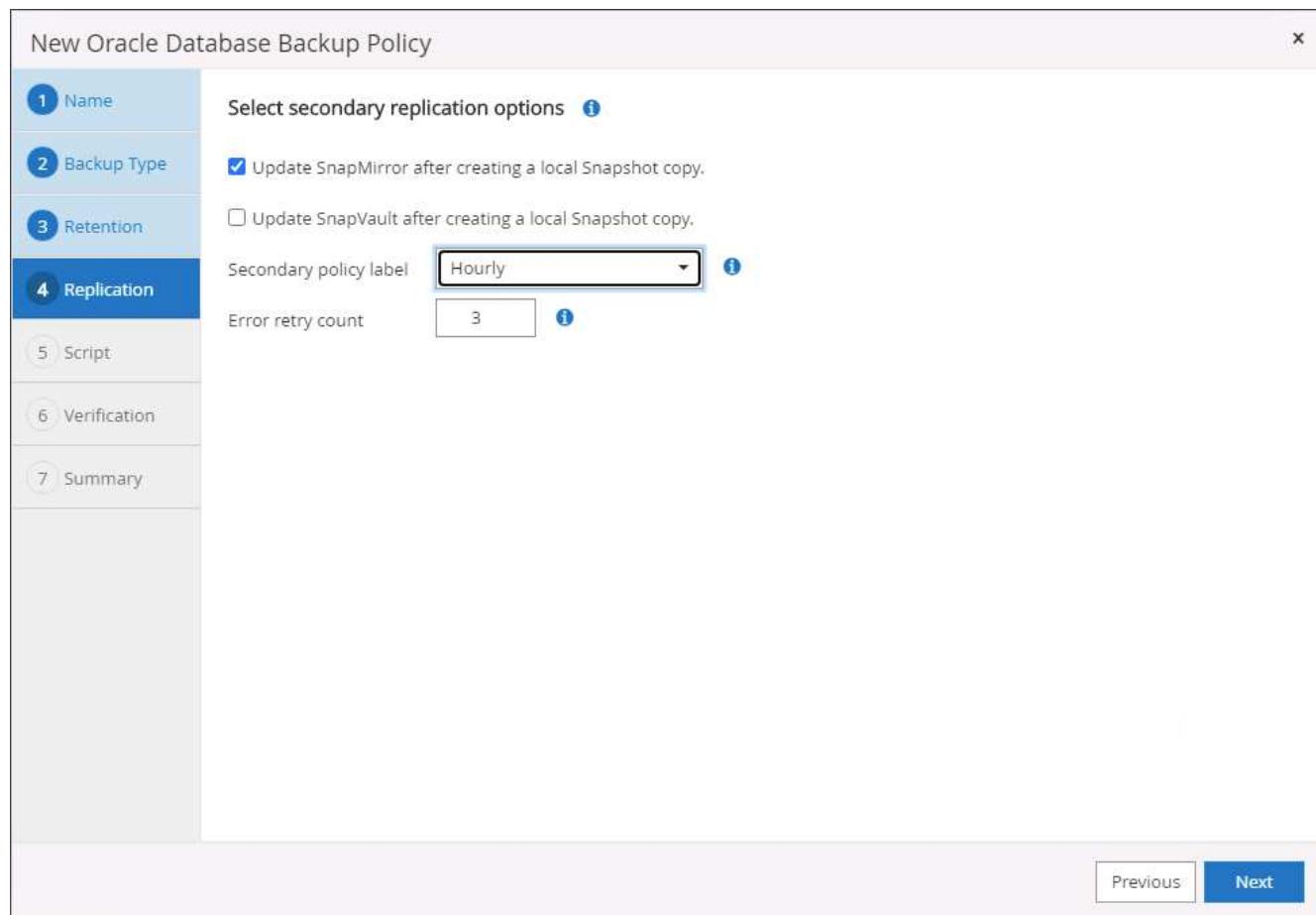
Total Snapshot copies to keep

Keep Snapshot copies for  days

Previous Next

The screenshot shows the 'New Oracle Database Backup Policy' wizard, specifically Step 3: Retention. On the left, a vertical navigation bar lists steps 1 through 7. Step 3, 'Retention', is highlighted. The main area displays 'Retention settings' with two sections: 'Data backup retention settings' and 'Archive Log backup retention settings'. Under each section, there are two radio button options: 'Total Snapshot copies to keep' (set to 7) and 'Keep Snapshot copies for' (set to 7 days). At the bottom right, there are 'Previous' and 'Next' buttons.

5. Enable replication to a secondary location in the public cloud.



6. Specify any optional scripts to run before and after log backup.

New Oracle Database Backup Policy X

Specify optional scripts to run before and after performing a backup job

**1 Name**

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Prescript full path: /var/opt/snapcenter/spl/scripts/ Enter Prescript path

Prescript arguments:

Postscript full path: /var/opt/snapcenter/spl/scripts/ Enter Postscript path

Postscript arguments:

Script timeout: 60 secs

Previous Next

7. Specify any backup verification scripts.

New Oracle Database Backup Policy X

**1 Name** Select the options to run backup verification

**2 Backup Type** Run Verifications for following backup schedules

**3 Retention** Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

**4 Replication**

**5 Script**

**6 Verification** Verification script commands

Script timeout 60 secs

Prescript full path /var/opt/snapcenter/spl/scripts/ Enter Prescript path

Prescript arguments Choose optional arguments...

Postscript full path /var/opt/snapcenter/spl/scripts/ Enter Postscript path

Postscript arguments Choose optional arguments...

[Previous](#) [Next](#)

8. Summary.

New Oracle Database Backup Policy

<b>1 Name</b>	Summary
<b>2 Backup Type</b>	Policy name: Oracle Archive Log Backup Details: Backup Oracle archive logs
<b>3 Retention</b>	Backup type: Online backup
<b>4 Replication</b>	Schedule type: Hourly RMAN catalog backup: Disabled
<b>5 Script</b>	Archive log pruning: None
<b>6 Verification</b>	On demand data backup retention: None
<b>7 Summary</b>	On demand archive log backup retention: None Hourly data backup retention: None Hourly archive log backup retention: Delete Snapshot copies older than : 7 days Daily data backup retention: None Daily archive log backup retention: None Weekly data backup retention: None Weekly archive log backup retention: None Monthly data backup retention: None Monthly archive log backup retention: None Replication: SnapMirror enabled , Secondary policy label: Hourly , Error retry count: 3
<a href="#">Previous</a> <a href="#">Finish</a>	

## Create a full database backup policy for SQL

1. Log into SnapCenter with a database management user ID, click Settings, and then click Policies.

The screenshot shows the NetApp SnapCenter web interface. On the left is a navigation sidebar with links for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings (which is selected), and Alerts. The main content area has a header 'NetApp SnapCenter®' with tabs for 'Policies' (selected) and 'Credential'. A dropdown menu shows 'Microsoft SQL Server'. Below this is a search bar labeled 'Search by Name'. The main table has columns for 'Name', 'Backup Type', 'Schedule Type', 'Replication', and 'Verification'. A message at the bottom of the table says 'There is no match for your search or data is not available.'

2. Click New to launch a new backup policy creation workflow, or choose an existing policy for modification.

New SQL Server Backup Policy

**1 Name**

Provide a policy name

Policy name: SQL Server Full Backup i

Details: Backup all data and log files

**2 Backup Type**

**3 Retention**

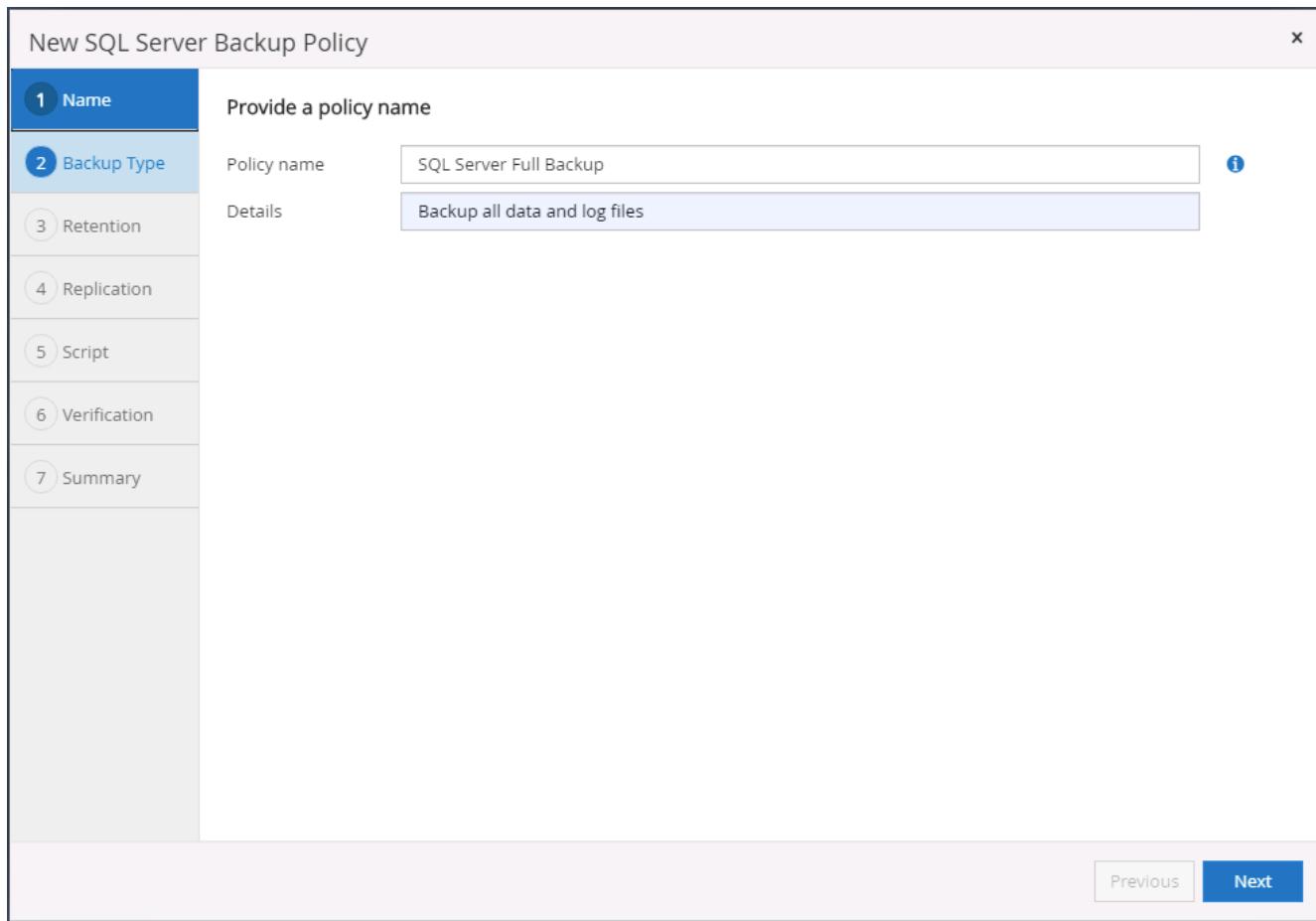
**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Previous Next



3. Define the backup option and schedule frequency. For SQL Server configured with an availability group, a preferred backup replica can be set.

New SQL Server Backup Policy X

**1 Name**

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Select SQL server backup options

Choose backup type

Full backup and log backup

Full backup

Log backup

Copy only backup i

Maximum databases backed up per Snapshot copy: 100 i

**Availability Group Settings** ▼

Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

On demand

Hourly

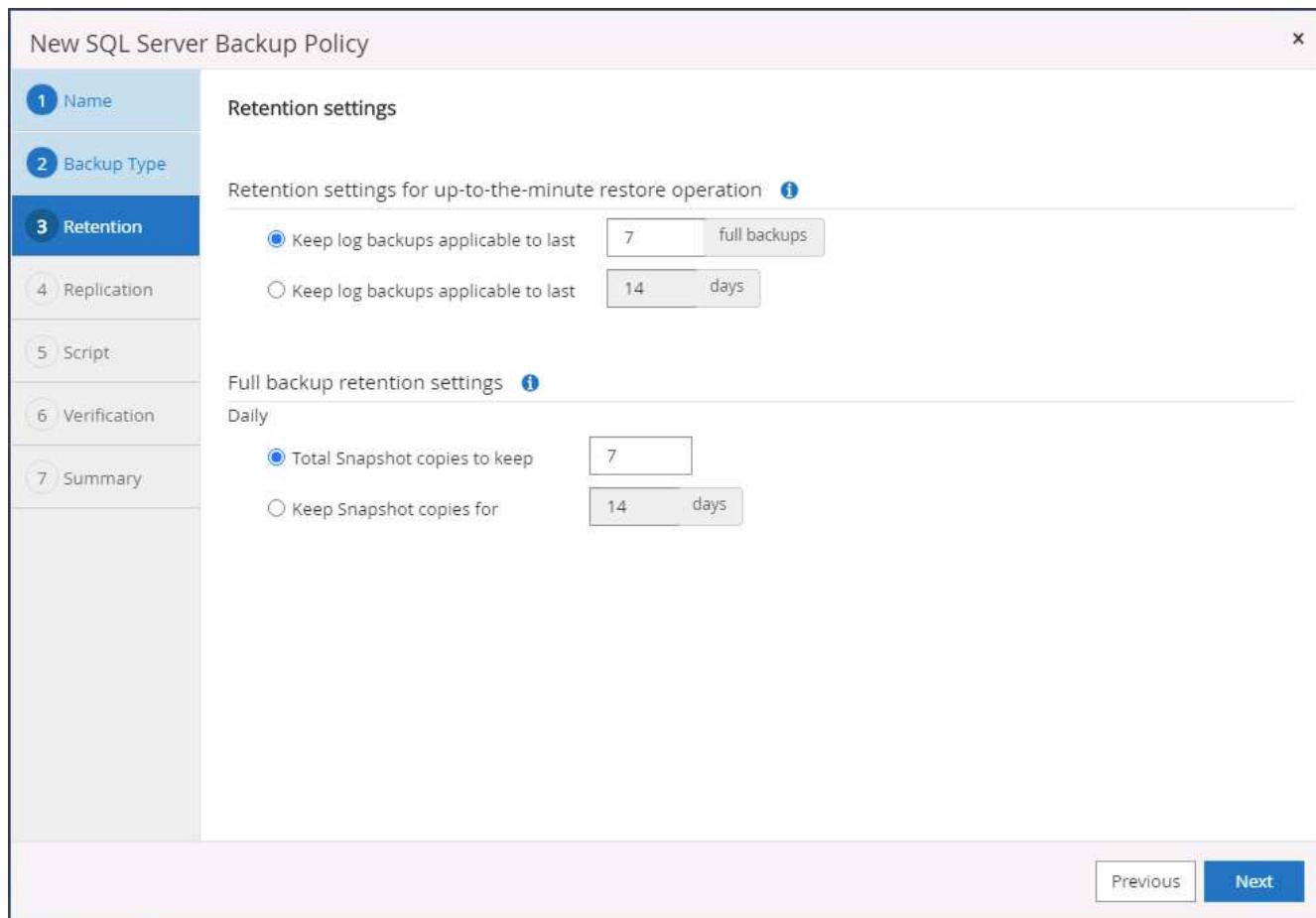
Daily

Weekly

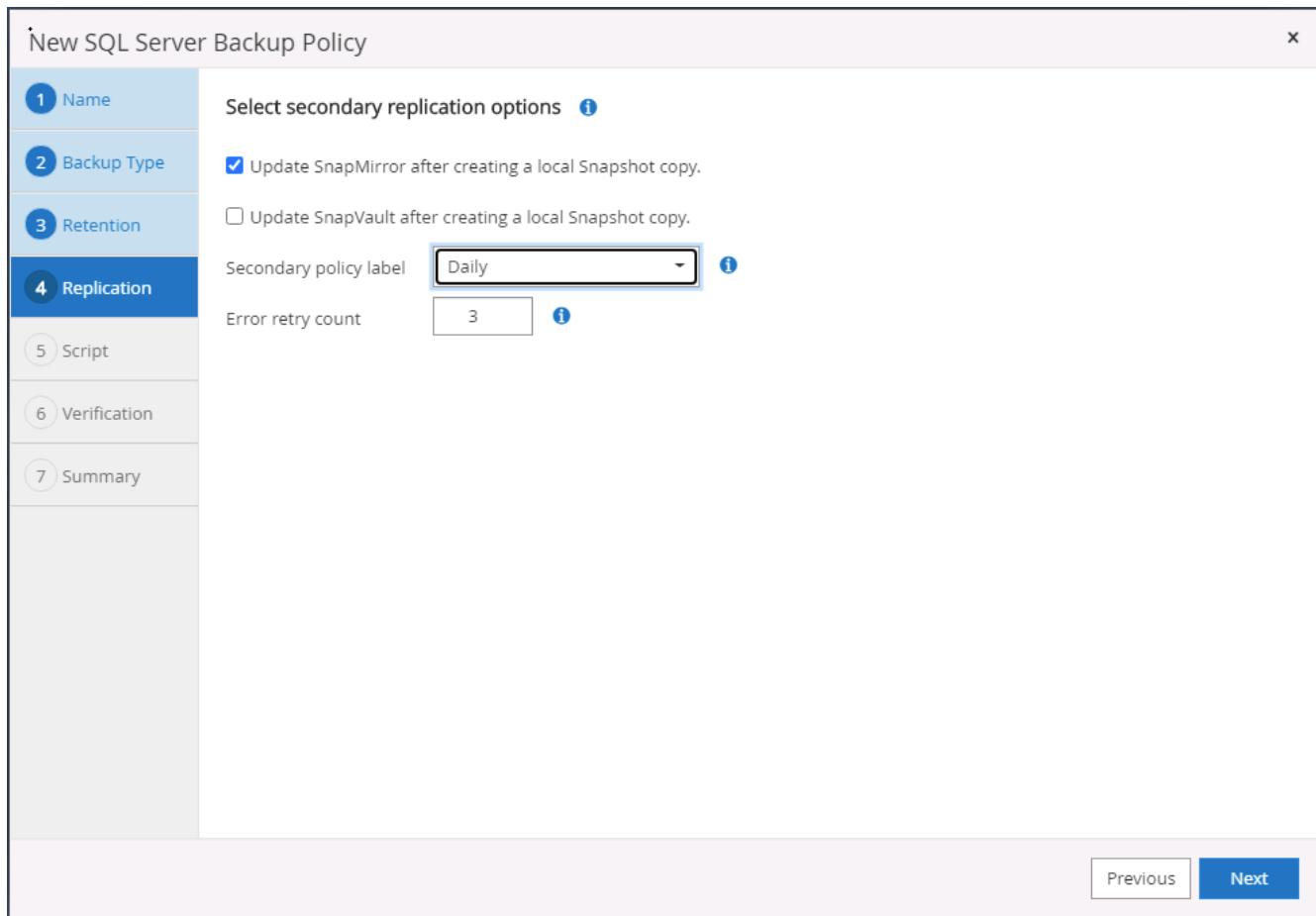
Monthly

Previous Next

4. Set the backup retention period.



5. Enable backup copy replication to a secondary location in cloud.



6. Specify any optional scripts to run before or after a backup job.

New SQL Server Backup Policy X

**1 Name** Specify optional scripts to run before performing a backup job

**2 Backup Type** Prescript full path

**3 Retention** Prescript arguments  Choose optional arguments...

**4 Replication**

**5 Script** Specify optional scripts to run after performing a backup job

**6 Verification** Postscript full path

**7 Summary** Postscript arguments  Choose optional arguments...

Script timeout  secs

Previous Next

7. Specify the options to run backup verification.

New SQL Server Backup Policy

**1 Name**

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Select the options to run backup verification

Run verifications for the following backup schedules

Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

Daily

Database consistency checks options

Limit the integrity structure to physical structure of the database (PHYSICAL\_ONLY)

Suppress all information message (NO\_INFOMSGS)

Display all reported error messages per object (ALL\_ERRORMSGGS)

Do not check non-clustered indexes (NOINDEX)

Limit the checks and obtain the locks instead of using an internal database Snapshot copy (TABLOCK)

Log backup

Verify log backup. i

Verification script settings

Script timeout  secs

Previous Next

8. Summary.

New SQL Server Backup Policy X

1 Name	Summary
2 Backup Type	Policy name: SQL Server Full Backup
3 Retention	Details: Backup all data and log files
4 Replication	Backup type: Full backup and log backup
5 Script	Availability group settings: Backup only on preferred backup replica
6 Verification	Schedule Type: Daily UTM retention: Total backup copies to retain : 7 Daily Full backup retention: Total backup copies to retain : 7 Replication: SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3
7 Summary	Backup prescript settings: undefined Prescript arguments: Backup postscript settings: undefined Postscript arguments: Verification for backup schedule type: none Verification prescript settings: undefined Prescript arguments: Verification postscript settings: undefined Postscript arguments:
<a href="#">Previous</a> <span style="background-color: #0070C0; color: white; padding: 2px 10px; border-radius: 5px;">Finish</span>	

### Create a database log backup policy for SQL.

1. Log into SnapCenter with a database management user ID, click Settings > Policies, and then New to launch a new policy creation workflow.

New SQL Server Backup Policy

**1 Name**

Provide a policy name

Policy name: SQL Server Log Backup

Details: Backup SQL server log

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Previous Next

The screenshot shows the 'New SQL Server Backup Policy' wizard. The 'Name' tab is active. The 'Policy name' field is set to 'SQL Server Log Backup'. The 'Details' field contains the text 'Backup SQL server log'. The sidebar on the left lists other tabs: 'Backup Type', 'Retention', 'Replication', 'Script', 'Verification', and 'Summary'. At the bottom right are 'Previous' and 'Next' buttons.

- Define the log backup option and schedule frequency. For SQL Server configured with a availability group, a preferred backup replica can be set.

New SQL Server Backup Policy X

**1 Name**

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Select SQL server backup options

Choose backup type

Full backup and log backup  
 Full backup  
 Log backup  
 Copy only backup i

Maximum databases backed up per Snapshot copy: 100 i

**Availability Group Settings** ▼

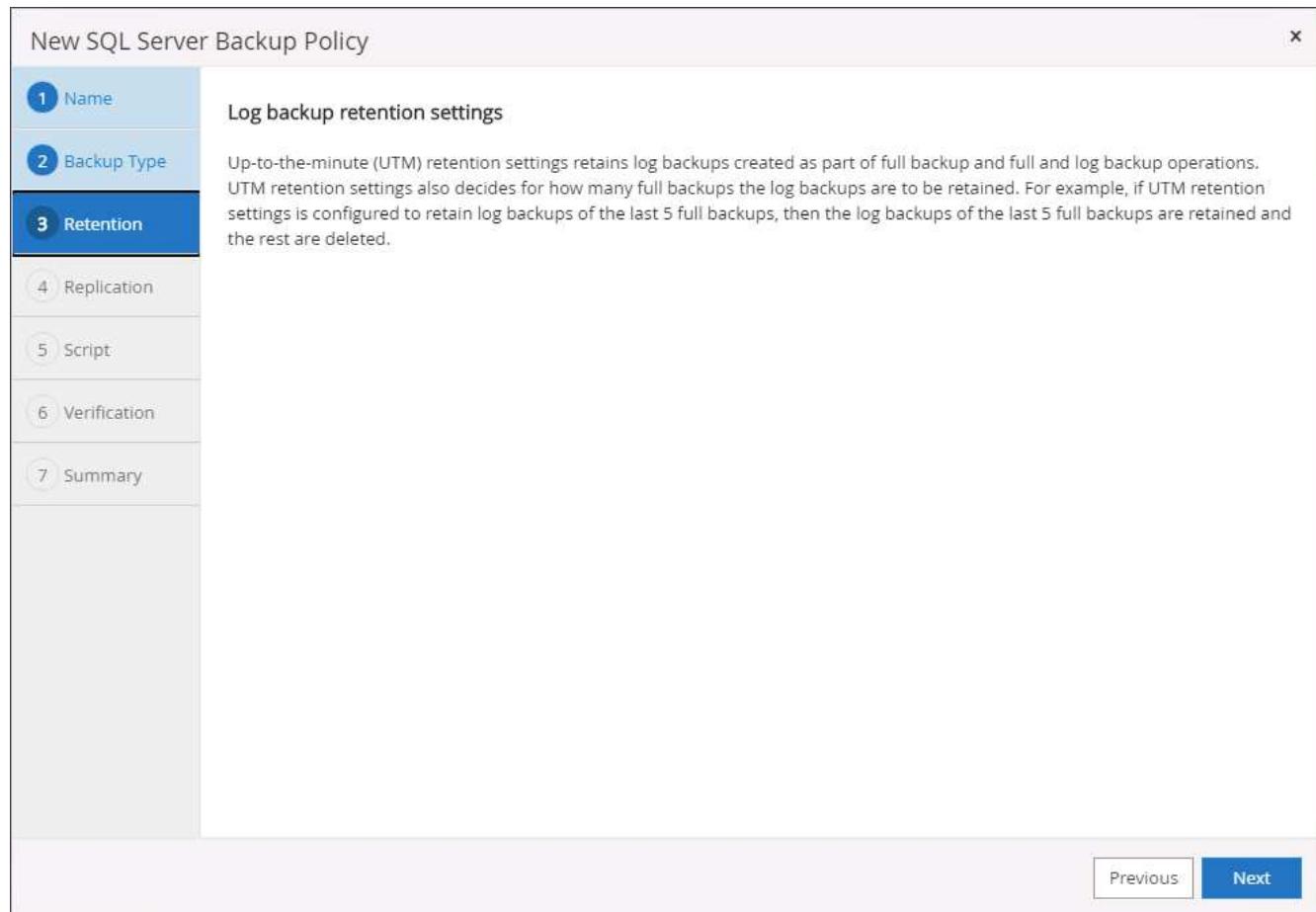
Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

