



Linuxホストでの双方向SSL通信の設定と有効化

SnapCenter Software 6.0

NetApp
July 23, 2024

目次

Linuxホストでの双方向SSL通信の設定と有効化.....	1
Linuxホストでの双方向SSL通信の設定.....	1
LinuxホストでSSL通信を有効にする.....	2

Linuxホストでの双方向SSL通信の設定と有効化

Linuxホストでの双方向SSL通信の設定

双方向SSL通信を設定して、Linuxホスト上のSnapCenterサーバとプラグインの間の相互通信を保護する必要があります。

作業を開始する前に

- LinuxホストのCA証明書を設定しておく必要があります。
- すべてのプラグインホストとSnapCenterサーバで双方向SSL通信を有効にしておく必要があります。

手順


1. `certificate.pem` *を `/etc/pki/ca-trust/source/anchors/` にコピーします。
2. Linuxホストの信頼リストに証明書を追加します。
 - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
 - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
 - `update-ca-trust extract`
3. 証明書が信頼リストに追加されたかどうかを確認します。 `trust list | grep "<CN of your certificate>"`
4. SnapCenter * `nginx` ファイルの `ssl_certificate` と `ssl_certificate_key` *を更新して再起動してください。
 - `vim /etc/nginx/conf.d/snapcenter.conf`
 - `systemctl restart nginx`
5. SnapCenterサーバGUIリンクを更新します。
6. `<installation path>/NetApp/snapcenter/SnapManagerWeb_` および * `SMCoreServiceHost.dll.config` * (`<installation path>/NetApp/snapcenter/SMCore_`) で次のキーの値を更新します。
 - `<add key="SERVICE_CERTIFICATE_PATH" value="<path of certificate.pfx>" />`
 - `<add key="SERVICE_CERTIFICATE_PASSWORD" value="<password>" />`
7. 次のサービスを再起動します。
 - `systemctl restart smcore.service`
 - `systemctl restart snapmanagerweb.service`
8. 証明書がSnapManager Webポートに接続されていることを確認します。 `openssl s_client -connect localhost:8146 -brief`
9. 証明書がsmcoreポートに接続されていることを確認します。 `openssl s_client -connect localhost:8145 -brief`
10. SPLキーストアとエイリアスのパスワードを管理します。
 - a. SPLプロパティファイルの* `spl_keystore_pass` *キーに割り当てられたSPLキーストアのデフォルトパスワードを取得します。
 - b. キーストアのパスワードを変更します。 `keytool -storepasswd -keystore keystore.jks`

- c. 秘密鍵エントリのすべてのエイリアスのパスワードを変更します。 `keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
 - d. `_spl.properties_`のキー* `spl_keystore_pass` *と同じパスワードを更新します。
 - e. サービスを再起動します。
11. プラグインLinuxホストで、SPLプラグインのキーストアにルート証明書と中間証明書を追加します。
- `keytool -import -trustcacerts -alias <any preferred alias name> -file <path of root-ca.pem> -keystore <path of keystore.jks mentioned in spl.properties file>`
 - `keytool -importkeystore -srckeystore <path of certificate.pfx> -srcstoretype pkcs12 -destkeystore <path of keystore.jks mentioned in spl.properties file> -deststoretype JKS`
 - i. `keystore.jks`のエントリを確認します。 `keytool -list -v -keystore <path to keystore.jks>`
 - ii. 必要に応じてエイリアスの名前を変更します。 `keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas`
12. `_spl.properties_`ファイルの* `spl_certificate_alias` の値を **keystore.jks** に格納されている `certificate.pfx` *のエイリアスで更新し、SPLサービスを再起動します。 `systemctl restart spl`
13. 証明書がsmcoreポートに接続されていることを確認します。 `openssl s_client -connect localhost:8145 -brief`

LinuxホストでSSL通信を有効にする

PowerShellコマンドを使用して双方向SSL通信を有効にすると、Linuxホスト上のSnapCenterサーバとプラグインの間の相互通信を保護できます。

ステップ

1. 一方向SSL通信を有効にするには、次の手順を実行します。
 - a. SnapCenter GUIにログインします。
 - b. >[グローバル設定]をクリックし、[SnapCenterサーバーで証明書の検証を有効にする]*を選択します。
 - c. >[管理対象ホスト]*をクリックし、一方向SSLを有効にするプラグインホストを選択します。
 - d. アイコンをクリックし 、*[証明書の検証を有効にする]*をクリックします。
2. SnapCenterサーバLinuxホストからの双方向SSL通信を有効にします。
 - `Open-SmConnection`
 - `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName <Plugin Host Name>`
 - `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName localhost`
 - `Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}`

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。