



Windowsホストで双方向SSL通信を設定して有効にする

SnapCenter Software 6.0

NetApp
July 23, 2024

目次

Windowsホストで双方向SSL通信を設定して有効にする	1
Windowsホストでの双方向SSL通信の設定	1
Windowsホストで双方向SSL通信を有効にする	3

Windowsホストで双方向SSL通信を設定して有効にする

Windowsホストでの双方向SSL通信の設定

Windows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ために、双方向SSL通信を設定する必要があります。

作業を開始する前に

- 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。
- 秘密鍵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、を参照してください ["CA証明書の設定セクション"](#)

- 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。

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

手順

1. ポートをバインドするには、PowerShellコマンドを使用して、SnapCenter IIS Webサーバポート8146（デフォルト）およびSMCoreポート8145（デフォルト）のSnapCenterサーバホストで次の手順を実行します。

- 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/IIS port>
```

例：

```
> 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サーバと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=$certappid="$guid" clientcertnegotiation=enable  
verifyclientcertrevocation=disable
```

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

例：

```
> $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証明書の権限にアクセスするには、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、SnapCenterのデフォルトのIIS Webサーバユーザ「* IIS AppPool\SnapCenter *」を証明書の権限のリストに追加します。
 - a. Microsoft管理コンソール（MMC）に移動し、[ファイル]>*[SnapIn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、[Certificates] を選択し、[Add] をクリックします。
 - c. [証明書] スナップインウィンドウで、[Computer account] 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] の順をクリックします。
 - 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]>*[秘密鍵の管理]*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権限*の場合、次のパスからSnapCenterサーバーに新しい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\SecurityProviders\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プラグインを設定します

SnapCenter Windowsプラグインは、PowerShellコマンドを使用して双方向SSL通信用に設定する必要があります。

作業を開始する前に

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>
```

例：

```
> 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>
```

例：

```
> $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ホストで双方向SSL通信を有効にする

PowerShellコマンドを使用して、Windows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ために、双方向SSL通信を有効にすることができます。

- 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最初に実行し、次に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、プラグイン、サーバー、および双方向SSL通信が必要な各エージェントに対して、SnapCenterサーバーで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"}
```

1. 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"
2. 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通信を無効にします

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最初に実行し、次に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サーバー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、すべてのプラグインホストとSnapCenterホストに対してSnapCenterサーバーで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"}
```

1. 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"

2. 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

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。