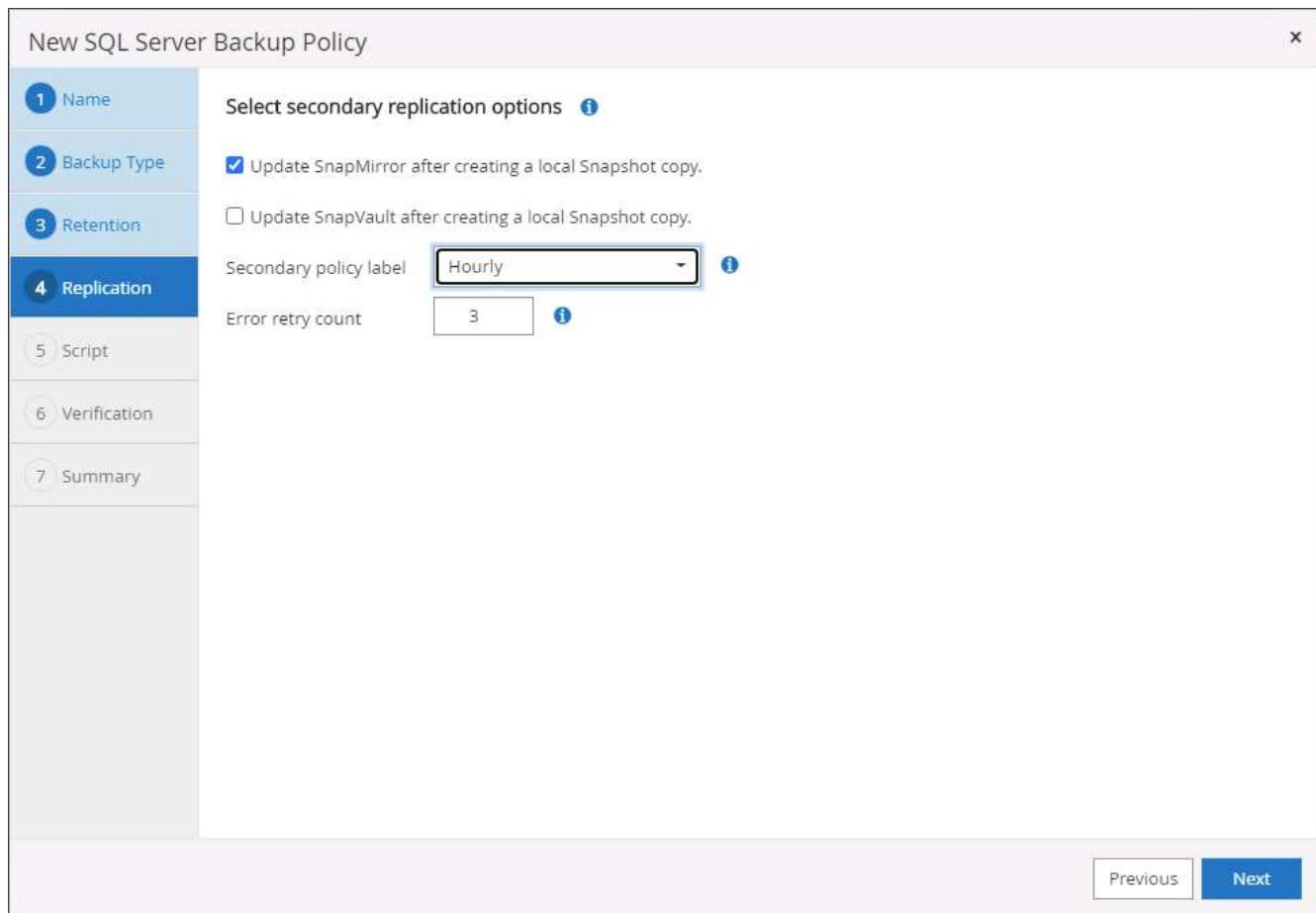
On demand  
 Hourly  
 Daily  
 Weekly  
 Monthly

Previous Next

3. SQL server data backup policy defines the log backup retention; accept the defaults here.



4. Enable log backup replication to secondary in the cloud.



5. Specify any optional scripts to run before or after a backup job.

New SQL Server Backup Policy X

**1 Name**

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments  Choose optional arguments...

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments  Choose optional arguments...

Script timeout  60  secs

**6 Verification**

**7 Summary**

Previous Next

6. Summary.

New SQL Server Backup Policy

Step	Summary
1 Name	Policy name: SQL Server Log Backup
2 Backup Type	Details: Backup SQL server log Backup type: Log transaction backup
3 Retention	Availability group settings: Backup only on preferred backup replica
4 Replication	Schedule Type: Hourly
5 Script	Replication: SnapMirror enabled, Secondary policy label: Hourly, Error retry count: 3
6 Verification	Backup prescript settings: undefined Prescript arguments: Backup postscript settings: undefined Postscript arguments:
7 Summary	Verification for backup schedule type: none Verification prescript settings: undefined Prescript arguments: Verification postscript settings: undefined Postscript arguments:

[Previous](#) [Finish](#)

## 8. Implement backup policy to protect database

SnapCenter uses a resource group to backup a database in a logical grouping of database resources, such as multiple databases hosted on a server, a database sharing the same storage volumes, multiple databases supporting a business application, and so on. Protecting a single database creates a resource group of its own. The following procedures demonstrate how to implement a backup policy created in section 7 to protect Oracle and SQL Server databases.

### Create a resource group for full backup of Oracle

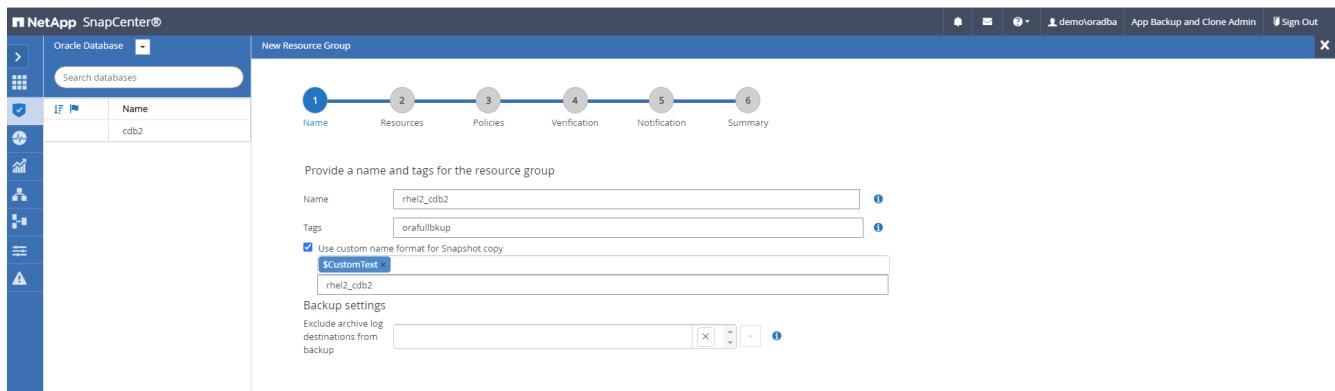
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either Database or Resource Group to launch the resource group creation workflow.

The screenshot shows the NetApp SnapCenter interface. The top navigation bar includes links for Dashboard, Oracle Database, demotoradb, App Backup and Clone Admin, and Sign Out. The left sidebar has links for Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main content area is titled "Oracle Database" and shows a table with one row:

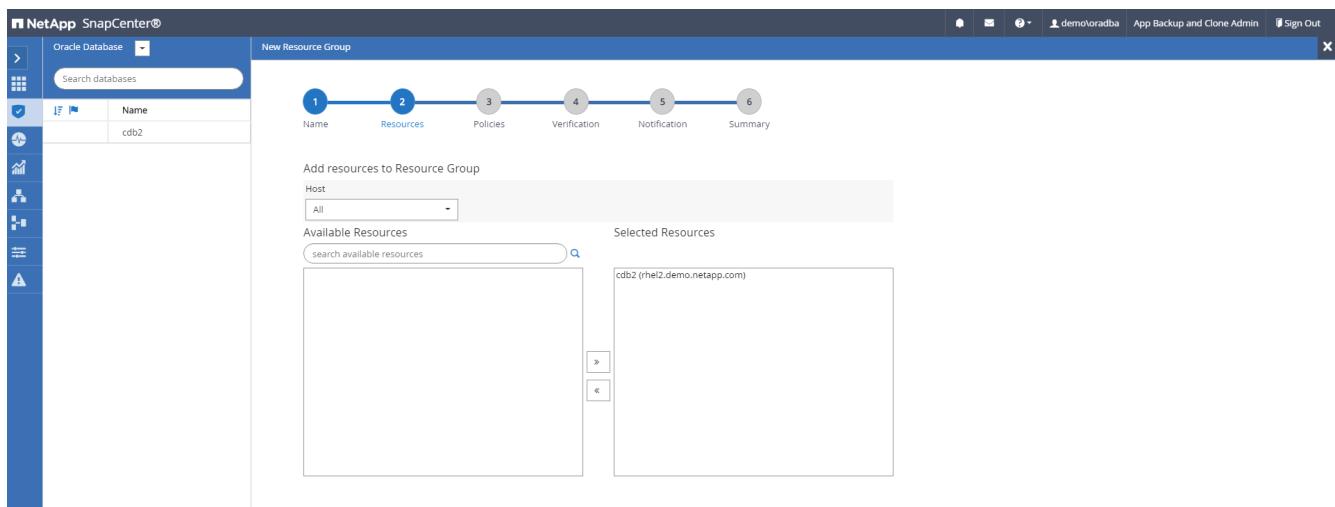
Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com				Not protected

Buttons at the bottom right include Refresh Resources and New Resource Group.

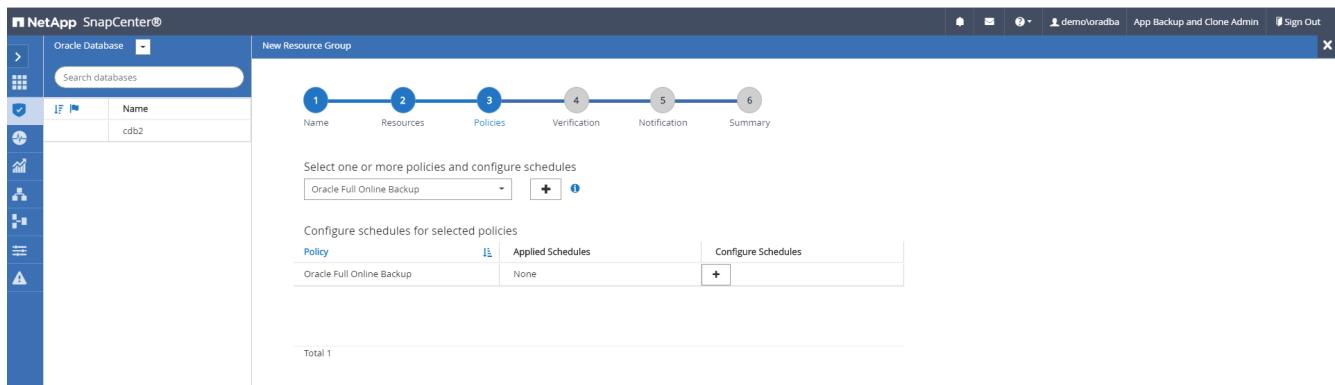
2. Provide a name and tags for the resource group. You can define a naming format for the Snapshot copy and bypass the redundant archive log destination if configured.



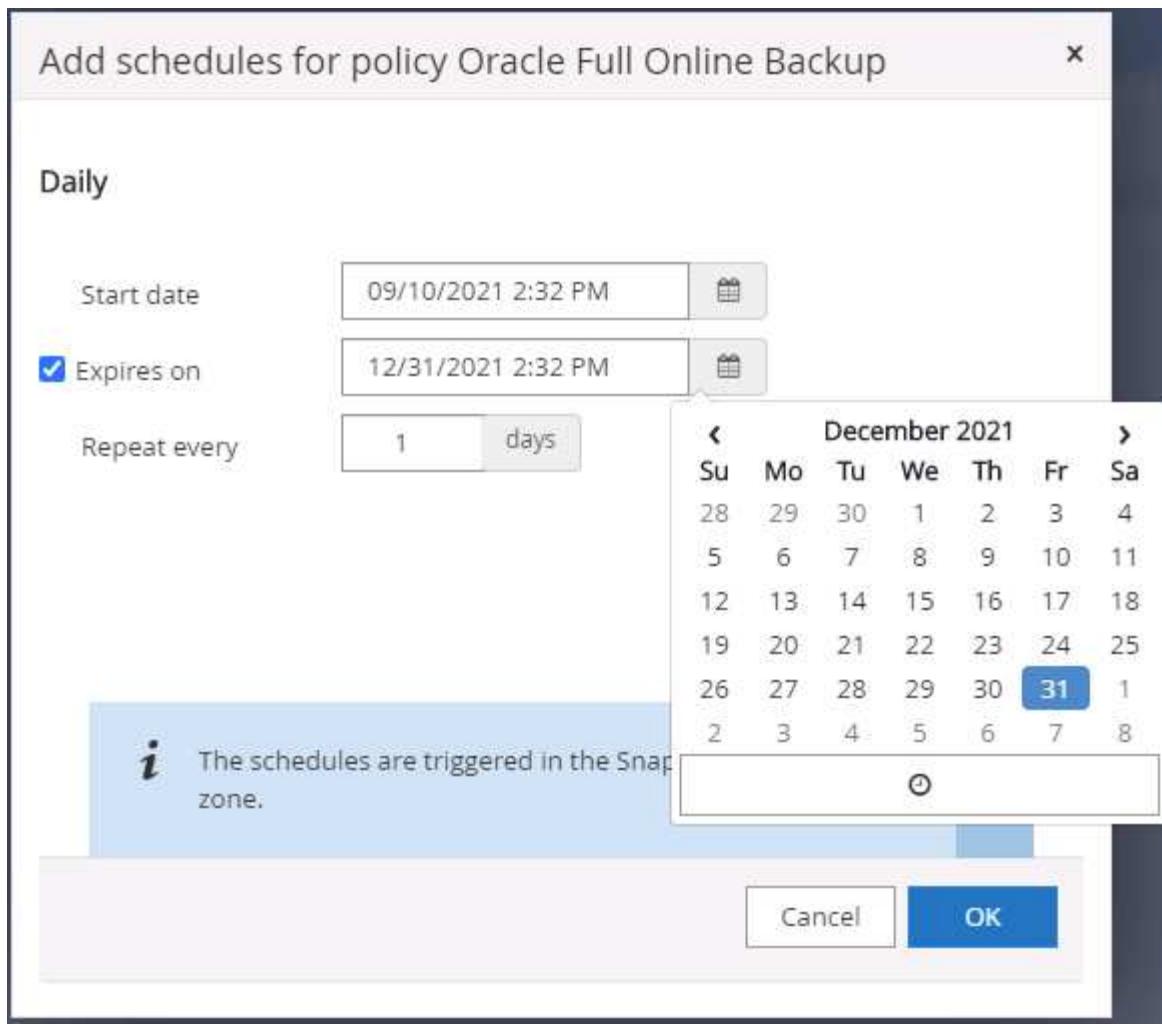
### 3. Add database resources to the resource group.



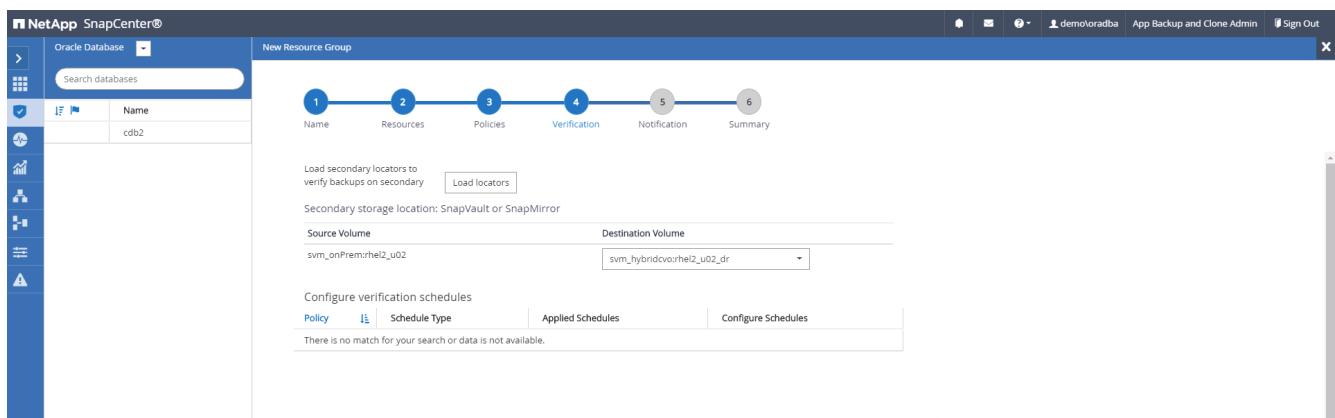
### 4. Select a full backup policy created in section 7 from the drop-down list.



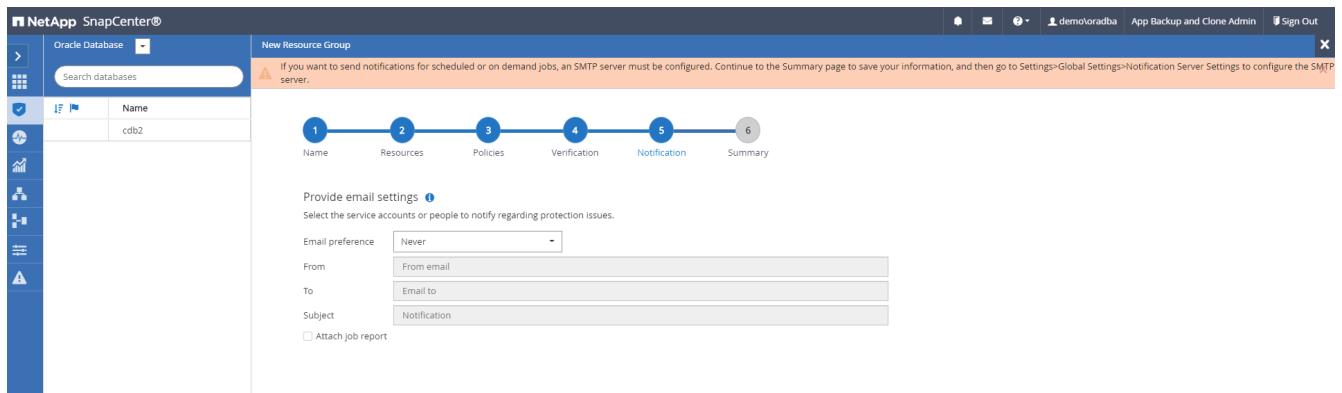
### 5. Click the (+) sign to configure the desired backup schedule.



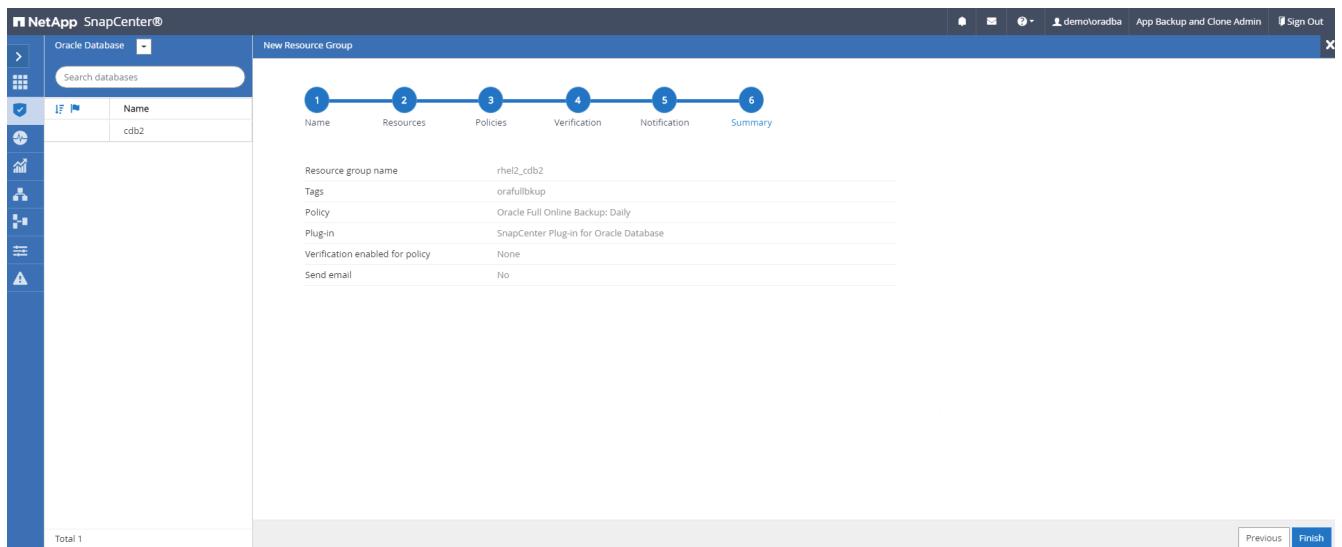
6. Click Load Locators to load the source and destination volume.



7. Configure the SMTP server for email notification if desired.

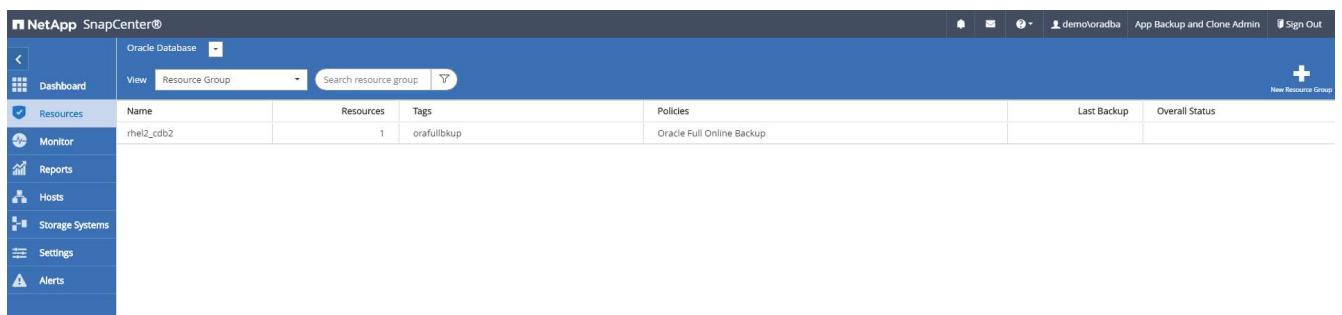


## 8. Summary.

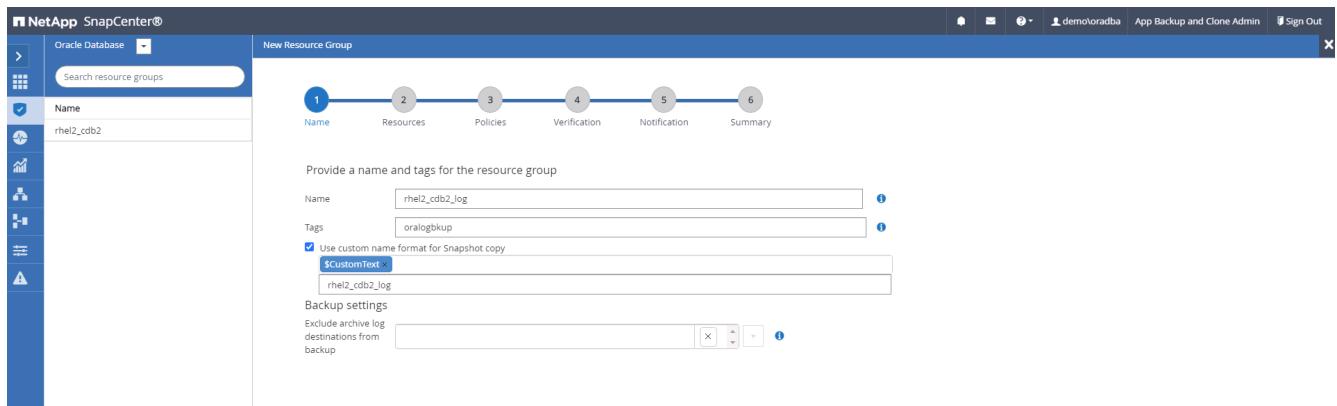


## Create a resource group for log backup of Oracle

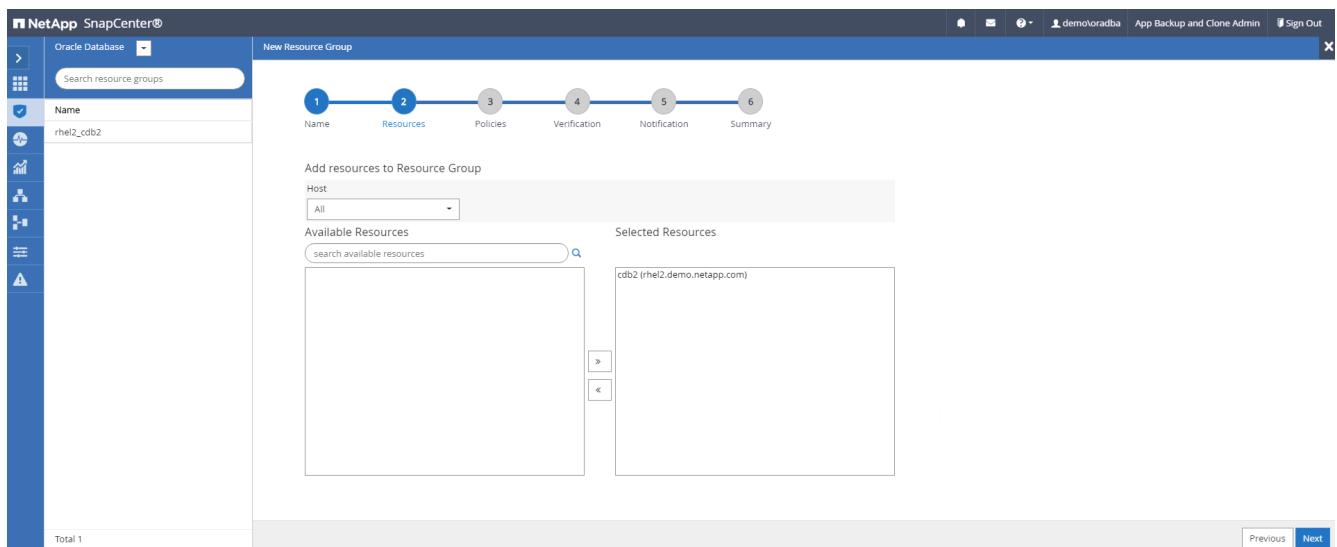
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either Database or Resource Group to launch the resource group creation workflow.



