COHESITY

Version 1.2

July 2024

Sudoers List for Cohesity's Oracle Adapter

Configure Cohesity Agent Privileges for Cohesity Oracle Adapter

ABSTRACT

When you use the Cohesity Oracle Adapter to integrate Cohesity Helios platform with Oracle Recovery Manager (RMAN), you need to ensure that the Cohesity Agent has Sudo privileges on the Linux or Unix system where it runs. Use this guide to configure those privileges properly.

Table of Contents

Tables

Introduction to Sudo Privileges for Oracle Adapter

The Cohesity Oracle Adapter natively integrates with Oracle Recovery Manager (RMAN) to provide application-consistent backup and recovery for Oracle Single Instance, Real Application Clusters (RAC), and Oracle Veritas Active-Passive. To perform these data protection tasks, the Cohesity Oracle Adapter relies on its interactions with the Cohesity Agent that run on the Linux servers hosting the databases that you need to protect. For those interactions to work, you need to ensure that the Cohesity Agent is running via an OS user account that has sudo (administrator) privileges.

This guide helps you set the sudo privileges you need for the installation and operation of the Cohesity Oracle Adapter on Linux and Unix OS environments.

Why the Cohesity Agent Needs Sudo Privileges

The Cohesity Agent requires the user account to have administrator permissions and privileges to execute OS and DB commands. These permissions are also necessary to enable several functions of the Cohesity Oracle Adapter, including database recovery, OS and database authentication, Protection Group (Protection Job formerly) configuration, and more.

Configure Sudo Privileges for the Agent User Account

Before you install the Cohesity Agent on your Oracle database server, you need to configure the right privileges for the user account that will run the Cohesity Agent on that server, whether you are an existing or new user.

There are two ways to set the privileges:

- Configure default permissions (All)
- Configure restricted permission (Specific)

The commands you need to configure permissions vary by operating system. See Table 1 below for the specific commands in your OS.

Table 1: Required Configuration Commands for Different OSs

OPERATING SYSTEM	COMMAND LIST
Oracle Enterprise Linux 6/7 Red Hat Enterprise Linux 6/7 CentOS SLES 11/12	Mount, umount, cp, chown, chmod, mkdir, rm, tee, hostname, stat, timeout, ls, rsync, blkid, lsof, losetup, dmsetup, lvs, vgs, lvcreate, lvremove, lvchange, srvctl, lltconfig, hagrp, hares
IBM AIX 7 (7.1/7.2)	mkdir, rm, tee, cp, mount, umount, chmod, chown, srvctl, lltconfig, hagrp, hares

Configure Default Permissions

To configure default privileges to the user, add the following entry to the sudoers file, `/etc/sudoers`.

```
cohesity ALL=(ALL) NOPASSWD:ALL
Defaults:cohesity !requiretty
```

Configure Restricted Permission

The user account that is used to install and run the Cohesity Agent must be configured in restricted mode for the Linux or Unix environment where the default sudo permission (NOPASSWD:ALL) is not allowed. In restricted mode, the user account requires sudo permissions to execute OS-dependent commands.

NOTE: It is also necessary to use the absolute path when whitelisting the command as part of the sudoers list (`/etc/sudoers`).

All the commands that need to go into the sudoers file must have their absolute paths.

Cohesity Agent Command Paths

Table 2 below shows the commands and their default paths based on the OS types. Backup and database administrators can copy the relevant paths from the table and add them to the list in `/etc/sudoers`.

Table 2: Cohesity Agent Command Paths

COMMAND	OS FLAVORS		
	OEL/RHEL/CENTOS	SUSE	AIX
chmod	/usr/bin/chmod		
chown	/usr/bin/chown		
cp	/usr/bin/cp		
mkdir	/usr/bin/mkdir		
mount	/usr/sbin/mount		
rm	/usr/bin/rm		
tee	/usr/bin/tee		
umount	/usr/bin/umount		
ls	/usr/bin/ls		N/A
rsync	/usr/bin/rsync		N/A
stat	/usr/bin/stat		N/A
timeout	/usr/bin/timeout		N/A
hostname	/usr/bin/hostname	/bin/hostname	N/A
blkid	/usr/sbin/blkid	/sbin/blkid	N/A
dmsetup	/usr/sbin/dmsetup	/sbin/dmsetup	N/A
losetup	/usr/sbin/losetup	/sbin/losetup	N/A
lsof	/usr/sbin/lsof	/usr/bin/lsof	N/A
lvchange	/usr/sbin/lvchange	/sbin/lvchange	N/A
lvcreate	/usr/sbin/lvcreate	/sbin/lvcreate	N/A
lvremove	/usr/sbin/lvremove	/sbin/lvremove	N/A
lvs	/usr/sbin/lvs	/sbin/lvs	N/A

COMMAND	OS FLAVORS		
	OEL/RHEL/CENTOS	SUSE	AIX
vgs	/usr/sbin/vgs	/sbin/lvs	N/A

Additional Commands for Oracle on VCS

If you have deployed Oracle on a Veritas Cluster Server (VCS) cluster (as an alternative to Oracle RAC), also add the following commands to the sudoers list, in addition to the commands in Table 2 above.

