



Enterprise Databases

NetApp Solutions

NetApp
February 15, 2023

This PDF was generated from <https://docs.netapp.com/us-en/netapp-solutions/databases/nva-1155-link.html> on February 15, 2023. Always check docs.netapp.com for the latest.

Table of Contents

NetApp Enterprise Database Solutions	1
Oracle Database	1
Microsoft SQL Server	173
Open Source Databases	214
SnapCenter for databases	231

NetApp Enterprise Database Solutions

Oracle Database

NVA-1155: Oracle 19c RAC databases on FlexPod Datacenter with Cisco UCS and NetApp AFF A800 over FC - Design and deployment guide

Allen Cao, NetApp

This design and deployment guide for Oracle 19c RAC databases on FlexPod Datacenter with Cisco UCS and NetApp AFF A800 over FC provides details of the solution design as well as step-by-step deployment processes for hosting Oracle RAC databases on most recent FlexPod Datacenter infrastructure with the Oracle Linux 8.2 operating system and a Red Hat compatible kernel.

[NVA-1155: Oracle 19c RAC databases on FlexPod Datacenter with Cisco UCS and NetApp AFF A800 over FC](#)

TR-4250: SAP with Oracle on UNIX and NFS with NetApp Clustered Data ONTAP and SnapManager for SAP 3.4

Nils Bauer, NetApp

TR-4250 addresses the challenges of designing storage solutions to support SAP business suite products using an Oracle database. The primary focus of this document is the common storage infrastructure design, deployment, operation, and management challenges faced by business and IT leaders who use the latest generation of SAP solutions. The recommendations in this document are generic; they are not specific to an SAP application or to the size and scope of the SAP implementation. TR-4250 assumes that the reader has a basic understanding of the technology and operation of NetApp and SAP products. TR-4250 was developed based on the interaction of technical staff from NetApp, SAP, Oracle, and our customers.

[TR-4250: SAP with Oracle on UNIX and NFS with NetApp Clustered Data ONTAP and SnapManager for SAP 3.4](#)

Deploying Oracle Database

TR-3633: Oracle databases on ONTAP

Jeffrey Steiner, NetApp

Consult the [Interoperability Matrix Tool \(IMT\)](#) to determine whether the environment, configurations, and versions specified in TR-3633 support your environment.

[TR-3633: Oracle databases on ONTAP](#)

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 (video)
- Part 2: Variables and Running the Playbook
 - ▶ 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 (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.

- 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

- 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](#)
- After the Ansible control host is configured, you can git clone the Ansible Automation repository.
- Edit the hosts file with the IPs and/or hostnames of your ONTAP cluster management and Oracle server's management IPs.
- Fill out the variables specific to your environment, and copy and paste them into the `vars.yml` file.
- Each Oracle host has a variable file identified by its hostname that contains host-specific variables.
- 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
Ansible environment	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>
ONTAP	ONTAP version 9.3 - 9.7 Two data aggregates NFS vlan and ifgrp created
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 increase file descriptor hard limit Create pam.d session file
oracle_config	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 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.
- Click Save.
- 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>",
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 dedicates 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: &quot<span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"><i>{{groups.oracle[0]}}_u02</i></span>&quot,
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: &quot<span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"><i>{{groups.oracle[0]}}_u03</i></span>&quot,
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:adnnfsvolumes();">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>&quot;, name: ""<span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>infra_NFS</i></span>&quot;,,
protocol: ""<span <div 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>

```

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 hte 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>", aggr_name: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>aggr01_node01</i>, lif: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>172.21.94.200</i>, size: <span <div contenteditable='true'><i>25</i>}"}
- {vol_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>{{groups.oracle[0]}}_u02</i>", aggr_name: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>aggr01_node01</i>, lif: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>172.21.94.200</i>, size: <span <div contenteditable='true'><i>25</i>}"}
- {vol_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>{{groups.oracle[0]}}_u03</i>", aggr_name: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>aggr01_node01</i>, lif: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>172.21.94.200</i>, size: <span <div contenteditable='true'><i>25</i>}"}

More NFS volumes<div id="select_more_nfs_volumes"></div>Enter NFS volumes' details<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> #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
Ansible environment	AWX/Tower Ansible v.2.10 and higher Python 3 Python libraries - netapp-lib - xmltodict - jmespath
ONTAP	ONTAP version 9.8 + Two data aggregates NFS vlan and ifgrp created
Oracle server(s)	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
Ansible environment	AWX/Tower Ansible v.2.10 and higher Python 3 Python libraries - netapp-lib - xmltodict - jmespath
ONTAP	ONTAP version 9.8 + Two data aggregates NFS vlan and ifgrp created
Oracle server(s)	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](#).

Step-by-step deployment procedure

AWX/Tower Oracle Data Protection

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. Navigate to the Groups sub-menu and click Add.
 - e. Provide the name oracle for your first group and click Save.
 - f. Repeat the process for a second group called dr_oracle.
 - g. Select the oracle group created, go to the Hosts sub-menu and click Add New Host.
 - h. Provide the IP address of the Source Oracle host's management IP, and click Save.
 - i. This process must be repeated for the dr_oracle group and add the DR/Destination Oracle host's management IP/hostname.



Below are instructions for creating the credential types and credentials for either On-Prem with ONTAP, or CVO on AWS.

On-Prem

1. Configure the credentials.
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: dst_cluster_username  
    type: string  
    label: Destination Cluster Username  
  - id: dst_cluster_password  
    type: string  
    label: Destination Cluster Password  
    secret: true  
  - id: src_cluster_username  
    type: string  
    label: Source Cluster Username  
  - id: src_cluster_password  
    type: string  
    label: Source Cluster Password  
    secret: true
```

- d. Paste the following content into Injector Configuration and then click Save:

```
extra_vars:  
  dst_cluster_username: '{{ dst_cluster_username }}'  
  dst_cluster_password: '{{ dst_cluster_password }}'  
  src_cluster_username: '{{ src_cluster_username }}'  
  src_cluster_password: '{{ src_cluster_password }}'
```

3. Create Credential for ONTAP

- a. Navigate to Resources → Credentials, and click Add.
- b. Enter the name and organization details for the ONTAP Credentials
- c. Select the credential type that was created in the previous step.
- d. Under Type Details, enter the Username and Password for your Source and Destination Clusters.
- e. Click Save

4. Create Credential for Oracle

- a. Navigate to Resources → Credentials, and click Add.
- b. Enter the name and organization details for Oracle

- c. Select the Machine credential type.
- d. Under Type Details, enter the Username and Password for the Oracle hosts.
- e. Select the correct Privilege Escalation Method, and enter the username and password.
- f. Click Save
- g. Repeat process if needed for a different credential for the dr_oracle host.

CVO

1. Configure the credentials.
2. Create credential types. For solutions involving ONTAP, you must configure the credential type to match username and password entries, we will also add entries for Cloud Central and AWS.
 - 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: dst_cluster_username
    type: string
    label: CVO Username
  - id: dst_cluster_password
    type: string
    label: CVO Password
    secret: true
  - id: cvo_svm_password
    type: string
    label: CVO SVM Password
    secret: true
  - id: src_cluster_username
    type: string
    label: Source Cluster Username
  - id: src_cluster_password
    type: string
    label: Source Cluster Password
    secret: true
  - id: regular_id
    type: string
    label: Cloud Central ID
    secret: true
  - id: email_id
    type: string
    label: Cloud Manager Email
    secret: true
  - id: cm_password
    type: string
    label: Cloud Manager Password
    secret: true
  - id: access_key
    type: string
    label: AWS Access Key
    secret: true
  - id: secret_key
    type: string
    label: AWS Secret Key
    secret: true
  - id: token
    type: string
    label: Cloud Central Refresh Token
    secret: true
```

d. Paste the following content into Injector Configuration and click Save:

```

extra_vars:
  dst_cluster_username: '{{ dst_cluster_username }}'
  dst_cluster_password: '{{ dst_cluster_password }}'
  cvo_svm_password: '{{ cvo_svm_password }}'
  src_cluster_username: '{{ src_cluster_username }}'
  src_cluster_password: '{{ src_cluster_password }}'
  regular_id: '{{ regular_id }}'
  email_id: '{{ email_id }}'
  cm_password: '{{ cm_password }}'
  access_key: '{{ access_key }}'
  secret_key: '{{ secret_key }}'
  token: '{{ token }}'

```

3. Create Credential for ONTAP/CVO/AWS

- Navigate to Resources → Credentials, and click Add.
- Enter the name and organization details for the ONTAP Credentials
- Select the credential type that was created in the previous step.
- Under Type Details, enter the Username and Password for your Source and CVO Clusters, Cloud Central/Manager, AWS Access/Secret Key and Cloud Central Refresh Token.
- Click Save

4. Create Credential for Oracle (Source)

- Navigate to Resources → Credentials, and click Add.
- Enter the name and organization details for Oracle host
- Select the Machine credential type.
- Under Type Details, enter the Username and Password for the Oracle hosts.
- Select the correct Privilege Escalation Method, and enter the username and password.
- Click Save

5. Create Credential for Oracle Destination

- Navigate to Resources → Credentials, and click Add.
- Enter the name and organization details for the DR Oracle host
- Select the Machine credential type.
- Under Type Details, enter the Username (ec2-user or if you have changed it from default enter that), and the SSH Private Key
- Select the correct Privilege Escalation Method (sudo), and enter the username and password if needed.
- Click Save

Create a project

- 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_data_protection.git as the source control URL.
- d. Click Save.
- e. The project might need to sync occasionally when the source code changes.

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.

On-Prem

```
<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_binary_vols {
  display: block;
}
#more_binary_vols_button {
  display: none;
}
#more_database_vols {
  display: block;
}
#more_database_vols_button {
  display: none;
}
#more_log_vols {
  display: block;
}
#more_log_vols_button {
  display: none;
}
</style>
<div class="listingblock"><div class="content"><div><button id="copy-button-onprem" onclick="CopyClassText ()">Copy</button></div><pre><code><div class="CopyMeClass" id="CopyOnPrem">
#####
<##</code></pre></div>
```

```

##### Oracle Data Protection global user configuration variables
#####
##### Consolidate all variables from ontap, aws, 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>

#####
# Inter-cluster LIF details
#####
#Names of the Nodes in the Source ONTAP Cluster
src_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>

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

```

```

#Define whether or not to create intercluster lifs on source cluster
(ONLY CHANGE to 'No' IF YOU HAVE ALREADY CREATED THE INTERCLUSTER
LIFs)

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

source_intercluster_network_port_details:
    using_dedicated_ports: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;" /><i>yes</i></span>
    using_ifgrp: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;" /><i>yes</i></span>
    using_vlans: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;" /><i>yes</i></span>
    failover_for_shared_individual_ports: <span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline; text-
decoration:underline;" /><i>yes</i></span>
    ifgrp_name: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;" /><i>a0a</i></span>
    vlan_id: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;" /><i>10</i></span>
    ports:
        - <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;" /><i>e0b</i></span>
        - <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;" /><i>e0g</i></span>
    broadcast_domain: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;" /><i>NFS</i></span>
    ipspace: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;" /><i>Default</i></span>
    failover_group_name: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-
decoration:underline;" /><i>iclifs</i></span>

source_intercluster_lif_details:

```

```

    - name: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;" /><i>ic1_1</i></span>
        address: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;" /><i>10.0.0.1</i></span>
        netmask: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;" /><i>255.255.255.0</i></span>
        home_port: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;" /><i>a0a-
10</i></span>
        node: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;" /><i>AFF-01</i></span>
    - name: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;" /><i>ic1_2</i></span>
        address: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;" /><i>10.0.0.2</i></span>
        netmask: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;" /><i>255.255.255.0</i></span>
        home_port: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;" /><i>a0a-
10</i></span>
        node: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;" /><i>AFF-02</i></span>

#Define whether or not to create intercluster lifs on destination
cluster (ONLY CHANGE to 'No' IF YOU HAVE ALREADY CREATED THE
INTERCLUSTER LIFS)
create_destination_intercluster_lifs: <span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline; text-
decoration:underline;" /><i>yes</i></span>

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

```

```

        style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"/><i>yes</i></span>
    using_vlans: <span <div contenteditable="true"
        style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"/><i>yes</i></span>
    failover_for_shared_individual_ports: <span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"/><i>yes</i></span>
    ifgrp_name: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"/><i>a0a</i></span>
    vlan_id: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"/><i>10</i></span>
    ports:
        - <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"/><i>e0b</i></span>
        - <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"/><i>e0g</i></span>
    broadcast_domain: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;"/><i>NFS</i></span>
    ipspace: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"/><i>Default</i></span>
    failover_group_name: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-
decoration:underline;"/><i>iclifs</i></span>

destination_intercluster_lif_details:
    - name: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"/><i>icl_1</i></span>
        address: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"/><i>10.0.0.3</i></span>
        netmask: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"/><i>255.255.255.0</i></span>
        home_port: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;"/><i>a0a-

```

```

10</i></span>
    node: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"><i>DR-AFF-01</i></span>
      - name: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"><i>icl_2</i></span>
        address: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"><i>10.0.0.4</i></span>
        netmask: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"><i>255.255.255.0</i></span>
        home_port: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;"><i>a0a-
10</i></span>
        node: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"><i>DR-AFF-02</i></span>

#####
#####
# Variables for SnapMirror Peering
#####
#####
#####src_lif: #Will be retrieve through Ansible Task
#####dst_lif: #Will be retrieve through Ansible Task
#####passphrase: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"><i>your-passphrase</i></span>

#####
#####
# Source & Destination List
#####
#####
#####Please Enter Destination Cluster Name
#####dst_cluster_name: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;"><i>dst-cluster-
name</i></span>

#####Please Enter Destination Cluster
#####dst_cluster_ip: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-

```

```

decoration:underline; text-decoration:underline;"/><i>dst-cluster-
ip</i></span>

#Please Enter Destination SVM to create mirror relationship
dst_vserver: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"><i>dst-vserver</i></span>

#Please Enter NFS Lif for dst vserver
dst_nfs_lif: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"><i>dst-nfs-lif</i></span>

#Please Enter Source Cluster Name
src_cluster_name: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;"><i>src-cluster-
name</i></span>

#Please Enter Source Cluster
src_cluster_ip: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;"><i>src-cluster-
ip</i></span>

#Please Enter Source SVM
src_vserver: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"><i>src-vserver</i></span>

#####
#####
#
# Variable for Oracle Volumes and SnapMirror Details
#####
#####
#
#Please Enter Source Snapshot Prefix Name
cg_snapshot_name_prefix: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-
decoration:underline;"><i>oracle</i></span>

#Please Enter Source Oracle Binary Volume(s)
src_orabinary_vols:
  - <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>binary_vol</i></span>

```

```

<a id="more_binary_vols"
    href="javascript:binaryvolsdropdown();">More Binary Vols</a><div
    id="select_more_binary_vols"></div><a id="more_binary_vols_button"
    href="javascript:addbinaryvols();">Enter Volume details</a><div
    id="extra_binary_vols"></div>
#Please Enter Source Database Volume(s)
src_db_vols:
    - <span <div contenteditable="true" style="color:#004EFF; font-
        weight:bold; font-style:italic; text-decoration:underline; text-
        decoration:underline;"><i>db_vol</i></span>
<a id="more_database_vols"
    href="javascript:databasevolsdropdown();">More Database Vols</a><div
    id="select_more_database_vols"></div><a
    id="more_database_vols_button"
    href="javascript:adddatabasevols();">Enter Volume details</a><div
    id="extra_database_vols"></div>
#Please Enter Source Archive Volume(s)
src_archivelog_vols:
    - <span <div contenteditable="true" style="color:#004EFF; font-
        weight:bold; font-style:italic; text-decoration:underline; text-
        decoration:underline;"><i>log_vol</i></span>
<a id="more_log_vols" href="javascript:logvolsdropdown();">More Log
Vols</a><div id="select_more_log_vols"></div><a
    id="more_log_vols_button" href="javascript:addlogvols();">Enter
    Volume details</a><div id="extra_log_vols"></div>
#Please Enter Destination Snapmirror Policy
snapmirror_policy: <span <div contenteditable="true"
    style="color:#004EFF; font-weight:bold; font-style:italic; text-
    decoration:underline; text-
    decoration:underline;"><i>async_policy_oracle</i></span>

#####
#####
# Export Policy Details
#####
#####
#Enter the destination export policy details
export_policy_details:
    name: <span <div contenteditable="true" style="color:#004EFF;
        font-weight:bold; font-style:italic; text-decoration:underline;
        text-decoration:underline;"><i>nfs_export_policy</i></span>
        client_match: <span <div contenteditable="true"
            style="color:#004EFF; font-weight:bold; font-style:italic; text-
            decoration:underline; text-
            decoration:underline;"><i>0.0.0.0/0</i></span>
        ro_rule: sys

```

```

rw_rule: sys

#####
### 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 #####
#####

#Recovery Type (leave as scn)
recovery_type: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>scn</i></span>

#Oracle Control Files
control_files:
  - <span <div contenteditable="true" style="color:#004EFF; font-

```

```

    weight:bold; font-style:italic; text-decoration:underline;"/><i>/u02/oradata/CDB2/control01.ctl</i></span>
    - <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"/><i>/u03/orareco/CDB2/control02.ctl</i></span>
    >

</div></code></pre></div></div>
<script>
function CopyClassText() {
    var textToCopy = document.getElementById("CopyOnPrem");
    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_binary_vols").style.display =
"none";
    document.getElementById("more_database_vols").style.display =
"none";
    document.getElementById("more_log_vols").style.display = "none";
    var command = document.execCommand("copy");
    if (command)
    {
        document.getElementById("copy-button-onprem").innerHTML =
"Copied!";
        setTimeout(revert_copy, 3000);
    }
    window.getSelection().removeRange(CopyRange);
    if(currentRange)
    {
        window.getSelection().addRange(currentRange);
    }
}
function revert_copy() {
    document.getElementById("copy-button-onprem").innerHTML =
"Copy";
}

```

```

        document.getElementById("more_binary_vols").style.display =
"block";
        document.getElementById("more_database_vols").style.display =
"block";
        document.getElementById("more_log_vols").style.display =
"block";
    }
    function binaryvolsdropdown() {
        document.getElementById("more_binary_vols").style.display =
"none";
        document.getElementById("more_binary_vols_button").style.display =
"block";
        var x=1;
        var myHTML = '';
        var buildup = '';
        var wrapper =
document.getElementById("select_more_binary_vols");
        while (x < 10) {
            buildup += '<option value="' + x + '">' + x + '</option>';
            x++;
        }
        myHTML += '<a id="more_binary_vols_info">How many extra volumes
do you wish to add?</a><select name="number_of_extra_binary_vols"
id="number_of_extra_binary_vols">' + buildup + '</select>';
        wrapper.innerHTML = myHTML;
    }
    function addbinaryvols() {
        var y =
document.getElementById("number_of_extra_binary_vols").value;
        var j=0;
        var myHTML = '';
        var wrapper = document.getElementById("extra_binary_vols");
        while (j < y) {
            j++;
            myHTML += ' - <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-
decoration:underline;"><i>binary_vols</i></span><br>';
        }
        wrapper.innerHTML = myHTML;
        document.getElementById("select_more_binary_vols").style.display =
"none";
        document.getElementById("more_binary_vols_button").style.display =
"none";
    }
    function databasevolsdropdown() {

```

```

        document.getElementById("more_database_vols").style.display =
    "none";

document.getElementById("more_database_vols_button").style.display =
"block";
    var x=1;
    var myHTML = '';
    var buildup = '';
    var wrapper =
document.getElementById("select_more_database_vols");
    while (x < 10) {
        buildup += '<option value="' + x + '">' + x + '</option>';
        x++;
    }
    myHTML += '<a id="more_database_vols_info">How many extra
volumes do you wish to add?</a><select
name="number_of_extra_database_vols"
id="number_of_extra_database_vols">' + buildup + '</select>';
    wrapper.innerHTML = myHTML;
}
function adddatabasevols() {
    var y =
document.getElementById("number_of_extra_database_vols").value;
    var j=0;
    var myHTML = '';
    var wrapper = document.getElementById("extra_database_vols");
    while (j < y) {
        j++;
        myHTML += ' - <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-
decoration:underline;"><i>db_vol</i></span><br>';
    }
    wrapper.innerHTML = myHTML;

document.getElementById("select_more_database_vols").style.display =
"none";

document.getElementById("more_database_vols_button").style.display =
"none";
}

function logvolsdropdown() {
    document.getElementById("more_log_vols").style.display = "none";
    document.getElementById("more_log_vols_button").style.display =
"block";
    var x=1;

```

```

var myHTML = '';
var buildup = '';
var wrapper = document.getElementById("select_more_log_vols");
while (x < 10) {
    buildup += '<option value="' + x + '">' + x + '</option>';
    x++;
}
myHTML += '<a id="more_database_vols_info">How many extra
volumes do you wish to add?</a><select
name="number_of_extra_log_vols" id="number_of_extra_log_vols">' +
buildup + '</select>';
wrapper.innerHTML = myHTML;
}

function addlogvols() {
    var y =
document.getElementById("number_of_extra_log_vols").value;
    var j=0;
    var myHTML = '';
    var wrapper = document.getElementById("extra_log_vols");
    while (j < y) {
        j++;
        myHTML += ' - <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-
decoration:underline;"><i>log_vol</i></span><br>';
    }
    wrapper.innerHTML = myHTML;
    document.getElementById("select_more_log_vols").style.display =
"none";
    document.getElementById("more_log_vols_button").style.display =
"none";
}

</script>

```

CVO

```

<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_binary_vols1 {
    display: block;
}
#more_binary_vols1_button {
    display: none;
}
#more_database_vols1 {
    display: block;
}
#more_database_vols1_button {
    display: none;
}
#more_log_vols1 {
    display: block;
}
#more_log_vols1_button {
    display: none;
}

```

</style>

```

<div class="listingblock"><div class="content"><div><button
id="copy-button-cvo"
onclick="CopyClassTextCVO()">Copy</button></div><pre><code><div
class="CopyMeClassCVO" id="CopyCVO">
#####
## Oracle Data Protection global user configuration variables
#####
##### Consolidate all variables from ontap, aws, CVO 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 Source ONTAP Cluster
src_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>

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

#Define whether or not to create intercluster lifs on source cluster
(ONLY CHANGE to 'No' IF YOU HAVE ALREADY CREATED THE INTERCLUSTER
LIFS)
create_source_intercluster_lifs: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;" /><i>yes</i></span>

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

```

```

decoration:underline; text-decoration:underline;"/><i>yes</i></span>
using_vlans: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;"/><i>yes</i></span>
failover_for_shared_individual_ports: <span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline; text-
decoration:underline;"/><i>yes</i></span>
ifgrp_name: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;"/><i>a0a</i></span>
vlan_id: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"/><i>10</i></span>
ports:
- <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"/><i>e0b</i></span>
- <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"/><i>e0g</i></span>
broadcast_domain: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;"/><i>NFS</i></span>
ipspace: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"/><i>Default</i></span>
failover_group_name: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-
decoration:underline;"/><i>iclifs</i></span>

source_intercluster_lif_details:
- name: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"/><i>icl_1</i></span>
address: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"/><i>10.0.0.1</i></span>
netmask: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"/><i>255.255.255.0</i></span>
home_port: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;"/><i>a0a-
10</i></span>

```

```

        node: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;" /><i>AFF-01</i></span>
      - name: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;" /><i>icl_2</i></span>
        address: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;" /><i>10.0.0.2</i></span>
        netmask: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;" /><i>255.255.255.0</i></span>
        home_port: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;" /><i>a0a-
10</i></span>
        node: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;" /><i>AFF-02</i></span>

#####
### CVO Deployment Variables ###
#####

##### Access Keys Variables #####
# Region where your CVO will be deployed.
region_deploy: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;" /><i>us-east-1</i></span>

##### CVO and Connector Vars #####
# AWS Managed Policy required to give permission for IAM role
creation.
aws_policy: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;" /><i>arn:aws:iam::1234567:policy/OCCM</i></spa
n>

# Specify your aws role name, a new role is created if one already
does not exist.
aws_role_name: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;" /><i>arn:aws:iam::1234567:policy/OCCM</i></spa
n>
```

```

# Name your connector.
connector_name: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"><i>awx_connector</i></span>

# Name of the key pair generated in AWS.
key_pair: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"><i>key_pair</i></span>

# Name of the Subnet that has the range of IP addresses in your VPC.
subnet: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"><i>subnet-12345</i></span>

# ID of your AWS security group that allows access to on-prem
resources.
security_group: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"><i>sg-123123123</i></span>

# Your Cloud Manager Account ID.
account: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"><i>account-A23123A</i></span>

# Name of your CVO instance
cvo_name: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"><i>test_cvo</i></span>

# ID of the VPC in AWS.
vpc: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline;"><i>vpc-
123123123</i></span>

#####
#####
# Variables for - Add on-prem ONTAP to Connector in Cloud Manager
#####
#####

# For Federated users, Client ID from API Authentication Section of
Cloud Central to generate access token.
sso_id: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-

```



```

text-decoration:underline;"/><i>dst-nfs-lif</i></span>

#Please Enter Source Cluster Name
src_cluster_name: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;"/><i>src-cluster-
name</i></span>

#Please Enter Source Cluster
src_cluster_ip: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-decoration:underline;"/><i>src-cluster-
ip</i></span>

#Please Enter Source SVM
src_vserver: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"/><i>src-vserver</i></span>

#####
#####
#
# Variable for Oracle Volumes and SnapMirror Details
#####
#####
#####
#
# Please Enter Source Snapshot Prefix Name
cg_snapshot_name_prefix: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-
decoration:underline;"/><i>oracle</i></span>

#Please Enter Source Oracle Binary Volume(s)
src_orabinary_vols:
  - <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"/><i>binary_vol</i></span>
<a id="more_binary_vols1"
href="javascript:binaryvols1dropdown();">More Binary Vols</a><div
id="select_more_binary_vols1"></div><a id="more_binary_vols1_button"
href="javascript:addbinaryvols1();">Enter Volume details</a><div
id="extra_binary_vols1"></div>
#Please Enter Source Database Volume(s)
src_db_vols:
  - <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"/><i>db_vol</i></span>
<a id="more_database_vols1"

```

```

    href="javascript:databasevols1dropdown();">More Database
Vols</a><div id="select_more_database_vols1"></div><a
id="more_database_vols1_button"
href="javascript:adddatabasevols1();">Enter Volume details</a><div
id="extra_database_vols1"></div>
#Please Enter Source Archive Volume(s)
src_archivelog_vols:
    - <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>log_vol</i></span>
<a id="more_log_vols1" href="javascript:logvols1dropdown();">More
Log Vols</a><div id="select_more_log_vols1"></div><a
id="more_log_vols1_button" href="javascript:addlogvols1();">Enter
Volume details</a><div id="extra_log_vols1"></div>
#Please Enter Destination Snapmirror Policy
snapmirror_policy: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-
decoration:underline;"><i>async_policy_oracle</i></span>

#####
#####
#
# Export Policy Details
#####
#####
#
#Enter the destination export policy details (Once CVO is Created
Add this Variable to all templates)
export_policy_details:
    name: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline;
text-decoration:underline;"><i>nfs_export_policy</i></span>
    client_match: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-
decoration:underline;"><i>0.0.0.0/0</i></span>
    ro_rule: sys
    rw_rule: sys

#####
#####
#
### 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 ##
#####
#Recovery Type (leave as scn)
recovery_type: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>scn</i></span>

#Oracle Control Files
control_files:
    - <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>/u02/oradata/CDB2/control01.ctl</i></span>
    - <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>/u03/orareco/CDB2/control02.ctl</i></span>

```

```

</div></code></pre></div></div>
<script>
function CopyClassTextCVO() {
    var textToCopy = document.getElementById("CopyCVO");
    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_binary_vols1").style.display =
"none";
    document.getElementById("more_database_vols1").style.display =
"none";
    document.getElementById("more_log_vols1").style.display =
"none";
    var command = document.execCommand("copy");
    if (command)
    {
        document.getElementById("copy-button-cvo").innerHTML =
"Copied!";
        setTimeout(revert_copy, 3000);
    }
    window.getSelection().removeRange(CopyRange);
    if(currentRange)
    {
        window.getSelection().addRange(currentRange);
    }
}
function revert_copy() {
    document.getElementById("copy-button-cvo").innerHTML = "Copy";
    document.getElementById("more_binary_vols1").style.display =
"block";
    document.getElementById("more_database_vols1").style.display =
"block";
    document.getElementById("more_log_vols1").style.display =
"block";
}
function binaryvols1dropdown() {

```

```

        document.getElementById("more_binary_vols1").style.display =
"none";

document.getElementById("more_binary_vols1_button").style.display =
"block";
    var x=1;
    var myHTML = '';
    var buildup = '';
    var wrapper =
document.getElementById("select_more_binary_vols1");
    while (x < 10) {
        buildup += '<option value="' + x + '">' + x + '</option>';
        x++;
    }
    myHTML += '<a id="more_binary_vols1_info">How many extra volumes
do you wish to add?</a><select name="number_of_extra_binary_vols1"
id="number_of_extra_binary_vols1">' + buildup + '</select>';
    wrapper.innerHTML = myHTML;
}
function addbinaryvols1() {
    var y =
document.getElementById("number_of_extra_binary_vols1").value;
    var j=0;
    var myHTML = '';
    var wrapper = document.getElementById("extra_binary_vols1");
    while (j < y) {
        j++;
        myHTML += ' - <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-
decoration:underline;"><i>binary_vol</i></span><br>';
    }
    wrapper.innerHTML = myHTML;

document.getElementById("select_more_binary_vols1").style.display =
"none";
}

document.getElementById("more_binary_vols1_button").style.display =
"none";
}

function databasevols1dropdown() {
    document.getElementById("more_database_vols1").style.display =
"none";

document.getElementById("more_database_vols1_button").style.display =
"block";

```

```

var x=1;
var myHTML = '';
var buildup = '';
var wrapper =
document.getElementById("select_more_database_vols1");
while (x < 10) {
    buildup += '<option value="' + x + '">' + x + '</option>';
    x++;
}
myHTML += '<a id="more_database_vols1_info">How many extra
volumes do you wish to add?</a><select
name="number_of_extra_database_vols1"
id="number_of_extra_database_vols1">' + buildup + '</select>';
wrapper.innerHTML = myHTML;
}

function adddatabasevols1() {
    var y =
document.getElementById("number_of_extra_database_vols1").value;
    var j=0;
    var myHTML = '';
    var wrapper = document.getElementById("extra_database_vols1");
    while (j < y) {
        j++;
        myHTML += ' - <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-
decoration:underline;"><i>db_vol</i></span><br>';
    }
    wrapper.innerHTML = myHTML;

document.getElementById("select_more_database_vols1").style.display
= "none";

document.getElementById("more_database_vols1_button").style.display
= "none";
}
function logvols1dropdown() {
    document.getElementById("more_log_vols1").style.display =
"none";
    document.getElementById("more_log_vols1_button").style.display =
"block";
    var x=1;
    var myHTML = '';
    var buildup = '';
    var wrapper = document.getElementById("select_more_log_vols1");
    while (x < 10) {

```

```

        buildup += '<option value="' + x + '">' + x + '</option>';
        x++;
    }
    myHTML += '<a id="more_database_vols_info">How many extra
volumes do you wish to add?</a><select
name="number_of_extra_log_vols1" id="number_of_extra_log_vols1">' +
buildup + '</select>';
    wrapper.innerHTML = myHTML;
}
function addlogvols1() {
    var y =
document.getElementById("number_of_extra_log_vols1").value;
    var j=0;
    var myHTML = '';
    var wrapper = document.getElementById("extra_log_vols1");
    while (j < y) {
        j++;
        myHTML += ' - <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline; text-
decoration:underline;"><i>log_vol</i></span><br>';
    }
    wrapper.innerHTML = myHTML;
    document.getElementById("select_more_log_vols1").style.display =
"none";
    document.getElementById("more_log_vols1_button").style.display =
"none";
}

```

</script>

Automation Playbooks

There are four separate playbooks that need to be ran.

1. Playbook for Setting up your environment, On-Prem or CVO.
2. Playbook for replicating Oracle Binaries and Databases on a schedule
3. Playbook for replicating Oracle Logs on a schedule
4. Playbook for Recovering your database on a destination host

ONTAP/CVO Setup

ONTAP and CVO Setup

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 ONTAP/CVO Setup
 - c. Select the Job type; Run configures the system based on a playbook.
 - d. Select the corresponding inventory, project, playbook, and credentials for the playbook.
 - e. Select the ontap_setup.yml playbook for an On-Prem environment or select the cvo_setup.yml for replicating to a CVO instance.
 - f. Paste global variables copied from step 4 into the Template Variables field under the YAML tab.
 - g. Click Save.
2. Launch the job template.
 - a. Navigate to Resources → Templates.
 - b. Click the desired template and then click Launch.



We will use this template and copy it out for the other playbooks.

Replication For Binary and Database Volumes

Scheduling the Binary and Database Replication Playbook

Configure and launch the job template.

1. Copy the previously created job template.
 - a. Navigate to Resources → Templates.
 - b. Find the ONTAP/CVO Setup Template, and on the far right click on Copy Template
 - c. Click Edit Template on the copied template, and change the name to Binary and Database Replication Playbook.
 - d. Keep the same inventory, project, credentials for the template.
 - e. Select the ora_replication_cg.yml as the playbook to be executed.
 - f. The variables will remain the same, but the CVO cluster IP will need to be set in the variable dst_cluster_ip.
 - g. Click Save.
2. Schedule the job template.
 - a. Navigate to Resources → Templates.
 - b. Click the Binary and Database Replication Playbook template and then click Schedules at the top set of options.
 - c. Click Add, add Name Schedule for Binary and Database Replication, choose the Start date/time at the beginning of the hour, choose your Local time zone, and Run frequency. Run frequency will be often the SnapMirror replication will be updated.



A separate schedule will be created for the Log volume replication, so that it can be replicated on a more frequent cadence.

Replication for Log Volumes

Scheduling the Log Replication Playbook

Configure and launch the job template.

1. Copy the previously created job template.
 - a. Navigate to Resources → Templates.
 - b. Find the ONTAP/CVO Setup Template, and on the far right click on Copy Template
 - c. Click Edit Template on the copied template, and change the name to Log Replication Playbook.
 - d. Keep the same inventory, project, credentials for the template.
 - e. Select the ora_replication_logs.yml as the playbook to be executed.
 - f. The variables will remain the same, but the CVO cluster IP will need to be set in the variable dst_cluster_ip.
 - g. Click Save.
2. Schedule the job template.
 - a. Navigate to Resources → Templates.
 - b. Click the Log Replication Playbook template and then click Schedules at the top set of options.
 - c. Click Add, add Name Schedule for Log Replication, choose the Start date/time at the beginning of the hour, choose your Local time zone, and Run frequency. Run frequency will be often the SnapMirror replication will be updated.



It is recommended to set the log schedule to update every hour to ensure the recovery to the last hourly update.

Restore and Recover Database

Scheduling the Log Replication Playbook

Configure and launch the job template.

1. Copy the previously created job template.
 - a. Navigate to Resources → Templates.
 - b. Find the ONTAP/CVO Setup Template, and on the far right click on Copy Template
 - c. Click Edit Template on the copied template, and change the name to Restore and Recovery Playbook.
 - d. Keep the same inventory, project, credentials for the template.
 - e. Select the ora_recovery.yml as the playbook to be executed.
 - f. The variables will remain the same, but the CVO cluster IP will need to be set in the variable dst_cluster_ip.
 - g. Click Save.



This playbook will not be ran until you are ready to restore your database at the remote site.

Recovering Oracle Database

1. On-premises production Oracle databases data volumes are protected via NetApp SnapMirror replication to either a redundant ONTAP cluster in secondary data center or Cloud Volume ONTAP in public cloud. In a fully configured disaster recovery environment, recovery compute instances in secondary data center or public cloud are standby and ready to recover the production database in the case of a disaster. The standby compute instances are kept in sync with on-prem instances by running parallel updates on OS kernel patch or upgrade in a lockstep.
2. In this solution demonstrated, Oracle binary volume is replicated to target and mounted at target instance to bring up Oracle software stack. This approach to recover Oracle has advantage over a fresh installation of Oracle at last minute when a disaster occurred. It guarantees Oracle installation is fully in sync with current on-prem production software installation and patch levels etc. However, this may or may not have additional software licensing implication for the replicated Oracle binary volume at recovery site depending on how the software licensing is structured with Oracle. User is recommended to check with its software licensing personnel to assess the potential Oracle licensing requirement before deciding to use the same approach.
3. The standby Oracle host at the destination is configured with the Oracle prerequisite configurations.
4. The SnapMirrors are broken and the volumes are made writable and mounted to the standby Oracle host.
5. The Oracle recovery module performs following tasks to recovery and startup Oracle at recovery site after all DB volumes are mounted at standby compute instance.
 - a. Sync the control file: We deployed duplicate Oracle control files on different database volume to protect critical database control file. One is on the data volume and another is on log volume. Since data and log volumes are replicated at different frequency, they will be out of sync at the time of recovery.
 - b. Relink Oracle binary: Since the Oracle binary is relocated to a new host, it needs a relink.
 - c. Recover Oracle database: The recovery mechanism retrieves last System Change Number in last available archived log in Oracle log volume from control file and recovers Oracle database to recoup all business transactions that was able to be replicated to DR site at the time of failure. The database is then started up in a new incarnation to carry on user connections and business transaction at recovery site.



Before running the Recovering playbook make sure you have the following:
Make sure it copy over the /etc/oratab and /etc/oralInst.loc from the source Oracle host to the destination host

TR-4794: Oracle databases on NetApp EF-Series

Mitch Blackburn, Ebin Kadavy, NetApp

TR-4794 is intended to help storage administrators and database administrators successfully deploy Oracle on NetApp EF-Series storage.

[TR-4794: Oracle databases on NetApp EF-Series](#)

Oracle Database Deployment on AWS EC2 and FSx Best Practices

WP-7357: Oracle Database Deployment on EC2 and FSx Best Practices Introduction

Allen Cao, Niyaz Mohamed, Jeffrey Steiner, NetApp

Many mission-critical enterprise Oracle databases are still hosted on-premises, and many enterprises are looking to migrate these Oracle databases to a public cloud. Often, these Oracle databases are application centric and thus require user-specific configurations, a capability that is missing from many database-as-a-service public-cloud offerings. Therefore, the current database landscape calls for a public-cloud-based Oracle database solution built from a high-performance, scalable compute and storage service that can accommodate unique requirements. AWS EC2 compute instances and the AWS FSx storage service might be the missing pieces of this puzzle that you can leverage to build and migrate your mission critical Oracle database workloads to a public cloud.

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for enterprises. The simple Amazon EC2 web-service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment.

Amazon FSx for ONTAP is an AWS storage service that uses industry-leading NetApp ONTAP block and file storage, which exposes NFS, SMB, and iSCSI. With such a powerful storage engine, it has never been easier to relocate mission-critical Oracle database apps to AWS with sub-millisecond response times, multiple Gbps of throughput, and 100,000+ IOPS per database instance. Better yet, the FSx storage service comes with native replication capability that allows you to easily migrate your on-premises Oracle database to AWS or to replicate your mission critical Oracle database to a secondary AWS availability zone for HA or DR.

The goal of this documentation is to provide step-by-step processes, procedures, and best-practice guidance on how to deploy and configure an Oracle database with FSx storage and an EC2 instance that delivers performance similar to an on-premises system. NetApp also provides an automation toolkit that automates most of the tasks that are required for the deployment, configuration, and management of your Oracle database workload in the AWS public cloud.

To learn more about the solution and use case, take a look at following overview video:

[Modernize your Oracle database with hybrid cloud in AWS and FSx ONTAP, Part1 - Use case and solution architecture](#)

[Next: Solutions architecture.](#)

Solution architecture

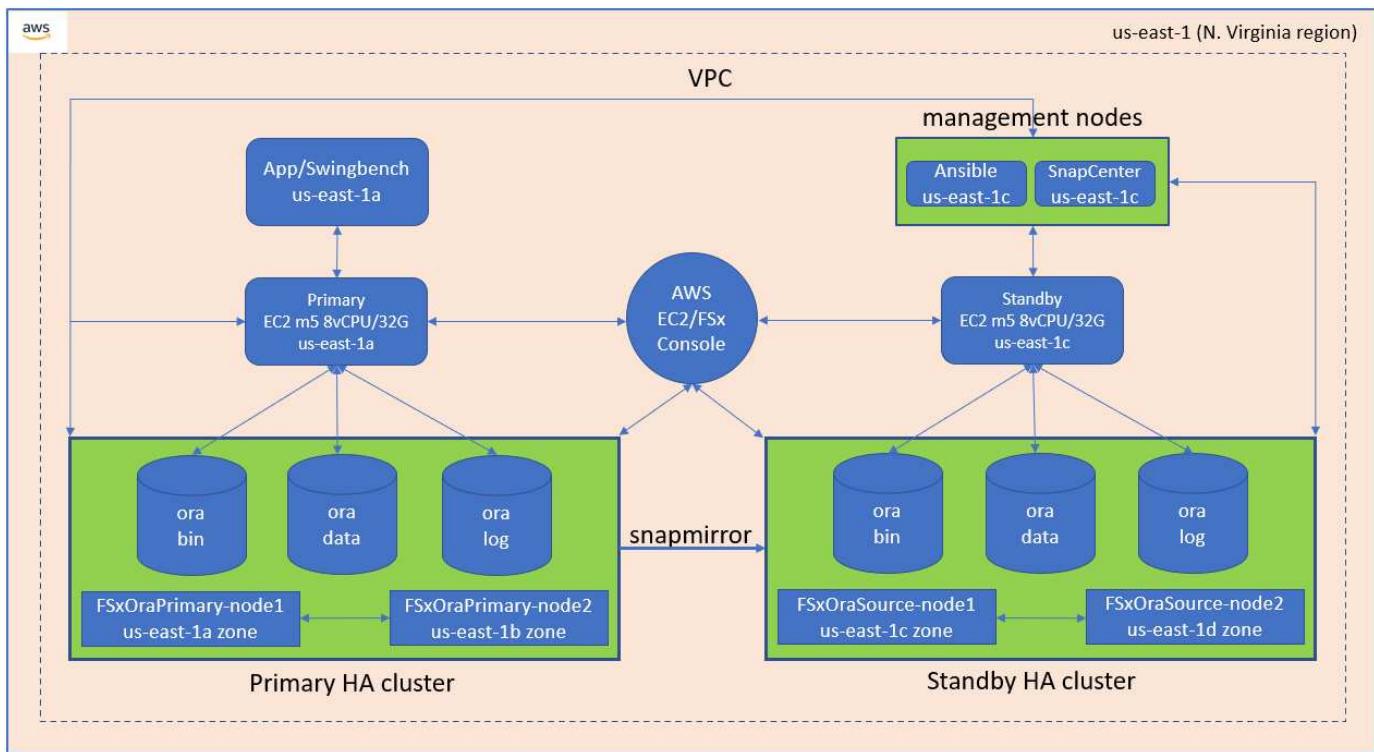
[Previous: Introduction.](#)

The following architecture diagram illustrates a highly available Oracle database deployment on an AWS EC2 instance with the FSx storage service. A similar deployment scheme but with the standby in a different region can be set up for disaster recovery.

Within the environment, the Oracle compute instance is deployed via an AWS EC2 instance console. There are multiple EC2 instance types available from the console. NetApp recommends deploying a database-oriented EC2 instance type such as an m5 Ami image with RedHat enterprise Linux 8 and up to 10Gps of network bandwidth.

Oracle database storage on FSx volumes on the other hand is deployed with the AWS FSx console or CLI.

The Oracle binary, data, or log volumes are subsequently presented and mounted on an EC2 instance Linux host. Each data or log volume can have multiple LUNs allocated depending on the underlying storage protocol employed.



An FSx storage cluster is designed with double redundancy, so that both the primary and standby storage clusters are deployed in two different availability zones. Database volumes are replicated from a primary FSx cluster to a standby FSx cluster at a user-configurable interval for all Oracle binary, data, and log volumes.

This high availability Oracle environment is managed with an Ansible controller node and a SnapCenter backup server and UI tool. Oracle installation, configuration, and replication are automated using Ansible playbook-based tool kits. Any update to the Oracle EC2 instance kernel operating system or Oracle patching can be executed in parallel to keep the primary and standby in sync. In fact, the initial automation setup can be easily expanded to perform some repeating daily Oracle tasks if needed.

SnapCenter provides workflows for Oracle database point-in-time recovery or for database cloning at either the primary or standby zones if needed. Through the SnapCenter UI, you can configure Oracle database backup and replication to standby FSx storage for high availability or disaster recovery based on your RTO or RPO objectives.

The solution provides an alternative process that delivers capabilities similar to those available from Oracle RAC and Data Guard deployment.

[Next: Factors to consider.](#)

Factors to consider for Oracle database deployment

[Previous: Solution architecture.](#)

A public cloud provides many choices for compute and storage, and using the correct type of compute instance and storage engine is a good place to start for database deployment. You should also select compute and storage configurations that are optimized for Oracle databases.

The following sections describe the key considerations when deploying Oracle database in an AWS public cloud on an EC2 instance with FSx storage.

VM performance

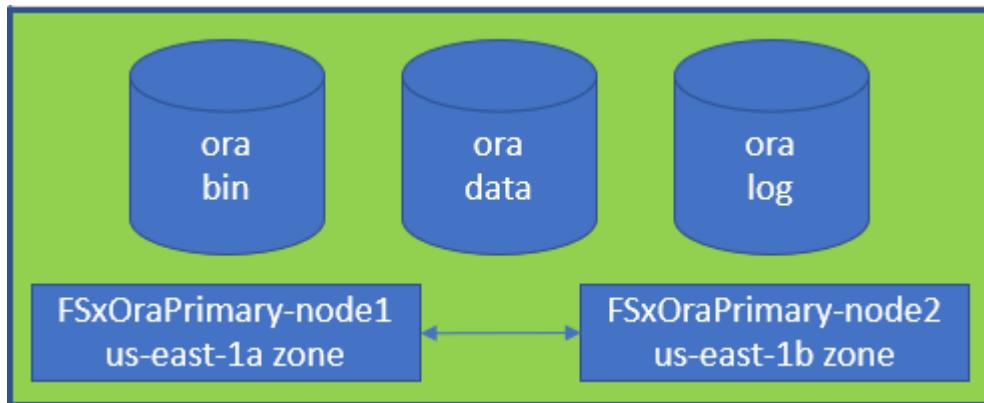
Selecting the right VM size is important for optimal performance of a relational database in a public cloud. For better performance, NetApp recommends using an EC2 M5 Series instance for Oracle deployment, which is optimized for database workloads. The same instance type is also used to power a RDS instance for Oracle by AWS.

- Choose the correct vCPU and RAM combination based on workload characteristics.
- Add swap space to a VM. The default EC2 instance deployment does not create a swap space, which is not optimal for a database.

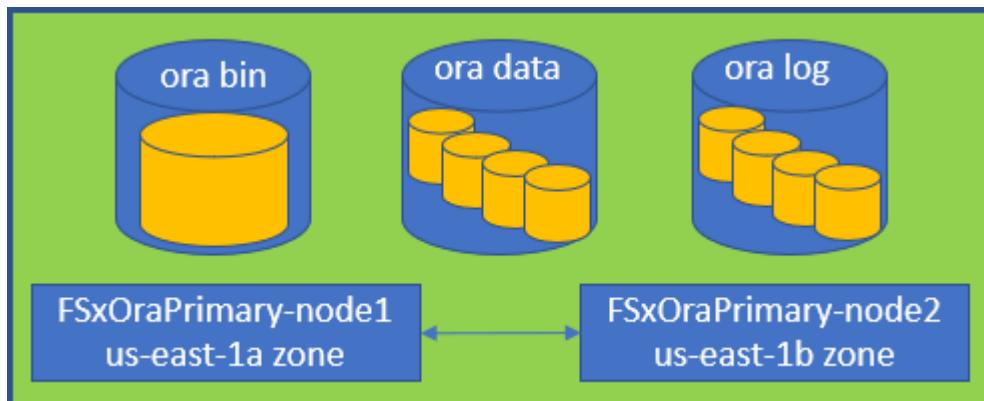
Storage layout and settings

NetApp recommends the following storage layout:

- For NFS storage, the recommended volume layout is three volumes: one for the Oracle binary; one for Oracle data and a duplicate control file; and one for the Oracle active log, archived log, and control file.



- For iSCSI storage, the recommended volume layout is three volumes: one for the Oracle binary; one for Oracle data and a duplicate control file; and one for the Oracle active log, archived log, and control file. However, each data and log volume ideally should contain four LUNs. The LUNs are ideally balanced on the HA cluster nodes.



- For storage IOPS and throughput, you can choose the threshold for provisioned IOPS and throughput for the FSx storage cluster, and these parameters can be adjusted on the fly anytime the workload changes.

- The auto IOPS setting is three IOPS per GiB of allocated storage capacity or user defined storage up to 80,000.
- The throughput level is incremented as follow: 128, 256, 512, 1024, 2045 MBps.

Review the [Amazon FSx for NetApp ONTAP performance](#) documentation when sizing throughput and IOPS.

NFS configuration

Linux, the most common operating system, includes native NFS capabilities. Oracle offers the direct NFS (dNFS) client natively integrated into Oracle. Oracle has supported NFSv3 for over 20 years, and NFSv4 is supported with Oracle 12.1.0.2 and later. Automated Oracle deployment using the NetApp automation toolkit automatically configures dNFS on NFSv3.

Other factors to consider:

- TCP slot tables are the NFS equivalent of host-bus-adapter (HBA) queue depth. These tables control the number of NFS operations that can be outstanding at any one time. The default value is usually 16, which is far too low for optimum performance. The opposite problem occurs on newer Linux kernels, which can automatically increase the TCP slot table limit to a level that saturates the NFS server with requests.

For optimum performance and to prevent performance problems, adjust the kernel parameters that control the TCP slot tables to 128.

```
sysctl -a | grep tcp.*.slot_table
```

- The following table provides recommended NFS mount options for Linux NFSv3 - single instance.

File Type	Mount Options
<ul style="list-style-type: none"> • Control files • Data files • Redo logs 	<code>rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wszie=65536</code>
<ul style="list-style-type: none"> • ORACLE_HOME • ORACLE_BASE 	<code>rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wszie=65536</code>

 Before using dNFS, verify that the patches described in Oracle Doc 1495104.1 are installed. Starting with Oracle 12c, DNFS includes support for NFSv3, NFSv4, and NFSv4.1. NetApp support policies cover v3 and v4 for all clients, but, at the time of writing, NFSv4.1 is not supported for use with Oracle dNFS.

High availability

As indicated in the solution architecture, HA is built on storage-level replication. Therefore, the startup and availability of Oracle is contingent on how quickly the compute and storage can be brought up and recovered. See the following key factors:

- Have a standby compute instance ready and synced up with the primary through Ansible parallel update to both hosts.
- Replicate the binary volume from the primary for standby purposes so that you do not need to install Oracle at the last minute and figure out what needs to be installed and patched.

- Replication frequency dictates how fast the Oracle database can be recovered to make service available. There is a trade off between the replication frequency and storage consumption.
- Leverage automation to make recovery and switch over to standby quick and free of human error. NetApp provides an automation toolkit for this purpose.

[Next: Deployment procedures.](#)

Step-by-Step Oracle Deployment Procedures on AWS EC2 and FSx

[Previous: Solution architecture.](#)

Deploy an EC2 Linux instance for Oracle via EC2 console

If you are new to AWS, you first need to set up an AWS environment. The documentation tab at the AWS website landing page provides EC2 instruction links on how to deploy a Linux EC2 instance that can be used to host your Oracle database via the AWS EC2 console. The following section is a summary of these steps. For details, see the linked AWS EC2-specific documentation.

Setting up your AWS EC2 environment

You must create an AWS account to provision the necessary resources to run your Oracle environment on the EC2 and FSx service. The following AWS documentation provides the necessary details:

- [Set up to use Amazon EC2](#)

Key topics:

- Sign up for AWS.
- Create a key pair.
- Create a security group.

Enabling multiple availability zones in AWS account attributes

For an Oracle high availability configuration as demonstrated in the architecture diagram, you must enable at least four availability zones in a region. The multiple availability zones can also be situated in different regions to meet the required distances for disaster recovery.

The screenshot shows the AWS EC2 Dashboard in the US East (N. Virginia) Region. The left sidebar includes links for New EC2 Experience, EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (with sub-links for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations), Images (AMIs, AMI Catalog), Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), and Network & Security. The main content area displays resource counts: Instances (running) 8, Dedicated Hosts 0, Elastic IPs 5; Instances 12, Key pairs 48, Load balancers 0; Placement groups 25, Security groups 34, Snapshots 0; Volumes 19. A callout box suggests using the AWS Launch Wizard for Microsoft SQL Server Always On availability groups. The Service Health section shows four availability zones: us-east-1a, us-east-1b, us-east-1c, and us-east-1d, each associated with a Zone ID (use1-az6, use1-az1, use1-az2, use1-az4). The right sidebar contains sections for Account attributes (Supported platforms, Default VPC, Settings, EBS encryption, Zones, EC2 Serial Console, Default credit specification, Console experiments), Explore AWS (10 Things You Can Do Today to Reduce AWS Costs, Enable Best Price-Performance with AWS Graviton2, Save Up to 45% on ML Inference), and Additional information.

Creating and connecting to an EC2 instance for hosting Oracle database

See the tutorial [Get started with Amazon EC2 Linux instances](#) for step-by-step deployment procedures and best practices.

Key topics:

- Overview.
- Prerequisites.
- Step 1: Launch an instance.
- Step 2: Connect to your instance.
- Step 3: Clean up your instance.

The following screen shots demonstrate the deployment of an m5-type Linux instance with the EC2 console for running Oracle.

1. From the EC2 dashboard, click the yellow Launch Instance button to start the EC2 instance deployment workflow.

The screenshot shows the AWS EC2 Dashboard. On the left sidebar, there are sections for EC2 Global View, Events, Tags, Instances (with sub-options like Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations), and Images (AMIs). The main content area displays 'Resources' with metrics like Instances (running) at 6, Dedicated Hosts at 0, Elastic IPs at 5, Instances at 12, Key pairs at 48, Load balancers at 0, Placement groups at 25, Security groups at 33, and Volumes at 19. A callout box suggests using the AWS Launch Wizard for SQL Server. To the right, the 'Account attributes' section shows supported platforms (VPC), default VPC (none), settings, EBS encryption, zones, and EC2 Serial Console. An 'Explore AWS' section highlights savings on EC2 with Spot Instances.

2. In Step 1, select "Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-0b0af3577fe5e3532 (64-bit x86) / ami-01fc429821bf1f4b4 (64-bit Arm)."

This screenshot shows the 'Choose an Amazon Machine Image (AMI)' step of the AWS wizard. It lists three options: Amazon RDS (disabled), Red Hat Enterprise Linux 8 (HVM, SSD Volume Type - ami-0b0af3577fe5e3532 (64-bit x86) / ami-01fc429821bf1f4b4 (64-bit Arm)), and SUSE Linux Enterprise Server 15 SP3 (HVM, SSD Volume Type - ami-08895422b5f3aa64a (64-bit x86) / ami-08f182b25f271ef79 (64-bit Arm)). The Red Hat option is selected. The interface includes tabs for 'Choose AMI', 'Choose Instance Type', 'Configure Instance', 'Add Storage', 'Add Tags', 'Configure Security Group', and 'Review'. Buttons for 'Cancel and Exit' and 'Select' are visible.

3. In Step 2, select an m5 instance type with the appropriate CPU and memory allocation based on your Oracle database workload. Click "Next: Configure Instance Details."

This screenshot shows the 'Choose an Instance Type' step of the AWS wizard. It displays a table of m5 instance types with their details. The m5.2xlarge instance is selected. The table includes columns for instance type, CPU, memory, storage, and network. The 'Select' button is located at the bottom right of the table.

	m4	m4.16xlarge	64	256	EBS only	Yes	25 Gigabit	Yes
<input type="checkbox"/>	m5	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	m5	m5.xlarge	4	16	EBS only	Yes	Up to 10 Gigabit	Yes
<input checked="" type="checkbox"/>	m5	m5.2xlarge	8	32	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	m5	m5.4xlarge	16	64	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	m5	m5.8xlarge	32	128	EBS only	Yes	10 Gigabit	Yes
<input type="checkbox"/>	m5	m5.12xlarge	48	192	EBS only	Yes	10 Gigabit	Yes
<input type="checkbox"/>	m5	m5.16xlarge	64	256	EBS only	Yes	20 Gigabit	Yes
<input type="checkbox"/>	m5	m5.24xlarge	96	384	EBS only	Yes	25 Gigabit	Yes
<input type="checkbox"/>	m5	m5.metal	96	384	EBS only	Yes	25 Gigabit	Yes

4. In Step 3, choose the VPC and subnet where the instance should be placed and enable public IP assignment. Click "Next: Add Storage."

Screenshot of the AWS EC2 instance creation wizard Step 3: Configure Instance Details.

No default VPC found. Select another VPC, or create a new default VPC.

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot Instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1

Purchasing option: Request Spot Instances

Network: No default VPC found. Create a new default VPC.

Subnet: 250 IP Addresses available

Auto-assign Public IP: Enable

Hostname type:

DNS Hostname:

- Enable IP name IPv4 (A record) DNS requests
- Enable resource-based IPv4 (A record) DNS requests
- Enable resource-based IPv6 (AAAA record) DNS requests

Placement group: Add instance to placement group

Capacity Reservation:

Domain join directory:

IAM role:

Buttons: Cancel, Previous, **Review and Launch**, Next: Add Storage

5. In Step 4, allocate enough space for the root disk. You may need the space to add a swap. By default, EC2 instance assign zero swap space, which is not optimal for running Oracle.

Screenshot of the AWS EC2 instance creation wizard Step 4: Add Storage.

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-03a3ad00558b4d17c	50	General Purpose SSD (gp2)	150 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Shared file systems

You currently don't have any file systems on this instance. Select "Add file system" button below to add a file system.

Add file system

Buttons: Cancel, Previous, **Review and Launch**, Next: Add Tags

6. In Step 5, add a tag for instance identification if needed.

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. [Learn more about tagging your Amazon EC2 resources.](#)

Key	(128 characters maximum)	Value	(256 characters maximum)
Instances (1) Volumes (1) Network Interfaces (1)			

This resource currently has no tags

Choose the Add tag button or click to add a Name tag.
Make sure your IAM policy includes permissions to create tags.

Add Tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

- In Step 6, select an existing security group or create a new one with the desired inbound and outbound policy for the instance.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a new security group Select an existing security group

Security Group ID	Name	Description	Actions
<input type="checkbox"/> sg-0d746a0908b897c48	AviOccm03112021OCCM1635951256631-OCCMSecurityGroup-B3QFHUHJRUWV	NetApp OCCM Instance External Security Group	Copy to new
<input type="checkbox"/> sg-07b0625cd54aae16	AviOCCM0311OCCM1635943382952-OCCMSecurityGroup-1L8D4QX2SC945	NetApp OCCM Instance External Security Group	Copy to new
<input type="checkbox"/> sg-0618122caef6c50e9	AviOccm1103OCCM163594422113-OCCMSecurityGroup-DX5PHX6CKVKC	NetApp OCCM Instance External Security Group	Copy to new
<input type="checkbox"/> sg-0d53ea8c79897e666	AviOccm1209OCCM1631452667252-OCCMSecurityGroup-T5KVZ1Q4SH48	NetApp OCCM Instance External Security Group	Copy to new
<input type="checkbox"/> sg-0aed9f836b48c52d	AviOccmFSxOCCM1638110371156-OCCMSecurityGroup-N0ENZJW3TVYB	NetApp OCCM Instance External Security Group	Copy to new
<input type="checkbox"/> sg-083a6ea5ca9a12375	connector01OCCM1631455604110-OCCMSecurityGroup-1790QV45PH3ZW	NetApp OCCM Instance External Security Group	Copy to new
<input checked="" type="checkbox"/> sg-08148ca915189ac87	default	default VPC security group	Copy to new
<input type="checkbox"/> sg-07fc527620e3bb22	fsx02OCCM163339531669-OCCMSecurityGroup-1XZYC5WM15NP7	NetApp OCCM Instance External Security Group	Copy to new
<input type="checkbox"/> sg-0f359d2ba38db749f	SG-Version10-0CE6MEs-NetAppExternalSecurityGroup-N8B50KGTK8U	ONTAP Cloud firewall rules for management and data interface	Copy to new

Inbound rules for sg-08148ca915189ac87 (Selected security groups: sg-08148ca915189ac87)

Type (1)	Protocol (1)	Port Range (1)	Source (1)	Description (1)
All traffic	All	All	192.168.1.0/24	
All traffic	All	All	sg-08148ca915189ac87 (default)	

Cancel Previous Review and Launch

- In Step 7, review the instance configuration summary, and click Launch to start instance deployment. You are prompted to create a key pair or select a key pair for access to the instance.

Screenshot of the AWS EC2 Instance Launch Wizard Step 7: Review Instance Launch. The page shows the selected AMI (Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-0b0af3577fe5e3532), Instance Type (m5.2xlarge), and Security Group (default). It also lists inbound rules for the security group. A modal window titled "Select an existing key pair or create a new key pair" is displayed, containing instructions about key pairs, a note about selecting a key pair, a dropdown for choosing a key pair, a dropdown for selecting a key pair, and a checkbox for acknowledging access to the private key file. Buttons for "Cancel" and "Launch Instances" are at the bottom.

- Log into EC2 instance using an SSH key pair. Make changes to your key name and instance IP address as appropriate.