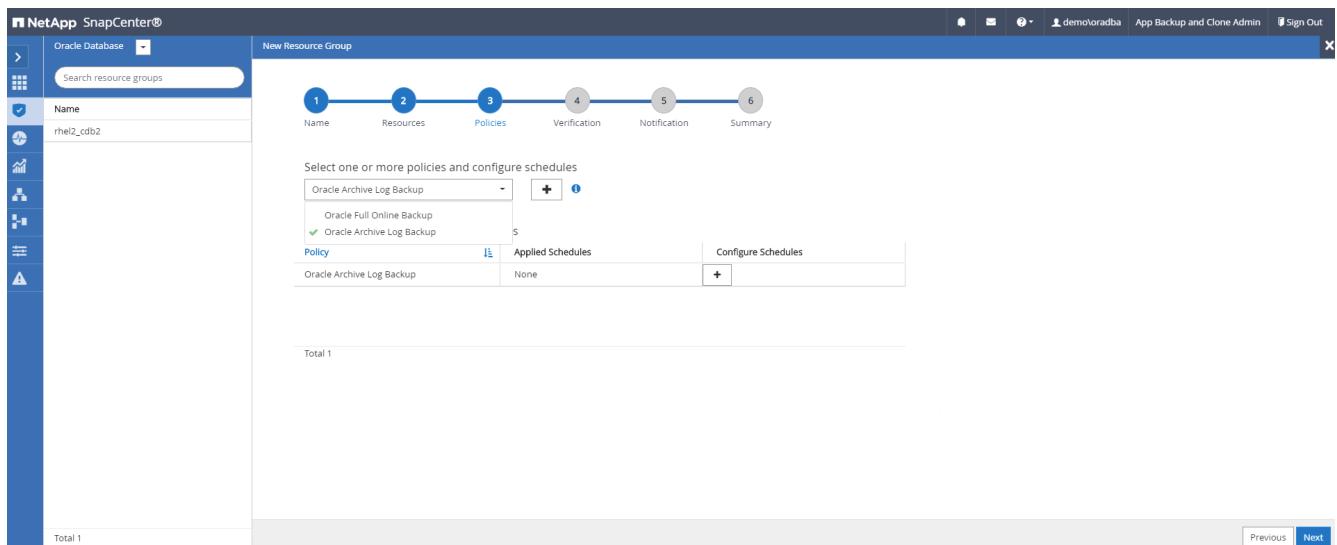
2. Provide a name and tags for the resource group. You can define a naming format for the Snapshot copy and bypass the redundant archive log destination if configured.



3. Add database resources to the resource group.



4. Select a log backup policy created in section 7 from the drop-down list.



5. Click on the (+) sign to configure the desired backup schedule.

Add schedules for policy Oracle Archive Log Backup x

**Hourly**

Start date   

Expires on   

Repeat every  hours  mins

**i** The schedules are triggered in the SnapCenter Server time zone. X

Cancel OK

6. If backup verification is configured, it displays here.

NetApp SnapCenter®

Oracle Database  

New Resource Group

Name

Search resource groups

1 Name      2 Resources      3 Policies      4 Verification      5 Notification      6 Summary

Configure verification schedules

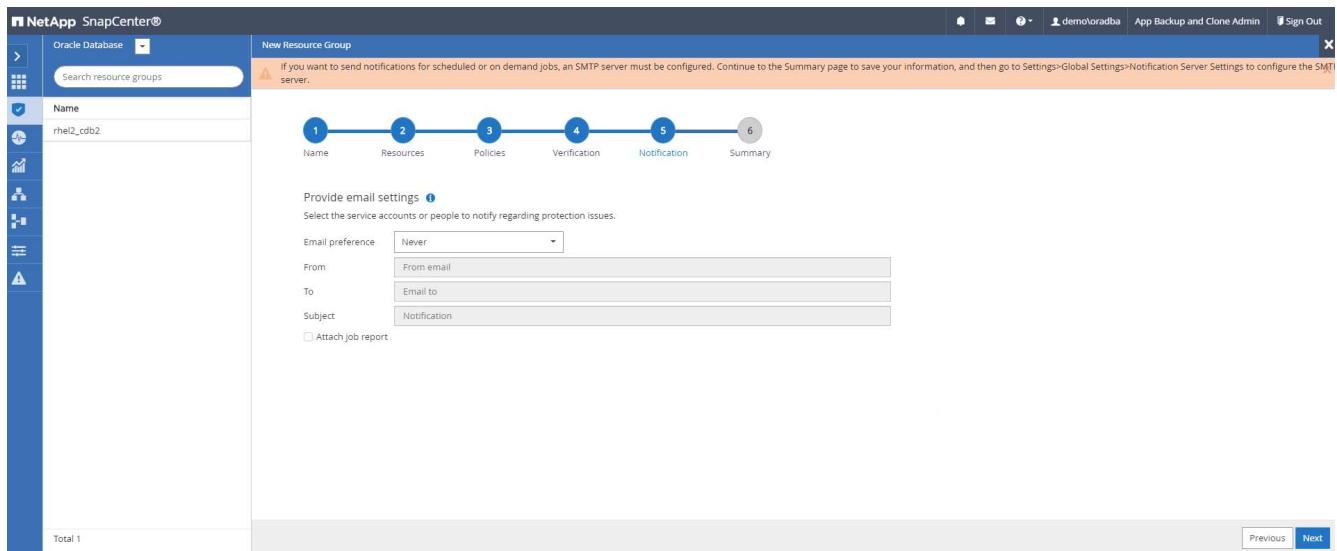
Policy   Schedule Type   Applied Schedules   Configure Schedules

There is no match for your search or data is not available.

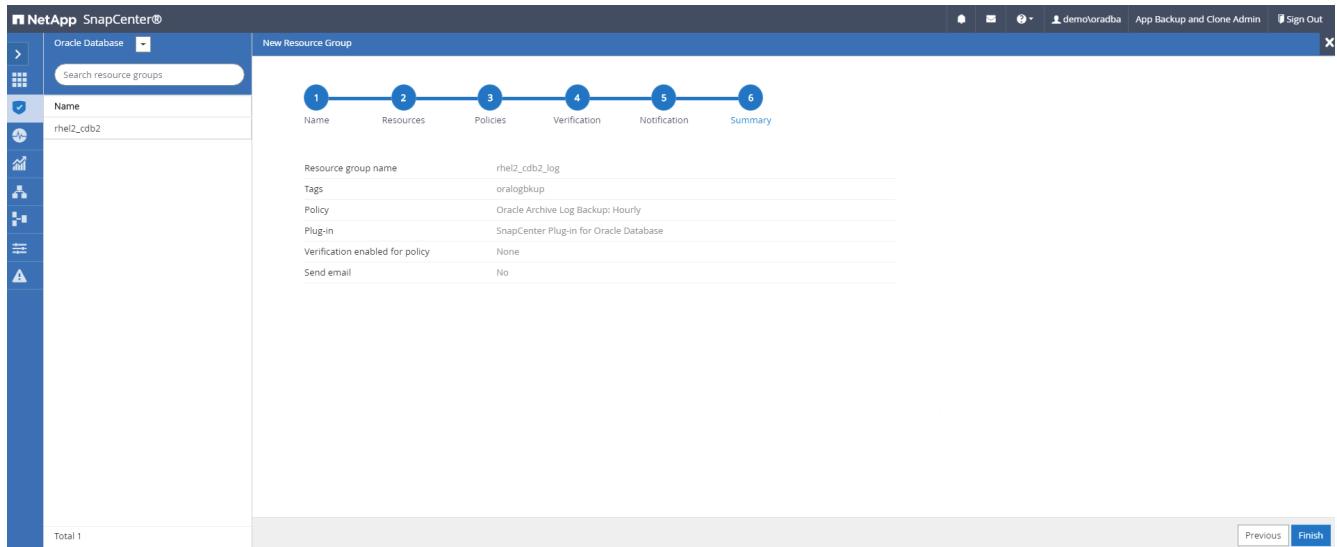
Total 0

Previous Next

7. Configure an SMTP server for email notification if desired.

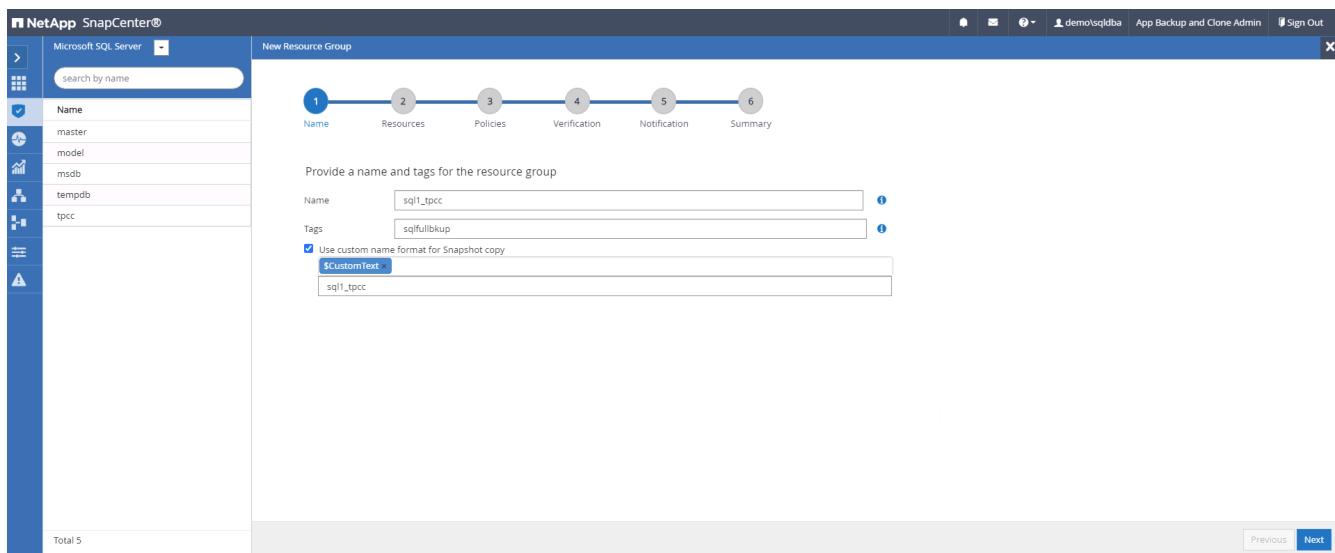


## 8. Summary.

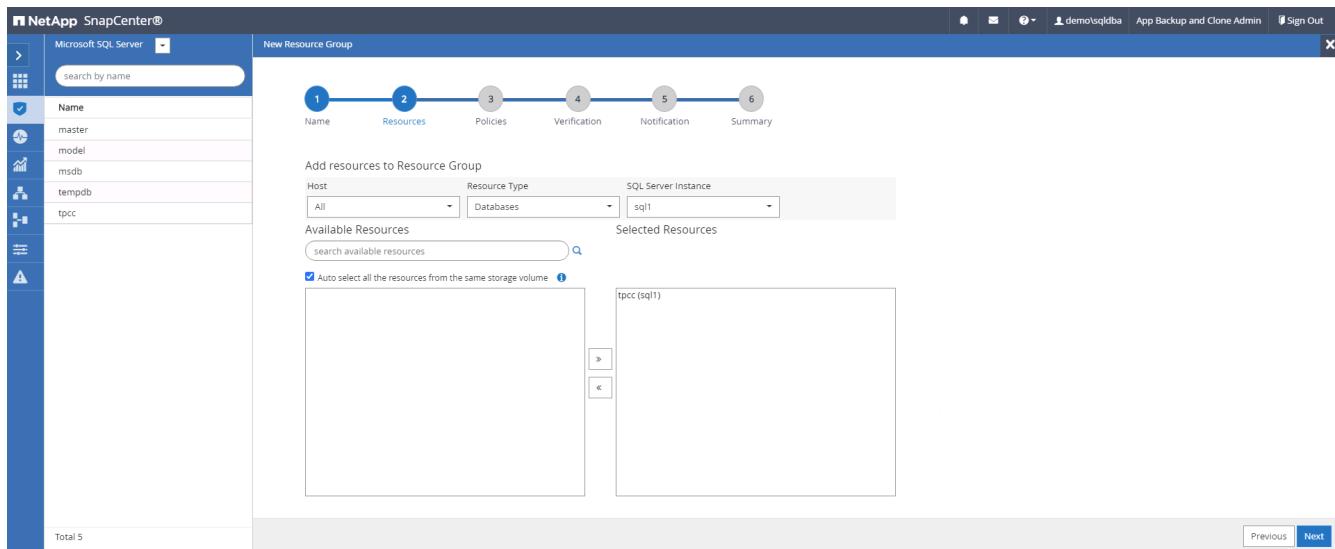


## Create a resource group for full backup of SQL Server

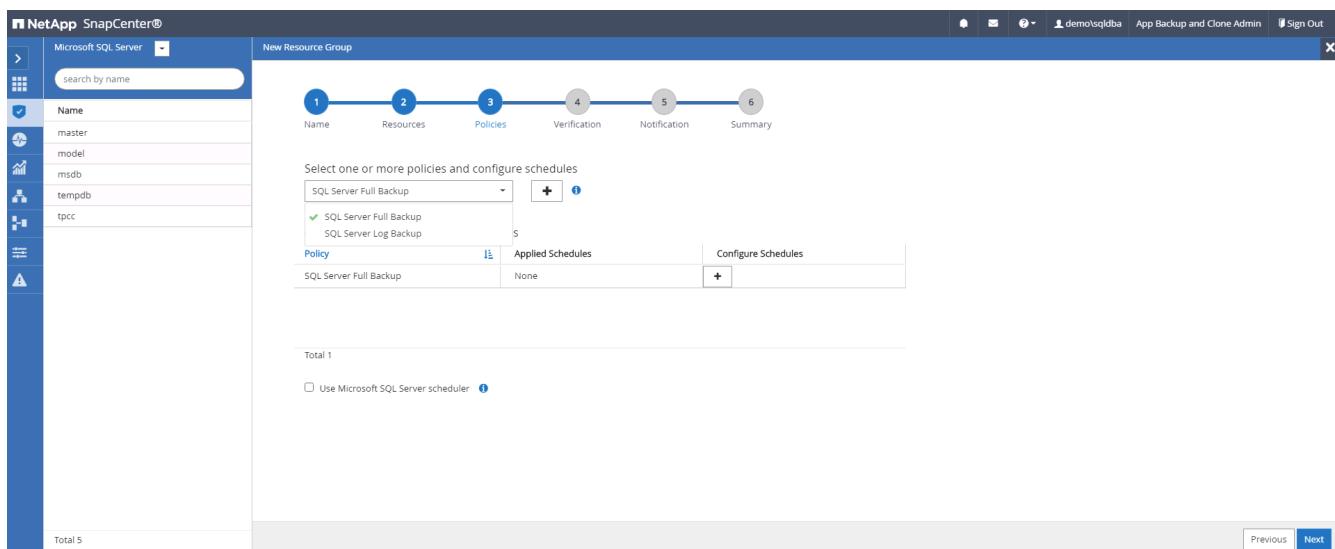
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either a Database or Resource Group to launch the resource group creation workflow. Provide a name and tags for the resource group. You can define a naming format for the Snapshot copy.



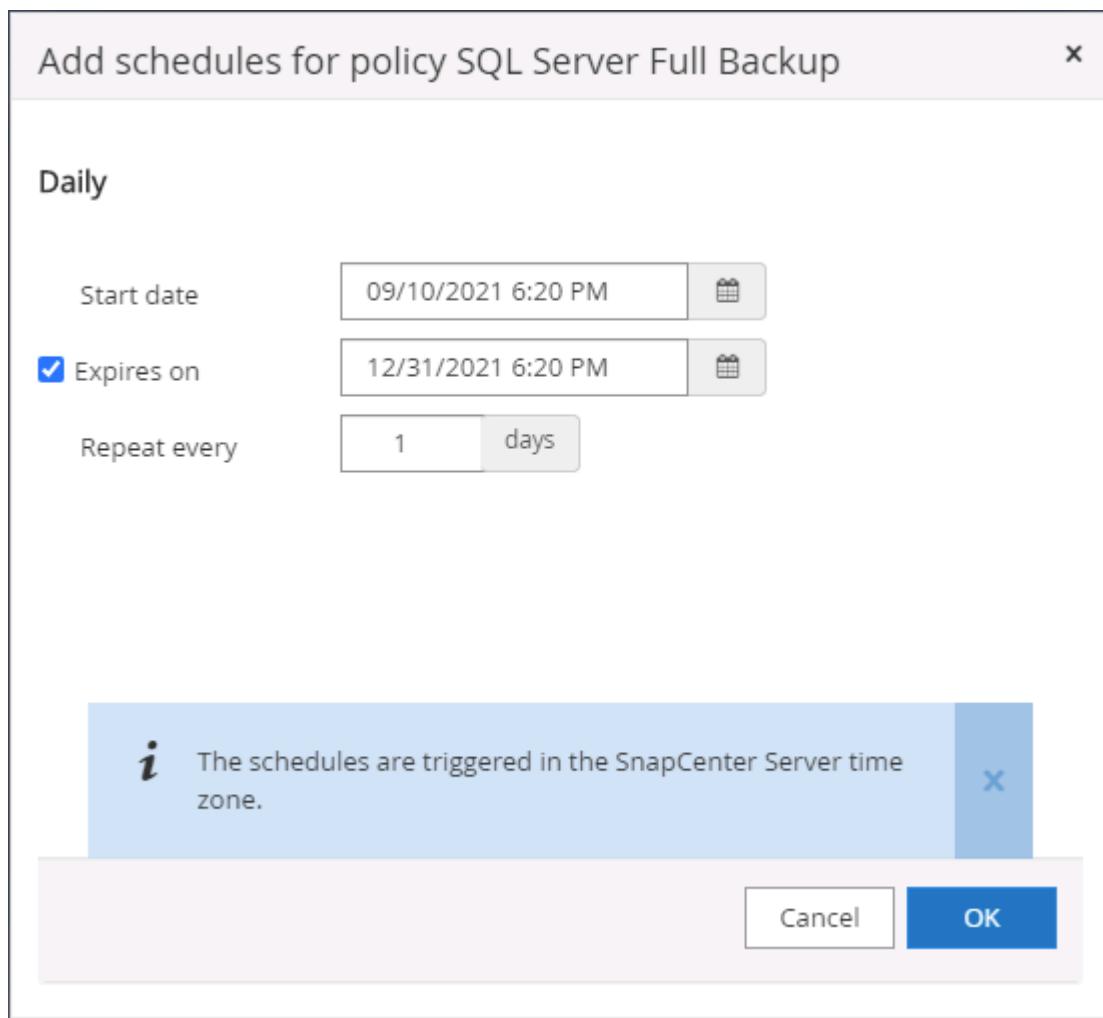
## 2. Select the database resources to be backed up.



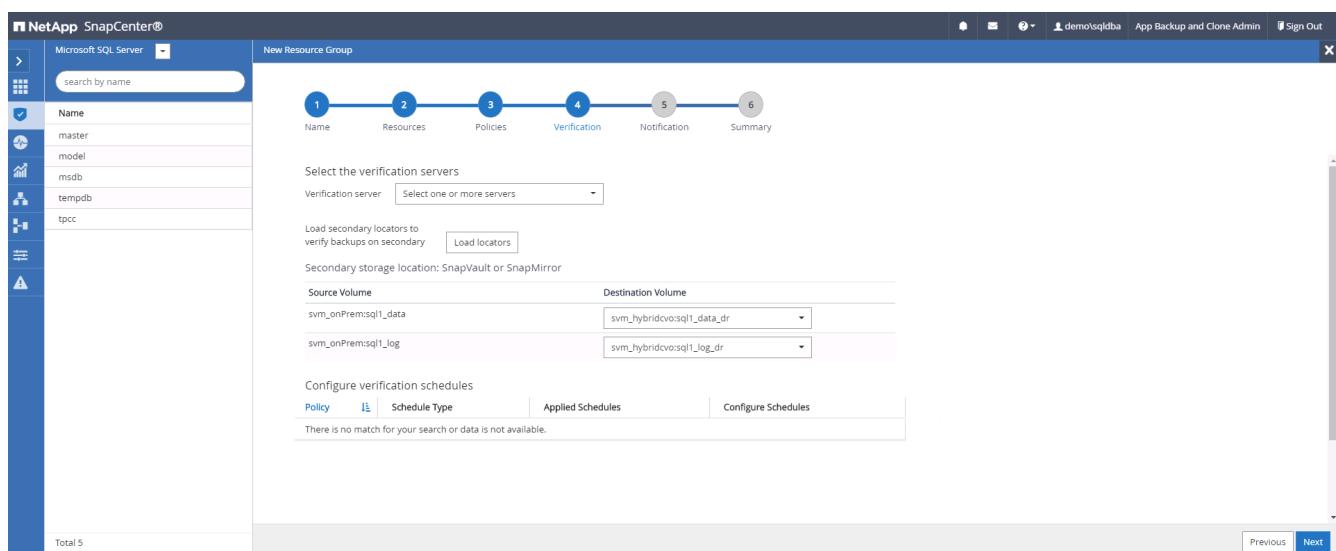
## 3. Select a full SQL backup policy created in section 7.



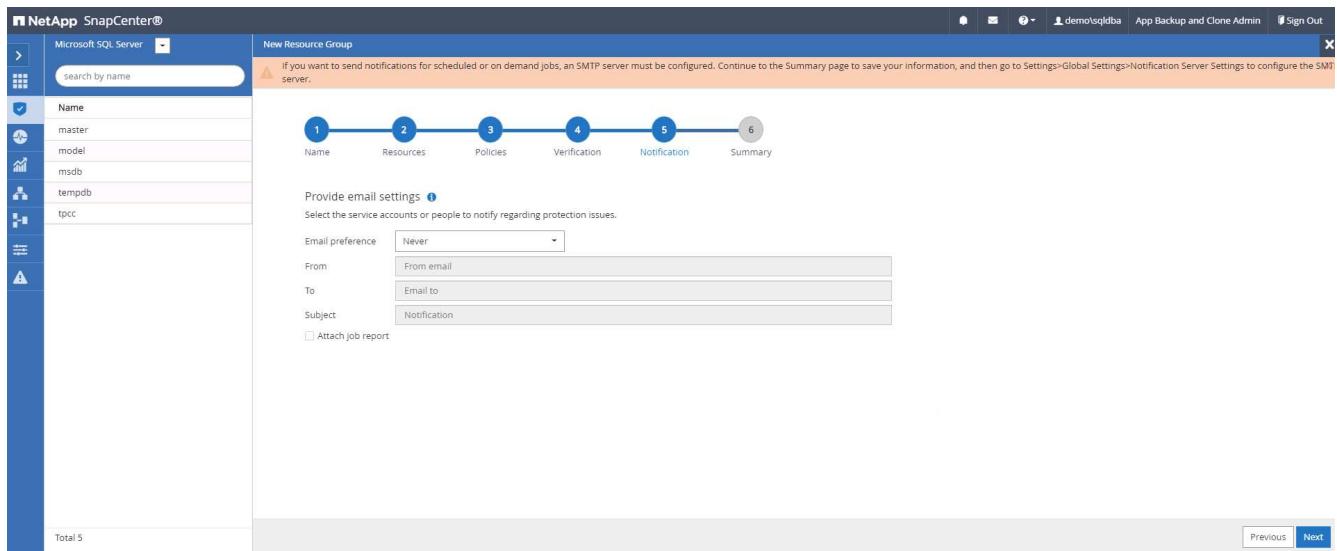
- Add exact timing for backups as well as the frequency.



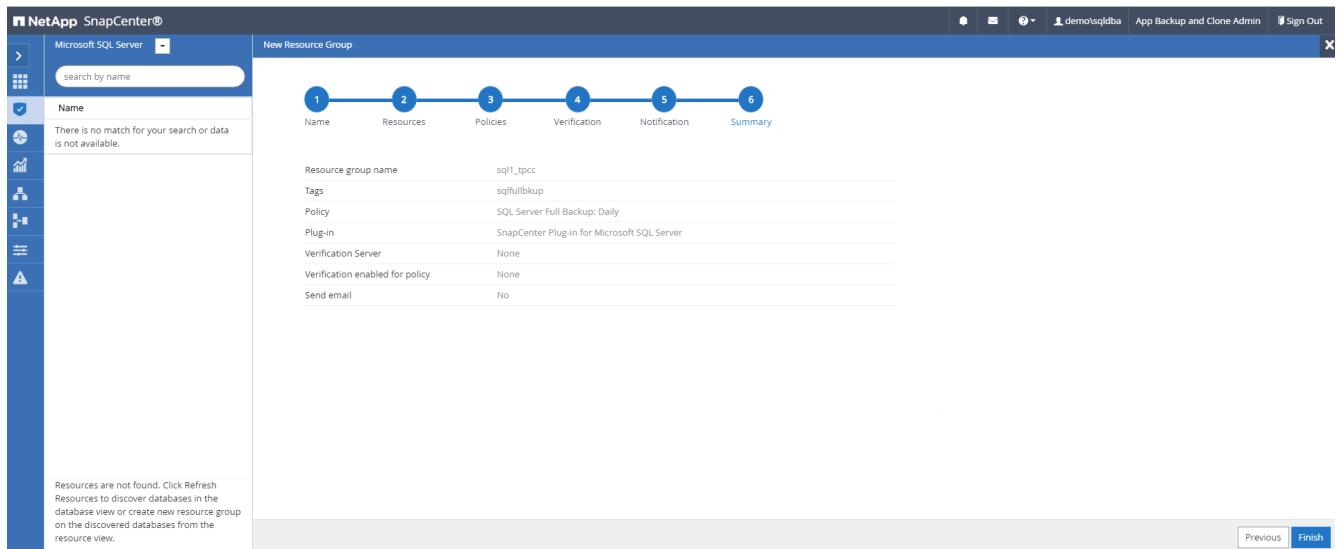
- Choose the verification server for the backup on secondary if backup verification is to be performed. Click Load Locator to populate the secondary storage location.



