



# Database management

## NetApp Solutions

NetApp  
October 20, 2023

This PDF was generated from [https://docs.netapp.com/us-en/netapp-solutions/databases/aws\\_ora\\_fsx\\_ec2\\_mgmt.html](https://docs.netapp.com/us-en/netapp-solutions/databases/aws_ora_fsx_ec2_mgmt.html) on October 20, 2023. Always check docs.netapp.com for the latest.

# Table of Contents

- EC2 and FSx Oracle database management ..... 1
  - Taking a snapshot ..... 1
  - Restoring to a point in time ..... 4
  - Creating a database clone ..... 14
  - HA failover to standby and resync ..... 23

# 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 failback 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.

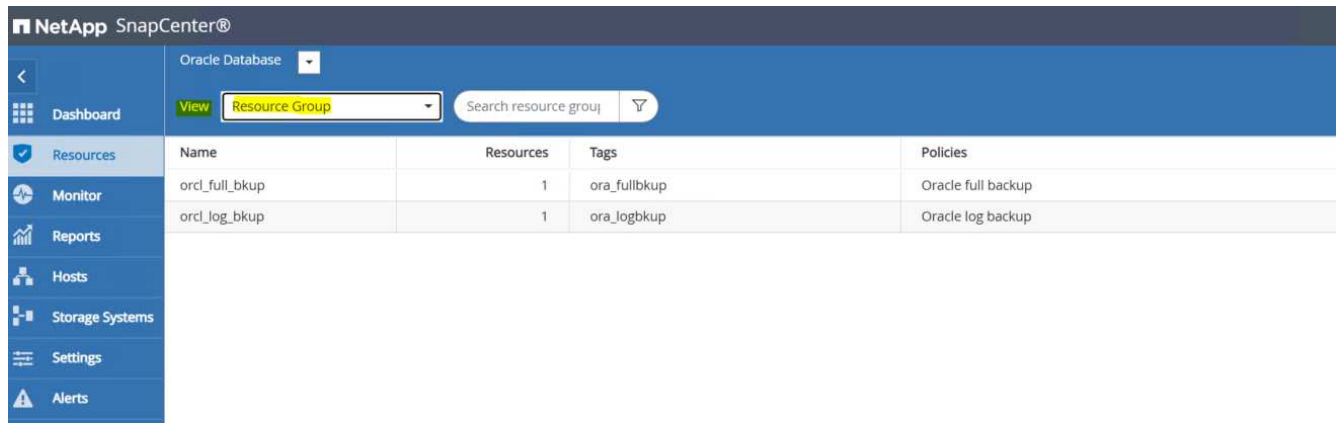
## Taking a snapshot

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.

