



# **SnapCenter Plug-in for Unixファイルシステムのインストール**

## **SnapCenter Software 5.0**

NetApp  
April 04, 2024

This PDF was generated from [https://docs.netapp.com/ja-jp/snapcenter/protect-scu/reference\\_prerequisites\\_for\\_adding\\_hosts\\_and\\_installing\\_snapcenter\\_plug\\_ins\\_package\\_for\\_linux.html](https://docs.netapp.com/ja-jp/snapcenter/protect-scu/reference_prerequisites_for_adding_hosts_and_installing_snapcenter_plug_ins_package_for_linux.html) on April 04, 2024. Always check docs.netapp.com for the latest.

# 目次

SnapCenter Plug-in for Unixファイルシステムのインストール .....	1
ホストを追加してPlug-ins Package for Linuxをインストールするための前提条件 .....	1
GUIを使用したホストの追加とPlug-ins Package for Linuxのインストール .....	2
SnapCenter Plug-in Loader サービスを設定します .....	5
Linux ホストに SnapCenter Plug-in Loader （SPL）サービスを使用して CA 証明書を設定します .....	8
プラグインの CA 証明書を有効にします .....	11

# SnapCenter Plug-in for Unixファイルシステムのインストール

## ホストを追加してPlug-ins Package for Linuxをインストールするための前提条件

ホストを追加してLinux用のプラグインパッケージをインストールする前に、すべての要件を満たしておく必要があります。

- iSCSI を使用している場合は、iSCSI サービスが実行されている必要があります。
- rootユーザまたはroot以外のユーザ、またはSSHキーベースの認証にはパスワードベースの認証を使用できます。

SnapCenter Plug-in for Unix File Systemsは、root以外のユーザがインストールできます。ただし、プラグインプロセスをインストールして開始できるように root 以外のユーザに sudo 権限を設定する必要があります。プラグインをインストールすると、有効なroot以外のユーザとしてプロセスが実行されるようになります。

- インストールユーザのクレデンシャルを、認証モードをLinuxに設定して作成します。
- Java 1.8.xまたはJava 11（64ビット）をLinuxホストにインストールしておく必要があります。



LinuxホストにJava 11の認定エディションのみがインストールされていることを確認します。

Java のダウンロード方法については、次を参照してください。"[すべてのオペレーティングシステム用のJava のダウンロード](#)"

- プラグインのインストールには、デフォルトのシェルとして\* bash \*が必要です。

### Linux ホストの要件

SnapCenter Plug-ins Package for Linux をインストールする前に、ホストが要件を満たしていることを確認する必要があります。

項目	要件
オペレーティングシステム	<ul style="list-style-type: none"><li>• Red Hat Enterprise Linux の場合</li><li>• Oracle Linux の場合</li><li>• SUSE Linux Enterprise Server （ SLES ）</li></ul>
ホスト上の SnapCenter プラグインの最小 RAM	2 GB

項目	要件
ホスト上の SnapCenter プラグインのインストールおよびログの最小スペース	2 GB <div>  <p>十分なディスクスペースを割り当て、logs フォルダによるストレージ消費を監視する必要があります。必要なログスペースは、保護するエンティティの数とデータ保護処理の頻度によって異なります。十分なディスクスペースがない場合、最近実行した処理に対してログは作成されません。</p> </div>
必要なソフトウェアパッケージ	<ul style="list-style-type: none"> <li>• Java 1.8.x (64ビット) Oracle JavaおよびOpenJDK</li> <li>• Java 11 (64ビット) Oracle JavaおよびOpenJDK</li> </ul> <div>  <p>LinuxホストにJava 11の認定エディションのみがインストールされていることを確認します。</p> </div> <p>Java を最新バージョンにアップグレードした場合は、/var/opt/snapcenter/etc/sp/etc/spl.properties にある JAVA_HOME オプションが正しい Java バージョンに設定されていること、および正しいパスが指定されていることを確認する必要があります。</p>

サポートされているバージョンの最新情報については、を参照してください ["NetApp Interoperability Matrix Tool で確認できます"](#)。

## GUIを使用したホストの追加とPlug-ins Package for Linuxのインストール


[ホストの追加]ページを使用してホストを追加し、SnapCenter Plug-ins Package for Linuxをインストールできます。プラグインは、自動的にリモートホストにインストールされます。