- Configure the SMTP server for email notification if desired.

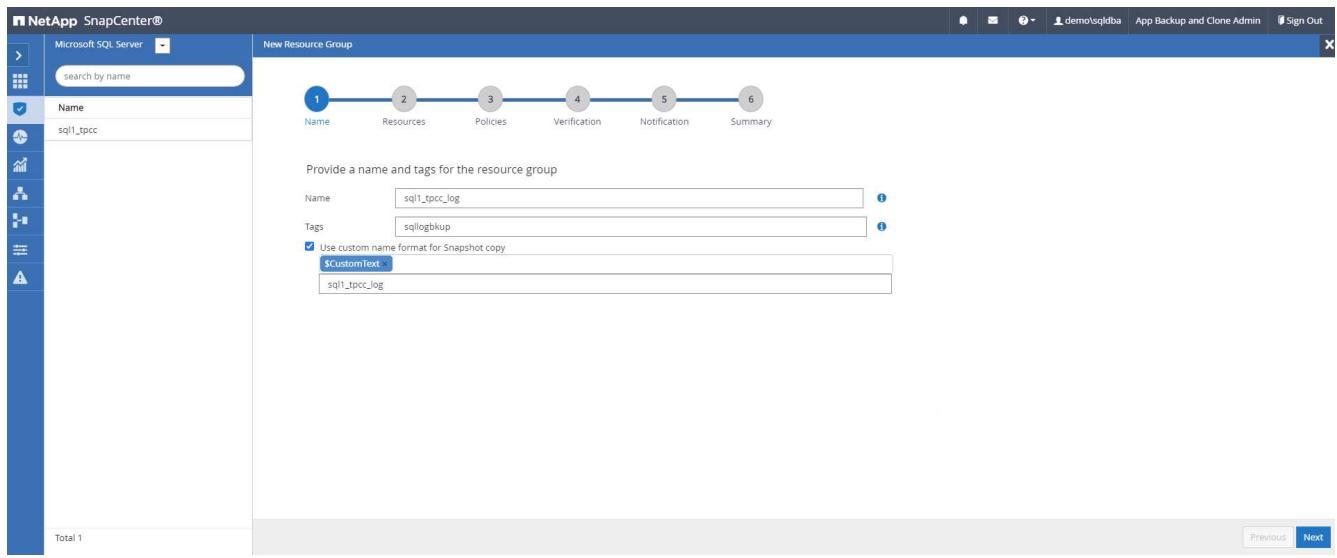


## 7. Summary.

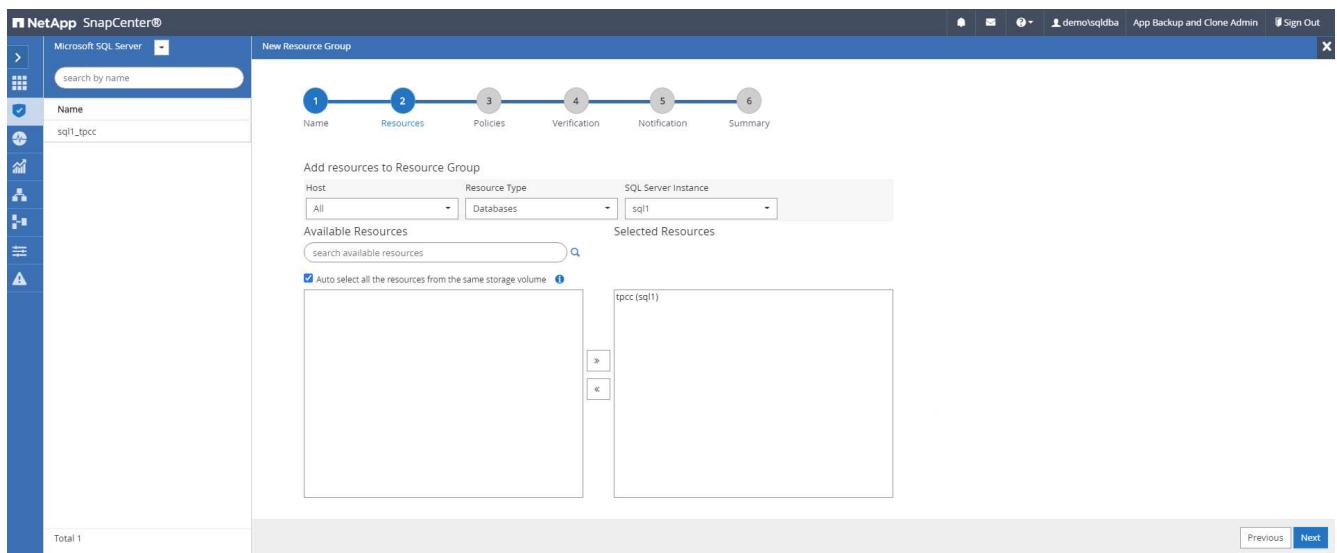


## Create a resource group for log backup of SQL Server

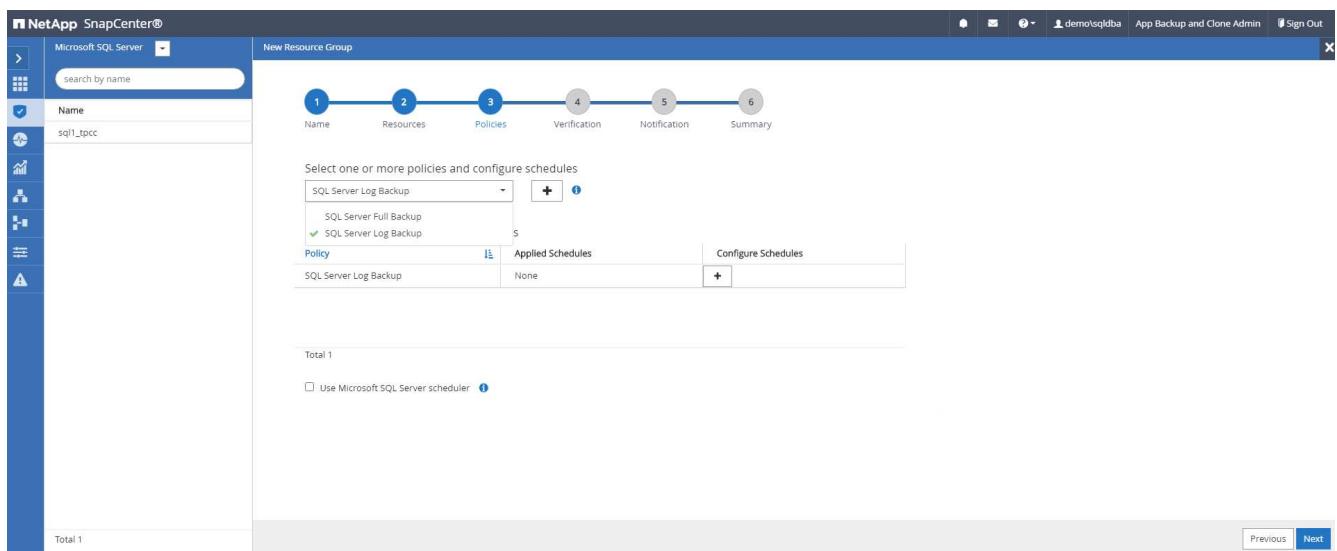
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either a Database or Resource Group to launch the resource group creation workflow. Provide the name and tags for the resource group. You can define a naming format for the Snapshot copy.



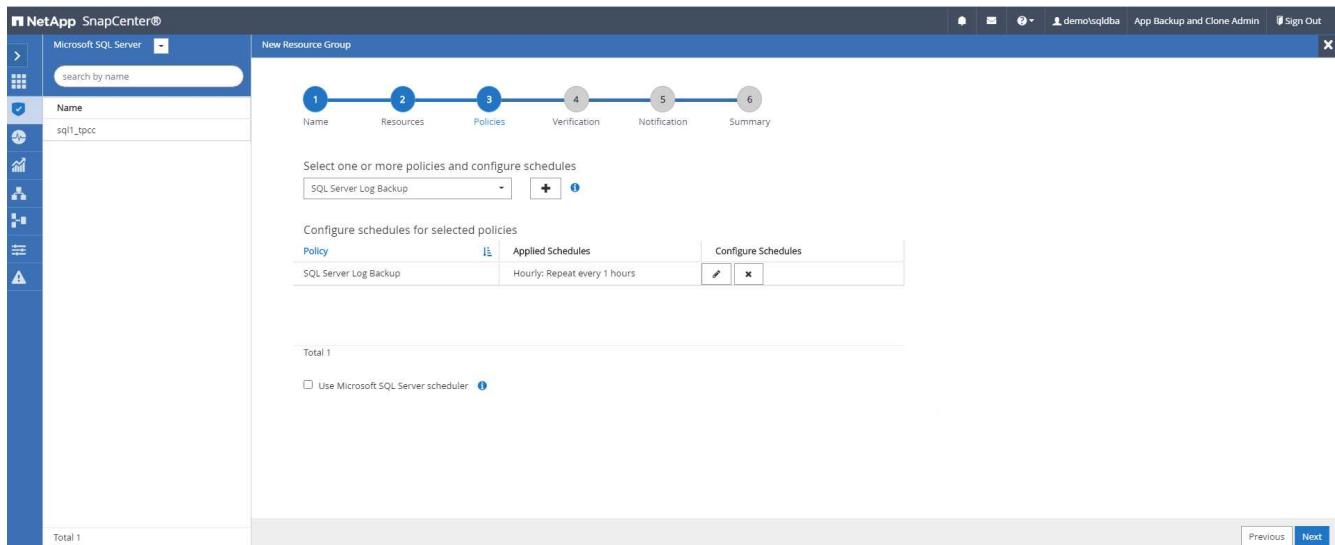
2. Select the database resources to be backed up.



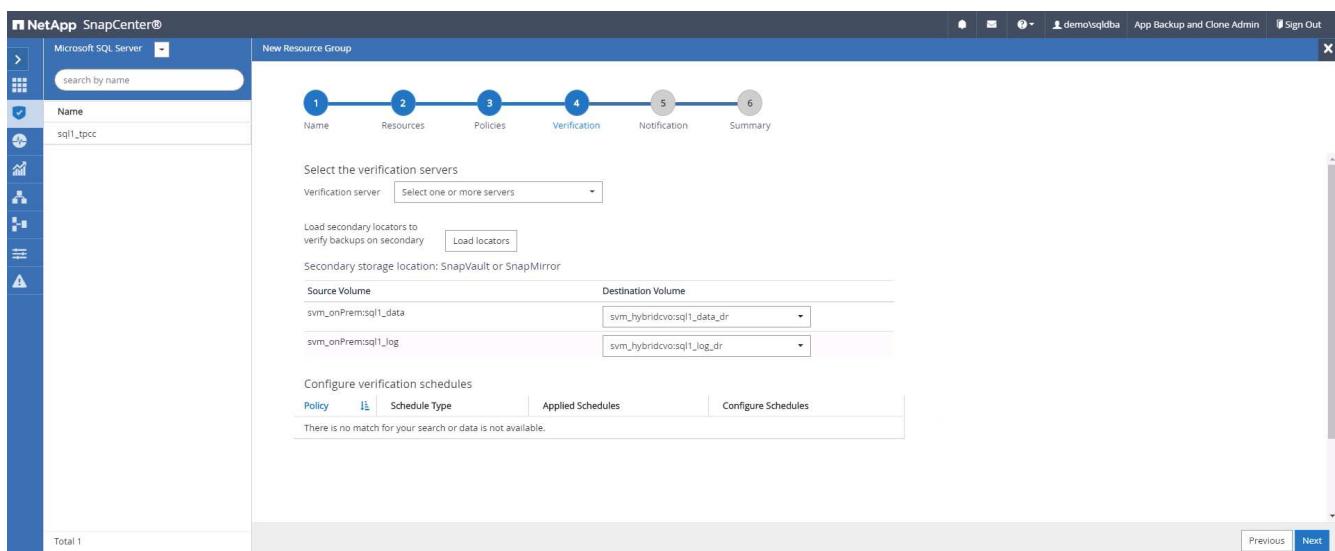
3. Select a SQL log backup policy created in section 7.



4. Add exact timing for the backup as well as the frequency.



5. Choose the verification server for the backup on secondary if backup verification is to be performed. Click the Load Locator to populate the secondary storage location.



6. Configure the SMTP server for email notification if desired.

## 7. Summary.

## 9. Validate backup

After database backup resource groups are created to protect database resources, the backup jobs runs according to the predefined schedule. Check the job execution status under the Monitor tab.

ID	Status	Name	Start date	End date	Owner
532	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 8:35:01 PM	09/14/2021 8:37:10 PM	demo\sqldba
528	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 7:35:01 PM	09/14/2021 7:37:09 PM	demo\sqldba
524	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 6:35:01 PM	09/14/2021 6:37:08 PM	demo\sqldba
521	✓	Backup of Resource Group 'sql1_tpcc' with policy 'SQL Server Full Backup'	09/14/2021 6:25:01 PM	09/14/2021 6:27:14 PM	demo\sqldba
517	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 5:35:01 PM	09/14/2021 5:37:09 PM	demo\sqldba
513	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 4:35:01 PM	09/14/2021 4:37:08 PM	demo\sqldba
509	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 3:35:01 PM	09/14/2021 3:37:09 PM	demo\sqldba
503	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 2:35:01 PM	09/14/2021 2:37:09 PM	demo\sqldba

Go to the Resources tab, click the database name to view details of database backup, and toggle between Local copies and mirror copies to verify that Snapshot backups are replicated to a secondary location in the

public cloud.

The screenshot shows the NetApp SnapCenter interface for Oracle Database. On the left, a sidebar lists databases: cdb2, cdb2dev, cdb2dr, cdb2dr2, and cdb2test. The main area displays 'cdb2 Topology' with a summary card showing 394 Backups, 28 Data Backups, 366 Log Backups, and 3 Clones. It also shows 'Manage Copies' for Local copies (197 Backups, 0 Clones) and Mirror copies (197 Backups, 3 Clones). Below this is a table titled 'Primary Backup(s)' listing five backups with details like Count, Type, End Date, Verified, Mounted, RMAN Cataloged, and SCN.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_09-23-2021_14.35.03.3242_1	1	Log	09/23/2021 2:35:45 PM	Not Applicable	False	Not Cataloged	6872761
rhel2_cdb2_09-23-2021_14.35.03.3242_0	1	Data	09/23/2021 2:35:30 PM	Unverified	False	Not Cataloged	6872715
rhel2_cdb2_09-22-2021_14.35.02.0014_1	1	Log	09/22/2021 2:35:24 PM	Not Applicable	False	Not Cataloged	6737479
rhel2_cdb2_09-22-2021_14.35.02.0014_0	1	Data	09/22/2021 2:35:14 PM	Unverified	False	Not Cataloged	6737395
rhel2_cdb2_09-21-2021_14.35.02.1884_1	1	Log	09/21/2021 2:35:35 PM	Not Available	False	Not Cataloged	6598735

At this point, database backup copies in the cloud are ready to clone to run dev/test processes or for disaster recovery in the event of a primary failure.

Next: [Getting Started with AWS public cloud](#).

## 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.



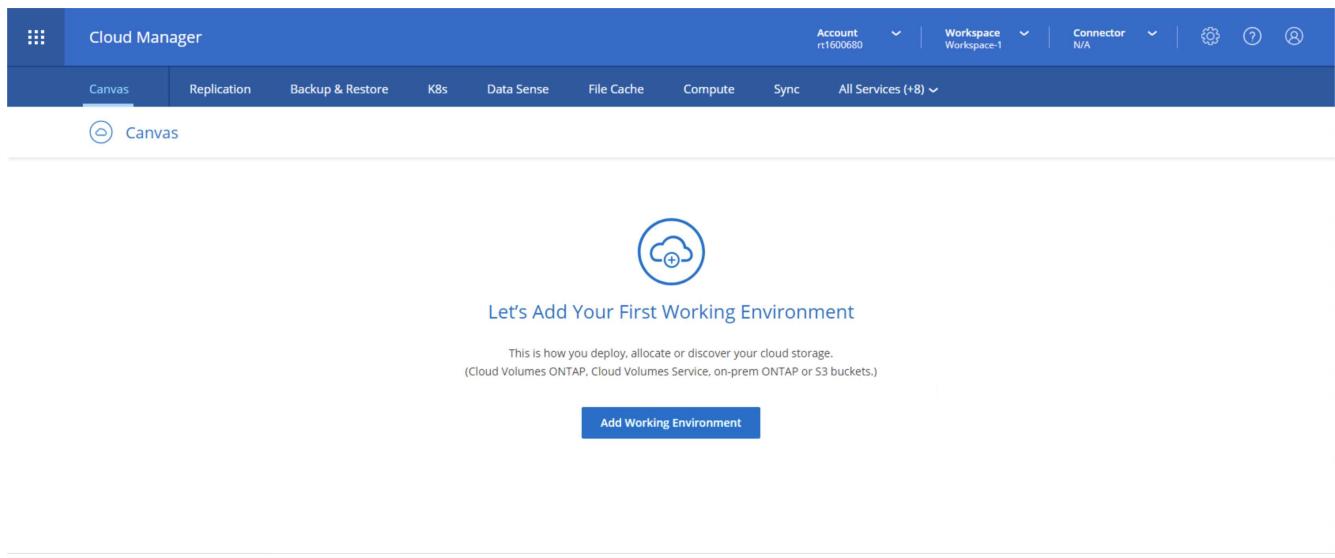
[Continue to Cloud Manager](#)

## Log In to NetApp Cloud Central

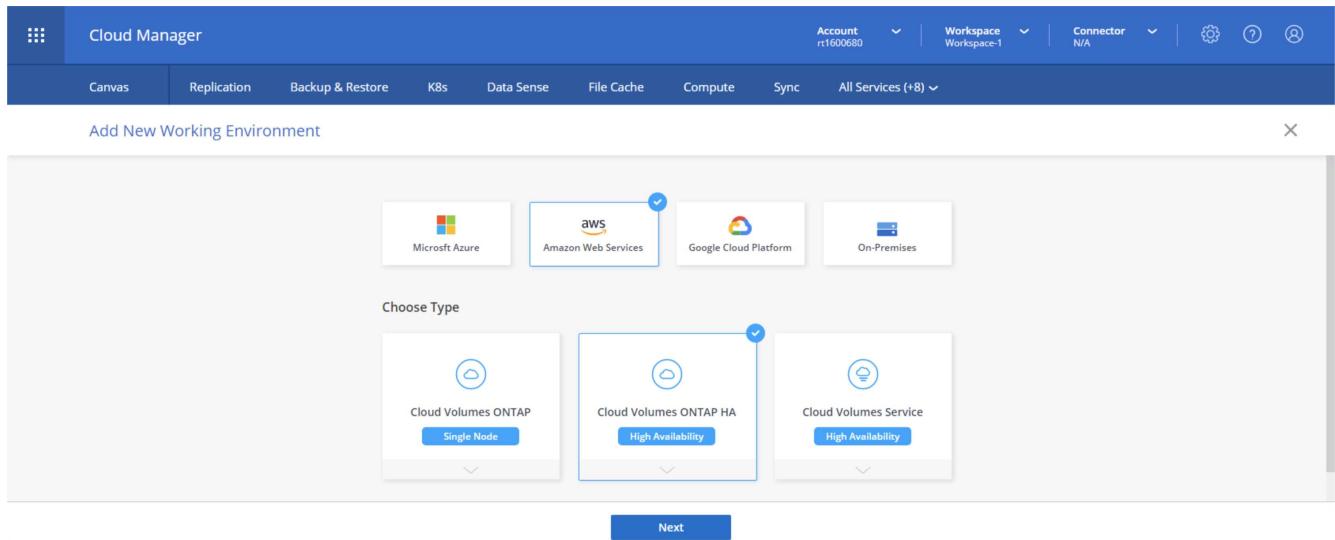
Don't have an account yet? [Sign Up](#)

[Forgot your password?](#)

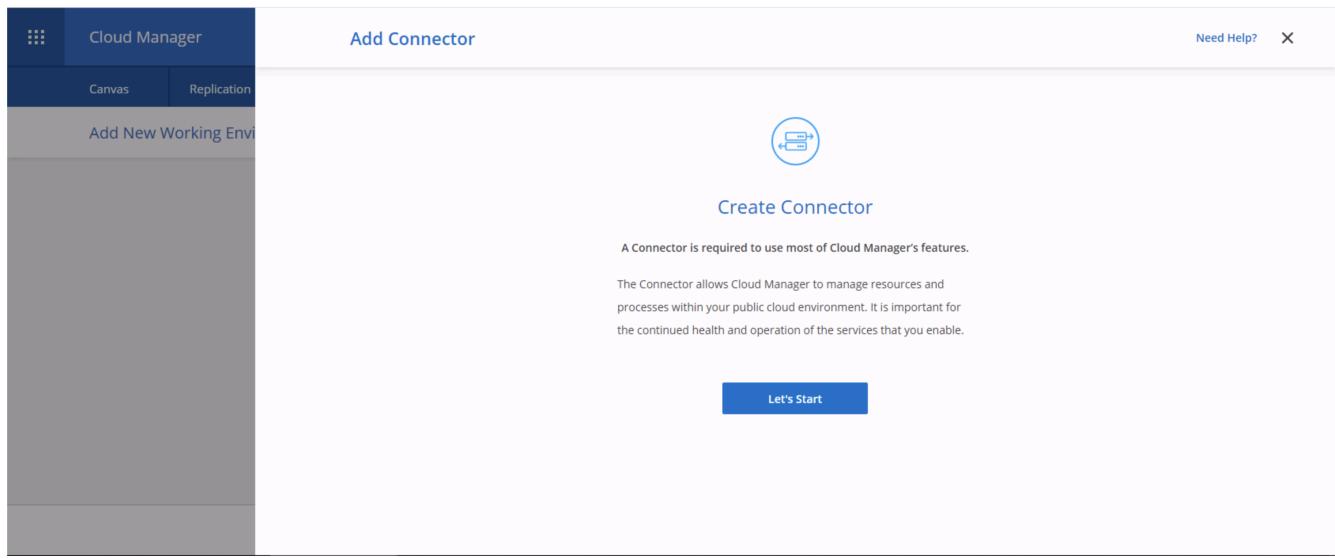
2. After you log in, you should be taken to the Canvas.



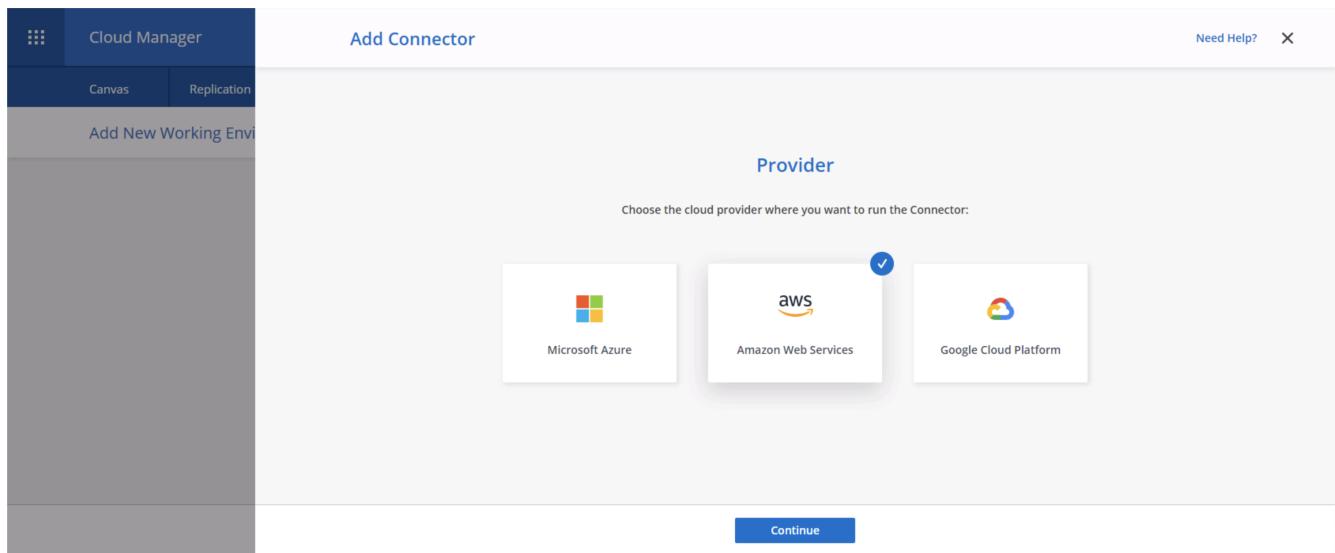
3. Click "Add Working Environment" and choose Cloud Volumes ONTAP in AWS. Here, you also choose whether you want to deploy a single node system or a high availability pair. I have chosen to deploy a high availability pair.