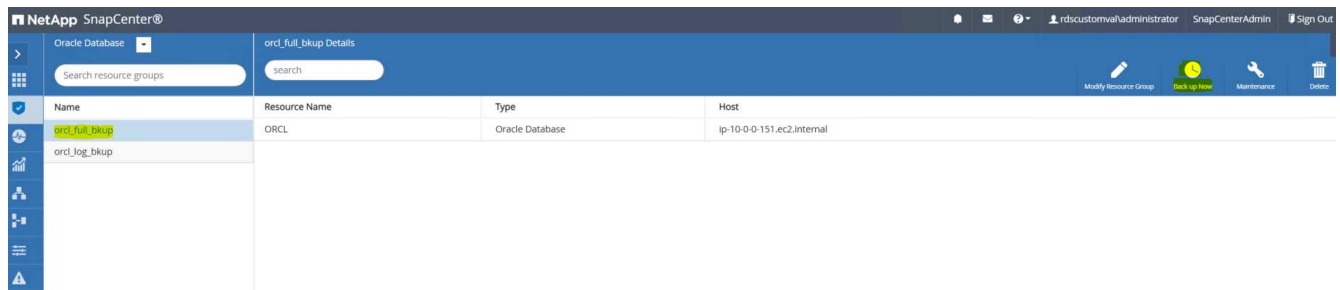
### Taking a full database snapshot

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

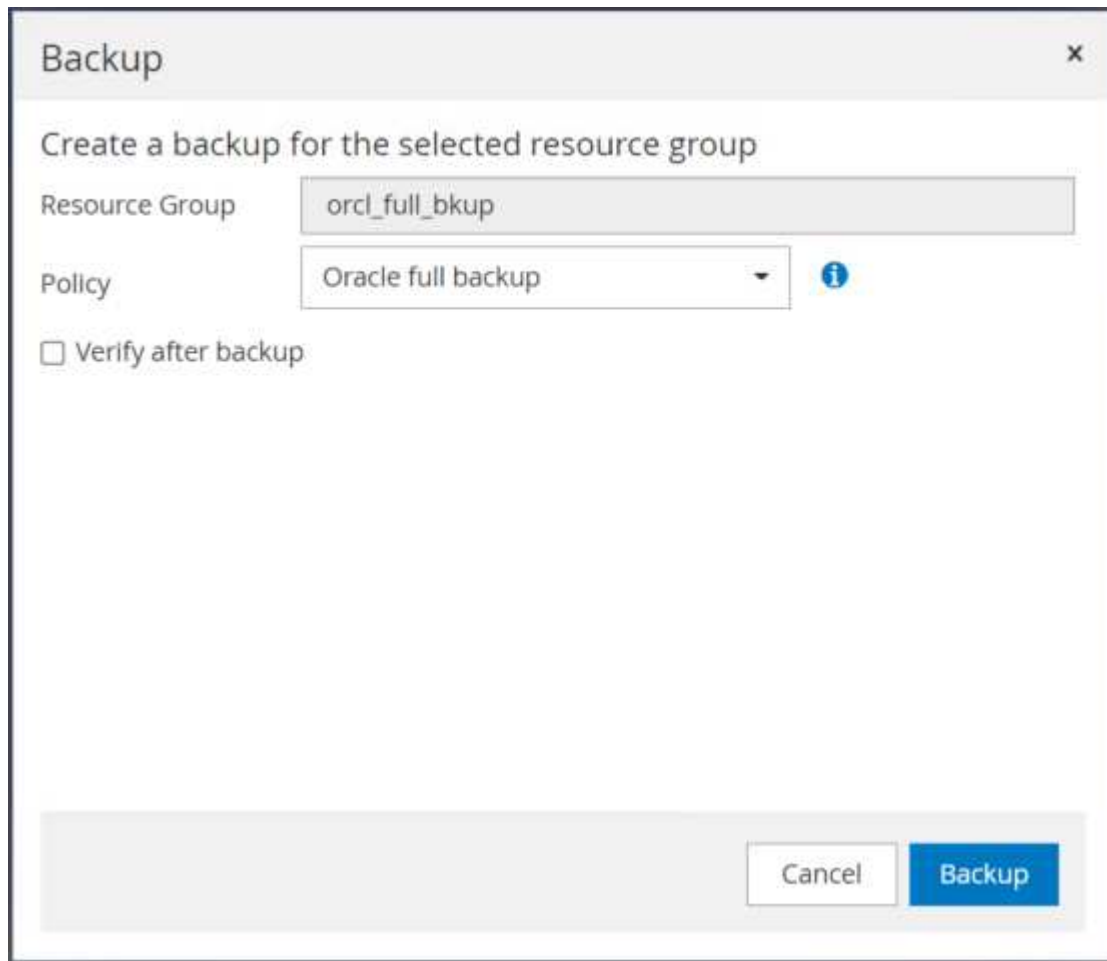
1. Log into the SnapCenter UI and click Resources in the left-side menu. From the View dropdown, change to the Resource Group view.



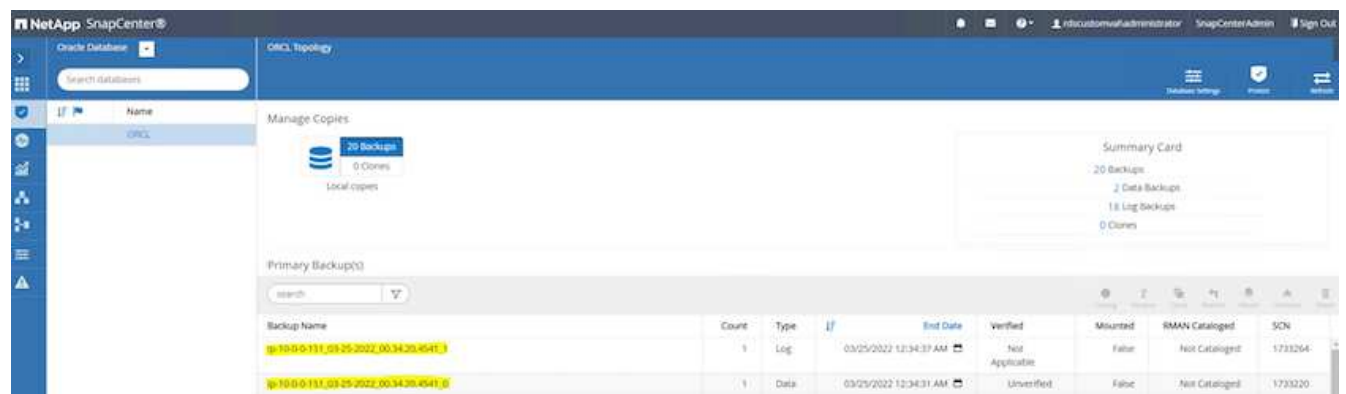
- Click the full backup resource name, and then click the Backup Now icon to initiate an add-hoc backup.