### • 手順 \*

1. 左側のナビゲーションペインで、\* Hosts \* (ホスト) をクリックします。
2. 上部で [Managed Hosts] タブが選択されていることを確認します。
3. [追加 (Add)] をクリックします。
4. Hosts ページで、次の操作を実行します。

フィールド	手順
ホストタイプ	ホストタイプとして* Linux *を選択します。
ホスト名	<p>ホストの完全修飾ドメイン名（FQDN）または IP アドレスを入力します。</p> <p>SnapCenter は、DNS の適切な設定によって異なります。そのため、FQDN を入力することを推奨します。</p> <p>SnapCenter を使用してホストを追加する際、ホストがサブドメインの一部である場合は、FQDN を指定する必要があります。</p>
クレデンシャル	<p>作成したクレデンシャル名を選択するか、新しいクレデンシャルを作成します。</p> <p>このクレデンシャルには、リモートホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。</p> <p>クレデンシャルの詳細を表示するには、指定したクレデンシャル名にカーソルを合わせます。</p> <div>  <p>クレデンシャル認証モードは、ホストの追加ウィザードで指定したホストタイプによって決まります。</p> </div>

5. [Select Plug-ins to Install]セクションで、\*[Unix File Systems]\*を選択します。
6. （オプション） \* その他のオプション \* をクリックします。

フィールド	手順
ポート	<p>デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。</p> <p>デフォルトのポート番号は 8145 です。SnapCenter サーバがカスタムポートにインストールされている場合は、そのポート番号がデフォルトポートとして表示されます。</p> <div>  <p>プラグインを手動でインストールし、カスタムポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理は失敗します。</p> </div>

フィールド	手順
インストールパス	<p>デフォルトパスは、 <code>_/opt/NetApp/snapcenter _</code> です。</p> <p>必要に応じて、パスをカスタマイズできます。カスタムパスを使用する場合は、<code>sudoers</code>のデフォルトのコンテンツがカスタムパスで更新されていることを確認してください。</p>
オプションのプレインストールチェックを省略します	<p>プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、このチェックボックスを選択します。</p>

7. [Submit（送信）] をクリックします。

[ 事前確認をスキップする ] チェックボックスを選択していない場合、ホストがプラグインのインストール要件を満たしているかどうかを検証されます。



ファイアウォールの拒否ルールで指定されているプラグインポートのファイアウォールステータスは、事前確認スクリプトで検証されません。

最小要件を満たしていない場合は、該当するエラーまたは警告メッセージが表示されます。エラーがディスクスペースまたは RAM に関連している場合は、`C : \Program Files\NetApp\Virtual\SnapCenter WebApp` にある `web.config` ファイルを更新してデフォルト値を変更できます。エラーが他のパラメータに関連する場合は、問題を修正する必要があります。



HA セットアップで `web.config` ファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

8. 指紋を確認し、 \* 確認して送信 \* をクリックします。



SnapCenter は ECDSA アルゴリズムをサポートしていません。



同じホストを以前に SnapCenter に追加し、フィンガープリントを確認した場合でも、フィンガープリントの検証は必須です。

1. インストールの進行状況を監視します。

インストール固有のログファイルは、 `_ / custom_location / snapcenter / log_` にあります。

• 結果 \*






ホストにマウントされているすべてのファイルシステムが自動的に検出され、[Resources] ページに表示されます。何も表示されない場合は、 \* リソースを更新 \* をクリックします。

## インストールステータスを監視する

SnapCenter プラグインパッケージのインストールの進捗状況は、Jobs ページで監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題があるかどうかを確認できます。