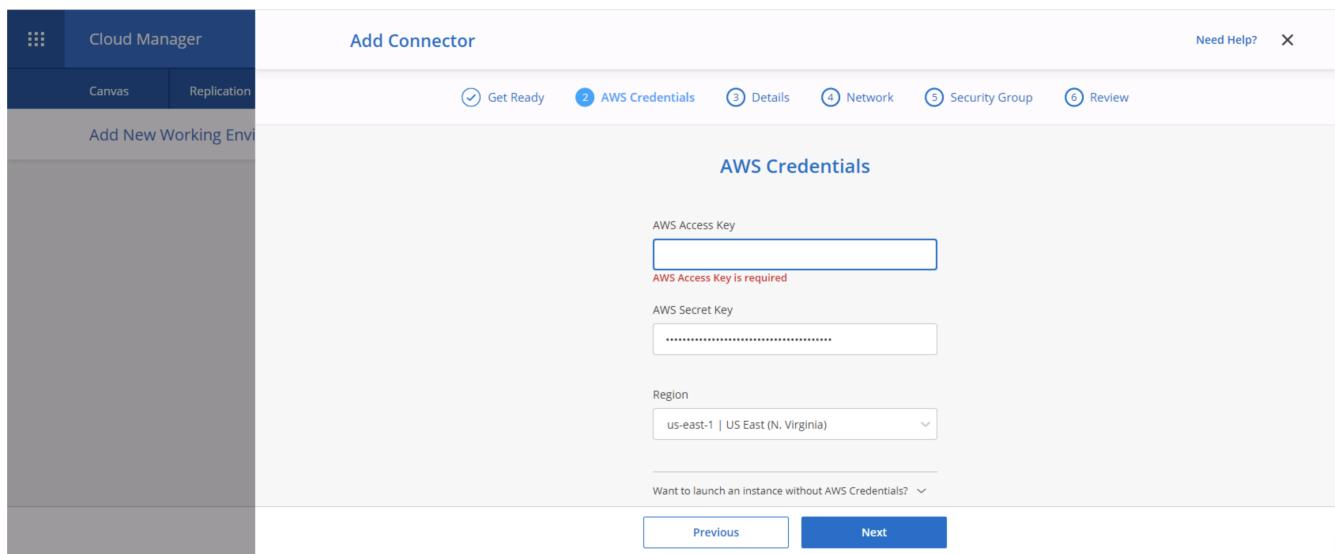
4. If no connector has been created, a pop-up appears asking you to create a connector.



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...

Key Pair: rt1600680

Public IP: Enable

Proxy Configuration (Optional)

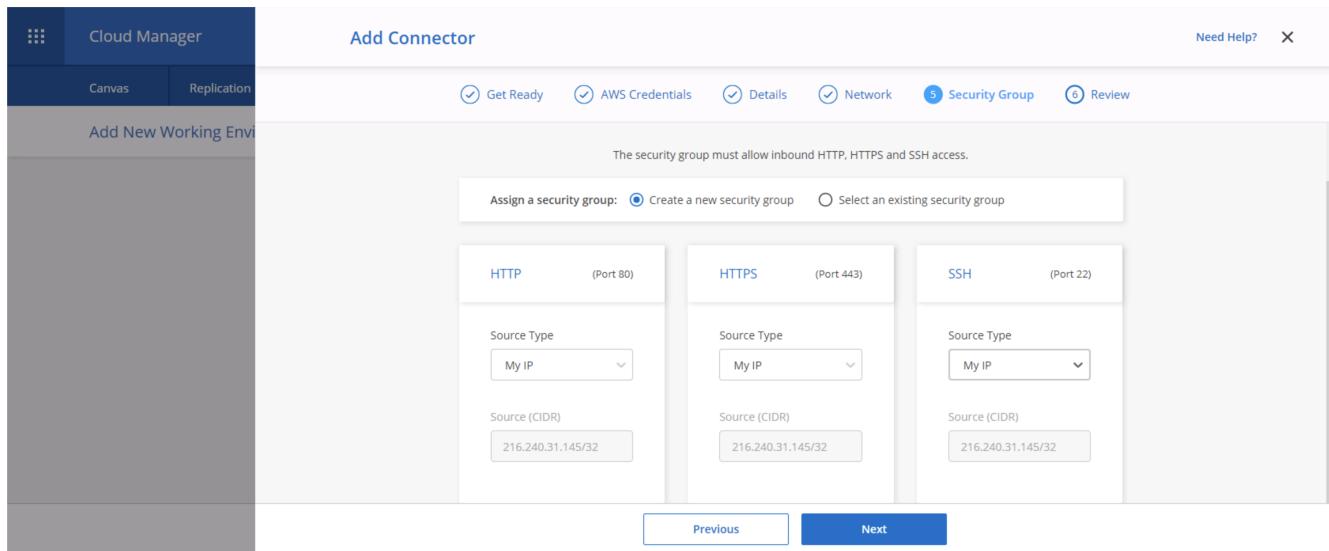
HTTP Proxy: Example: http://172.16.254.1:8080

Define Credentials for this Proxy

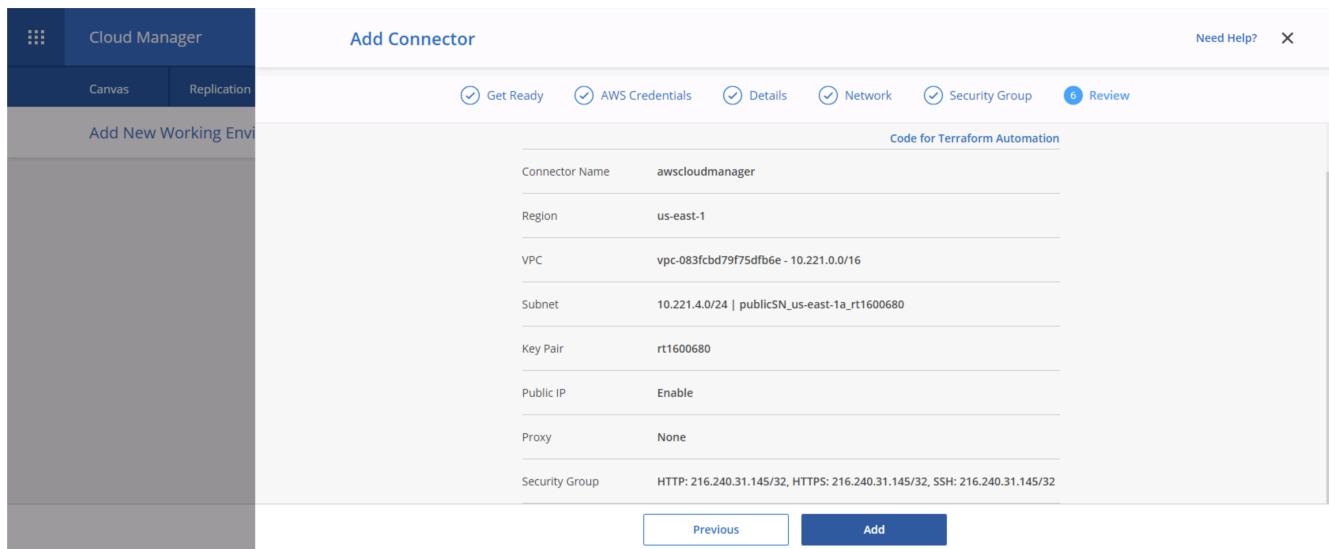
Upload a root certificate

Previous Next

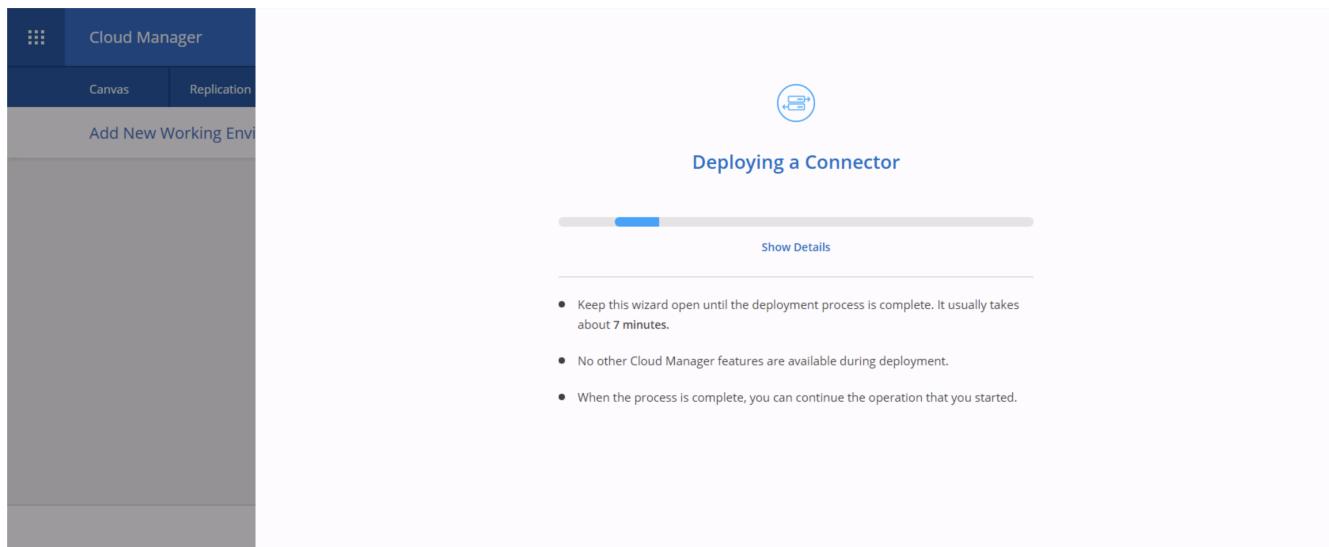
9. Provide communication with the connector via SSH, HTTP, and HTTPS by either providing a security group or creating a new security group. I have enabled access to the connector from my IP address only.



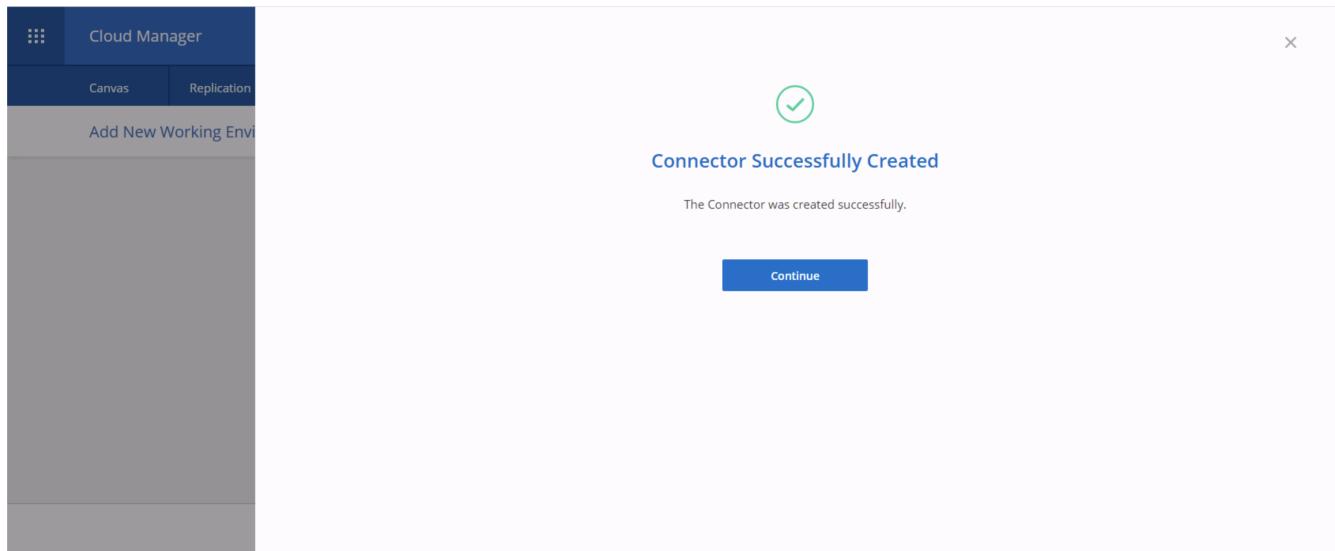
10. Review the information on the summary page and click Add to deploy the connector.



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

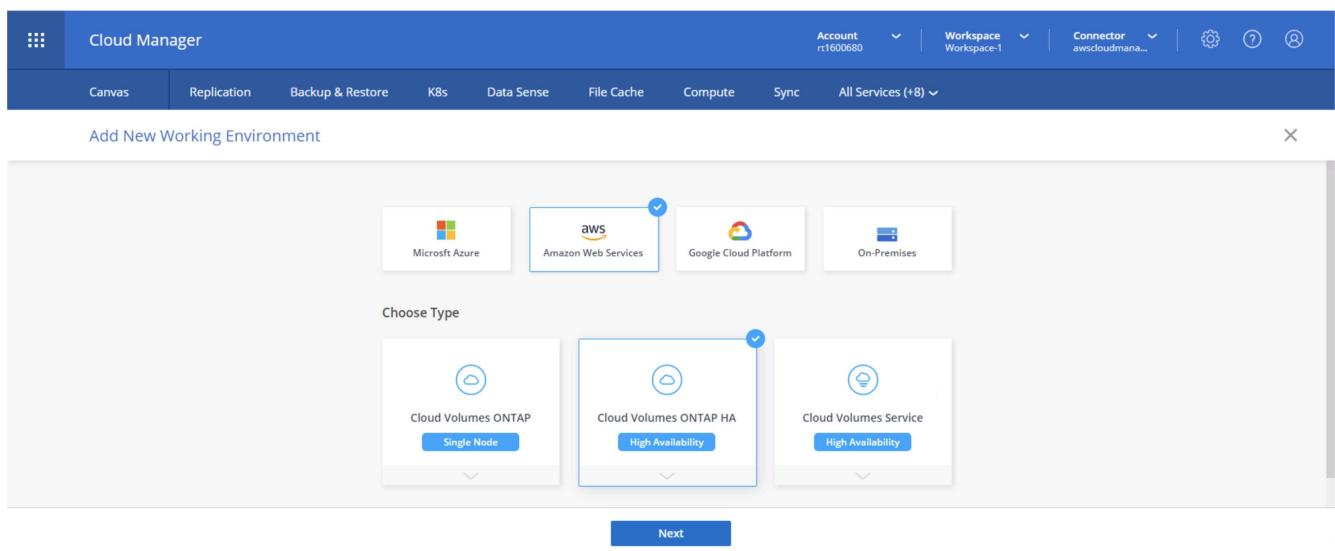


12. When the deployment is complete, a success page appears.



## 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.

Create a New Working Environment

Details and Credentials

↑ Previous Step      Instance Profile      Credential Name      Account ID      No subscription is associated      Marketplace Subscription      Edit Credentials

Details      Credentials

Working Environment Name (Cluster Name)      User Name  
Up to 40 characters      admin

Add Tags      Optional Field | Up to four tags      Password

Confirm Password

Continue

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

### 3. Choose Add Subscription.

Create a New Working Environment

Details and Credentials

↑ Previous Step      Instance Profile      Credential Name

Associate Subscription to Credentials ⓘ

Credentials      Instance Profile | Account ID: 322944748816

Marketplace Subscription      No subscription is associated with this credential

Add Subscription

Apply      Cancel

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

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

Create a New Working Environment

Edit Credentials & Add Subscription

Select a subscription option and click Continue. The AWS Marketplace enables you to view pricing details and then subscribe.

Pay-Per-TiB - Annual Contract  
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

Pay-as-you-go  
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 AWS Marketplace  
Subscribe and then click Set Up Your Account to configure your account.
- 2 Cloud Manager  
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue      Cancel

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

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

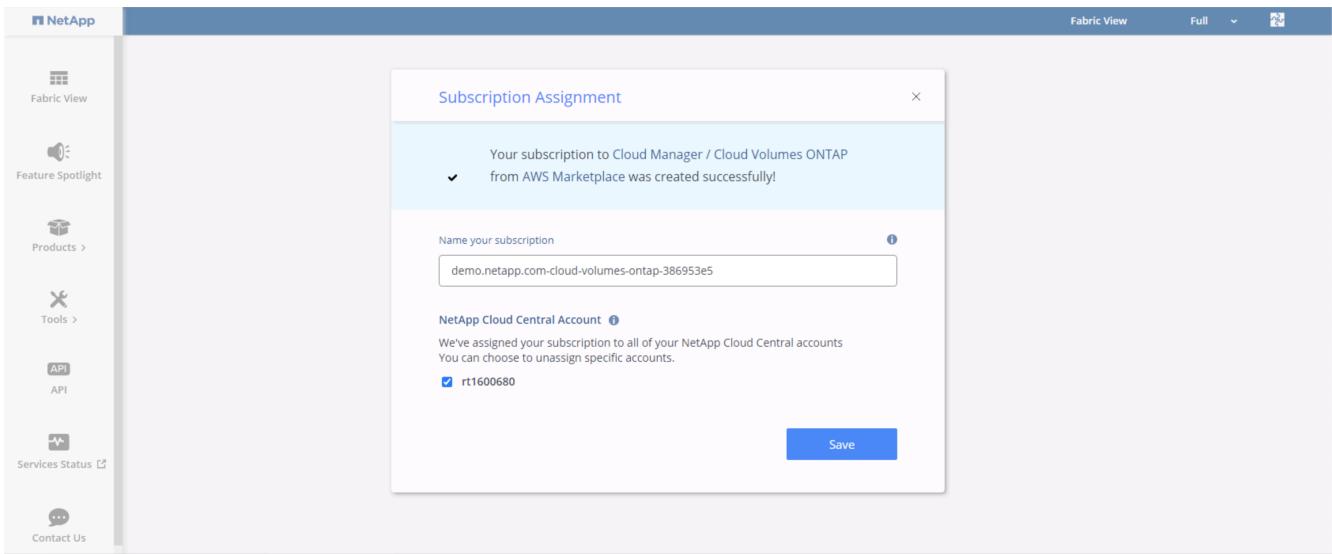
The screenshot shows the AWS Marketplace interface for the NetApp Cloud Manager product. The product title is 'Cloud Manager - Deploy & Manage NetApp Cloud Data Services'. It is sold by 'NetApp, Inc.'. Below the title, there is a brief description: 'Start here to deploy and manage Cloud Volumes ONTAP, Cloud Tiering, Cloud Data Sense, Cloud Backup and Cloud Volumes Service. Accelerate critical business apps with speed,' followed by a 'Show more' link. To the right of the description is a 'Continue to Subscribe' button and a 'Save to list' link. Below the main title, there are tabs for 'Overview', 'Pricing', 'Usage', 'Support', and 'Reviews'. The 'Overview' tab is selected. On the right side, there 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
- Enable your IT administrators to audit and track your cloud storage resource spend

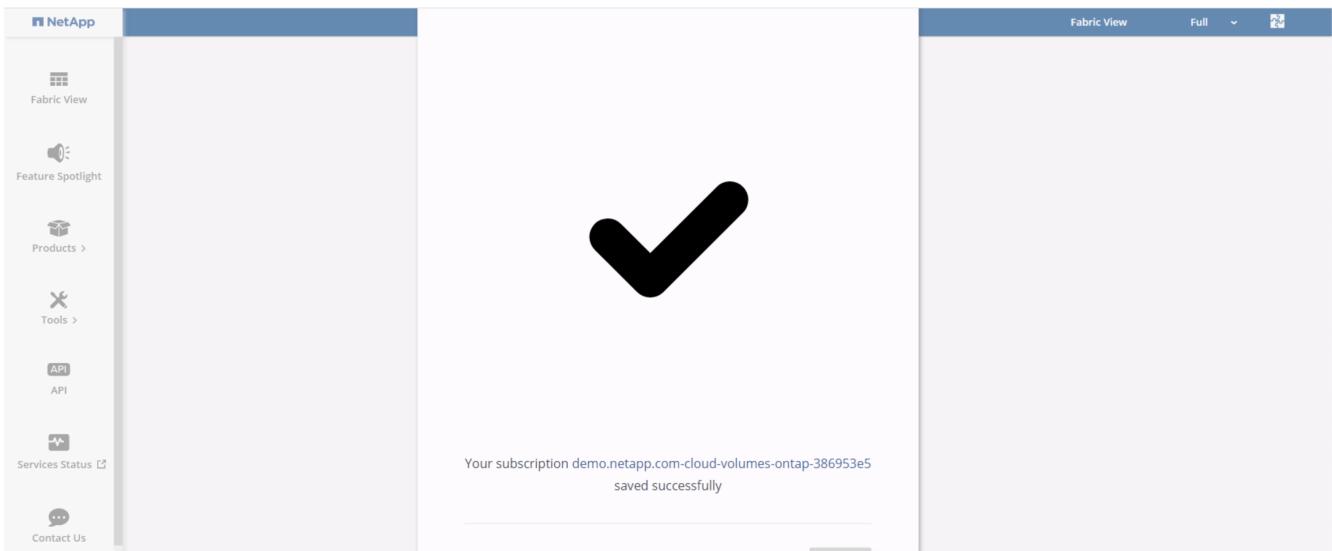
6. Subscribe and you are redirected back to NetApp Cloud Central. If you have already subscribed and don't get redirected, choose the "Click here" link.

The screenshot shows the AWS Marketplace confirmation page for the NetApp Cloud Manager subscription. It displays a message: 'You are extended multiple offers! Select an offer first and review the pricing information and EULA.' Below this, it shows the 'Offer name' as 'NetApp, Inc. for SaaS 2020-07-20- Private Offer - current subscription'. To the right, it says 'You are subscribed to this offer.' with details: 'By: NetApp, Inc.' and 'Offer ID: offer-hmolsqhv7ii'. It also notes that 'This offer is going to expire on August 1, 2022 UTC'. At the bottom, there is 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.'

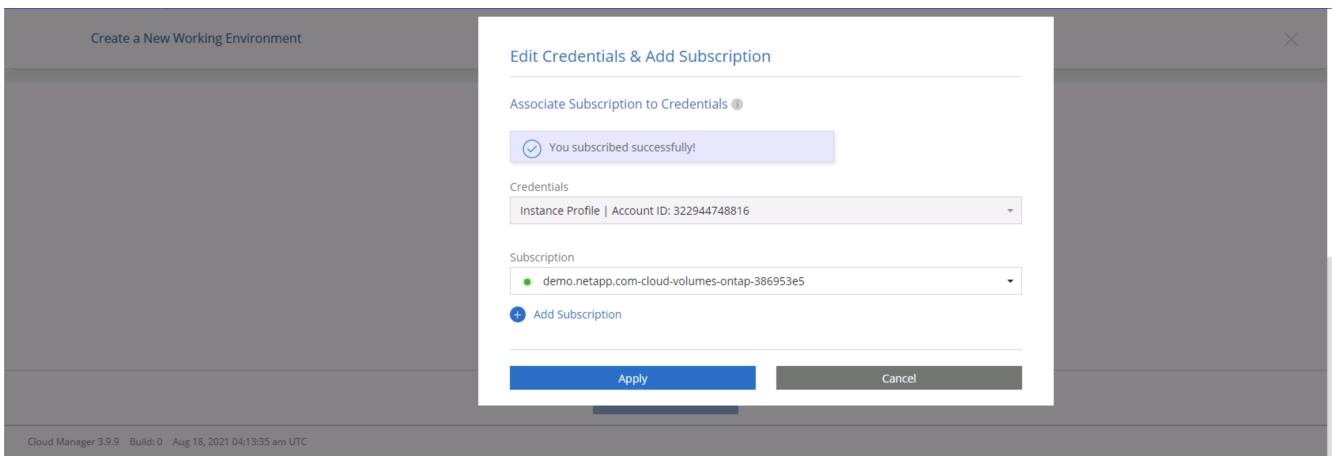
7. You are redirected to Cloud Central where you must name your subscription and assign it to your Cloud Central account.



- 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:

- 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 top navigation bar includes 'Account: rt1600680', 'Workspace: Workspace-1', 'Connector: awscloudman...', and various icons. Below the title, there's a 'Previous Step' link, an 'Instance Profile' section (322944748816), and a 'Details and Credentials' section. In the 'Details' tab, the 'Working Environment Name (Cluster Name)' is set to 'hybridawsco'. In the 'Credentials' tab, the 'User Name' is 'admin', 'Password' is '\*\*\*\*\*', and 'Confirm Password' is also '\*\*\*\*\*'. 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 top navigation bar includes 'Account: rt1600680', 'Workspace: Workspace-1', 'Connector: awscloudman...', and various icons. Below the title, there's a 'Previous Step' link and a 'Services' section. It lists three services: 'Data Sense & Compliance' (selected), 'Backup to Cloud' (selected), and 'Monitoring' (selected). Each service has a toggle switch and a dropdown arrow. 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.

The screenshot shows the Cloud Manager interface with the title "Cloud Manager" at the top. Below it is a navigation bar with tabs: Canvas, Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+8). The "Compute" tab is selected. The main content area has two sections: "Create a New Working Environment" and "HA Deployment Models". The "HA Deployment Models" section compares "Multiple Availability Zones" and "Single Availability Zone".

Multiple Availability Zones	Single Availability Zone
Provides maximum protection against AZ failures.	Protects against failures within a single AZ.
Enables selection of 3 availability zones.	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.	An HA node serves data if its partner goes offline.

At the bottom left, there is a note: "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.

The screenshot shows the Cloud Manager interface with the title "Cloud Manager" at the top. Below it is a navigation bar with tabs: Canvas, Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+8). The "Compute" tab is selected. The main content area has two sections: "Create a New Working Environment" and "Region & VPC".

In the "Region & VPC" section, there are three main fields:

- AWS Region: US East | N. Virginia
- VPC: vpc-083fcbd79f75dfb6e - 10.221.0.0/16
- Security group: Use a generated security group

Below these fields are three sub-sections for "Node 1", "Node 2", and "Mediator", each with "Availability Zone" and "Subnet" dropdowns. The "Subnet" dropdown for the "Mediator" section is highlighted with a blue selection bar.

At the bottom center is a "Continue" button.

At the very bottom left, there is a note: "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.

The screenshot shows the Cloud Manager interface with the title "Cloud Manager" at the top. Below it is a navigation bar with tabs: Canvas, Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+8). The "Compute" tab is selected. The main content area has two sections: "Create a New Working Environment" and "Connectivity & SSH Authentication".