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



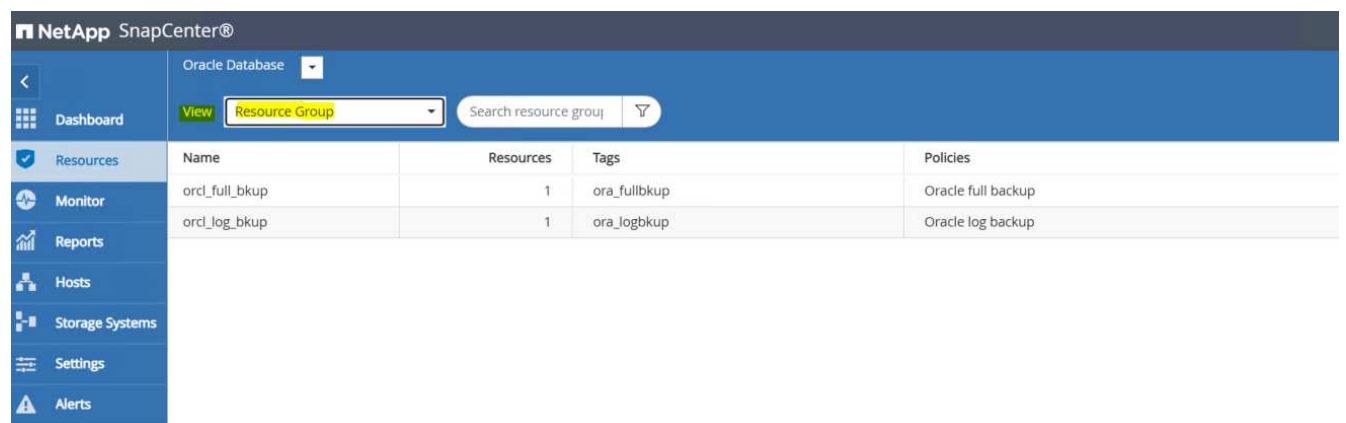
From the Resource view for the database, open the database Managed Backup Copies page to verify that the one-off backup completed successfully. A full database backup creates two snapshots: one for the data volume and one for the log volume.



## 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.



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



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

Backup

Create a backup for the selected resource group

Resource Group

orcl\_log\_bkup

Policy

Oracle log backup

Cancel

Backup

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.

NetApp SnapCenter®

Oracle Database

ORCL Topology

Search databases

Database Settings

Protect

Admin

27 Backups

0 Clones

Local copies

Summary Card

27 Backups

2 Data Backups

25 Log Backups

0 Clones

Primary Backup(s)

Search

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
sp-15-0-0-1101-03-25-2022-01:58:38.0731.1	1	Log	03/25/2022 1:58:40 AM	Not Applicable	False	Not Cataloged	1730201

