



Prerequisites for adding hosts and installing Plug-ins Package for Linux or AIX SnapCenter Software

NetApp
June 18, 2021

This PDF was generated from https://docs.netapp.com/us-en/snapcenter/protect-sco/reference_host_requirements_for_installing_the_snapcenter_plug_in_package_for_linux.html on June 18, 2021. Always check docs.netapp.com for the latest.

Table of Contents

- Prerequisites for adding hosts and installing Plug-ins Package for Linux or AIX 1
 - Host requirements for installing Plug-ins Package for Linux 1
 - Host requirements for installing Plug-ins Package for AIX 4
- Set up credentials for installing Plug-ins Package for Linux or AIX 6
- Configure credentials for an Oracle database 7

Prerequisites for adding hosts and installing Plug-ins Package for Linux or AIX

Before you add a host and install the plug-ins packages, you must complete all the requirements.

- If you are using iSCSI, the iSCSI service must be running.
- You must have enabled the password-based SSH connection for the root or non-root user.

SnapCenter Plug-in for Oracle Database can be installed by a non-root user. However, you should configure the sudo privileges for the non-root user to install and start the plug-in process. After installing the plug-in, the processes will be running as an effective root user.

- If you are installing the SnapCenter Plug-ins Package for AIX on AIX host, you should have manually resolved the directory level symbolic links.

The SnapCenter Plug-ins Package for AIX automatically resolves the file level symbolic link but not the directory level symbolic links to obtain the JAVA_HOME absolute path.

- Create credentials with authentication mode as Linux or AIX for the install user.
- You must have installed Java 1.8.x, 64-bit, on your Linux or AIX host.

For information to download JAVA, see:

- [Java Downloads for All Operating Systems](#)
- [IBM Java for AIX](#)

- For Oracle databases that are running on a Linux or AIX host, you should install both SnapCenter Plug-in for Oracle Database and SnapCenter Plug-in for UNIX.





You can use the Plug-in for Oracle Database to manage Oracle databases for SAP as well. However, SAP BR*Tools integration is not supported.

- If you are using Oracle database 11.2.0.3 or later, you must install the 13366202 Oracle patch.

Host requirements for installing Plug-ins Package for Linux

You should ensure that the host meets the requirements before installing the SnapCenter Plug-ins Package for Linux.

Item	Requirements
Operating systems	<ul style="list-style-type: none"> • Red Hat Enterprise Linux • Oracle Linux <div>  <p>If you are using Oracle database on LVM in Oracle Linux or Red Hat Enterprise Linux 6.6 or 7.0 operating systems, you must install the latest version of Logical Volume Manager (LVM).</p> </div> <ul style="list-style-type: none"> • SUSE Linux Enterprise Server (SLES)
Minimum RAM for the SnapCenter plug-in on host	1 GB
Minimum install and log space for the SnapCenter plug-in on host	2 GB <div>  <p>You should allocate sufficient disk space and monitor the storage consumption by the logs folder. The log space required varies depending on the number of the entities to be protected and the frequency of data protection operations. If there is no sufficient disk space, the logs will not be created for the recently run operations.</p> </div>
Required software packages	Java 1.8 (64-bit) Oracle Java and OpenJDK flavors <p>If you have upgraded JAVA to the latest version, you must ensure that the JAVA_HOME option located at <code>/var/opt/snapcenter/spl/etc/spl.properties</code> is set to the correct JAVA version and the correct path.</p>

For the latest information about supported versions, see the [NetApp Interoperability Matrix Tool](#).

Configuring sudo privileges for non-root users for Linux plug-in host

SnapCenter 2.0 and later releases allow a non-root user to install the SnapCenter Plug-ins Package for Linux and to start the plug-in process. You should configure sudo privileges for the non-root user to provide access to several paths.

What you will need

- Sudo 1.8.7 or later.
- Ensure that the non-root user is part of the Oracle installation group.

- Edit the `/etc/ssh/sshd_config` file to configure the message authentication code algorithms: MACs hmac-sha2-256 and MACs hmac-sha2-512.

Restart the sshd service after updating the configuration file.