```
ssh -i ora-db1v2.pem ec2-user@54.80.114.77
```

You need to create two EC2 instances as primary and standby Oracle servers in their designated availability

zone as demonstrated in the architecture diagram.

Provision FSx for ONTAP file systems for Oracle database storage

EC2 instance deployment allocates an EBS root volume for the OS. FSx for ONTAP file systems provides Oracle database storage volumes, including the Oracle binary, data, and log volumes. The FSx storage NFS volumes can be either provisioned from the AWS FSx console or from Oracle installation, and configuration automation that allocates the volumes as the user configures in a automation parameter file.

Creating FSx for ONTAP file systems

Referred to this documentation [Managing FSx for ONTAP file systems](#) for creating FSx for ONTAP file systems.

Key considerations:

- SSD storage capacity. Minimum 1024 GiB, maximum 192 TiB.
- Provisioned SSD IOPS. Based on workload requirements, a maximum of 80,000 SSD IOPS per file system.
- Throughput capacity.
- Set administrator fsxadmin/vsadmin password. Required for FSx configuration automation.
- Backup and maintenance. Disable automatic daily backups; database storage backup is executed through SnapCenter scheduling.
- Retrieve the SVM management IP address as well as protocol-specific access addresses from SVM details page. Required for FSx configuration automation.

The screenshot shows the AWS FSx console interface. On the left, there's a sidebar with navigation links: Amazon FSx, File systems, Volumes, Backups, ONTAP (Storage virtual machines), OpenZFS (Snapshots), Windows File Server, Lustre (Data repository tasks), and FSx on Service Quotas. The main area displays the details for a file system named 'fsx (svm-005c6edf027866ca4)'. The 'Summary' tab is selected, showing information like SVM ID (svm-005c6edf027866ca4), SVM name (fsx), UUID (1a07ea1f-7d6e-11ec-97a9-7df96ee2a64a), File system ID (fs-0a51a3f08922224d5), and Resource ARN (arn:aws:fsx:us-east-1:759995470648:storage-virtual-machine/fsx-0a51a3f08922224d5/svm-005c6edf027866ca4). The 'Endpoints' tab is also visible, listing Management DNS name (svm-005c6edf027866ca4.fs-0a51a3f08922224d5.fsx.us-east-1.amazonaws.com), NFS DNS name (svm-005c6edf027866ca4.fs-0a51a3f08922224d5.fsx.us-east-1.amazonaws.com), and iSCSI DNS name (iscsi.svm-005c6edf027866ca4.fs-0a51a3f08922224d5.fsx.us-east-1.amazonaws.com). The 'Management IP address' (198.19.255.68), 'NFS IP address' (198.19.255.68), and 'iSCSI IP addresses' (10.0.1.200, 10.0.0.86) are highlighted with red boxes.

See the following step-by-step procedures for setting up either a primary or standby HA FSx cluster.

1. From the FSx console, click Create File System to start the FSx provision workflow.

2. Select Amazon FSx for NetApp ONTAP. Then click Next.

Select file system type

File system options

- Amazon FSx for NetApp ONTAP
- Amazon FSx for OpenZFS
- Amazon FSx for Windows File Server
- Amazon FSx for Lustre

Amazon FSx for NetApp ONTAP

Amazon FSx for NetApp ONTAP provides feature-rich, high-performance, and highly-reliable storage built on NetApp's popular ONTAP file system and fully managed by AWS.

- Broadly accessible from Linux, Windows, and macOS compute instances and containers (running on AWS or on-premises) via industry-standard NFS, SMB, and iSCSI protocols.
- Provides ONTAP's popular data management capabilities like Snapshots, SnapMirror (for data replication), FlexClone (for data cloning), and data compression / deduplication.
- Delivers hundreds of thousands of IOPS with consistent sub-millisecond latencies, and up to 3 GB/s of throughput.
- Offers highly-available and highly-durable multi-AZ SSD storage with support for cross-region replication and built-in, fully managed backups.
- Automatically tiers infrequently-accessed data to capacity pool storage, a fully elastic storage tier that can scale to petabytes in size and is cost-optimized for infrequently-accessed data.
- Integrates with Microsoft Active Directory (AD) to support Windows-based environments and enterprises.

Cancel

Next

3. Select Standard Create and, in File System Details, name your file system, Multi-AZ HA. Based on your database workload, choose either Automatic or User-Provisioned IOPS up to 80,000 SSD IOPS. FSx storage comes with up to 2TiB NVMe caching at the backend that can deliver even higher measured IOPS.

File system details

File system name - optional [Info](#)

aws_ora_prod

Maximum of 256 Unicode letters, whitespace, and numbers, plus + - = . _ : /

Deployment type [Info](#)

Multi-AZ

Single-AZ

SSD storage capacity [Info](#)

1024

Minimum 1024 GiB; Maximum 192 TiB.

Provisioned SSD IOPS

Amazon FSx provides 3 IOPS per GiB of storage capacity. You can also provision additional SSD IOPS as needed.

Automatic (3 IOPS per GiB of SSD storage)

User-provisioned

40000

Maximum 80,000 IOPS

Throughput capacity [Info](#)

The sustained speed at which the file server hosting your file system can serve data. The file server can also burst to higher speeds for periods of time.

Recommended throughput capacity

128 MB/s

Specify throughput capacity

Throughput capacity

512 MB/s



4. In the Network & Security section, select the VPC, security group, and subnets. These should be created before FSx deployment. Based on the role of the FSx cluster (primary or standby), place the FSx storage nodes in the appropriate zones.

Network & security

Virtual Private Cloud (VPC) [Info](#)

Specify the VPC from which your file system is accessible.

vpc-0474064fc537e5182



VPC Security Groups [Info](#)

Specify VPC Security Groups to associate with your file system's network interfaces.

Choose VPC security group(s)



sg-08148ca915189ac87 (default)

Preferred subnet [Info](#)

Specify the preferred subnet for your file system.

subnet-08c952541f4ab282d (us-east-1a)



Standby subnet

subnet-0a84d6eeeb0f4e5c0 (us-east-1b)



VPC route tables

Specify the VPC route tables associated with your file system.

VPC's default route table

Select one or more VPC route tables

Endpoint IP address range

Specify the IP address range in which the endpoints to access your file system will be created

No preference

Select an IP address range

5. In the Security & Encryption section, accept the default, and enter the fsxadmin password.

Security & encryption

Encryption key [Info](#)

AWS Key Management Service (KMS) encryption key that protects your file system data at rest.

aws/fsx (default)



Description	Account	KMS key ID
Default master key that protects my FSx resources when no other key is defined	759995470648	5b31feff-6759-4306-a852-9c99a743982a

File system administrative password

Password for this file system's "fsxadmin" user, which you can use to access the ONTAP CLI or REST API.

Don't specify a password

Specify a password

Password

Confirm password

6. Enter the SVM name and the vsadmin password.

Default storage virtual machine configuration

Storage virtual machine name

SVM administrative password
Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.

Don't specify a password
 Specify a password
Password

Confirm password

Active Directory
Joining an Active Directory enables access from Windows and MacOS clients over the SMB protocol.

Do not join an Active Directory
 Join an Active Directory

7. Leave the volume configuration blank; you do not need to create a volume at this point.

Default volume configuration

Volume name

vol1

Maximum of 203 alphanumeric characters, plus _.

Junction path

/vol1

The location within your file system where your volume will be mounted.

Volume size

1024

Minimum 20 MiB; Maximum 104857600 MiB

Storage efficiency

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

- Enabled (recommended)
 Disabled

Capacity pool tiering policy

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.

Auto



► Backup and maintenance - *optional*

► Tags - *optional*

Cancel

Back

Next

8. Review the Summary page, and click Create File System to complete FSx file system provision.

Screenshot of the AWS FSx Create file system wizard - Step 3: Review and create.

Summary
Verify the following attributes before proceeding

Attribute	Value	Editable after creation
File system type	Amazon FSx for NetApp ONTAP	
File system name	aws_ora_prod	✓
Deployment type	Multi-AZ	
Storage type	SSD	
SSD storage capacity	1,024 GiB	✓
Minimum SSD IOPS	40000 IOPS	✓
Throughput capacity	512 MB/s	✓
Virtual Private Cloud (VPC)	vpc-0474064fc537e5182	
VPC Security Groups	sg-08148ca915189ac87	✓
Preferred subnet	subnet-08c952541f4ab282d	
Standby subnet	subnet-0a84d6eeeb0f4e5c0	
VPC route tables	VPC's default route table	
Endpoint IP address range	No preference	
KMS key ID	arn:aws:kms:us-east-1:759995470648:key/5b31feff-6759-4306-a852-9c99a743982a	
Daily automatic backup window	No preference	✓
Automatic backup	7 day(s)	✓

Provisioning of database volumes for Oracle database

See [Managing FSx for ONTAP volumes - creating a volume](#) for details.

Key considerations:

- Sizing the database volumes appropriately.
- Disabling capacity pool tiering policy for performance configuration.
- Enabling Oracle dNFS for NFS storage volumes.
- Setting up multipath for iSCSI storage volumes.

Create database volume from FSx console

From the AWS FSx console, you can create three volumes for Oracle database file storage: one for the Oracle binary, one for the Oracle data, and one for the Oracle log. Make sure that volume naming matches the Oracle host name (defined in the hosts file in the automation toolkit) for proper identification. In this example, we use db1 as the EC2 Oracle host name instead of a typical IP-address-based host name for an EC2 instance.

Create volume

X

File system

ONTAP | fs-0a51a3f08922224d5 | rdscustomfs007



Storage virtual machine

svm-005c6edf027866ca4 | fsx



Volume name

db1_bin

Maximum of 203 alphanumeric characters, plus _.

Junction path

/db1_bin

The location within your file system where your volume will be mounted.

Volume size

51200

Minimum 20 MiB; Maximum 104857600 MiB

Storage efficiency

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

- Enabled (recommended)
- Disabled

Capacity pool tiering policy

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.

None



Cancel

Confirm

Create volume

X

File system

ONTAP | fs-0a51a3f08922224d5 | rdscustomfs007



Storage virtual machine

svm-005c6edf027866ca4 | fsx



Volume name

db1_data

Maximum of 203 alphanumeric characters, plus _.

Junction path

/db1_data

The location within your file system where your volume will be mounted.

Volume size

512000

Minimum 20 MiB; Maximum 104857600 MiB

Storage efficiency

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

- Enabled (recommended)
- Disabled

Capacity pool tiering policy

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.

None



Cancel

Confirm

Create volume

File system

ONTAP | fs-0a51a3f08922224d5 | rdscustomfs007

Storage virtual machine

svm-005c6edf027866ca4 | fsx

Volume name

db1_log

Maximum of 203 alphanumeric characters, plus _.

Junction path

/db1_log

The location within your file system where your volume will be mounted.

Volume size

256000

Minimum 20 MiB; Maximum 104857600 MiB

Storage efficiency

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

Enabled (recommended)

Disabled

Capacity pool tiering policy

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.

None

Cancel **Confirm**



Creating iSCSI LUNs is not currently supported by the FSx console. For iSCSI LUNs deployment for Oracle, the volumes and LUNs can be created by using automation for ONTAP with the NetApp Automation Toolkit.

Install and configure Oracle on an EC2 instance with FSx database volumes

The NetApp automation team provide an automation kit to run Oracle installation and configuration on EC2 instances according to best practices. The current version of the automation kit supports Oracle 19c on NFS with the default RU patch 19.8. The automation kit can be easily adapted for other RU patches if needed.

Prepare a Ansible controller to run automation

Follow the instruction in the section "[Creating and connecting to an EC2 instance for hosting Oracle database](#)" to provision a small EC2 Linux instance to run the Ansible controller. Rather than using RedHat, Amazon Linux t2.large with 2vCPU and 8G RAM should be sufficient.

Retrieve NetApp Oracle deployment automation toolkit

Log into the EC2 Ansible controller instance provisioned from step 1 as ec2-user and from the ec2-user home directory, execute the `git clone` command to clone a copy of the automation code.

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

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

Execute automated Oracle 19c deployment using automation toolkit

See these detailed instruction [CLI deployment Oracle 19c Database](#) to deploy Oracle 19c with CLI automation. There is a small change in command syntax for playbook execution because you are using an SSH key pair instead of a password for host access authentication. The following list is a high level summary:

1. By default, an EC2 instance uses an SSH key pair for access authentication. From Ansible controller automation root directories `/home/ec2-user/na_oracle19c_deploy`, and `/home/ec2-user/na_rds_fsx_oranfs_config`, make a copy of the SSH key `accesststkey.pem` for the Oracle host deployed in the step "[Creating and connecting to an EC2 instance for hosting Oracle database](#)".
2. Log into the EC2 instance DB host as ec2-user, and install the python3 library.

```
sudo yum install python3
```

3. Create a 16G swap space from the root disk drive. By default, an EC2 instance creates zero swap space. Follow this AWS documentation: [How do I allocate memory to work as swap space in an Amazon EC2 instance by using a swap file?](#).
4. Return to the Ansible controller (`cd /home/ec2-user/na_rds_fsx_oranfs_config`), and execute the preclone playbook with the appropriate requirements and `linux_config` tags.

```
ansible-playbook -i hosts rds_preclone_config.yml -u ec2-user --private
-key accesststkey.pem -e @vars/fsx_vars.yml -t requirements_config
```

```
ansible-playbook -i hosts rds_preclone_config.yml -u ec2-user --private
-key accesststkey.pem -e @vars/fsx_vars.yml -t linux_config
```

5. Switch to the `/home/ec2-user/na_oracle19c_deploy-master` directory, read the README file, and populate the `global vars.yml` file with the relevant global parameters.

6. Populate the `host_name.yml` file with the relevant parameters in the `host_vars` directory.
7. Execute the playbook for Linux, and press Enter when prompted for the `vsadmin` password.

```
ansible-playbook -i hosts all_playbook.yml -u ec2-user --private-key  
accesststkey.pem -t linux_config -e @vars/vars.yml
```

8. Execute the playbook for Oracle, and press enter when prompted for the `vsadmin` password.

```
ansible-playbook -i hosts all_playbook.yml -u ec2-user --private-key  
accesststkey.pem -t oracle_config -e @vars/vars.yml
```

Change the permission bit on the SSH key file to 400 if needed. Change the Oracle host (`ansible_host` in the `host_vars` file) IP address to your EC2 instance public address.

Setting up SnapMirror between primary and standby FSx HA cluster

For high availability and disaster recovery, you can set up SnapMirror replication between the primary and standby FSx storage cluster. Unlike other cloud storage services, FSx enables a user to control and manage storage replication at a desired frequency and replication throughput. It also enables users to test HA/DR without any effect on availability.

The following steps show how to set up replication between a primary and standby FSx storage cluster.

1. Setup primary and standby cluster peering. Log into the primary cluster as the `fsxadmin` user and execute the following command. This reciprocal create process executes the `create` command on both the primary cluster and the standby cluster. Replace `standby_cluster_name` with the appropriate name for your environment.

```
cluster peer create -peer-addrs  
standby_cluster_name,inter_cluster_ip_address -username fsxadmin  
-initial-allowed-vserver-peers *
```

2. Set up vServer peering between the primary and standby cluster. Log into the primary cluster as the `vsadmin` user and execute the following command. Replace `primary_vserver_name`, `standby_vserver_name`, `standby_cluster_name` with the appropriate names for your environment.

```
vserver peer create -vserver primary_vserver_name -peer-vserver  
standby_vserver_name -peer-cluster standby_cluster_name -applications  
snapmirror
```

3. Verify that the cluster and vserver peerings are set up correctly.

```

FsxId00164454fac5591e6::> cluster peer show
Peer Cluster Name          Cluster Serial Number Availability  Authentication
-----
FsxId0b6a95149d07aa82e    1-80-000011           Available      ok

FsxId00164454fac5591e6::> vserver peer show
      Peer      Peer          Peering      Remote
Vserver   Vserver   State     Peer Cluster Applications  Vserver
-----
svm_FsxEraSource
      svm_FsxEraTarget
                  peered      FsxId0b6a95149d07aa82e
                                         snapmirror      svm_FsxEraTarget

FsxId00164454fac5591e6::>

```

4. Create target NFS volumes at the standby FSx cluster for each source volume at the primary FSx cluster. Replace the volume name as appropriate for your environment.

```

vol create -volume dr_db1_bin -aggregate aggr1 -size 50G -state online
-policy default -type DP

```

```

vol create -volume dr_db1_data -aggregate aggr1 -size 500G -state online
-policy default -type DP

```

```

vol create -volume dr_db1_log -aggregate aggr1 -size 250G -state online
-policy default -type DP

```

5. You can also create iSCSI volumes and LUNs for the Oracle binary, Oracle data, and the Oracle log if the iSCSI protocol is employed for data access. Leave approximately 10% free space in the volumes for snapshots.

```

vol create -volume dr_db1_bin -aggregate aggr1 -size 50G -state online
-policy default -unix-permissions ---rwxr-xr-x -type RW

```

```

lun create -path /vol/dr_db1_bin/dr_db1_bin_01 -size 45G -ostype linux

```

```

vol create -volume dr_db1_data -aggregate aggr1 -size 500G -state online
-policy default -unix-permissions ---rwxr-xr-x -type RW

```

```

lun create -path /vol/dr_db1_data/dr_db1_data_01 -size 100G -ostype
linux

```

```
lun create -path /vol/dr_db1_data/dr_db1_data_02 -size 100G -ostype  
linux
```

```
lun create -path /vol/dr_db1_data/dr_db1_data_03 -size 100G -ostype  
linux
```

```
lun create -path /vol/dr_db1_data/dr_db1_data_04 -size 100G -ostype  
linux
```

```
vol create -volume dr_db1_log -aggregate aggr1 -size 250G -state online -policy default -unix-permissions  
---rwxr-xr-x -type RW
```

```
lun create -path /vol/dr_db1_log/dr_db1_log_01 -size 45G -ostype linux
```

```
lun create -path /vol/dr_db1_log/dr_db1_log_02 -size 45G -ostype linux
```

```
lun create -path /vol/dr_db1_log/dr_db1_log_03 -size 45G -ostype linux
```

```
lun create -path /vol/dr_db1_log/dr_db1_log_04 -size 45G -ostype linux
```

6. For iSCSI LUNs, create mapping for the Oracle host initiator for each LUN, using the binary LUN as an example. Replace the igroup with an appropriate name for your environment, and increment the lun-id for each additional LUN.

```
lun mapping create -path /vol/dr_db1_bin/dr_db1_bin_01 -igroup ip-10-0-  
1-136 -lun-id 0
```

```
lun mapping create -path /vol/dr_db1_data/dr_db1_data_01 -igroup ip-10-  
0-1-136 -lun-id 1
```

7. Create a SnapMirror relationship between the primary and standby database volumes. Replace the appropriate SVM name for your environment.s

```
snapmirror create -source-path svm_FSxOraSource:db1_bin -destination  
-path svm_FSxOraTarget:dr_db1_bin -vserver svm_FSxOraTarget -throttle  
unlimited -identity-preserve false -policy MirrorAllSnapshots -type DP
```

```
snapmirror create -source-path svm_FSxOraSource:db1_data -destination  
-path svm_FSxOraTarget:dr_db1_data -vserver svm_FSxOraTarget -throttle  
unlimited -identity-preserve false -policy MirrorAllSnapshots -type DP
```

```
snapmirror create -source-path svm_FSxOraSource:db1_log -destination  
-path svm_FSxOraTarget:dr_db1_log -vserver svm_FSxOraTarget -throttle  
unlimited -identity-preserve false -policy MirrorAllSnapshots -type DP
```

This SnapMirror setup can be automated with a NetApp Automation Toolkit for NFS database volumes. The toolkit is available for download from the NetApp public GitHub site.

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

Read the README instructions carefully before attempting setup and failover testing.



Replicating the Oracle binary from the primary to a standby cluster might have Oracle license implications. Contact your Oracle license representative for clarification. The alternative is to have Oracle installed and configured at the time of recovery and failover.

SnapCenter Deployment

SnapCenter installation

Follow [Installing the SnapCenter Server](#) to install SnapCenter server. This documentation covers how to install a standalone SnapCenter server. A SaaS version of SnapCenter is in beta review and could be available shortly. Check with your NetApp representative for availability if needed.

Configure SnapCenter plugin for EC2 Oracle host

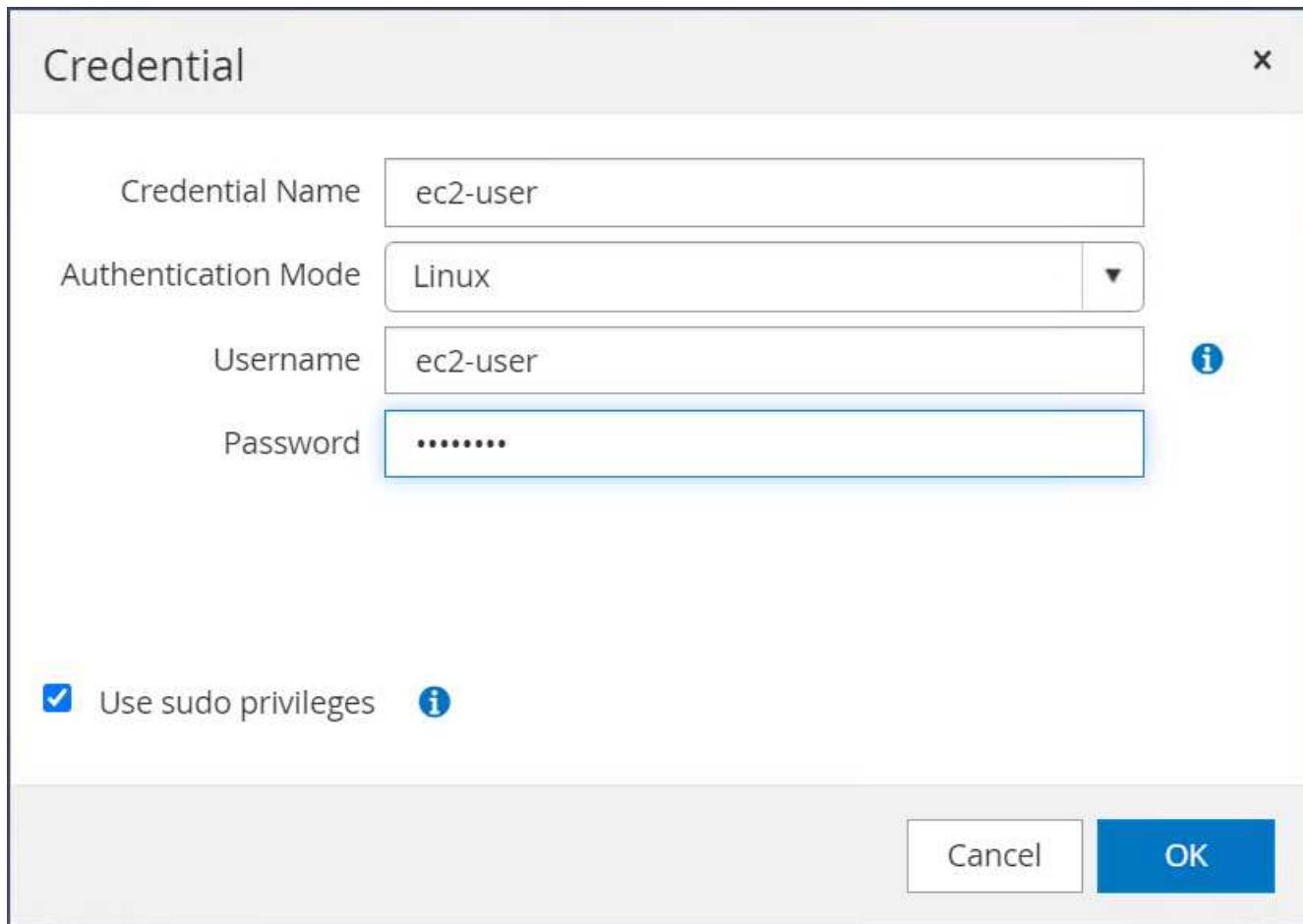
1. After automated SnapCenter installation, log into SnapCenter as an administrative user for the Window host on which the SnapCenter server is installed.



- From the left-side menu, click Settings, and then Credential and New to add ec2-user credentials for SnapCenter plugin installation.

Credential Name	Authentication Mode	Details
244rdscustomdb	SQL	UserId:admin
42rdscustomdb	SQL	UserId:admin
admin	SQL	UserId:admin
administrator	Windows	UserId:administrator
ec2-user	Linux	UserId:ec2-user
onpremSQL	Windows	UserId:rdscustomval\administrator
rdsdb2	Windows	UserId:administrator
rdsdb244	Windows	UserId:administrator
rdssql	Windows	UserId:administrator
tst244	SQL	UserId:admin
tstcredfordemo	Windows	UserId:administrator

- Reset the ec2-user password and enable password SSH authentication by editing the `/etc/ssh/sshd_config` file on the EC2 instance host.
- Verify that the "Use sudo privileges" checkbox is selected. You just reset the ec2-user password in the previous step.



5. Add the SnapCenter server name and the IP address to the EC2 instance host file for name resolution.

```
[ec2-user@ip-10-0-0-151 ~]$ sudo vi /etc/hosts
[ec2-user@ip-10-0-0-151 ~]$ cat /etc/hosts
127.0.0.1    localhost localhost.localdomain localhost4
localhost4.localdomain4
::1          localhost localhost.localdomain localhost6
localhost6.localdomain6
10.0.1.233   rdscustomvalsc.rdscustomval.com rdscustomvalsc
```

6. On the SnapCenter server Windows host, add the EC2 instance host IP address to the Windows host file C:\Windows\System32\drivers\etc\hosts.

```
10.0.0.151      ip-10-0-0-151.ec2.internal
```

7. In the left-side menu, select Hosts > Managed Hosts, and then click Add to add the EC2 instance host to SnapCenter.

The screenshot shows the NetApp SnapCenter interface. The left sidebar has a 'Hosts' icon highlighted. The main area is titled 'Managed Hosts' and lists two hosts:

	Name	Type	System	Plug-in	Version	Overall Status
<input type="checkbox"/>	RDSAMA7-VJ0DQK0	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Host down
<input type="checkbox"/>	rdscustommssql1.rdscustomval.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running

Check Oracle Database, and, before you submit, click More Options.

The screenshot shows the 'Add Host' dialog box. It includes fields for Host Type (Linux), Host Name (10.0.0.151), and Credentials (ec2-user). Below the form is a section for selecting plug-ins:

Select Plug-ins to Install SnapCenter Plug-Ins Package 4.5 P2 for Linux

Oracle Database
 SAP HANA

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

At the bottom are 'Submit' and 'Cancel' buttons.

Check Skip Preinstall Checks. Confirm Skipping Preinstall Checks, and then click Submit After Save.

More Options

Port	8145	
Installation Path	/opt/NetApp/snapcenter	
<input checked="" type="checkbox"/> Skip preinstall checks		
Custom Plug-ins Choose a File <input type="button" value="Browse"/> <input type="button" value="Upload"/> <div style="border: 1px solid #ccc; padding: 5px; height: 40px; margin-top: 10px;">No plug-ins found.</div>		
<input type="button" value="Save"/>		<input type="button" value="Cancel"/>

You are prompted with Confirm Fingerprint, and then click Confirm and Submit.

Confirm Fingerprint

Authenticity of the host cannot be determined			
Host name		Fingerprint	Valid
ip-10-0-0-151.ec2.internal		ssh-rsa 2048 97:6F:3C:7D:38:42:F6:54:B7:AF:E3:61:61:BA:2E:6F	
<input type="button" value="Confirm and Submit"/> <input type="button" value="Close"/>			

After successful plugin configuration, the managed host's overall status show as Running.

Managed Hosts							
		Disks	Shares	Initiator Groups	ISCSI Session		
Search by Name						Add	Remove
<input type="checkbox"/>	Name		Type	System	Plug-in	Version	Overall Status
<input type="checkbox"/>	ip-10-0-0-151.ec2.internal		Linux	Stand-alone	UNIX, Oracle Database	4.5	Running

Configure backup policy for Oracle database

Refer to this section [Setup database backup policy in SnapCenter](#) for details on configuring the Oracle database backup policy.

Generally you need create a policy for the full snapshot Oracle database backup and a policy for the Oracle archive-log-only snapshot backup.



You can enable Oracle archive log pruning in the backup policy to control log-archive space. Check "Update SnapMirror after creating a local Snapshot copy" in "Select secondary replication option" as you need to replicate to a standby location for HA or DR.

Configure Oracle database backup and scheduling

Database backup in SnapCenter is user configurable and can be set up either individually or as a group in a resource group. The backup interval depends on the RTO and RPO objectives. NetApp recommends that you run a full database backup every few hours and archive the log backup at a higher frequency such as 10-15 mins for quick recovery.

Refer to the Oracle section of [Implement backup policy to protect database](#) for a detailed step-by-step processes for implementing the backup policy created in the section [Configure backup policy for Oracle database](#) and for backup job scheduling.

The following image provides an example of the resources groups that are set up to back up an Oracle database.

A screenshot of the NetApp SnapCenter UI. The top navigation bar shows 'NetApp SnapCenter®', the user 'rdscustomval/administrator', and 'SnapCenter/Admin'. The left sidebar includes links for Dashboard, Resources (selected), Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main content area is titled 'Oracle Database' with a dropdown menu. A search bar contains 'Search databases'. Below is a table with the following data:

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
ORCL	Single Instance	ip-10-0-0-151.ec2.internal	orcl_full_bkup orcl_log_bkup	Oracle full backup Oracle log backup	03/24/2022 8:40:08 PM	Backup succeeded

[Next: Database management.](#)

EC2 and FSx Oracle database management

[Previous: Deployment procedures.](#)

In addition to the AWS EC2 and FSx management console, the Ansible control node and the SnapCenter UI tool are deployed for database management in this Oracle environment.

An Ansible control node can be used to manage Oracle environment configuration, with parallel updates that keep primary and standby instances in sync for kernel or patch updates. Failover, resync, and fallback can be automated with the NetApp Automation Toolkit to archive fast application recovery and availability with Ansible. Some repeatable database management tasks can be executed using a playbook to reduce human errors.

The SnapCenter UI tool can perform database snapshot backup, point-in-time recovery, database cloning, and so on with the SnapCenter plugin for Oracle databases. For more information about Oracle plugin features, see the [SnapCenter Plug-in for Oracle Database overview](#).

The following sections provide details on how key functions of Oracle database management are fulfilled with the SnapCenter UI:

- Database snapshot backups
- Database point-in-time restore
- Database clone creation

Database cloning creates a replica of a primary database on a separate EC2 host for data recovery in the event of logical data error or corruption, and clones can also be used for application testing, debugging, patch validation, and so on.

Taking a snapshot

An EC2/FSx Oracle database is regularly backed up at intervals configured by the user. A user can also take a one-off snapshot backup at any time. This applies to both full-database snapshot backups as well as archive-log-only snapshot backups.

Taking a full database snapshot

A full database snapshot includes all Oracle files, including data files, control files, and archive log files.

1. Log into the SnapCenter UI and click Resources in the left-side menu. From the View dropdown, change to the Resource Group view.

Name	Resources	Tags	Policies
ordl_full_bkup	1	ora_fullbkup	Oracle full backup
ordl_log_bkup	1	ora_logbkup	Oracle log backup

2. Click the full backup resource name, and then click the Backup Now icon to initiate an add-hoc backup.

Name	Resource Name	Type	Host
ordl_full_bkup	ORCL	Oracle Database	ip-10-0-0-151.ec2.internal
ordl_log_bkup			

3. Click Backup and then confirm the backup to start a full database backup.



From the Resource view for the database, open the database Managed Backup Copies page to verify that the one-off backup completed successfully. A full database backup creates two snapshots: one for the data volume and one for the log volume.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
[p-10-0-0-151_03-25-2022_00.34.20.4541.1]	1	Log	03/25/2022 12:34:37 AM	Not Applicable	False	Not Cataloged	1733264
[p-10-0-0-151_03-25-2022_00.34.20.4541.0]	1	Data	03/25/2022 12:34:31 AM	Unverified	False	Not Cataloged	1733220

Taking an archive log snapshot

An archive log snapshot is only taken for the Oracle archive log volume.

1. Log into the SnapCenter UI and click the Resources tab in the left-side menu bar. From the View dropdown, change to the Resource Group view.

The screenshot shows the NetApp SnapCenter interface. On the left is a navigation 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 'View' dropdown is set to 'Resource Group' and a search bar says 'Search resource group'. A table lists two resources: 'ordl_full_bkup' and 'ordl_log_bkup'. Both have a count of 1 and are associated with tags 'ora_fullbkup' and 'ora_logbkup' respectively. Policies for both are listed as 'Oracle full backup' and 'Oracle log backup'.

2. Click the log backup resource name, and then click the Backup Now icon to initiate an add-hoc backup for archive logs.

This screenshot shows the 'ordl_log_bkup Details' page. The left sidebar shows the resource group 'ordl_log_bkup' is selected. The main table displays the following details:

Name	Resource Name	Type	Host
ordl_log_bkup	ORCL	Oracle Database	ip-10-0-0-151.ec2.internal

On the right, there are buttons for 'Modify Resource Group', 'Backup Now' (highlighted in yellow), 'Maintenance', and 'Delete'.

3. Click Backup and then confirm the backup to start an archive log backup.

This screenshot shows a 'Backup' dialog box. It asks 'Create a backup for the selected resource group'. The 'Resource Group' field contains 'ordl_log_bkup'. The 'Policy' field is set to 'Oracle log backup'. At the bottom are 'Cancel' and 'Backup' buttons.

From the Resource view for the database, open the database Managed Backup Copies page to verify that the one-off archive log backup completed successfully. An archive log backup creates one snapshot for the log volume.

The screenshot shows the NetApp SnapCenter interface for an Oracle Database named ORCL. The left sidebar has a 'Resources' section with 'Database' selected. The main area shows 'ORCL Topology' with a summary card indicating 27 Backups, 2 Data Backups, 25 Log Backups, and 0 Clones. Below this is a 'Primary Backup(s)' table:

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
ip-10-0-0-151_03-25-2022_01:59:38.0733_1	1	Log	03/25/2022 1:59:46 AM	Not Applicable	False	Not Cataloged	1739201

Restoring to a point in time

SnapCenter-based restore to a point in time is executed on the same EC2 instance host. Complete the following steps to perform the restore:

1. From the SnapCenter Resources tab > Database view, click the database name to open the database backup.

The screenshot shows the NetApp SnapCenter interface with the 'Resources' tab selected. Under 'View', 'Database' is chosen. A table lists the database 'ORCL' with the following details:

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
ORCL	Single Instance	ip-10-0-0-151.ec2.internal	ord_full_bkup ord_log_bkup	Oracle full backup Oracle log backup	03/25/2022 1:10:09 PM	Backup succeeded

2. Select the database backup copy and the desired point in time to be restored. Also mark down the corresponding SCN number for the point in time. The point-in-time restore can be performed using either the time or the SCN.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
ip-10-0-0-151_03-25-2022_12.40.01.1098_1	1	Log	03/25/2022 12:40:09 PM	Not Applicable	False	Not Cataloged	1784293
ip-10-0-0-151_03-25-2022_12.25.01.0080_1	1	Log	03/25/2022 12:25:09 PM	Not Applicable	False	Not Cataloged	1783383
ip-10-0-0-151_03-25-2022_12.10.01.1097_1	1	Log	03/25/2022 12:10:09 PM	Not Applicable	False	Not Cataloged	1782417
ip-10-0-0-151_03-25-2022_11.55.01.0500_1	1	Log	03/25/2022 11:55:09 AM	Not Applicable	False	Not Cataloged	1781160
ip-10-0-0-151_03-25-2022_11.40.01.0323_1	1	Log	03/25/2022 11:40:09 AM	Not Applicable	False	Not Cataloged	1780268
ip-10-0-0-151_03-25-2022_11.25.01.0430_1	1	Log	03/25/2022 11:25:09 AM	Not Applicable	False	Not Cataloged	1779368
ip-10-0-0-151_03-25-2022_11.15.01.1503_1	1	Log	03/25/2022 11:15:17 AM	Not Applicable	False	Not Cataloged	1778546
ip-10-0-0-151_03-25-2022_11.15.01.1503_0	1	Data	03/25/2022 11:15:11 AM	Unverified	False	Not Cataloged	1778504
ip-10-0-0-151_03-25-2022_11.10.01.1834_1	1	Log	03/25/2022 11:10:09 AM	Not Applicable	False	Not Cataloged	1778184

3. Highlight the log volume snapshot and click the Mount button to mount the volume.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
ip-10-0-0-151_03-25-2022_12.40.01.1098_1	1	Log	03/25/2022 12:40:09 PM	Not Applicable	False	Not Cataloged	1784293
ip-10-0-0-151_03-25-2022_12.25.01.0080_1	1	Log	03/25/2022 12:25:09 PM	Not Applicable	False	Not Cataloged	1783383
ip-10-0-0-151_03-25-2022_12.10.01.1097_1	1	Log	03/25/2022 12:10:09 PM	Not Applicable	False	Not Cataloged	1782417
ip-10-0-0-151_03-25-2022_11.55.01.0500_1	1	Log	03/25/2022 11:55:09 AM	Not Applicable	False	Not Cataloged	1781160
ip-10-0-0-151_03-25-2022_11.40.01.0323_1	1	Log	03/25/2022 11:40:09 AM	Not Applicable	False	Not Cataloged	1780268
ip-10-0-0-151_03-25-2022_11.25.01.0430_1	1	Log	03/25/2022 11:25:09 AM	Not Applicable	False	Not Cataloged	1779368
ip-10-0-0-151_03-25-2022_11.15.01.1503_1	1	Log	03/25/2022 11:15:17 AM	Not Applicable	False	Not Cataloged	1778546
ip-10-0-0-151_03-25-2022_11.15.01.1503_0	1	Data	03/25/2022 11:15:11 AM	Unverified	False	Not Cataloged	1778504
ip-10-0-0-151_03-25-2022_11.10.01.1834_1	1	Log	03/25/2022 11:10:09 AM	Not Applicable	False	Not Cataloged	1778184

4. Choose the primary EC2 instance to mount the log volume.



5. Verify that the mount job completes successfully. Also check on the EC2 instance host to see that log volume mounted and also the mount point path.

```
[root@ip-10-0-0-151 ec2-user]# df -h
Filesystem      Size  Used Avail Mounted on
/devtmpfs        7.6G   0    7.6G  0% /dev
tmpfs           1.6G  7.0G  8.3G  46% /dev/shm
tmpfs           7.7G  604K  7.6G  1% /run
tmpfs           7.7G   0    7.7G  0% /sys/fs/cgroup
/dev/nvme0n1p1   9.8G  5.4G  4.3G  56% /
198.19.255.68:/ora_nfs_log  48G  95M  48G  1% /ora_nfs_log
198.19.255.68:/ora_nfs_data  48G  3.4G  45G  8% /ora_nfs_data
/dev/mapper/bdata01-lvdbdata01  40G  471M  38G  2% /rdsdbdata
/dev/nvme5n1     25G   12G  13G  49% /rdsdbbin
tmpfs           1.6G   0    1.6G  0% /run/user/61001
tmpfs           1.6G   0    1.6G  0% /run/user/61005
198.19.255.68:/Scef91c793-5583-480d-9a34-6275dab17f5b  48G  91M  48G  1% /var/opt/snapcenter/sco/backup_mount/ip-10-0-0-151_03-25-2022_11.15.01.1503_1/ORCL/
[root@ip-10-0-0-151 ec2-user]#
```

6. Copy the archive logs from the mounted log volume to the current archive log directory.

```
[ec2-user@ip-10-0-0-151 ~]$ cp /var/opt/snapcenter/sco/backup_mount/ip-10-0-0-151_03-25-2022_11.15.01.1503_1/ORCL/1/db/ORCL_A/arch/*.arc /ora_nfs_log/db/ORCL_A/arch/
```

7. Return to the SnapCenter Resource tab > database backup page, highlight the data snapshot copy, and click the Restore button to start the database restore workflow.

Manage Copies

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
ip-10-0-0-151_03-25-2022_12.10.01.1097_1	1	Log	03/25/2022 12:10:09 PM	Not Applicable	False	Not Cataloged	1782417
ip-10-0-0-151_03-25-2022_11.55.01.0500_1	1	Log	03/25/2022 11:55:09 AM	Not Applicable	False	Not Cataloged	1781160
ip-10-0-0-151_03-25-2022_11.40.01.0323_1	1	Log	03/25/2022 11:40:09 AM	Not Applicable	False	Not Cataloged	1780268
ip-10-0-0-151_03-25-2022_11.25.01.0430_1	1	Log	03/25/2022 11:25:09 AM	Not Applicable	False	Not Cataloged	1779368
ip-10-0-0-151_03-25-2022_11.15.01.1503_1	1	Log	03/25/2022 11:15:17 AM	Not Applicable	True	Not Cataloged	1778546
ip-10-0-0-151_03-25-2022_11.15.01.1503_0	1	Data	03/25/2022 11:15:11 AM	Unverified	False	Not Cataloged	1778504
ip-10-0-0-151_03-25-2022_11.10.01.1834_1	1	Log	03/25/2022 11:10:09 AM	Not Applicable	False	Not Cataloged	1778184

8. Check "All Datafiles" and "Change database state if needed for restore and recovery", and click Next.

Restore ORCL

1 Restore Scope

Restore Scope

All Datafiles

Tablespaces

Control files

Database State

Change database state if needed for restore and recovery

Restore Mode

Force in place restore

If this check box is not selected and if any of the in place restore criteria is not met, restore will be performed using the connect and copy method. The connect and copy restore method might take time based on the files being restored.

Previous

Next

9. Choose a desired recovery scope using either SCN or time. Rather than copying the mounted archive logs

to the current log directory as demonstrated in step 6, the mounted archive log path can be listed in "Specify external archive log files locations" for recovery.



10. Specify an optional prescript to run if necessary.

Restore ORCL

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Specify optional scripts to run before performing a restore job i

Prescript full path Enter Prescript path

Arguments

Script timeout secs

Previous Next

The screenshot shows the Oracle SnapCenter Restore wizard interface. The title bar says "Restore ORCL". On the left, a vertical navigation menu lists steps: 1. Restore Scope, 2. Recovery Scope, 3. PreOps (which is selected and highlighted in blue), 4. PostOps, 5. Notification, and 6. Summary. The main panel title is "Specify optional scripts to run before performing a restore job" with an information icon. It contains three input fields: "Prescript full path" with the value "/var/opt/snapcenter/spl/scripts/", "Enter Prescript path" (empty), "Arguments" (empty), and "Script timeout" with the value "60" and unit "secs". At the bottom right are "Previous" and "Next" buttons.

11. Specify an optional afterscript to run if necessary. Check the open database after recovery.

Restore ORCL

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Specify optional scripts to run after performing a restore job ?

Postscript full path Enter Postscript path

Arguments

Open the database or container database in READ-WRITE mode after recovery

Previous Next

12. Provide an SMTP server and email address if a job notification is needed.

Restore ORCL

Provide email settings i

Email preference	Never
From	From email
To	Email to
Subject	Notification

Attach job report

Previous **Next**

The screenshot shows a step-by-step restoration wizard titled "Restore ORCL". The current step is "5 Notification". On the left, a vertical navigation bar lists steps 1 through 6: "1 Restore Scope", "2 Recovery Scope", "3 PreOps", "4 PostOps", "5 Notification" (which is highlighted in blue), and "6 Summary". The main panel contains fields for providing email settings, including dropdowns for "Email preference" (set to "Never"), "From" (set to "From email"), "To" (set to "Email to"), and "Subject" (set to "Notification"). There is also an unchecked checkbox for "Attach job report". At the bottom right, there are "Previous" and "Next" buttons.

13. Restore the job summary. Click finish to launch the restore job.

Restore ORCL

X

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Summary

Backup name	ip-10-0-0-151_03-25-2022_11.15.01.1503_0
Backup date	03/25/2022 11:15:11 AM
Restore scope	All DataFiles
Recovery scope	Until SCN 1778546
Auxiliary destination	
Options	Change database state if necessary , Open the database or container database in READ-WRITE mode after recovery
Prescript full path	None
Prescript arguments	
Postscript full path	None
Postscript arguments	
Send email	No

Previous **Finish**

14. Validate the restore from SnapCenter.

Job Details

Restore 'ip-10-0-0-151.ec2.internal\ORCL'

- ✓ ▾ Restore 'ip-10-0-0-151.ec2.internal\ORCL'
- ✓ ▾ ip-10-0-0-151.ec2.Internal
 - ✓ ► Prescripts
 - ✓ ► Pre Restore
 - ✓ ► Restore
 - ✓ ► Post Restore
 - ✓ ► Postscripts
 - ✓ ► Post Restore Cleanup
 - ✓ ► Data Collection
 - ✓ ► Send EMS Messages

Task Name: ip-10-0-0-151.ec2.Internal Start Time: 03/25/2022 3:33:53 PM End Time: 03/25/2022 3:35:10 PM

[View Logs](#) [Cancel job](#) [Close](#)

15. Validate the restore from the EC2 instance host.

```

-bash-4.2$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Mar 25 15:44:08 2022
Version 19.8.0.0.0

Copyright (c) 1982, 2020, 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, RESETLOGS_CHANGE#, RESETLOGS_TIME, open_mode from v$database;

NAME      RESETLOGS_CHANGE# RESETLOGS OPEN_MODE
-----  -----
ORCL          1778547 25-MAR-22 READ WRITE

SQL>

```

16. To unmount the restore log volume, reverse the steps in step 4.

Creating a database clone

The following section demonstrates how to use the SnapCenter clone workflow to create a database clone from a primary database to a standby EC2 instance.

1. Take a full snapshot backup of the primary database from SnapCenter using the full backup resource group.

This screenshot shows the NetApp SnapCenter interface. The left sidebar has a 'Resource Groups' icon. The main area shows a table for 'orc_full_bkup Details'. The table has columns: Name, Resource Name, Type, and Host. One row is selected, showing 'orc_full_bkup' as the Name, 'ORCL' as the Resource Name, 'Oracle Database' as the Type, and 'ip-10-0-0-151.ec2.internal' as the Host. There are buttons at the top right: 'Modify Resource Group', 'Backup Now', 'Maintenance', and 'Delete'.

2. From the SnapCenter Resource tab > Database view, open the Database Backup Management page for the primary database that the replica is to be created from.

This screenshot shows the NetApp SnapCenter Database Backup Management page for the 'ORCL' database. The left sidebar has a 'Databases' icon. The main area shows a summary card with '93 Backups', '6 Data Backups', '87 Log Backups', and '0 Clones'. Below this is a table titled 'Primary Backup(s)' with columns: Backup Name, Count, Type, End Date, Verified, Mounted, RMAN Cataloged, and SCN. Five backup entries are listed, each with a timestamp like '03/25/2022 5:55:09 PM' and a status like 'Not Applicable' or 'Unverified'. There are buttons at the top right: 'Database Settings', 'Protect', and 'Refine'.

3. Mount the log volume snapshot taken in step 4 to the standby EC2 instance host.

ORCL Topology

Manage Copies

Local copies

Primary Backup(s)						
Backup Name	Count	Type	IF	End Date	Verified	Mounted
ip-10-0-0-151_03-25-2022_18.55.01.0309_1	1	Log		03/25/2022 6:55:09 PM	Not Applicable	False
ip-10-0-0-151_03-25-2022_18.40.00.9602_1	1	Log		03/25/2022 6:40:23 PM	Not Applicable	False
ip-10-0-0-151_03-25-2022_17.55.01.0197_1	1	Log		03/25/2022 5:55:09 PM	Not Applicable	False
ip-10-0-0-151_03-25-2022_17.50.55.0853_1	1	Log		03/25/2022 5:51:12 PM	Not Applicable	False
ip-10-0-0-151_03-25-2022_17.50.55.0853_0	1	Data		03/25/2022 5:51:05 PM	Unverified	False
ip-10-0-0-151_03-25-2022_17.40.00.9758_1	1	Log		03/25/2022 5:40:08 PM	Not	False

Mount backups

Choose the host to mount the backup : ip-10-0-0-47.ec2.internal

Mount path : /var/opt/snapcenter/sco/backup_mount/ip-10-0-0-151_03-25-2022_17.50.55.0853_1/ORCL

Mount **Cancel**

- Highlight the snapshot copy to be cloned for the replica, and click the Clone button to start the clone procedure.

ORCL Topology

Manage Copies

Local copies

Primary Backup(s)						
Backup Name	Count	Type	IF	End Date	Verified	Mounted
ip-10-0-0-151_03-25-2022_17.55.01.0197_1	1	Log		03/25/2022 5:55:09 PM	Not Applicable	False
ip-10-0-0-151_03-25-2022_17.50.55.0853_1	1	Log		03/25/2022 5:51:12 PM	Not Applicable	False
ip-10-0-0-151_03-25-2022_17.50.55.0853_0	1	Data		03/25/2022 5:51:05 PM	Unverified	False
ip-10-0-0-151_03-25-2022_17.40.00.9758_1	1	Log		03/25/2022 5:40:08 PM	Not Applicable	False
ip-10-0-0-151_03-25-2022_17.25.01.0539_1	1	Log		03/25/2022 5:25:08 PM	Not	False

5. Change the replica copy name so that it is different from the primary database name. Click Next.



6. Change the clone host to the standby EC2 host, accept the default naming, and click Next.

Clone from ORCL

1 Name

Select the host to create a clone

Clone host: ip-10-0-0-47.ec2.internal

2 Locations

Datafile locations: /ora_nfs_data_ORCLREAD

Control files: /ora_nfs_data_ORCLREAD/ORCLREAD/control/control01.ctl

Redo logs:

Group	Size	Unit	Number of files
RedoGroup 1	128	MB	1
RedoGroup 2	128	MB	1

Previous Next

7. Change your Oracle home settings to match those configured for the target Oracle server host, and click Next.

Clone from ORCL

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 'Clone from ORCL' wizard in progress, specifically the 'Credentials' step (step 3). On the left, a vertical navigation bar lists steps 1 through 7. Step 3, 'Credentials', is highlighted. The main area contains two sections: 'Database Credentials for the clone' and 'Oracle Home Settings'. In the 'Database Credentials' section, the 'Credential name for sys user' dropdown is set to 'None', with a '+' button and an information icon next to it. The 'Database port' field is set to '1521'. In the 'Oracle Home Settings' section, the 'Oracle Home' field is '/rdsdbbin/oracle', 'Oracle OS User' is 'rdsdb', and 'Oracle OS Group' is 'database'. At the bottom right, there are 'Previous' and 'Next' buttons.

8. Specify a recovery point using either time or the SCN and mounted archive log path.



9. Send the SMTP email settings if needed.

Clone from ORCL

Provide email settings i

Email preference	Never
From	From email
To	Email to
Subject	Notification

Attach job report

6 Notification

7 Summary

Previous **Next**

10. Clone the job summary, and click Finish to launch the clone job.

Clone from ORCL

	Summary
1 Name	
2 Locations	Clone from backup ip-10-0-0-151_03-25-2022_17.50.55.0853_0
3 Credentials	Clone SID ORCLREAD
4 PreOps	Clone server ip-10-0-0-47.ec2.internal
5 PostOps	Oracle home /rdsdbbin/oracle
6 Notification	Oracle OS user rdsdb
7 Summary	Oracle OS group database Datafile mountpaths /ora_nfs_data_ORCLREAD Control files /ora_nfs_data_ORCLREAD/ORCLREAD/control/control01.ctl Redo groups RedoGroup =1 TotalSize =128 Path =/ora_nfs_data_ORCLREAD/ORCLREAD/redolog redo04.log RedoGroup =2 TotalSize =128 Path =/ora_nfs_data_ORCLREAD/ORCLREAD/redolog redo03.log RedoGroup =3 TotalSize =128 Path =/ora_nfs_data_ORCLREAD/ORCLREAD/redolog redo02.log RedoGroup =4 TotalSize =128 Path =/ora_nfs_data_ORCLREAD/ORCLREAD/redolog redo01.log Recovery scope Until SCN 1788879 Prescript full path none Prescript arguments Postscript full path none Postscript arguments Send email No

[Previous](#) **Finish**

11. Validate the replica clone by reviewing the clone job log.

Job Details

Clone from backup 'ip-10-0-0-151_03-25-2022_17.50.55.0853_0'

- ✓ ▾ Clone from backup 'ip-10-0-0-151_03-25-2022_17.50.55.0853_0'
- ✓ ▾ ip-10-0-0-47.ec2.internal
 - ✓ ► Prescripts
 - ✓ ► Query Host Information
 - ✓ ► Prepare for Cloning
 - ✓ ► Cloning Resources
 - ✓ ► FileSystem Clone
 - ✓ ► Application Clone
 - ✓ ► Postscripts
 - ✓ ► Register Clone
 - ✓ ► Unmount Clone
 - ✓ ► Data Collection
 - ✓ ► Send EMS Messages

Task Name: ip-10-0-0-47.ec2.internal Start Time: 03/25/2022 9:08:32 PM End Time: 03/25/2022 9:12:03 PM

[View Logs](#) [Cancel Job](#) [Close](#)

The cloned database is registered in SnapCenter immediately.

NetApp SnapCenter®

Oracle Database

View	Database	Search databases	
<input checked="" type="checkbox"/> Resources	ORCL	Single Instance	Host/Cluster: ip-10-0-0-151.ec2.internal Resource Group: orcl_full_bkup Policies: Oracle full backup Last Backup: 03/25/2022 9:10:09 PM Overall Status: Backup succeeded
<input type="checkbox"/> Monitor	ORCLREAD	Single Instance	Host/Cluster: ip-10-0-0-47.ec2.internal Resource Group: orcl_log_bkup Policies: Oracle log backup Last Backup: N/A Overall Status: Not protected

12. Turn off Oracle archive log mode. Log into the EC2 instance as oracle user and execute following command:

```
sqlplus / as sysdba
```

```
shutdown immediate;
```

```
startup mount;
```

```
alter database noarchivelog;
```

```
alter database open;
```



Instead primary Oracle backup copies, a clone can also be created from replicated secondary backup copies on target FSx cluster with same procedures.

HA failover to standby and resync

The standby Oracle HA cluster provides high availability in the event of failure in the primary site, either in the compute layer or in the storage layer. One significant benefit of the solution is that a user can test and validate the infrastructure at any time or with any frequency. Failover can be user simulated or triggered by real failure. The failover processes are identical and can be automated for fast application recovery.

See the following list of failover procedures:

1. For a simulated failover, run a log snapshot backup to flush the latest transactions to the standby site, as demonstrated in the section [Taking an archive log snapshot](#). For a failover triggered by an actual failure, the last recoverable data is replicated to the standby site with the last successful scheduled log volume backup.
2. Break the SnapMirror between primary and standby FSx cluster.
3. Mount the replicated standby database volumes at the standby EC2 instance host.
4. Relink the Oracle binary if the replicated Oracle binary is used for Oracle recovery.
5. Recover the standby Oracle database to the last available archive log.
6. Open the standby Oracle database for application and user access.
7. For an actual primary site failure, the standby Oracle database now takes the role of the new primary site and database volumes can be used to rebuild the failed primary site as a new standby site with the reverse SnapMirror method.
8. For a simulated primary site failure for testing or validation, shut down the standby Oracle database after the completion of testing exercises. Then unmount the standby database volumes from the standby EC2 instance host and resync replication from the primary site to the standby site.

These procedures can be performed with the NetApp Automation Toolkit available for download at the public NetApp GitHub site.

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

Read the README instruction carefully before attempting setup and failover testing.

[Next: Database migration.](#)

Database migration from on-prem to public cloud

[Previous: Database management.](#)

Database migration is a challenging endeavor by any means. Migrating an Oracle database from on-premises to the cloud is no exception.

The following sections provide key factors to consider when migrating Oracle databases to the AWS public cloud with the AWS EC2 compute and FSx storage platform.

ONTAP storage is available on-premises

If the on-premises Oracle database is sitting on an ONTAP storage array, then it is easier to set up replication for database migration using the NetApp SnapMirror technology that is built into AWS FSx ONTAP storage. The migration process can be orchestrated using NetApp BlueXP console.

1. Build a target compute EC2 instance that matches the on-premises instance.
2. Provision matching, equally sized database volumes from FSx console.
3. Mount the FSx database volumes to the EC2 instance.
4. Set up SnapMirror replication between the on-premises database volumes to the target FSx database volumes. The initial sync might take some time to move the primary source data, but any following incremental updates are much quicker.
5. At the time of switchover, shut down the primary application to stop all transactions. From the Oracle sqlplus CLI interface, execute an Oracle online log switch and allow SnapMirror sync to push the last archived log to the target volume.
6. Break up the mirrored volumes, run Oracle recovery at the target, and bring up the database for service.
7. Point applications to the Oracle database in the cloud.

The following video demonstrates how to migrate an Oracle database from on-premises to AWS FSx/EC2 using the NetApp BlueXP console and SnapMirror replication.

[Oracle Database Migration from On-premises to FSx/EC2 via SnapMirror and BlueXP](#)

ONTAP storage is not available on premises

If the on-premises Oracle database is hosted on third-party storage other than ONTAP, database migration is based on the restore of a Oracle database backup copy. You must play the archive log to make it current before switching over.

AWS S3 can be used as a staging storage area for database move and migration. See the following high level steps for this method:

1. Provision a new, matching EC2 instance that is comparable with the on-premises instance.
2. Provision equal database volumes from FSx storage and mount the volumes to the EC2 instance.
3. Create a disk-level Oracle backup copy.
4. Move the backup copy to AWS S3 storage.
5. Recreate the Oracle control file and restore and recover the database by pulling data and the archive log from S3 storage.
6. Sync the target Oracle database with the on-premises source database.
7. At switchover, shut down the application and source Oracle database. Copy the last few archive logs and apply them to the target Oracle database to bring it up to date.
8. Start up the target database for user access.
9. Redirect application to the target database to complete the switchover.

Migrate on-premises Oracle databases to AWS FSx/EC2 using PDB relocation with maximum availability

This migration approach is best suited to Oracle databases that are already deployed in PDB/CDB multitenant model, and ONTAP storage is not available on-premises. The PDB relocation method utilizes Oracle PDB hot clone technology to move PDBs between a source CDB and a target CDB while minimizing service interruption.

First, create CDB in the AWS FSx/EC2 with sufficient storage to host PDBs to be migrated from on-premises. Multiple on-premises PDBs can be relocated one at a time.

1. If the on-premises database is deployed in a single instance rather than in the multitenant PDB/CDB model, follow the instructions in [Converting a single instance non-CDB to a PDB in a multitenant CDB](#) to convert the single instance to multitenant PDB/CDB. Then follow the next step to migrate the converted PDB to CDB in AWS FSx/EC2.
2. If the on-premises database is already deployed in the multitenant PDB/CDB model, follow the instructions in [Migrate on-premises Oracle databases to cloud with PDB relocation](#) to perform the migration.

The following video demonstrates how an Oracle database (PDB) can be migrated to FSx/EC2 using PDB relocation with maximum availability.

[Migrate on-prem Oracle PDB to AWS CDB with max availability](#)



Although the instructions in step 1 and 2 are illustrated in the context of Azure public cloud, the procedures are applicable to AWS cloud without any changes.

The NetApp Solutions Automation team provides a migration toolkit that can facilitate Oracle database migration from on-premises to the AWS cloud. Use following command to download the Oracle database migration toolkit for PDB relocation.

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

Oracle Database Deployment and Protection on Azure NetApp Files

TR-4954: Oracle Database Deployment and Protection on Azure NetApp Files

Allen Cao, Niyaz Mohamed, NetApp

Many mission-critical Oracle enterprise databases are still hosted on-premises, and many enterprises are looking to migrate these Oracle databases to a public cloud. Often, these Oracle databases are application centric and thus require user-specific configurations, a capability that is missing from many database-as-a-service public-cloud offerings. Therefore, the current database landscape calls for a public-cloud-based Oracle database solution built from a high-performance, scalable compute and storage service that can accommodate unique requirements. Azure virtual machine compute instances and the Azure NetApp Files storage service might be the missing pieces of this puzzle that you can leverage to build and migrate your mission-critical Oracle database workloads to a public cloud.

Azure virtual machines are one of several types of on-demand, scalable computing resources that Azure offers. Typically, you choose a virtual machine when you need more control over the computing environment than the other choices offer. Azure virtual machines offer a quick and easy way to create a computer with specific configurations required to run your Oracle database, whether it is for compute- or memory-intensive workloads. Virtual machines in an Azure virtual network can easily be connected to your organization's network, for example through a secured VPN tunnel.

Azure NetApp Files is a fully managed Microsoft service that will take your database workload to the cloud faster and more securely than ever before. It was designed to meet the core requirements of running high-performance workloads such as Oracle databases in the cloud, and it provides performance tiers that reflect the real-world range of IOPS demands, low latency, high availability, high durability, manageability at scale, and fast and efficient backup, recovery, and cloning. These capabilities are possible because Azure NetApp Files is based on physical all-flash NetApp ONTAP systems running within the Azure data center environment. Azure NetApp Files is completely integrated into the Azure DCs and portal, and customers can use the same comfortable graphical interface and APIs for creating and managing shared files as with any other Azure object. With Azure NetApp file, you can unlock the full capabilities of Azure without extra risk, cost, or time and trust the only enterprise file service native to Azure.

This documentation describes in detail how to deploy, configure, and protect an Oracle database with an Azure virtual machine and Azure NetApp Files storage service that delivers performance and durability similar to an on-premises system. For best-practices guidance, see TR-4780 [Oracle Databases on Microsoft Azure](#). More importantly, NetApp also provides automation toolkits that automate most of the tasks that are required for the deployment, configuration, data protection, migration, and management of your Oracle database workload in the Azure public cloud. The automation toolkits are available for download at NetApp public GitHub site: [NetApp-Automation](#).

Next: [Solutions architecture](#).

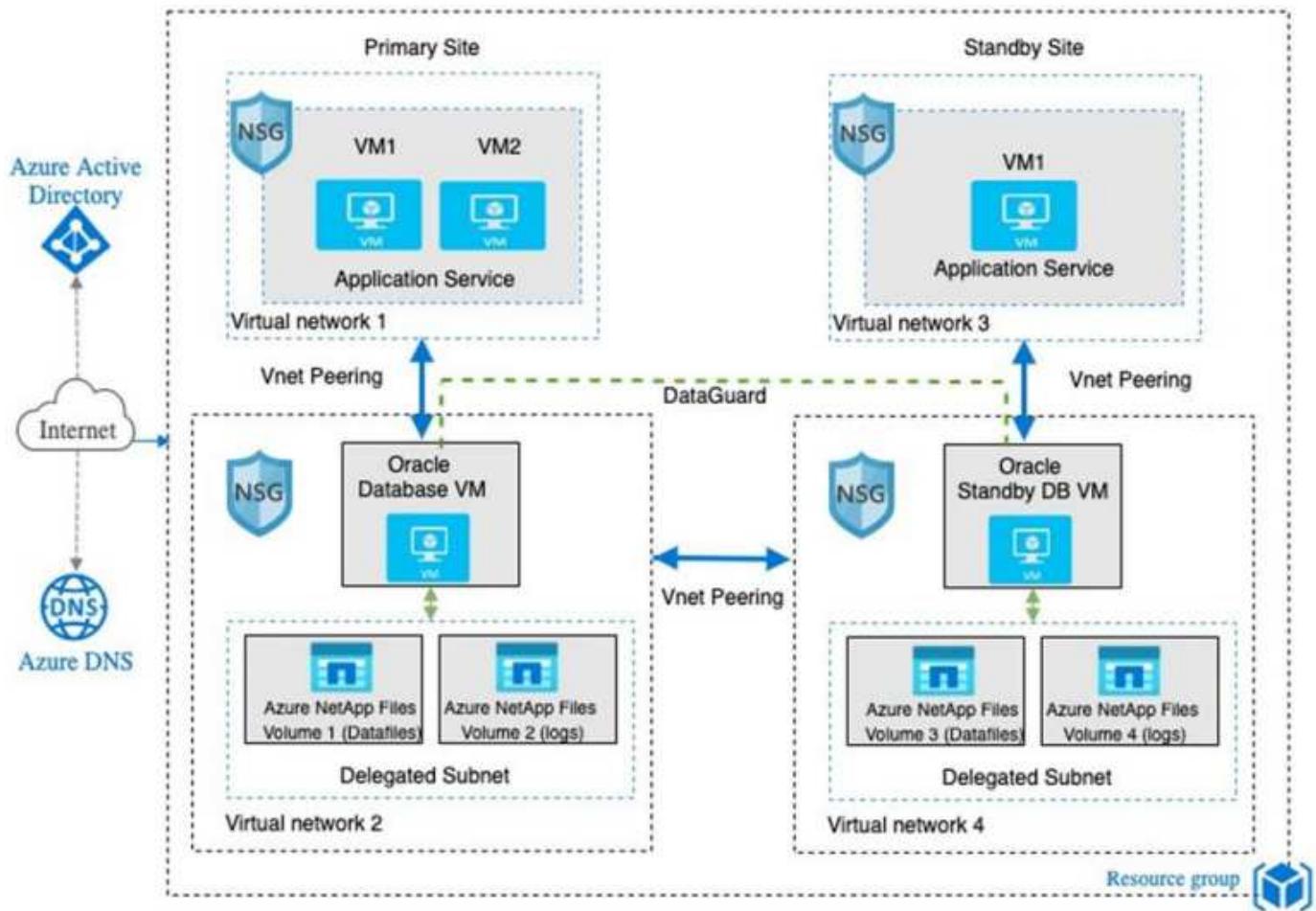
Solution Architecture

Previous: [Introduction](#).

The following architecture diagram illustrates a highly available Oracle database deployment on Azure VM instances and the Azure NetApp Files storage.

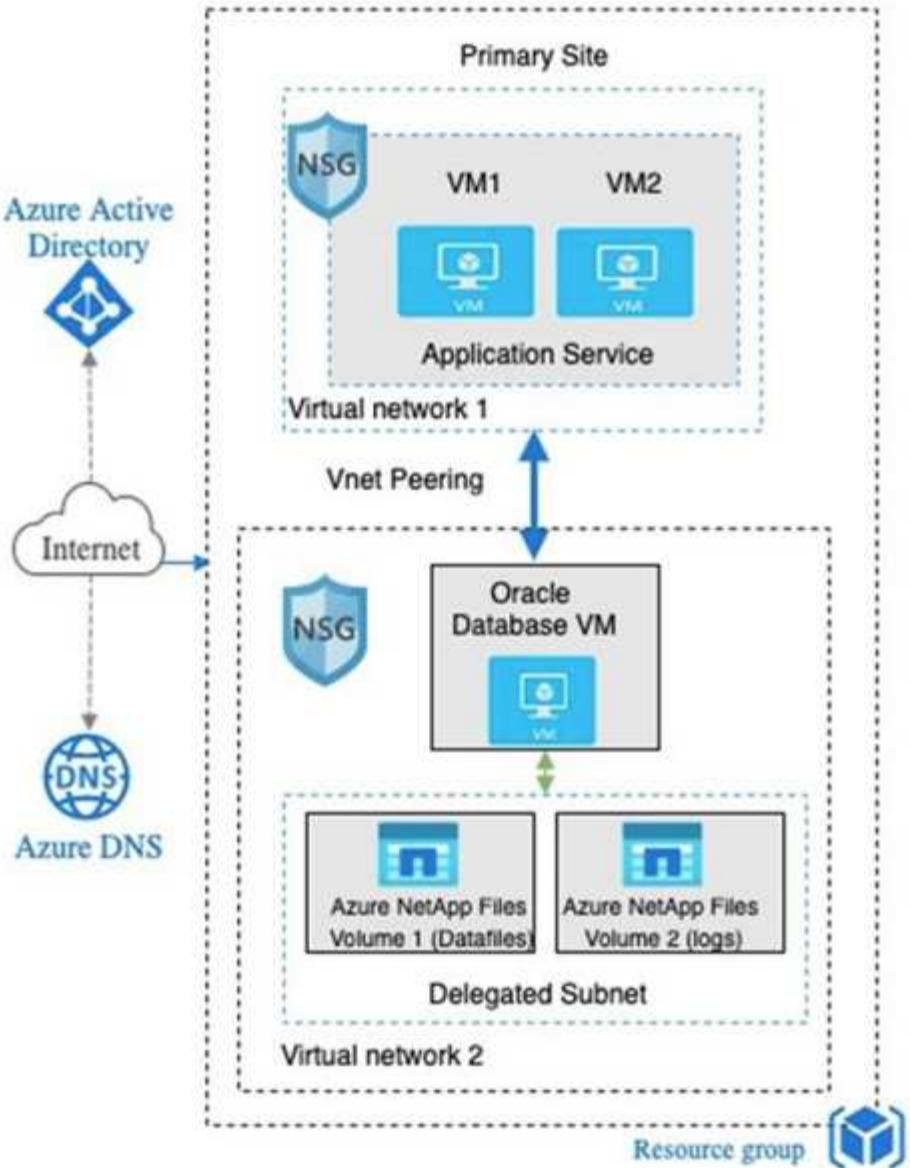
Within the environment, the Oracle compute instance is deployed via an Azure services VM console. There are multiple Azure instance types available from the console. NetApp recommends deploying a database-oriented Azure VM instance that meets your expected workload.

Oracle database storage on the other hand is deployed with the Azure NetApp Files service available from Azure console. The Oracle binary, data, or log volumes are subsequently presented and mounted on an Azure VM instance Linux host.



In many respects, the implementation of Azure NetApp Files in Azure cloud is very similar to an on-premises ONTAP data storage architecture with many built-in redundancies, such as RAID and dual controllers. For disaster recovery, a standby site can be setup in different regions and database can be synced up with the primary site using application-level replication (for example, Oracle Data Guard).

In our test validation for Oracle database deployment and data protection, the Oracle database is deployed on a single Azure VM as illustrated in the following diagram:



The Azure Oracle environment can be managed with an Ansible controller node for automation using tool kits provided by NetApp for database deployment, backup, recovery, and database migration. Any updates to the Oracle Azure VM instance operating-system kernel or Oracle patching can be performed in parallel to keep the primary and standby in sync. In fact, the initial toolkits can be easily expanded to perform daily Oracle tasks if needed. If you need help to set up a CLI Ansible controller, see [NetApp Solution Automation](#) to get started.

Next: Factors to consider.

Factors to consider for Oracle database deployment

[Previous: Solution architecture.](#)

A public cloud provides many choices for compute and storage, and using the correct type of compute instance and storage engine is a good place to start for database deployment. You should also select compute and storage configurations that are optimized for Oracle databases.

The following sections describe the key considerations when deploying an Oracle database in the Azure public cloud on an Azure virtual machine instance with Azure NetApp Files storage.

VM type and sizing

Selecting the right VM type and size is important for optimal performance of a relational database in a public cloud. An Azure virtual machine provides a variety of compute instances that can be used to host Oracle database workloads. See the Microsoft documentation [Sizes for virtual machines in Azure](#) for different types of Azure virtual machines and their sizing. In general, NetApp recommends using a general-purpose Azure virtual machine for the deployment of small- and medium-sized Oracle databases. For the deployment of larger Oracle databases, a memory-optimized Azure VM is appropriate. With more available RAM, a larger Oracle SGA or smart flash cache can be configured to reduce the physical I/O, which in turn improves database performance.

Azure NetApp Files works as an NFS mount attached to an Azure virtual machine, which offers higher throughput and overcomes the storage-optimized VM throughput limit with local storage. Therefore, running Oracle on Azure NetApp Files could reduce the licensable Oracle CPU core count and licensing costs. See [TR-4780: Oracle Databases on Microsoft Azure](#), Section 7 - How Does Oracle Licensing Work?

Other factors to consider include the following:

- Choose the correct vCPU and RAM combination based on workload characteristics. As the RAM size increases on the VM, so does the number of vCPU cores. There should be a balance at some point as the Oracle license fees are charged on the number of vCPU cores.
- Add swap space to a VM. The default Azure VM deployment does not create a swap space, which is not optimal for a database.

Azure NetApp Files performance

Azure NetApp Files volumes are allocated from a capacity pool the customer must provision in their Azure NetApp Files storage account. Each capacity pool is assigned as follows:

- To a service level that defines the overall performance capability.
- The initially provisioned storage capacity or tiering for that capacity pool. A quality of service (QoS) level that defines the overall maximum throughput per provisioned space.

The service level and initially provisioned storage capacity determines the performance level for a particular Oracle database volume.

1. Service Levels for Azure NetApp Files

Azure NetApp Files supports three service levels: Ultra, Premium, and Standard.

- **Ultra storage.** This tier provides up to 128MiBps of throughput per 1TiB of volume quota assigned.
- **Premium storage.** This tier provides up to 64MiBps of throughput per 1TiB of volume quota assigned.
- **Standard storage.** This tier provides up to 16MiBps of throughput per 1TiB of volume quota assigned.

2. Capacity pool and quality of service

Each of the desired service levels has an associated cost for provisioned capacity and includes a quality-of-service (QoS) level that defines the overall maximum throughput for provisioned space.

For example, a 10TiB-provisioned single-capacity pool with the premium service level provides an overall available throughput for all volumes in this capacity pool of 10x 64MBps, so 640MBps with 40,000 (16K) IOPs or 80,000 (8K) IOPs.

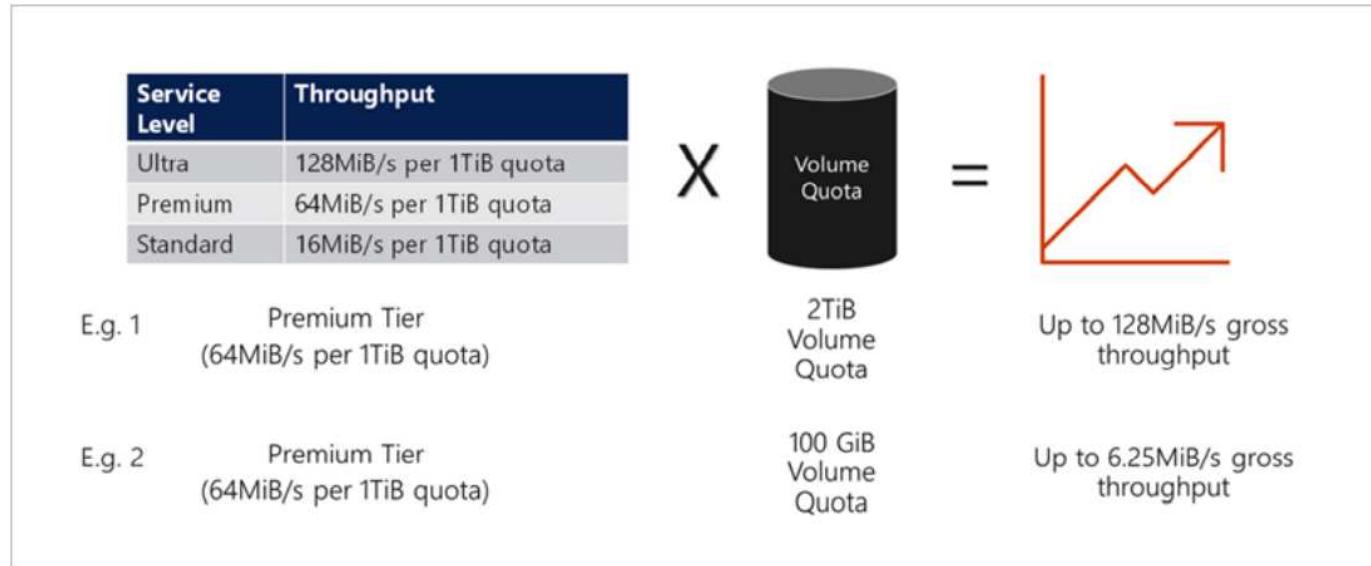
The minimum capacity pool size is 4TiB. You can change the size of a capacity pool in 1TiB increments in

response to changes in your workload requirements to manage storage needs and costs.

3. Calculate the service level at a database volume

The throughput limit for an Oracle database volume is determined by a combination of the following factors:
The service level of the capacity pool to which the volume belongs and The quota assigned to the volume.

The following diagram shows how the throughput limit for an Oracle database volume is calculated.



In example 1, a volume from a capacity pool with the Premium storage tier that is assigned 2TiB of quota is assigned a throughput limit of 128MiBps ($2\text{TiB} * 64\text{MiBps}$). This scenario applies regardless of the capacity pool size or the actual volume consumption.

In example 2, a volume from a capacity pool with the Premium storage tier that is assigned 100GiB of quota is assigned a throughput limit of 6.25MiBps ($0.09765625\text{TiB} * 64\text{MiBps}$). This scenario applies regardless of the capacity pool size or the actual volume consumption.

Please note that the minimum volume size is 100GiB.

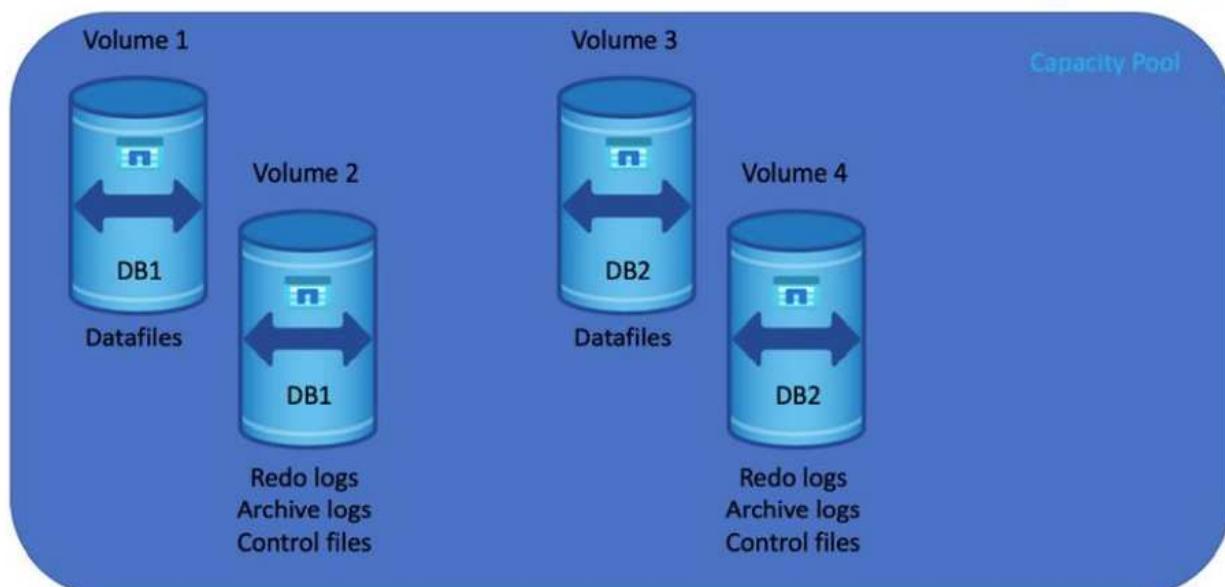
Storage layout and settings

NetApp recommends the following storage layout:

- For small databases, using single volume layout for all Oracle files.



- For large databases, the recommended volume layout is multiple volumes: one for Oracle data and a duplicate control file and one for the Oracle active log, archived log, and control file. NetApp highly recommends allocating a volume for the Oracle binary instead of the local drive so that the database can be relocated to a new host and quickly restored.



NFS configuration

Linux, the most common operating system, includes native NFS capabilities. Oracle offers a direct NFS (dNFS) client natively integrated into Oracle. Oracle dNFS bypasses the OS cache and enables parallel processing to

improve database performance. Oracle has supported NFSv3 for over 20 years, and NFSv4 is supported with Oracle 12.1.0.2 and later.

By using dNFS (available since Oracle 11g), an Oracle database running on an Azure Virtual Machine can drive significantly more I/O than the native NFS client. Automated Oracle deployment using the NetApp automation toolkit automatically configures dNFS on NFSv3.

The following diagram demonstrates the SLOB benchmark on Azure NetApp Files with Oracle dNFS.



Other factors to consider:

- TCP slot tables are the NFS equivalent of host-bus-adapter (HBA) queue depth. These tables control the number of NFS operations that can be outstanding at any one time. The default value is usually 16, which is far too low for optimum performance. The opposite problem occurs on newer Linux kernels, which can automatically increase the TCP slot table limit to a level that saturates the NFS server with requests.

For optimum performance and to prevent performance problems, adjust the kernel parameters that control TCP slot tables to 128.

```
sysctl -a | grep tcp.*slot_table
```

- The following table provides recommended NFS mount options for a single instance of Linux NFSv3.

File Type	Mount Options
<ul style="list-style-type: none"> • Control files • Data files • Redo logs 	<code>rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsize=65536</code>
<ul style="list-style-type: none"> • ORACLE_HOME • ORACLE_BASE 	<code>rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsize=65536</code>

 Before using dNFS, verify that the patches described in Oracle Doc 1495104.1 are installed. Starting with Oracle 12c, DNFS includes support for NFSv3, NFSv4, and NFSv4.1. NetApp support policies cover v3 and v4 for all clients, but, at the time of writing, NFSv4.1 is not supported for use with Oracle dNFS.

Next: [Deployment procedures](#).

Step-by-Step Oracle deployment procedures on Azure VM and Azure NetApp Files

Previous: [Factors to consider](#).

Deploy an Azure VM with ANF for Oracle via Azure portal console

If you are new to Azure, you first need to set up an Azure account environment. This includes signing up your organization to use Azure Active Directory. The following section is a summary of these steps. For details, see the linked Azure-specific documentation.

Create and consume Azure resources

After your Azure environment is set up and an account is created and associated with a subscription, you can log into Azure portal with the account to create the necessary resources to run Oracle.

1. Create a virtual network or VNet

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VMs), to securely communicate with each other, the internet, and on-premises networks. Before provisioning an Azure VM, a VNet (where a VM is deployed) must first be configured.

See [Create a virtual network using the Azure portal](#) to create a VNet.

2. Create a NetApp storage account and capacity pool for ANF

In this deployment scenario, an Azure VM OS is provisioned using regular Azure storage, but ANF volumes are provisioned to run Oracle database via NFS. First, you need to create a NetApp storage account and a capacity pool to host the storage volumes.

See [Set up Azure NetApp Files and create an NFS volume](#) to set up an ANF capacity pool.

3. Provision Azure VM for Oracle

Based on your workload, determine what type of Azure VM you need and the size of the VM vCPU and RAM to deploy for Oracle. Then, from the Azure console, click the VM icon to launch the VM deployment workflow.

- From the Azure VM page, click **Create** and then choose **Azure virtual machine**.

Name	Type	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disks
acao-ora01	Virtual machine	Hybrid Cloud TME Onprem	TMEstorres	South Central US	Stopped (deallocated)	Linux	Standard_B4ms	13.65.63.157	1
ANFAVFW02JH	Virtual machine	Hybrid Cloud TME Onprem	ANFAVSVAL2	West Europe	Running	Windows	Standard_DS2_v2	20.229.80.88	1
ANFAVSfio01	Virtual machine	Hybrid Cloud TME Onprem	anfavsg	South Central US	Stopped (deallocated)	Linux	Standard_D32ds_v4	-	1
ANFAVSfioA21	Virtual machine	Hybrid Cloud TME Onprem	anfavsg	South Central US	Running	Linux	Standard_E32as_v4	40.124.74.246	1
ANFAVSfioA22	Virtual machine	Hybrid Cloud TME Onprem	anfavsg	South Central US	Stopped (deallocated)	Linux	Standard_E32as_v4	40.124.178.111	1
ANFAVSfioAZ3	Virtual machine	Hybrid Cloud TME Onprem	anfavsg	South Central US	Stopped (deallocated)	Linux	Standard_E32as_v4	40.124.194.32	1
ANFAVsiaIDC	Virtual machine	Hybrid Cloud TME Onprem	anfavsg	South Central US	Stopped (deallocated)	Windows	Standard_B4ms	-	1
ANFAVSviaIH	Virtual machine	Hybrid Cloud TME Onprem	anfavsg	South Central US	Running	Windows	Standard_B2ms	70.37.66.218	1
ANFAVSviaI2	Virtual machine	Hybrid Cloud TME Onprem	anfavsg	South Central US	Running	Windows	Standard_B2s	20.225.210.195	1
ANFCVOCM	Virtual machine	Hybrid Cloud TME Onprem	anfcval2	West Europe	Running	Linux	Standard_DS3_v2	-	1
ANFCVOORDC2	Virtual machine	Hybrid Cloud TME Onprem	anfcval2	West Europe	Running	Windows	Standard_B2s	-	1
ANFCVOORDemo	Virtual machine	Hybrid Cloud TME Onprem	anfcvordemo-rg	West Europe	Running	Linux	Standard_E4s_v3	-	5
AVSCVOPerfinguest	Virtual machine	Hybrid Cloud TME Onprem	avscvoperfinguest-rg	West Europe	Stopped (deallocated)	Linux	Standard_DS15_v2	-	5

- Choose the subscription ID for the deployment, and then choose the resource group, region, host name, VM image, size, and authentication method. Go to the Disk page.

[Home](#) > [Virtual machines](#) >

Create a virtual machine

...

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Advanced](#) [Tags](#) [Review + create](#)

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Hybrid Cloud TME Onprem

Resource group * ⓘ

ANFAVSRG

[Create new](#)

Instance details

Virtual machine name * ⓘ

acao-ora01



Region * ⓘ

(US) South Central US



Availability options ⓘ

No infrastructure redundancy required



Security type ⓘ

Standard



Image * ⓘ

Red Hat Enterprise Linux 8.0 (LVM) - Gen2

[See all images](#) | [Configure VM generation](#)

Run with Azure Spot discount ⓘ



Size * ⓘ

Standard_D8s_v3 - 8 vcpus, 32 GiB memory (\$273.02/month)

[See all sizes](#)

Administrator account

Authentication type ⓘ

 SSH public key Password[Review + create](#)[< Previous](#)[Next : Disks >](#)

[Home](#) > [Virtual machines](#) >

Create a virtual machine

Size * ⓘ

Standard_D8s_v3 - 8 vcpus, 32 GiB memory (\$273.02/month)

[See all sizes](#)

Administrator account

Authentication type ⓘ

 SSH public key Password

Username * ⓘ

azureuser



Password * ⓘ



Confirm password * ⓘ



Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ

 None Allow selected ports

Select inbound ports *

SSH (22)



⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Licensing

If you have eligible Red Hat Enterprise Linux subscriptions that are enabled for Red Hat Cloud Access, you can use Azure Hybrid Benefit to attach your Red Hat subscriptions to this VM and save money on compute costs [Learn more ↗](#)

Your Azure subscription is currently not a part of Red Hat Cloud Access. In order to enable AHB for this VM, you must add this Azure subscription to Cloud Access. [Learn more ↗](#)

[Review + create](#)[< Previous](#)[Next : Disks >](#)

3. Choose **premium SSD** for OS local redundancy and leave the data disk blank because the data disks are mounted from ANF storage. Go to the Networking page.

[Home](#) > [Virtual machines](#) >

Create a virtual machine

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Advanced](#) [Tags](#) [Review + create](#)

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

Disk options

OS disk type * ⓘ

Premium SSD (locally-redundant storage)

Delete with VM ⓘ



Enable encryption at host ⓘ



Encryption at host is not registered for the selected subscription. [Learn more about enabling this feature](#)

Encryption type *

(Default) Encryption at-rest with a platform-managed key

Enable Ultra Disk compatibility ⓘ



Data disks for acao-ora01

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM ⓘ
-----	------	------------	-----------	--------------	------------------

[Create and attach a new disk](#) [Attach an existing disk](#)

▼ Advanced

[Review + create](#)[< Previous](#)[Next : Networking >](#)

4. Choose the VNet and subnet. Allocate a public IP for external VM access. Then go to the Management page.

[Home](#) > [Virtual machines](#) >

Create a virtual machine

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * (i)

 ▼
[Create new](#)

Subnet * (i)

 ▼
[Manage subnet configuration](#)

Public IP (i)

 ▼
[Create new](#)

NIC network security group (i)

- None
 Basic
 Advanced

Public inbound ports * (i)

- None
 Allow selected ports

Select inbound ports *

 ▼

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Delete public IP and NIC when VM is deleted (i)

Enable accelerated networking (i)

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#) ↗

Place this virtual machine behind an existing load balancing solution?

[Review + create](#)

[< Previous](#)

[Next : Management >](#)

5. Keep all defaults for Management and move to the Advanced page.

Home > Virtual machines >

Create a virtual machine

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Advanced](#) [Tags](#) [Review + create](#)

Configure monitoring and management options for your VM.

Microsoft Defender for Cloud

Microsoft Defender for Cloud provides unified security management and advanced threat protection across hybrid cloud workloads. [Learn more ↗](#)

Your subscription is protected by Microsoft Defender for Cloud basic plan.

Monitoring

Boot diagnostics ⓘ

- Enable with managed storage account (recommended)
 Enable with custom storage account
 Disable

Enable OS guest diagnostics ⓘ

Identity

Enable system assigned managed identity ⓘ

Azure AD

Login with Azure AD ⓘ

RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine User Login is required when using Azure AD login. [Learn more ↗](#)

Azure AD login now uses SSH certificate-based authentication. You will need to use an SSH client that supports OpenSSH certificates. You can use Azure CLI or Cloud Shell from the Azure Portal. [Learn more ↗](#)

Auto-shutdown

Enable auto-shutdown ⓘ

Backup

[Review + create](#)< PreviousNext : Advanced >

6. Keep all defaults for the Advanced page unless you need to customize a VM after deployment with custom scripts. Then go to Tags page.

[Home](#) > [Virtual machines](#) >

Create a virtual machine

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Advanced](#) [Tags](#) [Review + create](#)

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions

Extensions provide post-deployment configuration and automation.

[Extensions](#) ⓘ[Select an extension to install](#)

VM applications

VM applications contain application files that are securely and reliably downloaded on your VM after deployment. In addition to the application files, an install and uninstall script are included in the application. You can easily add or remove applications on your VM after create. [Learn more ↗](#)

[Select a VM application to install](#)

Custom data

Pass a script, configuration file, or other data into the virtual machine **while it is being provisioned**. The data will be saved on the VM in a known location. [Learn more about custom data for VMs ↗](#)

[Custom data](#)

Your image must have a code to support consumption of custom data. If your image supports cloud-init, custom-data will be processed by cloud-init. [Learn more about custom data for VMs ↗](#)

User data

Pass a script, configuration file, or other data that will be accessible to your applications **throughout the lifetime of the virtual machine**. Don't use user data for storing your secrets or passwords. [Learn more about user data for VMs ↗](#)

[Enable user data](#)[Review + create](#)< PreviousNext : Tags >

7. Add a tag for the VM if desired. Then, go to the Review + create page.

[Home](#) > [Virtual machines](#) >

Create a virtual machine

Basics Disks Networking Management Advanced **Tags** Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name ⓘ	Value ⓘ	Resource
database	: oracle	12 selected <input type="button"/>
	:	12 selected <input type="button"/>

[Review + create](#)

[< Previous](#)

[Next : Review + create >](#)

8. The deployment workflow runs a validation on the configuration, and, if the validation passes, click **Create** to create the VM.

4. Provision ANF database volumes for Oracle

You must create three NFS volumes for an ANF capacity pool for the Oracle binary, data, and log volumes respectively.

- From the Azure console, under the list of Azure services, click Azure NetApp Files to open a volume creation workflow. If you have more than one ANF storage account, click the account that you would like to provision volumes from.

The screenshot shows the Microsoft Azure portal's main dashboard. At the top, there's a blue header bar with the 'Microsoft Azure' logo and a search bar. Below the header, a row of service icons is displayed: 'Create a resource' (plus sign), 'Azure NetApp Files' (highlighted with a yellow box), 'Virtual networks', 'Virtual machines', 'Storage accounts', 'Users', 'Subscriptions', 'Azure Active Directory', 'Quickstart Center', and 'More services'. Underneath this, there's a section titled 'Resources' with tabs for 'Recent' and 'Favorite'. A table lists various resources with columns for 'Name', 'Type', and 'Last Viewed'. Some entries include icons like a network, a virtual machine, a key, and a disk. The 'Recent' section includes items like 'ANFAVSAcct' (NetApp account), 'ANFAVSAval' (Virtual network), 'acao-ora01' (Virtual machine), and 'Hybrid Cloud TME Onprem' (Subscription). The 'Last Viewed' column shows times ranging from 'a few seconds ago' to '3 weeks ago'.

Name	Type	Last Viewed
ANFAVSAcct	NetApp account	a few seconds ago
ANFAVSAval	Virtual network	3 hours ago
acao-ora01	Virtual machine	5 days ago
Hybrid Cloud TME Onprem	Subscription	2 weeks ago
WEANFAVSAcct	NetApp account	2 weeks ago
ANFAVSAcct/CapPool/acao-ora01-u03	Volume	2 weeks ago
ANFAVSAcct/CapPool/acao-ora01-u02	Volume	2 weeks ago
ANFAVSAcct/CapPool/acao-ora01-u01	Volume	2 weeks ago
acao-ora01_OsDisk_1_673bad70ccce4709af8c1278e2bc97cb	Disk	2 weeks ago
acao-ora0166	Network Interface	3 weeks ago
TMEtstres	Resource group	3 weeks ago

- Under your NetApp storage account, click **Volumes**, and then **Add volume** to create new Oracle volumes.

The screenshot shows the 'ANFAVSAcct' blade within the Azure NetApp Files service. The left sidebar has a tree view with nodes like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Settings', 'Quota', 'Properties', 'Locks', 'Azure NetApp Files', 'Active Directory connections', 'Storage service', 'Capacity pools', 'Volumes' (highlighted with a yellow box), 'Data protection', 'Snapshot policies', 'Storage service add-ons', 'NetApp add-ons', 'Automation', 'Tasks (preview)', 'Export template', and 'Support + troubleshooting'. The main content area shows the 'Overview' tab for the 'ANFAVSAcct' NetApp account. It displays details such as 'Resource group (move) : ANFAVSRG', 'Location : South Central US', 'Subscription (move) : Hybrid Cloud TME Onprem', 'Subscription ID : 0efazdfb-917c-4497-b56a-b3f4eadb8111', and 'Tags (edit) : product_line : Field use - various'. Provisioning state is listed as 'Succeeded'. Below this, there's a section titled 'Enterprise files storage, powered by NetApp' with links to 'Connect to Active Directory', 'Capacity pools', and 'Volumes'. At the bottom, there are buttons for 'View AD connections', 'View capacity pools', and 'View volumes'.

3. As a good practice, identify Oracle volumes with the VM hostname as a prefix and then followed by the mount point on the host, such as u01 for Oracle binary, u02 for Oracle data, and u03 for Oracle log. Choose the same VNet for the volume as for the VM. Click **Next: Protocol>**.

4. Choose the NFS protocol, add the Oracle host IP address to the allowed client, and remove the default policy that allows all IP addresses 0.0.0.0/0. Then click **Next: Tags>**.

Microsoft Azure

Search resources, services, and docs (G+)

Home > Azure NetApp Files > ANFAVSAcct | Volumes >

ANFAVSAcct | Volumes

NetApp account

Create a volume

Basics Protocol Tags Review + create

Configure access to your volume.

Access

Protocol type: NFS SMB Dual-protocol

Configuration

File path *

Versions *

Kerberos: Enabled Disabled

LDAP: Enabled Disabled

Azure VMware Solution DataStore

Export policy

Configure the volume's export policy. This can be edited later. [Learn more](#)

Index	Allowed clients	Access	Root Access	...
1	172.30.137.142	Read & Write	On	<input type="checkbox"/>
2	172.30.137.142	Read & Write	On	<input type="checkbox"/>

Review + create < Previous Next : Tags >

5. Add a volume tag if desired. Then click **Review + Create>**.

Microsoft Azure

Search resources, services, and docs (G+ /)

Home > Azure NetApp Files > ANFAVSAcct | Volumes >

ANFAVSAcct | Volumes

NetApp account

Search (Ctrl+ /) Add volume ...

Overview

Activity log

Access control (IAM)

Tags

Settings

Quota

Properties

Locks

Azure NetApp Files

Active Directory connections

Storage service

Capacity pools

Volumes

Data protection

Snapshot policies

Storage service add-ons

NetApp add-ons

Automation

Tasks (preview)

Export template

Support + troubleshooting

New Support Request

+ Add volume ...

Search volumes

Name	↑↓	Quota
anf2-z1-stdds01	200 GiB	
anf2-z1-stdds02	200 GiB	
anf2-z1-stdds03	100 GiB	
anf2-z1-stdds04	100 GiB	
anf2-z1-stdds05	100 GiB	
anf2-z1-stdds06	100 GiB	
anf2-z1-stdds07	100 GiB	
anf2-z1-stdds08	100 GiB	
anf-z1-stdds01	6 TiB	
anf-z1-stdds02	200 GiB	
anf-z1-stdds03	1 TiB	
anf-z1-stdds04	200 GiB	
anf-z1-stdds06	200 GiB	
anf-z1-stdds07	200 GiB	
anf-z1-stdds08	200 GiB	
anf-zq-stdds05	1 TiB	
vol1	1 TiB	
vol3basic	100 GiB	
volnfsbasic	100 GiB	
volnfsstd	100 GiB	
volnfsstdnew	100 GiB	
zone1basic	6 TiB	
zone2basic	100 GiB	

Create a volume ...

Basics Protocol Tags Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name database Value oracle

Review + create < Previous Next : Review + create >

The screenshot shows the 'Create a volume' wizard in the Azure NetApp Files portal. The 'Tags' tab is active. A single tag named 'database' with the value 'oracle' is listed. The 'Review + create' button is visible at the bottom.

6. If the validation passes, click **Create** to create the volume.

Install and configure Oracle on Azure VM with ANF

The NetApp solutions team has created many Ansible-based automation toolkits to help you deploy Oracle in Azure smoothly. Follow these steps to deploy Oracle on an Azure VM.

Set up an Ansible controller

If you have not set up an Ansible controller, see [NetApp Solution Automation](#), which has detailed instructions on how to setup an Ansible controller.

Obtain Oracle deployment automation toolkit

Clone a copy of the Oracle deployment toolkit in your home directory under the user ID that you use to log into the Ansible controller.

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

Execute the toolkit with your configuration

See the [CLI deployment Oracle 19c Database](#) to execute the playbook with the CLI. You can ignore the ONTAP portion of the variables configuration in the global VARS file when you create database volumes from

the Azure console rather than the CLI.



The toolkit default deploys Oracle 19c with RU 19.8. It can be easily adapted for any other patch level with minor default configuration changes. Also default seed-database active log files are deployed into the data volume. If you need active log files on the log volume, it should be relocated after initial deployment. Reach out to the NetApp Solution team for help if needed.

Set up AzAcSnap backup tool for app-consistent snapshots for Oracle

The Azure Application-Consistent Snapshot tool (AzAcSnap) is a command-line tool that enables data protection for third-party databases by handling all the orchestration required to put them into an application-consistent state before taking a storage snapshot. It then returns these databases to an operational state. NetApp recommends installing the tool on the database server host. See the following installation and configuration procedures.

Install AzAcSnap tool

1. Get the most recent version of the [the AzArcSnap Installer](#).
2. Copy the downloaded self-installer to the target system.
3. Execute the self-installer as the root user with the default installation option. If necessary, make the file executable using the `chmod +x *.run` command.

```
./azacsnap_installer_v5.0.run -I
```

Configure Oracle connectivity

The snapshot tools communicate with the Oracle database and need a database user with appropriate permissions to enable or disable backup mode.

1. Set up AzAcSnap database user

The following examples show the setup of the Oracle database user and the use of sqlplus for communication to the Oracle database. The example commands set up a user (AZACSNAP) in the Oracle database and change the IP address, usernames, and passwords as appropriate.

1. From the Oracle database installation, launch sqlplus to log into the database.

```
su - oracle  
sqlplus / AS SYSDBA
```

2. Create the user.

```
CREATE USER azacsnap IDENTIFIED BY password;
```

3. Grant the user permissions. This example sets the permission for the AZACSNAP user to enable putting the database into backup mode.

```
GRANT CREATE SESSION TO azacsnap;
GRANT SYSBACKUP TO azacsnap;
```

4. Change the default user's password expiration to unlimited.

```
ALTER PROFILE default LIMIT PASSWORD_LIFE_TIME unlimited;
```

5. Validate azacsnap connectivity for the database.

```
connect azacsnap/password
quit;
```

2. Configure Linux-user azacsnap for DB access with Oracle wallet

The AzAcSnap default installation creates an azacsnap OS user. It's Bash shell environment must be configured for Oracle database access with the password stored in an Oracle wallet.

1. As root user, run the `cat /etc/oratab` command to identify the ORACLE_HOME and ORACLE_SID variables on the host.

```
cat /etc/oratab
```

2. Add ORACLE_HOME, ORACLE_SID, TNS_ADMIN, and PATH variables to the azacsnap user bash profile. Change the variables as needed.

```
echo "export ORACLE_SID=ORATEST" >> /home/azacsnap/.bash_profile
echo "export ORACLE_HOME=/u01/app/oracle/product/19800/ORATST" >>
/home/azacsnap/.bash_profile
echo "export TNS_ADMIN=/home/azacsnap" >> /home/azacsnap/.bash_profile
echo "export PATH=\$PATH:\$ORACLE_HOME/bin" >>
/home/azacsnap/.bash_profile
```

3. As the Linux user azacsnap, create the wallet. You are prompted for the wallet password.

```
sudo su - azacsnap
```

```
mkstore -wrl $TNS_ADMIN/.oracle_wallet/ -create
```

4. Add the connect string credentials to the Oracle Wallet. In the following example command, AZACSNAP is the ConnectString to be used by AzAcSnap, azacsnap is the Oracle Database User, and AzPasswd1 is the

Oracle User's database password. You are again prompted for the wallet password.

```
mkstore -wrl $TNS_ADMIN/.oracle_wallet/ -createCredential AZACSNAP  
azacsnap AzPasswd1
```

5. Create the `tnsnames.ora` file. In the following example command, HOST should be set to the IP address of the Oracle Database and the Server SID should be set to the Oracle Database SID.

```
echo "# Connection string  
AZACSNAP=\\"(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP) (HOST=172.30.137.142) (POR  
T=1521)) (CONNECT_DATA=(SID=ORATST)))\\"  
" > $TNS_ADMIN/tnsnames.ora
```

6. Create the `sqlnet.ora` file.

```
echo "SQLNET.WALLET_OVERRIDE = TRUE  
WALLET_LOCATION=()  
    SOURCE=(METHOD=FILE)  
        (METHOD_DATA=(DIRECTORY=\$TNS_ADMIN/.oracle_wallet))  
)" > $TNS_ADMIN/sqlnet.ora
```

7. Test Oracle access using the wallet.

```
sqlplus /@AZACSNAP as SYSBACKUP
```

The expected output from the command:

```
[azacsnap@acao-ora01 ~]$ sqlplus /@AZACSNAP as SYSBACKUP
```

```
SQL*Plus: Release 19.0.0.0.0 - Production on Thu Sep 8 18:02:07 2022  
Version 19.8.0.0
```

```
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>
```

Configure ANF connectivity

This section explains how to enable communication with Azure NetApp Files (with a VM).

1. Within an Azure Cloud Shell session, make sure that you are logged into the subscription that you want to be associated with the service principal by default.

```
az account show
```

2. If the subscription isn't correct, use the following command:

```
az account set -s <subscription name or id>
```

3. Create a service principal using the Azure CLI as in the following example:

```
az ad sp create-for-rbac --name "AzAcSnap" --role Contributor --scopes /subscriptions/{subscription-id} --sdk-auth
```

The expected output:

```
{  
  "clientId": "00aa000a-aaaa-0000-00a0-00aa000aaa0a",  
  "clientSecret": "00aa000a-aaaa-0000-00a0-00aa000aaa0a",  
  "subscriptionId": "00aa000a-aaaa-0000-00a0-00aa000aaa0a",  
  "tenantId": "00aa000a-aaaa-0000-00a0-00aa000aaa0a",  
  "activeDirectoryEndpointUrl": "https://login.microsoftonline.com",  
  "resourceManagerEndpointUrl": "https://management.azure.com/",  
  "activeDirectoryGraphResourceId": "https://graph.windows.net/",  
  "sqlManagementEndpointUrl": "https://management.core.windows.net:8443/",  
  "galleryEndpointUrl": "https://gallery.azure.com/",  
  "managementEndpointUrl": "https://management.core.windows.net/"  
}
```

4. Cut and paste the output content into a file called `oracle.json` stored in the Linux user `azacsnap` user bin directory and secure the file with the appropriate system permissions.



Make sure the format of the JSON file is exactly as described above, especially with the URLs enclosed in double quotes ("").

Complete the setup of AzAcSnap tool

Follow these steps to configure and test the snapshot tools. After successful testing, you can perform the first database-consistent storage snapshot.

1. Change into the snapshot user account.

```
su - azacsnap
```

2. Change the location of commands.

```
cd /home/azacsnap/bin/
```

3. Configure a storage backup detail file. This creates an `azacsnap.json` configuration file.

```
azacsnap -c configure --configuration new
```

The expected output with three Oracle volumes:

```
[azacsnap@acao-ora01 bin]$ azacsnap -c configure --configuration new
Building new config file
Add comment to config file (blank entry to exit adding comments): Oracle snapshot bkup
Add comment to config file (blank entry to exit adding comments):
Enter the database type to add, 'hana', 'oracle', or 'exit' (for no database): oracle

==== Add Oracle Database details ====
Oracle Database SID (e.g. CDB1): ORATST
Database Server's Address (hostname or IP address): 172.30.137.142
Oracle connect string (e.g. /@AZACSNAP): /@AZACSNAP

==== Azure NetApp Files Storage details ====<br> Are you using Azure NetApp Files for the database? (y/n)
[n]: y<br> --- DATA Volumes have the Application put into a consistent state before they are snapshot
---<br> Add Azure NetApp Files resource to DATA Volume section of Database configuration? (y/n) [n]:
y<br> Full Azure NetApp Files Storage Volume Resource ID (e.g.
/subscriptions/&#8230;&#8203;/resourceGroups/&#8230;&#8203;/providers/Microsoft.NetApp/netAppAcco
unts/&#8230;&#8203;/capacityPools/Premium/volumes/&#8230;&#8203;): /subscriptions/0efa2dfb-917c-
4497-b56a-
b3f4eadb8111/resourceGroups/ANFAVSRG/providers/Microsoft.NetApp/netAppAccounts/ANFAVSAcct/ca
pacityPools/CapPool/volumes/acao-ora01-u01<br> Service Principal Authentication filename or Azure Key
Vault Resource ID (e.g. auth-file.json or <a href="https://&#8230;&#8203;" class="bare">https://&#8230;&#
8203;</a>): oracle.json<br> Add Azure NetApp Files resource to DATA Volume section of Database
configuration? (y/n) [n]: y<br> Full Azure NetApp Files Storage Volume Resource ID (e.g.
/subscriptions/&#8230;&#8203;/resourceGroups/&#8230;&#8203;/providers/Microsoft.NetApp/netAppAcco
unts/&#8230;&#8203;/capacityPools/Premium/volumes/&#8230;&#8203;): /subscriptions/0efa2dfb-917c-
4497-b56a-
b3f4eadb8111/resourceGroups/ANFAVSRG/providers/Microsoft.NetApp/netAppAccounts/ANFAVSAcct/ca
pacityPools/CapPool/volumes/acao-ora01-u02<br> Service Principal Authentication filename or Azure Key
Vault Resource ID (e.g. auth-file.json or <a href="https://&#8230;&#8203;" class="bare">https://&#8230;&#
8203;</a>): oracle.json<br> Add Azure NetApp Files resource to DATA Volume section of Database
configuration? (y/n) [n]: n<br> --- OTHER Volumes are snapshot immediately without preparing any
application for snapshot ---<br> Add Azure NetApp Files resource to OTHER Volume section of Database
configuration? (y/n) [n]: y<br> Full Azure NetApp Files Storage Volume Resource ID (e.g.
/subscriptions/&#8230;&#8203;/resourceGroups/&#8230;&#8203;/providers/Microsoft.NetApp/netAppAcco
unts/&#8230;&#8203;/capacityPools/Premium/volumes/&#8230;&#8203;): /subscriptions/0efa2dfb-917c-
4497-b56a-
b3f4eadb8111/resourceGroups/ANFAVSRG/providers/Microsoft.NetApp/netAppAccounts/ANFAVSAcct/ca
pacityPools/CapPool/volumes/acao-ora01-u03<br> Service Principal Authentication filename or Azure Key
Vault Resource ID (e.g. auth-file.json or <a href="https://&#8230;&#8203;" class="bare">https://&#8230;&#
8203;</a>): oracle.json<br> Add Azure NetApp Files resource to OTHER Volume section of Database
configuration? (y/n) [n]: n

==== Azure Managed Disk details ====
Are you using Azure Managed Disks for the database? (y/n) [n]: n

==== Azure Large Instance (Bare Metal) Storage details ====
```

Are you using Azure Large Instance (Bare Metal) for the database? (y/n) [n]: n

Enter the database type to add, 'hana', 'oracle', or 'exit' (for no database): exit

Editing configuration complete, writing output to 'azacsnap.json'.

4. As the azacsnap Linux user, run the azacsnap test command for an Oracle backup.

```
cd ~/bin  
azacsnap -c test --test oracle --configfile azacsnap.json
```

The expected output:

```
[azacsnap@acao-ora01 bin]$ azacsnap -c test --test oracle --configfile azacsnap.json  
BEGIN : Test process started for 'oracle'  
BEGIN : Oracle DB tests  
PASSED: Successful connectivity to Oracle DB version 1908000000  
END : Test process complete for 'oracle'  
[azacsnap@acao-ora01 bin]$
```

5. Run your first snapshot backup.

```
azacsnap -c backup --volume data --prefix ora_test --retention=1
```

[Next: Database protection.](#)

Protect your Oracle database in Azure cloud

[Previous: Deployment procedures.](#)

Backup Oracle database with snapshot using AzAcSnap tool

The Azure Application-Consistent Snapshot tool (AzAcSnap) is a command-line tool that enables data protection for third-party databases by handling all the orchestration required to put them into an application-consistent state before taking a storage snapshot, after which it returns the databases to an operational state.

In the case of Oracle, you put the database in backup mode to take a snapshot and then take the database out of backup mode.

Backup data and log volumes

The backup can be set up on the database server host with simple shell script that executes the snapshot command. Then, the script can be scheduled to run from crontab.

Generally, the frequency of backup depends on the desired RTO and RPO. Frequent snapshot creation consumes more storage space. There is a trade off between the frequency of backup and space consumption.

Data volumes typically consume more storage space than log volumes. Therefore, you can take snapshots on data volumes every few hours and more frequent snapshots on log volumes every 15 to 30 minutes.

See the following examples of backup scripts and scheduling.

For data volume snapshots:

```
# /bin/sh
cd /home/azacsnap/bin
. ~/.bash_profile
azacsnap -c backup --volume data --prefix acao-ora01-data --retention 36
azacsnap -c backup --volume other --prefix acao-ora01-log --retention 250
```

For log volume snapshots:

```
# /bin/sh
cd /home/azacsnap/bin
. ~/.bash_profile
azacsnap -c backup --volume other --prefix acao-ora01-log --retention 250
```

Crontab schedule:

```
15,30,45 * * * * /home/azacsnap/snap_log.sh
0 */2 * * * /home/azacsnap/snap_data.sh
```



When setting up the backup `azacsnap.json` configuration file, add all data volumes, including the binary volume, to `dataVolume` and all log volumes to `otherVolume`. The maximum retention of snapshots is 250 copies.

Validate the snapshots

Go to the Azure portal > Azure NetApp Files/volumes to check if the snapshots have been successfully created.

The screenshot shows two side-by-side Azure portal pages. The left page is titled 'ANFAVSAcct | Volumes' and lists several volumes: 'acao-ora01-u01' (100 GB), 'acao-ora01-u02' (100 GB), 'acao-ora01-u03' (100 GB), 'anf2-z1-stdds01' (200 GB), 'anf2-z1-stdds02' (200 GB), 'anf2-z1-stdds03' (100 GB), 'anf2-z1-stdds04' (100 GB), 'anf2-z1-stdds05' (100 GB), 'anf2-z1-stdds06' (100 GB), 'anf2-z1-stdds07' (100 GB), 'anf2-z1-stdds08' (100 GB), and 'anf2-z1-stdds09' (6 TB). The right page is titled 'acao-ora01-u01 (ANFAVSAcct/CapPool/acao-ora01-u01) | Snapshots' and lists two snapshots: 'acao-ora01-data_2022-09-09T165255-82588522' (Created 09/09/2022, 12:53:22 PM) and 'acao-ora01-data_2022-09-12T160536-98098392' (Created 09/12/2022, 12:05:55 PM).

The screenshot shows the Microsoft Azure portal interface. On the left, the 'ANFAVSAct | Volumes' page is displayed, showing a list of volumes including 'acao-ora01-u01' (100 GiB), 'acao-ora01-u02' (100 GiB), and 'acao-ora01-u03' (100 GiB). The 'Volumes' section is selected. On the right, a detailed view of the 'acao-ora01-u03' volume is shown, specifically the 'Schemas' tab under 'Schemas'. Below this, a table lists 'Schemas' and their 'Status'. At the bottom, there are tabs for 'Script', 'SQL', and 'PowerShell'.

Oracle restore and recovery from local backup

One of key benefits of snapshot backup is that it coexists with source database volumes, and the primary database volumes can be rolled back almost instantly.

Restore and recovery of Oracle on the primary server

The following example demonstrates how to restore and recover an Oracle database from the Azure dashboard and CLI on the same Oracle host.

1. Create a test table in the database to be restored.
[oracle@acao-ora01 ~]\$ sqlplus / as sysdba

```
SQL*Plus: Release 19.0.0.0.0 - Production on Mon Sep 12 19:02:35 2022
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> create table testsnapshot(
id integer,
event varchar(100),
dt timestamp);
```

Table created.

```
SQL> insert into testsnapshot values(1,'insert a data marker to validate snapshot restore',sysdate);
```

1 row created.

```
SQL> commit;
```

Commit complete.

```
SQL> select * from testsnapshot;
```

ID

EVENT

DT

1
insert a data marker to validate snapshot restore
12-SEP-22 07.07.35.000000 PM

2. Drop the table after the snapshot backups.

```
[oracle@acao-ora01 ~]$ sqlplus / as sysdba
```

```
SQL*Plus: Release 19.0.0.0.0 - Production on Tue Sep 13 14:20:22 2022
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> drop table testsnapshot;
```

```
Table dropped.
```

```
SQL> select * from testsnapshot;
select * from testsnapshot
*
ERROR at line 1:
ORA-00942: table or view does not exist
```

```
SQL> shutdown immediate;
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL> exit
Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.8.0.0.0
```

3. From the Azure NetApp Files dashboard, restore the log volume to the last available snapshot. Choose **Revert volume**.

ANFAVSACct | Volumes

- Overview
- Activity log
- Access control (IAM)
- Tags
- Settings
- Quota
- Properties
- Locks
- Azure NetApp Files
- Active Directory connections
- Storage service
- Capacity pools
- Volumes
- Application volume groups
- Data protection

acao-ora01-u03 (ANFAVSACct/CapPool/acao-ora01-u03) | Snapshots

- Overview
- Activity log
- Access control (IAM)
- Tags
- Settings
- Properties
- Locks
- Storage service
- Mount instructions
- Export policy
- Snapshots
- Replication
- Monitoring
- Metrics
- Automation

4. Confirm revert volume and click Revert to complete the volume reversion to the latest available backup.

Revert volume to snapshot

Revert volume acao-ora01-u03 to snapshot acao-ora01-log_2022-09-13...

This action is irreversible and it will delete all the volumes snapshots that are newer than acao-ora01-log_2022-09-13T134502-0449919Z. Please type the volume name acao-ora01-u03 to confirm.

Are you sure you want to revert the volume to the state of acao-ora01-log_2022-09-13T134502-0449919Z? Please type the volume name acao-ora01-u03 to confirm.

acao-ora01-u03

Revert **Cancel**

5. Repeat the same steps for the data volume, and make sure that the backup contains the table to be recovered.

Revert volume to snapshot

Revert volume acao-ora01-u02 to snapshot acao-ora01-data_2022-09-13T020001-9503384Z

This action is irreversible and it will delete all the volumes snapshots that are newer than acao-ora01-data_2022-09-13T020001-9503384Z. Please type the volume name acao-ora01-u02 to confirm.

Are you sure you want to revert the volume to the state of acao-ora01-data_2022-09-13T020001-9503384Z? Please type the volume name acao-ora01-u02 to confirm.

acao-ora01-u02

Revert **Cancel**

6. Again confirm the volume reversion, and click "Revert."

The screenshot shows the Azure NetApp Files interface. On the left, the 'Volumes' section lists several volumes, including 'acao-ora01-u01', 'acao-ora01-u02' (which is selected), 'acao-ora01-u03', and others. On the right, the 'Schemas' section shows a list of snapshots. A modal window titled 'Revert volume to snapshot' is displayed, containing a warning message about irreversible deletion of snapshots older than the target. It includes a text input field with 'acao-ora01-u02' and two buttons: 'Revert' (highlighted in yellow) and 'Cancel'.

7. Resync the control files if you have multiple copies of them, and replace the old control file with the latest copy available.

```
[oracle@acao-ora01 ~]$ mv /u02/oradata/ORATST/control01.ctl /u02/oradata/ORATST/control01.ctl.bk
[oracle@acao-ora01 ~]$ cp /u03/orareco/ORATST/control02.ctl /u02/oradata/ORATST/control01.ctl
```

8. Log into the Oracle server VM and run database recovery with sqlplus.

```
[oracle@acao-ora01 ~]$ sqlplus / as sysdba
```

```
SQL*Plus: Release 19.0.0.0.0 - Production on Tue Sep 13 15:10:17 2022
Version 19.8.0.0
```

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

Connected to an idle instance.

```
SQL> startup mount;
ORACLE instance started.
```

Total System Global Area 6442448984 bytes

Fixed Size 8910936 bytes

Variable Size 1090519040 bytes

Database Buffers 5335154688 bytes

Redo Buffers 7864320 bytes

Database mounted.