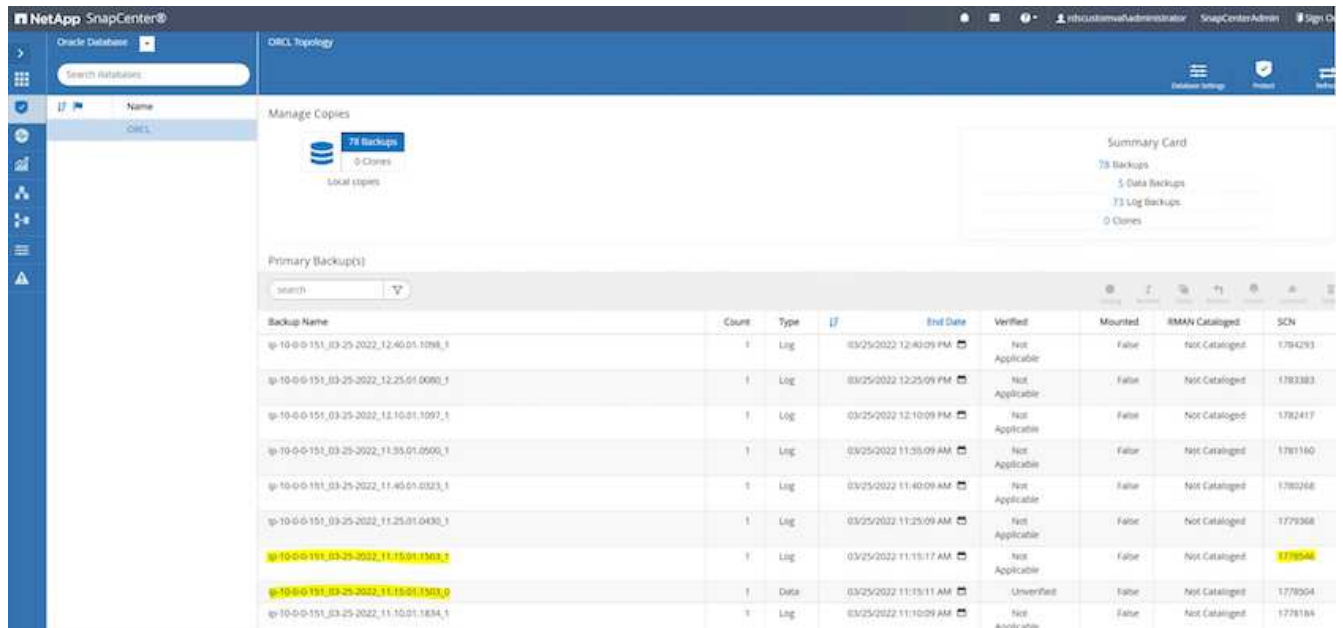
## Restoring to a point in time

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

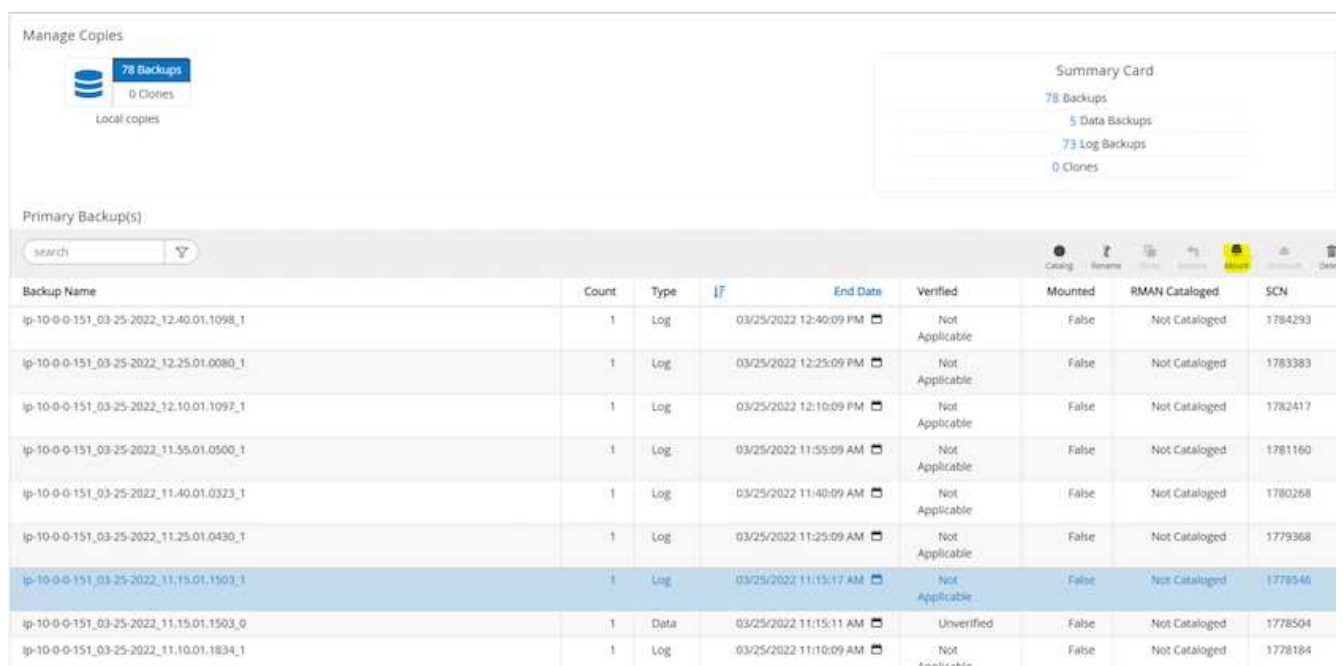
1. From the SnapCenter Resources tab > Database view, click the database name to open the database backup.



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.



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



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

### Mount backups

Choose the host to mount the backup

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

Mount path : /var/opt/snapcenter/sco/backup\_mount/ip-10-0-0-151\_03-25-2022\_11.15.01.1503\_1/ORCL

Mount Cancel

- 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.