Example:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

About this task

You should configure sudo privileges for the non-root user to provide access to the following paths:

- `/home/SUDO_USER/.sc_netapp/snapcenter_linux_host_plugin.bin`
- `/custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall`
- `/custom_location/NetApp/snapcenter/spl/bin/spl`

Steps

1. Log in to the Linux host on which you want to install the SnapCenter Plug-ins Package for Linux.
2. Add the following lines to the `/etc/sudoers` file by using the visudo Linux utility.

```
Cmdnd_Alias SCCMD = sha224:checksum_value== /home/
SUDO_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmdnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
SUDO_USER/.sc_netapp/Linux_Prechecks.sh
SUDO_USER ALL=(ALL) NOPASSWD:SETENV: SCCMD, PRECHECKCMD
Defaults: SUDO_USER env_keep=JAVA_HOME
Defaults: SUDO_USER !visiblepw
Defaults: SUDO_USER !requiretty
```

`SUDO_USER` is the name of the non-root user that you created.

You can obtain the checksum value from the `oracle_checksum.txt` file, which is located at

C:\ProgramData\NetApp\SnapCenter\Package Repository.

If you have specified a custom location, the location will be *custom_path\NetApp\SnapCenter\Package Repository*.




The example should be used only as a reference for creating your own data.

Best Practice: For security reasons, you should remove the sudo entry after completing every installation or upgrade.

Host requirements for installing Plug-ins Package for AIX

You should ensure that the host meets the requirements before installing the SnapCenter Plug-ins Package for AIX.

Item	Requirements
Operating systems	AIX 6.1 or later
Minimum RAM for the SnapCenter plug-in on host	4 GB
Minimum install and log space for the SnapCenter plug-in on host	1 GB  You should allocate sufficient disk space and monitor the storage consumption by the logs folder. The log space required varies depending on the number of the entities to be protected and the frequency of data protection operations. If there is no sufficient disk space, the logs will not be created for the recently run operations.
Required software packages	Java 1.8.x (64-bit)IBM Java If you have upgraded JAVA to the latest version, you must ensure that the JAVA_HOME option located at <code>/var/opt/snapcenter/spl/etc/spl.properties</code> is set to the correct JAVA version and the correct path.

For the latest information about supported versions, see the [NetApp Interoperability Matrix Tool](#).

Configure sudo privileges for non-root user for AIX plug-in host

SnapCenter 4.4 and later allows a non-root user to install the SnapCenter Plug-ins Package for AIX and to start the plug-in process. You should configure sudo privileges for the non-root user to provide access to several paths.

What you will need

- Sudo 1.8.7 or later.
- Ensure that the non-root user is part of the Oracle installation group.
- Edit the `/etc/ssh/sshd_config` file to configure the message authentication code algorithms: MACs hmac-sha2-256 and MACs hmac-sha2-512.

Restart the sshd service after updating the configuration file.

Example:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

About this task

You should configure sudo privileges for the non-root user to provide access to the following paths:

- `/home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx`
- `/custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall`
- `/custom_location/NetApp/snapcenter/spl/bin/spl`