```
SQL> recover database using backup controlfile until cancel;
```

ORA-00279: change 3188523 generated at 09/13/2022 10:00:09 needed for thread 1

ORA-00289: suggestion :

/u03/orareco/ORATST/archivelog/2022_09_13/o1_mf_1_43_22rnjq9q_.arc

ORA-00280: change 3188523 for thread 1 is in sequence #43

Specify log: {<RET>=suggested | filename | AUTO | CANCEL}

ORA-00279: change 3188862 generated at 09/13/2022 10:01:20 needed for thread 1
ORA-00289: suggestion :
/u03/orareco/ORATST/archivelog/2022_09_13/o1_mf_1_4429f2lgb5_.arc
ORA-00280: *change 3188862 for thread 1 is in sequence #44*
ORA-00278: *log file*
'/u03/orareco/ORATST/archivelog/2022_09_13/o1_mf_1_4322rnjq9q_.arc' no longer
needed for this recovery

Specify log: {<RET>=suggested | filename | AUTO | CANCEL}

ORA-00279: change 3193117 generated at 09/13/2022 12:00:08 needed for thread 1
ORA-00289: suggestion :
/u03/orareco/ORATST/archivelog/2022_09_13/o1_mf_1_4529h6qqyw_.arc
ORA-00280: *change 3193117 for thread 1 is in sequence #45*
ORA-00278: *log file*
'/u03/orareco/ORATST/archivelog/2022_09_13/o1_mf_1_4429f2lgb5_.arc' no longer
needed for this recovery

Specify log: {<RET>=suggested | filename | AUTO | CANCEL}

ORA-00279: change 3193440 generated at 09/13/2022 12:01:20 needed for thread 1
ORA-00289: suggestion :
/u03/orareco/ORATST/archivelog/2022_09_13/o1_mf_1_46_%u_.arc
ORA-00280: *change 3193440 for thread 1 is in sequence #46*
ORA-00278: *log file*
'/u03/orareco/ORATST/archivelog/2022_09_13/o1_mf_1_45_29h6qqyw_.arc' no longer
needed for this recovery

Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
cancel

Media recovery cancelled.

SQL> alter database open resetlogs;

Database altered.

SQL> select * from testsnapshot;

ID

```

EVENT
-----
-----
DT
-----
---

1
insert a data marker to validate snapshot restore
12-SEP-22 07.07.35.000000 PM

SQL> select systimestamp from dual;

SYSTIMESTAMP
-----
---
13-SEP-22 03.28.52.646977 PM +00:00

```

This screen demonstrates that the dropped table has been recovered using local snapshot backups.

[Next: Database migration.](#)

Database migration from on-premises to Azure cloud

[Previous: Database protection.](#)

As a result of the Oracle decision to phase out single-instance databases, many organizations have converted single-instance Oracle databases to multitenant container databases. This enables the easy relocation of a subset of container databases called PDB to cloud with the maximum availability option, which minimize downtime during migration.

However, if you still have a single instance of a Oracle database, it can first be converted into a multitenant container database in place before attempting PDB relocation.

The following sections provide details for the migration of on-premises Oracle databases to Azure cloud in either scenarios.

Converting a single instance non-CDB to a PDB in a multitenant CDB

If you still have a single-instance Oracle database, it must be converted into a multitenant container database whether you wish to migrate it to the cloud or not, because Oracle will stop supporting single-instance databases some time soon.

The following procedures plug a single instance database into a container database as a pluggable database or PDB.

1. Build a shell container database on the same host as the single-instance database in a separate ORACLE_HOME.
2. Shut down the single instance database and restart it in read-only mode.

3. Run the DBMS_PDB.DESCRIBE procedure to generate the database metadata.

```
BEGIN
    DBMS_PDB.DESCRIBE(
        pdb_descr_file => '/home/oracle/ncdb.xml');
END;
/
```

4. Shut down the single-instance database.
5. Start up the container database.
6. Run the DBMS_PDB.CHECK_PLUG_COMPATIBILITY function to determine whether the non-CDB is compatible with the CDB.

```
SET SERVEROUTPUT ON
DECLARE
    compatible CONSTANT VARCHAR2(3) :=
        CASE DBMS_PDB.CHECK_PLUG_COMPATIBILITY(
            pdb_descr_file => '/disk1/oracle/ncdb.xml',
            pdb_name       => 'NCDB')
            WHEN TRUE THEN 'YES'
            ELSE 'NO'
        END;
BEGIN
    DBMS_OUTPUT.PUT_LINE(compatible);
END;
/
```

If the output is YES, then the non-CDB is compatible, and you can continue with the next step.

If the output is NO, then the non-CDB is not compatible, and you can check the PDB_PLUG_IN_VIOLATIONS view to see why it is not compatible. All violations must be corrected before you continue. For example, any version or patch mismatches should be resolved by running an upgrade or the opatch utility. After correcting the violations, run DBMS_PDB.CHECK_PLUG_COMPATIBILITY again to ensure that the non-CDB is compatible with the CDB.

7. Plug in the single instance non-CDB.

```
CREATE PLUGGABLE DATABASE ncdb USING '/home/oracle/ncdb.xml'
COPY
FILE_NAME_CONVERT = ('/disk1/oracle/dbs/', '/disk2/oracle/ncdb/')
;
```



If there is not sufficient space on the host, the NOCOPY option can be used to create the PDB. In that case, a single-instance non-CDB is not useable after plug in as a PDB because the original data files has been used for the PDB. Make sure to create a backup before the conversion so that there is something to fall back on if anything goes wrong.

8. Start with PDB upgrade after conversion if the version between the source single-instance non-CDB and the target CDB are different. For the same-version conversion, this step can be skipped.

```
sqlplus / as sysdba;
```

```
alter session set container=ncdb;
```

```
alter pluggable database open upgrade;  
exit;
```

```
dbupgrade -c ncdb -l /home/oracle
```

Review the upgrade log file in the /home/oracle directory.

9. Open the pluggable database, check for pdb plug-in violations, and recompile the invalid objects.

```
alter pluggable database ncdb open;
```

```
alter session set container=ncdb;  
select message from pdb_plug_inViolations where type like '%ERR%' and  
status <> 'RESOLVED';
```

```
$ORACLE_HOME/perl/bin/perl $ORACLE_HOME/rdbms/admin/catcon.pl -n 1 -c  
'ncdb' -e -b utlrp -d $ORACLE_HOME/rdbms/admin utlrp.sql
```

10. Execute noncdb_to_pdb.sql to update the data dictionary.

```
sqlplus / as sysdba
```

```
alter session set container=ncdb;  
@$ORACLE_HOME/rdbms/admin/noncdb_to_pdb.sql;
```

Shut down and restart the container DB. The ncdb is taken out of restricted mode.

Migrate on-premises Oracle databases to Azure with PDB relocation

Oracle PDB relocation with the maximum-availability option uses PDB hot-clone technology, which enables source PDB availability while the PDB is being copied over to the target. Upon switchover, sessions and connections are redirected to the target PDB automatically. Thus, down time is minimized independent of the size of the PDB being relocated. NetApp provides an Ansible-based toolkit that automates the migration procedure.

1. Create a CDB in the Azure public cloud on an Azure VM with the same version and patch level.
2. From the Ansible controller, clone a copy of the automation toolkit.

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

3. Read the instruction in the README file.
4. Configure the Ansible host variable files for both the source and target Oracle servers and the DB server host's configuration file for name resolution.
5. Install the Ansible controller prerequisites on Ansible controller.

```
ansible-playbook -i hosts requirements.yml  
ansible-galaxy collection install -r collections/requirements.yml  
--force
```

6. Execute any pre-migration tasks against the on-premises server.

```
ansible-playbook -i hosts ora_pdb_relocate.yml -u admin -k -K -t  
ora_pdb_relo_onprem
```



The admin user is the management user on the on-premises Oracle server host with sudo privileges. The admin user is authenticated with a password.

7. Execute Oracle PDB relocation from on-premises to the target Azure Oracle host.

```
ansible-playbook -i hosts ora_pdb_relocate.yml -u azureuser --private  
-key dbl.pem -t ora_pdb_relo_primary
```



The Ansible controller can be located either on-premises or in the Azure cloud. The controller needs connectivity to the on-premises Oracle server host and the Azure Oracle VM host. The Oracle database port (such as 1521) is open between the on-premises Oracle server host and the Azure Oracle VM host.

Additional Oracle database migration options

Please see the Microsoft documentation for additional migration options: [Oracle database migration decision process](#).

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

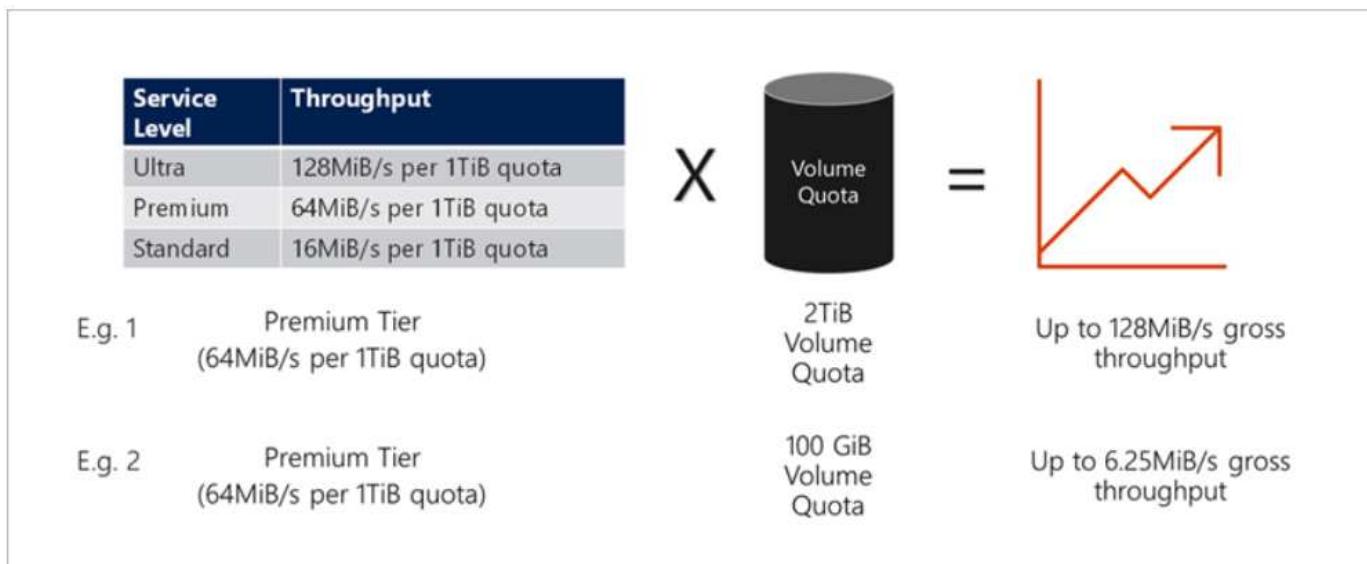
Next : Tags >

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](#).



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

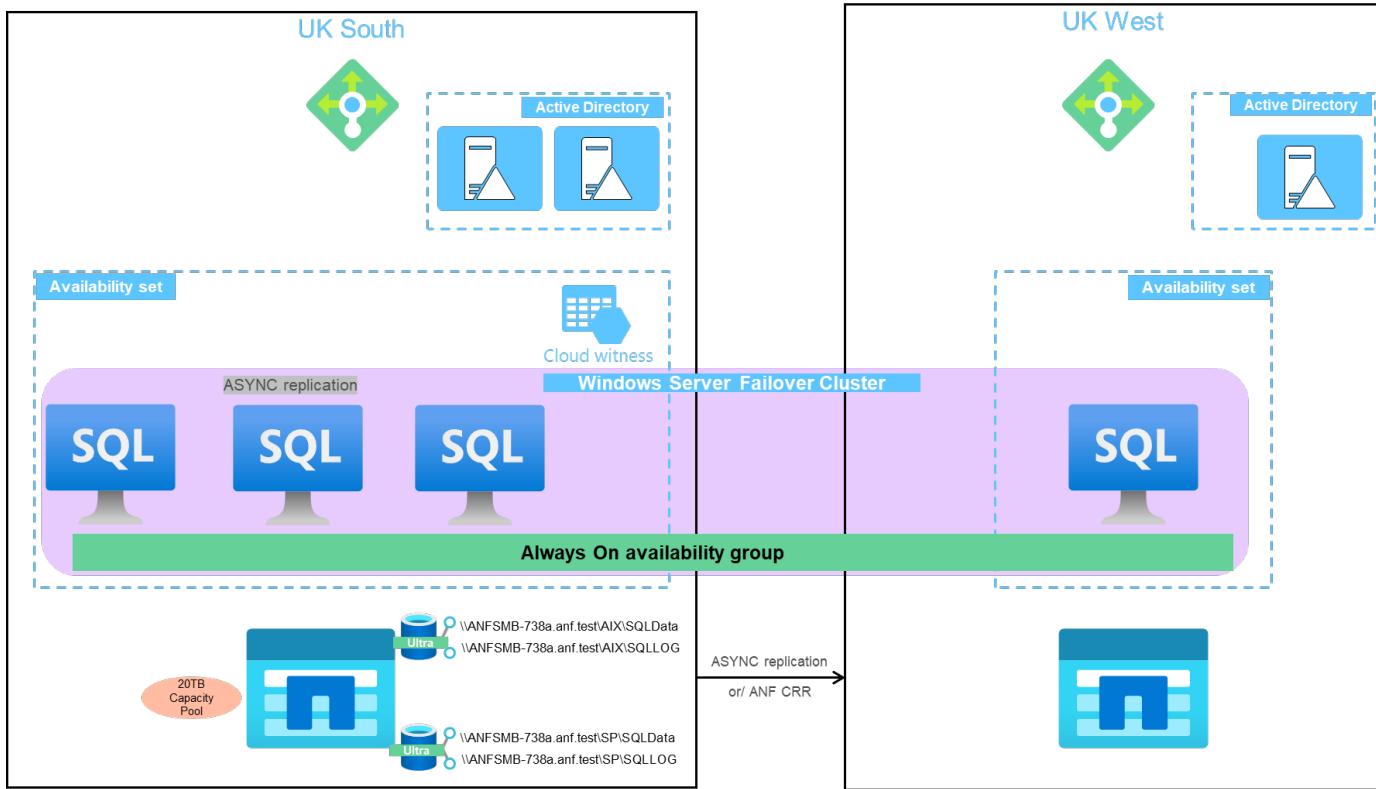
This section covers a real-time deployment of a SQL database estate in an AOAG configuration using an Azure NetApp Files SMB volume.

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

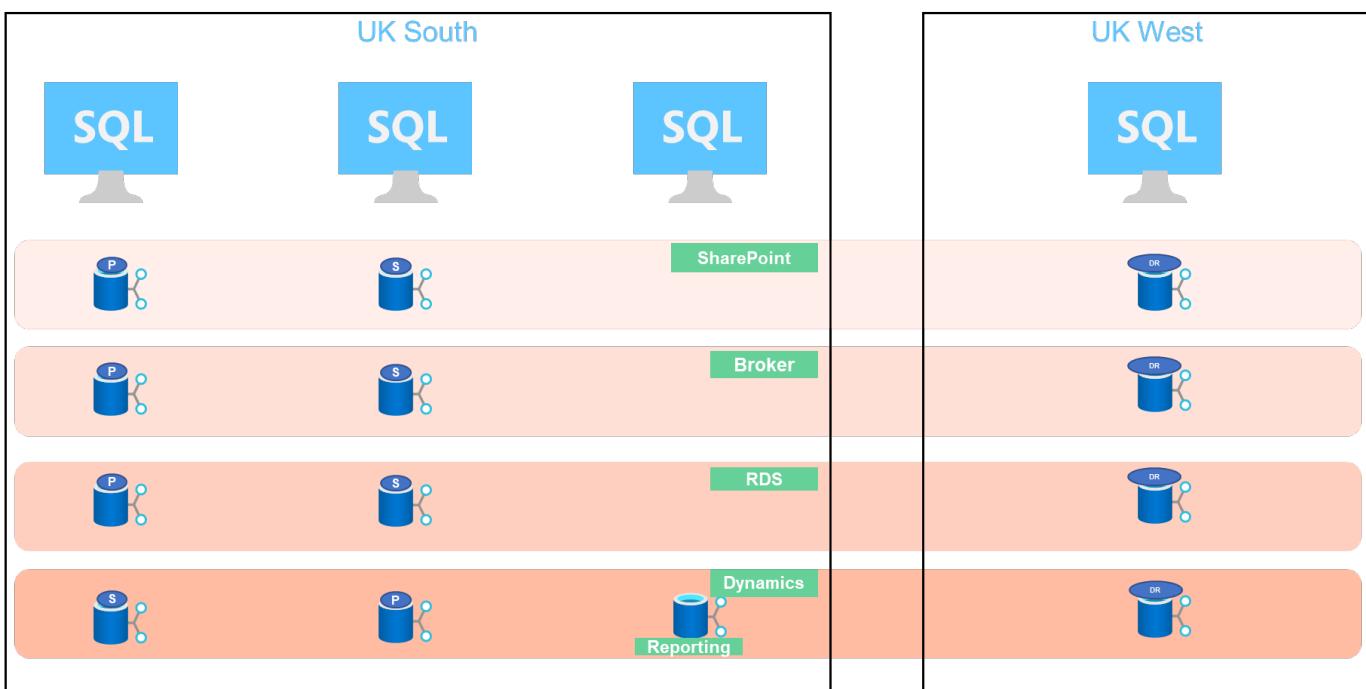
- Backup retention: 7 days
- Backup archive: 365 days



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.

Avg Total throughput for volume1 [edit]

Add metric Add filter Apply splitting Line chart ▼ Drill into Logs ▼ New alert rule Pin to dashboard ...

Scope	Metric Namespace	Metric	Aggregation
volume1	NetApp Volumes stand...	Total throughput	Avg

Percentage Volume Consumed Size
Read iops
Read throughput
Total throughput
Volume allocated size
Volume Backup Bytes

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>

TR-4923: SQL Server on AWS EC2 using Amazon FSx for NetApp ONTAP

Authors: Pat Sinthusan and Niyaz Mohamed, NetApp

Introduction

Many companies that would like to migrate applications from on-premises to the cloud find that the effort is hindered by the differences in capabilities offered by on-premises storage systems and cloud storage services. That gap has made migrating enterprise applications such as Microsoft SQL Server much more problematic. In particular, gaps in the services needed to run an enterprise application such as robust snapshots, storage efficiency capabilities, high availability, reliability, and consistent performance have forced customers to make design tradeoffs or forgo application migration. With FSx for NetApp ONTAP, customers no longer need to compromise. FSx for NetApp ONTAP is a native (1st party) AWS service sold, supported, billed, and fully managed by AWS. It uses the power of NetApp ONTAP to provide the same enterprise grade storage and data management capabilities NetApp has provided on-premises for three decades in AWS as a managed service.

With SQL Server on EC2 instances, database administrators can access and customize their database environment and the underlying operating system. A SQL Server on EC2 instance in combination with [AWS FSx ONTAP](#) to store the database files, enables high performance, data management, and a simple and easy migration path using block-level replication. Therefore, you can run your complex database on AWS VPC with an easy lift-and-shift approach, fewer clicks, and no schema conversions.

Benefits of using Amazon FSx for NetApp ONTAP with SQL Server

Amazon FSx for NetApp ONTAP is the ideal file storage for SQL Server deployments in AWS. Benefits include the following:

- Consistent high performance and throughput with low latency
- Intelligent caching with NVMe cache to improve performance
- Flexible sizing so that you can increase or shrink capacity, throughput, and IOPs on the fly
- Efficient on-premises-to-AWS block replication
- The use of iSCSI, a well-known protocol for the database environment
- Storage efficiency features like thin provisioning and zero-footprint clones
- Backup time reduction from hours to mins, thereby reducing the RTO
- Granular backup and recovery of SQL databases with the intuitive NetApp SnapCenter UI
- The ability to perform multiple test migrations before actual migration
- Shorter downtime during migration and overcoming migration challenges with file-level or I/O-level copy
- Reducing MTTR by finding the root cause after a major release or patch update

Deploying SQL Server databases on FSx ONTAP with the iSCSI protocol, as is commonly used on-premises, provides an ideal database storage environment with superior performance, storage efficiency, and data-management capabilities. Using multiple iSCSI sessions, assuming a 5% working set size, fitting a Flash Cache delivers over 100K IOPs with the FSx ONTAP service. This configuration provides complete control over performance for the most demanding applications. SQL Server running on smaller EC2 instances connected to FSx for ONTAP can perform the same as SQL Server running on a much larger EC2 instance, because only network bandwidth limits are applied against FSx for ONTAP. Reducing the size of instances also reduces the compute cost, which provides a TCO-optimised deployment. The combination of SQL using iSCSI, SMB3.0 with multichannel, continuous availability shares on FSx for ONTAP provides great advantages for SQL workloads.

Before you begin

The combination of Amazon FSx for NetApp ONTAP and SQL Server on EC2 instance enables the creation of enterprise-level database storage designs that can meet today's most demanding application requirements. To optimize both technologies, it is vital to understand SQL Server I/O patterns and characteristics. A well-designed storage layout for a SQL Server database supports the performance of SQL Server and the management of the SQL Server infrastructure. A good storage layout also allows the initial deployment to be successful and the environment to grow smoothly over time as your business grows.

Prerequisites

Before you complete the steps in this document, you should have the following prerequisites:

- An AWS account
- Appropriate IAM roles to provision EC2 and FSx for ONTAP
- A Windows Active Directory domain on EC2
- All SQL Server nodes must be able to communicate with each other
- Make sure DNS resolution works and host names can be resolved. If not, use host file entry.
- General knowledge of SQL Server installation

Also, please refer to the NetApp Best Practices for SQL Server environments to ensure the best storage configuration.

Best practice configurations for SQL Server environments on EC2

With FSx ONTAP, procuring storage is the easiest task and can be performed by updating the file system. This simple process enables dynamic cost and performance optimization as needed, it helps to balance the SQL workload, and it is also a great enabler for thin provisioning. FSx ONTAP thin provisioning is designed to present more logical storage to EC2 instances running SQL Server than what is provisioned in the file system. Instead of allocating space upfront, storage space is dynamically allocated to each volume or LUN as data is written. In most configurations, free space is also released back when data in the volume or LUN is deleted (and is not being held by any Snapshot copies). The following table provides configuration settings for dynamically allocating storage.

Setting	Configuration
Volume guarantee	None (set by default)
LUN reservation	Enabled
fractional_reserve	0% (set by default)
snap_reserve	0%
Autodelete	volume / oldest_first
Autosize	On
try_first	Autogrow
Volume tiering policy	Snapshot only
Snapshot policy	None

With this configuration, the total size of the volumes can be greater than the actual storage available in the file system. If the LUNs or Snapshot copies require more space than is available in the volume, the volumes automatically grow, taking more space from the containing file system. Autogrow allows FSx ONTAP to automatically increase the size of the volume up to a maximum size that you predetermine. There must be space available in the containing file system to support the automatic growth of the volume. Therefore, with autogrow enabled, you should monitor the free space in the containing filesystem and update the file system when needed.

Along with this, set the [space-allocation](#) option on LUN to enabled so that FSx ONTAP notifies the EC2 host when the volume has run out of space and the LUN in the volume cannot accept writes. Also, this option enables FSx for ONTAP to reclaim space automatically when the SQL Server on EC2 host deletes data. The space-allocation option is set to disabled by default.



If a space-reserved LUN is created in a none-guaranteed volume, then the LUN behaves the same as a non-space-reserved LUN. This is because a none-guaranteed volume has no space to allocate to the LUN; the volume itself can only allocate space as it is written to due to its none guarantee.

With this configuration, FSx ONTAP administrators can generally size the volume so that they must manage and monitor the used space in the LUN on the host side and in the file system.



NetApp recommends using a separate file system for SQL server workloads. If the file system is used for multiple applications, monitor the space usage of both the file system and volumes within the file system to make sure that volumes are not competing for available space.



Snapshot copies used to create FlexClone volumes are not deleted by the autodelete option.



Overcommitment of storage must be carefully considered and managed for a mission-critical application such as SQL server for which even a minimal outage cannot be tolerated. In such a case, it is best to monitor storage consumption trends to determine how much, if any, overcommitment is acceptable.

Best Practices

- For optimal storage performance, provision file-system capacity to 1.5x times the size of total database usage.
- Appropriate monitoring accompanied by an effective action plan is required when using thin provisioning to avoid application downtime.
- Make sure to set Cloudwatch and other monitoring tool alerts so that people are contacted with enough time to react as storage is filled.

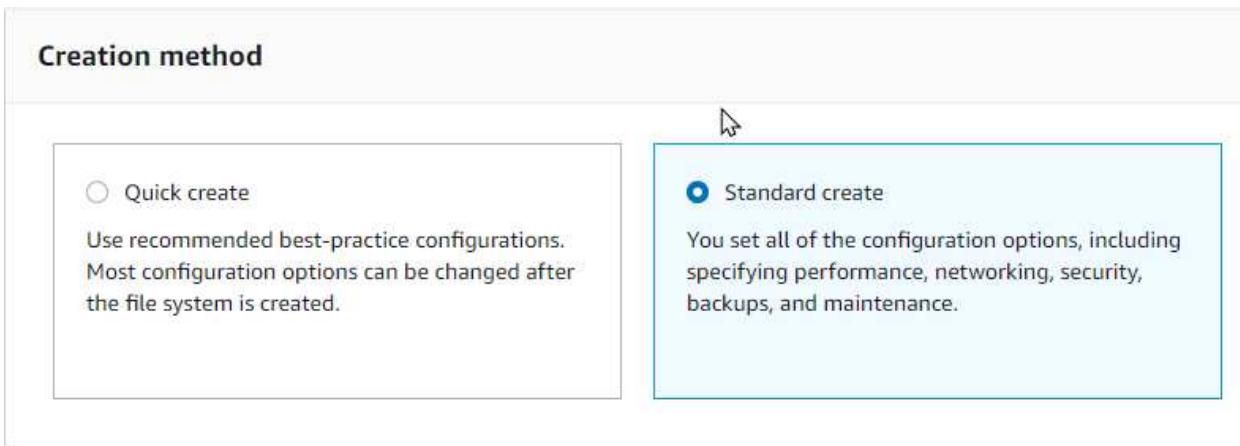
Configure Storage for SQL Server and deploy Snapcenter for Backup, Restore and clone operations

In order to perform SQL server operations with SnapCenter, you must first create volumes and LUNs for SQL server.

Create volumes and LUNs for SQL Server

To create volumes and LUNs for SQL Server, complete the following steps:

1. Open the Amazon FSx console at <https://console.aws.amazon.com/fsx/>
2. Create an Amazon FSx for the NetApp ONTAP file system using the Standard Create option under Creation Method. This allows you to define FSxadmin and vsadmin credentials.



3. Specify the password for fsxadmin.

File system administrative password

Password for this file system's "fsxadmin" user, which you can use to access the ONTAP CLI or REST API.

- Don't specify a password
 Specify a password

Password

Confirm password

4. Specify the password for SVMs.

SVM administrative password

Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.

- Don't specify a password
 Specify a password

Password

Confirm password

5. Create volumes by following the step listed in [Creating a volume on FSx for NetApp ONTAP](#).

Best practices

- Disable storage Snapshot copy schedules and retention policies. Instead, use NetApp SnapCenter to coordinate Snapshot copies of the SQL Server data and log volumes.
- Configure databases on individual LUNs on separate volumes to leverage fast and granular restore functionality.
- Place user data files (.mdf) on separate volumes because they are random read/write workloads. It is common to create transaction log backups more frequently than database backups. For this reason, place transaction log files (.ldf) on a separate volume from the data files so that independent backup schedules can be created for each. This separation also isolates the sequential write I/O of the log files from the random read/write I/O of data files and significantly improves SQL Server performance.
- Tempdb is a system database used by Microsoft SQL Server as a temporary workspace, especially for I/O intensive DBCC CHECKDB operations. Therefore, place this database on a dedicated volume. In large environments in which volume count is a challenge, you can consolidate tempdb into fewer volumes and store it in the same volume as other system databases after careful planning. Data protection for tempdb is not a high priority because this database is recreated every time Microsoft SQL Server is restarted.

6. Use the following SSH command to create volumes:

```
Vol create -vserver svm001 -volume vol_awssqlprod01_data -aggregate aggr1 -size 800GB -state online -tiering-policy snapshot-only -percent-snapshot-space 0 -autosize-mode grow -snapshot-policy none -security-style ntfs -aggregate aggr1
volume modify -vserver svm001 -volume vol_awssqlprod01_data -fractional-reserve 0
volume modify -vserver svm001 -volume vol_awssqlprod01_data -space -mgmt-try-first vol_grow
volume snapshot autodelete modify -vserver svm001 -volume vol_awssqlprod01_data -delete-order oldest_first
```

7. Start the iSCSI service with PowerShell using elevated privileges in Windows Servers.

```
Start-service -Name msiscsi
Set-Service -Name msiscsi -StartupType Automatic
```

8. Install Multipath-IO with PowerShell using elevated privileges in Windows Servers.

```
Install-WindowsFeature -name Multipath-IO -Restart
```

9. Find the Windows initiator Name with PowerShell using elevated privileges in Windows Servers.

```
Get-InitiatorPort | select NodeAddress
```

```
PS C:\Users\administrator.CONTOSO> Get-InitiatorPort | select NodeAddress  
NodeAddress  
-----  
iqn.1991-05.com.microsoft:ws2019-sql1.contoso.net
```

10. Connect to Storage virtual machines (SVM) using putty and create an iGroup.

```
igroup create -igroup igrp_ws2019sql1 -protocol iscsi -ostype windows -initiator iqn.1991-05.com.microsoft:ws2019-sql1.contoso.net
```

11. Use the following SSH command to create LUNs:

```
lun create -path /vol/vol_awssqlprod01_data/lun_awssqlprod01_data -size 700GB -ostype windows_2008 -space-reserve enabled -space-allocation enabled lun create -path /vol/vol_awssqlprod01_log/lun_awssqlprod01_log -size 100GB -ostype windows_2008 -space-reserve enabled -space-allocation enabled
```

```
svmsql::> lun create -path /vol/vol_awssqlprod01_data/lun_awssqlprod01_data -size 700GB -ostype windows_2008  
created a LUN of size 700g (751619276800)  
svmsql::> lun create -path /vol/vol_awssqlprod01_log/lun_awssqlprod01_log -size 100GB -ostype windows_2008  
Created a LUN of size 100g (107374182400)  
svmsql::> lun show  
Vserver Path State Mapped Type Size  
-----  
svmsql /vol/vol_awssqlprod01_data/lun_awssqlprod01_data online unmapped windows_2008  
700GB  
svmsql /vol/vol_awssqlprod01_log/lun_awssqlprod01_log online unmapped windows_2008  
100GB  
2 entries were displayed.
```

12. To achieve I/O alignment with the OS partitioning scheme, use windows_2008 as the recommended LUN type. Refer [here](#) for additional information.
13. Use the following SSH command to map igroup to the LUNs that you just created.

```
lun show  
lun map -path /vol/vol_awssqlprod01_data/lun_awssqlprod01_data -igroup igrp_awssqlprod01 lun map -path /vol/vol_awssqlprod01_log/lun_awssqlprod01_log -igroup igrp_awssqlprod01
```

```

svmsql::> lun show
Vserver   Path           State  Mapped  Type      Size
-----  -----
svmsql    /vol/vol_awssqlprod01_data/lun_awssqlprod01_data
          online  unmapped windows_2008
                           700GB
svmsql    /vol/vol_awssqlprod01_log/lun_awssqlprod01_log
          online  unmapped windows_2008
                           100GB
2 entries were displayed.

svmsql::> lun map -path /vol/vol_awssqlprod01_data/lun_awssqlprod01_data -igroup igrp_awssqlprod01
svmsql::> lun map -path /vol/vol_awssqlprod01_log/lun_awssqlprod01_log -igroup igrp_awssqlprod01
svmsql::>
svmsql::> lun show
Vserver   Path           State  Mapped  Type      Size
-----  -----
svmsql    /vol/vol_awssqlprod01_data/lun_awssqlprod01_data
          online  mapped   windows_2008
                           700GB
svmsql    /vol/vol_awssqlprod01_log/lun_awssqlprod01_log
          online  mapped   windows_2008
                           100GB
2 entries were displayed.

```

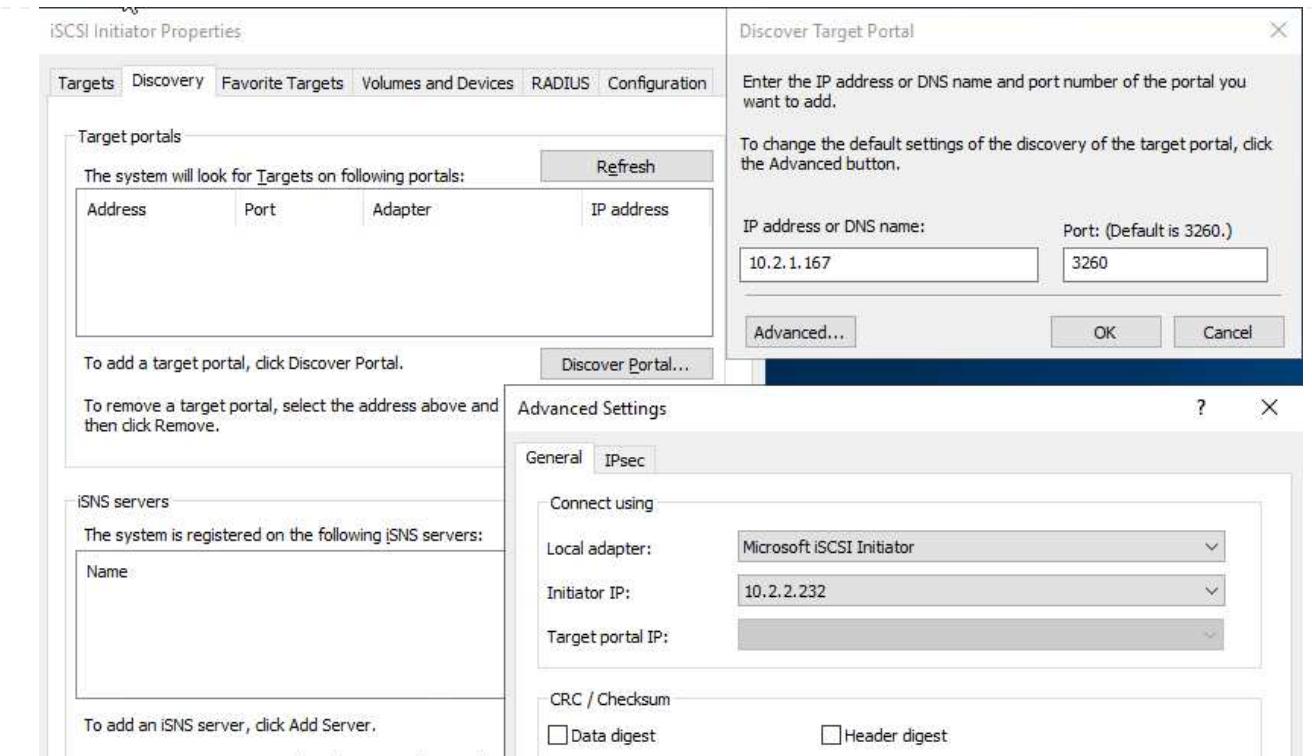
14. For a shared disk that uses the Windows Failover Cluster, run an SSH command to map the same LUN to the igroup that belong to all servers that participate in the Windows Failover Cluster.
15. Connect Windows Server to an SVM with an iSCSI target. Find the target IP address from AWS Portal.

svmsql (svm-09e98ab33a31b724a)

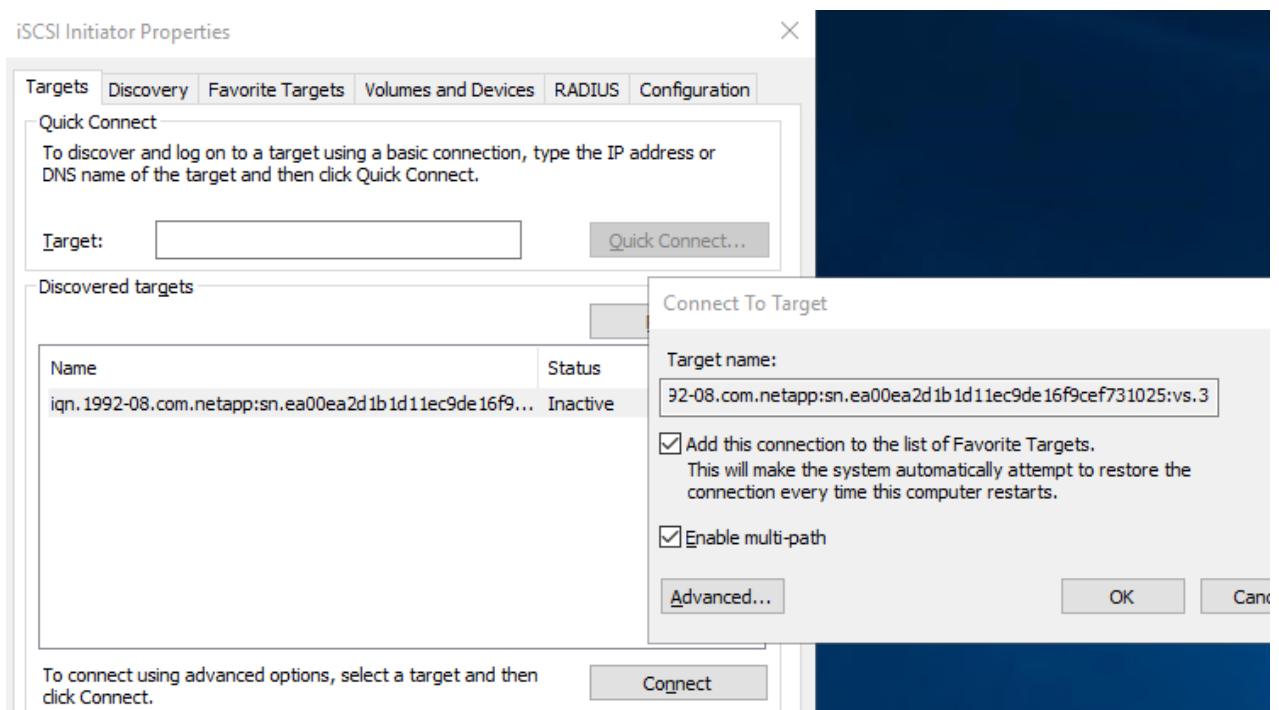
Summary	
SVM ID	Creation time 2021-09-21T13:19:34-07:00
svm-09e98ab33a31b724a	Lifecycle state Created
SVM name	Subtype DEFAULT
svmsql	
UUID	
ea00ea2d-1b1d-11ec-9de1-6f9cef731025	
File system ID	
fs-0ab4b447ebd6082aa	
Resource ARN	
arn:aws:fsx:us-west-2:139763910815:storage-virtual-machine/fs-0ab4b447ebd6082aa/svm-09e98ab33a31b724a	

Endpoints	
Management DNS name	Management IP address 198.19.255.153
svm-09e98ab33a31b724a.fs-0ab4b447ebd6082aa.fsx.us-west-2.amazonaws.com	
NFS DNS name	NFS IP address 198.19.255.153
svm-09e98ab33a31b724a.fs-0ab4b447ebd6082aa.fsx.us-west-2.amazonaws.com	
iSCSI DNS name	iSCSI IP addresses 10.2.1.167, 10.2.2.12
iscsi.svm-09e98ab33a31b724a.fs-0ab4b447ebd6082aa.fsx.us-west-2.amazonaws.com	

16. From Server Manager and the Tools menu, select the iSCSI Initiator. Select the Discovery tab and then select Discover Portal. Supply the iSCSI IP address from previous step and select Advanced. From Local Adapter, select Microsoft iSCSI Initiator. From Initiator IP, select the IP of the server. Then select OK to close all windows.



17. Repeat step 12 for the second iSCSI IP from the SVM.
18. Select the **Targets** tab, select **Connect**, and select **Enable multi-path**.



19. For best performance, add more sessions; NetApp recommends creating five iSCSI sessions. Select **Properties** > ***Add session** > ***Advanced** and repeat step 12.

```
$TargetPortals = ('10.2.1.167', '10.2.2.12')
foreach ($TargetPortal in $TargetPortals) {New-IscsiTargetPortal
-TargetPortalAddress $TargetPortal}
```

```
$TargetPortals = ('10.2.1.167', '10.2.2.12')
foreach ($TargetPortal in $TargetPortals) {New-IscsiTargetPortal -TargetPortalAddress $TargetPortal}

InitiatorInstanceName :
InitiatorPortalAddress :
IsDataDigest : False
IsHeaderDigest : False
TargetPortalAddress : 10.2.1.167
TargetPortalPortNumber : 3260
PSCoputerName :

InitiatorInstanceName :
InitiatorPortalAddress :
IsDataDigest : False
IsHeaderDigest : False
TargetPortalAddress : 10.2.2.12
TargetPortalPortNumber : 3260
PSCoputerName :
```

Best Practices

- Configure five iSCSI sessions per target interface for optimal performance.
- Configure a round-robin policy for the best overall iSCSI performance.
- Make sure that the allocation unit size is set to 64K for partitions when formatting the LUNs

20. Run the following PowerShell command to make sure that the iSCSI session is persisted.

```
$targets = Get-IscsiTarget
foreach ($target in $targets)
{
    Connect-IscsiTarget -IsMultipathEnabled $true -NodeAddress
    $target.NodeAddress -IsPersistent $true
}
```

```
PS C:\Windows\system32> Connect-IscsiTarget -NodeAddress (Get-IscsiTarget | select -ExpandProperty NodeAddress)

AuthenticationType : NONE
InitiatorInstanceName : ROOT\ISCSIPRT\0000_0
InitiatorNodeAddress : iqn.1991-05.com.microsoft:awssqlprod01.cloudheroes.dom
InitiatorPortalAddress : 0.0.0
InitiatorSideIdentifier : 400001370000
IsConnected : True
IsDataDigest : False
IsDiscovered : True
IsHeaderDigest : False
IsPersistent : True
NumberOfConnections : 1
SessionIdentifier : ffff9988350ff010-4000013700000012
TargetNodeAddress : iqn.1992-08.com.netapp:sn.ea00ea2d1b1d11ec9de16f9cef731025:vs.3
TargetsSideIdentifier : 0200
PSCoputerName :
```

21. Initialize disks with the following PowerShell command.

```
$disks = Get-Disk | where PartitionStyle -eq raw
foreach ($disk in $disks) {Initialize-Disk $disk.Number}
```

Number Friendly Name		Serial Number	HealthStatus	OperationalStatus	Total Size	Partition Style
0	AWS PVDISK	vo10541c31fc4c790ab	Healthy	Online	30 GB	MBR
1	NETAPP LUN C-Mode	TwB0p7RmR2s2	Healthy	Online	700 GB	GPT
2	NETAPP LUN C-Mode	TwB0p7RmR2s3	Healthy	Online	100 GB	GPT

22. Run the Create Partition and Format Disk commands with PowerShell.

```
New-Partition -DiskNumber 1 -DriveLetter F -UseMaximumSize
Format-Volume -DriveLetter F -FileSystem NTFS -AllocationUnitSize
65536
New-Partition -DiskNumber 2 -DriveLetter G -UseMaximumSize
Format-Volume -DriveLetter G -FileSystem NTFS -AllocationUnitSize
65536
```

You can automate volume and LUN creation using the PowerShell script from Appendix B. LUNs can also be created using SnapCenter.

Once the volumes and LUNs are defined, you need to set up SnapCenter to be able to perform the database operations.

SnapCenter overview

NetApp SnapCenter is next-generation data protection software for tier-1 enterprise applications. SnapCenter, with its single-pane-of-glass management interface, automates and simplifies the manual, complex, and time-consuming processes associated with the backup, recovery, and cloning of multiple databases and other application workloads. SnapCenter leverages NetApp technologies, including NetApp Snapshots, NetApp SnapMirror, SnapRestore, and NetApp FlexClone. This integration allows IT organizations to scale their storage infrastructure, meet increasingly stringent SLA commitments, and improve the productivity of administrators across the enterprise.

SnapCenter Server requirements

The following table lists the minimum requirements for installing the SnapCenter Server and plug-in on Microsoft Windows Server.

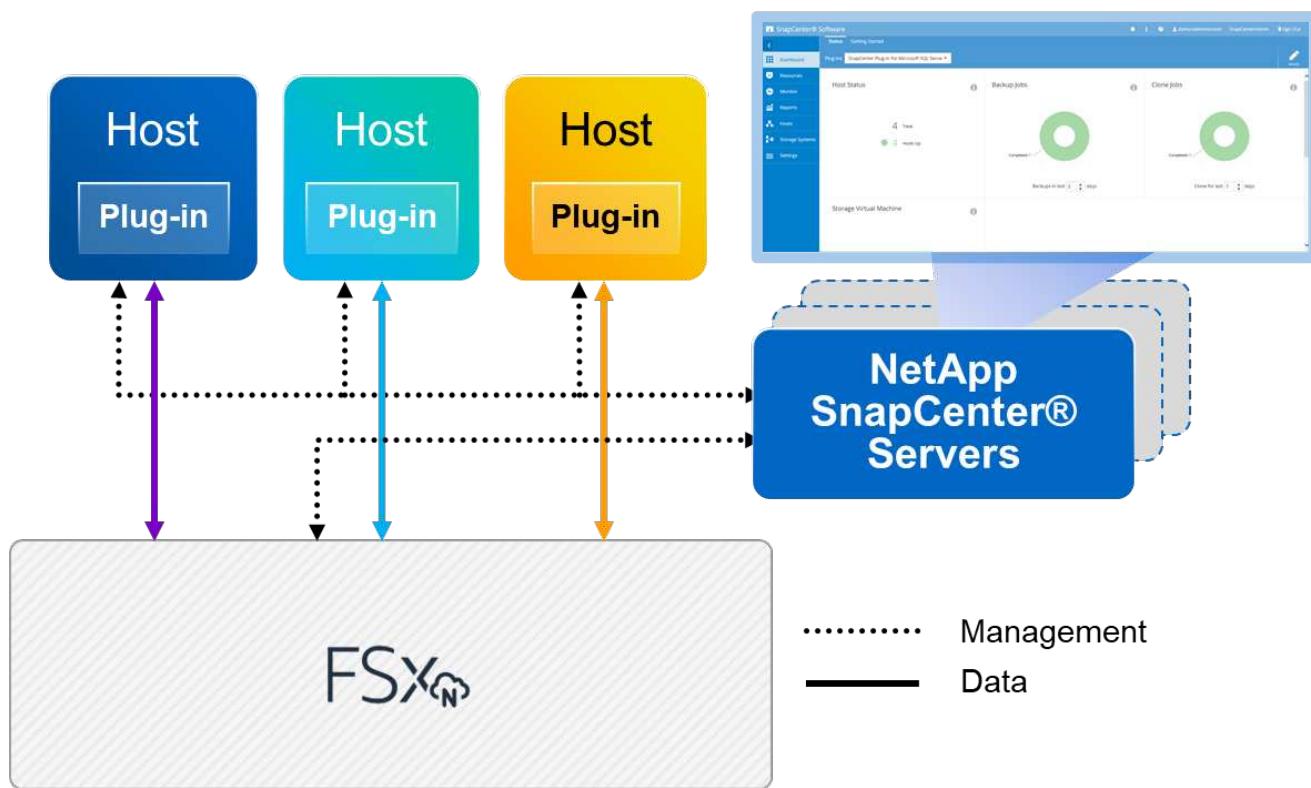
Components	Requirement
Minimum CPU count	Four cores/vCPUs
Memory	Minimum: 8GB Recommended: 32GB
Storage space	Minimum space for installation: 10GB Minimum space for repository: 10GB
Supported operating system	<ul style="list-style-type: none">Windows Server 2012Windows Server 2012 R2Windows Server 2016Windows Server 2019
Software packages	<ul style="list-style-type: none">.NET 4.5.2 or laterWindows Management Framework (WMF) 4.0 or laterPowerShell 4.0 or later

For detailed information, refer to Space and sizing requirements (https://docs.netapp.com/us-en/snapcenter/install/reference_space_and_sizing_requirements.html)

For version compatibility, see the [NetApp Interoperability Matrix Tool](#).

Database storage layout

The following figure depicts some considerations for creating the Microsoft SQL Server database storage layout when backing up with SnapCenter.



Best practices

- Place databases with I/O-intensive queries or with large database size (say 500GB or more) on a separate volume for faster recovery. This volume should also be backed up by separate jobs.
- Consolidate small-to-medium size databases that are less critical or have fewer I/O requirements to a single volume. Backing up a large number of databases residing in the same volume leads to fewer Snapshot copies that need to be maintained. It is also a best practice to consolidate Microsoft SQL Server instances to use the same volumes to control the number of backup Snapshot copies taken.
- Create separate LUNs to store full text-related files and file-streaming related files.
- Assign separate LUNs per host to store Microsoft SQL Server log backups.
- System databases that store database server metadata configuration and job details are not updated frequently. Place system databases/tempdb in separate drives or LUNs. Do not place system databases in the same volume as the user databases. User databases have a different backup policy, and the frequency of user database backup is not same for system databases.
- For Microsoft SQL Server Availability Group setup, place the data and log files for replicas in an identical folder structure on all nodes.

In addition to the performance benefit of segregating the user database layout into different volumes, the database also significantly affects the time required to back up and restore. Having separate volumes for data and log files significantly improves the restore time as compared to a volume hosting multiple user data files. Similarly, user databases with a high I/O intensive application are prone to an increase in the

backup time. A more detailed explanation about backup and restore practices is provided later in this document.



Starting with SQL Server 2012 (11.x), system databases (Master, Model, MSDB, and TempDB), and Database Engine user databases can be installed with an SMB file server as a storage option. This applies to both stand-alone SQL Server and SQL Server failover cluster installations. This enables you to use FSx for ONTAP with all its performance and data management capabilities, including volume capacity, performance scalability, and data protection features, which SQL Server can take advantage of. Shares used by the application servers must be configured with the continuously available property set and the volume should be created with NTFS security style. NetApp Snapcenter cannot be used with databases placed on SMB shares from FSx for ONTAP.



For SQL Server databases that do not use SnapCenter to perform backups, Microsoft recommends placing the data and log files on separate drives. For applications that simultaneously update and request data, the log file is write intensive, and the data file (depending on your application) is read/write intensive. For data retrieval, the log file is not needed. Therefore, requests for data can be satisfied from the data file placed on its own drive.



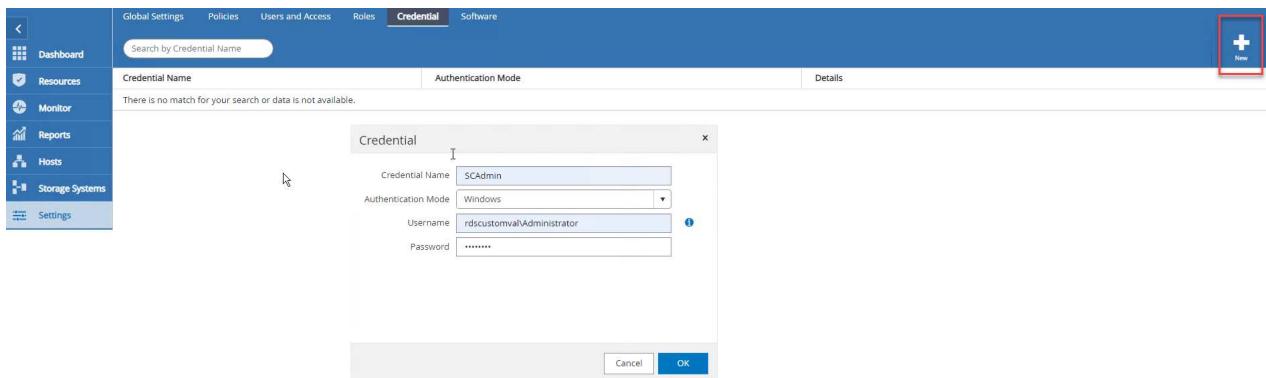
When you create a new database, Microsoft recommends specifying separate drives for the data and logs. To move files after the database is created, the database must be taken offline. For more Microsoft recommendations, see [Place Data and Log Files on Separate Drives](#).

Installation and setup for SnapCenter

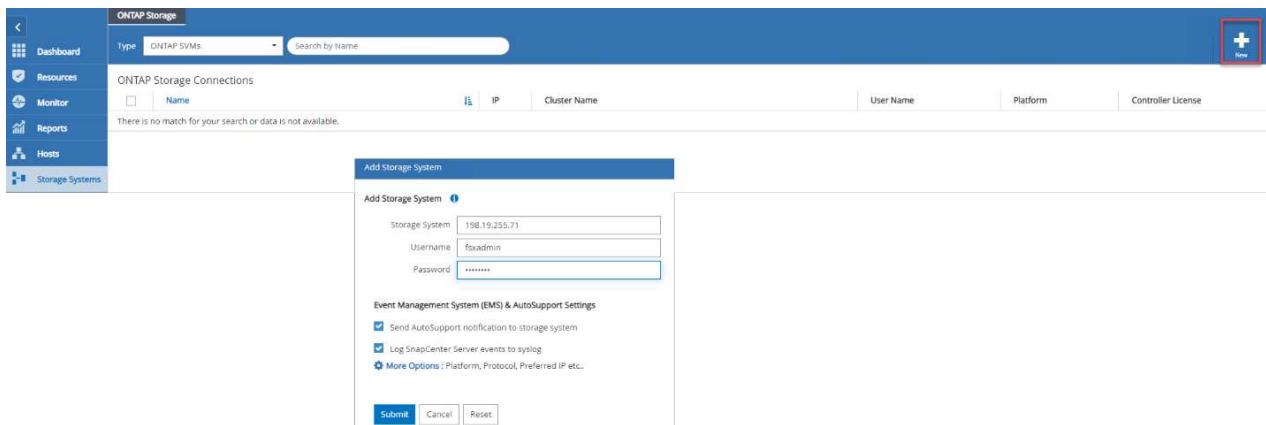
Follow the [Install the SnapCenter Server](#) and [Installing SnapCenter Plug-in for Microsoft SQL Server](#) to install and setup SnapCenter.

After Installing SnapCenter, complete the following steps to set it up.

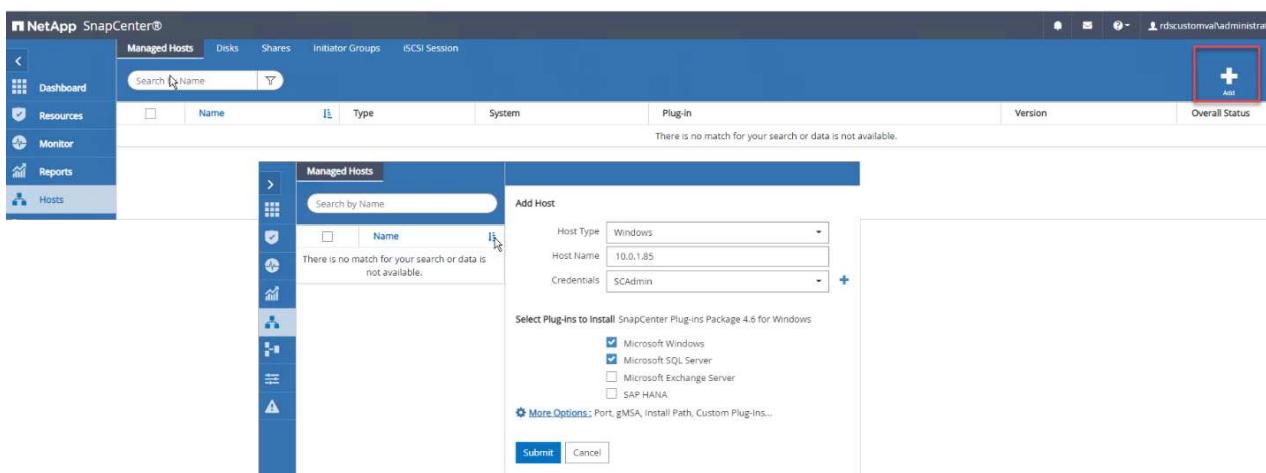
1. To set up credentials, select **Settings > New** and then enter the credential information.



2. Add the storage system by selecting **Storage Systems > New** and the provide the appropriate FSx for ONTAP storage information.



3. Add hosts by selecting **Hosts > Add**, and then provide the host information. SnapCenter automatically installs the Windows and SQL Server plug-in. This process might take some time.



After all Plug-ins are installed, you must configure the log directory. This is the location where the transaction log backup resides. You can configure the log directory by selecting the host and then select configure the log directory.



SnapCenter uses a host log directory to store transaction log backup data. This is at the host and instance level. Each SQL Server host used by SnapCenter must have a host log directory configured to perform log backups. SnapCenter has a database repository, so metadata related to backup, restore, or cloning operations is stored in a central database repository.

The size of the host log directory is calculated as follows:

$$\text{Size of host log directory} = \text{system database size} + (\text{maximum DB LDF size} \times \text{daily log change rate \%}) \times (\text{Snapshot copy retention}) \div (1 - \text{LUN overhead space \%})$$

The host log directory sizing formula assumes the following:

- A system database backup that does not include the tempdb database
- A 10% LUN overhead spacePlace the host log directory on a dedicated volume or LUN. The amount of data in the host log directory depends on the size of the backups and the number of days that backups are retained.

Managed Hosts

Search by Name

Name
<input checked="" type="checkbox"/> RDSAMAZ-FFIDFMR.rdscustomval.com

Host Details

Host Name: RDSAMAZ-FFIDFMR.rdscustomval.com

Host IP: 10.0.1.56

Overall Status: Configure log directory

Host Type: Windows

System: Stand-alone

Credentials: SCAdmin

Plug-ins: SnapCenter Plug-ins package 4.6.0.6965 for Windows

- ✓ Microsoft Windows
- ✓ Microsoft SQL Server [Remove](#) [Configure log directory](#) i

⚙️ [More Options](#): Port, gMSA, Install Path, Add Plug-Ins...

Submit Cancel Reset

If the LUNs have already been provisioned, you can select the mount point to represent the host log directory.

Configure Plug-in for SQL Server

X

Configure the log backup directory for RDSAMAZ-FFIDFMR.rdscustomval.com

Configure host log directory

Host log directory

dedicated disk directory path

Browse

Choose directory on NetApp Storage

 RDSAMAZ-FFIDFMR.rdscustomval.com

- D:\FSxN\Data\
- D:\FSxN\HLD\
- D:\FSxN\Log\

Save

Close

Now you are ready to perform backup, restore and clone operations for SQL Server.

Backup database with SnapCenter

After placing the database and log files on the FSx ONTAP LUNs, SnapCenter can be used to back up the databases. The following processes are used to create a full backup.

Best Practices

- In SnapCenter terms, RPO can be identified as the backup frequency, for example, how frequently you want to schedule the backup so that you can reduce the loss of data to up to few minutes. SnapCenter allows you to schedule backups as frequently as every five minutes. However, there might be a few instances in which a backup might not complete within five minutes during peak transaction times or when the rate of change of data is more in the given time. A best practice is to schedule frequent transaction log backups instead of full backups.
- There are numerous approaches to handle the RPO and RTO. One alternative to this backup approach is to have separate backup policies for data and logs with different intervals. For example, from SnapCenter, schedule log backups in 15-minute intervals and data backups in 6-hour intervals.
- Use a resource group for a backup configuration for Snapshot optimization and the number of jobs to be managed.

- Select **Resources**, and then select **Microsoft SQL Server** *on the drop-down menu on the top left. Select *Refresh Resources.

The screenshot shows the NetApp SnapCenter interface. On the left, a sidebar navigation bar includes links for Dashboard, Resources (which is selected), Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main content area has a title "Microsoft SQL Server" with dropdown menus for View, Database, and a search bar. Below this is a table listing databases:

Name	Instance	Host	Last Backup	Overall Status	Type
DWConfiguration	RDSAMAZ-FFIDFMR	RDSAMAZ-FFIDFMR.rdscustomval.com		Not available for backup	User database
DWDiagnostics	RDSAMAZ-FFIDFMR	RDSAMAZ-FFIDFMR.rdscustomval.com		Not available for backup	User database
DWQueue	RDSAMAZ-FFIDFMR	RDSAMAZ-FFIDFMR.rdscustomval.com		Not available for backup	User database
master	RDSAMAZ-FFIDFMR	RDSAMAZ-FFIDFMR.rdscustomval.com		Not available for backup	System database
model	RDSAMAZ-FFIDFMR	RDSAMAZ-FFIDFMR.rdscustomval.com		Not available for backup	System database
msdb	RDSAMAZ-FFIDFMR	RDSAMAZ-FFIDFMR.rdscustomval.com		Not available for backup	System database
SeattleRetail	RDSAMAZ-FFIDFMR	RDSAMAZ-FFIDFMR.rdscustomval.com		Not protected	User database
tempdb	RDSAMAZ-FFIDFMR	RDSAMAZ-FFIDFMR.rdscustomval.com		Not available for backup	System database

- Select the database to be backed up, then select **Next** and (+) to add the policy if one has not been created. Follow the **New SQL Server Backup Policy** to create a new policy.

The screenshot shows the "New SQL Server Backup Policy" wizard. The steps are numbered 1 through 5: Resource, Policies, Verification, Notification, and Summary. Step 1 is "Resource" and step 2 is "Policies".

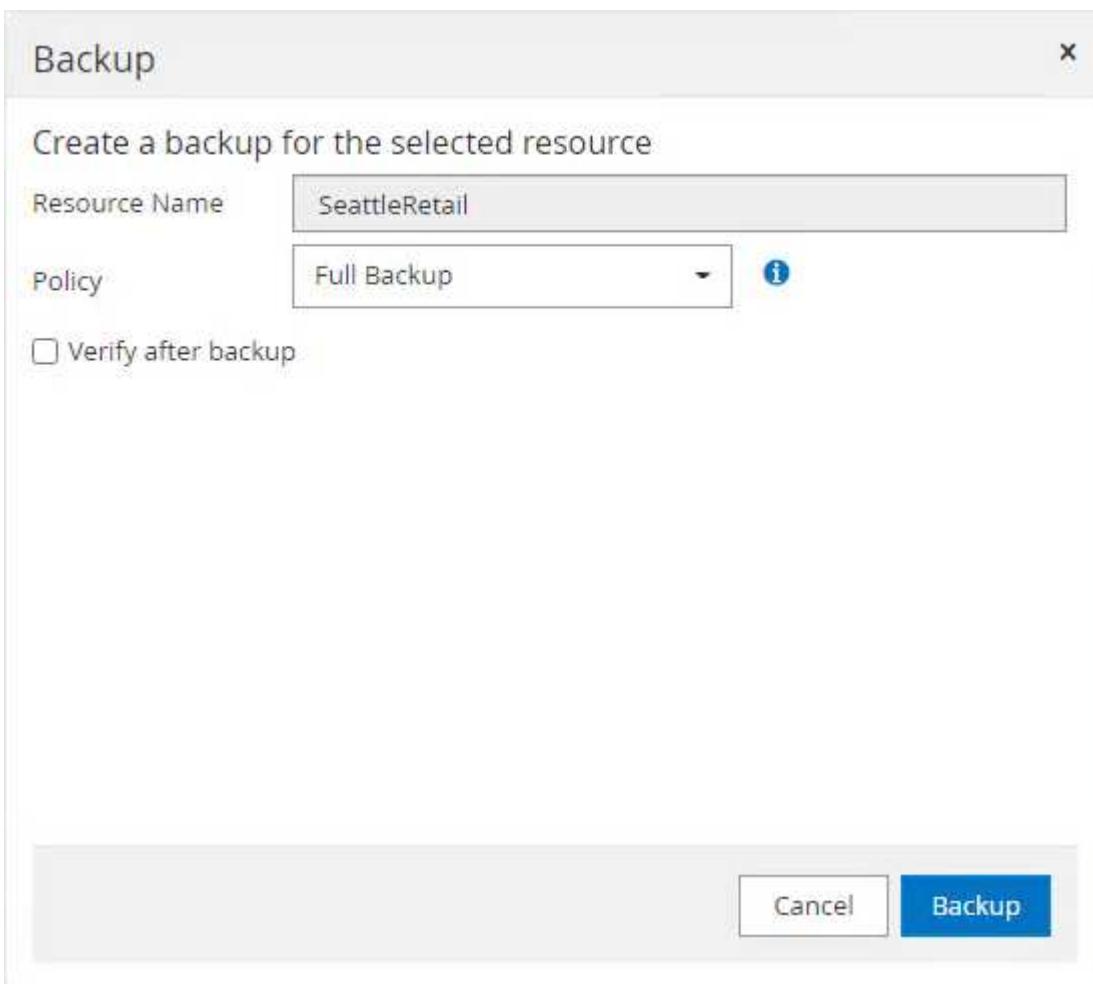
Under "Policies", a table lists existing policies: Full Backup, Differential Backup, Transaction Log Backup, and File and Filegroup Backup. The "Full Backup" policy is selected. Below the table, it says "Select one or more policies and configure schedules". A dropdown menu shows "Full Backup" and a "+" button to add more policies.

Under "Verification", it says "Configure schedules for selected policies". A table shows the "Full Backup" policy with "None" applied and a note: "To schedule operations select a policy that has the appropriate schedule associated, or modify the selected policy to allow schedules."

- Select the verification server if necessary. This server is the server that SnapCenter runs DBCC CHECKDB after a full backup has been created. Click **Next** for notification, and then select **Summary** to review. After reviewing, click **Finish**.

The screenshot shows the 'Verification' step of a five-step process. The steps are: Resource, Policies, Verification, Notification, and Summary. The 'Verification' step is highlighted with a blue circle containing the number 3. On the left, a list of resources is shown, with 'SeattleRetail' selected. In the center, there is a section titled 'Select the verification servers' with a dropdown menu labeled 'Select one or more servers'. Below it, there is a section titled 'Configure verification schedules' with tabs for 'Policy', 'Schedule Type', 'Applied Schedules', and 'Configure Schedules'. A message at the bottom states 'There is no match for your search or data is not available.'

4. Click **Back up Now** to test the backup. In the pop-up windows, select **Backup**.



5. Select **Monitor** to verify that the backup has been completed.

The screenshot shows the 'Monitor' tab of the NetApp SnapCenter interface. It displays a table of jobs with the following data:

ID	Status	Name	Start date	End date	Owner
94	✓	Backup of Resource Group 'RDSAMAZ-FRIDFMR_SeattleRetail' with policy 'Full Backup'	03/29/2022 1:47:30 AM	03/29/2022 1:47:41 AM	RDSCUSTOMVAL\administrator
93	✓	Create Resource Group 'RDSAMAZ-FRIDFMR_SeattleRetail'	03/29/2022 1:45:24 AM	03/29/2022 1:45:26 AM	RDSCUSTOMVAL\administrator
92	✓	Create Policy 'Full Backup'	03/29/2022 1:41:37 AM	03/29/2022 1:41:40 AM	RDSCUSTOMVAL\administrator
91	✓	Discover resources for all hosts	03/29/2022 1:38:12 AM	03/29/2022 1:38:17 AM	RDSCUSTOMVAL\administrator

Best Practices

- Backup the transaction log backup from SnapCenter so that during the restoration process, SnapCenter can read all the backup files and restore in sequence automatically.
- If third party products are used for backup, select Copy backup in SnapCenter to avoid log sequence issues, and test the restore functionality before rolling into production.

Restore database with SnapCenter

One of the major benefits of using FSx ONTAP with SQL Server on EC2 is its ability to perform fast and granular restore at each database level.

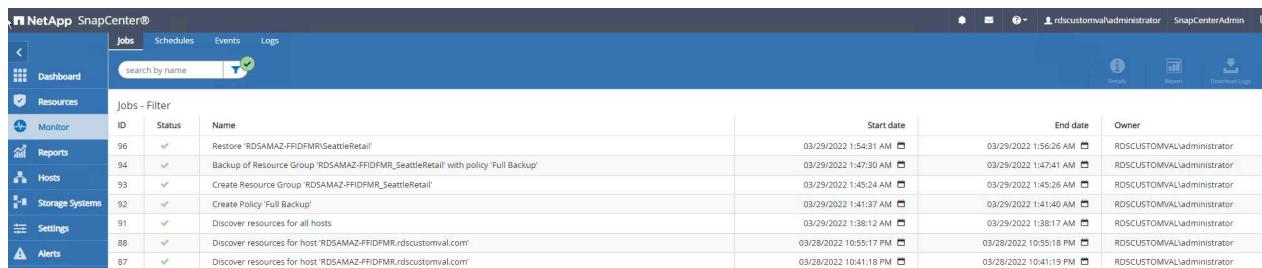
Complete the following steps to restore an individual database to a specific point in time or up to the minute with SnapCenter.

1. Select Resources and then select the database that you would like to restore.



The screenshot shows the Microsoft SQL Server Management Studio interface. On the left, a tree view lists databases: Name (DWConfiguration, DW.Diagnostics, DWQueue, master, model, msdb, SeattleRetail, tempdb). The 'SeattleRetail' database is selected. In the center, under 'Manage Copies', there is a summary card: 'Summary Card' (1 Backup, 0 Clones). Below it, 'Primary Backup(s)' are listed: 'RDSAMAZ-FFIDFMR_SeattleRetail_RDSAMAZ-FFIDFMR_03-29-2022_01.47.31.3117' (Count: 1, Type: Full backup, End Date: 03/29/2022 1:47:37 AM, Verified: Unverified).

2. Select the backup name that the database needs to be restored from and then select restore.
3. Follow the **Restore** pop-up windows to restore the database.
4. Select **Monitor** to verify that the restore process is successful.



The screenshot shows the NetApp SnapCenter interface. On the left, a sidebar lists categories: Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The 'Jobs' tab is selected. A table titled 'Jobs - Filter' lists the following tasks:

ID	Status	Name	Start date	End date	Owner
96	✓	Restore 'RDSAMAZ-FFIDFMR.SeattleRetail'	03/29/2022 1:54:31 AM	03/29/2022 1:56:26 AM	RDSCUSTOMVAL\administrator
94	✓	Backup of Resource Group 'RDSAMAZ-FFIDFMR_SeattleRetail' with policy 'Full Backup'	03/29/2022 1:47:30 AM	03/29/2022 1:47:41 AM	RDSCUSTOMVAL\administrator
93	✓	Create Resource Group 'RDSAMAZ-FFIDFMR_SeattleRetail'	03/29/2022 1:45:24 AM	03/29/2022 1:45:26 AM	RDSCUSTOMVAL\administrator
92	✓	Create Policy 'Full Backup'	03/29/2022 1:41:37 AM	03/29/2022 1:41:40 AM	RDSCUSTOMVAL\administrator
91	✓	Discover resources for all hosts	03/29/2022 1:38:12 AM	03/29/2022 1:38:17 AM	RDSCUSTOMVAL\administrator
88	✓	Discover resources for host 'RDSAMAZ-FFIDFMR.rdscustomval.com'	03/28/2022 10:55:17 PM	03/28/2022 10:55:18 PM	RDSCUSTOMVAL\administrator
87	✓	Discover resources for host 'RDSAMAZ-FFIDFMR.rdscustomval.com'	03/28/2022 10:41:18 PM	03/28/2022 10:41:19 PM	RDSCUSTOMVAL\administrator

Considerations for an instance with a large number of small-to-large size databases

SnapCenter can back up a large number of sizeable databases in an instance or group of instances within a resource group. The size of a database is not the major factor in backup time. The duration of a backup can vary depending on number of LUNs per volume, the load on Microsoft SQL Server, the total number of databases per instance, and, specifically, the I/O bandwidth and usage. While configuring the policy to back up databases from an instance or resource group, NetApp recommends that you restrict the maximum database backed up per Snapshot copy to 100 per host. Make sure the total number of Snapshot copies does not exceed the 1,023-copy limit.

NetApp also recommends that you limit the backup jobs running in parallel by grouping the number of databases instead of creating multiple jobs for each database or instance. For optimal performance of the backup duration, reduce the number of backup jobs to a number that can back up around 100 or fewer databases at a time.

As previously mentioned, I/O usage is an important factor in the backup process. The backup process must wait to quiesce until all the I/O operations on a database are complete. Databases with highly intensive I/O operations should be deferred to another backup time or should be isolated from other backup jobs to avoid affecting other resources within the same resource group that are to be backed up.

For an environment that has six Microsoft SQL Server hosts hosting 200 databases per instance, assuming four LUNs per host and one LUN per volume created, set the full backup policy with the maximum databases backed up per Snapshot copy to 100. Two hundred databases on each instance are laid out as 200 data files distributed equally on two LUNs, and 200 log files are distributed equally on two LUNs, which is 100 files per LUN per volume.

Schedule three backup jobs by creating three resource groups, each grouping two instances that include a total of 400 databases.

Running all three backup jobs in parallel backs up 1,200 databases simultaneously. Depending on the load on the server and I/O usage, the start and end time on each instance can vary. In this instance, a total of 24 Snapshot copies are created.

In addition to the full backup, NetApp recommends that you configure a transaction log backup for critical databases. Make sure that the database property is set to full recovery model.

Best practices

- Do not include the tempdb database in a backup because the data it contains is temporary. Place tempdb on a LUN or an SMB share that is in a storage system volume in which Snapshot copies will not be created.
- A Microsoft SQL Server instance with a high I/O intensive application should be isolated in a different backup job to reduce the overall backup time for other resources.
- Limit the set of databases to be simultaneously backed up to approximately 100 and stagger the remaining set of database backups to avoid a simultaneous process.
- Use the Microsoft SQL Server instance name in the resource group instead of multiple databases because whenever new databases are created in Microsoft SQL Server instance, SnapCenter automatically considers a new database for backup.
- If you change the database configuration, such as changing the database recovery model to the full recovery model, perform a backup immediately to allow up-to-the-minute restore operations.
- SnapCenter cannot restore transaction log backups created outside of SnapCenter.
- When cloning FlexVol volumes, make sure that you have sufficient space for the clone metadata.
- When restoring databases, make sure that sufficient space is available on the volume.
- Create a separate policy to manage and back up system databases at least once a week.

Cloning databases with SnapCenter

To restore a database onto another location on a dev or test environment or to create a copy for business analysis purposes, the NetApp best practice is to leverage the cloning methodology to create a copy of the database on the same instance or an alternate instance.

The cloning of databases that are 500GB on an iSCSI disk hosted on a FSx for ONTAP environment typically takes less than five minutes. After cloning is complete, the user can then perform all the required read/write operation on the cloned database. Most of the time is consumed for disk scanning (diskpart). The NetApp cloning procedure typically take less than 2 minutes regardless of the size of the databases.

The cloning of a database can be performed with the dual method: you can create a clone from the latest backup or you can use clone life-cycle management through which the latest copy can be made available on the secondary instance.

SnapCenter allows you to mount the clone copy on the required disk to maintain the format of the folder structure on the secondary instance and continue to schedule backup jobs.

Clone databases to the new database name in the same instance

The following steps can be used to clone databases to the new database name in the same SQL server instance running on EC2:

1. Select Resources and then the database that need to be cloned.
2. Select the backup name that you would like to clone and select Clone.
3. Follow the clone instructions from the backup windows to finish the clone process.
4. Select Monitor to make sure that cloning is completed.

Clone databases into the new SQL Server instance running on EC2

The following step are used to clone databases to the new SQL server instance running on EC2:

1. Create a new SQL Server on EC2 in the same VPC.
2. Enable the iSCSI protocol and MPIO, and then setup the iSCSI connection to FSx for ONTAP by following step 3 and 4 in the section “Create volumes and LUNs for SQL Server.”
3. Add a new SQL Server on EC2 into SnapCenter by follow step 3 in the section “Installing and setup for SnapCenter.”
4. Select Resource > View Instance, and then select Refresh Resource.
5. Select Resources, and then the database that you would like to clone.
6. Select the backup name that you would like to clone, and then select Clone.

The screenshot shows the NetApp SnapCenter interface. On the left, a sidebar lists databases: Name, DWConfiguration, DWdiagnostics, DWqueue, master, model, msdb, SeattleRetail, and tempdb. SeattleRetail is selected. In the main pane, under "Manage Copies", there is a "Backup" section with 1 Backup and 0 Clones. Below it is a "Primary Backup(s)" section with a search bar and a table. The table has columns: Backup Name, Count, Type, LF, End Date, and Verified. One entry is shown: RDSAMAZ-FFDFMR_SeattleRetail_RDSAMAZ-FFDFMR_03-29-2022_01.47.31.3117, with Count 1, Type Full backup, End Date 03/29/2022 1:47:37 AM, and Verified Unverified. A summary card on the right shows 1 Backup and 0 Clones.

7. Follow the Clone from Backup instructions by providing the new SQL Server instance on EC2 and instance name to finish the clone process.
8. Select Monitor to make sure that cloning is completed.

The screenshot shows the NetApp SnapCenter interface with the "Jobs" tab selected. The left sidebar shows Resources, Monitor, and Reports. The main pane displays a table of jobs. The table has columns: ID, Status, Name, Start date, End date, and Owner. Two entries are listed: Job ID 108, Status Green, Name "Clone from backup RDSAMAZ-FFDFMR_SeattleRetail_RDSAMAZ-FFDFMR_03-29-2022_01.47.31.3117", Start date 03/30/2022 6:09:10 PM, End date 03/30/2022 6:09:55 PM, Owner rdscustomval\administrator. Job ID 107, Status Green, Name "Discover resources for all hosts", Start date 03/30/2022 6:06:40 PM, End date 03/30/2022 6:06:54 PM, Owner RDSCUSTOMVAL\administrator.

Appendices

Appendix A: YAML file for use in Cloud Formation Template

The following .yaml file can be used with the Cloud Formation Template in AWS Console.

- <https://github.com/NetApp-Automation/fsxn-iscsisetup-cft>

To automate ISCSI LUN creation and NetApp SnapCenter installation with PowerShell, clone the repo from [this GitHub link](#).

Appendix B: Powershell scripts for provisioning volumes and LUNs

The following script is used to provision volumes and LUNs and also to set up iSCSI based on the instruction provided above. There are two PowerShell scripts:

- `_EnableMPIO.ps1`