このタスクについて

以下のアイコンがジョブページに表示され、操作の状態を示します。

-  実行中です
-  正常に完了しました
-  失敗しました
-  警告で終了したか、警告が原因で起動できませんでした
-  キューに登録され

手順

1. 左側のナビゲーションペインで、**Monitor** をクリックします。
2. [\* Monitor\*] ページで、[\* Jobs] をクリックします。
3. [ジョブ]ページで、プラグインのインストール処理のみが表示されるようにリストをフィルタリングするには、次の手順を実行します。
  - a. [\* フィルタ\* (Filter\*) ] をクリック
  - b. オプション：開始日と終了日を指定します。
  - c. タイプドロップダウンメニューから、\* プラグインインストール\* を選択します。
  - d. Status ドロップダウンメニューから、インストールステータスを選択します。
  - e. [ 適用 (Apply) ] をクリックします。
4. インストールジョブを選択し、[\* 詳細\*] をクリックしてジョブの詳細を表示します。
5. [\* ジョブの詳細\*] ページで、[\* ログの表示\*] をクリックします。

## SnapCenter Plug-in Loader サービスを設定します

SnapCenter Plug-in Loaderサービスは、SnapCenterサーバと対話するために、Linux用のプラグインパッケージをロードします。SnapCenter Plug-in Loaderサービスは、SnapCenter Plug-ins Package for Linuxをインストールするとインストールされます。

- このタスクについて \*

SnapCenter Plug-ins Package for Linuxをインストールすると、SnapCenter Plug-in Loaderサービスが自動的に開始されます。SnapCenter Plug-in Loader サービスが自動的に開始されない場合は、次のことをする必要があります。

- プラグインが動作しているディレクトリが削除されていないことを確認してください
- Java 仮想マシンに割り当てられているメモリ容量を増やします

spl.properties ファイルは、`/custom_location/NetApp/snapcenter /spl/etc/` にあり、次のパラメータを含みます。これらのパラメータにはデフォルト値が割り当てられています。

パラメータ名	説明
LOG_LEVEL の値	<p>サポートされるログレベルを表示します。</p> <p>指定できる値は、trace、debug、info、warn、error、致命的だ</p>
SPL プロトコル	<p>SnapCenter Plug-in Loader でサポートされているプロトコルを表示します。</p> <p>HTTPS プロトコルのみがサポートされています。デフォルト値がない場合は、値を追加できます。</p>
SNAPCENTER_server_protocol」を参照してください	<p>SnapCenter サーバでサポートされているプロトコルを表示します。</p> <p>HTTPS プロトコルのみがサポートされています。デフォルト値がない場合は、値を追加できます。</p>
ske_JAVAHOME_update を実行します	<p>デフォルトでは、SPL サービスは Java パスを検出し、JAVA_HOME パラメータを更新します。</p> <p>したがって、デフォルト値は FALSE に設定されません。デフォルトの動作を無効にして Java パスを手動で修正する場合は、true に設定します。</p>
SPL キーストアパス	<p>キーストアファイルのパスワードを表示します。</p> <p>この値は、パスワードを変更する場合や新しいキーストアファイルを作成する場合にのみ変更できます。</p>
SPL ポート	<p>SnapCenter Plug-in Loader サービスが実行されているポート番号を表示します。</p> <p>デフォルト値がない場合は、値を追加できます。</p> <div> プラグインのインストール後は値を変更しないでください。</div>
SNAPCENTER_server_host が必要です	<p>SnapCenter サーバの IP アドレスまたはホスト名を表示します。</p>
SPL キーストアパス	<p>キーストアファイルの絶対パスを表示します。</p>



パラメータ名	説明
SNAPCENTER_SERVER_PORT	SnapCenter サーバが稼働しているポート番号を表示します。
logs_MAX_COUNT	<p>SnapCenter Plug-in Loader ログファイルのうち、 _/_custom_location/snapcenter /spl/logs_folder に保持されているファイルの数を表示します。</p> <p>デフォルト値は 5000 に設定されています。指定した値よりも多い数のファイルがある場合は、変更後の最新の 5000 個のファイルが保持されます。ファイル数のチェックは、SnapCenter Plug-in Loader サービスが開始されたときから 24 時間ごとに自動的に行われます。</p> <div>  <p>spl.properties ファイルを手動で削除すると、保持されるファイル数は 9999 に設定されます。</p> </div>
JAVA_HOME にアクセスします	<p>SPL サービスの開始に使用される JAVA_HOME の絶対ディレクトリパスを表示します。</p> <p>このパスは、インストール時および SPL の開始時に決定されます。</p>
LOG_MAX_SIZE	<p>ジョブログファイルの最大サイズを表示します。</p> <p>最大サイズに達すると、ログファイルが圧縮され、そのジョブの新しいファイルにログが書き込まれます。</p>
retain_logs_of_last_days	ログを保持する日数が表示されます。
enable_certificate_validationを実行します	<p>ホストでCA証明書の検証が有効になっている場合はtrueと表示されます。</p> <p>このパラメータを有効または無効にするには、spl.propertiesを編集するか、SnapCenter GUIまたはコマンドレットを使用します。</p>