NetApp SnapCenter®
Jobs Schedules Events Logs
Dashboard
Resources
Monitor
Reports

All jobs

ID	Status	Name	Start date	End date	Owner
4390		Backup of Resource Group 'ora_nfs_log' with policy 'Oracle log backup'	3/25/2022 1:40:00 PM	3/25/2022 1:40:13 PM	ntbscustomva@administrator
4388		Mount backup to ip-10-0-0-151_03-25-2022_11.15.01.1503_1	03/25/2022 1:38:30 PM	03/25/2022 1:38:53 PM	ntbscustomva@administrator

```

[root@ip-10-0-0-151 ec2-user]# df -h
Filesystem              Size  Used Avail Use% Mounted on
devtmpfs                7.6G   0  7.6G   0% /dev
tmpfs                   16G   0  16G   0% /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/obdata01-lvdbdata01 40G 471M  39G   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:/Sce91c793-5583-480d-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/1

```

- 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/
```

- 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

80 Backups

0 Clones

Local copies

Summary Card

80 Backups

5 Data Backups

75 Log Backups

0 Clones

Primary Backup(s)

search

Catalog

Refresh

Clone

Mount

Unmount

More

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_11:55:09.0500_1	1	Log	03/25/2022 11:55:09 AM	Not Applicable	False	Not Cataloged	1781160
ip-10-0-0-151_03-25-2022_11:40:09.0323_1	1	Log	03/25/2022 11:40:09 AM	Not Applicable	False	Not Cataloged	1780268
ip-10-0-0-151_03-25-2022_11:25:09.0430_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

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

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.

Restore ORCL

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Choose Recovery Scope

All Logs

Until SCN (System Change Number)

Date and Time

No recovery

SCN

1778546

Specify external archive log files locations

Previous

Next

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

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Arguments

Script timeout

60

secs

Previous

Next

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

/var/opt/snapcenter/spl/scripts/

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

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Provide email settings ⓘ

Email preference

Never

From

From email

To

Email to

Subject

Notification

☐ Attach job report

Previous

Next

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

Restore ORCL

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

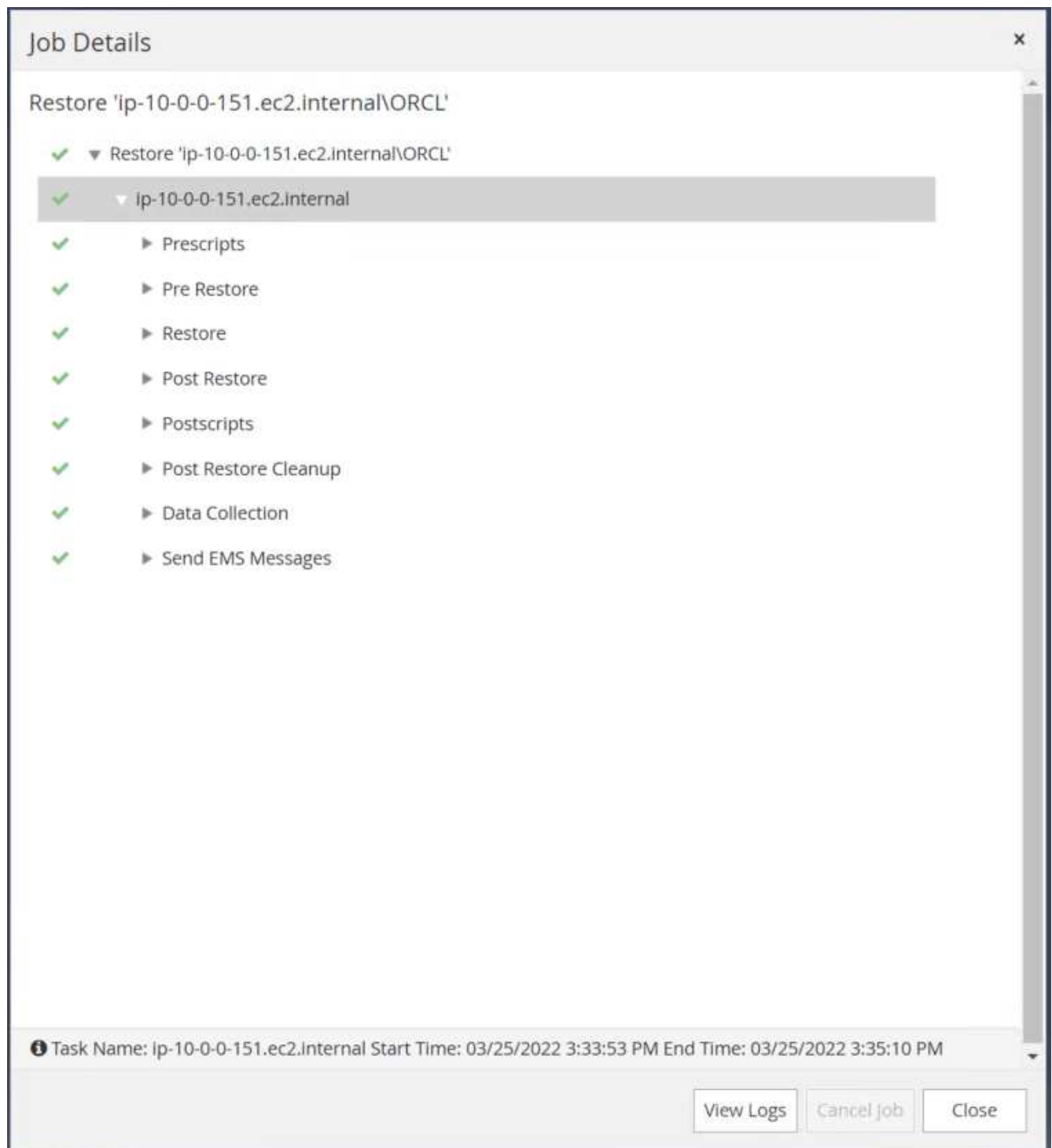
Summary

Backup name	lp-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.



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_TIME OPEN_MODE
-----
ORCL          1778547 25-MAR-22 READ WRITE

SQL>

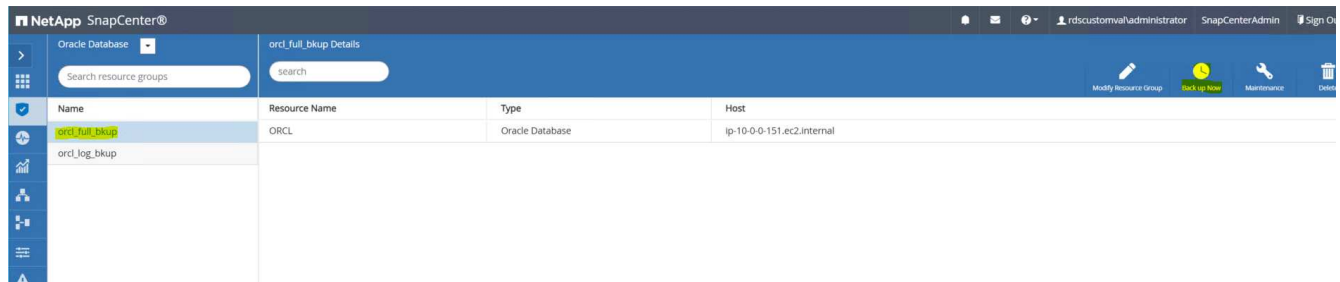
```