```
Function Install_MPIO_ssh {
    $hostname = $env:COMPUTERNAME
    $hostname = $hostname.Replace('-', '_')

    #Add schedule action for the next step
    $path = Get-Location
    $path = $path.Path + '\2_CreateDisks.ps1'
    $arg = '-NoProfile -WindowStyle Hidden -File ' +$path
    $schAction = New-ScheduledTaskAction -Execute "Powershell.exe"
    -Argument $arg
    $schTrigger = New-ScheduledTaskTrigger -AtStartup
    $schPrincipal = New-ScheduledTaskPrincipal -UserId "NT
AUTHORITY\SYSTEM" -LogonType ServiceAccount -RunLevel Highest
    $return = Register-ScheduledTask -Action $schAction -Trigger
    $schTrigger -TaskName "Create Vols and LUNs" -Description "Scheduled
Task to run configuration Script At Startup" -Principal $schPrincipal
    #Install -Module Posh-SSH
    Write-host 'Enable MPIO and SSH for PowerShell' -ForegroundColor
Yellow
    $return = Find-PackageProvider -Name 'Nuget' -ForceBootstrap
    -IncludeDependencies
    $return = Find-Module PoSH-SSH | Install-Module -Force
    #Install Multipath-IO with PowerShell using elevated privileges in
Windows Servers
    Write-host 'Enable MPIO' -ForegroundColor Yellow
    $return = Install-WindowsFeature -name Multipath-IO -Restart
}
Install_MPIO_ssh
Remove-Item -Path $MyInvocation.MyCommand.Source
```

- `_CreateDisks.ps1`

```
#Enable MPIO and Start iSCSI Service
Function PrepISCSI {
    $return = Enable-MSDSMAutomaticClaim -BusType iSCSI
    #Start iSCSI service with PowerShell using elevated privileges in
Windows Servers
    $return = Start-service -Name msiscsi
```

```

$return = Set-Service -Name msiscsi -StartupType Automatic
}

Function Create_igroup_vols_luns ($fsxN) {
    $hostname = $env:COMPUTERNAME
    $hostname = $hostname.Replace('-', '_')
    $volsluns = @()
    for ($i = 1;$i -lt 10;$i++) {
        if ($i -eq 9){
            $volsluns
        +=(@{volname=('v_'+$hostname+'_log');volsize=$fsxN.logvolsize;lunname=(

'1_'+$hostname+'_log');lunsize=$fsxN.loglunsize})
        } else {
            $volsluns
        +=(@{volname=('v_'+$hostname+'_data'+[string]$i);volsize=$fsxN.datavols

ize;lunname=('1_'+$hostname+'_data'+[string]$i);lunsize=$fsxN.datalunsi

ze})
        }
    }
    $secStringPassword = ConvertTo-SecureString $fsxN.password
    -AsPlainText -Force
    $credObject = New-Object System.Management.Automation.PSCredential
    ($fsxN.login, $secStringPassword)
    $igroup = 'igrp_'+$hostname
    #Connect to FSx N filesystem
    $session = New-SSHSession -ComputerName $fsxN.svmip -Credential
    $credObject -AcceptKey:$true
    #Create igroup
    Write-host 'Creating igroup' -ForegroundColor Yellow
    #Find Windows initiator Name with PowerShell using elevated
    privileges in Windows Servers
    $initport = Get-InitiatorPort | select -ExpandProperty NodeAddress
    $sshcCmd = 'igroup create -igroup ' + $igroup + ' -protocol iscsi
    -ostype windows -initiator ' + $initport
    $ret = Invoke-SSHCommand -Command $sshcCmd -SSHSession $session
    #Create vols
    Write-host 'Creating Volumes' -ForegroundColor Yellow
    foreach ($vollun in $volsluns){
        $sshcCmd = 'vol create ' + $vollun.volname + ' -aggregate aggr1
        -size ' + $vollun.volsize #' -vserver ' + $vserver
        $return = Invoke-SSHCommand -Command $sshcCmd -SSHSession
    $session
    }
    #Create LUNs and mapped LUN to igroup
    Write-host 'Creating LUNs and map to igroup' -ForegroundColor
    Yellow
    foreach ($vollun in $volsluns){

```

```

        $sshcmd = "lun create -path /vol/" + $vollun.volname + "/" +
$vollun.lunname + " -size " + $vollun.lunsize + " -ostype Windows_2008
" #-vserver " +$vserver
        $return = Invoke-SSHCommand -Command $sshcmd -SSHSession
$session
        #map all luns to igroup
        $sshcmd = "lun map -path /vol/" + $vollun.volname + "/" +
$vollun.lunname + " -igroup " + $igroup
        $return = Invoke-SSHCommand -Command $sshcmd -SSHSession
$session
    }
}

Function Connect_iSCSI_to_SVM ($TargetPortals){
    Write-host 'Online, Initialize and format disks' -ForegroundColor Yellow
    #Connect Windows Server to svm with iSCSI target.
    foreach ($TargetPortal in $TargetPortals) {
        New-IscsiTargetPortal -TargetPortalAddress $TargetPortal
        for ($i = 1; $i -lt 5; $i++){
            $return = Connect-IscsiTarget -IsMultipathEnabled $true
-IsPersistent $true -NodeAddress (Get-iscsiTarget | select
-ExpandProperty NodeAddress)
        }
    }
}

Function Create_Partition_Format_Disks{

    #Create Partition and format disk
    $disks = Get-Disk | where PartitionStyle -eq raw
    foreach ($disk in $disks) {
        $return = Initialize-Disk $disk.Number
        $partition = New-Partition -DiskNumber $disk.Number
-AssignDriveLetter -UseMaximumSize | Format-Volume -FileSystem NTFS
-AllocationUnitSize 65536 -Confirm:$false -Force
        #$return = Format-Volume -DriveLetter $partition.DriveLetter
-FileSystem NTFS -AllocationUnitSize 65536
    }
}

Function UnregisterTask {
    Unregister-ScheduledTask -TaskName "Create Vols and LUNS"
-Confirm:$false
}

Start-Sleep -s 30
$fsxN = @{svmip ='198.19.255.153';login =
'vesadmin';password='net@pp11';datavolsize='10GB';datalunsize='8GB';logv
olsize='8GB';loglunsize='6GB'}

```

```

$TargetPortals = ('10.2.1.167', '10.2.2.12')
PrepISCSI
Create_igroup_vols_luns $fsxN
Connect_iSCSI_to_SVM $TargetPortals
Create_Partition_Format_Disks
UnregisterTask
Remove-Item -Path $MyInvocation.MyCommand.Source

```

Run the file EnableMPIO.ps1 first and the second script executes automatically after the server has been rebooted. These PowerShell scripts can be removed after they have been executed due to credential access to the SVM.

Where to find additional information

- Amazon FSx for NetApp ONTAP

<https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/what-is-fsx-ontap.html>

- Getting Started with FSx for NetApp ONTAP

<https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/getting-started.html>

- Overview of the SnapCenter interface

<https://www.youtube.com/watch?v=lVEBF4kV6Ag&t=0s>

- Tour through SnapCenter navigation pane options

https://www.youtube.com/watch?v=_IDKt-koySQ

- Setup SnapCenter 4.0 for SQL Server plug-in

<https://www.youtube.com/watch?v=MopbUFSdHKE>

- How to back up and restore databases using SnapCenter with SQL Server plug-in

https://www.youtube.com/watch?v=K343qPD5_Ys

- How to clone a database using SnapCenter with SQL Server plug-in

<https://www.youtube.com/watch?v=ogEc4DkGv1E>

TR-4467: SAP with Microsoft SQL Server on Windows - Best practices using NetApp Clustered Data ONTAP and SnapCenter

Marco Schoen, NetApp

TR-4467 provides customers and partners with best practices for deploying clustered NetApp Data ONTAP in support of SAP Business Suite solutions running in a Microsoft SQL Server on Windows environment.

[TR-4467: SAP with Microsoft SQL Server on Windows - Best practices using NetApp Clustered Data ONTAP and SnapCenter](#)

Modernizing your Microsoft SQL Server environment

Optimize operations and unleash the power of your data - on the premises or in the cloud.

[Modernizing your Microsoft SQL Server environment](#)

TR-4764: Best practices for Microsoft SQL Server with NetApp EF-Series

Mitch Blackburn, Pat Sinthusan, NetApp

This best practices guide is intended to help storage administrators and database administrators successfully deploy Microsoft SQL Server on NetApp EF-Series storage.

[TR-4764: Best practices for Microsoft SQL Server with NetApp EF-Series](#)

Open Source Databases

TR-4956: Automated PostgreSQL High Availability Deployment and Disaster Recovery in AWS FSx/EC2

Allen Cao, Niyaz Mohamed, NetApp

Purpose

PostgreSQL is a widely used open-source database that is ranked number four among the top ten most popular database engines by [DB-Engines](#). On one hand, PostgreSQL derives its popularity from its license-free, open-source model while still possessing sophisticated features. On the other hand, because it is open sourced, there is shortage of detailed guidance on production-grade database deployment in the area of high availability and disaster recovery (HA/DR), particularly in the public cloud. In general, it can be difficult to set up a typical PostgreSQL HA/DR system with hot and warm standby, streaming replication, and so on. Testing the HA/DR environment by promoting the standby site and then switching back to the primary can be disruptive to production. There are well documented performance issues on the primary when read workloads are deployed on streaming hot standby.

In this documentation, we demonstrate how you can do away with an application-level PostgreSQL streaming HA/DR solution and build a PostgreSQL HA/DR solution based on AWS FSx ONTAP storage for database files and EC2 compute instances, such as PostgreSQL DB servers. The solution creates a simpler and comparable system and delivers equivalent results when compared with traditional PostgreSQL application-level streaming replication for HA/DR.

This solution is built on proven and mature NetApp SnapMirror storage-level replication technology that is available in AWS-native FSX ONTAP cloud storage for PostgreSQL HA/DR. It is simple to implement with an automation toolkit provided by the NetApp Solutions team. It provides similar functionality while eliminating the complexity and performance drag on the primary site with the application-level streaming-based HA/DR solution. The solution can be easily deployed and tested without affecting the active primary site.

This solution addresses the following use cases:

- Production grade HA/DR deployment for PostgreSQL in the public AWS cloud
- Testing and validating a PostgreSQL workload in the public AWS cloud
- Testing and validating a PostgreSQL HA/DR strategy based on NetApp SnapMirror replication technology

Audience

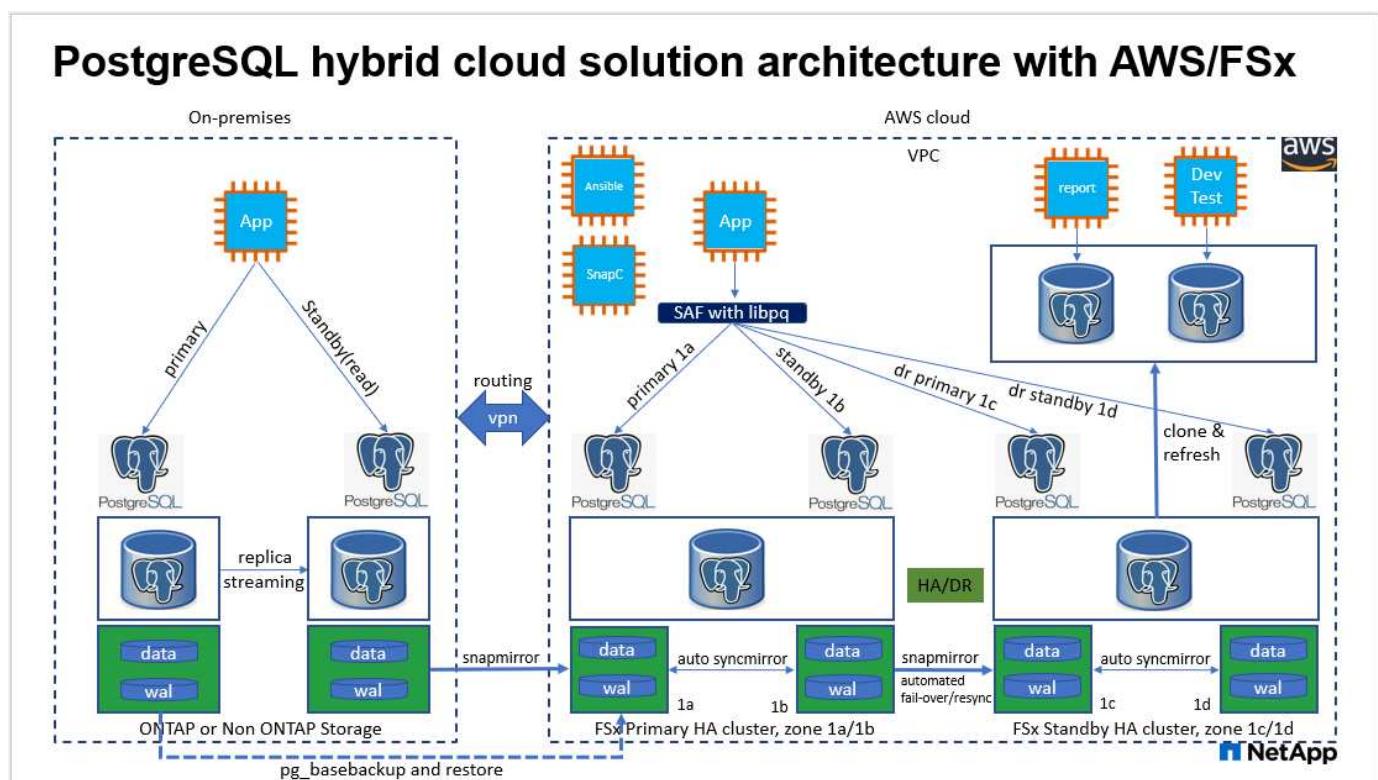
This solution is intended for the following people:

- The DBA who is interested in deploying PostgreSQL with HA/DR in the public AWS cloud.
- The database solution architect who is interested in testing PostgreSQL workloads in the public AWS cloud.
- The storage administrator who is interested in deploying and managing PostgreSQL instances deployed to AWS FSx storage.
- The application owner who is interested in standing up a PostgreSQL environment in AWS FSx/EC2.

Solution test and validation environment

The testing and validation of this solution was performed in an AWS FSx and EC2 environment that might not match the final deployment environment. For more information, see the section [\[Key Factors for Deployment Consideration\]](#).

Architecture



Hardware and software components

Hardware		
FSx ONTAP storage	Current version	Two FSx HA pairs in the same VPC and availability zone as primary and standby HA clusters
EC2 instance for compute	t2.xlarge/4vCPU/16G	Two EC2 T2 xlarge as primary and standby compute instances
Ansible controller	on-prem Centos VM/4vCPU/8G	A VM to host Ansible automation controller either on-premise or in the cloud

Software		
RedHat Linux	RHEL-8.6.0_HVM-20220503-x86_64-2-Hourly2-GP2	Deployed RedHat subscription for testing
Centos Linux	CentOS Linux release 8.2.2004 (Core)	Hosting Ansible controller deployed in on-premises lab
PostgreSQL	Version 14.5	Automation pulls the latest available version of PostgreSQL from the postgresql.ora yum repo
Ansible	Version 2.10.3	Prerequisites for required collections and libraries installed with requirements playbook

Key factors for deployment consideration

- **PostgreSQL database backup, restore, and recovery.** A PostgreSQL database supports a number of backup methods, such as a logical backup using pg_dump, a physical online backup with pg_basebackup or a lower-level OS backup command, and storage-level-consistent snapshots. This solution uses NetApp consistency-group snapshots for PostgreSQL database data and WAL volumes backup, restore, and recovery at the standby site. The NetApp consistency-group volume snapshots sequence I/O as it is written to storage and protect the integrity of database data files.
- **EC2 compute instances.** In these tests and validations, we used the AWS EC2 t2.xlarge instance type for the PostgreSQL database compute instance. NetApp recommends using an M5 type EC2 instance as the compute instance for PostgreSQL in deployment because it is optimized for database workloads. The standby compute instance should always be deployed in the same zone as the passive (standby) file system deployed for the FSx HA cluster.
- **FSx storage HA clusters single- or multi-zone deployment.** In these tests and validations, we deployed an FSx HA cluster in a single AWS availability zone. For production deployment, NetApp recommends deploying an FSx HA pair in two different availability zones. A disaster-recovery standby HA pair for business continuity can be set up in a different region if a specific distance is required between the primary and standby. An FSx HA cluster is always provisioned in a HA pair that is sync mirrored in a pair of active-passive file systems to provide storage-level redundancy.
- **PostgreSQL data and log placement.** Typical PostgreSQL deployments share the same root directory or volumes for data and log files. In our tests and validations, we have separated PostgreSQL data and logs into two separate volumes for performance. A soft link is used in the data directory to point to the log directory or volume that hosts PostgreSQL WAL logs and archived WAL logs.
- **PostgreSQL service startup delay timer.** This solution uses NFS mounted volumes to store the PostgreSQL database file and WAL log files. During a database host reboot, PostgreSQL service might try to start while the volume is not mounted. This results in database service startup failure. A 10 to 15 seconds timer delay is needed for the PostgreSQL database to start up correctly.
- **RPO/RTO for business continuity.** FSx data replication from primary to standby for DR is based on ASYNC, which means that the RPO depends on the frequency of Snapshot backups and SnapMirror replication. A higher frequency of Snapshot copy and SnapMirror replication reduces the RPO. Therefore, there is a balance between potential data loss in the event of a disaster and incremental storage cost. We have determined that Snapshot copy and SnapMirror replication can be implemented in as low as 5 minute intervals for RPO, and PostgreSQL can generally be recovered at the DR standby site in under a minute for the RTO.
- **Database backup.** After a PostgreSQL database is implemented or migrated into AWS FSx storage from an on-premises data center, the data is auto-sync mirrored in the FSx HA pair for protection. Data is further protected with a replicated standby site in case of a disaster. For longer-term backup retention or data protection, NetApp recommends using the built-in PostgreSQL pg_basebackup utility to run a full database backup that can be ported to S3 blob storage.

Solution Deployment

The deployment of this solution can be completed automatically using the NetApp Ansible-based automation toolkit by following the detailed instructions outlined below.

1. Read the instructions in the automation toolkit README.md [na_postgresql_aws_deploy_hadr](#).
2. Watch the following video walk through.
▶ https://docs.netapp.com/us-en/netapp-solutions/media/aws_postgres_fsx_ec2_deploy_hadr.mp4 (video)
3. Configure the required parameters files (hosts, host_vars/host_name.yml, fsx_vars.yml) by entering user-specific parameters into the template in the relevant sections. Then use the copy button to copy files to the Ansible controller host.

Prerequisites for automated deployment

Deployment requires the following prerequisites.

1. An AWS account has been set up, and the necessary VPC and network segments have been created within your AWS account.
2. From the AWS EC2 console, you must deploy two EC2 Linux instances, one as the primary PostgreSQL DB server at the primary and one at the standby DR site. For compute redundancy at the primary and standby DR sites, deploy two additional EC2 Linux instances as standby PostgreSQL DB servers. See the architecture diagram in the previous section for more details about the environment setup. Also review the [User Guide for Linux instances](#) for more information.
3. From the AWS EC2 console, deploy two FSx ONTAP storage HA clusters to host the PostgreSQL database volumes. If you are not familiar with the deployment of FSx storage, see the documentation [Creating FSx for ONTAP file systems](#) for step-by-step instructions.
4. Build a Centos Linux VM to host the Ansible controller. The Ansible controller can be located either on-premises or in the AWS cloud. If it is located on-premises, you must have SSH connectivity to the VPC, EC2 Linux instances, and FSx storage clusters.
5. Set up the Ansible controller as described in the section "Set up the Ansible Control Node for CLI deployments on RHEL/CentOS" from the resource [Getting Started with NetApp solution automation](#).
6. Clone a copy of the automation toolkit from the public NetApp GitHub site.

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

7. From the toolkit root directory, execute the prerequisite playbooks to install the required collections and libraries for the Ansible controller.

```
ansible-playbook -i hosts requirements.yml
```

```
ansible-galaxy collection install -r collections/requirements.yml  
--force --force-with-deps
```

8. Retrieve the required EC2 FSx instance parameters for the DB host variables file `host_vars/*` and the global variables file `fsx_vars.yml` configuration.

Configure the hosts file

Input the primary FSx ONTAP cluster management IP and EC2 instances hosts names into the hosts file.

```
# Primary FSx cluster management IP address
[fsx_ontap]
172.30.15.33
```

```
# Primary PostgreSQL DB server at primary site where database is
initialized at deployment time
[postgresql]
psql_01p ansible_ssh_private_key_file=psql_01p.pem
```

```
# Primary PostgreSQL DB server at standby site where postgresql service is
installed but disabled at deployment
# Standby DB server at primary site, to setup this server comment out
other servers in [dr_postgresql]
# Standby DB server at standby site, to setup this server comment out
other servers in [dr_postgresql]
[dr_postgresql] --
psql_01s ansible_ssh_private_key_file=psql_01s.pem
#psql_01ps ansible_ssh_private_key_file=psql_01ps.pem
#psql_01ss ansible_ssh_private_key_file=psql_01ss.pem
```

Configure the `host_name.yml` file in the `host_vars` folder

Enter the appropriate parameters for your system into the blue underlined fields, and then copy and paste the entries into the `host_name.yml` file in the Ansible controller `host_vars` folder.

```
<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 AWS EC2 instance IP address for the respective PostgreSQL
server 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>

# "{{groups.postgresql[0]}}" represents first PostgreSQL DB server as
defined in PostgreSQL hosts group [postgresql]. For concurrent multiple
PostgreSQL DB servers deployment, [0] will be incremented for each
additional DB server. For example, "{{groups.postgresql[1]}}" represents
DB server 2, "{{groups.postgresql[2]}}" represents DB server 3 ... As a
good practice and the default, two volumes are allocated to a PostgreSQL
DB server with corresponding /pgdata, /pglogs mount points, which store
PostgreSQL data, and PostgreSQL log files respectively. The number and
naming of DB volumes allocated to a DB server must match with what is
defined in global fsx_vars.yml file by src_db_vols, src_archivelog_vols
parameters, which dictates how many volumes are to be created for each DB
server. agr_name is agr1 by default. Do not change. lif address is the
NFS IP address for the SVM where PostgreSQL server is expected to mount
its database volumes. Primary site servers from primary SVM and standby
servers from standby SVM.

host_datastores_nfs:
- {vol_name: "<span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-

```

```

decoration:underline;"/><i>{{groups.postgresql[0]}}_pgdata</i></span>&quot
, aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"><i>aggr1</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" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>100</i></span>
- {vol_name: &quot<span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"><i>{{groups.postgresql[0]}}_pglogs</i></span>&quot
, aggr_name: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"><i>aggr1</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" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>100</i></span>}

# Add swap space to EC2 instance, that is equal to size of RAM up to 16G
max. Determine the number of blocks by dividing swap size in MB by 128.
swap_blocks: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>128</i></span>

# Postgresql user configurable parameters
pgsql_port: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>5432</i></span>
buffer_cache: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>8192MB</i></span>
archive_mode: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>"on"</i></span>
max_wal_size: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>5GB</i></span>
client_address: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>172.30.15.0/24</i></span>

</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>

```

Configure the global `fsx_vars.yml` file in the `vars` folder

Input the appropriate parameters for your system into the blue underlined fields, and then copy and paste the entries into the `fsx_vars.yml` file at the Ansible controller host.

```

<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">
#####
##### PostgreSQL HADR global user configuration variables #####
##### Consolidate all variables from FSx, Linux, and postgresql #####
#####
##### Ontap env specific config variables #####
#####

#####
# Variables for SnapMirror Peering
#####
#Passphrase for cluster peering authentication
passphrase: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-

```

```

decoration:underline;"/><i>xxxxxxxx</i></span>

#Please enter destination or standby FSx cluster name
dst_cluster_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>FsxId0cf8e0bccb14805e8</i></span>

#Please enter destination or standby FSx cluster management IP
dst_cluster_ip: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>172.30.15.90</i></span>

#Please enter destination or standby FSx cluster inter-cluster IP
dst_inter_ip: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>172.30.15.13</i></span>

#Please enter destination or standby SVM name to create mirror relationship
dst_vserver: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>dr</i></span>

#Please enter destination or standby SVM management IP
dst_vserver_mgmt_lif: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>172.30.15.88</i></span>

#Please enter destination or standby SVM NFS lif
dst_nfs_lif: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>172.30.15.88</i></span>

#Please enter source or primary FSx cluster name
src_cluster_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>FsxId0cf8e0bccb14805e8</i></span>

#Please enter source or primary FSx cluster management IP
src_cluster_ip: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>172.30.15.20</i></span>

#Please enter source or primary FSx cluster inter-cluster IP
src_inter_ip: <span <div contenteditable="true" style="color:#004EFF;

```

```

font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"/><i>172.30.15.5</i></span>

#Please enter source or primary SVM name to create mirror relationship
src_vserver: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"/><i>prod</i></span>

#Please enter source or primary SVM management IP
src_vserver_mgmt_lif: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"/><i>172.30.15.115</i></span>

#####
#####
#
# Variable for PostgreSQL Volumes, lif - source or primary FSx NFS lif address
#####
#####
#####

src_db_vols:
- {vol_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>{{groups.postgresql[0]}}_pgdata</i></span>", aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"/><i>aggr1</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" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"/><i>100</i></span>}"}

src_archivelog_vols:
- {vol_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>{{groups.postgresql[0]}}_pglogs</i></span>", aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"/><i>aggr1</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" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"/><i>100</i></span>}"}

```

```

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

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

#NFS Mount points for PostgreSQL DB volumes
mount_points:
  - <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>/pgdata</i></span>
  - <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>/pglogs</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>xxxxx</i></span>
redhat_sub_password: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>xxxxx</i></span>

#####
#####
### DB env specific install and config variables ###
#####
#####
#The latest version of PostgreSQL RPM is pulled/installed and config file is deployed from a preconfigured template
#Recovery type and point: default as all logs and promote and leave all PITR parameters blank

</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: " + i + ", name: " + infra_NFS + ", protocol: " + NFS + "}";
}
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: " + vol_name + ", ';
}

```

```

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>

```

PostgreSQL deployment and HA/DR setup

The following tasks deploy the PostgreSQL DB server service and initialize the database at the primary site on the primary EC2 DB server host. A standby primary EC2 DB server host is then set up at the standby site. Finally, DB volume replication is set up from the primary-site FSx cluster to the standby-site FSx cluster for disaster recovery.

1. Create DB volumes on the primary FSx cluster, and set up postgresql on the primary EC2 instance host.

```
ansible-playbook -i hosts postgresql_deploy.yml -u ec2-user --private
-key psql_01p.pem -e @vars/fsx_vars.yml
```

2. Set up the standby DR EC2 instance host.

```
ansible-playbook -i hosts postgresql_standby_setup.yml -u ec2-user
--private-key psql_01s.pem -e @vars/fsx_vars.yml
```

3. Set up FSx ONTAP cluster peering and database volume replication.

```
ansible-playbook -i hosts fsx_replication_setup.yml -e
@vars/fsx_vars.yml
```

4. Consolidate the previous steps into a single-step PostgreSQL deployment and HA/DR setup.

```
ansible-playbook -i hosts postgresql_hadr_setup.yml -u ec2-user -e @vars/fsx_vars.yml
```

5. For setting up a standby PostgreSQL DB host at either the primary or standby sites, comment out all other servers in the hosts file [dr_postgresql] section and then execute the postgresql_standby_setup.yml playbook with the respective target host (such as psql_01ps or standby EC2 compute instance at primary site). Make sure that a host parameters file such as psql_01ps.yml is configured under the host_vars directory.

```
[dr_postgresql] --  
#psql_01s ansible_ssh_private_key_file=psql_01s.pem  
psql_01ps ansible_ssh_private_key_file=psql_01ps.pem  
#psql_01ss ansible_ssh_private_key_file=psql_01ss.pem
```

```
ansible-playbook -i hosts postgresql_standby_setup.yml -u ec2-user  
--private-key psql_01ps.pem -e @vars/fsx_vars.yml
```

PostgreSQL database snapshot backup and replication to standby site

PostgreSQL database snapshot backup and replication to the standby site can be controlled and executed on the Ansible controller with a user-defined interval. We have validated that the interval can be as low as 5 minutes. Therefore, in the case of failure at the primary site, there is 5 minutes of potential data loss if failure occurs right before the next scheduled snapshot backup.

```
*/15 * * * * /home/admin/na_postgresql_aws_deploy_hadr/data_log_snap.sh
```

Failover to Standby Site for DR

For testing the PostgreSQL HA/DR system as a DR exercise, execute failover and PostgreSQL database recovery on the primary standby EC2 DB instance on standby site by executing following playbook. In an actually DR scenario, execute the same for an actually failover to DR site.

```
ansible-playbook -i hosts postgresql_failover.yml -u ec2-user --private  
-key psql_01s.pem -e @vars/fsx_vars.yml
```

Resync Replicated DB volumes after Failover Test

Run resync after the failover test to reestablish database-volume SnapMirror replication.