これらのパラメータのいずれかがデフォルト値に割り当てられていない場合、または値を割り当てたり変更したりする場合は、spl.properties ファイルを変更します。また、spl.properties ファイルを確認して編集し、パラメータに割り当てられている値に関連する問題のトラブルシューティングを行うこともできます。spl.properties ファイルを変更したら、SnapCenter Plug-in Loader サービスを再起動する必要があります。

• 手順 \*

1. 必要に応じて、次のいずれかの操作を実行します。

- SnapCenter Plug-in Loaderサービスを開始します。
  - rootユーザとして、次のコマンドを実行します。  
`/custom_location/NetApp/snapcenter/spl/bin/spl start`
  - root以外のユーザとして、次のコマンドを実行します。 `sudo`  
`/custom_location/NetApp/snapcenter/spl/bin/spl start`
- SnapCenter Plug-in Loader サービスを停止します。
  - rootユーザとして、次のコマンドを実行します。  
`/custom_location/NetApp/snapcenter/spl/bin/spl stop`
  - root以外のユーザとして、次のコマンドを実行します。 `sudo`  
`/custom_location/NetApp/snapcenter/spl/bin/spl stop`



stop コマンドに `-force` オプションを指定すると、SnapCenter Plug-in Loader サービスを強制的に停止できます。ただし、既存の処理が終了するため、実行する前に十分に注意する必要があります。

- SnapCenter Plug-in Loader サービスを再起動します。
  - rootユーザとして、次のコマンドを実行します。  
`/custom_location/NetApp/snapcenter/spl/bin/spl restart`
  - root以外のユーザとして、次のコマンドを実行します。 `sudo`  
`/custom_location/NetApp/snapcenter/spl/bin/spl restart`
- SnapCenter Plug-in Loader サービスのステータスを確認します。
  - rootユーザとして、次のコマンドを実行します。  
`/custom_location/NetApp/snapcenter/spl/bin/spl status`
  - root以外のユーザとして、次のコマンドを実行します。 `sudo`  
`/custom_location/NetApp/snapcenter/spl/bin/spl status`
- SnapCenter Plug-in Loader サービスで変更を探します。
  - rootユーザとして、次のコマンドを実行します。  
`/custom_location/NetApp/snapcenter/spl/bin/spl change`
  - root以外のユーザとして、次のコマンドを実行します。 `sudo`  
`/custom_location/NetApp/snapcenter/spl/bin/spl change`

## Linux ホストに SnapCenter Plug-in Loader （SPL）サービスを使用して CA 証明書を設定します

SPL キーストアとその証明書のパスワードを管理し、CA 証明書を設定し、ルート証明書または中間証明書を SPL の信頼ストアに設定し、CA 署名キーペアを SPL の信頼ストアと SnapCenter Plug-in Loader サービスを使用して設定して、インストールされたデジタル証明書をアクティブ化する必要があります。



SPL は、ファイル 'keystore.jks' を使用します。このファイルは、'/var/opt/snapcenter /spl/etc' にあり、どちらもトラストストアおよびキーストアとして使用されます。