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

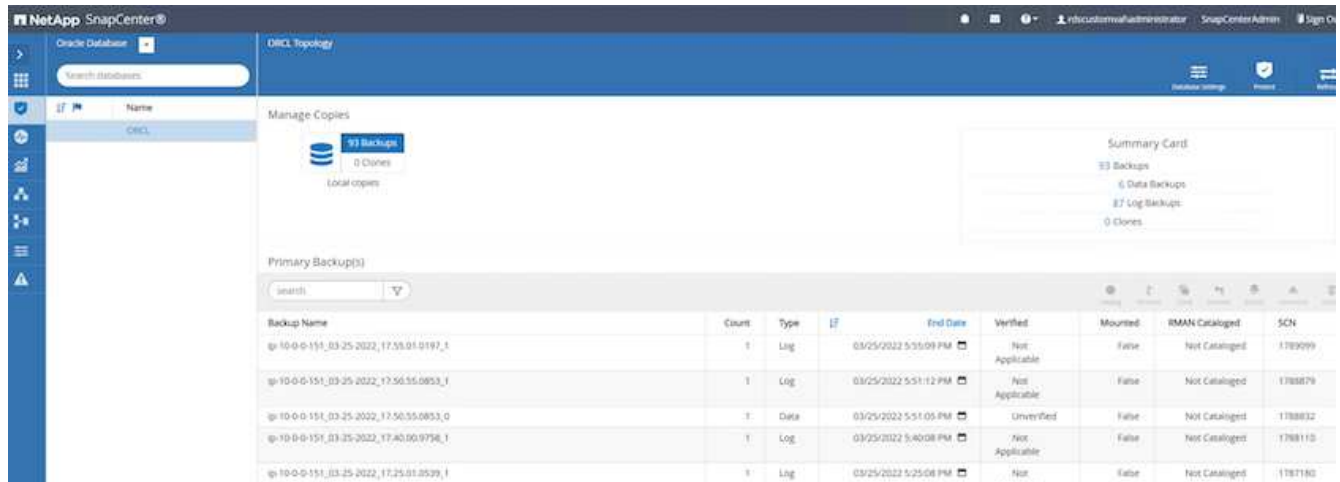
## Creating a database clone

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.