```
ansible-playbook -i hosts postgresql_standby_resync.yml -u ec2-user  
--private-key psql_01s.pem -e @vars/fsx_vars.yml
```

Failover from primary EC2 DB server to standby EC2 DB server due to EC2 compute instance failure

NetApp recommends running manual failover with well-established OS cluster-ware that might require a license.

Where to find additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

- Amazon FSx for NetApp ONTAP

<https://aws.amazon.com/fsx/netapp-ontap/>

- Amazon EC2

https://aws.amazon.com/pm/ec2/?trk=36c6da98-7b20-48fa-8225-4784bcd9843&sc_channel=ps&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2&ef_id=Cj0KCQiA54KfBhCKARIIsAJzSrdqwQrghn6I71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2

- NetApp Solution Automation

https://review.docs.netapp.com/us-en/netapp-solutions_aic_sql_aws/automation/automation_introduction.html

SnapCenter for databases

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

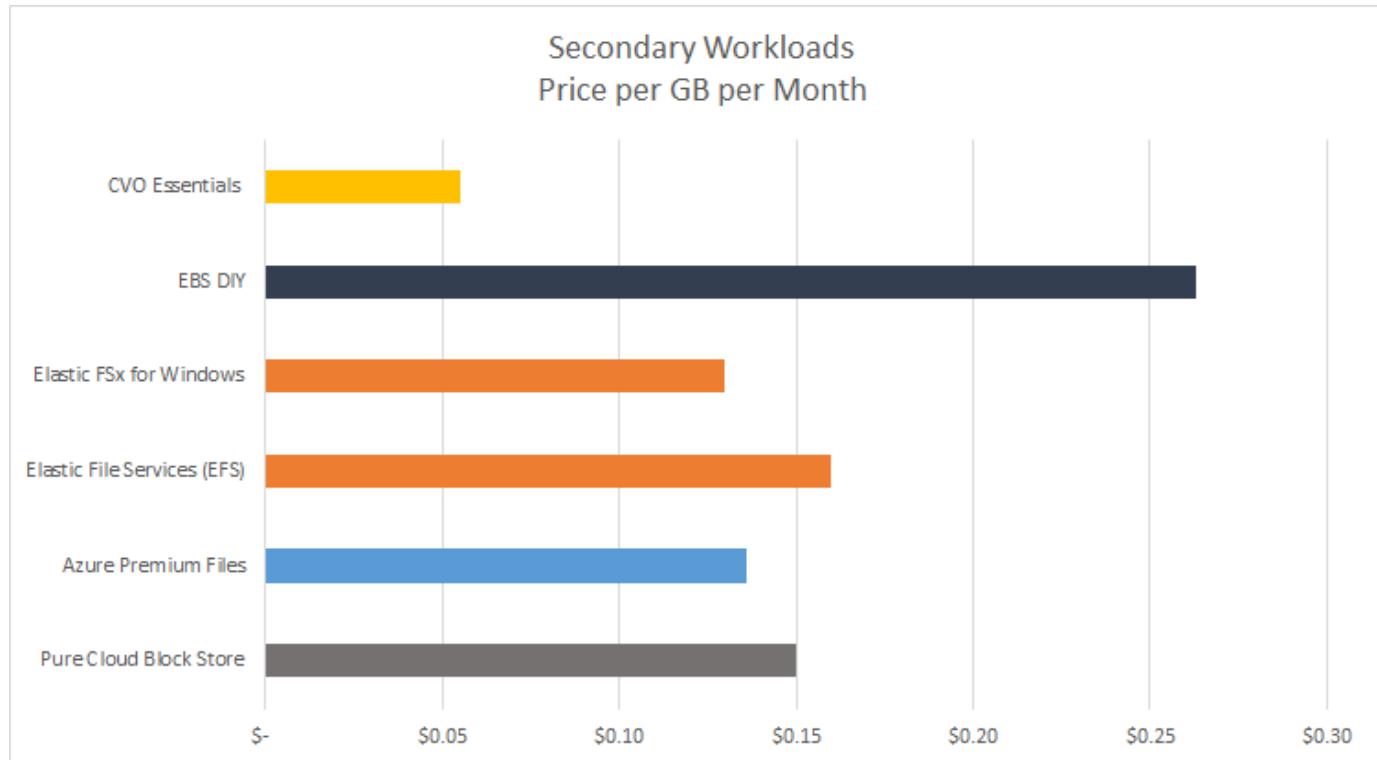
Today, many enterprise databases still reside in private corporate data centers for performance, security, and/or other reasons. This hybrid cloud database solution enables enterprises to operate their primary databases on site while using a public cloud for dev/test database operations as well as for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

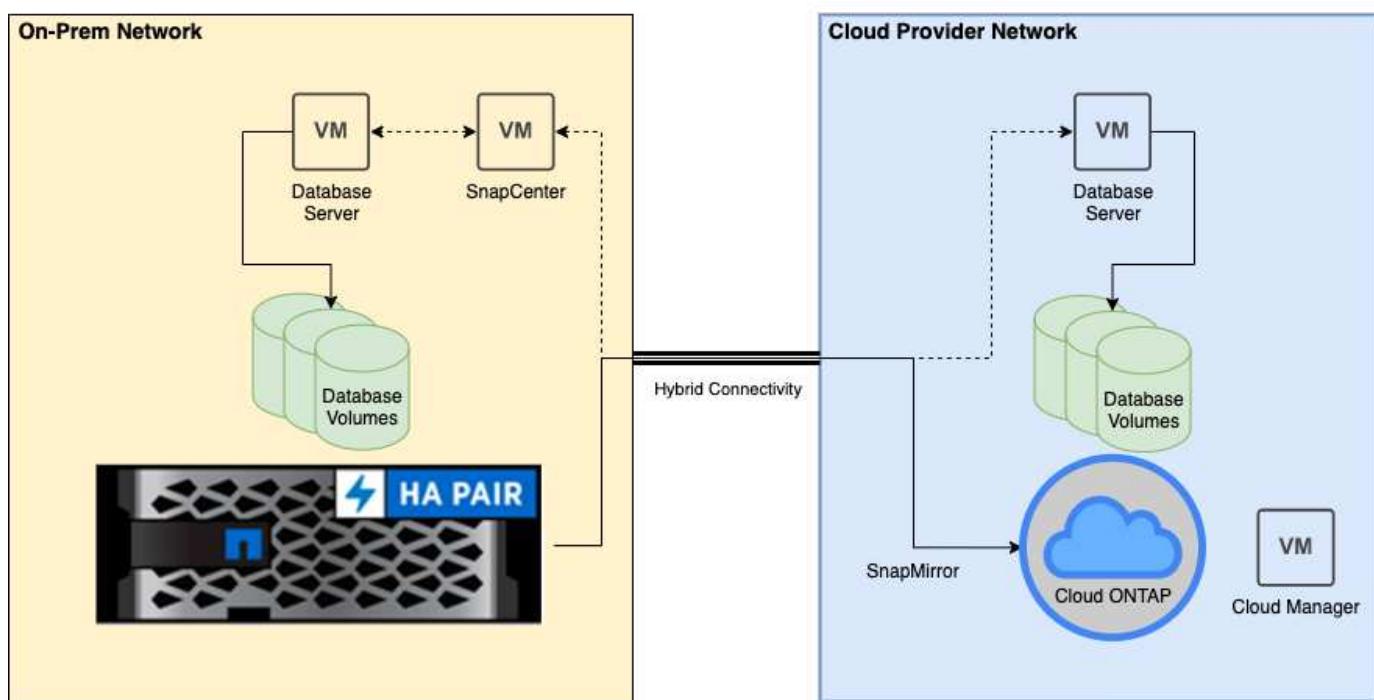
To test drive the solution and use cases for yourself, a NetApp Lab-on-Demand SL10680 can be requested at following xref:[./databases/ TL_AWS_004 HCoD: AWS - NW,SnapCenter\(OnPrem\)](#).

[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
On-premises	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
Cloud - AWS	Cloud Manager Connector Cloud Volumes ONTAP Matching DB OS EC2 instances to On-prem
Cloud - Azure	Cloud Manager Connector Cloud Volumes ONTAP Matching DB OS Azure Virtual Machines to On-prem
Cloud - GCP	Cloud Manager Connector Cloud Volumes ONTAP 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.

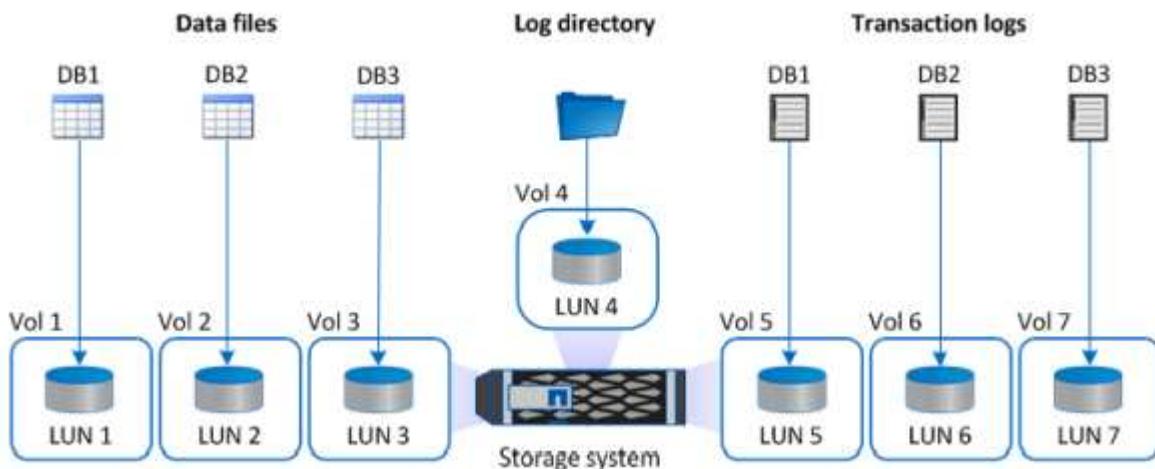
- **Single instance or HA deployment.** HA deployment provides redundancy in the case of a single SnapCenter instance server failure.
- **Name resolution.** DNS must be configured on the SnapCenter server to resolve all database hosts as well as on the storage SVM for forward and reverse lookup. DNS 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.

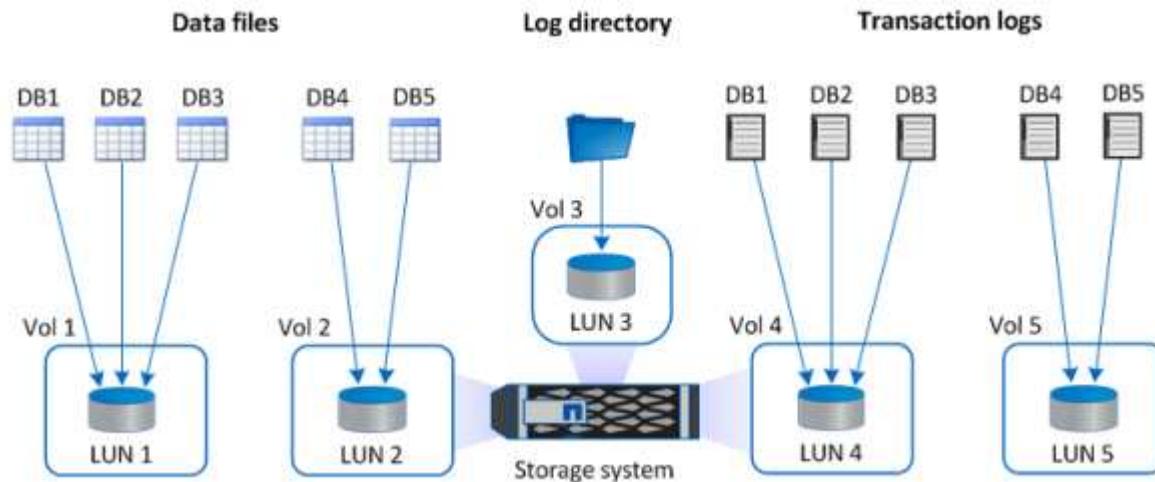
On-premises database server storage configuration

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.



i 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

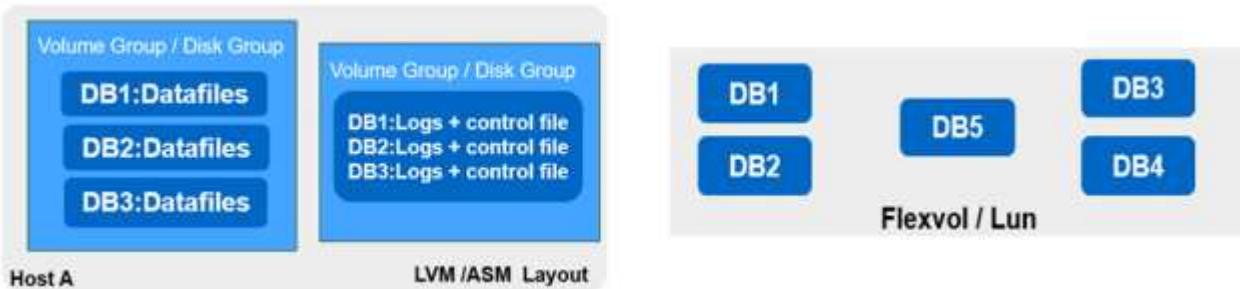
administrators to quickly restore (ONTAP single-file SnapRestore) or clone a large critical database (petabyte scale) using Snapshot technology within few seconds to minutes.



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
<input type="checkbox"/>	administrator	User	SnapCenterAdmin	demo
<input type="checkbox"/>	oradba	User	App Backup and Clone Admin	demo
<input type="checkbox"/>	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.

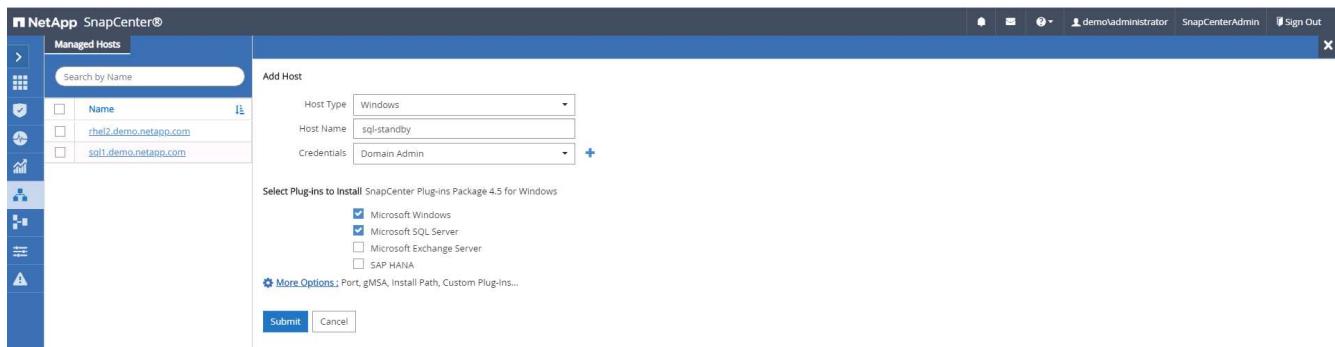
The following steps illustrate how a database host is added to SnapCenter while a SnapCenter plugin is installed on the host. The procedure applies to adding both on-premises hosts and cloud hosts. The following demonstration adds a Windows or a Linux host residing in AWS.

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.

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.



4. 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	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	Configure log directory

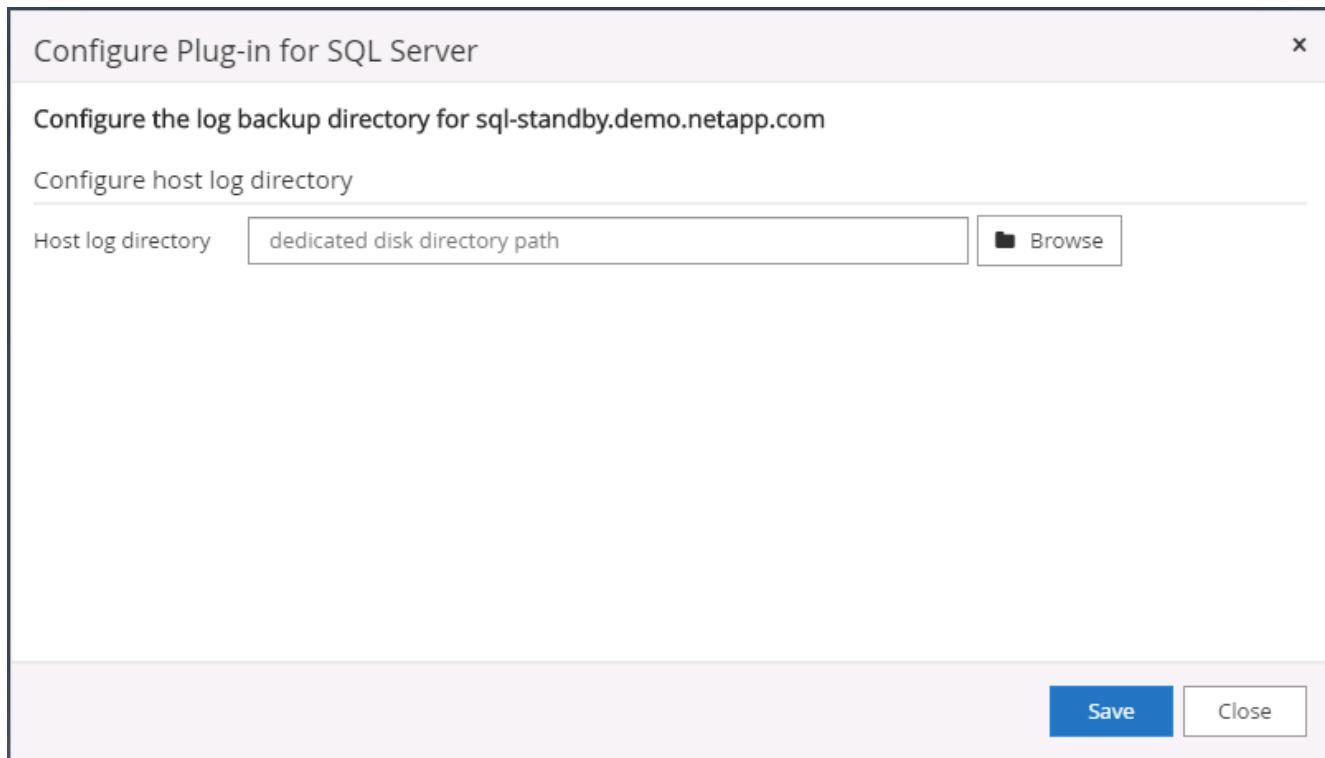
5. Click the Host Name to open the SQL Server log directory configuration.

Host Details

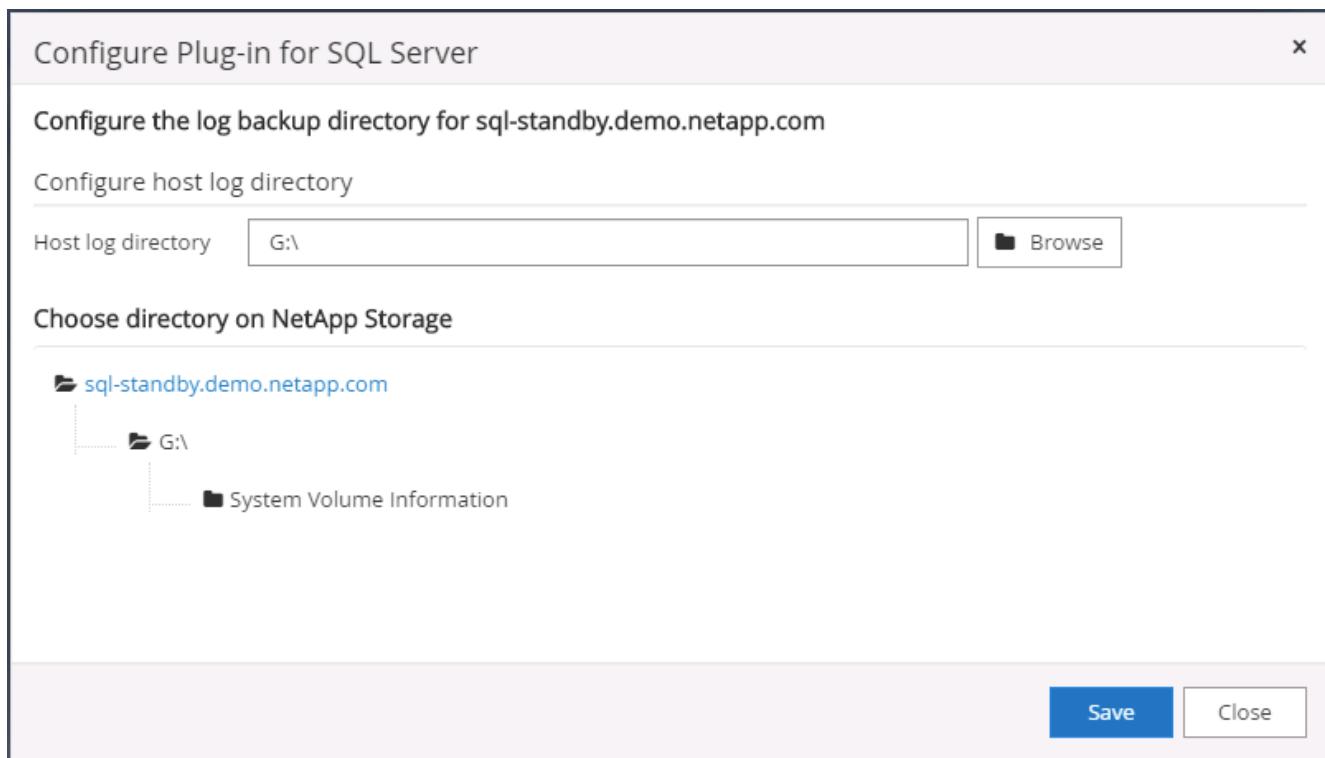
Host Name: sql-standby.demo.netapp.com
Host IP: 10.221.2.56
Overall Status: Configure log directory
Host Type: Windows
System: Stand-alone
Credentials: Domain Admin
Plug-ins: SnapCenter Plug-ins package 4.5.0.6123 for Windows
 ✓ Microsoft Windows
 ✓ Microsoft SQL Server [Remove](#) [Configure log directory](#)

More Options: Port, gMSA, Install Path, Add Plug-ins...

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



7. 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.

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

The screenshot shows the 'Managed Hosts' tab in the NetApp SnapCenter interface. On the left, there's a sidebar with icons for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area has a search bar and a table with columns: Name, Type, System, Version, and Overall Status. There are four hosts listed:

Name	Type	System	Version	Overall Status
rhel2.demo.netapp.com	Linux	Stand-alone	4.5	Running
sql1.demo.netapp.com	Windows	Stand-alone	4.5	Running
sql-standby.demo.netapp.com	Windows	Stand-alone	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.

The screenshot shows the 'Users and Access' tab in the NetApp SnapCenter interface. The sidebar is identical to the previous screenshot. The main area shows a table with columns: Name, Type, Roles, and Domain. Three users are listed:

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

The screenshot shows the 'Assign Assets' dialog box. The title is 'Assign Assets'. It has a dropdown for 'Asset Type' set to 'Host' and a search bar. Below is a list of assets with checkboxes:

	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

At the bottom are 'Save' and 'Close' buttons.

Add Unix host and installation of plugin on the host

- Log into SnapCenter with a user ID with SnapCenterAdmin privileges.
- Click the Hosts tab from left-hand menu, and click Add to open the Add Host workflow.
- 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**

- 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

Installation Path: /opt/NetApp/snapcenter

Skip preinstall checks

Add all hosts in the oracle RAC

Custom Plug-ins

Choose a File

Browse **Upload**

No plug-ins found.

Save **Cancel**

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

Host name	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	Domain	Roles
oradba	demo	App Backup and Clone Admin

Assign Assets

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		hnnt

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.

The screenshot shows the NetApp SnapCenter interface for an Oracle Database. The left sidebar includes options like Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area displays a table with columns: Name, Oracle Database Type, Host/Cluster, Resource Group, Policies, Last Backup, and Overall Status. One entry is shown: Name is cdb2, Oracle Database Type is Single Instance (Multitenant), Host/Cluster is rhel2.demo.netapp.com, and Overall Status is 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.

The screenshot shows the NetApp SnapCenter interface for Microsoft SQL Server. The left sidebar includes options like Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area displays a table with columns: Name, Instance, Host, Last Backup, Overall Status, and Type. Most databases (master, model, msdb, tempdb) have Overall Status as 'Not available for backup'. One database, tpcc, has Overall Status as 'Backup succeeded' with a timestamp of 09/14/2021 2:35:07 PM.

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.

The screenshot shows the NetApp SnapCenter interface for Microsoft SQL Server. The left sidebar includes options like Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area displays a table with columns: Name, Host, Resource Groups, Policies, State, and Type. Two instances are listed: sql-standby (Host: sql-standby.demo.netapp.com) and sql1 (Host: sql1.demo.netapp.com). The sql-standby instance has a red lock icon next to its name, indicating it is not accessible.

The screenshot shows the NetApp SnapCenter interface for Microsoft SQL Server. The left sidebar includes options like Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area displays a table titled 'Instance - Credentials' with columns: Name, Host, Resource Groups, Policies, State, and Type. Two instances are listed: sql-standby and sql1. A note at the top states: '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.' Below the table, there is a note: 'Not available for backup. DB is not on NetApp storage, auto-close is enabled or in recovery mode.'

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:

Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Protocols	Type
onPrem-01_IC	green		Default	192.168.0.113	onPrem-01	e0b		Intercluster
onPrem-01_mgmt1	green		Default	192.168.0.111	onPrem-01	e0c		Cluster/Node Mgmt
cluster_mngt	green		Default	192.168.0.101	onPrem-01	e0a		Cluster/Node Mgmt

Target CVO cluster:

ONTAP System Manager Overview

IPspaces

Cluster	Broadcast Domains
Cluster	Cluster
Default	Storage VMs svm_hybridcvo Broadcast Domains Default

Broadcast Domains

Cluster	9000 MTU	iPSpace: Cluster hybridcvo-01 e0b hybridcvo-02 e0b
Default	9001 MTU	iPSpace: Default hybridcvo-01 e0a hybridcvo-02 e0a

Network Interfaces

Name	Status	Storage VM	iPSpace	Address	Current Node	Current Port	Protocols	Type	Throughput (I)
hybridcvo-02_mgmt1	✓		Default	10.221.2.104	hybridcvo-02	e0a		Cluster/Node Mgmt	0
inter_1	✓		Default	10.221.1.180	hybridcvo-01	e0a		Intercluster,Cluster/Node Mgmt	0.02
inter_2	✓		Default	10.221.2.250	hybridcvo-02	e0a		Intercluster,Cluster/Node Mgmt	0.03
iscsi_1	✓	svm_hybridcvo	Default	10.221.1.5	hybridcvo-01	e0a	iSCSI	Data	0
iscsi_2	✓	svm_hybridcvo	Default	10.221.2.168	hybridcvo-02	e0a	iSCSI	Data	0

- 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:

- 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.

ONTAP System Manager (Return to classic version)

Overview

Applications

Volumes

LUNs

NVMe Namespaces

Shares

Qtrees

Quotas

Storage VMs

Tiers

NETWORK

Overview

Ethernet Ports

FC Ports

EVENTS & JOBS

PROTECTION

Overview

Relationships

HOSTS

CLUSTER

Overview

Settings

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 (highlighted)
Generate Passphrase
Manage Cluster Peers

Storage VM Peers

PEERED STORAGE VMs
✓ 1

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

Volumes

Protect (highlighted)

Name
onPrem_data
rhel2_u01
rhel2_u02
rhel2_u03
rhel2_u0309232119421203118
sql1_data
sql1_log
sql1_snapctr
svm_onPrem_root

rhel2_u03 Details

- STATUS:** Online
- STYLE:** FlexVol
- MOUNT PATH:** /rhel2_u03
- STORAGE VM:** svm_onPrem
- LOCAL TIER:** onPrem_01_SSD_1
- SNAPSHOT POLICY:** default
- QUOTA:** Off
- TYPE:** Read Write
- SPACE RESERVATION:**

Capacity
0 Bytes Available | 2.36 GB Used | 2.36 GB Overflow

Performance
Hour Day Week
Latency 1.5 1

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

Protect Volumes

PROTECTION POLICY: Asynchronous

Source:

- CLUSTER: onPrem
- STORAGE VM: svm_onPrem
- SELECTED VOLUMES: rhel2_u03

Destination:

- CLUSTER: hybridcvo
- STORAGE VM: svm_hybridcvo

Destination Settings: 2 matching labels

VOLUME NAME: vol_<SourceVolumeName>_dest

Configuration Details:

- Initialize relationship
- Enable FabricPool

Save **Cancel**

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

The screenshot shows the 'Volumes' section of the NetApp SnapCenter interface. On the left, a list of volumes is shown with columns for Name and Status. A volume named 'rhel2_u03' is selected, highlighted with a blue border. To the right, a detailed view of this volume is displayed with tabs for Overview, Snapshot Copies, Clone Hierarchy, and SnapMirror (Local or Remote). The 'SnapMirror (Local or Remote)' tab is active, showing a table with columns for Source, Destination, Protection Policy, Relationship Health, Relationship Status, and Lag. The table entry for 'rhel2_u03' indicates it is mirrored to 'svm_onPrem:rhel2_u03' with a protection policy of 'MirrorAllSnapshots', healthy relationship, mirrored status, and a lag of 12 seconds.

6. Add CVO database storage SVM to SnapCenter

1. Log into SnapCenter with a user ID with SnapCenterAdmin privileges.
2. 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.

The screenshot shows the 'Add Storage System' dialog box within the NetApp SnapCenter interface. The 'ONTAP Storage' tab is selected. In the main area, there is a form for entering storage system details: 'Storage System' (IP address 10.0.0.1), 'Username' (admin), and 'Password' (*****). Below the form are 'Event Management System (EMS) & AutoSupport Settings' options, including checkboxes for 'Send AutoSupport notification to storage system' and 'Log SnapCenter Server events to syslog'. There is also a link to 'More Options'. At the bottom of the dialog are 'Submit', 'Cancel', and 'Reset' buttons.

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

The screenshot shows the 'More Options' configuration dialog box. It contains fields for Platform (set to 'Cloud Volumes ONTAP'), Protocol (set to 'HTTPS'), Port (set to 443), Timeout (set to 60 seconds), and Preferred IP (checkbox is unchecked). A checkbox labeled 'Secondary' is checked. At the bottom are 'Save' and 'Cancel' buttons.

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

The screenshot shows the ONTAP Storage section of the NetApp SnapCenter interface. On the left is a navigation sidebar with options like Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems (which is selected), Settings, and Alerts. The main area is titled 'ONTAP Storage' and shows 'ONTAP Storage Connections'. A table lists three connections: 'svm_hybridcvo' (IP: 10.0.0.1, Cluster Name: 10.0.0.1, User Name: [redacted], Platform: CVO, Controller License: crossed out) and 'svm_onPrem' (IP: 192.168.0.101, Cluster Name: [redacted], User Name: [redacted], Platform: CVO, Controller License: checked). There are 'New' and 'Delete' buttons at the top right.

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 Polices.

The screenshot shows the Policies section of the NetApp SnapCenter interface. The navigation sidebar includes Storage Systems (selected), Settings, and Alerts. The main area is titled 'Policies' and shows 'Oracle Database' backup policies. A table lists two policies: 'Oracle Archive Log Backup' (Backup Type: LOG, ONLINE, Schedule Type: Hourly, Replication: SnapMirror, Verification: [redacted]) and 'Oracle Full Online Backup' (Backup Type: FULL, ONLINE, Schedule Type: Daily, Replication: SnapMirror, Verification: [redacted]). There are 'New', 'Edit', 'Copy', 'Delete', 'Details', and 'Clone' buttons at the top right.

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

Modify 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

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

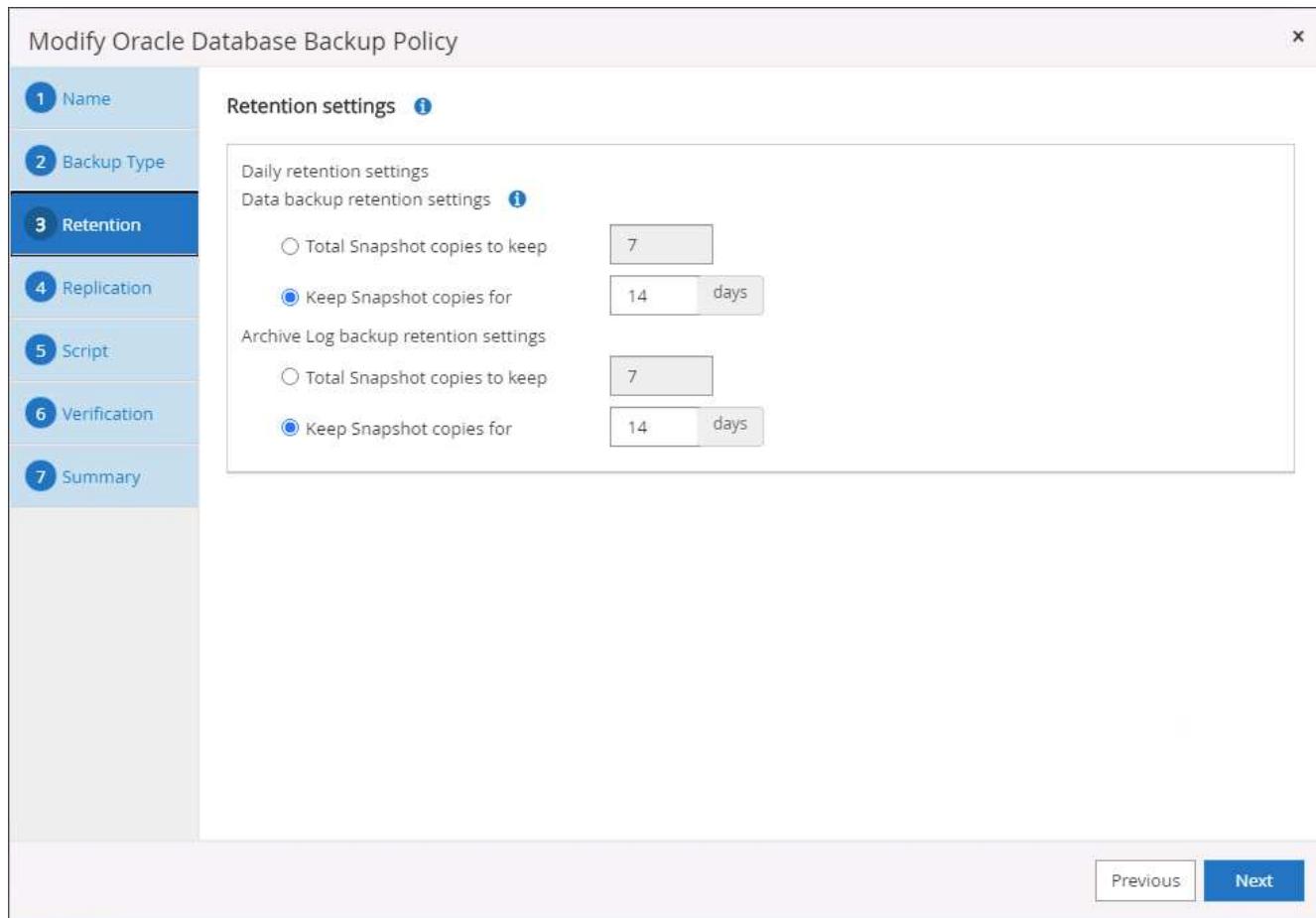
Daily

Previous

Next

This screenshot shows the 'Modify Oracle Database Backup Policy' wizard, specifically Step 2: Backup Type. The left sidebar lists steps 1 through 7. The main area is titled 'Select Oracle database backup options' and contains a section for 'Choose backup type'. Under 'Online backup', 'Datafiles, control files, and archive logs' is selected. There are also options for 'Datafiles and control files' and 'Archive logs'. Below this is another section for 'Choose schedule frequency' with 'Daily' selected. At the bottom right are 'Previous' and 'Next' buttons.

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

1 Name	Summary
2 Backup Type	Policy name: Oracle Full Online Backup Details: Backup all data and log files
3 Retention	Backup type: Online backup
4 Replication	Schedule type: Daily RMAN catalog backup: Disabled
5 Script	Archive log pruning: None On demand data backup retention: None
6 Verification	On demand archive log backup retention: None Hourly data backup retention: None Hourly archive log backup retention: None
7 Summary	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

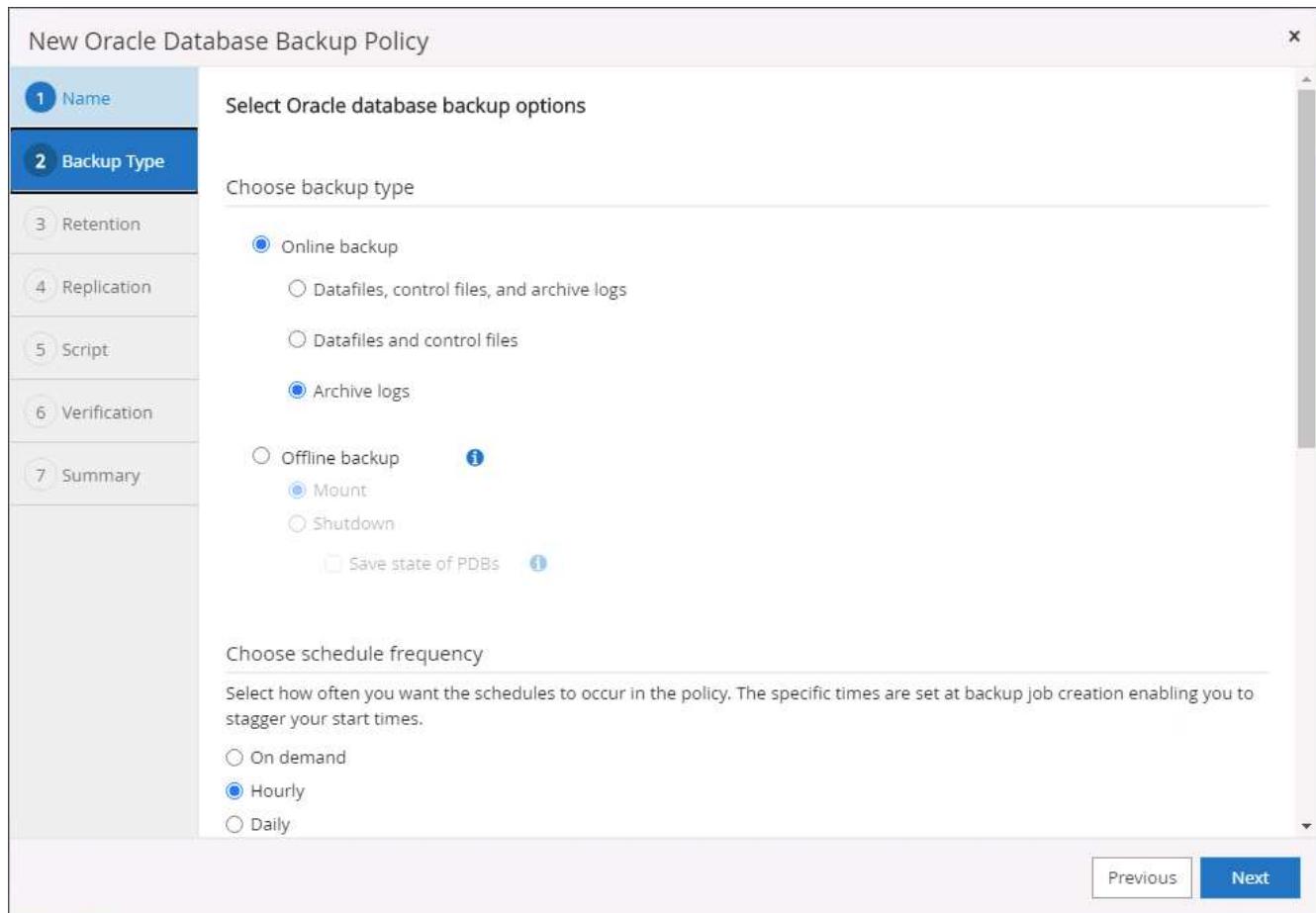
5 Script

6 Verification

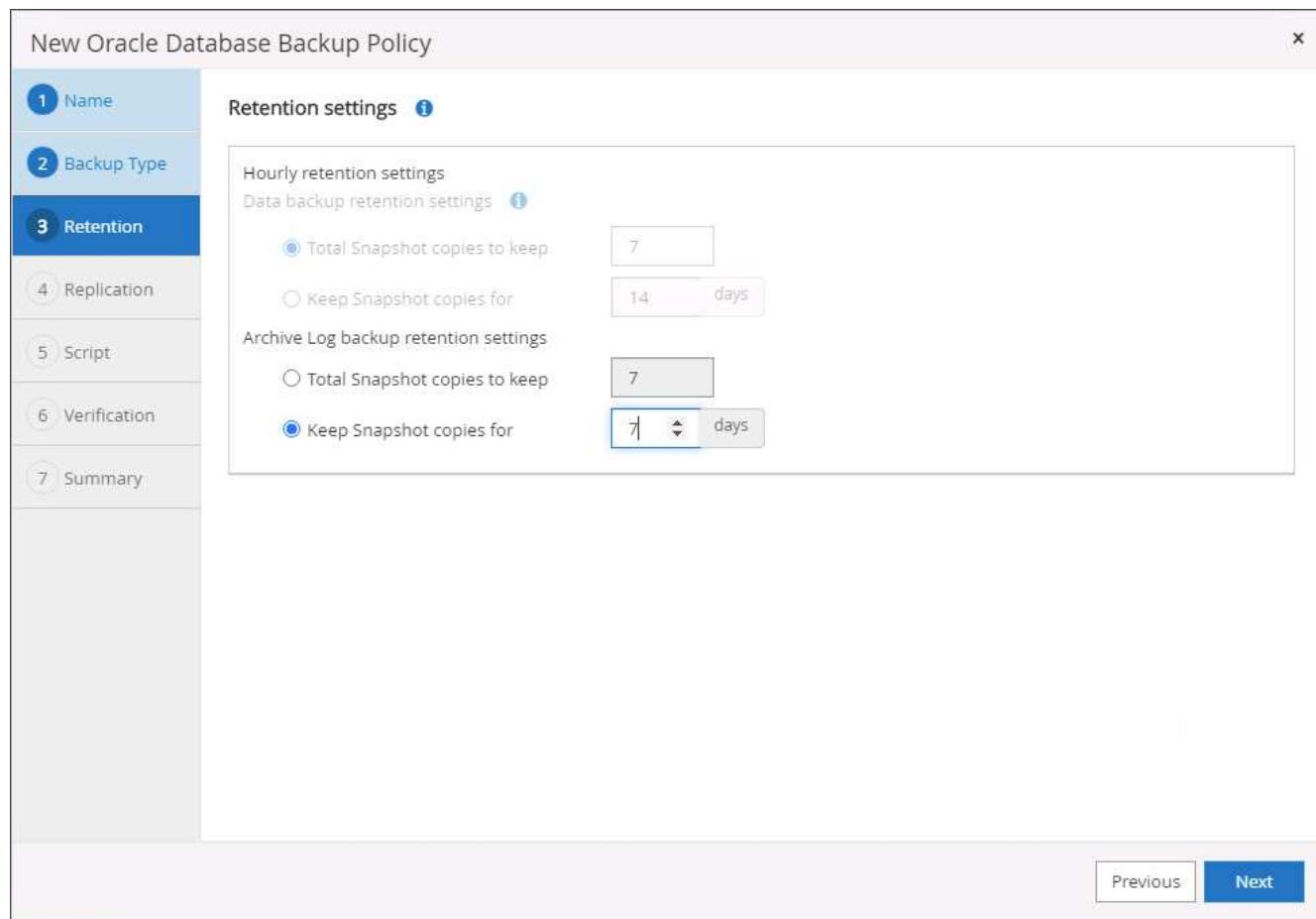
7 Summary

Previous Next

3. Select the backup type and schedule frequency.



4. Set the log retention period.



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

New Oracle Database Backup Policy

1 Name

Select secondary replication options [i](#)

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Secondary policy label [i](#)

Error retry count [i](#)

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

This screenshot shows the 'New Oracle Database Backup Policy' dialog box, specifically step 4: Replication. On the left, a vertical navigation bar lists steps 1 through 7. Step 4, 'Replication', is highlighted with a blue background. The main panel contains two sections: 'Select secondary replication options' with a link to information, and a list of checkboxes. The first checkbox, 'Update SnapMirror after creating a local Snapshot copy.', is checked and has a blue checkmark. The second checkbox, 'Update SnapVault after creating a local Snapshot copy.', is unchecked and has a grey outline. Below these are two input fields: 'Secondary policy label' with a dropdown menu showing 'Hourly' and a help icon, and 'Error retry count' with a text input field containing '3' and a help icon. At the bottom right are 'Previous' and 'Next' buttons.

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

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

5 Script

6 Verification

7 Summary

[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

1 Name	Summary
2 Backup Type	Policy name: Oracle Archive Log Backup Details: Backup Oracle archive logs
3 Retention	Backup type: Online backup
4 Replication	Schedule type: Hourly RMAN catalog backup: Disabled
5 Script	Archive log pruning: None
6 Verification	On demand data backup retention: None On demand archive log backup retention: None
7 Summary	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

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

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 interface. On the left is a navigation sidebar with icons for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings (which is selected), and Alerts. The main content area has a header with 'Policies' and 'Credential' tabs, and a dropdown for '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.' To the right of the table 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.

New SQL Server Backup Policy X

Provide a policy name

Policy name	SQL Server Full Backup	i
Details	Backup all data and log files	

1 Name 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' step is active, with the policy name set to 'SQL Server Full Backup' and the details set to 'Backup all data and log files'. The 'Backup Type' step is the next in the sequence.

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

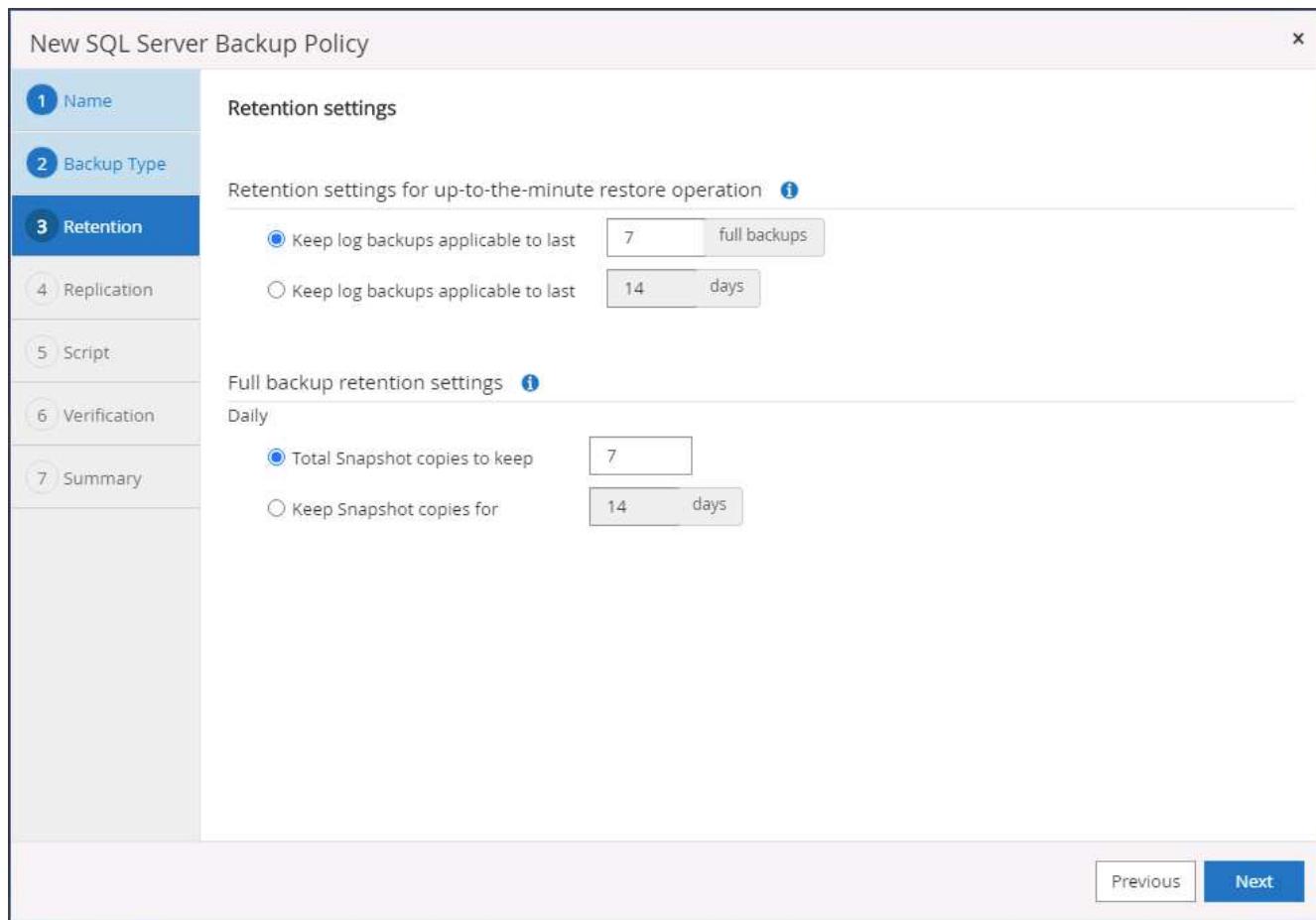
Daily

Weekly

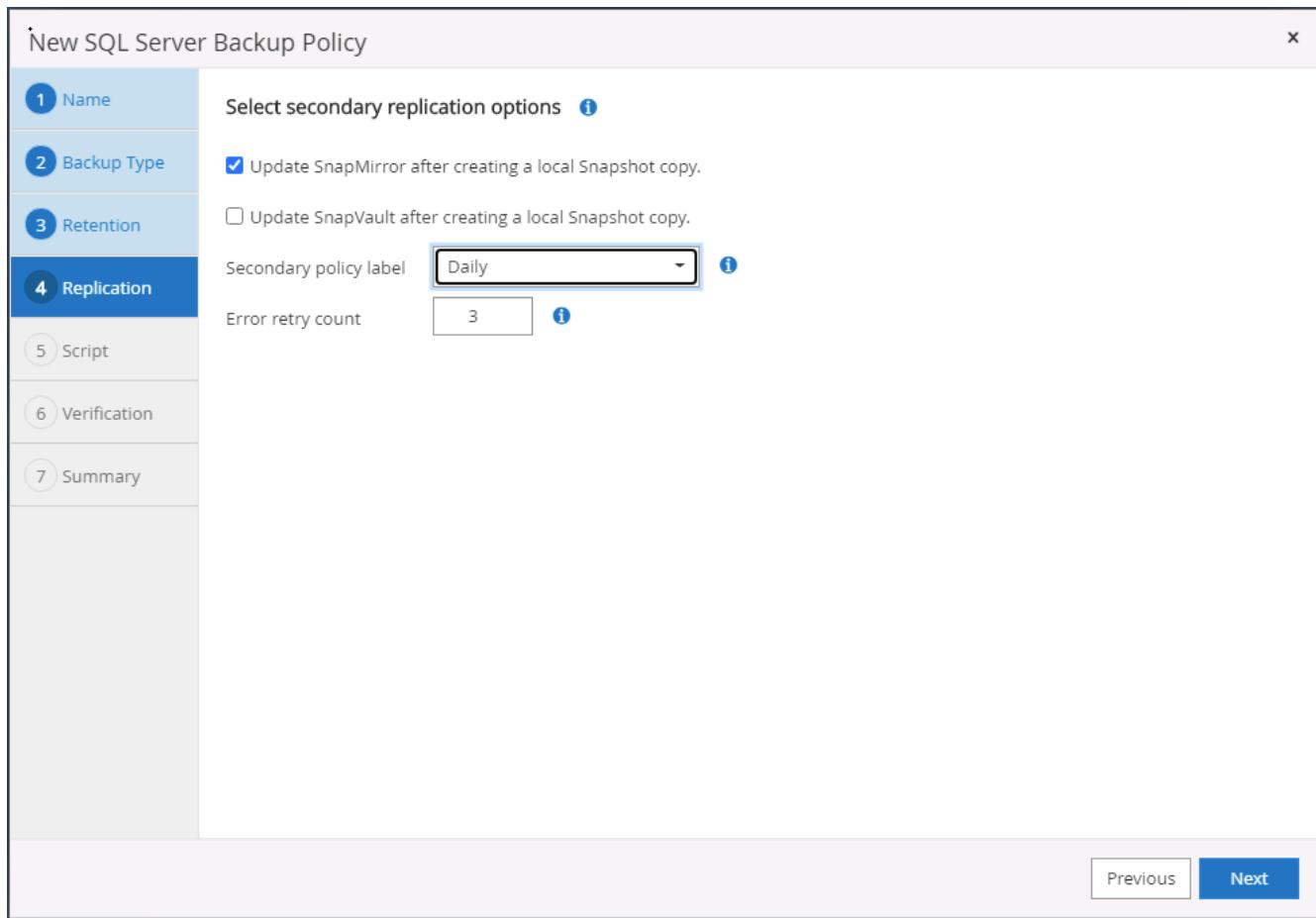
Monthly

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 Specify optional scripts to run after performing a backup job

5 Script Postscript full path
Postscript arguments Choose optional arguments...

6 Verification Script timeout 60 secs

7 Summary

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
7 Summary	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
	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:

Previous Finish

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' step is active. The 'Policy name' is set to 'SQL Server Log Backup'. The 'Details' field contains 'Backup SQL server log'. A blue information icon is visible on the right. Navigation buttons 'Previous' and 'Next' are at the bottom.

- 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 ▼

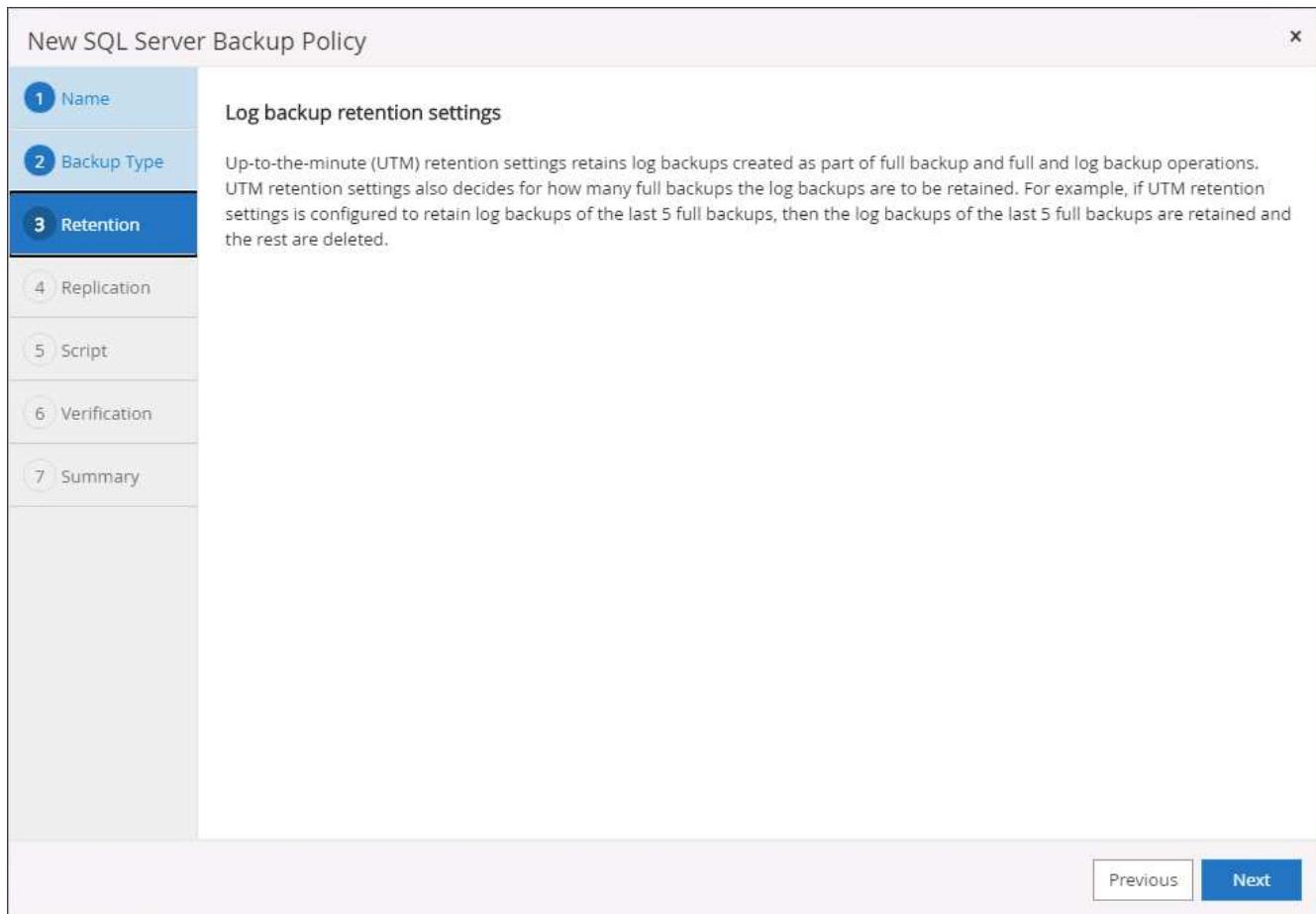
Schedule frequency

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.

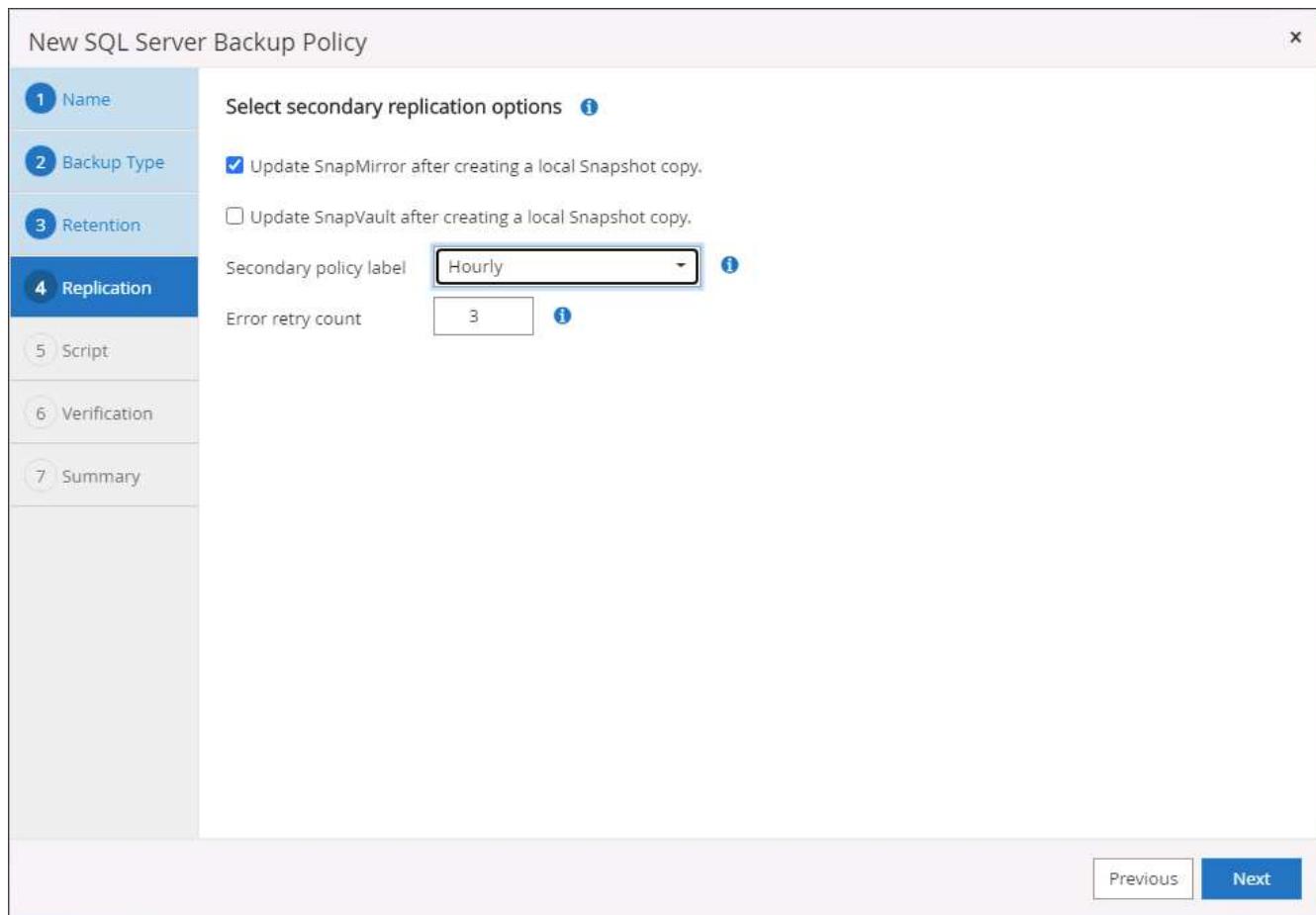
On demand
 Hourly
 Daily
 Weekly
 Monthly

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	Setting
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

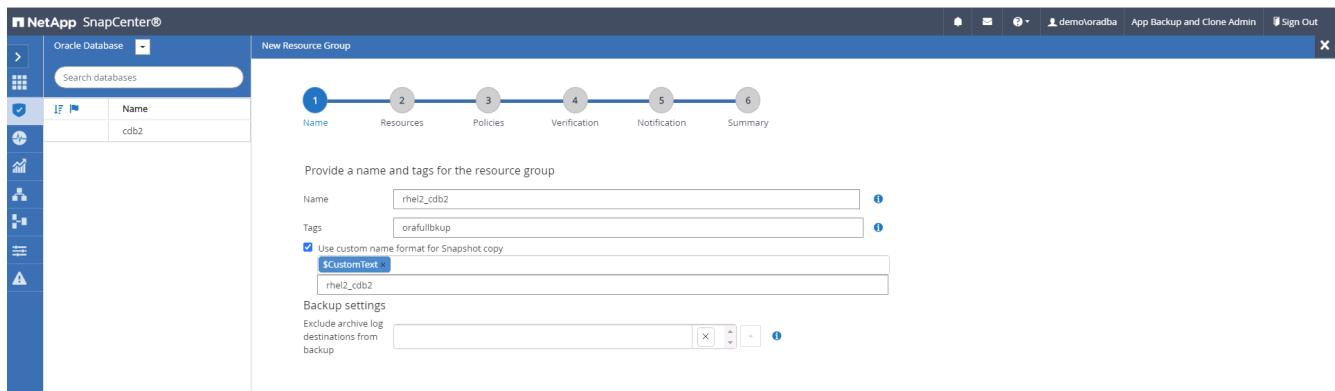
SnapCenter uses a resource group to backup a database in a logical grouping of database resources, such as multiple databases hosted on a server, a database sharing the same storage volumes, multiple databases supporting a business application, and so on. Protecting a single database creates a resource 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

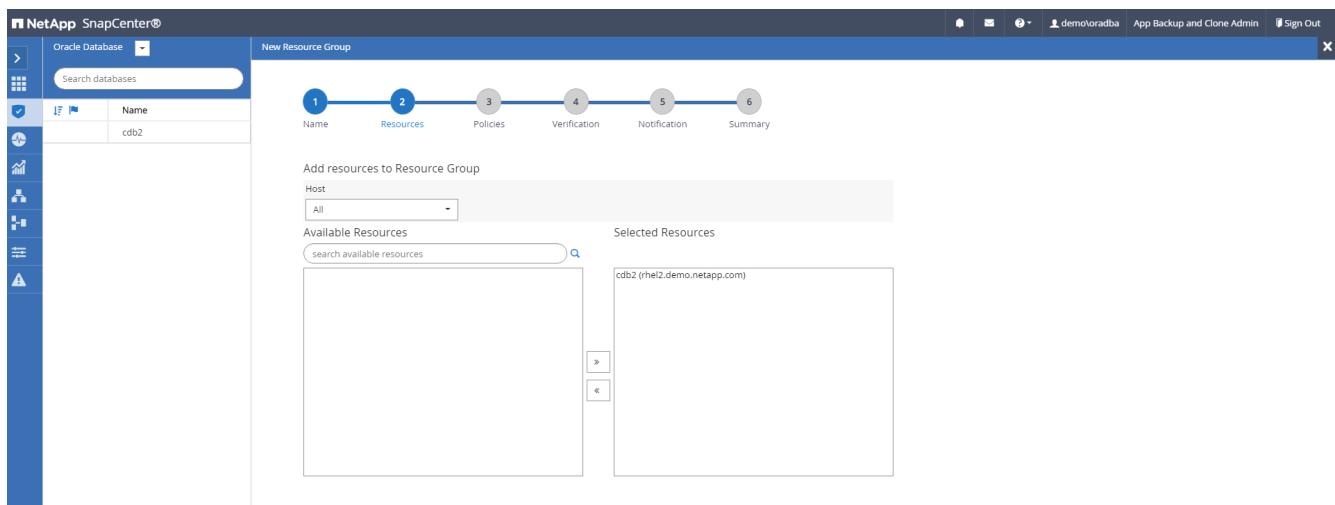
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either Database or Resource Group to launch the resource group creation workflow.

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

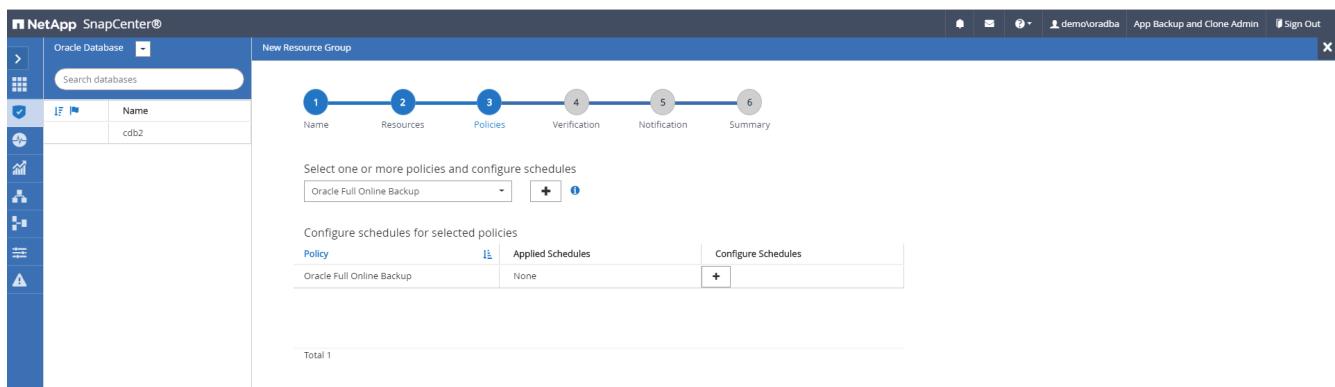
2. Provide a name and tags for the resource group. You can define a naming format for the Snapshot copy and bypass the redundant archive log destination if configured.



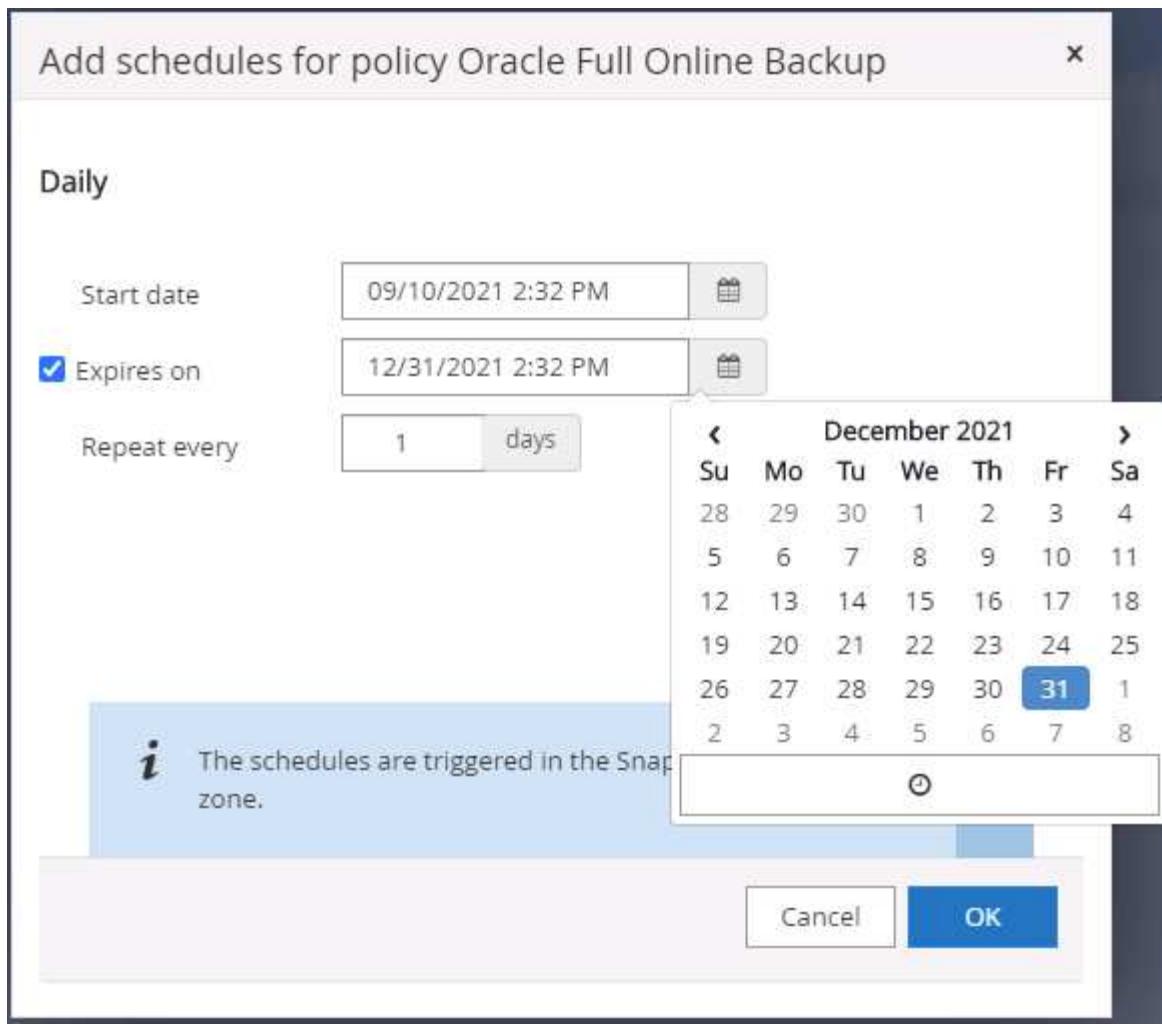
3. Add database resources to the resource group.



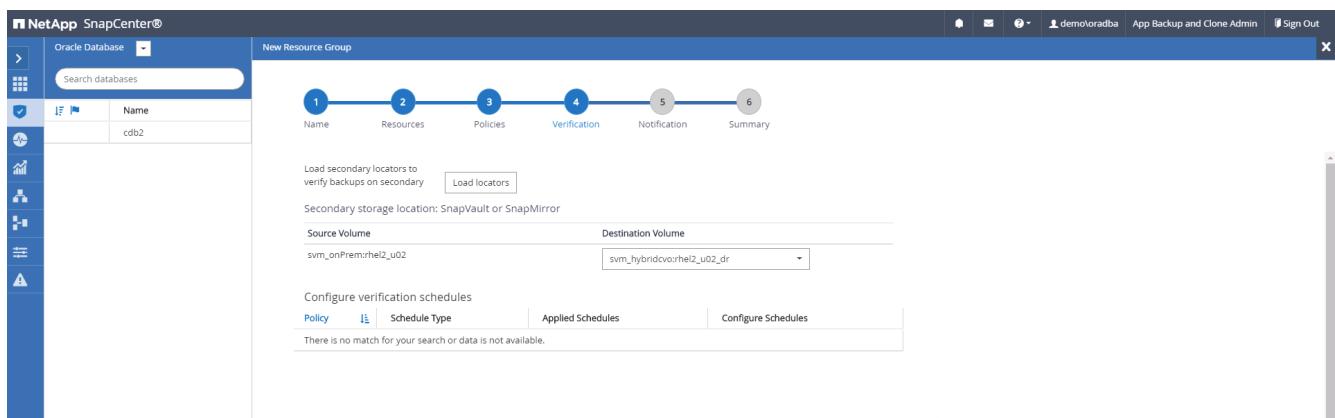
4. Select a full backup policy created in section 7 from the drop-down list.



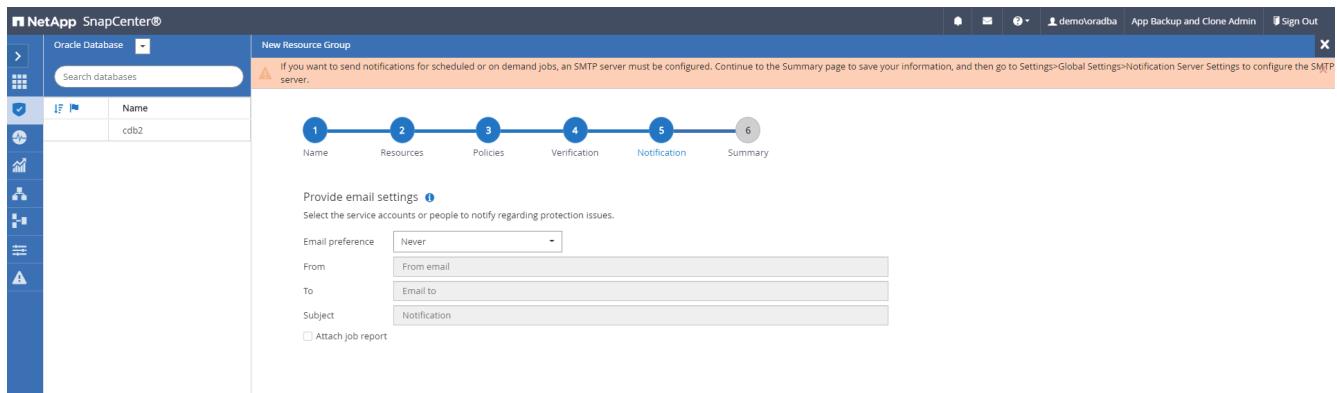
5. Click the (+) sign to configure the desired backup schedule.



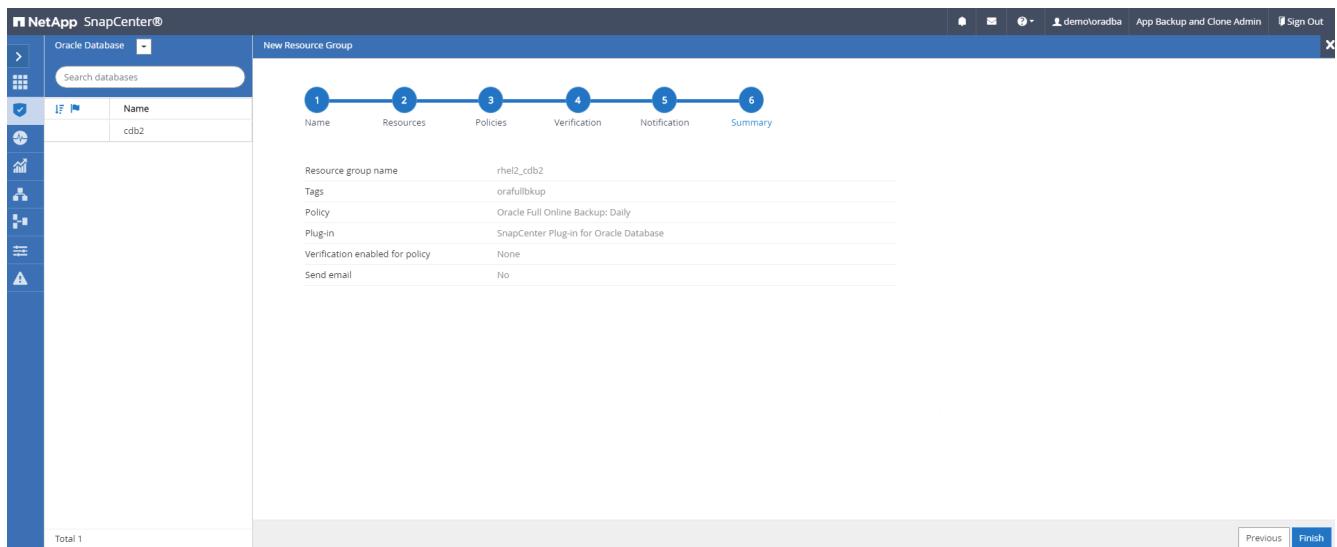
6. Click Load Locators to load the source and destination volume.



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



8. Summary.

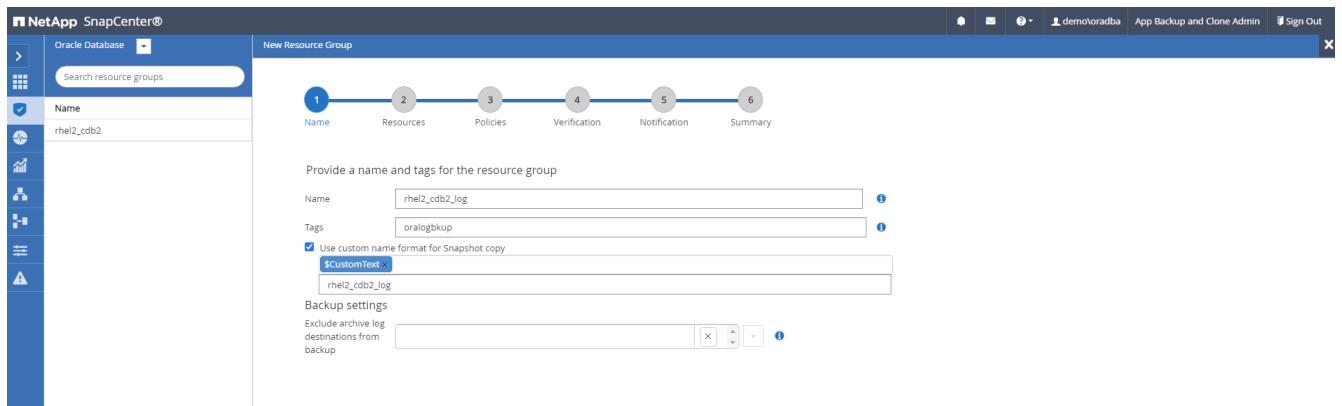


Create a resource group for log backup of Oracle

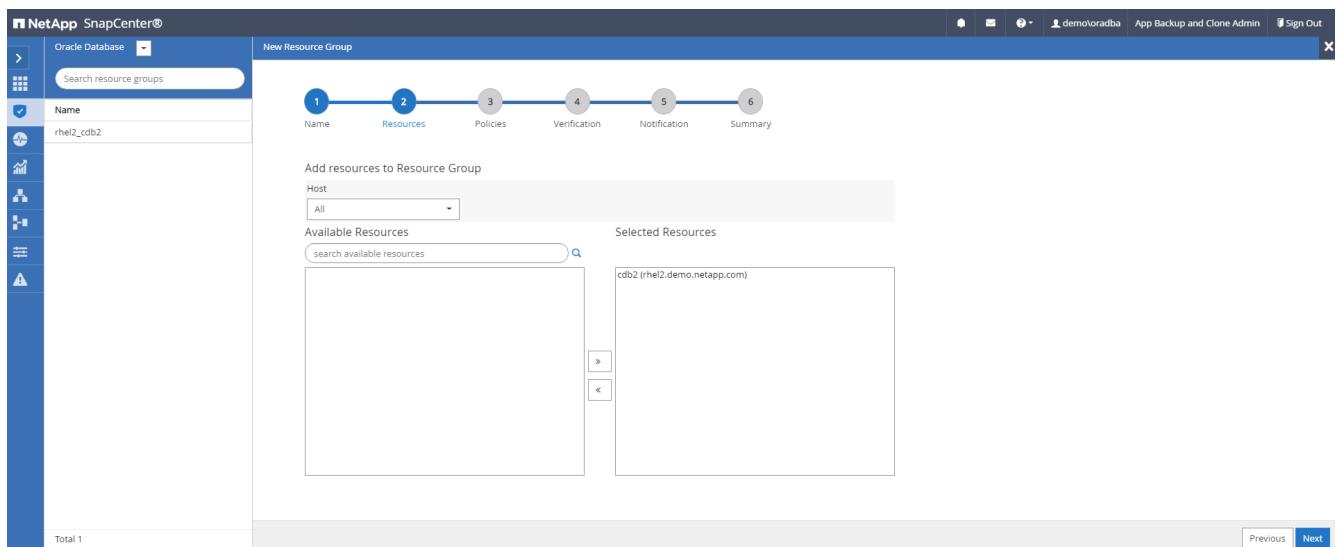
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either Database or Resource Group to launch the resource group creation workflow.



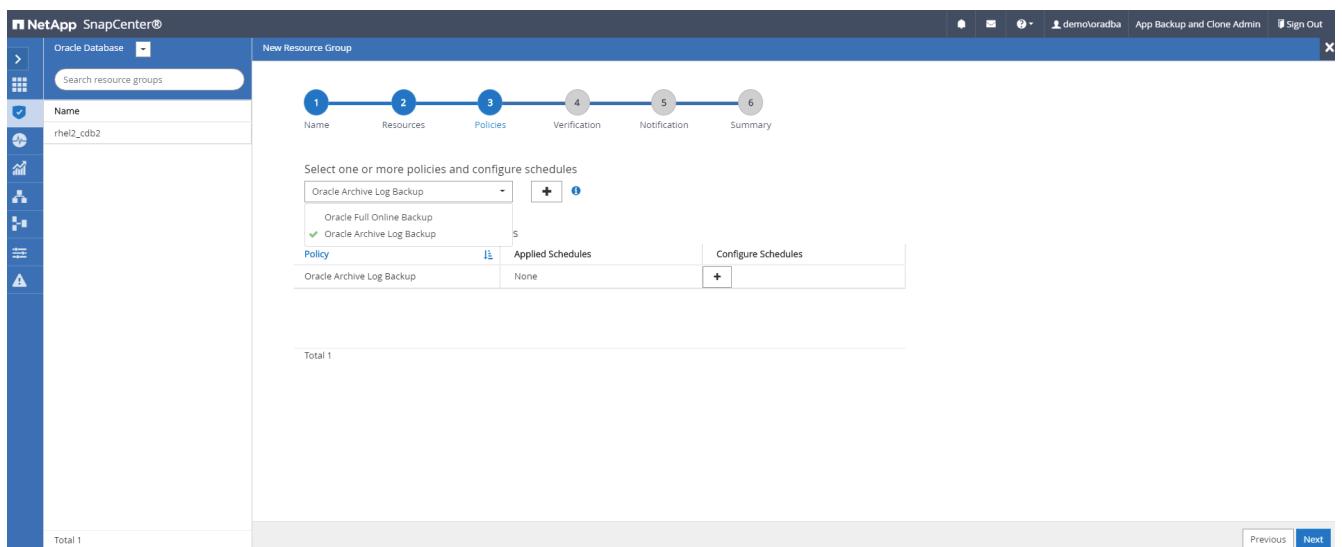
2. Provide a name and tags for the resource group. You can define a naming format for the Snapshot copy and bypass the redundant archive log destination if configured.



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

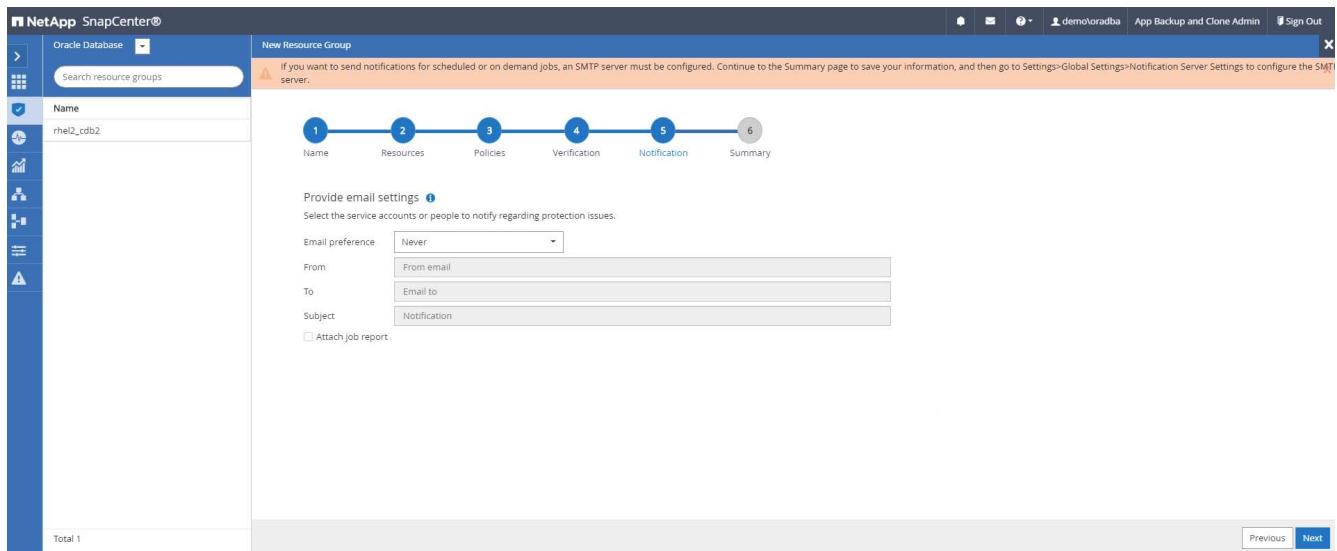
Policy Schedule Type Applied Schedules Configure Schedules

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

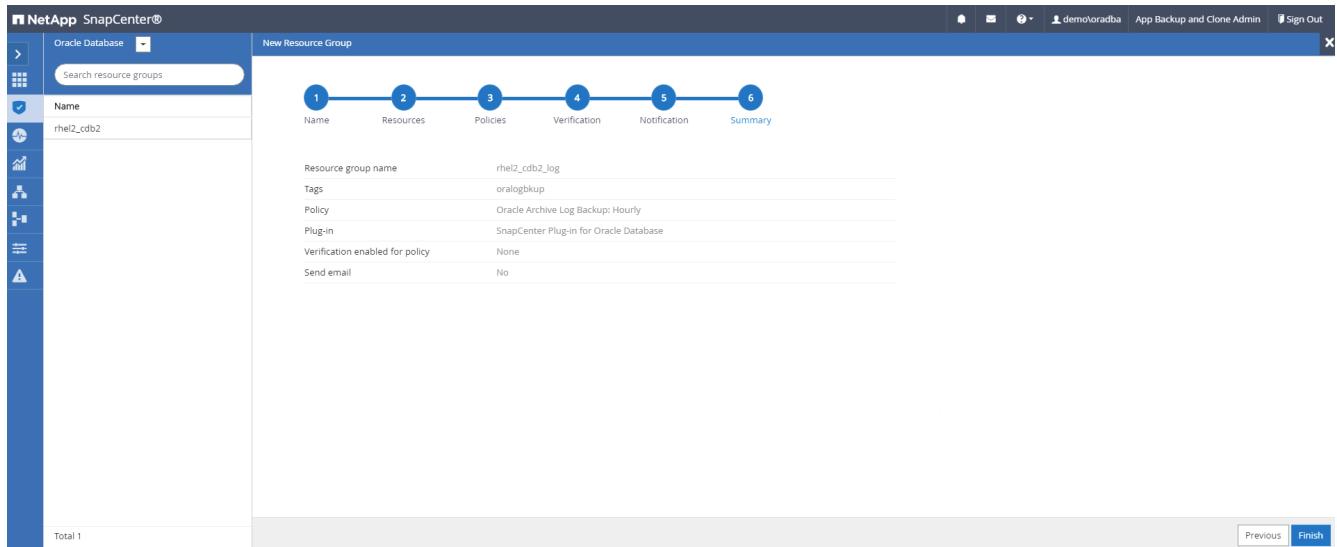
Total 0

Previous Next

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

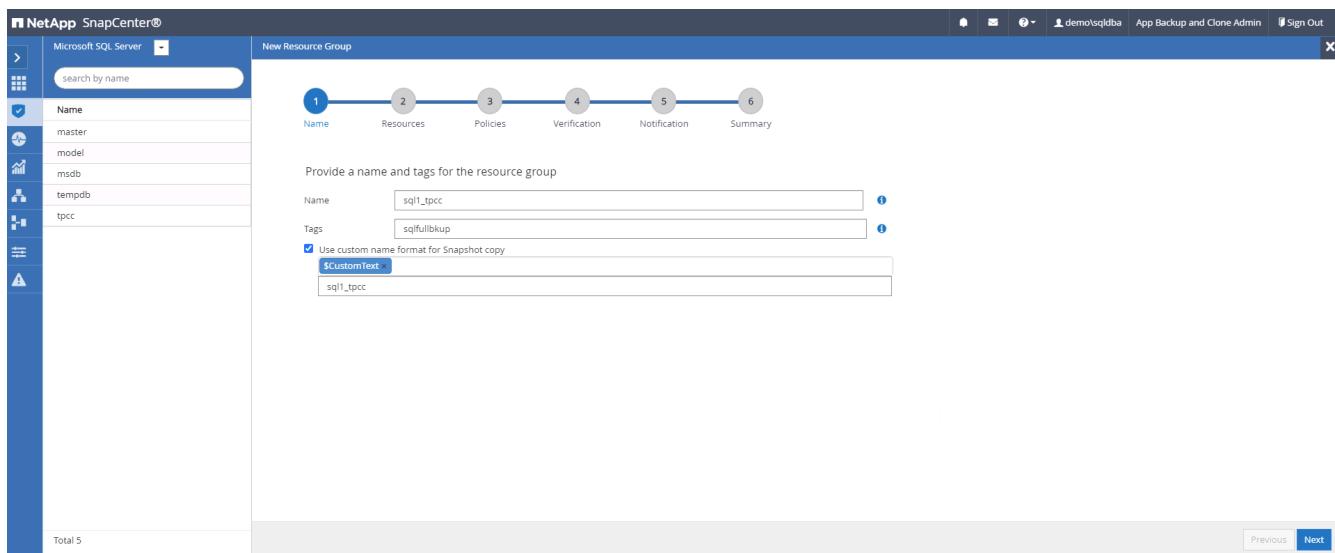


8. Summary.

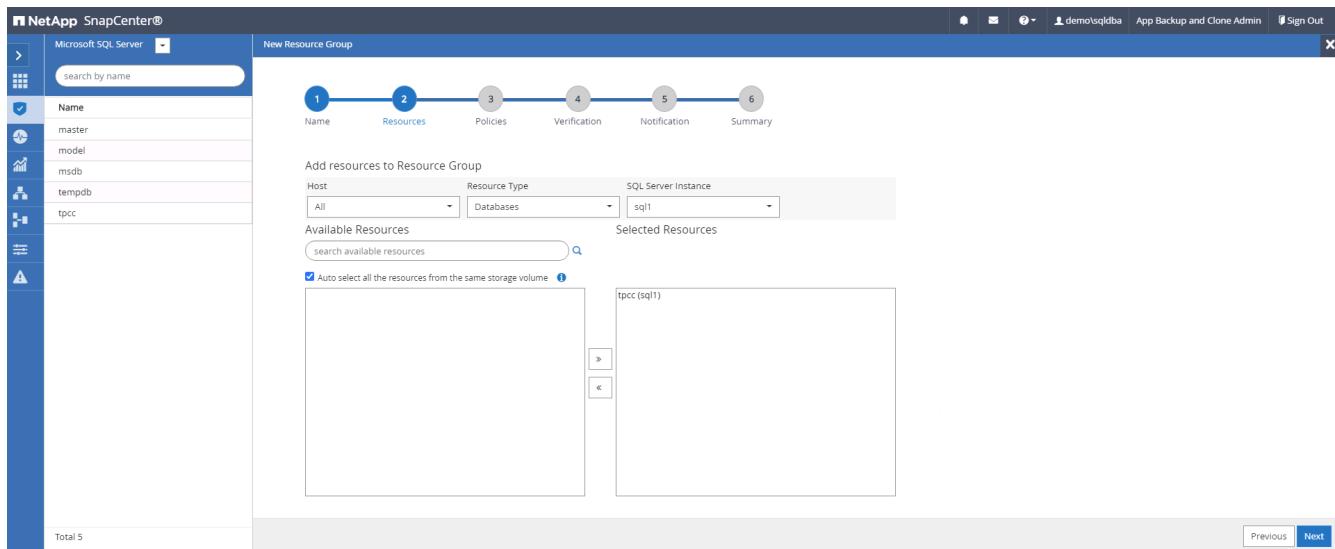


Create a resource group for full backup of SQL Server

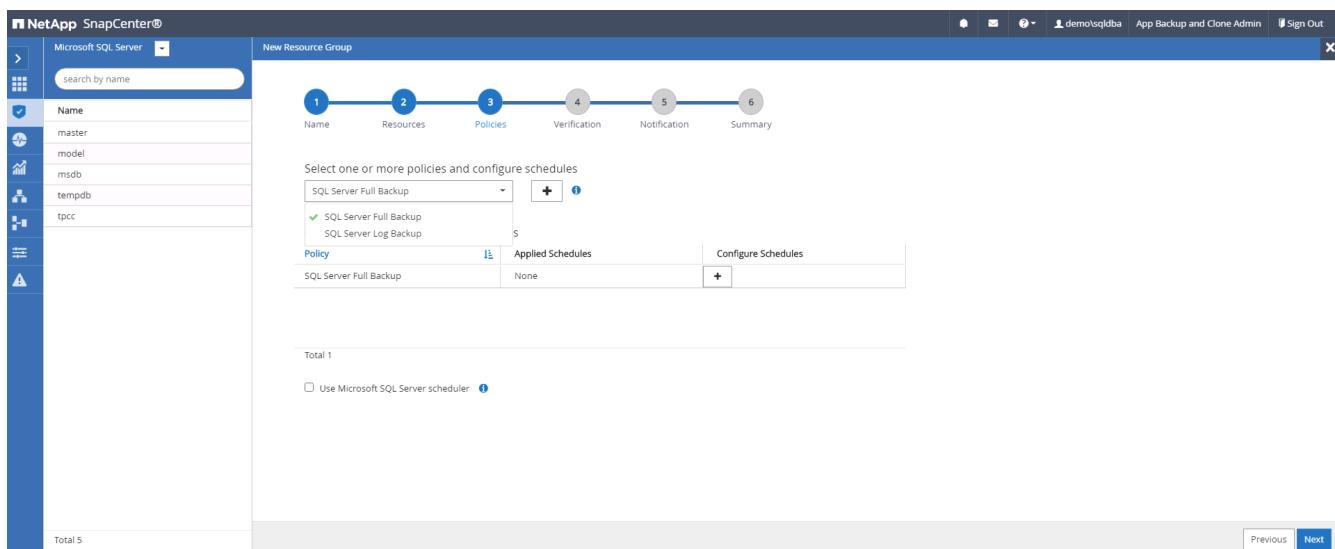
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either a Database or Resource Group to launch the resource group creation workflow. Provide a name and tags for the resource group. You can define a naming format for the Snapshot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



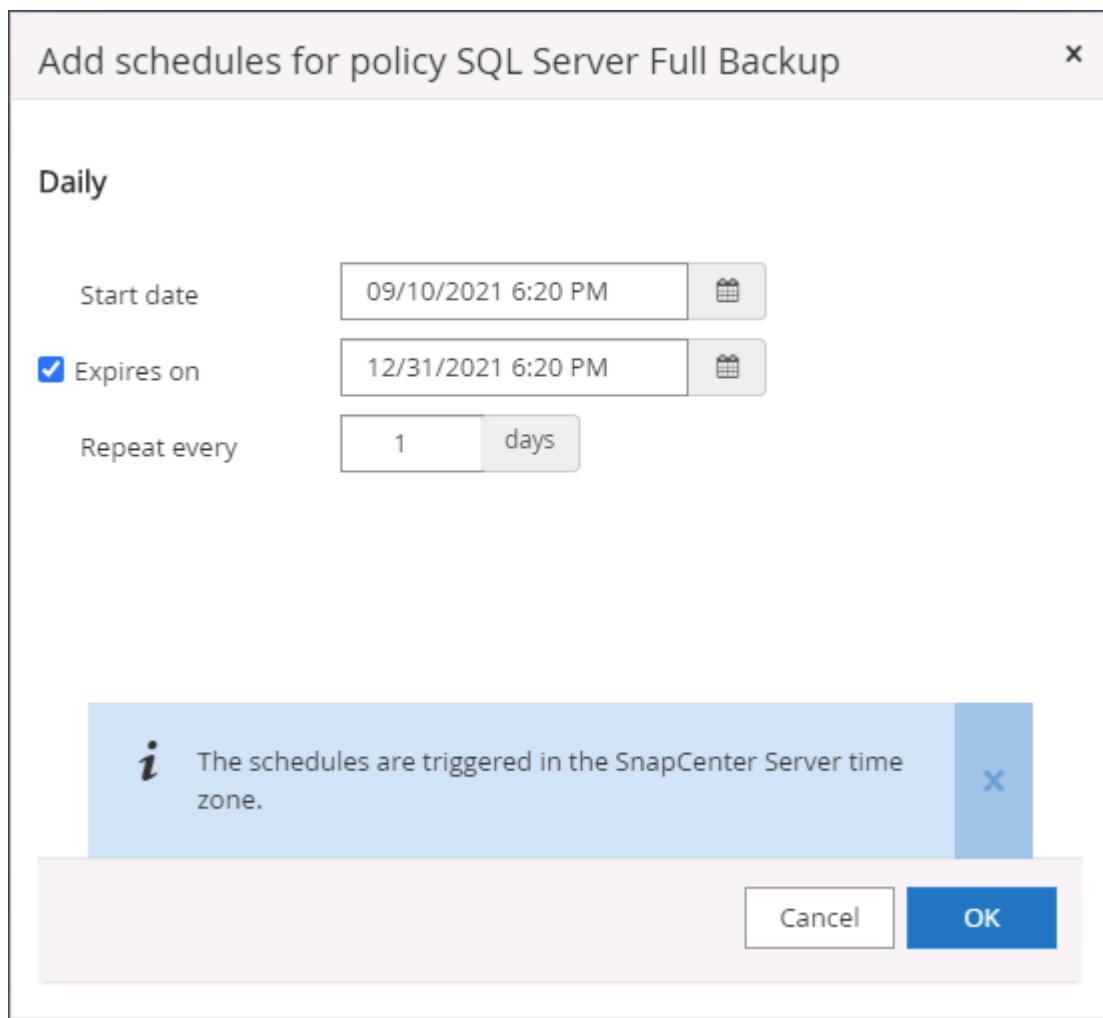
2. Select the database resources to be backed up.



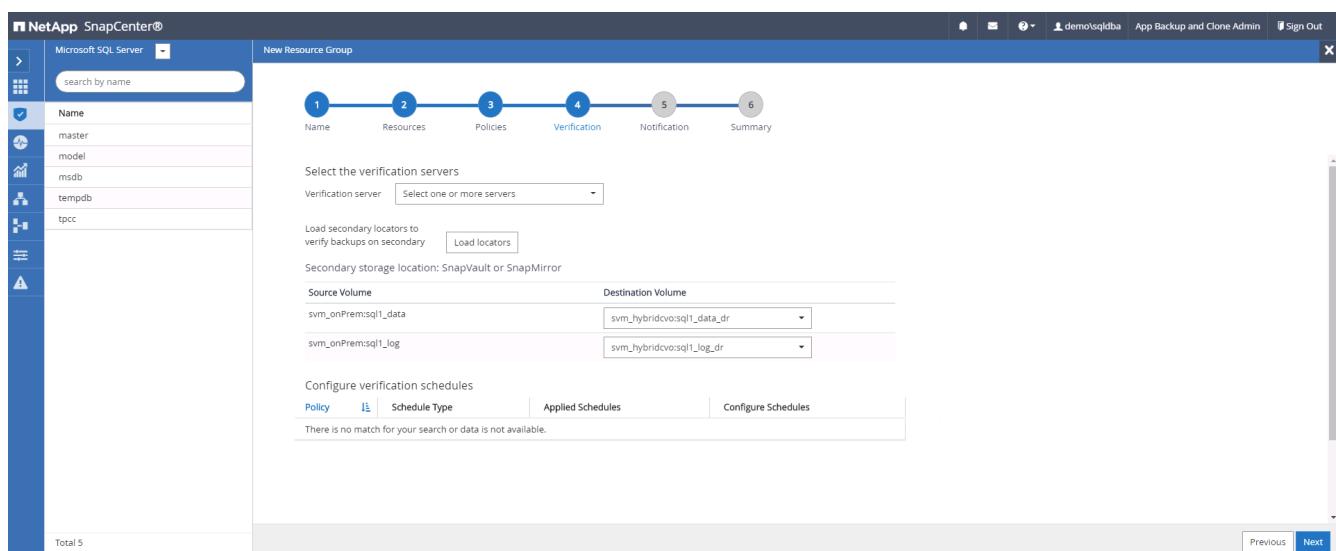
3. Select a full SQL backup policy created in section 7.



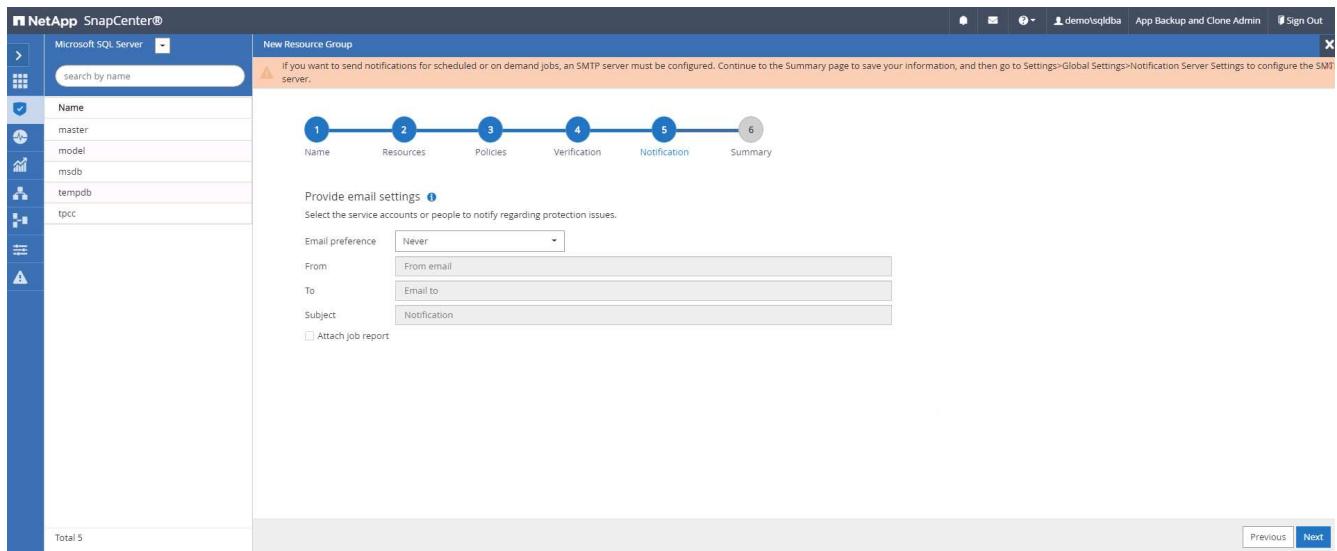
- Add exact timing for backups as well as the frequency.



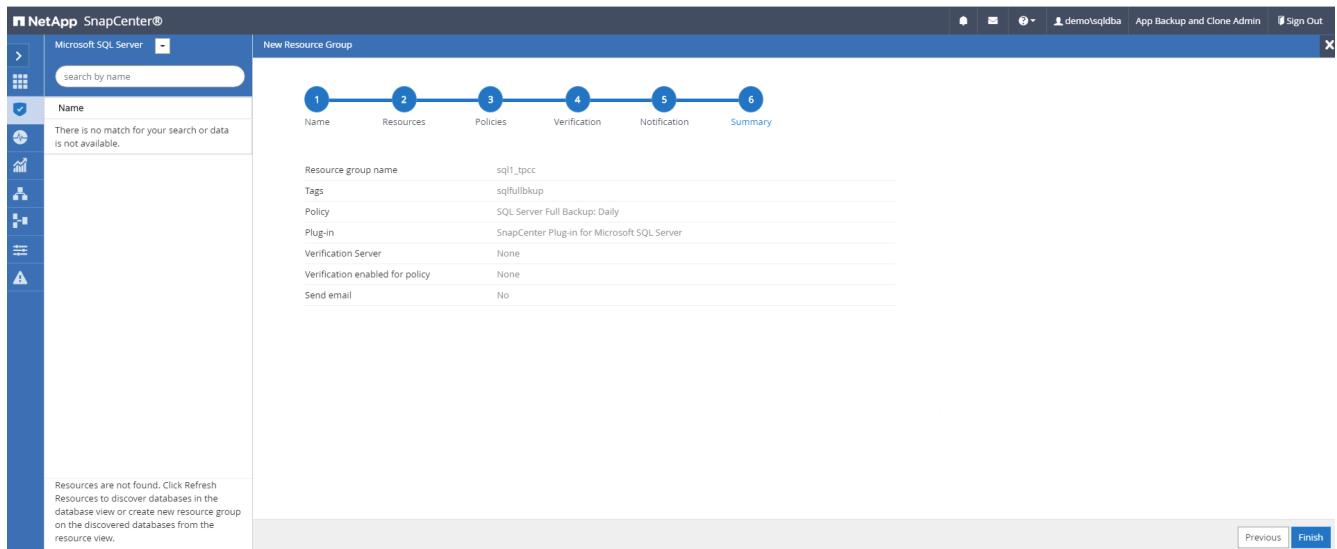
- Choose the verification server for the backup on secondary if backup verification is to be performed. Click Load Locator to populate the secondary storage location.