Table 3: Additional Commands for Oracle on VCS

COMMAND	OS FLAVORS		
	OEL/RHEL/CENTOS	SUSE	AIX
lltconfig	/sbin/lltconfig		N/A
hagrp	/opt/VRTSvcs/bin/hagrp		N/A
hares	/opt/VRTSvcs/bin/hares		N/A

Additional Command for Oracle RAC

If you have deployed Oracle on RAC, add the `srvctl` command to the sudoers list, in addition to the commands specified in Table 2 above.

Table 4: Additional Command for Oracle RAC

COMMAND	OS FLAVORS		
	OEL/RHEL/CENTOS	SUSE	AIX
srvctl	$ORACLE_HOME/srvctl		

NOTE: **`srvctl`** is an Oracle RAC-specific command, and for each unique `ORACLE_HOME` in the `/etc/oratab` file, there must be a corresponding entry in the `/etc/sudoers` file.

Configure the Sudoers List

To edit and configure sudoers, use a root user account to add the commands to the `/etc/sudoers` file.

IMPORTANT: The sudoers list needs to be updated on *each* Oracle host where the Cohesity Agent is installed.

To configure sudoers on an Oracle host:

1. Prepare the list of commands that you need to add to the sudoers list. You can copy the relevant paths from the tables in Configure Restricted Permission above. Alternatively, as a root user, you can use the which command to find the absolute path of the commands.

Input:

```
[root@myhost~]# which mount umount cp chown chmod mkdir rm tee hostname
stat timeout ls rsync srvctl blkid dmsetup losetup lsof lvchange lvcreate
lvremove lvs vgs lltconfig hagrp hares
```

Output:

```
/usr/bin/mount
/usr/bin/umount
/usr/bin/cp
/usr/bin/chown
/usr/bin/chmod
/usr/bin/mkdir
/usr/bin/rm
/usr/bin/tee
/usr/bin/hostname
/usr/bin/stat
/usr/bin/timeout
/usr/bin/ls
/usr/bin/rsync
/u01/app/oracle/product/12.1.0/db_1/bin/srvctl
/usr/sbin/blkid
/usr/sbin/dmsetup
/usr/sbin/losetup
/usr/sbin/lsof
/usr/sbin/lvchange
/usr/sbin/lvcreate
/usr/sbin/lvremove
/usr/sbin/lvs
/usr/sbin/vgs
/sbin/lltconfig
/opt/VRTSvcs/bin/hagrp
/opt/VRTSvcs/bin/hares
```

2. Use the root user account to edit the `/etc/sudoers` file and append the commands as shown below. (Note that you must enter the whole command as a single line.)

Input:

```
[root@myhost~]# vi /etc/sudoers
```

Output:

```
cohesity ALL=(ALL)
OPASSWD:/usr/bin/mount,/usr/bin/umount,/usr/bin/cp,/usr/bin/chown,/usr/bi
n/chmod,/usr/bin/mkdir,/usr/bin/rm,/usr/bin/tee,/usr/bin/hostname,/usr/bi
n/stat,/usr/sbin/blkid,/usr/sbin/lsof,/usr/bin/ls,/usr/sbin/losetup,/usr/
sbin/dmsetup,/usr/bin/rsync,/usr/bin/timeout,/usr/sbin/lvs,/usr/sbin/vgs,
/usr/sbin/lvcreate,/usr/sbin/lvremove,/usr/sbin/lvchang,/u01/app/oracle/p
roduct/12.1.0/db_1/bin/srvctl,/usr/sbin/blkid/,usr/sbin/dmsetup/,usr/sbin
/losetup/,usr/sbin/lsof/,usr/sbin/lvchange/,usr/sbin/lvcreate/,usr/sbin/l
vremove/,usr/sbin/lvs/,usr/sbin/vgs/,sbin/lltconfig/,opt/VRTSvcs/bin/hagr
p/,opt/VRTSvcs/bin/hares
```

Where `"cohesity"` is the OS user account used to install the Cohesity Agent.

Verify the Sudoers List

To verify the sudoers, use the sudo command to list the commands that are configured as sudoers. See the Linux/AIX example using the sudo -l command below.

Input:

```
[cohesity@host_linux_6.5 ~]$ sudo -l
```

Output:

```
User cohesity may run the following commands on host_linux_6.5:
(ALL) NOPASSWD: /usr/bin/mount,/usr/bin/umount,/usr/bin/cp,
/usr/bin/chown,/usr/bin/chmod,/usr/bin/mkdir,/usr/bin/rm,
/usr/bin/tee,/usr/bin/hostname,/usr/bin/stat,/usr/sbin/blkid,
/usr/sbin/lsof,/usr/bin/ls,/usr/sbin/losetup,/usr/sbin/dmsetup,
/usr/bin/rsync,/usr/bin/timeout,/usr/sbin/lvs,/usr/sbin/vgs,
/usr/sbin/lvcreate,/usr/sbin/lvremove,/usr/sbin/lvchang
```

Your Feedback

Was this document helpful? Send us your feedback!

About the Author

Balarameshwar Naik is a Technical Marketing Engineer at Cohesity. In his role, Balaramesh focuses on enterprise databases and data protection with enterprise cloud storage.

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.2	July 2024	Republishing
1.1	Oct 2021	Rebranding updates
1.0	Feb 2020	Original document

ABOUT COHESITY

Cohesity is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including six of the Fortune 10 and 44 of the Fortune 100.

Visit our website and blog, follow us on Twitter and LinkedIn and like us on Facebook.