



Install SnapCenter Plug-in for Unix file systems

SnapCenter Software 5.0

NetApp
July 18, 2024

This PDF was generated from https://docs.netapp.com/us-en/snapcenter-50/protect-scu/reference_prerequisites_for_adding_hosts_and_installing_snapcenter_plug_ins_package_for_linux.html on July 18, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Install SnapCenter Plug-in for Unix file systems 1
 - Prerequisites for adding hosts and installing Plug-ins Package for Linux 1
 - Add hosts and install Plug-ins Package for Linux using GUI 2
 - Configure the SnapCenter Plug-in Loader service 5
 - Configure CA certificate with SnapCenter Plug-in Loader (SPL) service on Linux host 8
 - Enable CA Certificates for plug-ins 10

Install SnapCenter Plug-in for Unix file systems

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

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

- If you are using iSCSI, the iSCSI service must be running.
- You can either use the password-based authentication for the root or non-root user or SSH key based authentication.

SnapCenter Plug-in for Unix File Systems 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 non-root user.

- Create credentials with authentication mode as Linux for the install user.
- You must have installed Java 1.8.x or Java 11, 64-bit, on your Linux host.



Ensure that you have installed only the certified edition of JAVA 11 on the Linux host.



For information to download JAVA, see: [Java Downloads for All Operating Systems](#)

- You should have **bash** as the default shell for plug-in installation.

Linux Host requirements

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• SUSE Linux Enterprise Server (SLES)
Minimum RAM for the SnapCenter plug-in on host	2 GB

Item	Requirements
Minimum install and log space for the SnapCenter plug-in on host	2 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	<ul style="list-style-type: none"> • Java 1.8.x (64-bit) Oracle Java and OpenJDK • Java 11 (64-bit) Oracle Java and OpenJDK  Ensure that you have installed only the certified edition of JAVA 11 on the Linux host. 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](#).


Add hosts and install Plug-ins Package for Linux using GUI

You can use the Add Host page to add hosts, and then install the SnapCenter Plug-ins Package for Linux. The plug-ins are automatically installed on the remote hosts.

Steps


1. In the left navigation pane, click **Hosts**.
2. Verify that the **Managed Hosts** tab is selected at the top.
3. Click **Add**.
4. In the Hosts page, perform the following actions:

For this field...	Do this...
Host Type	Select Linux as the host type.

For this field...	Do this...
Host name	<p>Enter the fully qualified domain name (FQDN) or the IP address of the host.</p> <p>SnapCenter depends on the proper configuration of the DNS. Therefore, the best practice is to enter the FQDN.</p> <p>If you are adding a host by using SnapCenter and the host is part of a subdomain, you must provide the FQDN.</p>
Credentials	<p>Either select the credential name that you created or create new credentials.</p> <p>The credential must have administrative rights on the remote host. For details, see the information about creating credentials.</p> <p>You can view details about the credentials by positioning the cursor over the credential name that you specified.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  <p>The credentials authentication mode is determined by the host type that you specify in the Add Host wizard.</p> </div>

5. In the Select Plug-ins to Install section, select **Unix File Systems**.

6. (Optional) Click **More Options**.

For this field...	Do this...
Port	<p>Either retain the default port number or specify the port number.</p> <p>The default port number is 8145. If the SnapCenter Server was installed on a custom port, that port number will be displayed as the default port.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  <p>If you manually installed the plug-ins and specified a custom port, you must specify the same port. Otherwise, the operation fails.</p> </div>
Installation Path	<p>The default path is <i>/opt/NetApp/snapcenter</i>.</p> <p>You can optionally customize the path. If you use the custom path, ensure that the default content of the sudoers is updated with the custom path.</p>

For this field...	Do this...
Skip optional preinstall checks	Select this check box if you have already installed the plug-ins manually and you do not want to validate whether the host meets the requirements for installing the plug-in.

7. Click **Submit**.

If you have not selected the Skip prechecks checkbox, the host is validated to verify whether the host meets the requirements for installing the plug-in.



The precheck script does not validate the plug-in port firewall status if it is specified in the firewall reject rules.

Appropriate error or warning messages are displayed if the minimum requirements are not met. If the error is related to disk space or RAM, you can update the web.config file located at *C:\Program Files\NetApp\SnapCenter WebApp* to modify the default values. If the error is related to other parameters, you should fix the issue.



In an HA setup, if you are updating web.config file, you must update the file on both nodes.

8. Verify the fingerprint, and then click **Confirm and Submit**.



SnapCenter does not support ECDSA algorithm.



Fingerprint verification is mandatory even if the same host was added earlier to SnapCenter and the fingerprint was confirmed.

9. Monitor the installation progress.

The installation-specific log files are located at */custom_location/snapcenter/logs*.

Result

All the file systems mounted on the host are automatically discovered and displayed under the Resources Page. If nothing is displayed, click **Refresh Resources**.



