Windowsホストでの双方向SSL通信の設定と有効化

SnapCenter software

NetApp
November 06, 2025

目次

Windowsホストでの双方向SSL通信の設定と有効化

Windowsホストでの双方向SSL通信の設定

Windowsホスト上のSnapCenter Serverとプラグインの間の相互通信を保護するために、双方向SSL通信を設定する必要があります。

開始する前に

- サポートされるキーの最小長が3072のCA証明書CSRファイルを生成しておく必要があります。
- CA証明書でサーバ認証とクライアント認証がサポートされている必要があります。
- 秘密キーとサムプリントの詳細が記載されたCA証明書が必要です。
- 一方向SSL設定を有効にしておく必要があります。

  詳細については、 "CA 証明書セクションを構成します。"

- すべてのプラグイン ホストとSnapCenter Serverで双方向SSL通信を有効にしておく必要があります。

  双方向SSL通信が一部のホストまたはサーバで有効になっていない環境はサポートされていません。

手順

1. ポートをバインドするには、SnapCenter Serverホストで次の手順を実行します。この手順はPowerShellコマンドを使用してSnapCenter IIS Webサーバのポート8146（デフォルト）で行ったあと、SMCoreポート8145（デフォルト）でも行います。

   a. 次のPowerShellコマンドを使用して、既存のSnapCenter自己署名証明書のポート バインドを削除します。

      ```
      > netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
      ```

      次に例を示します。

      ```
      > netsh http delete sslcert ipport=0.0.0.0:8145

      > netsh http delete sslcert ipport=0.0.0.0:8146
      ```

   b. 新しく取得したCA証明書をSnapCenter ServerとSMCoreポートにバインドします。

      ```
      > $cert = "<CA_certificate thumbprint>"

      > $guid = [guid]::NewGuid().ToString("B")

      > netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>
      certhash=$cert appid="$guid" clientcertnegotiation=enable
      verifyclientcertrevocation=disable

      > netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
      ```

      次に例を示します。

```
> $cert = "abc123abc123abc123abc123"

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:8146

> netsh http show sslcert ipport=0.0.0.0:8145
```

2. CA 証明書へのアクセス許可を得るには、次の手順を実行して、新しく取得した CA 証明書にアクセスし、証明書のアクセス許可リストに SnapCenter のデフォルトの IIS Web サーバー ユーザー「**IIS AppPool\ SnapCenter**」を追加します。
   a. Microsoft 管理コンソール (MMC) に移動し、[ファイル] > [スナップインの追加と削除] をクリックします。
   b. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。
   c. 証明書スナップイン ウィンドウで、[コンピューター アカウント] オプションを選択し、[完了] をクリックします。
   d. コンソール ルート > 証明書 **-** ローカル コンピューター > 個人 > 証明書 をクリックします。
   e. SnapCenter証明書を選択します。
   f. ユーザー\権限の追加ウィザードを開始するには、CA 証明書を右クリックし、[すべてのタスク] > [秘密キーの管理] を選択します。
   g. *追加*をクリックし、ユーザーとグループの選択ウィザードで場所をローカルコンピューター名（階層の最上位）に変更します。
   h. IIS AppPool\SnapCenterユーザを追加し、フル コントロール権限を付与します。
3. **CA** 証明書 **IIS** アクセス許可 については、次のパスからSnapCenter Server に新しい DWORD レジストリ キー エントリを追加します。

   Windowsレジストリ エディタで次のパスに移動します。

   ```
   HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProv ders\SCHANNEL
   ```

4. SCHANNELレジストリ設定のコンテキストで、新しいDWORDレジストリ キー エントリを作成します。

   ```
   SendTrustedIssuerList = 0

   ClientAuthTrustMode = 2
   ```

双方向**SSL**通信用の**SnapCenter Windows**プラグインの設定

PowerShellコマンドを使用して、SnapCenter Windowsプラグインで双方向SSL通信を使用できるように設定

する必要があります。

開始する前に

CA証明書サムプリントが使用可能であることを確認します。

手順

1. ポートをバインドするには、Windowsプラグイン ホストでSMCoreポート8145（デフォルト）に対して次の操作を実行します。

   a. 次のPowerShellコマンドを使用して、既存のSnapCenter自己署名証明書のポート バインドを削除します。

      ```
      > netsh http delete sslcert ipport=0.0.0.0:<SMCore port>
      ```

      次に例を示します。

      ```
      > netsh http delete sslcert ipport=0.0.0.0:8145
      ```

   b. 新しく取得したCA証明書をSMCoreポートにバインドします。

      ```
      > $cert = "<CA_certificate thumbprint>"

      > $guid = [guid]::NewGuid().ToString("B")

      > netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
      appid="$guid" clientcertnegotiation=enable
      verifyclientcertrevocation=disable

      > netsh http show sslcert ipport=0.0.0.0:<SMCore Port>
      ```

      次に例を示します。

      ```
      > $cert = "abc123abc123abc123abc123"

      > $guid = [guid]::NewGuid().ToString("B")

      > netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
      clientcertnegotiation=enable verifyclientcertrevocation=disable

    > netsh http show sslcert ipport=0.0.0.0:8145
      ```

Windowsホストでの双方向SSL通信の有効化

PowerShellコマンドを使用して、双方向SSL通信を有効にし、Windowsホスト上のSnapCenter Serverとプラグインの間の相互通信を保護できます。

始める前に

すべてのプラグインとSMCoreエージェントのコマンドを実行したあと、サーバのコマンドを実行します。

手順

1. 双方向SSL通信を有効にするには、SnapCenter Serverで、プラグイン、サーバ、および双方向SSL通信が必要な各エージェントに対して次のコマンドを実行します。

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName <Plugin_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

2. 次のコマンドを使用して、IIS SnapCenterアプリケーション プールのリサイクル操作を実行します。 `> Restart-WebAppPool -Name "SnapCenter"`
3. Windowsプラグインの場合は、次のPowerShellコマンドを実行してSMCoreサービスを再起動します。

```
> Restart-Service -Name SnapManagerCoreService
```

双方向SSL通信の無効化

PowerShellコマンドを使用して、双方向SSL通信を無効にすることができます。

このタスクについて

- すべてのプラグインとSMCoreエージェントのコマンドを実行したあと、サーバのコマンドを実行します。
- 双方向SSL通信を無効にしても、CA証明書とその設定は削除されません。
- SnapCenter Serverに新しいホストを追加するには、すべてのプラグイン ホストで双方向SSLを無効にする必要があります。
- NLBとF5はサポートされません。

手順

1. 双方向SSL通信を無効にするには、SnapCenter Serverですべてのプラグイン ホストとSnapCenterホストに対して次のコマンドを実行します。

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName <Agent_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

2. 次のコマンドを使用して、IIS SnapCenterアプリケーション プールのリサイクル操作を実行します。 `> Restart-WebAppPool -Name "SnapCenter"`
3. Windowsプラグインの場合は、次のPowerShellコマンドを実行してSMCoreサービスを再起動します。

```
> Restart-Service -Name SnapManagerCoreService
```

著作権に関する情報

商標に関する情報