- Configure the SMTP server for email notification if desired.

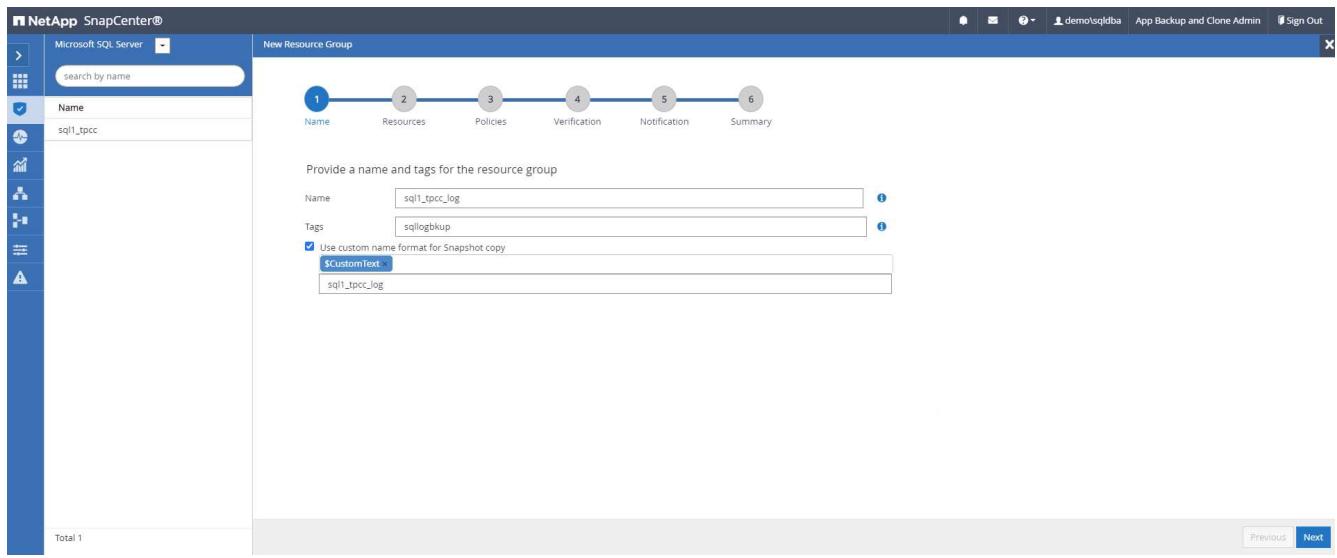


7. Summary.

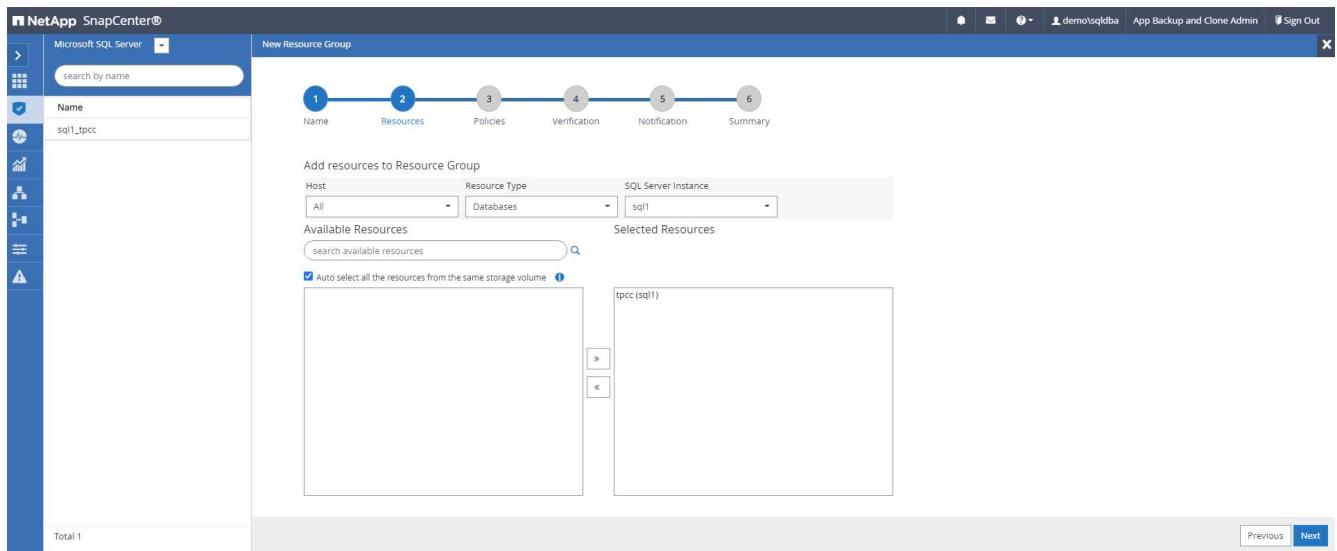


Create a resource group for log backup of SQL Server

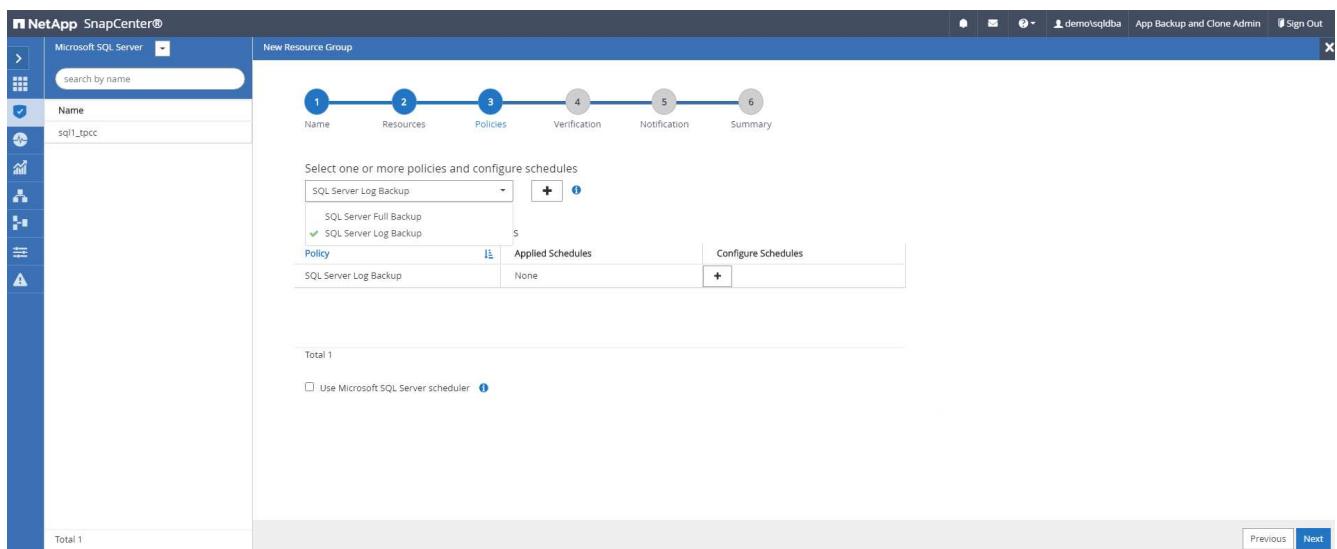
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either a Database or Resource Group to launch the resource group creation workflow. Provide the name and tags for the resource group. You can define a naming format for the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



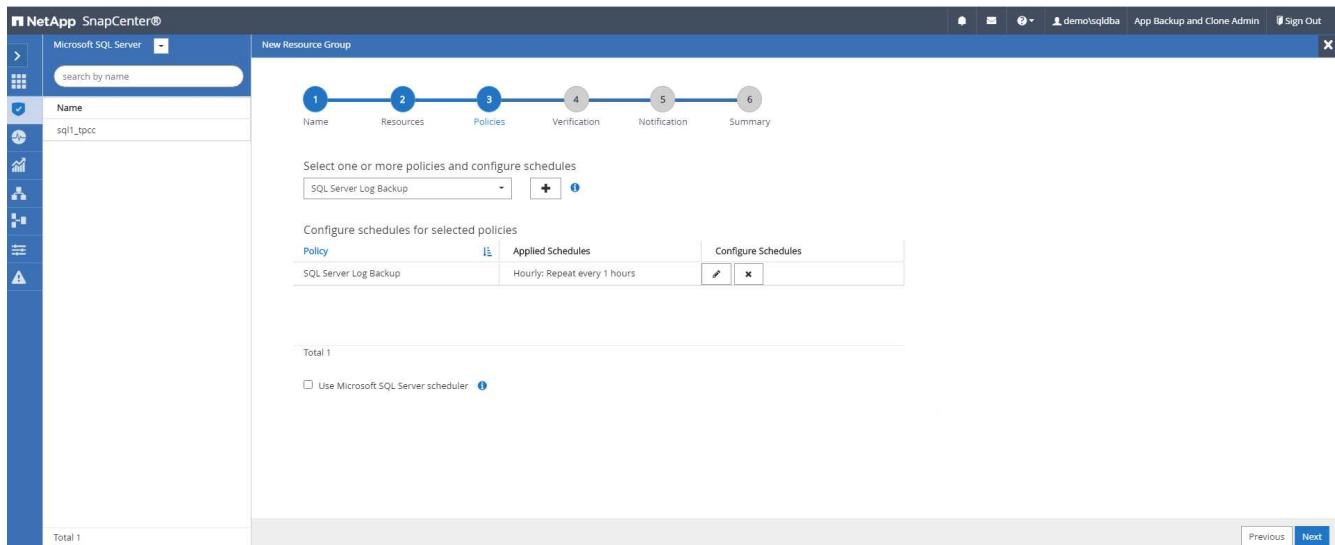
2. Select the database resources to be backed up.



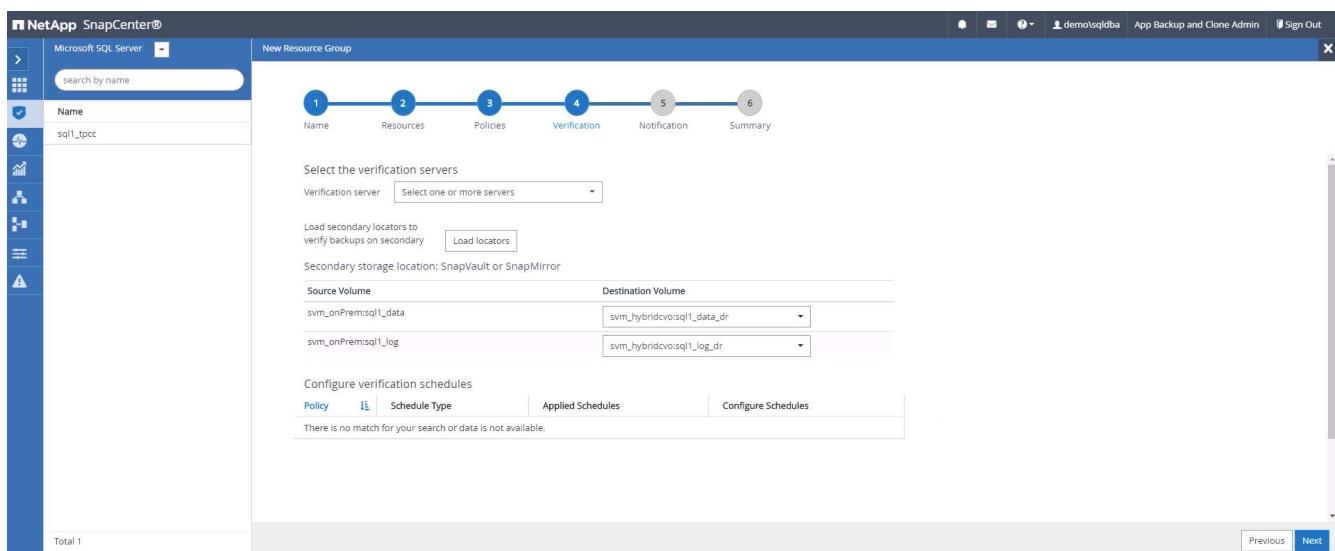
3. Select a SQL log backup policy created in section 7.



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_log' 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.



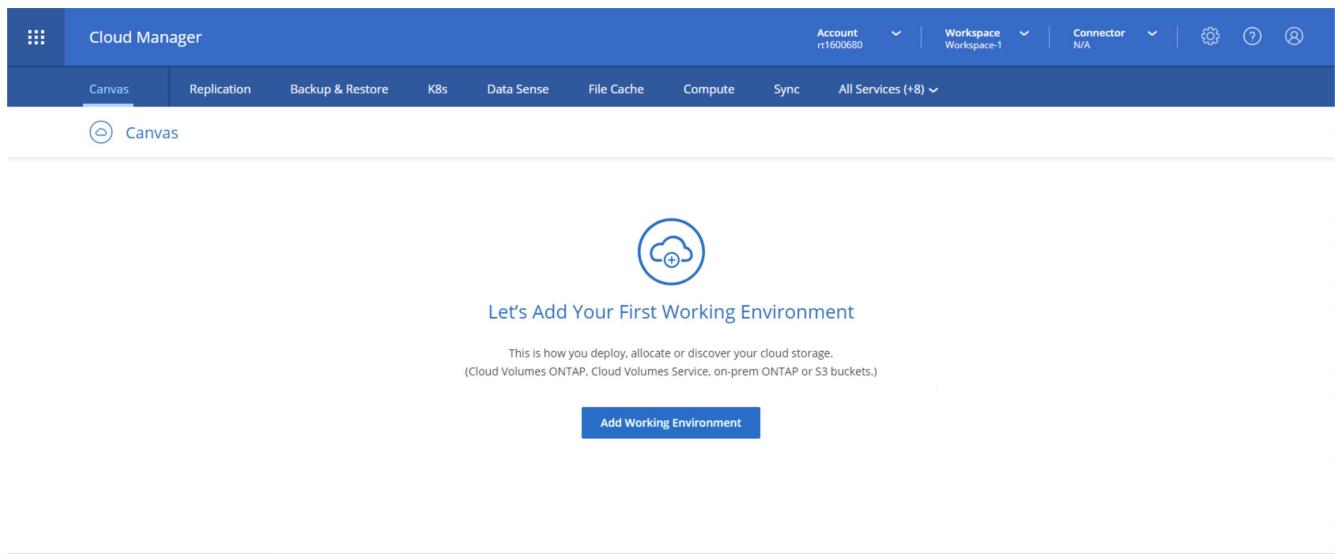
[Continue to Cloud Manager](#)

Log In to NetApp Cloud Central

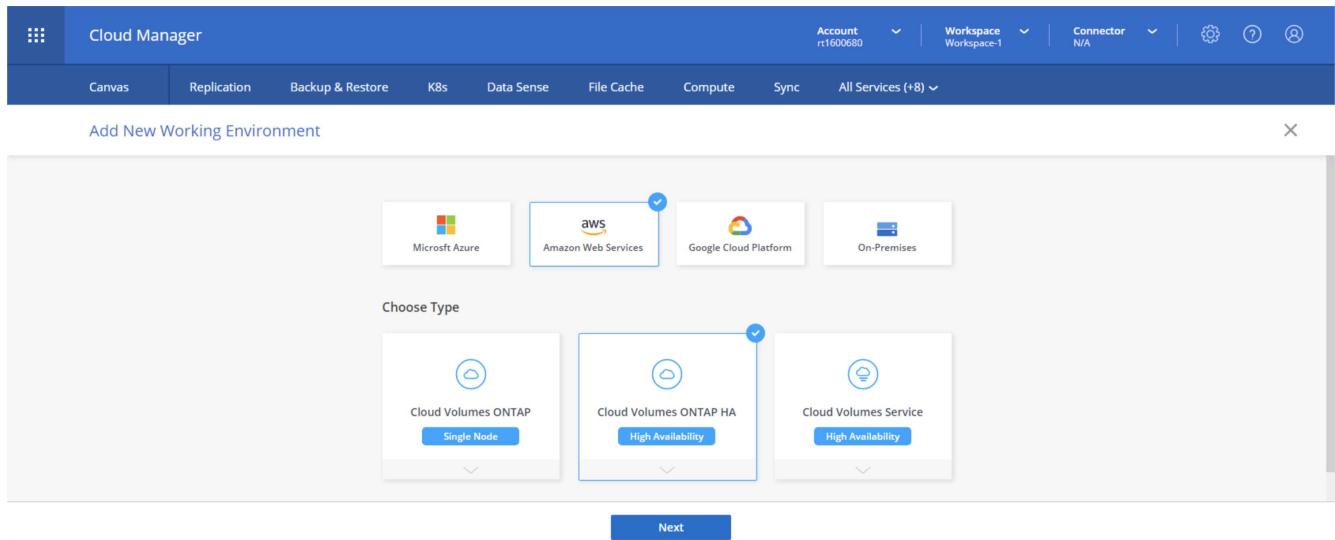
Don't have an account yet? [Sign Up](#)

[Forgot your password?](#)

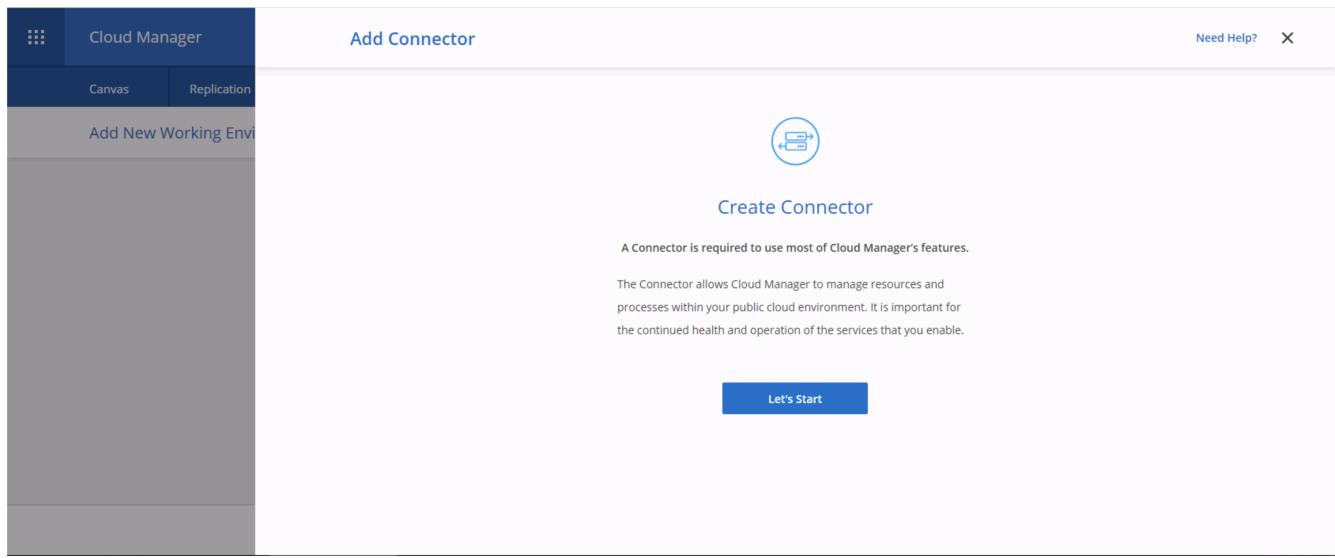
2. After you log in, you should be taken to the Canvas.



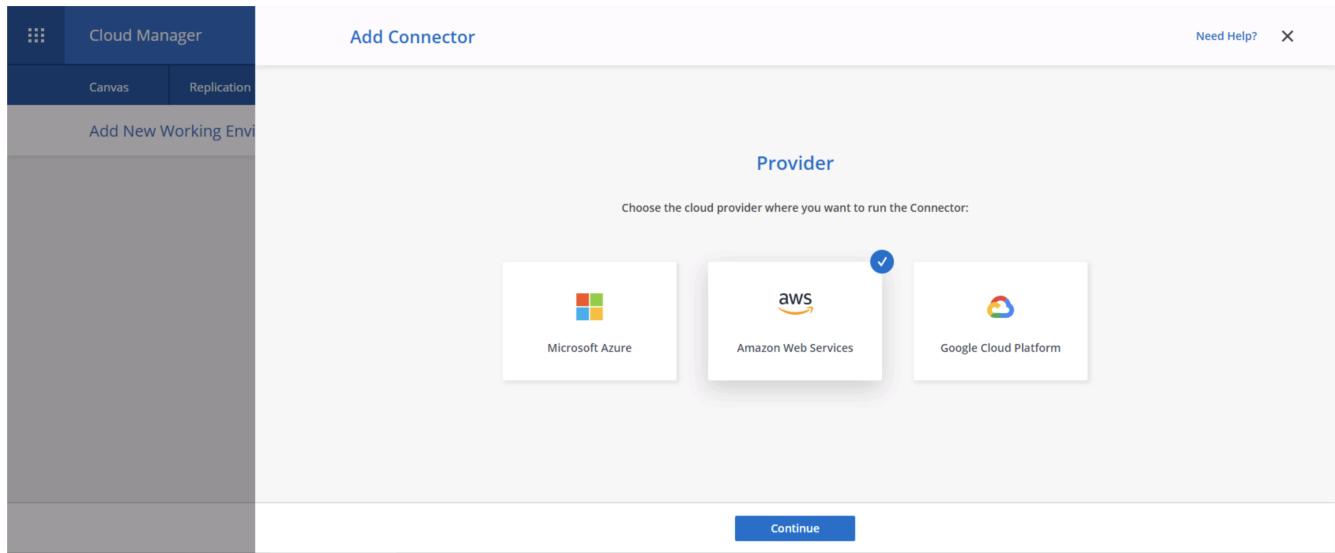
3. Click "Add Working Environment" and choose Cloud Volumes ONTAP in AWS. Here, you also choose whether you want to deploy a single node system or a high availability pair. I have chosen to deploy a high availability pair.



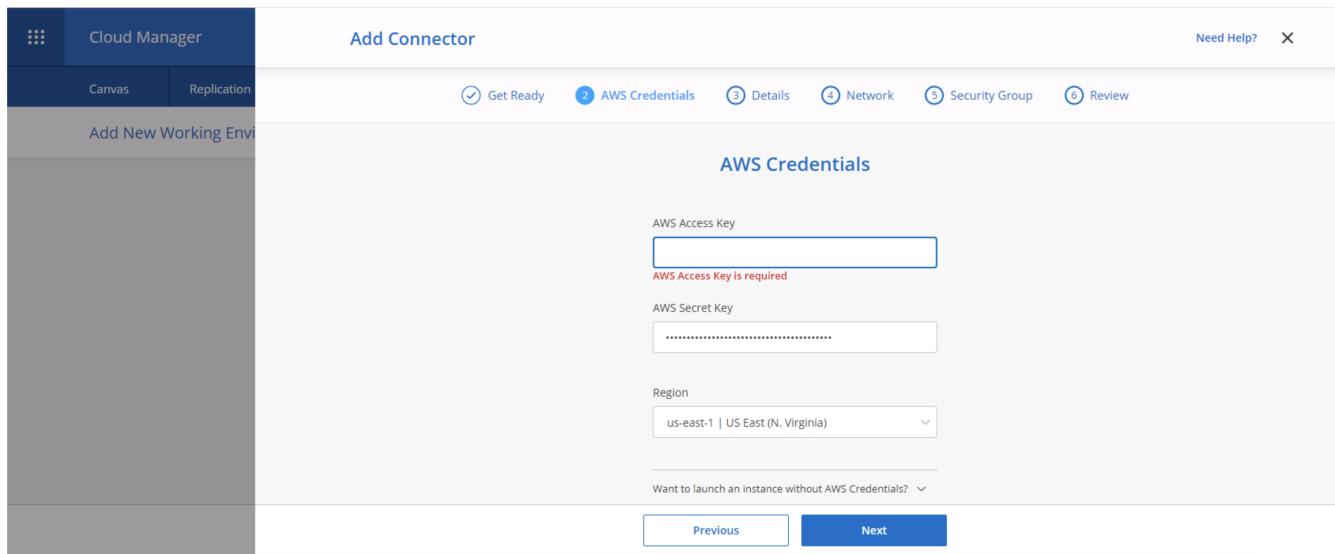
4. If no connector has been created, a pop-up appears asking you to create a connector.



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](#).



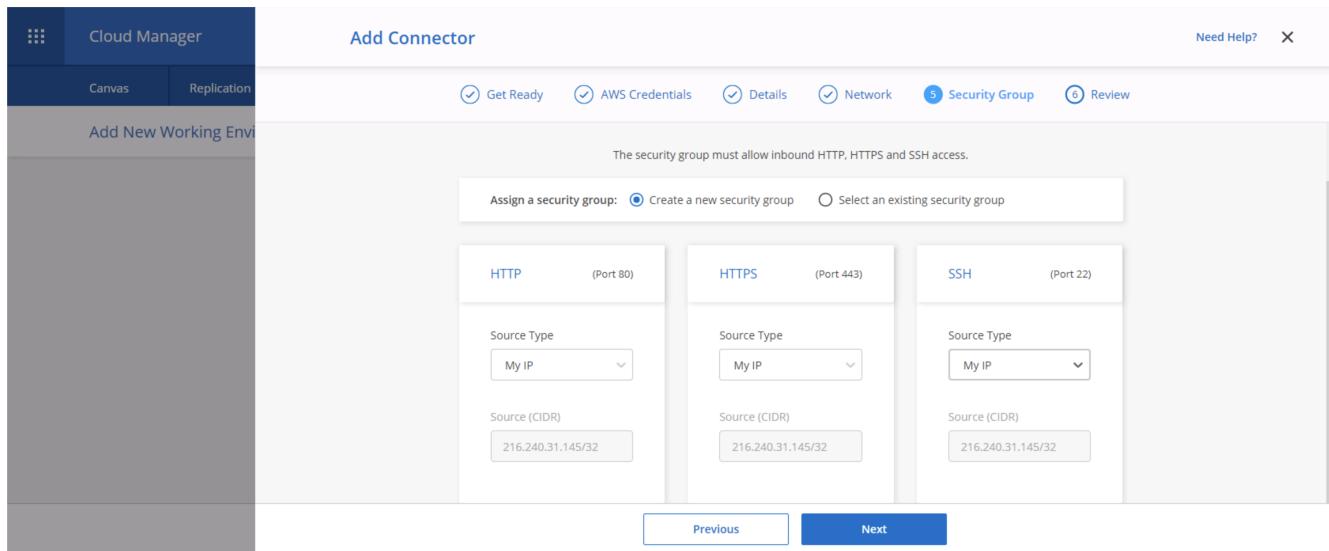
7. Give the connector a name and either use a predefined role as described on the [NetApp policies page](#) or ask Cloud Manager to create the role for you.

The screenshot shows the 'Add Connector' interface in Cloud Manager. The 'Details' step is active, indicated by a blue circle with the number 3. The 'Connector Instance Name' field contains 'awscloudmanager'. Under 'Connector Role', the 'Create Role' radio button is selected. The 'Role Name' field contains 'Cloud-Manager-Operator-IBNt24'. Below these fields is a link to 'Add Tags to Connector Instance'. At the bottom are 'Previous' and 'Next' buttons.

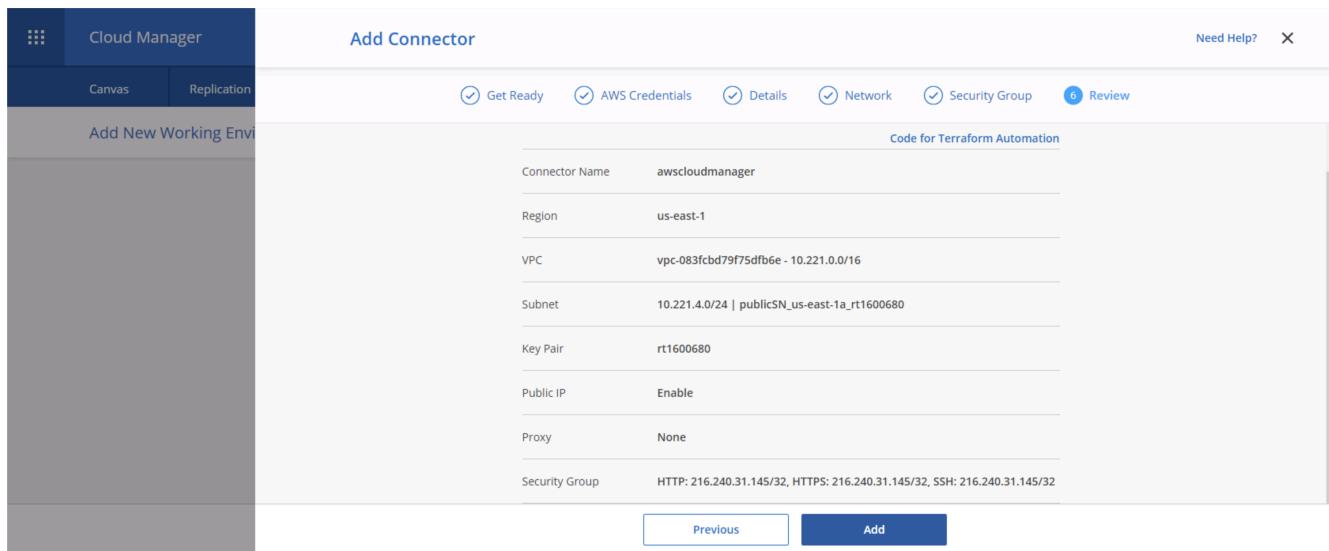
8. Give the networking information needed to deploy the connector. Verify that outbound internet access is enabled by:
- Giving the connector a public IP address
 - Giving the connector a proxy to work through
 - Giving the connector a route to the public internet through an Internet Gateway

The screenshot shows the 'Network' step of the 'Add Connector' process. The 'Network' tab is active, indicated by a blue circle with the number 4. The 'Connectivity' section includes fields for 'VPC' (set to 'vpc-083fcbd79f75dfb6e - 10.221.0.0/16'), 'Subnet' (set to '10.221.4.0/24 | publicSN_us-east-1a_rt1600...'), and 'Key Pair' (set to 'rt1600680'). The 'Proxy Configuration (Optional)' section includes a 'HTTP Proxy' field with the placeholder 'Example: http://172.16.254.1:8080'. Below these are 'Define Credentials for this Proxy' and 'Upload a root certificate' dropdowns. The 'Public IP' section has a 'Enable' dropdown. At the bottom are 'Previous' and 'Next' buttons.

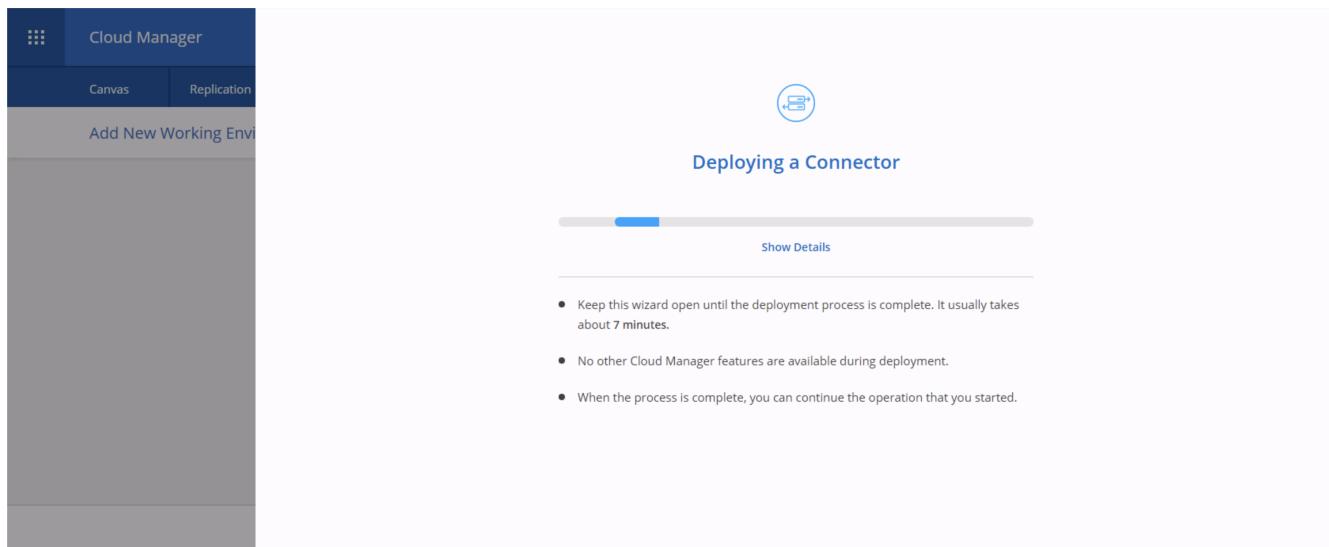
9. Provide communication with the connector via SSH, HTTP, and HTTPS by either providing a security group or creating a new security group. I have enabled access to the connector from my IP address only.



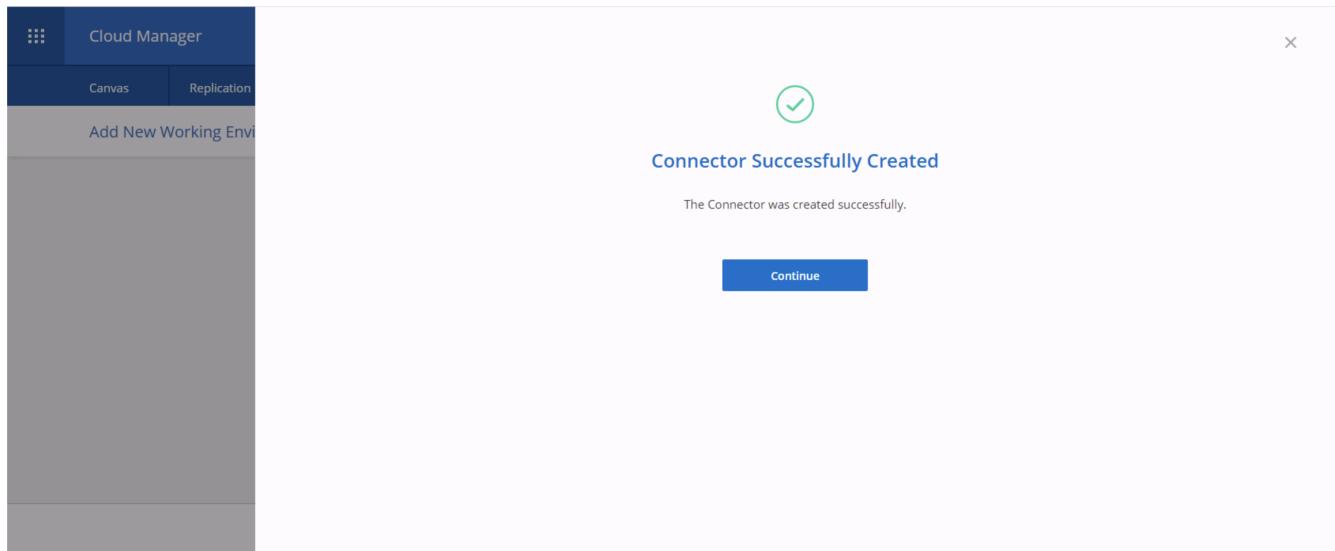
10. Review the information on the summary page and click Add to deploy the connector.



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

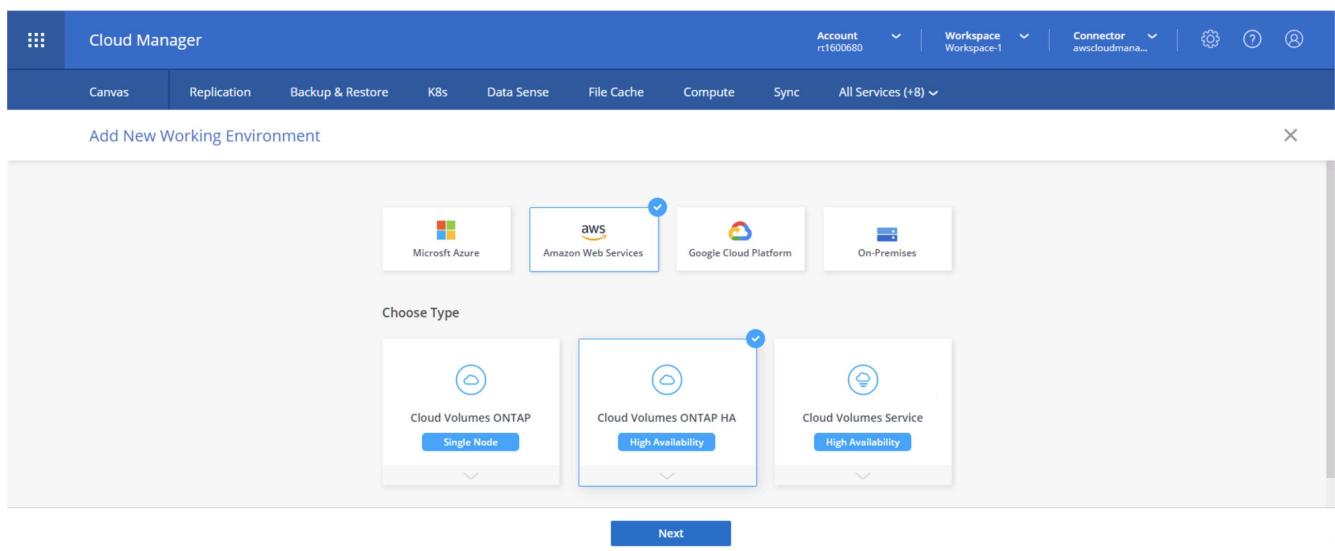


12. When the deployment is complete, a success page appears.



Deploy Cloud Volumes ONTAP

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



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

The screenshot shows the Cloud Manager interface with the title 'Cloud Manager' at the top. The main navigation bar includes 'Canvas', 'Replication', 'Backup & Restore', 'K8s', 'Data Sense', 'File Cache', 'Compute', 'Sync', and 'All Services (+8)'. On the right, account information (Account: rt1600680, Workspace: Workspace-1, Connector: awscloudman...), settings, and help icons are visible. The main content area is titled 'Create a New Working Environment' and 'Details and Credentials'. It shows an 'Instance Profile' section with 'Credential Name' set to '322944748816' and 'Account ID' set to 'Marketplace Subscription'. A button 'Edit Credentials' is present. Below this, there are two columns: 'Details' (Working Environment Name: 'Up to 40 characters') and 'Credentials' (User Name: 'admin', Password: empty, Confirm Password: empty). A 'Continue' button is at the bottom. At the very bottom, a footer note says 'Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC'.

3. Choose Add Subscription.

This screenshot shows the 'Edit Credentials & Add Subscription' step. The main content area is titled 'Edit Credentials & Add Subscription'. It features a 'Associate Subscription to Credentials' section with a dropdown menu showing 'Instance Profile | Account ID: 322944748816'. Below this is a 'Marketplace Subscription' section with a message 'No subscription is associated with this credential'. A 'Add Subscription' button is available. At the bottom are 'Apply' and 'Cancel' buttons. The footer note is '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.

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

Cloud Manager - Deploy & Manage NetApp Cloud Data Services

Sold by: [NetApp, Inc.](#)

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, [▼ Show more](#)

Overview **Pricing** **Usage** **Support** **Reviews**

Product Overview

NetApp Cloud Manager is the management and automation platform used for deploying and operating NetApp's Cloud Data Services including:

- Cloud Volumes ONTAP - File and block storage for enterprise workloads
- Cloud Backup - Incremental block-level Backup & Restore capabilities for protecting and archiving CVO and On-Premises ONTAP data to S3
- Cloud Tiering - Tiering infrequently-used data to object storage for AFF
- Cloud Data Sense - AI-driven data privacy controls and reporting
- Cloud Manager also manages Cloud Volumes Service on AWS

Cloud Manager eases the day-to-day requirements of operating your cloud storage environment including configuring, provisioning, and monitoring each of your active NetApp Cloud Data Services including their virtual and hardware storage nodes. It offers a

Highlights

- 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.

You are extended multiple offers! Select an offer first and review the pricing information and EULA.

Offer name: [NetApp, Inc. for SaaS 2020-07-20- Private Offer - current subscription](#)

You are subscribed to this offer.

By: NetApp, Inc.
Offer ID: [offer-hmolsqhv7ii](#)
This offer is going to expire on [August 1, 2022 UTC](#)

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

Having issues signing up for your product?
If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

You Have Subscribed to a Private Offer

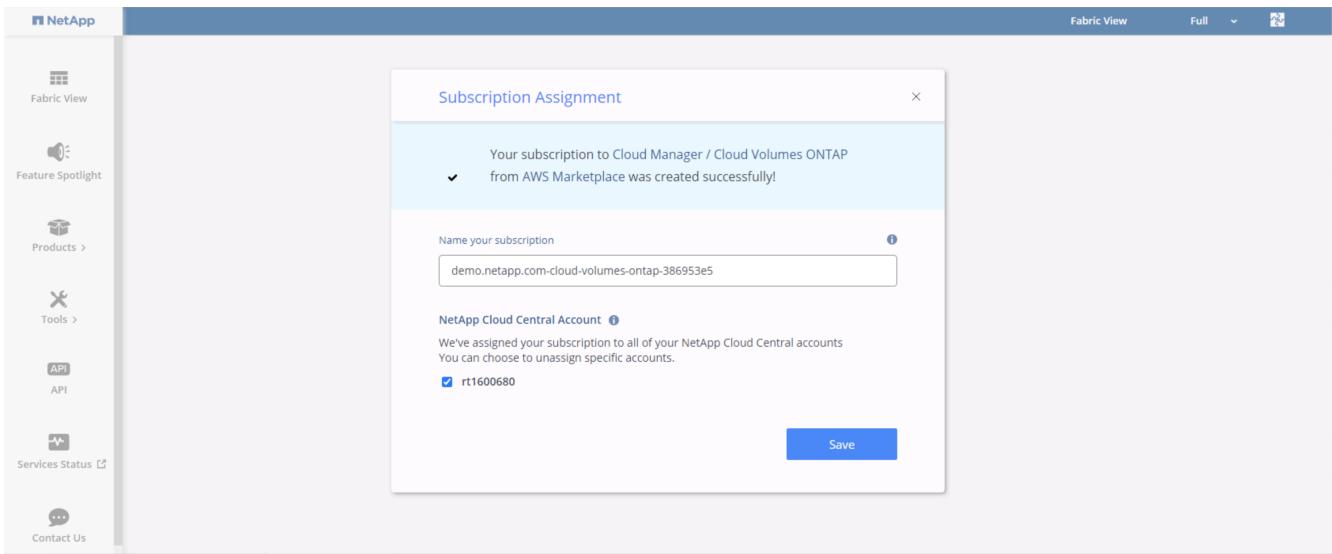
You have subscribed to this private offer on [July 21, 2020 UTC](#). The private offer will **expire on August 1, 2022 UTC**. Your use of this product after the expiration date of your private offer will be billed at the then current public pricing, which can be found on this product's detail page.

To avoid being charged for use beyond the expiration date of this offer, you can cancel your subscription to this product by [August 1, 2022 UTC](#). Please contact the vendor directly with any questions regarding this offer.

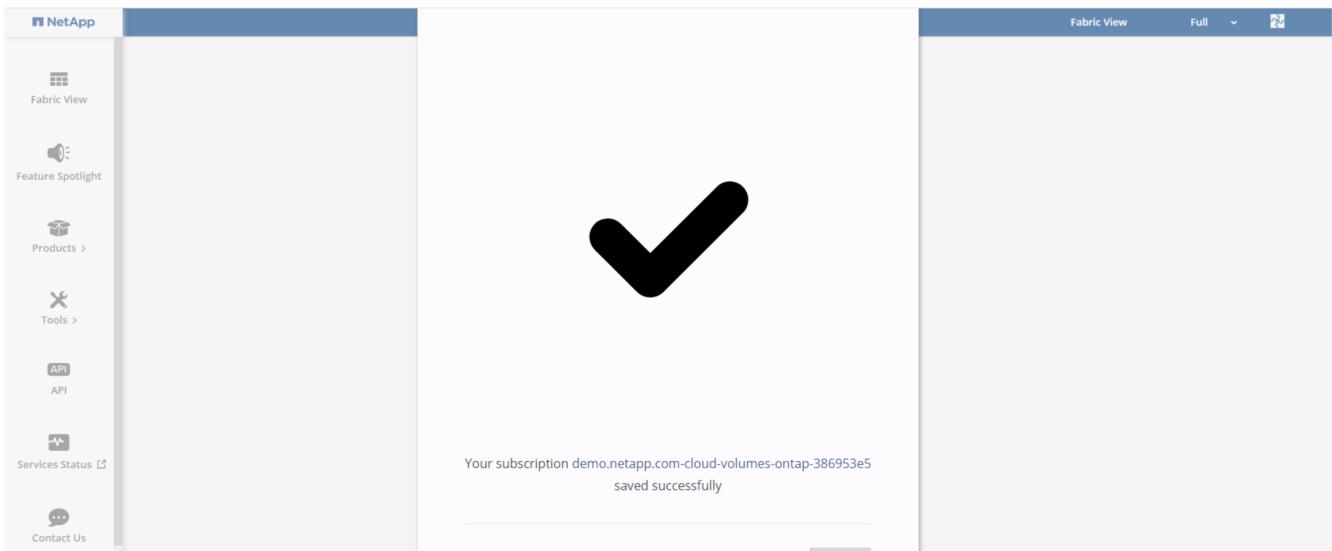
Subscribe

By subscribing to this software, you agree to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You also agree and acknowledge that AWS may share information about this transaction.

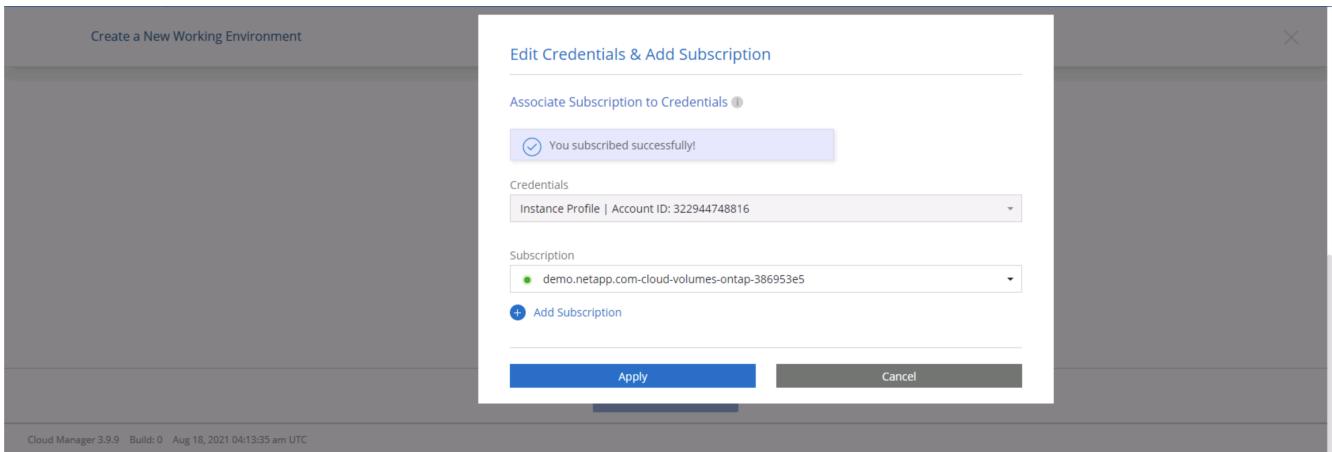
7. You are redirected to Cloud Central where you must name your subscription and assign it to your Cloud Central account.



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



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



- Enter the working environment details such as:

- a. Cluster name

b. Cluster password

c. AWS tags (Optional)

The screenshot shows the 'Cloud Manager' interface with the title 'Create a New Working Environment'. The 'Details and Credentials' tab is selected. On the left, there's a 'Previous Step' button and an 'Instance Profile' section with fields for '322944748816' and 'demo.netapp.com-cloud-vol...'. On the right, there's a 'Credential Name' field with 'Account ID' and 'Marketplace Subscription' dropdowns, and a 'Edit Credentials' button. Below these are 'Details' and 'Credentials' sections. The 'Details' section contains a 'Working Environment Name (Cluster Name)' input field with 'hybridawsco'. The 'Credentials' section has fields for 'User Name' (admin), 'Password' (*****), and 'Confirm Password' (*****). A 'Continue' button is at the bottom.

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

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

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

The screenshot shows the Cloud Manager interface with the title "Cloud Manager" at the top. The top navigation bar includes "Account: rt1600680", "Workspace: Workspace-1", "Connector: awscloudman...", and icons for gear, help, and refresh. Below the top bar, there are tabs for "Canvas", "Replication", "Backup & Restore", "K8s", "Data Sense", "File Cache", "Compute", "Sync", and "All Services (+8)". A search bar at the top right says "Create a New Working Environment". The main content area is titled "HA Deployment Models" and contains two sections: "Multiple Availability Zones" and "Single Availability Zone". Each section has three bullet points with icons. At the bottom of each section is a "Extended Info" link.

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. The top navigation bar includes "Account: rt1600680", "Workspace: Workspace-1", "Connector: awscloudman...", and icons for gear, help, and refresh. Below the top bar, there are tabs for "Canvas", "Replication", "Backup & Restore", "K8s", "Data Sense", "File Cache", "Compute", "Sync", and "All Services (+8)". A search bar at the top right says "Create a New Working Environment". The main content area is titled "Region & VPC" and contains fields for "AWS Region" (set to "US East | N. Virginia"), "VPC" (set to "vpc-083fcbd79f75dfb6e - 10.221.0.0/16"), and "Security group" (set to "Use a generated security group"). Below these fields are three columns for "Node 1", "Node 2", and "Mediator", each with "Availability Zone" and "Subnet" dropdowns. The "Subnet" dropdown for the "Mediator" column is highlighted. A "Continue" button is at the bottom.

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. The top navigation bar includes "Account: rt1600680", "Workspace: Workspace-1", "Connector: awscloudman...", and icons for gear, help, and refresh. Below the top bar, there are tabs for "Canvas", "Replication", "Backup & Restore", "K8s", "Data Sense", "File Cache", "Compute", "Sync", and "All Services (+8)". A search bar at the top right says "Create a New Working Environment". The main content area is titled "Connectivity & SSH Authentication" and contains two sections: "Nodes" and "Mediator". The "Nodes" section has a dropdown for "SSH Authentication Method" set to "Password". The "Mediator" section has dropdowns for "Security Group" (set to "Use a generated security group"), "Key Pair Name" (set to "rt1600680"), and "Internet Connection Method" (set to "Public IP address"). A "Continue" button is at the bottom.

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' tab selected. It displays fields for specifying floating IP addresses for cluster management, NFS/CIFS data, SVM management, and optional floating IP addresses. The 'Continue' button is visible at the bottom.

Floating IP address for cluster management: 10.222.0.200

Floating IP address 1 for NFS and CIFS data: 10.222.0.201

Floating IP address 2 for NFS and CIFS data: 10.222.0.202

Floating IP address for SVM management (Optional): Enter Floating IP Address

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' tab selected. It displays a table of route tables and their properties. The 'Continue' button is visible at the bottom.

Name	Main	ID	Associate with Subnet	Tags
private_rt_rt1600680	No	rtb-08b4cb88f65c826a5	3 Subnets	1 Tags
public_rt_rt1600680	Yes	rtb-0e46720d0da10c593	1 Subnets	1 Tags

2 Route Tables | The main route table is the default for the VPC

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. In the center, there's a diagram illustrating a hybrid environment setup. It shows two clouds: one labeled "hybridawsenvo Cloud Volumes ONTAP" with "HA" and "Initializing" status, and another labeled "Amazon S3" with "1 Buckets" and "1 Region". Below the diagram are "Add Working Environment" and "Working environments" sections. The "Working environments" section lists "1 Cloud Volumes ONTAP (High-Availability)" and "0 B Allocated Capacity" under a cloud icon, and "1 Amazon S3" with "0 Buckets" under a bucket icon. A zoom-in and zoom-out button is at the bottom 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 links to Canvas, Digital Wallet, and Timeline. The Services section includes links to Replication, Backup & Restore, K8s, Data Sense, Compliance, Tiering, Monitoring, File Cache, Compute, Sync, SnapCenter, and Active IQ. A link to the Timeline is also present at the bottom left.

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: Time (1), Service, Action, Agent (1), Resource, User, Status, and a Reset button. Below the filters is a table with columns: Time, Action, Service, Agent, Resource, User, and Status. The table contains three rows of log entries:

- 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 - Cloud Manager - awscloudma... - hybridawscvo - Full Name - Success

11. 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 is a 'Working environments' section with a 'Add Working Environment' button. On the right, there is a 'Working environments' panel showing two environments:

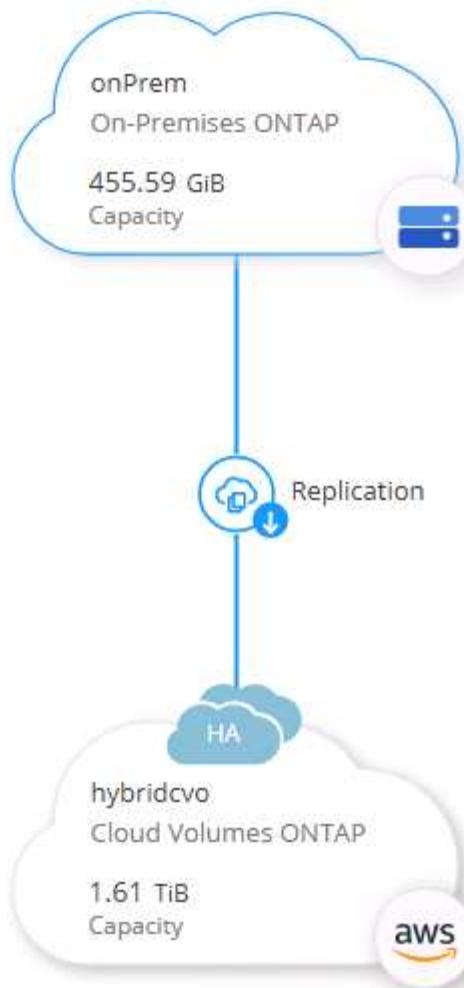
- Cloud Volumes ONTAP (High-Availability): 1 GiB Allocated Capacity
- Amazon S3: 2 Buckets, 1 Region

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](#).

1. 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.



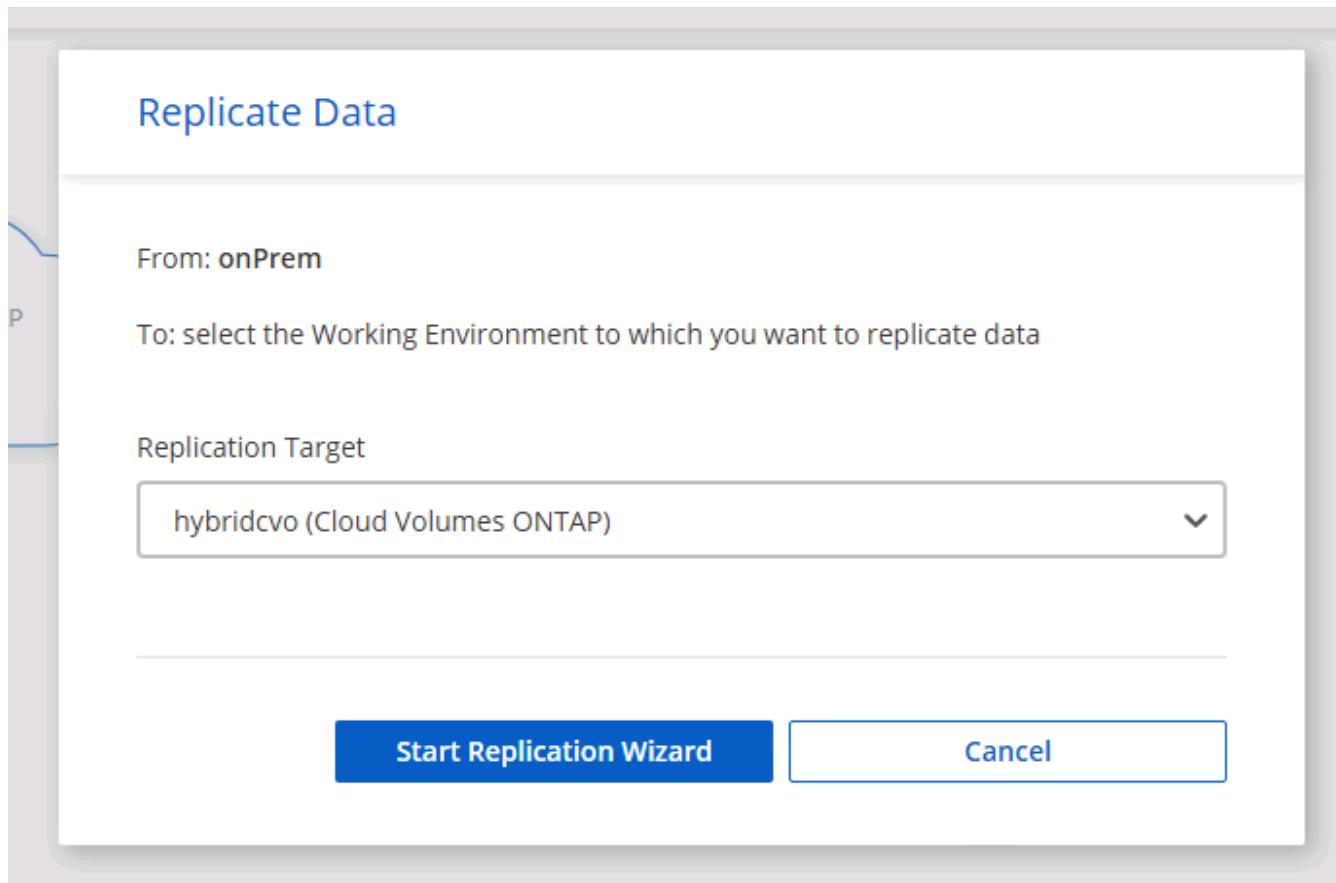
Or Options.

The screenshot shows the 'onPrem' cluster configuration in the NetApp ONTAP interface. At the top, there is 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', the text 'On-PremisesONTAP' is displayed. In the 'SERVICES' section, there is another circular icon with a cloud and server, followed by the text 'Replication' and a green square indicating 'On'. To the right, it shows '1 Replication Target' with a blue circular icon containing three dots. A horizontal line separates this from the bottom section.

Replicate.

This screenshot is similar to the one above, showing the 'onPrem' cluster configuration. It includes the cluster icon, 'onPrem' name, and 'On' status. The 'DETAILS' section shows 'On-PremisesONTAP'. The 'SERVICES' section shows 'Replication' (On) with 1 Replication Target. A dropdown menu is open over the 'Replication Target' entry, containing two items: 'View Replications' and 'Replicate'. The 'Replicate' item is highlighted with a blue arrow icon.

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.

Source Volume Selection			
rhel2_u03 INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW CAPACITY 100 GB Allocated 7.29 GB Disk Used	rhel2_u03 INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW CAPACITY 100 GB Allocated 35.83 MB Disk Used	sql1_data INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW CAPACITY 53.37 GB Allocated 45.09 GB Disk Used	
sql1_log INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW CAPACITY 21.35 GB Allocated 18.16 GB Disk Used	sql1_snapctr INFO Storage VM Name: svm_onPrem Tiering Policy: None Volume Type: RW CAPACITY 24.87 GB Allocated 21.23 GB Disk Used		

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

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

[↑ Previous Step](#)

Destination Disk Type



S3 Tiering

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

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

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

Destination Volume Name

Destination Volume Name

sql1_data_dr

Destination Aggregate

Automatically select the best aggregate ▾

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

Max Transfer Rate

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

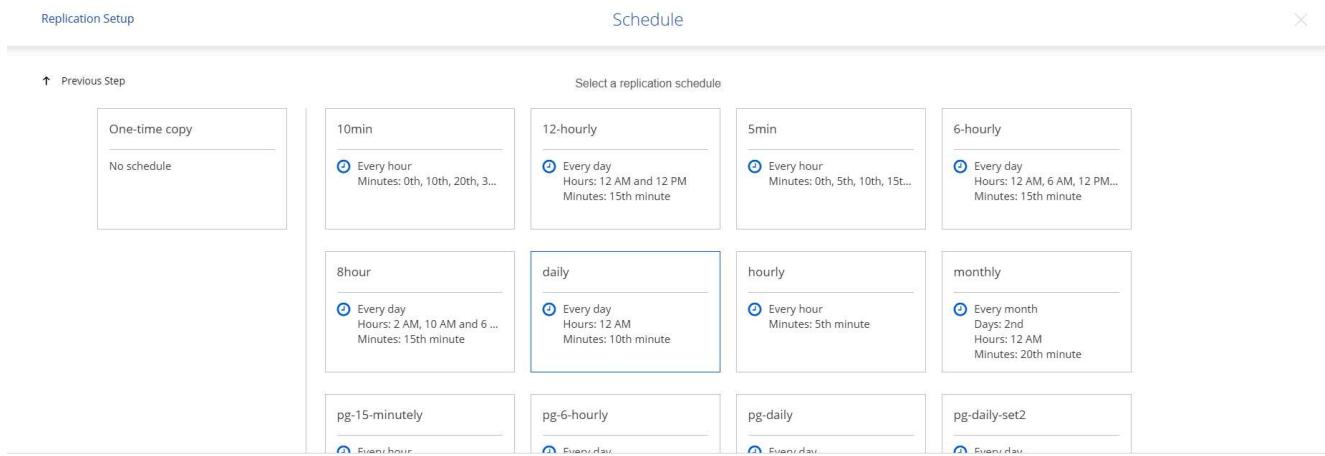
- Limited to: MB/s
- Unlimited (recommended for DR only machines)

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

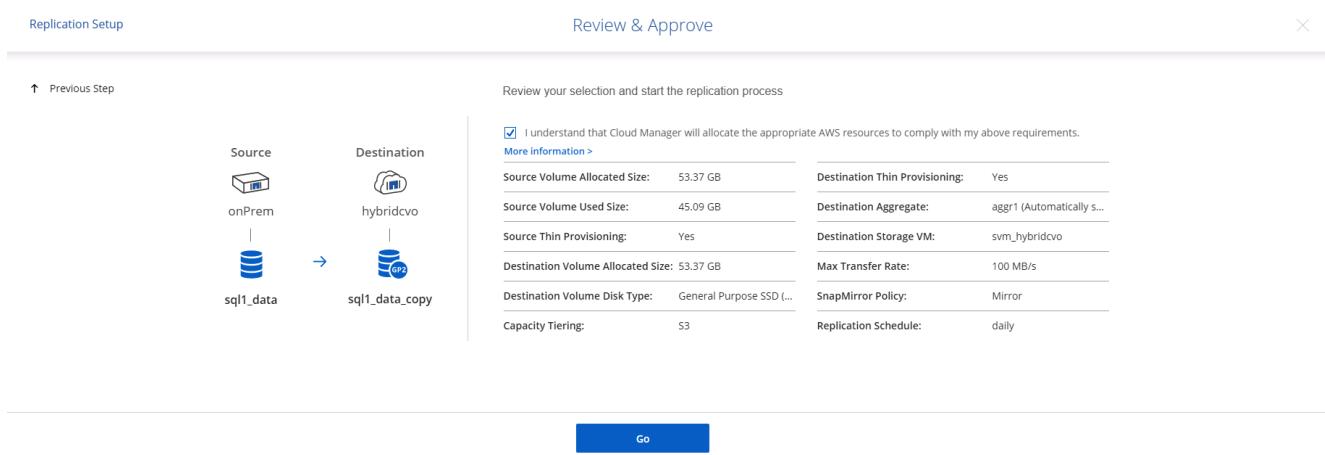
Replication Policy

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

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



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



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

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

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

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	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	False	Not Cataloged	5969474

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

NetApp SnapCenter®

Oracle Database

cdb2 Topology

Manage Copies

Local copies: 184 Backups, 0 Clones

Mirror copies: 184 Backups, 1 Clone

Secondary Mirror Backup(s)

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

Summary Card

- 368 Backups
- 16 Data Backups
- 352 Log Backups
- 1 Clone



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.

- 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

- 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

Datafile locations

/u02_cdb2test

Control files

/u02_cdb2test/cdb2test/control/control01.ctl
/u02_cdb2test/cdb2test/control/control02.ctl

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', and the 'Oracle OS User' and 'Oracle OS Group' are both set to 'oracle'. 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

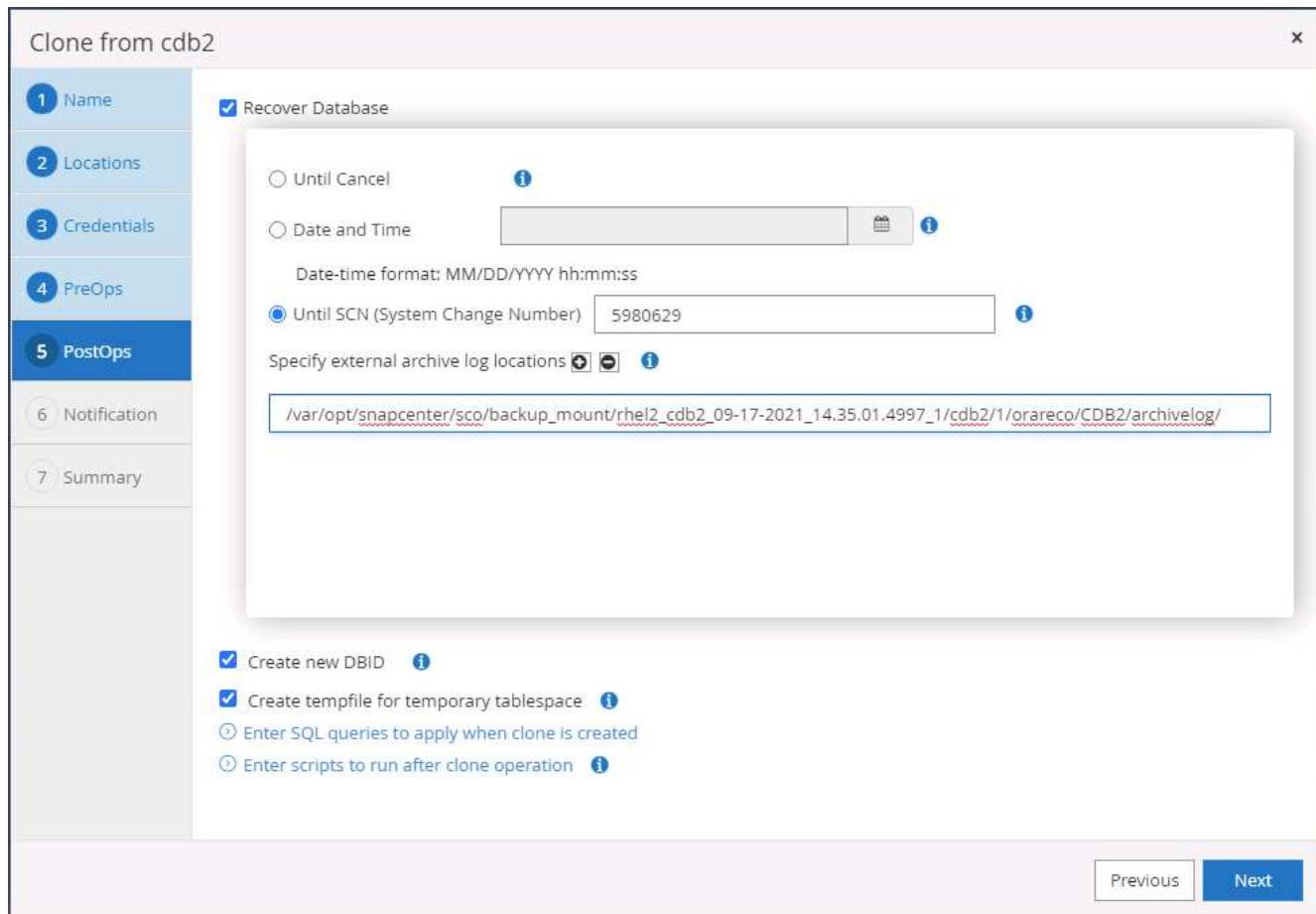
Database Parameter settings

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 X

Provide email settings i

1 Name	Email preference <input type="text" value="Never"/>
2 Locations	From <input type="text" value="From email"/>
3 Credentials	To <input type="text" value="Email to"/>
4 PreOps	Subject <input type="text" value="Notification"/>
5 PostOps	<input type="checkbox"/> Attach job report
6 Notification	
7 Summary	

⚠ 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

12. Clone summary.

Clone from cdb2

1 Name	Summary
2 Locations	Clone from backup rhel2_cdb2_09-17-2021_14.35.01.4997_0
3 Credentials	Clone SID cdb2test
4 PreOps	Clone server ora-standby.demo.netapp.com
5 PostOps	Exclude PDBs none
6 Notification	Oracle home /u01/app/oracle/product/19800/cdb2
7 Summary	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

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

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 Sever 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	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

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.

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
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

Clone Options

Clone settings

- Clone server: Choose
- Clone instance: Nothing selected
- Clone name: tpcc

Choose mount option

- Auto assign mount point
- Auto assign volume mount point under path

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

Next

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	i
Clone instance	sql-standby	i
Clone name	tpcc_clone	

Choose mount option

Auto assign mount point i

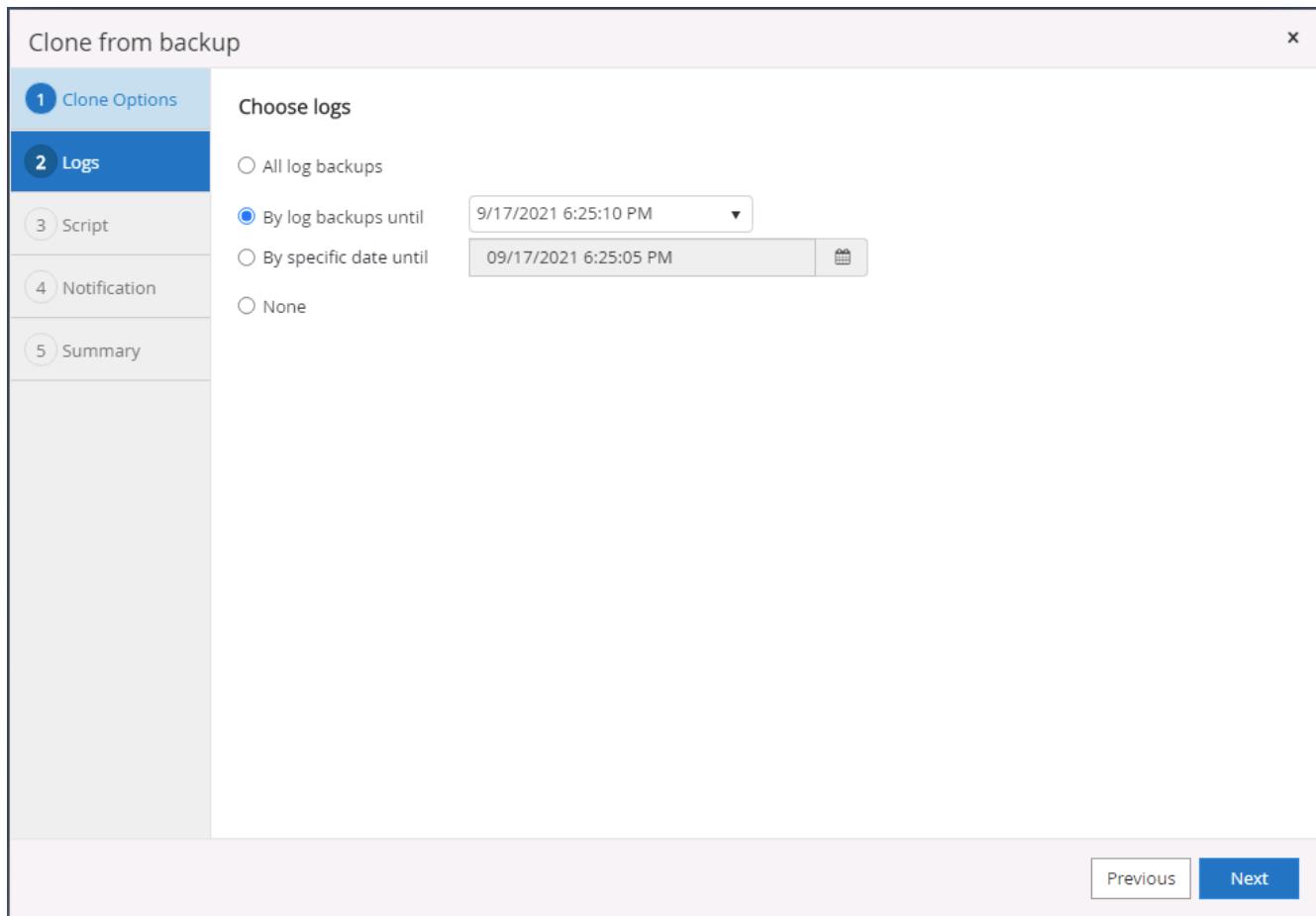
Auto assign volume mount point under path full file path i

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 dialog. The 'Script' tab is selected. It includes fields for specifying optional scripts to run before and after the clone operation, including Prescript and Postscript paths and arguments, and a script timeout setting. Navigation buttons for 'Previous' and 'Next' are visible at the bottom.

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

Clone Options

Logs

Script

Notification

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.

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 inquiries.

Next: [Disaster recovery workflow](#).

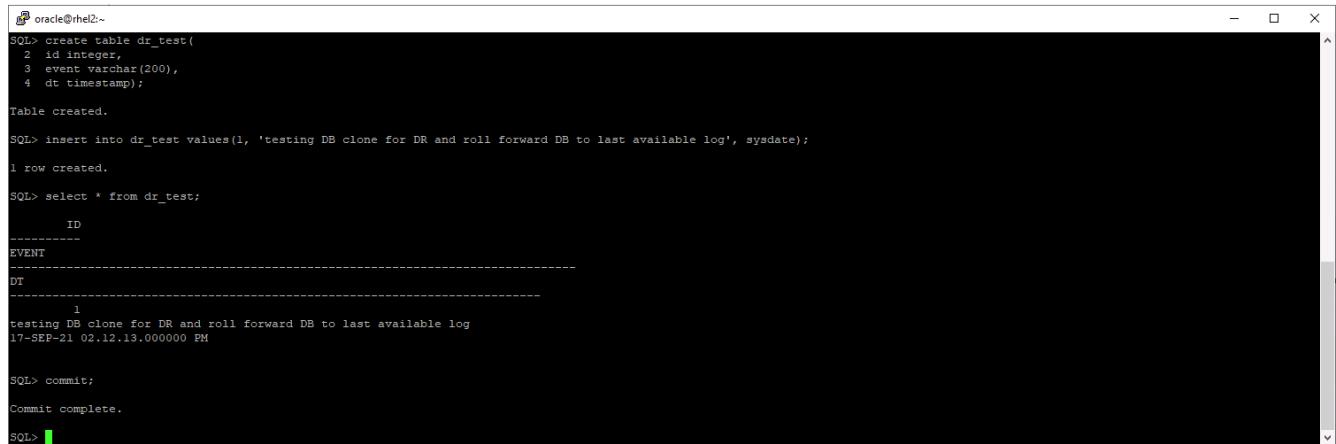
Disaster recovery workflow

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: 'rhe12_cdb2' (1 resource, orafullbkup tag, Oracle Full Online Backup policy, last backup 09/17/2021 2:38:16 PM, completed) and 'rhe12_cdb2_log' (1 resource, oralogbkup tag, Oracle Archive Log Backup policy, last backup 09/17/2021 6:02:13 PM, 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 sidebar and top navigation bar are identical to the previous screenshot. The main table now shows the details for 'rhe12_cdb2_log': Name (rhe12_cdb2), Resource Name (cdb2), Type (Oracle Database), and Host (rhe12.demo.netapp.com). Action buttons for Modify Resource Group, Back up Now, Maintenance, and Delete are at the top right.

A modal dialog box titled 'Backup' is displayed. It asks 'Create a backup for the selected resource group'. The 'Resource Group' field contains 'rhe12_cdb2_log'. The 'Policy' field is a dropdown set to 'Oracle Archive Log Backup', with an information icon next to it. At the bottom are 'Cancel' and 'Backup' buttons.



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). Below this, a section 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' and maps 'Source Volume' (svm_onPrem:rhel2_u03) to 'Destination Volume' (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 Oracle Database topology for the database 'cdb2'. It includes a summary card with the following statistics:

- 370 Backups
- 16 Data Backups
- 354 Log Backups
- 2 Clones

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

Clone from cdb2

1 Name

Complete Database Clone

Clone SID: **cdb2dr**

PDB Clone

Secondary storage location : Snap Vault / Snap Mirror

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

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. 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, NETWORK, EVENTS & JOBS, PROTECTION, and HOSTS. Under STORAGE, 'Volumes' is selected. The main area displays a list of volumes, including '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 overlaid, asking for a 'NAME' (set to 'ora_standby_u03') and 'CAPACITY' (set to '20 GB').