Steps

1. Log in to the AIX host on which you want to install the SnapCenter Plug-ins Package for AIX.
2. Add the following lines to the `/etc/sudoers` file by using the visudo Linux utility.

```
Cmnd_Alias SCCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
AIX_USER ALL=(ALL) NOPASSWD:SETENV: SCCMD, PRECHECKCMD
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

`AIX_USER` is the name of the non-root user that you created.

You can obtain the checksum value from the **oracle_checksum.txt** file, which is located at `C:\ProgramData\NetApp\SnapCenter\Package Repository`.

If you have specified a custom location, the location will be `custom_path\NetApp\SnapCenter\Package Repository`.



The example should be used only as a reference for creating your own data.

Best Practice: For security reasons, you should remove the sudo entry after completing every installation or upgrade.

Set up credentials for installing Plug-ins Package for Linux or AIX

SnapCenter uses credentials to authenticate users for SnapCenter operations. You should create credentials for installing the plug-in package on Linux or AIX hosts.

About this task

The credentials are created either for the root user or for a non-root user who has sudo privileges to install and start the plug-in process.

For information, see [Configure sudo privileges for Linux host](#) or [Configure sudo privileges for AIX host](#).

Best Practice: Although you are allowed to create credentials after deploying hosts and installing plug-ins, the best practice is to create credentials after you add SVMs, before you deploy hosts and install plug-ins.

Steps

1. In the left navigation pane, click **Settings**.
2. In the Settings page, click **Credential**.
3. Click **New**.
4. In the Credential page, enter the credential information:

For this field...	Do this...
Credential name	Enter a name for the credentials.

For this field...	Do this...
User name/Password	<p>Enter the user name and password that are to be used for authentication.</p> <ul style="list-style-type: none"> Domain administrator <p>Specify the domain administrator on the system on which you are installing the SnapCenter plug-in. Valid formats for the Username field are:</p> <ul style="list-style-type: none"> <i>NetBIOS\UserName</i> <i>Domain FQDN\UserName</i> Local administrator (for workgroups only) <p>For systems that belong to a workgroup, specify the built-in local administrator on the system on which you are installing the SnapCenter plug-in. You can specify a local user account that belongs to the local administrators group if the user account has elevated privileges or the User Access control feature is disabled on the host system. The valid format for the Username field is: <i>UserName</i></p>
Authentication Mode	<p>Select the authentication mode that you want to use.</p> <p>Depending on the operating system of the plug-in host, select either Linux or AIX.</p>
Use sudo privileges	<p>Select the Use sudo privileges check box if you are creating credentials for a non-root user.</p>

5. Click **OK**.

After you finish setting up the credentials, you might want to assign credential maintenance to a user or group of users on the My SnapCenter Assets page.

Configure credentials for an Oracle database

You must configure credentials that are used to perform data protection operations on Oracle databases.

About this task

You should review the different authentication methods supported for Oracle database. For information, see [Authentication methods for your credentials](#).

If you set up credentials for individual resource groups and the user name does not have full admin privileges,


the user name must at least have resource group and backup privileges.

If you have enabled Oracle database authentication, a red padlock icon is shown in the resources view. You must configure database credentials to be able to protect the database or add it to the resource group to perform data protection operations.



If you specify incorrect details while creating a credential, an error message is displayed. You must click **Cancel**, and then retry.

Steps


1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. In the Resources page, select **Database** from the **View** list.
3. Click , and then select the host name and the database type to filter the resources.

You can then click  to close the filter pane.

4. Select the database, and then click **Database Settings > Configure Database**.
5. In the Configure database settings section, from the **Use existing Credential** drop-down list, select the credential that should be used to perform data protection jobs on the Oracle database.




The Oracle user should have sysdba privileges.

You can also create a credential by clicking .

6. In the Configure ASM settings section, from the **Use existing Credential** drop-down list, select the credential that should be used to perform data protection jobs on the ASM instance.



The ASM user should have sysasm privilege.

You can also create a credential by clicking .

7. In the Configure RMAN catalog settings section, from the **Use existing credential** drop-down list, select the credential that should be used to perform data protection jobs on the Oracle Recovery Manager (RMAN) catalog database.

You can also create a credential by clicking .

In the **TNSName** field, enter the Transparent Network Substrate (TNS) file name that will be used by the SnapCenter Server to communicate with the database.

8. In the **Preferred RAC Nodes** field, specify the Real Application Cluster (RAC) nodes preferred for backup.

The preferred nodes might be one or all cluster nodes where the RAC database instances are present. The backup operation is triggered only on these preferred nodes in the order of preference.

In RAC One Node, only one node is listed in the preferred nodes, and this preferred node is the node where the database is currently hosted.

After failover or relocation of RAC One Node database, refreshing of resources in the SnapCenter Resources page will remove the host from the **Preferred RAC Nodes** list where the database was earlier hosted. The RAC node where the database is relocated will be listed in **RAC Nodes** and will need to be manually configured as the preferred RAC node.

For more information, see [Preferred nodes in RAC setup](#).

9. Click **OK**.

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

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

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

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

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

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.