Monitor installation status

You can monitor the progress of SnapCenter plug-in package installation by using the Jobs page. You might want to check the progress of installation to determine when it is complete or if there is an issue.

About this task

The following icons appear on the Jobs page and indicate the state of the operation:

- In progress
- Completed successfully
- Failed

-  Completed with warnings or could not start due to warnings
-  Queued

Steps

1. In the left navigation pane, click **Monitor**.
2. In the **Monitor** page, click **Jobs**.
3. In the **Jobs** page, to filter the list so that only plug-in installation operations are listed, do the following:
 - a. Click **Filter**.
 - b. Optional: Specify the start and end date.
 - c. From the Type drop-down menu, select **Plug-in installation**.
 - d. From the Status drop-down menu, select the installation status.
 - e. Click **Apply**.
4. Select the installation job and click **Details** to view the job details.
5. In the **Job Details** page, click **View logs**.

Configure the SnapCenter Plug-in Loader service

The SnapCenter Plug-in Loader service loads the plug-in package for Linux to interact with the SnapCenter Server. The SnapCenter Plug-in Loader service is installed when you install the SnapCenter Plug-ins Package for Linux.



About this task

After installing the SnapCenter Plug-ins Package for Linux, the SnapCenter Plug-in Loader service starts automatically. If the SnapCenter Plug-in Loader service fails to start automatically, you should:

- Ensure that the directory where the plug-in is operating is not deleted
- Increase the memory space allotted to the Java Virtual Machine

The `spl.properties` file, which is located at `/custom_location/NetApp/snapcenter/spl/etc/`, contains the following parameters. Default values are assigned to these parameters.

Parameter name	Description
LOG_LEVEL	Displays the log levels that are supported. The possible values are TRACE, DEBUG, INFO, WARN, ERROR, and FATAL.
SPL_PROTOCOL	Displays the protocol that is supported by SnapCenter Plug-in Loader. Only the HTTPS protocol is supported. You can add the value if the default value is missing.

Parameter name	Description
SNAPCENTER_SERVER_PROTOCOL	<p>Displays the protocol that is supported by SnapCenter Server.</p> <p>Only the HTTPS protocol is supported. You can add the value if the default value is missing.</p>
SKIP_JAVAHOME_UPDATE	<p>By default, the SPL service detects the java path and update JAVA_HOME parameter.</p> <p>Therefore the default value is set to FALSE. You can set to TRUE if you want to disable the default behavior and manually fix the java path.</p>
SPL_KEYSTORE_PASS	<p>Displays the password of the keystore file.</p> <p>You can change this value only if you change the password or create a new keystore file.</p>
SPL_PORT	<p>Displays the port number on which the SnapCenter Plug-in Loader service is running.</p> <p>You can add the value if the default value is missing.</p> <div style="display: flex; align-items: center;">  <p>You should not change the value after installing the plug-ins.</p> </div>
SNAPCENTER_SERVER_HOST	<p>Displays the IP address or host name of the SnapCenter Server.</p>
SPL_KEYSTORE_PATH	<p>Displays the absolute path of the keystore file.</p>
SNAPCENTER_SERVER_PORT	<p>Displays the port number on which the SnapCenter Server is running.</p>
LOGS_MAX_COUNT	<p>Displays the number of SnapCenter Plug-in Loader log files that are retained in the <i>/custom_location/snapcenter/spl/logs</i> folder.</p> <p>The default value is set to 5000. If the count is more than the specified value, then the last 5000 modified files are retained. The check for the number of files is done automatically every 24 hours from when SnapCenter Plug-in Loader service is started.</p> <div style="display: flex; align-items: center;">  <p>If you manually delete the <i>spl.properties</i> file, then the number of files to be retained is set to 9999.</p> </div>

Parameter name	Description
JAVA_HOME	Displays the absolute directory path of the JAVA_HOME which is used to start SPL service. This path is determined during installation and as part of starting SPL.
LOG_MAX_SIZE	Displays the maximum size of the job log file. Once the maximum size is reached, the log file is zipped, and the logs are written into the new file of that job.
RETAIN_LOGS_OF_LAST_DAYS	Displays the number of days up to which the logs are retained.
ENABLE_CERTIFICATE_VALIDATION	Displays true when CA certificate validation is enabled for the host. You can enable or disable this parameter either by editing the spl.properties or by using the SnapCenter GUI or cmdlet.

If any of these parameters are not assigned to the default value or if you want to assign or change the value, then you can modify the spl.properties file. You can also verify the spl.properties file and edit the file to troubleshoot any issues related to the values that are assigned to the parameters. After you modify the spl.properties file, you should restart the SnapCenter Plug-in Loader service.

Steps

1. Perform one of the following actions, as required:

- Start the SnapCenter Plug-in Loader service:

- As a root user, run: `/custom_location/NetApp/snapcenter/spl/bin/spl start`
- As a non-root user, run: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`

- Stop the SnapCenter Plug-in Loader service:

- As a root user, run: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
- As a non-root user, run: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`



You can use the `-force` option with the stop command to stop the SnapCenter Plug-in Loader service forcefully. However, you should use caution before doing so because it also terminates the existing operations.