In the "Connectivity & SSH Authentication" section, there are two main sections: "Nodes" and "Mediator".

**Nodes:** SSH Authentication Method is set to "Password".

**Mediator:**

- Security Group: Use a generated security group
- Key Pair Name: rt1600680
- Internet Connection Method: Public IP address

At the bottom center is a "Continue" button.

At the very bottom left, there is a note: "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 specifying floating IP addresses for cluster management, NFS/CIFS data, SVM management, and an optional floating IP address. A note explains that floating IPs can migrate between HA nodes if failures occur, and it's recommended to set up an AWS transit gateway. 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 available. 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.

Cloud Manager

Create a New Working Environment Create Volume

↑ Previous Step Details & Protection Protocol

Volume Name: Size (GB): Volume size

Snapshot Policy: default

Access Control: Custom export policy

Custom export policy: 10.221.0.0/16

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.

Cloud Manager

Create a New Working Environment Review & Approve

↑ Previous Step hybridawscvo Show API request

AWS | us-east-1 | HA

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. The main area displays two cloud icons: one for 'hybridawsenvo Cloud Volumes ONTAP' which is 'Initializing', and another for 'Amazon S3' showing 1 Bucket and 1 Region. To the right, a sidebar titled 'Working environments' lists 'Cloud Volumes ONTAP (High-Availability)' and 'Amazon S3'. A 'Go to Tabular View' button is at the top right.

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

The screenshot shows the Cloud Manager main dashboard. 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. Below the tabs, there are sections for 'Resources' and 'Services'. The 'Resources' section includes 'Canvas', 'Digital Wallet', and 'Timeline'. The 'Services' section includes 'Replication', 'Backup & Restore', 'K8s', 'Data Sense', 'Compliance', 'Tiering', 'Monitoring', 'File Cache', 'Compute', 'Sync', 'SnapCenter', and 'Active IQ'. A link to 'https://cloudmanager.netapp.com/timeline' is also present.

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 filters for Time, Service, Action, Agent, Resource, User, and Status, with 'Agent (1)' currently selected. The timeline table lists three 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. On the left, there's a 'Working environments' section with two clouds: one labeled 'Cloud Volumes ONTAP (High-Availability)' with '1 GiB Allocated Capacity' and another labeled 'Amazon S3' with '2 Buckets' and '1 Region'. On the right, there's a 'Working environments' panel with two entries:

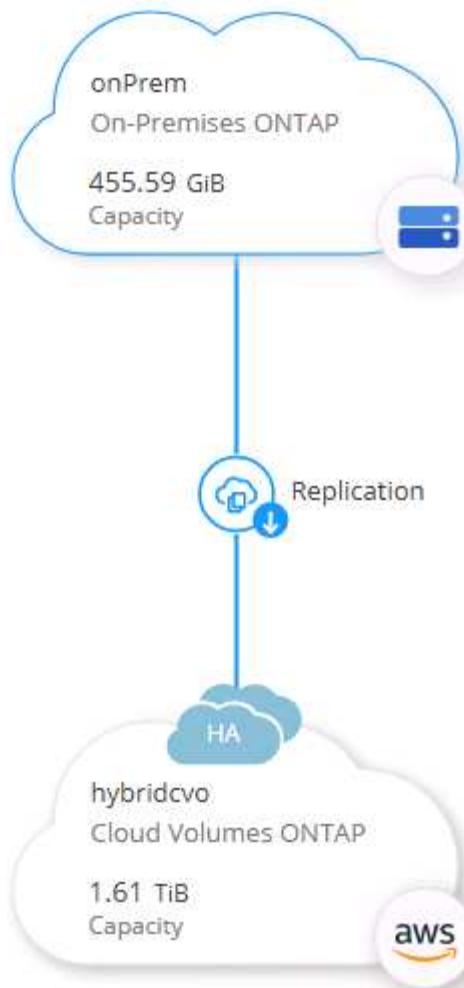
- 1 Cloud Volumes ONTAP (High-Availability)  
1 GiB Allocated Capacity
- 1 Amazon S3  
0 Buckets

## 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.



Or Options.

The screenshot shows the configuration of the 'onPrem' cluster. At the top, there's a circular icon with two servers, followed by the text 'onPrem' and a green square indicating 'On'. To the right are three blue circular icons with symbols for information, more options, and delete. Below this, the word 'DETAILS' is in bold. Under 'DETAILS', it says 'On-PremisesONTAP'. In the 'SERVICES' section, there's another server icon followed by 'Replication' and a green square 'On'. To its right, it shows '1 Replication Target' with a blue circular icon containing three dots. A horizontal line separates this from the 'Replicate.' section.

onPrem  
■ On

DETAILS

On-PremisesONTAP

SERVICES

Replication  
■ On

1 Replication Target

Replicate.

This screenshot is similar to the first one but includes a callout box over the 'Replication Target' 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.

onPrem  
■ On

DETAILS

On-PremisesONTAP

SERVICES

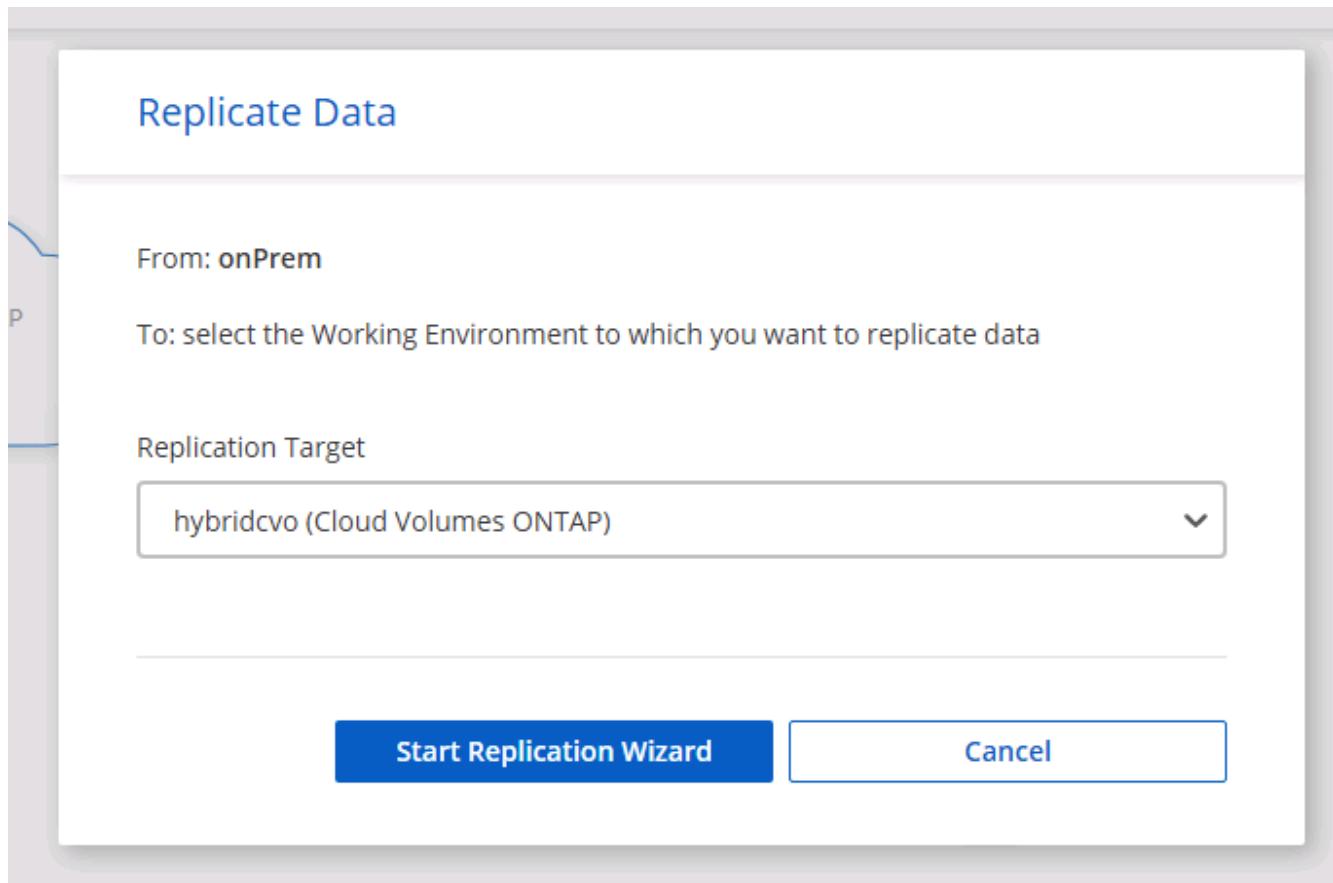
Replication  
■ On

1 Replication Target

View Replications

Replicate

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			
<b>rhel2_u03</b>	INFO Storage VM Name: <b>svm_onPrem</b> Tiering Policy: <b>None</b> Volume Type: <b>RW</b>	CAPACITY <b>100 GB Allocated</b> <b>7.29 GB Disk Used</b>	ONLINE	<b>rhel2_u0309232119421203118</b>	INFO Storage VM Name: <b>svm_onPrem</b> Tiering Policy: <b>None</b> Volume Type: <b>RW</b>	CAPACITY <b>100 GB Allocated</b> <b>35.83 MB Disk Used</b>	ONLINE
<b>sql1_data</b>	INFO Storage VM Name: <b>svm_onPrem</b> Tiering Policy: <b>None</b> Volume Type: <b>RW</b>	CAPACITY <b>53.37 GB Allocated</b> <b>45.09 GB Disk Used</b>	ONLINE	<b>sql1_log</b>	INFO Storage VM Name: <b>svm_onPrem</b> Tiering Policy: <b>None</b> Volume Type: <b>RW</b>	CAPACITY <b>21.35 GB Allocated</b> <b>18.16 GB Disk Used</b>	ONLINE
<b>sql1_snapctr</b>	INFO Storage VM Name: <b>svm_onPrem</b> Tiering Policy: <b>None</b> Volume Type: <b>RW</b>	CAPACITY <b>24.87 GB Allocated</b> <b>21.23 GB Disk Used</b>	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:

100

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

#### Mirror

Typically used for disaster recovery

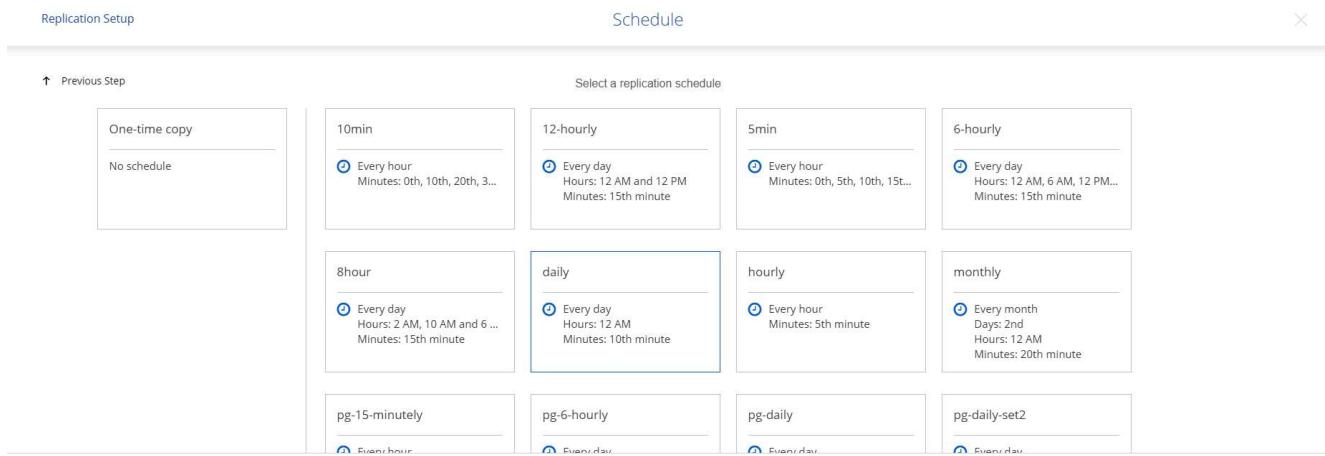
[More info](#)

#### Mirror and Backup (1 month retention)

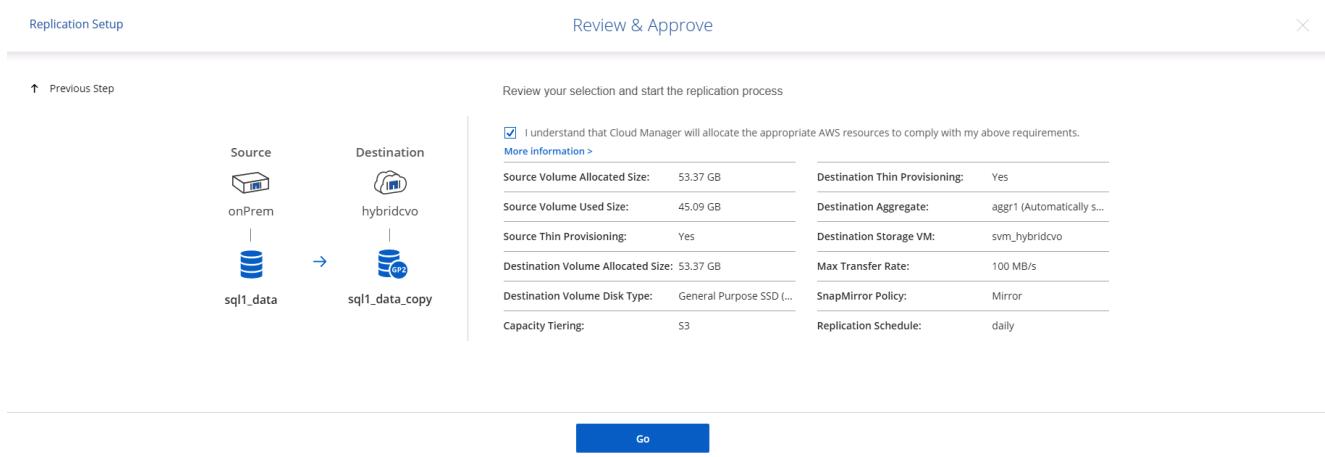
Configures disaster recovery and long-term retention of backups on the same destination volume

[More info](#)

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
<span>✓</span>	rhel2_u01 onPrem	rhel2_u01_dr hybridcvo	43 minutes 43 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:50 AM 19.73 MiB
<span>✓</span>	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
<span>✓</span>	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
<span>✓</span>	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
<span>✓</span>	rhel2_u04 onPrem	rhel2_u04_dr hybridcvo	1 hour 1 minute 40 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:30 AM 24.56 KiB
<span>✓</span>	rhel2_u05 onPrem	rhel2_u05_dr hybridcvo	1 hour 1 minute 40 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:30 AM 24.56 KiB
<span>✓</span>	rhel2_u06 onPrem	rhel2_u06_dr hybridcvo	1 hour 1 minute 40 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:30 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](#).

## **Workflow for dev/test bursting to cloud**

Previous: [Getting Started with AWS public cloud](#).

The agility of the public cloud, the time to value, and the cost savings are all meaningful value propositions for enterprises adopting the public cloud for database application development and testing effort. There is no better tool than SnapCenter to make this a reality. SnapCenter can not only protect your production database on-premises, but can also quickly clone a copy for application development or code testing in the public cloud while consuming very little extra storage. Following are details of the step-by-step processes for using this tool.

## Clone an Oracle Database for dev/test from a replicated snapshot backup

1. Log into SnapCenter with a database management user ID for Oracle. Navigate to the Resources tab, which shows the Oracle databases being protected by SnapCenter.

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com	rhel2_cdb2 rhel2_cdb2_log	Oracle Archive Log Backup Oracle Full Online Backup	09/17/2021 3:00:09 PM	Backup succeeded

2. Click the intended on-premises database name for the backup topology and the detailed view. If a secondary replicated location is enabled, it shows linked mirror backups.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log	09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_09-17-2021_14.35.01.4997_1	1	Log	09/17/2021 2:35:21 PM	Not Applicable	False	Not Cataloged	5980629
rhel2_cdb2_09-17-2021_14.35.01.4997_0	1	Data	09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log	09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388
rhel2_cdb2_log_09-17-2021_13.00.01.7389_1	1	Log	09/17/2021 1:00:11 PM	Not Applicable	False	Not Cataloged	5971535
rhel2_cdb2_log_09-17-2021_12.00.01.1142_1	1	Log	09/17/2021 12:00:10 PM	Not Applicable	False	Not Cataloged	5971773
rhel2_cdb2_log_09-17-2021_11.00.01.0895_1	1	Log	09/17/2021 11:00:10 AM	Not	False	Not Cataloged	5968474

3. Toggled to the mirrored backups view by clicking mirrored backups. The secondary mirror backup(s) is then displayed.

NetApp SnapCenter®

Oracle Database ▾

Search databases

cdb2 Topology

Manage Copies

Local copies

Mirror copies

Summary Card

368 Backups

16 Data Backups

352 Log Backups

0 Clones

Backup Name

	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log		09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5980203
rhel2_cdb2_09-17-2021_14.35.01.4997_1	1	Log		09/17/2021 2:35:21 PM	Not Applicable	False	Not Cataloged	5980629
rhel2_cdb2_09-17-2021_14.35.01.4997_0	1	Data		09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log		09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388
rhel2_cdb2_log_09-17-2021_13.00.01.7389_1	1	Log		09/17/2021 1:00:11 PM	Not Applicable	False	Not Cataloged	5975135
rhel2_cdb2_log_09-17-2021_12.00.01.1142_1	1	Log		09/17/2021 12:00:10 PM	Not Applicable	False	Not Cataloged	5971773
rhel2_cdb2_log_09-17-2021_11.00.01.0895_1	1	Log		09/17/2021 11:00:10 AM	Not Applicable	False	Not Cataloged	5968474

Total 1

- Choose a mirrored secondary database backup copy to be cloned and determine a recovery point either by time and system change number or by SCN. Generally, the recovery point should be trailing the full database backup time or SCN to be cloned. After a recovery point is decided, the required log file backup must be mounted for recovery. The log file backup should be mounted to target DB server where the clone database is to be hosted.

Mount backups

Choose the host to mount the backup : ora-standby.demo.netapp.com

Mount path : /var/opt/snapcenter/sco/backup\_mount/rhel2\_cdb2\_09-17-2021\_14.35.01.4997\_1/cdb2

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:rhel2_u03	svm_hybridcvo:rhel2_u03_dr

Mount Cancel

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_16.00.01.2156_1	1	Log	09/17/2021 4:00:10 PM	Not Applicable	False	Not Cataloged	5985272
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log	09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_09-17-2021_14.35.01.4997_1	1	Log	09/17/2021 2:35:21 PM	Not Applicable	True	Not Cataloged	5980629
rhel2_cdb2_09-17-2021_14.35.01.4997_0	1	Data	09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log	09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388



If log pruning is enabled and the recovery point is extended beyond the last log pruning, multiple archive log backups might need to be mounted.

5. Highlight the full database backup copy to be cloned, and then click the clone button to start the DB clone Workflow.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_16.00.01.2156_1	1	Log	09/17/2021 4:00:10 PM	Not Applicable	False	Not Cataloged	5985272
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log	09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_09-17-2021_14.35.01.4997_1	1	Log	09/17/2021 2:35:21 PM	Not Applicable	True	Not Cataloged	5980629
rhel2_cdb2_09-17-2021_14.35.01.4997_0	1	Data	09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log	09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388

6. Choose a proper clone DB SID for a complete container database or CDB clone.

Clone from cdb2

**1 Name**

Complete Database Clone

Clone SID: cdb2test

Exclude PDBs: Type to find PDBs

PDB Clone

Secondary storage location : Snap Vault / Snap Mirror

**Data**

Source Volume	Destination Volume
svm_onPrem:rhel2_u02	svm_hybridcvo:rhel2_u02_dr

**Logs**

Source Volume	Destination Volume
svm_onPrem:rhel2_u03	svm_hybridcvo:rhel2_u03_dr

[Previous](#) [Next](#)

7. Select the target clone host in the cloud, and datafile, control file, and redo log directories are created by the clone workflow.

Clone from cdb2

**1 Name**

Select the host to create a clone

Clone host

**2 Locations**

**3 Credentials**

**4 PreOps**

**5 PostOps**

**6 Notification**

**7 Summary**

**④ Datafile locations**

/u02\_cdb2test

**⑤ Control files**

/u02\_cdb2test/cdb2test/control/control01.ctl  
/u02\_cdb2test/cdb2test/control/control02.ctl

**⑥ Redo logs**

Group	Size	Unit	Number of files
RedoGroup 1	200	MB	1
/u02_cdb2test/cdb2test/redolog redo03.log			
RedoGroup 2	200	MB	1

- The None credential name is used for OS-based authentication, which renders the database port irrelevant. Fill in the proper Oracle Home, Oracle OS User, and Oracle OS Group as configured in the target clone DB server.

Clone from cdb2

**1 Name**

**2 Locations**

**3 Credentials**

**4 PreOps**

**5 PostOps**

**6 Notification**

**7 Summary**

Database Credentials for the clone

Credential name for sys user  + ?

Database port

Oracle Home Settings ?

Oracle Home

Oracle OS User

Oracle OS Group

Previous Next

The screenshot shows the Oracle Database Clone wizard interface. The left sidebar lists steps 1 through 7. Step 3, 'Credentials', is currently selected and highlighted in blue. The main panel shows 'Database Credentials for the clone' with a dropdown for 'Credential name for sys user' set to 'None'. Below it, the 'Database port' is set to '1521'. Under 'Oracle Home Settings', the 'Oracle Home' path is specified as '/u01/app/oracle/product/19800/cdb2'. The 'Oracle OS User' is 'oracle' and the 'Oracle OS Group' is 'oinstall'. At the bottom right, there are 'Previous' and 'Next' buttons.

9. Specify the scripts to run before clone operation. More importantly, the database instance parameter can be adjusted or defined here.

Clone from cdb2

**Specify scripts to run before clone operation**

Prescript full path	/var/opt/snapcenter/spl/scripts/	Enter Prescript path
Arguments		
Script timeout	60	secs

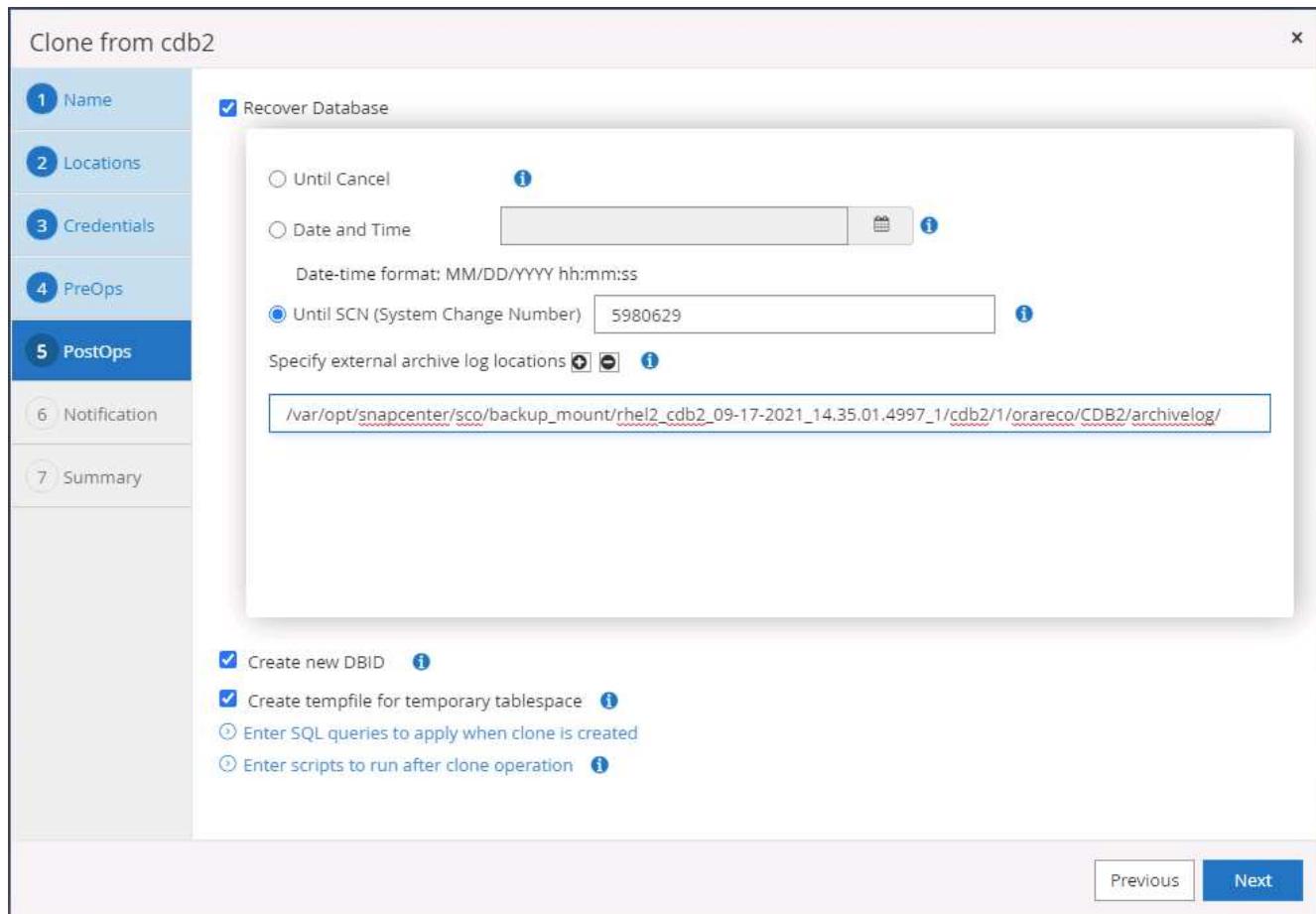
**Database Parameter settings**

processes	320	X
remote_login_passwordfile	EXCLUSIVE	X
sga_target	4311744512	X
undo_tablespace	UNDOTBS1	X