```

[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 in progress, specifically Step 2: Locations. The left sidebar lists steps 1 through 7. The main area is titled "Select the host to create a clone" and shows the "Clone host" set to "ora-standby.demo.netapp.com". Under "Datafile locations", the path "/u02_cdb2dr" is listed. In the "Control files" section, two paths are listed: "/u02_cdb2dr/cdb2dr/control/control01.ctl" and "/u03_cdb2dr/cdb2dr/control/control02.ctl". The "Redo logs" section contains a table with two groups: "RedoGroup 1" and "RedoGroup 2", each with a size of 200 MB and one file. At the bottom right are "Previous" and "Next" buttons.

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' and a port of '1521'. Below that, 'Oracle Home Settings' are configured with the Oracle Home path set to '/u01/app/oracle/product/19800/cdb2', and the Oracle OS User and Group both set to '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

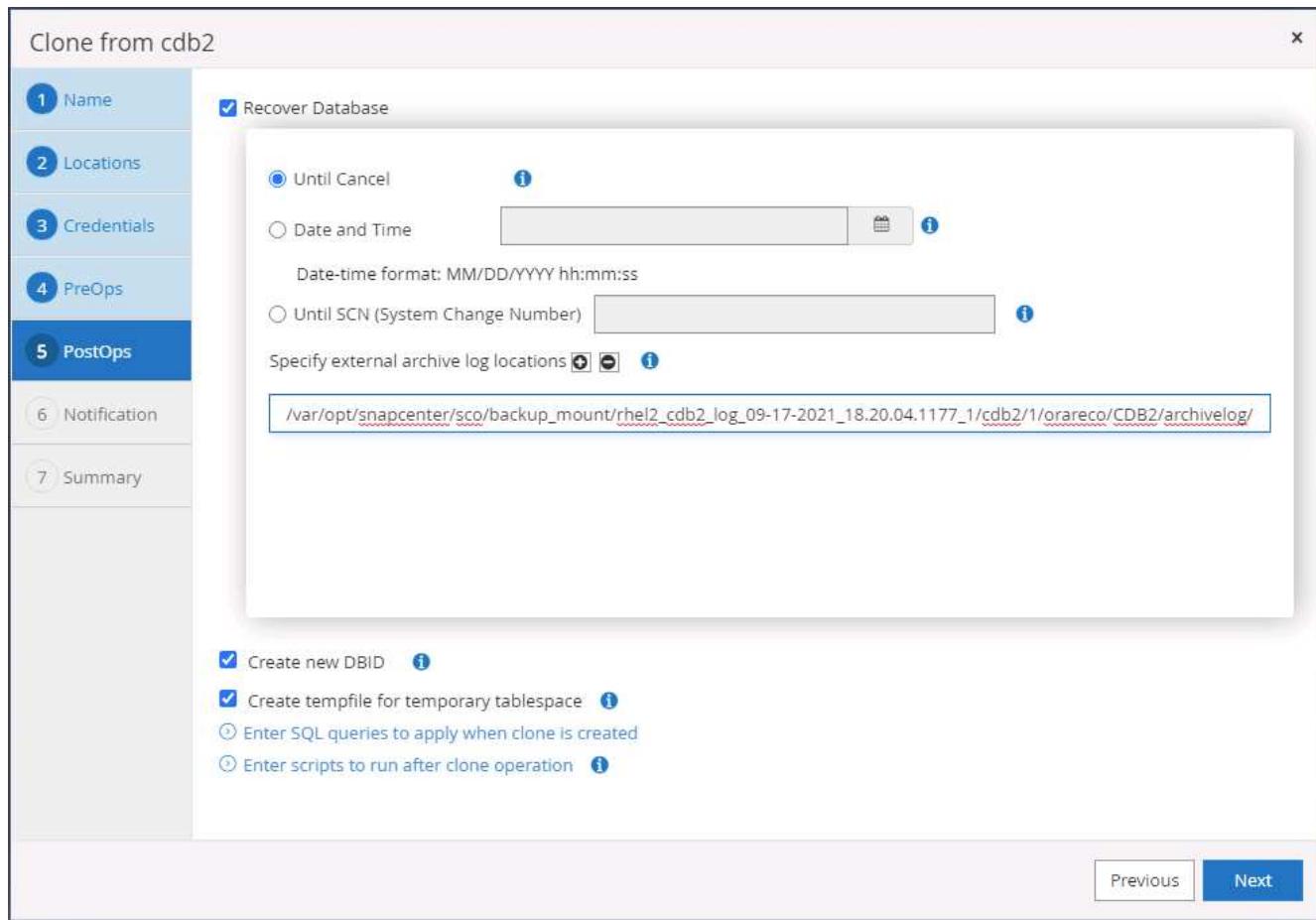
Database Parameter settings

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

1 Name	Summary
2 Locations	Clone from backup rhel2_cdb2_09-17-2021_14.35.01.4997_0
3 Credentials	Clone SID cdb2dr
4 PreOps	Clone server ora-standby.demo.netapp.com
5 PostOps	Exclude PDBs none
6 Notification	Oracle home /u01/app/oracle/product/19800/cdb2
7 Summary	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					
		View	Database	Search databases			
	Dashboard						
	Resources		cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com	rhel2_cdb2 rhel2_cdb2_log	Policies Last Backup Overall Status
	Monitor		cdb2dev	Single Instance (Multitenant)	ora-standby.demo.netapp.com		Oracle Archive Log Backup 09/17/2021 7:00:10 PM Backup succeeded
	Reports		cdb2dr	Single Instance (Multitenant)	ora-standby.demo.netapp.com		
	Hosts		cdb2test	Single Instance (Multitenant)	ora-standby.demo.netapp.com		
	Storage Systems						
	Settings						
	Alerts						

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.

5. 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.

Clone from backup

1 Clone Options

Clone settings

Clone server: sql-standby.demo.netapp.com

Clone instance: sql-standby

Clone name: tpcc_dr

Choose mount option

Auto assign mount point

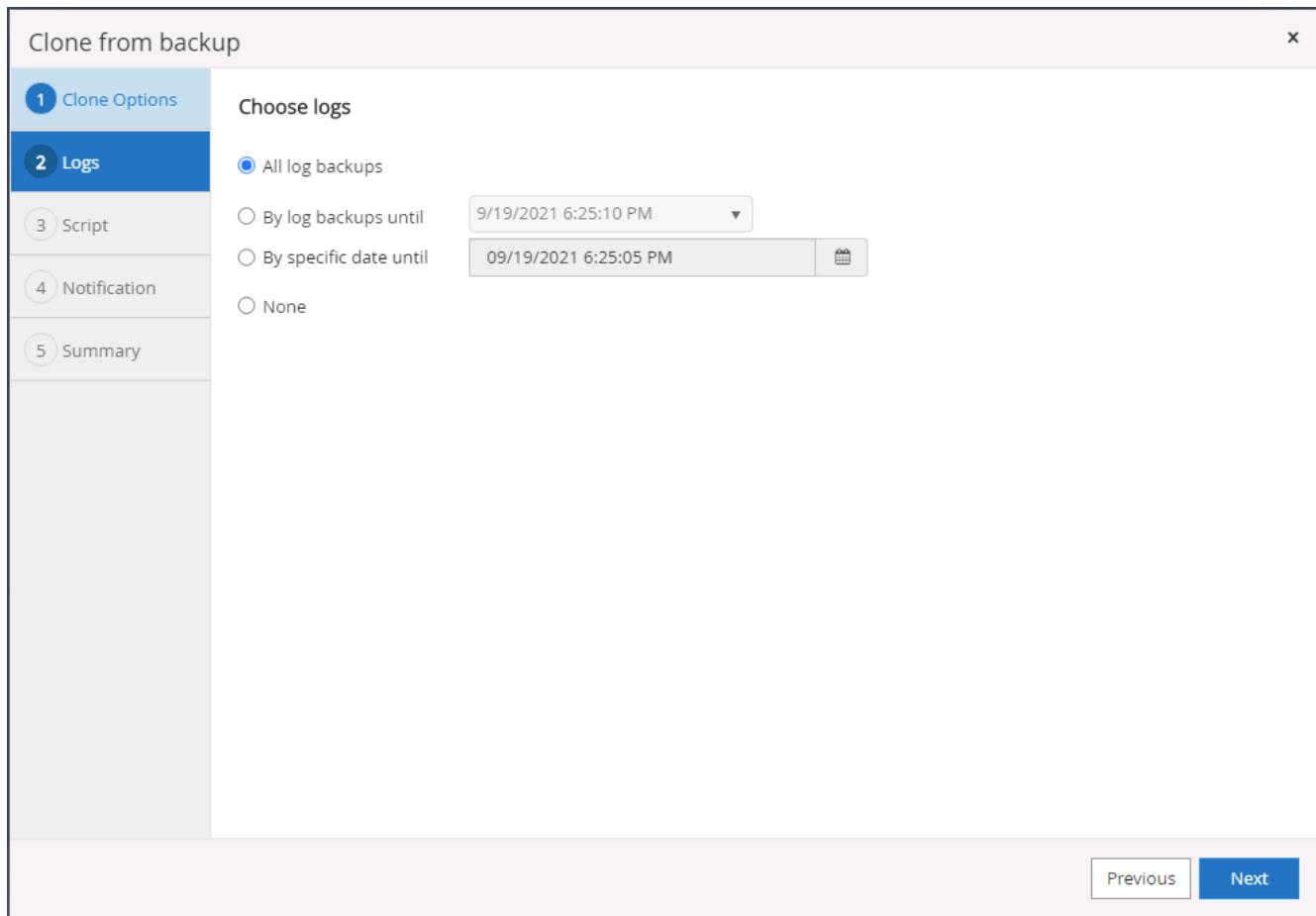
Auto assign volume mount point under path: full file path

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. 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

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 Clone Options
2 Logs
3 Script
4 Notification
5 Summary

- 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

Dashboard Resources Monitor Reports Hosts Storage Systems Settings Alerts

Refresh Resources New Resource Group

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_clev	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

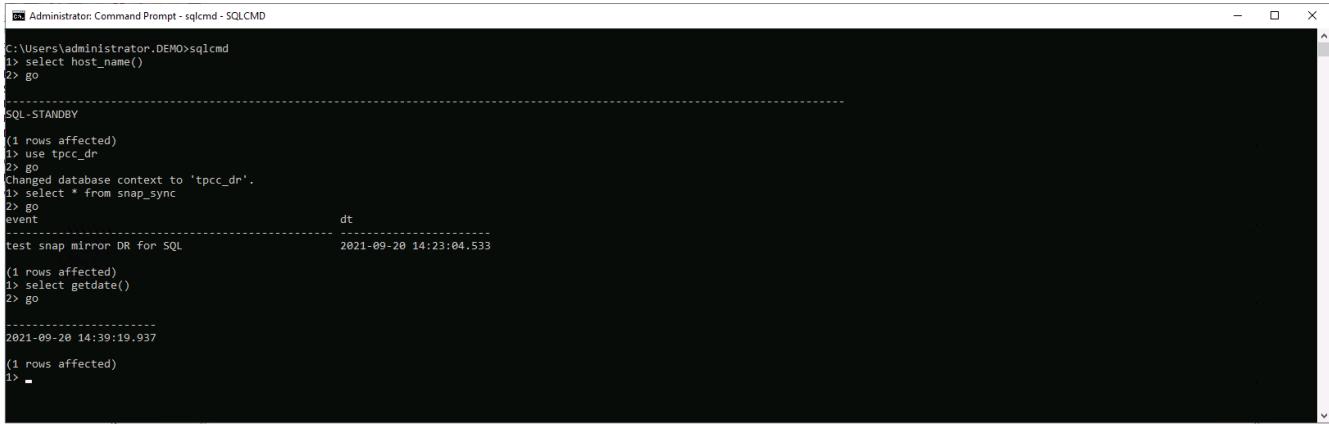
search by name

Dashboard Resources Monitor Reports Hosts Storage Systems Settings

Details Report Download Logs Cancel Job

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 2:26:17 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 1:36:01 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 1:26:50 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 © 2023 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—with 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

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.