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.





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

The screenshot displays the 'ORCL Topology' interface. At the top, there's a 'Manage Copies' section with a '95 Backups' badge and '0 Clones' under 'Local copies'. To the right is a 'Summary Card' showing '95 Backups', '6 Data Backups', '89 Log Backups', and '0 Clones'. Below this is a 'Primary Backup(s)' section with a search bar and a table of backups.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
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	Not Cataloged	1892563
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	Not Cataloged	1891375
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	Not Cataloged	1789099
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	Not Cataloged	1788679
ip-10-0-0-151_03-25-2022_17:50:55.0853_0	1	Data	03/25/2022 5:51:05 PM	Unverified	False	Not Cataloged	1788832
ip-10-0-0-151_03-25-2022_17:40:00.9758_1	1	Log	03/25/2022 5:40:08 PM	Not	False	Not Cataloged	1788110

Below the table is a 'Mount backups' dialog box. It has a title bar with a close button. Inside, it says 'Choose the host to mount the backup' with a dropdown menu showing 'ip-10-0-0-47.ec2.internal'. Below that, it shows 'Mount path : /var/opt/snapcenter/sco/backup\_mount/ip-10-0-0-151\_03-25-2022\_17:50:55.0853\_1/ORCL'. At the bottom right are 'Mount' and 'Cancel' buttons.

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

ORCL Topology

Database Settings Protect Refresh

Manage Copies

93 Backups  
0 Clones  
Local copies

Summary Card

93 Backups  
6 Data Backups  
87 Log Backups  
0 Clones

Primary Backup(s)

search

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
lp-10-0-0-151_03-25-2022_17:55:01.0197_1	1	Log	03/25/2022 5:55:09 PM	Not Applicable	False	Not Cataloged	1789099
lp-10-0-0-151_03-25-2022_17:50:55.0853_1	1	Log	03/25/2022 5:51:12 PM	Not Applicable	False	Not Cataloged	1788879
lp-10-0-0-151_03-25-2022_17:50:55.0853_0	1	Data	03/25/2022 5:51:05 PM	Unverified	False	Not Cataloged	1788832
lp-10-0-0-151_03-25-2022_17:40:00.9758_1	1	Log	03/25/2022 5:40:08 PM	Not Applicable	False	Not Cataloged	1788110
lp-10-0-0-151_03-25-2022_17:25:01.0539_1	1	Log	03/25/2022 5:25:08 PM	Not Applicable	False	Not Cataloged	1787180

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

Clone from ORCL

1 Name

Provide clone database SID

Clone SID ORCLREAD

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Previous Next

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

Clone from ORCL

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

Select the host to create a clone

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

Datafile locations ⓘ

/ora\_nfs\_data\_ORCLREAD
Reset

Control files ⓘ

/ora\_nfs\_data\_ORCLREAD/ORCLREAD/control/control01.ctl
Reset

Redo logs ⓘ

Group	Size	Unit	Number of files
<div> RedoGroup 1 </div> <div> /ora_nfs_data_ORCLREAD/ORCLREAD/redolog/redo04.log </div>	128	MB	1
<div> RedoGroup 2 </div>	128	MB	1

Previous
Next

- 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

None

+

i

Database port

1521

Oracle Home Settings

i

Oracle Home

/rdsdbbin/oracle

Oracle OS User

rdsdb

Oracle OS Group

database

Previous

Next

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

Clone from ORCL

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

☒ Recover Database

○ Until Cancel

○ Date and Time

☒ Until SCN (System Change Number)

1788879

Date-time format: MM/DD/YYYY hh:mm:ss

Specify external archive log locations

/var/opt/snapcenter/sco/backup\_mount/lp-10-0-0-151\_03-25-2022\_17.50.55.0853\_1/ORCL/1/db/ORCL\_A/arch