**Buttons:**

- Previous
- Next

- Specify the recovery point either by the date and time or SCN. Until Cancel recovers the database up to the available archive logs. Specify the external archive log location from the target host where the archive log volume is mounted. If target server Oracle owner is different from the on-premises production server, verify that the archive log directory is readable by the target server Oracle owner.



```
oracle@ora-standby:~$ ls /var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_09-17-2021_14.35.01.4997_1/cdb2/1/orareco/CDB2/archivelog/
2021_08_26 2021_08_28 2021_08_30 2021_09_01 2021_09_03 2021_09_05 2021_09_07 2021_09_09 2021_09_11 2021_09_13 2021_09_15 2021_09_17
2021_08_27 2021_08_29 2021_08_31 2021_09_02 2021_09_04 2021_09_06 2021_09_08 2021_09_10 2021_09_12 2021_09_14 2021_09_16
[oracle@ora-standby:~]$
```

11. Configure the SMTP server for email notification if desired.

Clone from cdb2

**Provide email settings i**

Email preference	Never
From	From email
To	Email to
Subject	Notification

Attach job report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

[Previous](#) [Next](#)

1. Name  
2. Locations  
3. Credentials  
4. PreOps  
5. PostOps  
**6. Notification**  
7. Summary

12. Clone summary.

Clone from cdb2

<b>1 Name</b>	Summary
<b>2 Locations</b>	Clone from backup      rhel2_cdb2_09-17-2021_14.35.01.4997_0
<b>3 Credentials</b>	Clone SID      cdb2test
<b>4 PreOps</b>	Clone server      ora-standby.demo.netapp.com
<b>5 PostOps</b>	Exclude PDBs      none
<b>6 Notification</b>	Oracle home      /u01/app/oracle/product/19800/cdb2
<b>7 Summary</b>	Oracle OS user      oracle Oracle OS group      oinstall Datafile mountpaths      /u02_cdb2test Control files      /u02_cdb2test/cdb2test/control/control01.ctl /u02_cdb2test/cdb2test/control/control02.ctl Redo groups      RedoGroup =1 TotalSize =200 Path =/u02_cdb2test/cdb2test/redolog redo03.log RedoGroup =2 TotalSize =200 Path =/u02_cdb2test/cdb2test/redolog redo02.log RedoGroup =3 TotalSize =200 Path =/u02_cdb2test/cdb2test/redolog redo01.log Recovery scope      Until SCN 5980629 Prescript full path      none Prescript arguments Postscript full path      none Postscript arguments
	<a href="#">Previous</a> <a href="#" style="background-color: blue; color: white; padding: 5px;">Finish</a>

13. You should validate after cloning to make sure that the cloned database is operational. Some additional tasks, such as starting up the listener or turning off the DB log archive mode, can be performed on the dev/test database.

```
oracle@ora-standby:/tmp
[oracle@ora-standby tmp]$ export ORACLE_SID=cdb2test
[oracle@ora-standby tmp]$ export ORACLE_HOME=/u01/app/oracle/product/19800/cdb2
[oracle@ora-standby tmp]$ export PATH=$PATH:$ORACLE_HOME/bin
[oracle@ora-standby tmp]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Sep 17 17:49:29 2021
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> select name, log_mode from v$database;
NAME      LOG MODE
-----
CDB2TEST  ARCHIVELOG

SQL> select instance_name, host_name from v$instance;
INSTANCE_NAME
-----
HOST NAME
-----
cdb2test
ora-standby.demo.netapp.com

SQL> show pdbs
CON_ID CON_NAME          OPEN MODE RESTRICTED
----- -----
  2 PDB$SEED        READ ONLY NO
  3 CDB2_PDB1       READ WRITE NO
  4 CDB2_PDB2       READ WRITE NO
  5 CDB2_PDB3       READ WRITE NO

SQL>
```

## Clone a SQL database for dev/test from a replicated Snapshot backup

1. Log into SnapCenter with a database management user ID for SQL Server. Navigate to the Resources tab, which shows the SQL Server user databases being protected by SnapCenter and a target standby SQL instance in the public cloud.

Name	Instance	Host	Last Backup	Overall Status	Type
master	sql1	sql1.demo.netapp.com		Not available for backup	System database
model	sql1	sql1.demo.netapp.com		Not available for backup	System database
msdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tempdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tpcc	sql1	sql1.demo.netapp.com	09/16/2021 7:35:05 PM	Backup succeeded	User database
master	sql1-standby	sql1-standby.demo.netapp.com		Not available for backup	System database
model	sql1-standby	sql1-standby.demo.netapp.com		Not available for backup	System database
msdb	sql1-standby	sql1-standby.demo.netapp.com		Not available for backup	System database
tempdb	sql1-standby	sql1-standby.demo.netapp.com		Not available for backup	System database

2. Click on the intended on-premises SQL Server user database name for the backups topology and detailed view. If a secondary replicated location is enabled, it shows linked mirror backups.

Backup Name	Count	Type	End Date	Verified
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup	09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-15-2021_18.25.01.4604	1	Full backup	09/15/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup	09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup	09/13/2021 6:25:05 PM	Unverified
sql1_tpcc_09-12-2021_18.25.01.4016	1	Full backup	09/12/2021 6:25:05 PM	Unverified
sql1_tpcc_09-11-2021_18.25.01.3753	1	Full backup	09/11/2021 6:25:05 PM	Unverified
sql1_tpcc_09-10-2021_18.36.25.5430	1	Full backup	09/10/2021 6:36:29 PM	Unverified

3. Toggle to the Mirrored Backups view by clicking Mirrored Backups. Secondary Mirror Backup(s) are then displayed. Because SnapCenter backs up the SQL Server transaction log to a dedicated drive for recovery, only full database backups are displayed here.

Backup Name	Count	Type	End Date	Verified
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup	09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-15-2021_18.25.01.4604	1	Full backup	09/15/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup	09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup	09/13/2021 6:25:05 PM	Unverified
sql1_tpcc_09-12-2021_18.25.01.4016	1	Full backup	09/12/2021 6:25:05 PM	Unverified
sql1_tpcc_09-11-2021_18.25.01.3753	1	Full backup	09/11/2021 6:25:05 PM	Unverified
sql1_tpcc_09-10-2021_18.36.25.5430	1	Full backup	09/10/2021 6:36:29 PM	Unverified

4. Choose a backup copy, and then click the Clone button to launch the Clone from Backup workflow.

The screenshot shows the NetApp SnapCenter interface for a Microsoft SQL Server topology named 'tpcc (sql1)'. On the left, a sidebar lists databases: master, model, msdb, tempdb, tpcc, and tpcc\_clone. The 'tpcc' database is selected. The main pane displays 'Manage Copies' with a summary: 7 Backups, 0 Clones, and 1 Clone under 'Local copies'. Below this, a section for 'Secondary Mirror Backup(s)' shows a search bar and a table of backup entries. The table has columns: Backup Name, Count, Type, End Date, and Verified. The first backup entry is highlighted in blue.

Backup Name	Count	Type	End Date	Verified
sql1_tpcc_09-19-2021_18.25.01.4134	1	Full backup	09/19/2021 6:25:05 PM	Unverified
sql1_tpcc_09-18-2021_18.25.01.3963	1	Full backup	09/18/2021 6:25:05 PM	Unverified
<b>sql1_tpcc_09-17-2021_18.25.01.4218</b>	<b>1</b>	<b>Full backup</b>	<b>09/17/2021 6:25:05 PM</b>	<b>Unverified</b>
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup	09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-15-2021_18.25.01.4604	1	Full backup	09/15/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup	09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup	09/13/2021 6:25:05 PM	Unverified

The screenshot shows the 'Clone from backup' wizard, Step 1: Clone Options. The left sidebar lists steps: 1. Clone Options (selected), 2. Logs, 3. Script, 4. Notification, and 5. Summary. The main area is titled 'Clone settings' and includes fields for 'Clone server' (Choose), 'Clone instance' (Nothing selected), and 'Clone name' (tpcc). Below this, a section titled 'Choose mount option' offers two choices: 'Auto assign mount point' (selected) and 'Auto assign volume mount point under path' (full file path). The next section, 'Secondary storage location : Snap Vault / Snap Mirror', shows mappings between source volumes (svm\_onPrem:sql1\_data and svm\_onPrem:sql1\_log) and destination volumes (svm\_hybridcvo:sql1\_data\_dr and svm\_hybridcvo:sql1\_log\_dr). At the bottom are 'Previous' and 'Next' buttons.

5. Select a cloud server as the target clone server, clone instance name, and clone database name. Choose either an auto-assign mount point or a user-defined mount point path.

Clone from backup x

**1 Clone Options**

**Clone settings**

Clone server	sql-standby.demo.netapp.com	<span style="color: blue;">i</span>
Clone instance	sql-standby	<span style="color: blue;">i</span>
Clone name	tpcc_clone	

Choose mount option

Auto assign mount point i

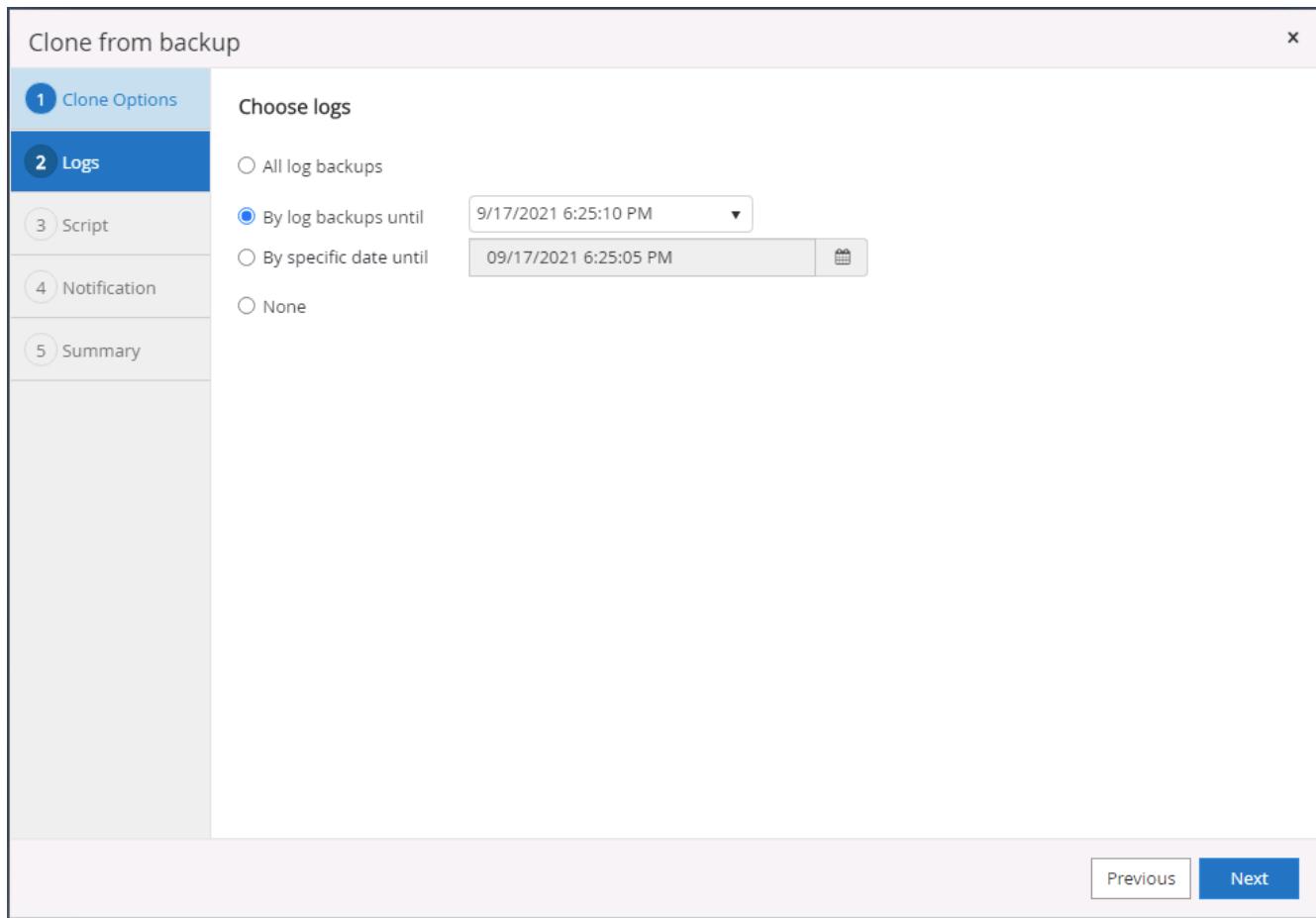
Auto assign volume mount point under path full file path i

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcvo:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcvo:sql1_log_dr

Previous Next

6. Determine a recovery point either by a log backup time or by a specific date and time.



7. Specify optional scripts to run before and after the cloning operation.

Clone from backup

X

1 Clone Options

2 Logs

**3 Script**

4 Notification

5 Summary

Specify optional scripts to run before and after performing a clone from backup job

Prescript full path

Prescript arguments  Choose optional arguments...

Postscript full path

Postscript arguments  Choose optional arguments...

Script timeout  60 secs

Previous **Next**

This screenshot shows the 'Clone from backup' configuration interface. The 'Script' tab is active, allowing users to specify optional scripts to run before and after the clone operation. Fields include Prescript and Postscript full paths, their respective argument inputs, and a script timeout set to 60 seconds.

8. Configure an SMTP server if email notification is desired.

Clone from backup X

**1 Clone Options**

**2 Logs**

**3 Script**

**4 Notification**

**5 Summary**

Provide email settings i

Email preference	Never
From	From email
To	Email to
Subject	Notification

Attach Job Report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server. X

Previous Next

## 9. Clone Summary.

Clone from backup

**1 Clone Options**

**2 Logs**

**3 Script**

**4 Notification**

**5 Summary**

Summary	
Clone server	sql-standby.demo.netapp.com
Clone instance	sql-standby
Clone name	tpcc_dev
Mount option	Auto assign volume mount point under custom path
Prescript full path	None
Prescript arguments	
Postscript full path	None
Postscript arguments	
Send email	No

[Previous](#) [Finish](#)

- Monitor the job status and validate that the intended user database has been attached to a target SQL instance in the cloud clone server.

Jobs - Filter					
ID	Status	Name	Start date	End date	Owner
766	✓	Clone from backup 'sql1_tpcc_09-16-2021_18:25:01.4024'	09/16/2021 8:05:25 PM	09/16/2021 8:06:17 PM	demo\sqldba
763	✓	Discover resources for all hosts	09/16/2021 7:56:49 PM	09/16/2021 7:56:54 PM	demo\sqldba
761	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 7:59:00 PM	09/16/2021 7:57:08 PM	demo\sqldba
760	⚠	Discover resources for all hosts	09/16/2021 7:19:05 PM	09/16/2021 7:19:09 PM	demo\sqldba
759	⚠	Discover resources for all hosts	09/16/2021 7:18:43 PM	09/16/2021 7:18:48 PM	demo\sqldba
756	⚠	Discover resources for all hosts	09/16/2021 6:59:51 PM	09/16/2021 6:59:56 PM	demo\sqldba
753	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 6:35:00 PM	09/16/2021 6:37:07 PM	demo\sqldba
750	✓	Backup of Resource Group 'sql1_tpcc' with policy 'SQL Server Full Backup'	09/16/2021 6:25:01 PM	09/16/2021 6:27:14 PM	demo\sqldba
749	✓	Discover resources for host 'sql-standby.demo.netapp.com'	09/16/2021 6:19:00 PM	09/16/2021 6:19:05 PM	Demo\administrator
745	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 5:35:00 PM	09/16/2021 5:37:08 PM	demo\sqldba

## Post-clone configuration

- An Oracle production database on-premises is usually running in log archive mode. This mode is not necessary for a development or test database. To turn off log archive mode, log into the Oracle DB as sysdba, execute a log mode change command, and start the database for access.
- Configure an Oracle listener, or register the newly cloned DB with an existing listener for user access.
- For SQL Server, change the log mode from Full to Easy so that the SQL Server dev/test log file can be readily shrunk when it is filling up the log volume.

## Refresh clone database

1. Drop cloned databases and clean up the cloud DB server environment. Then follow the previous procedures to clone a new DB with fresh data. It only takes few minutes to clone a new database.
2. Shutdown the clone database, run a clone refresh command by using the CLI. See the following SnapCenter documentation for details: [Refresh a clone](#).

## Where to go for help?

If you need help with this solution and use cases, join the [NetApp Solution Automation community support Slack channel](#) and look for the solution-automation channel to post your questions or inquires.

Next: [Disaster recovery workflow](#).

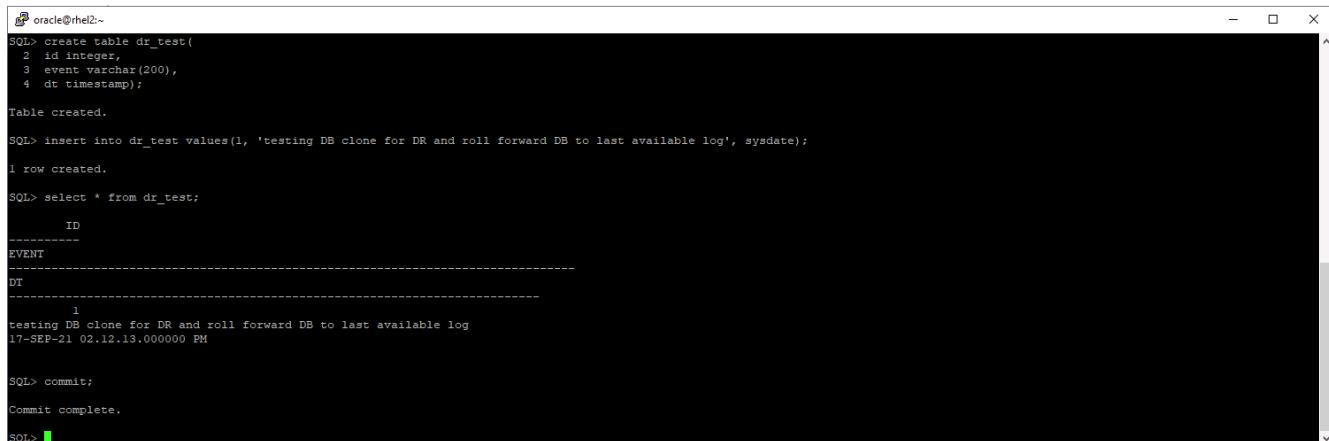
## Disaster recovery workflow

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

Enterprises have embraced the public cloud as a viable resource and destination for disaster recovery. SnapCenter makes this process as seamless as possible. This disaster recovery workflow is very similar to the clone workflow, but database recovery runs through the last available log that was replicated to cloud to recover all the business transactions possible. However, there are additional pre-configuration and post-configuration steps specific to disaster recovery.

### Clone an on-premises Oracle production DB to cloud for DR

1. To validate that the clone recovery runs through last available log, we created a small test table and inserted a row. The test data would be recovered after a full recovery to last available log.



```
oracle@rhel2:~$ SQL> create table dr_test(
  2  id integer,
  3  event varchar(200),
  4  dt timestamp);
Table created.

SQL> insert into dr_test values(1, 'testing DB clone for DR and roll forward DB to last available log', sysdate);
1 row created.

SQL> select * from dr_test;
      ID
-----
EVENT
-----
DT
-----
1
testing DB clone for DR and roll forward DB to last available log
17-SEP-21 02.12.13.000000 PM

SQL> commit;
Commit complete.

SQL>
```

2. Log into SnapCenter as a database management user ID for Oracle. Navigate to the Resources tab, which shows the Oracle databases being protected by SnapCenter.

The screenshot shows the NetApp SnapCenter interface. On the left, there's a sidebar with icons for Dashboard, Resources (selected), Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area has a dropdown menu set to 'Oracle Database'. Below it, a search bar says 'Resource Group' and a search field contains 'rhe12\_cdb2\_log'. A table lists resources under 'rhe12\_cdb2' and 'rhe12\_cdb2\_log'. The 'rhe12\_cdb2\_log' row has a 'Tags' column with 'orafullbkup' and a 'Policies' column with 'Oracle Full Online Backup'. The 'Last Backup' column shows '09/17/2021 2:38:16 PM' and the 'Overall Status' column shows 'Completed'. A 'New Resource Group' button is in the top right.

3. Select the Oracle log resource group and click Backup Now to manually run an Oracle log backup to flush the latest transaction to the destination in the cloud. In a real DR scenario, the last transaction recoverable depends on the database log volume replication frequency to the cloud, which in turn depends on the RTO or RPO policy of the company.

This screenshot shows the 'rhe12\_cdb2\_log' resource group details. The left sidebar is identical to the previous screenshot. The main area shows a table with columns: Name, Resource Name, Type, and Host. The 'rhe12\_cdb2' row has 'cdb2' in Resource Name, 'Oracle Database' in Type, and 'rhe12.demo.netapp.com' in Host. There are buttons for 'Modify Resource Group', 'Backup Now', 'Maintenance', and 'Delete' at the top right.

This screenshot shows a 'Backup' dialog box. At the top, it says 'Create a backup for the selected resource group'. It has two input fields: 'Resource Group' containing 'rhe12\_cdb2\_log' and 'Policy' containing 'Oracle Archive Log Backup'. Below these are 'Cancel' and 'Backup' buttons. The 'Backup' button is highlighted in blue.



Asynchronous SnapMirror loses data that has not made it to the cloud destination in the database log backup interval in a disaster recovery scenario. To minimize data loss, more frequent log backup can be scheduled. However there is a limit to the log backup frequency that is technically achievable.

4. Select the last log backup on the Secondary Mirror Backup(s), and mount the log backup.

The screenshot shows the NetApp SnapCenter interface for Oracle Database management. On the left, a sidebar lists databases: cdb2, cdb2dev, and cdb2test. The main pane displays 'cdb2 Topology' with a diagram showing 'Local copies' (185 Backups, 0 Clones) connected to 'Mirror copies' (185 Backups, 2 Clones). A summary card on the right provides an overview of backups: 370 Backups, 16 Data Backups, 354 Log Backups, and 2 Clones. Below this, a table titled 'Secondary Mirror Backup(s)' lists three log backups:

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_18.20.04.1177_1	1	Log	09/17/2021 6:20:13 PM	Not Applicable	False	Not Cataloged	5994710
rhel2_cdb2_log_09-17-2021_18.00.01.2424_1	1	Log	09/17/2021 6:00:09 PM	Not Applicable	False	Not Cataloged	5992079
rhel2_cdb2_log_09-17-2021_17.00.01.1566_1	1	Log	09/17/2021 5:00:20 PM	Not Applicable	False	Not Cataloged	5988842

The dialog box is titled 'Mount backups'. It asks 'Choose the host to mount the backup' (set to 'ora-standby.demo.netapp.com') and specifies the 'Mount path' as '/var/opt/snapcenter/sco/backup\_mount/rhel2\_cdb2\_log\_09-17-2021\_18.20.04.1177\_1/cdb2'. It also shows the 'Secondary storage location : Snap Vault / Snap Mirror' section with 'Source Volume' set to 'svm\_onPrem:rhel2\_u03' and 'Destination Volume' set to 'svm\_hybridcvo:rhel2\_u03\_dr'. At the bottom are 'Mount' and 'Cancel' buttons.

5. Select the last full database backup and click Clone to initiate the clone workflow.

The screenshot shows the NetApp SnapCenter interface for managing Oracle databases. The top navigation bar includes links for Oracle Database, demoloradba, App Backup and Clone Admin, and Sign Out. The main area displays the 'cdb2 Topology' for the database 'cdb2'. It shows 'Manage Copies' with 'Local copies' (185 Backups, 0 Clones) and 'Mirror copies' (185 Backups, 2 Clones). A 'Summary Card' provides a quick overview of backup statistics: 370 Backups, 16 Data Backups, 354 Log Backups, and 2 Clones. Below this, a table lists 'Secondary Mirror Backup(s)' with columns for Backup Name, Count, Type, End Date, Verified, Mounted, RMAN Cataloged, and SCN. The table contains six entries, all of which are Log type backups.

## 6. Select a unique clone DB ID on the host.

The screenshot shows the 'Clone from cdb2' wizard in progress. The current step is '1 Name'. The 'Complete Database Clone' option is selected. The 'Clone SID' field is populated with 'cdb2dr'. The sidebar on the left lists the following steps: 1 Name, 2 Locations, 3 Credentials, 4 PreOps, 5 PostOps, 6 Notification, and 7 Summary. The right side of the screen shows configuration for the clone, including 'Secondary storage location : Snap Vault / Snap Mirror' and sections for 'Data' and 'Logs' mapping source volumes to destination volumes.