## SPL キーストアのパスワードと使用中の **CA** 署名済みキーペアのエイリアスを管理します

### • 手順 \*

1. SPL プロパティファイルから SPL キーストアのデフォルトパスワードを取得できます。

これはキー 'PL\_keystore.pass' に対応する値です。

2. キーストアのパスワードを変更します。

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

・ キーストア内の秘密鍵エントリのすべてのエイリアスのパスワードを、キーストアに使用されているパスワードと同じパスワードに変更します。

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

spl.properties ファイル内のキー SPL の \_keystore.pass に対しても同じ内容を更新します。

3. パスワードを変更したら、サービスを再起動してください。



SPL キーストアのパスワードと秘密鍵に関連付けられているすべてのエイリアスパスワードが同じである必要があります。

## ルート証明書または中間証明書を **SPL** の信頼ストアに設定します

SPL の信頼ストアへの秘密鍵を使用せずにルート証明書または中間証明書を設定する必要があります。

### • 手順 \*

1. SPL キーストアが格納されているフォルダ（ /var/opt/snapcenter /spl/etc\_ ）に移動します。
2. ファイル 'keystore.jks' を探します。
3. キーストアに追加された証明書を表示します。

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

・ ルート証明書または中間証明書を追加します。

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

・ SPL

の信頼ストアにルート証明書または中間証明書を設定したら、サービスを再起動します。



ルート CA 証明書、中間 CA 証明書の順に追加する必要があります。

## CA 署名キーペアを SPL の信頼ストアに設定します

CA 署名鍵ペアを SPL 信頼ストアに設定する必要があります。

### • 手順 \*

1. SPL のキーストア `/var/opt/snapcenter /spl/` などを含むフォルダに移動します
2. ファイル 'keystore.jks' を探します。
3. キーストアに追加された証明書を表示します。

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

． 秘密鍵と公開鍵の両方を含む CA 証明書を追加します。

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

． キーストアに追加された証明書を表示します。

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

． キーストアに、キーストアに追加された新しい CA 証明書に対応するエイリアスが含まれていることを確認します。  
． CA 証明書用に追加された秘密鍵のパスワードをキーストアのパスワードに変更します。

デフォルトの SPL キーストアパスワードは、`spl.properties` ファイル内のキー SPL の `keystore.pass` の値です。

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

． CA 証明書のエイリアス名が長く、スペースまたは特殊文字（「`*`」、「`」`」、「`」`」）が含まれている場合は、エイリアス名を単純な名前に変更します。

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

． `spl.properties` ファイルにあるキーストアからエイリアス名を設定します。

この値をキー SPL の `certificate_alias` に更新します。

4. CA 署名済みキーペアを SPL 信頼ストアに設定したら、サービスを再起動します。

## SPL の証明書失効リスト（CRL）を設定します

SPL 用に CRL を設定する必要があります

- このタスクについて \*
- SPL は、事前に設定されたディレクトリ内の CRL ファイルを検索します。
- SPL の CRL ファイルのデフォルトディレクトリは、`_var/opt/snapcenter /spl/etc/crl_`です。
- 手順 \*
- 1. `spl.properties` ファイル内のデフォルトディレクトリを、キー `SPL_CRL_PATH` に対して変更および更新できます。
- 2. このディレクトリに複数の CRL ファイルを配置できます。

着信証明書は各 CRL に対して検証されます。

## プラグインの CA 証明書を有効にします

CA 証明書を設定し、SnapCenter サーバと対応するプラグインホストに CA 証明書を導入する必要があります。プラグインの CA 証明書検証を有効にする必要があります。

作業を開始する前に

- CA 証明書を有効または無効にするには、`run_Set-SmCertificateSetting_cmdlet` を使用します。
- このプラグインの証明書ステータスは、`Get-SmCertificateSettings` を使用して表示できます。





コマンドレットで使用できるパラメータとその説明については、`RUN_Get-Help コマンド NAME` を実行して参照できます。または、を参照することもできます ["SnapCenter ソフトウェアコマンドレットリファレンスガイド"](#)。

手順

1. 左側のナビゲーションペインで、`* Hosts *`（ホスト）をクリックします。
2. [Hosts] ページで、`[*Managed Hosts]` をクリックします。
3. 1 つまたは複数のプラグインホストを選択します。
4. `[* その他のオプション *]` をクリックします。
5. `[ 証明書の検証を有効にする ]` を選択します。

完了後

管理対象ホストタブのホストには鍵が表示され、SnapCenter サーバとプラグインホストの間の接続のステータスが南京錠の色で示されます。

-  は、CA 証明書が有効になっておらず、プラグインホストにも割り当てられていないことを示します。
-  CA 証明書が正常に検証されたことを示します。
-  は、CA 証明書を検証できなかったことを示します。
-  接続情報を取得できなかったことを示します。



ステータスが黄色または緑のときは、データ保護処理が正常に完了しています。

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。