☒ Create new DBID

☒ Create tempfile for temporary tablespace

○ Enter SQL queries to apply when clone is created

○ Enter scripts to run after clone operation

Previous

Next

9. Send the SMTP email settings if needed.

19

Clone from ORCL

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Provide email settings ⓘ

Email preference

Never

From

From email

To

Email to

Subject

Notification

☐ Attach job report

Previous

Next

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

Clone from ORCL

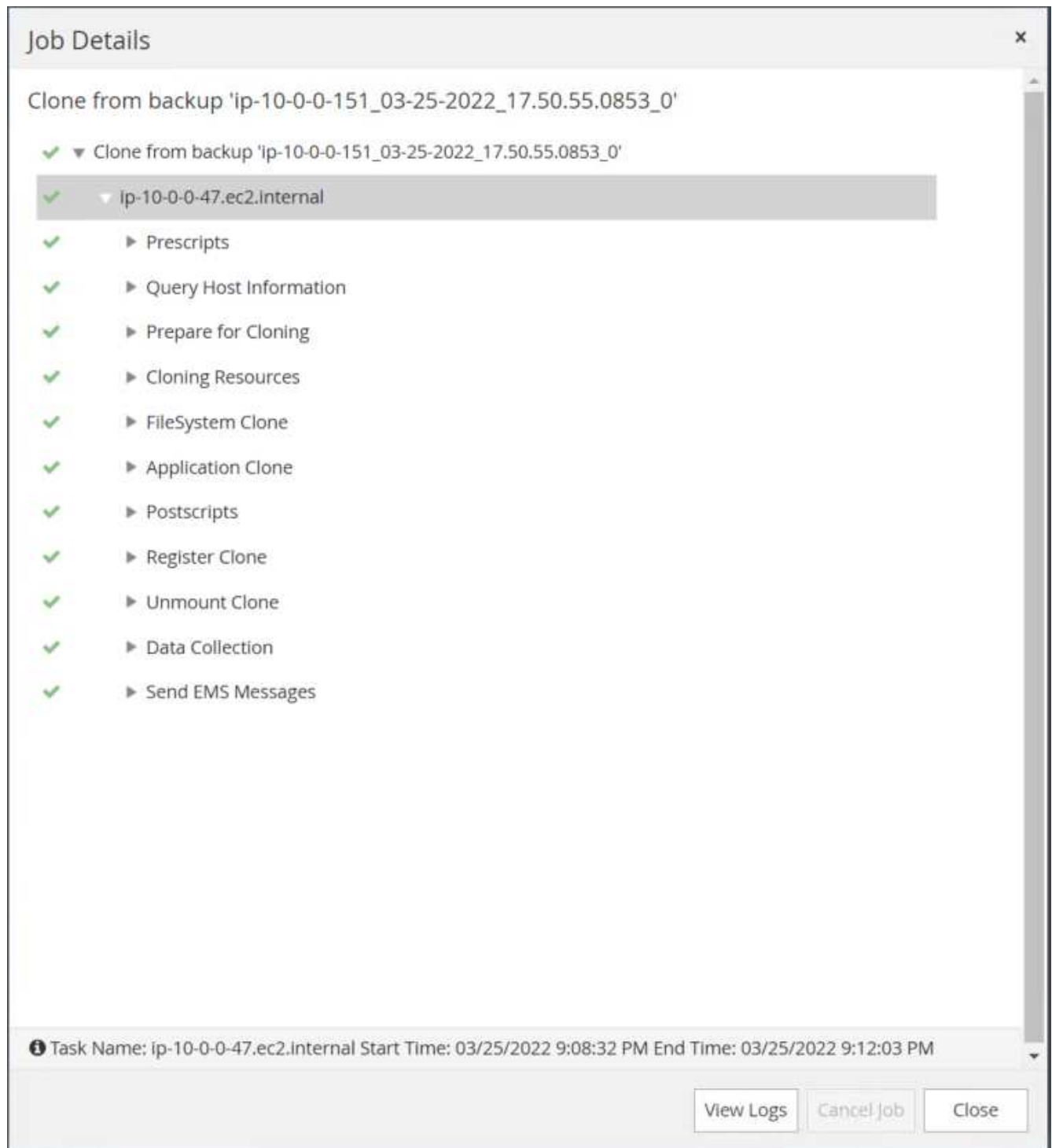
1 Name
2 Locations
3 Credentials
4 PreOps
5 PostOps
6 Notification
7 Summary

Summary

Clone from backup	ip-10-0-0-151_03-25-2022_17:50:55.0853_0
Clone SID	ORCLREAD
Clone server	ip-10-0-0-47.ec2.internal
Oracle home	/rdsdbbin/oracle
Oracle OS user	rdsdb
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.



The cloned database is registered in SnapCenter immediately.





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_oracle_hadr_failover_resync.git
```

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

[Next: Database migration.](#)

## 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—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

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.