## 7. Provision a log volume and mount it to the target DR server for the Oracle flash recovery area and online logs.

The screenshot shows the ONTAP System Manager interface. On the left, there's a navigation sidebar with sections like DASHBOARD, STORAGE (Overview, Applications, Volumes), LUNs, Shares, Qtrees, Quotas, Storage VMs, Tiers, NETWORK, EVENTS & JOBS, PROTECTION, and HOSTS. The main area is titled 'Volumes' and lists several volumes: 'ora\_standby\_u01', 'rhel2\_u01\_dr', 'rhel2\_u02\_dr', 'rhel2\_u02\_dr09172116081193\_60', 'rhel2\_u02\_dr09172117035348\_63', 'rhel2\_u03\_dr', and 'rhel2\_u03\_dr09172118245747\_75'. A modal window titled 'Add Volume' is open, prompting for a 'NAME' (set to 'ora\_standby\_u03') and 'CAPACITY' (set to '20 GB'). There are 'More Options' and 'Save' buttons.

```

[ec2-user@ora-standby:tmp]$ sudo mkdir /u03_cdb2dr
[ec2-user@ora-standby tmp]$ chown oracle:oinstall /u03_cdb2dr
chown: changing ownership of '/u03_cdb2dr': Operation not permitted
[ec2-user@ora-standby tmp]$ sudo chown oracle:oinstall /u03_cdb2dr
[ec2-user@ora-standby tmp]$ sudo mount -t nfs 10.221.1.6:/ora_standby_u03 /u03_cdb2dr
[ec2-user@ora-standby tmp]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/tmpfs       7.6G  0    7.6G  0% /dev
tmpfs           7.6G  0    7.6G  0% /dev/shm
tmpfs           7.6G  17M  7.6G  1% /run
tmpfs           7.6G  0    7.6G  0% /sys/fs/cgroup
/dev/nvme0nlp2   10G  9.0G  1.1G  90% /
10.221.1.6:/ora_standby_u01   31G  13G  18G  42% /u01
tmpfs           1.6G  0    1.6G  0% /run/user/1000
10.221.1.6:/Sc28182452-3fa8-448c-9e4a-c5a9e465f353 100G  3.1G  97G  4% /u02_cdb2dev
tmpfs           1.6G  0    1.6G  0% /run/user/54321
10.221.1.6:/Sc39c05df8-4b00-4b3a-853c-9d6d338e5df7 100G  3.7G  97G  4% /u02_cdb2test
10.221.1.6:/Scff88ea5c-3273-475e-ad97-472b2a8dccee 100G  3.8G  97G  4% /var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_log_09-17-2021_18.20.04.1177_1/cdb2/1
10.221.1.6:/ora_standby_u03   21G  320K  20G  1% /u03_cdb2dr
[ec2-user@ora-standby tmp]$

```



The Oracle clone procedure does not create a log volume, which needs to be provisioned on the DR server before cloning.

8. Select the target clone host and location to place the data files, control files, and redo logs.

Clone from cdb2

**1 Name**

Select the host to create a clone

Clone host ora-standby.demo.netapp.com

**2 Locations**

Datafile locations /u02\_cdb2dr

Control files /u02\_cdb2dr/cdb2dr/control/control01.ctl  
/u03\_cdb2dr/cdb2dr/control/control02.ctl

Redo logs

Group	Size	Unit	Number of files
RedoGroup 1	200	MB	1
RedoGroup 2	200	MB	1

Previous Next

The screenshot shows the Oracle Database Clone wizard interface. The left sidebar lists steps 1 through 7. Step 2, 'Locations', is selected and active. The main area is titled 'Select the host to create a clone' and shows the 'Clone host' as 'ora-standby.demo.netapp.com'. Below this, under 'Datafile locations', the path '/u02\_cdb2dr' is listed. Under 'Control files', two paths are listed: '/u02\_cdb2dr/cdb2dr/control/control01.ctl' and '/u03\_cdb2dr/cdb2dr/control/control02.ctl'. Under 'Redo logs', there is a table with three columns: Group, Size, and Unit. It contains two entries: 'RedoGroup 1' with size 200 MB and 1 file, and 'RedoGroup 2' with size 200 MB and 1 file. The 'Next' button is highlighted in blue at the bottom right.

9. Select the credentials for the clone. Fill in the details of the Oracle home configuration on the target server.

Clone from cdb2

**1 Name**

**2 Locations**

**3 Credentials**

**4 PreOps**

**5 PostOps**

**6 Notification**

**7 Summary**

Database Credentials for the clone

Credential name for sys user  + ?

Database port

Oracle Home Settings ?

Oracle Home

Oracle OS User

Oracle OS Group

Previous Next

The screenshot shows the Oracle Database Clone wizard interface. The left sidebar lists steps 1 through 7. Step 3, 'Credentials', is currently selected and highlighted in blue. The main panel shows 'Database Credentials for the clone' with a dropdown for 'Credential name for sys user' set to 'None'. Below it, the 'Database port' is set to '1521'. Under 'Oracle Home Settings', the 'Oracle Home' path is '/u01/app/oracle/product/19800/cdb2', and the 'Oracle OS User' and 'Oracle OS Group' are both 'oracle'. At the bottom right are 'Previous' and 'Next' buttons.

10. Specify the scripts to run before cloning. Database parameters can be adjusted if needed.

Clone from cdb2

**Specify scripts to run before clone operation** ⓘ

Prescript full path	/var/opt/snapcenter/spl/scripts/	Enter Prescript path
Arguments		
Script timeout	60	secs

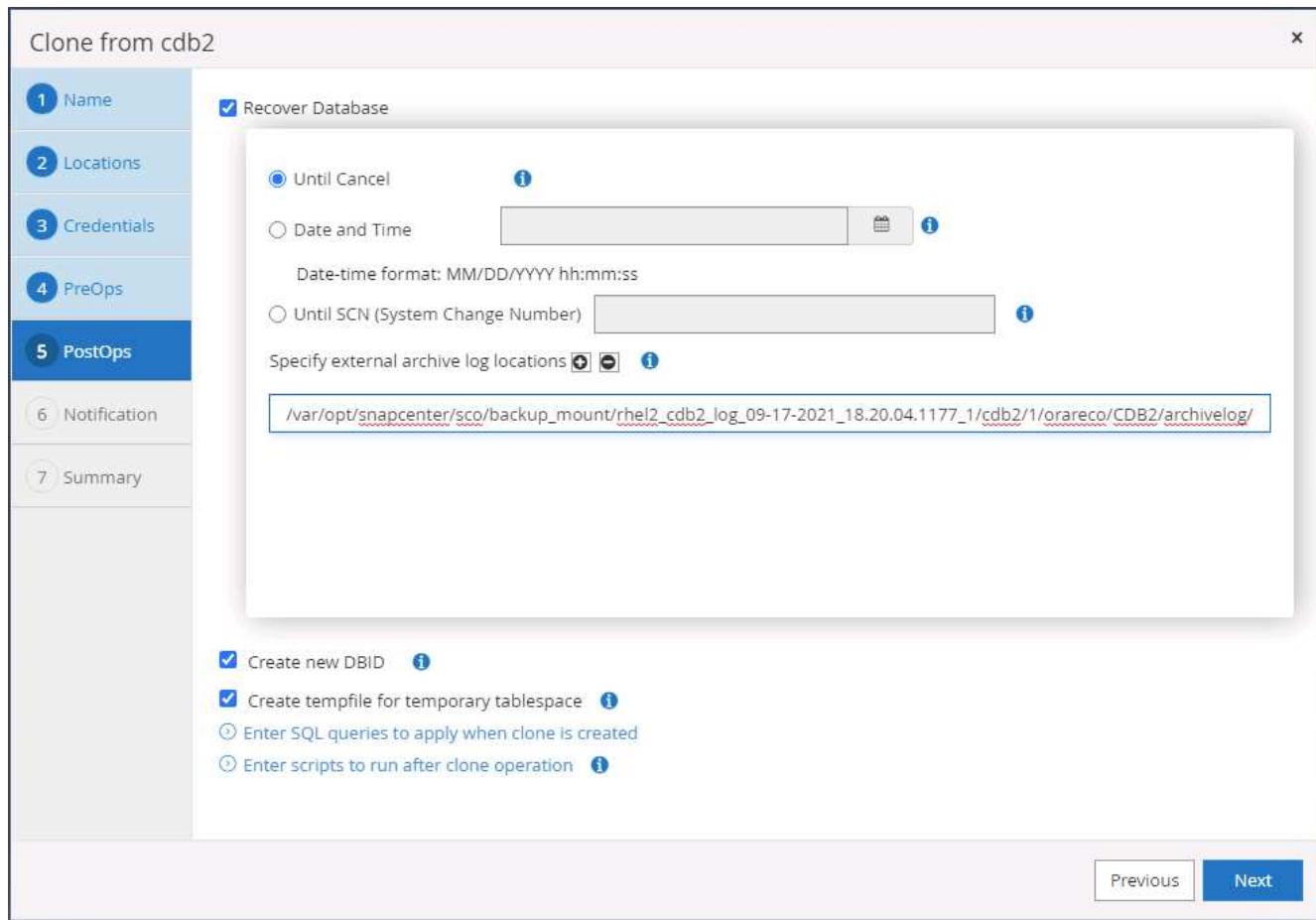
**Database Parameter settings**

audit_file_dest	/u01/app/oracle/admin/cdb2dr/adump	X
audit_trail	DB	X
open_cursors	300	X
pga_aggregate_target	1432354816	X

**Buttons:**

- Previous
- Next

- Select Until Cancel as the recovery option so that the recovery runs through all available archive logs to recoup the last transaction replicated to the secondary cloud location.



12. Configure the SMTP server for email notification if needed.

Clone from cdb2

**Provide email settings i**

Email preference	Never
From	From email
To	Email to
Subject	Notification

Attach job report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

[Previous](#) [Next](#)

1. Name

2. Locations

3. Credentials

4. PreOps

5. PostOps

**6. Notification**

7. Summary

13. DR clone summary.

Clone from cdb2

<b>1 Name</b>	Summary
<b>2 Locations</b>	Clone from backup      rhel2_cdb2_09-17-2021_14.35.01.4997_0
<b>3 Credentials</b>	Clone SID      cdb2dr
<b>4 PreOps</b>	Clone server      ora-standby.demo.netapp.com
<b>5 PostOps</b>	Exclude PDBs      none
<b>6 Notification</b>	Oracle home      /u01/app/oracle/product/19800/cdb2
<b>7 Summary</b>	Oracle OS user      oracle
	Oracle OS group      oinstall
	Datafile mountpaths      /u02_cdb2dr
	Control files      /u02_cdb2dr/cdb2dr/control/control01.ctl /u03_cdb2dr/cdb2dr/control/control02.ctl
	Redo groups      RedoGroup =1 TotalSize =200 Path =/u03_cdb2dr/cdb2dr/redolog/redo03.log RedoGroup =2 TotalSize =200 Path =/u03_cdb2dr/cdb2dr/redolog/redo02.log RedoGroup =3 TotalSize =200 Path =/u03_cdb2dr/cdb2dr/redolog/redo01.log
	Recovery scope      Until Cancel
	Prescript full path      none
	Prescript arguments
	Postscript full path      none
	Postscript arguments

[Previous](#) [Finish](#)

14. Cloned DBs are registered with SnapCenter immediately after clone completion and are then available for backup protection.

NetApp SnapCenter							
		Oracle Database					
Resources		Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup
		cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com	rhel2_cdb2 rhel2_cdb2_log	Oracle Archive Log Backup Oracle Full Online Backup	09/17/2021 7:00:10 PM
		cdb2dev	Single Instance (Multitenant)	ora-standby.demo.netapp.com			Not protected
		cdb2dr	Single Instance (Multitenant)	ora-standby.demo.netapp.com			Not protected
		cdb2test	Single Instance (Multitenant)	ora-standby.demo.netapp.com			Not protected

## Post DR clone validation and configuration for Oracle

1. Validate the last test transaction that has been flushed, replicated, and recovered at the DR location in the cloud.

```
oracle@ora-standby:/u01/app/oracle/product/19000/cdb2/dbs
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> set lin 200
SQL> select instance_name, host_name from v$instance;

INSTANCE_NAME      HOST_NAME
cdb2dr            ora-standby.demo.netapp.com

SQL> alter pluggable database cdb2_pdb1 open;
Pluggable database altered.

SQL> alter session set container=cdb2_pdb1;
Session altered.

SQL> select * from pdbadmin.dr_test;

ID
EVENT
DT
1
testing DB clone for DR and roll forward DB to last available log
17-SEP-21 02.12.13.000000 PM

SQL>
```

## 2. Configure the flash recovery area.

```
[oracle@ora-standby:/u01/app/oracle/product/19000/cdb2/dbs]
[oracle@ora-standby dbs]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Sep 17 22:07:11 2021
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> show parameter db_recovery_file_dest

NAME          TYPE        VALUE
-----
db_recovery_file_dest    string
db_recovery_file_dest_size  big integer 17208M
SQL> alter system set db_recovery_file_dest='/u03_cdb2dr/cdb2dr' scope=both;

System altered.

SQL> show parameter db_recovery_file_dest

NAME          TYPE        VALUE
-----
db_recovery_file_dest    string    /u03_cdb2dr/cdb2dr
db_recovery_file_dest_size  big integer 17208M
SQL>
```

## 3. Configure the Oracle listener for user access.

## 4. Split the cloned volume off of the replicated source volume.

## 5. Reverse replication from the cloud to on-premises and rebuild the failed on-premises database server.



Clone split may incur temporary storage space utilization that is much higher than normal operation. However, after the on-premises DB server is rebuilt, extra space can be released.

## Clone an on-premises SQL production DB to cloud for DR

- Similarly, to validate that the SQL clone recovery ran through last available log, we created a small test table and inserted a row. The test data would be recovered after a full recovery to the last available log.

```

Administrator: Command Prompt - sqlcmd - SQLCMD
C:\Users\administrator.DEMO>sqlcmd
1> select host_name()
2> go

-----
SQL1

(1 rows affected)
1> use tpcc
2> go
Changed database context to 'tpcc'.
1> insert into snap_sync values ('test snap mirror DR for SQL', getdate())
2> go

(1 rows affected)
1> select * from snap_sync
2> go
event                                dt
test snap mirror DR for SQL          2021-09-20 14:23:04.533
(1 rows affected)
1> -

```

- Log into SnapCenter with a database management user ID for SQL Server. Navigate to the Resources tab, which shows the SQL Server protection resources group.

Name	Resource Name	Type	Host
sql1_tpcc	tpcc (sql1)	SQL Database	sql1.demo.netapp.com
sql1_tpcc_log			

- Manually run a log backup to flush the last transaction to be replicated to secondary storage in the public cloud.

Backup

Create a backup for the selected resource group

Resource Group: sql1\_tpcc\_log

Policy: SQL Server Log Backup

Cancel      Backup

- Select the last full SQL Server backup for the clone.

The screenshot shows the NetApp SnapCenter interface for managing a Microsoft SQL Server topology named 'tpcc (sql11)'. On the left, a sidebar lists database names: master, model, msdb, tempdb, tpcc, master, model, msdb, tempdb, tpcc\_clone, and tpcc\_dev. The 'tpcc' entry is selected. The main pane displays 'Manage Copies' with a diagram showing 'Local copies' (7 Backups, 0 Clones) connected to 'Mirror copies' (7 Backups, 2 Clones). Below this is a table for 'Secondary Mirror Backup(s)' with three entries:

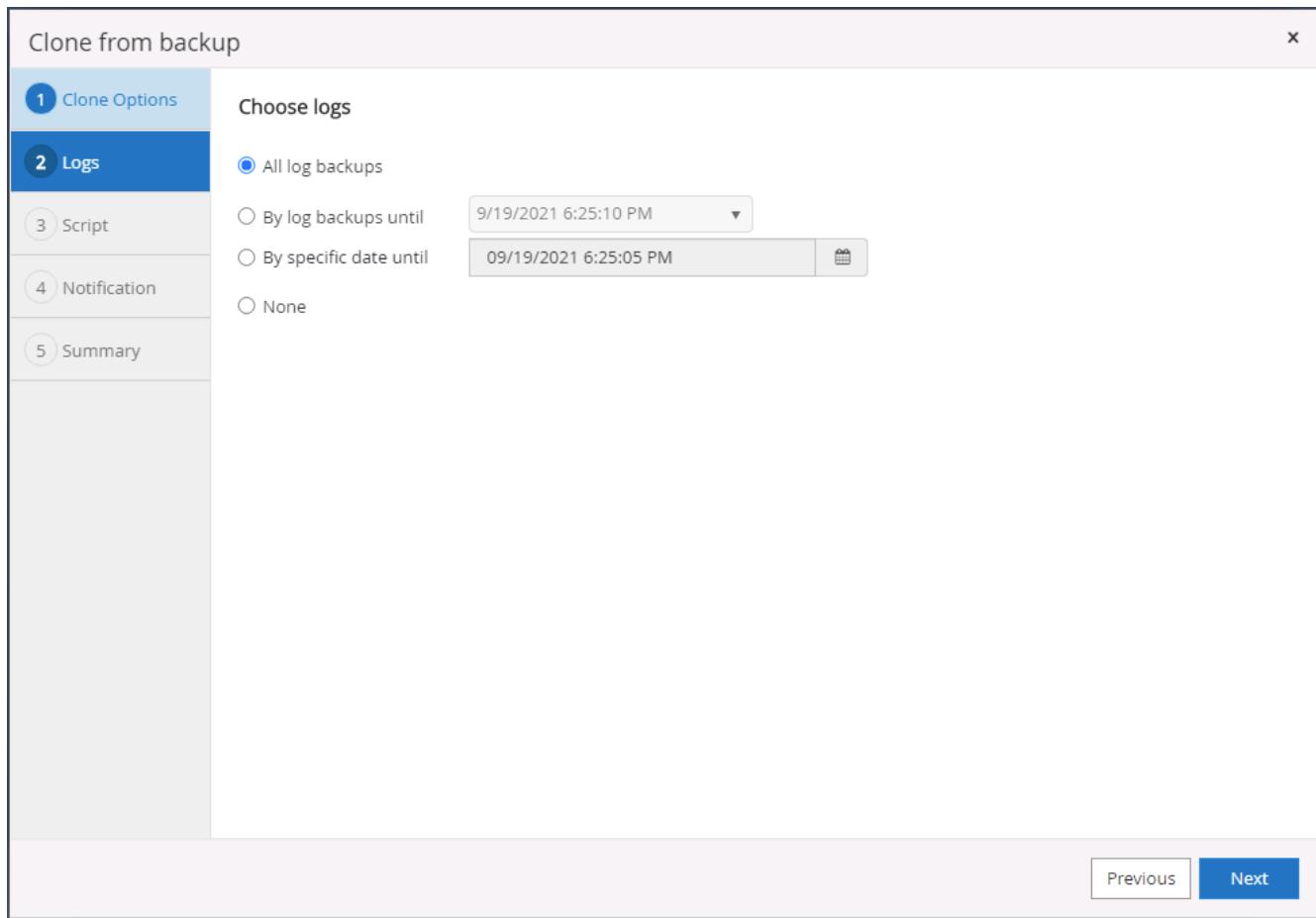
Backup Name	Count	Type	End Date	Verified
sql1_tpcc_09-19-2021_18.25.01.4134	1	Full backup	09/19/2021 6:25:05 PM	Unverified
sql1_tpcc_09-18-2021_18.25.01.3963	1	Full backup	09/18/2021 6:25:05 PM	Unverified
sql1_tpcc_09-17-2021_18.25.01.4218	1	Full backup	09/17/2021 6:25:05 PM	Unverified

- Set the clone setting such as the Clone Server, Clone Instance, Clone Name, and mount option. The secondary storage location where cloning is performed is auto-populated.

The screenshot shows the 'Clone from backup' wizard, Step 1: Clone Options. The left sidebar shows steps 1 through 5. The main area is titled 'Clone settings' and includes fields for 'Clone server' (sql-standby.demo.netapp.com), 'Clone instance' (sql-standby), and 'Clone name' (tpcc\_dr). Below this is a section for 'Choose mount option' with two radio buttons: 'Auto assign mount point' (selected) and 'Auto assign volume mount point under path' (full file path). The next section, 'Secondary storage location : Snap Vault / Snap Mirror', lists source and destination volumes for both data and log volumes. At the bottom are 'Previous' and 'Next' buttons.

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcvo:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcvo:sql1_log_dr

- Select all log backups to be applied.



7. Specify any optional scripts to run before or after cloning.

Clone from backup x

**1 Clone Options**

**2 Logs**

**3 Script**

**4 Notification**

**5 Summary**

Specify optional scripts to run before and after performing a clone from backup job

Prescript full path

Prescript arguments  Choose optional arguments...

Postscript full path

Postscript arguments  Choose optional arguments...

Script timeout  60 secs

Previous Next

8. Specify an SMTP server if email notification is desired.

Clone from backup

**1 Clone Options**

**2 Logs**

**3 Script**

**4 Notification**

**5 Summary**

Provide email settings i

Email preference: Never

From: From email

To: Email to

Subject: Notification

Attach Job Report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

Previous

Next

The screenshot shows the 'Clone from backup' wizard with the 'Notification' tab selected. The interface includes a sidebar with tabs for 'Clone Options', 'Logs', 'Script', 'Notification' (selected), and 'Summary'. The main area is titled 'Provide email settings' with an information icon. It contains fields for 'Email preference' (set to 'Never'), 'From' (set to 'From email'), 'To' (set to 'Email to'), and 'Subject' (set to 'Notification'). There is also a checkbox for 'Attach Job Report'. A note at the bottom of the screen states: '⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.' Navigation buttons 'Previous' and 'Next' are located at the bottom right.

9. DR clone summary. Cloned databases are immediately registered with SnapCenter and available for backup protection.

Clone from backup

**1 Clone Options**

**2 Logs**

**3 Script**

**4 Notification**

**5 Summary**

Summary	
Clone server	sql-standby.demo.netapp.com
Clone instance	sql-standby
Clone name	tpcc_dr
Mount option	Auto Mount
Prescript full path	None
Prescript arguments	
Postscript full path	None
Postscript arguments	
Send email	No

**Previous** **Finish**

NetApp SnapCenter®

Microsoft SQL Server

View Database search by name

Refresh Resources New Resource Group

Resources	Name	Instance	Host	Last Backup	Overall Status	Type
master	sql1	sql1.demo.netapp.com			Not available for backup	System database
model	sql1	sql1.demo.netapp.com			Not available for backup	System database
msdb	sql1	sql1.demo.netapp.com			Not available for backup	System database
tempdb	sql1	sql1.demo.netapp.com			Not available for backup	System database
tpcc	sql1	sql1.demo.netapp.com		09/22/2021 5:35:08 PM	Backup failed, Schedules on hold	User database
master	sql-standby	sql-standby.demo.netapp.com			Not available for backup	System database
model	sql-standby	sql-standby.demo.netapp.com			Not available for backup	System database
msdb	sql-standby	sql-standby.demo.netapp.com			Not available for backup	System database
tempdb	sql-standby	sql-standby.demo.netapp.com			Not available for backup	System database
tpcc_clone	sql-standby	sql-standby.demo.netapp.com			Not protected	User database
tpcc_dlev	sql-standby	sql-standby.demo.netapp.com			Not protected	User database
tpcc_dr	sql-standby	sql-standby.demo.netapp.com			Not protected	User database

## Post DR clone validation and configuration for SQL

### 1. Monitor clone job status.

NetApp SnapCenter®

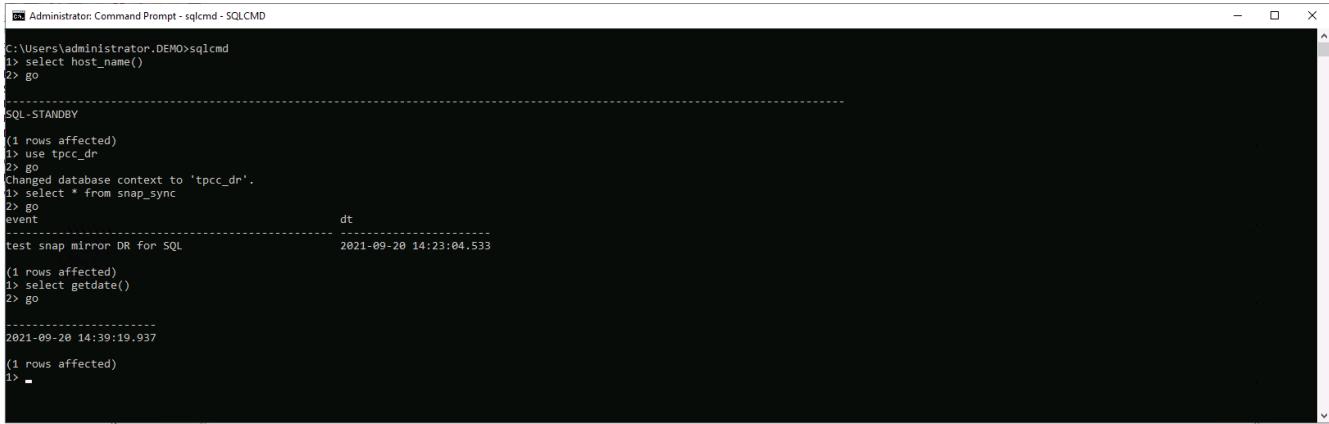
Jobs Schedules Events Logs

Search by name

Details Reports Download Logs Cancel All

ID	Status	Name	Start date	End date	Owner
1052	✓	Clone from backup 'sql1_tpcc_09-19-2021_18.25.01.4134'	09/20/2021 2:36:17 PM	09/20/2021 2:37:06 PM	demo\sqldba
1047	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 2:35:01 PM	09/20/2021 2:37:08 PM	demo\sqldba
1045	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 2:28:17 PM	09/20/2021 2:30:25 PM	demo\sqldba
1044	✓	Clone from backup 'sql1_tpcc_09-17-2021_18.25.01.4218'	09/20/2021 1:39:24 PM	09/20/2021 1:40:09 PM	demo\sqldba
1042	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 1:35:01 PM	09/20/2021 1:37:08 PM	demo\sqldba
1040	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 1:25:01 PM	09/20/2021 1:27:08 PM	demo\sqldba

### 2. Validate that last transaction has been replicated and recovered with all log file clones and recovery.



```
C:\Users\administrator.DEMO>sqlcmd
1> select host_name()
2> go
-----
SQL STANDBY
(1 rows affected)
1> use tpcc_dr
2> go
Changed database context to 'tpcc_dr'.
1> select * from snap_sync
2> go
event                                dt
test snap mirror DR for SQL          2021-09-20 14:23:04.533
(1 rows affected)
1> select getdate()
2> go
-----
2021-09-20 14:39:19.937
(1 rows affected)
1> -
```

3. Configure a new SnapCenter log directory on the DR server for SQL Server log backup.
4. Split the cloned volume off of the replicated source volume.
5. Reverse replication from the cloud to on-premises and rebuild the failed on-premises database server.

### Where to go for help?

If you need help with this solution and use cases, please join the [NetApp Solution Automation community support Slack channel](#) and look for the solution-automation channel to post your questions or inquiries.

## **Copyright Information**

Copyright © 2022 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.