- Restart the SnapCenter Plug-in Loader service:

- As a root user, run: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`

- As a non-root user, run: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
- Find the status of the SnapCenter Plug-in Loader service:
 - As a root user, run: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
 - As a non root user, run: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
- Find the change in the SnapCenter Plug-in Loader service:
 - As a root user, run: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
 - As a non-root user, run: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Configure CA certificate with SnapCenter Plug-in Loader (SPL) service on Linux host

You should manage the password of SPL keystore and its certificate, configure the CA certificate, configure root or intermediate certificates to SPL trust-store, and configure CA signed key pair to SPL trust-store with SnapCenter Plug-in Loader service to activate the installed digital certificate.



SPL uses the file 'keystore.jks', which is located at '/var/opt/snapcenter/spl/etc' both as its trust-store and key-store.

Manage password for SPL keystore and alias of the CA signed key pair in use

Steps

1. You can retrieve SPL keystore default password from SPL property file.

It is the value corresponding to the key 'SPL_KEYSTORE_PASS'.

2. Change the keystore password:

```
keytool -storepasswd -keystore keystore.jks
```

3. Change the password for all aliases of private key entries in the keystore to the same password used for the keystore:

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

Update the same for the key SPL_KEYSTORE_PASS in spl.properties file.

4. Restart the service after changing the password.



Password for SPL keystore and for all the associated alias password of the private key should be same.

Configure root or intermediate certificates to SPL trust-store

You should configure the root or intermediate certificates without the private key to SPL trust-store.

Steps

1. Navigate to the folder containing the SPL keystore: */var/opt/snapcenter/spl/etc*.
2. Locate the file 'keystore.jks'.
3. List the added certificates in the keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Add a root or intermediate certificate:

```
keytool -import -trustcacerts -alias <AliasNameForCertificateToBeImported>  
-file /<CertificatePath> -keystore keystore.jks
```

5. Restart the service after configuring the root or intermediate certificates to SPL trust-store.



You should add the root CA certificate and then the intermediate CA certificates.

Configure CA signed key pair to SPL trust-store

You should configure the CA signed key pair to the SPL trust-store.

Steps

1. Navigate to the folder containing the SPL's keystore */var/opt/snapcenter/spl/etc*.
2. Locate the file 'keystore.jks'.
3. List the added certificates in the keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Add the CA certificate having both private and public key.

```
keytool -importkeystore -srckeystore <CertificatePathToImport>  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. List the added certificates in the keystore.

```
keytool -list -v -keystore keystore.jks
```

6. Verify that the keystore contains the alias corresponding to the new CA certificate, which was added to the keystore.
7. Change the added private key password for CA certificate to the keystore password.

Default SPL keystore password is the value of the key `SPL_KEYSTORE_PASS` in `spl.properties` file.

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks
```

8. If the alias name in the CA certificate is long and contains space or special characters ("*", ",",), change the alias name to a simple name:

```
keytool -changealias -alias "<OriginalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks
```

9. Configure the alias name from the keystore located in `spl.properties` file.

Update this value against the key `SPL_CERTIFICATE_ALIAS`.

10. Restart the service after configuring the CA signed key pair to SPL trust-store.

Configure certificate revocation list (CRL) for SPL

You should configure the CRL for SPL

About this task

- SPL will look for the CRL files in a pre-configured directory.
- Default directory for the CRL files for SPL is `/var/opt/snapcenter/spl/etc/crl`.

Steps

1. You can modify and update the default directory in `spl.properties` file against the key `SPL_CRL_PATH`.
2. You can place more than one CRL file in this directory.

The incoming certificates will be verified against each CRL.

Enable CA Certificates for plug-ins

You should configure the CA certificates and deploy the CA certificates in the SnapCenter Server and the corresponding plug-in hosts. You should enable the CA certificate validation for the plug-ins.

Before you begin

- You can enable or disable the CA certificates using the run *Set-SmCertificateSettings* cmdlet.
- You can display the certificate status for the plug-ins using the *Get-SmCertificateSettings*.





The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the [SnapCenter Software Cmdlet Reference Guide](#).

Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **Managed Hosts**.
3. Select single or multiple plug-in hosts.
4. Click **More options**.
5. Select **Enable Certificate Validation**.

After you finish

The Managed Hosts tab host displays a padlock and the color of the padlock indicates the status of the connection between SnapCenter Server and the plug-in host.

-  indicates that the CA certificate is neither enabled nor assigned to the plug-in host.
-  indicates that the CA certificate is successfully validated.
-  indicates that the CA certificate could not be validated.
-  indicates that the connection information could not be retrieved.



When the status is yellow or green, the data protection operations completes successfully.

Copyright information

Copyright © 2024 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.