テクニカル レポート

NetApp SnapCenterセキュリティ強化ガイド

NetApp
ONTAP TMEチーム、
2024年1月| TR-4957

概要

このテクニカルレポートでは、組織が情報システムの機密性、整合性、可用性に関して規定されたセキュリティ目標を達成するのに役立つ、NetApp®SnapCenter®ソフトウェアのガイダンスと構成設定について説明します。

表一覧

図一覧

Windowsサーバで実行されているSnapCenterサーバとプラグインのセキュリティ強化

はじめに

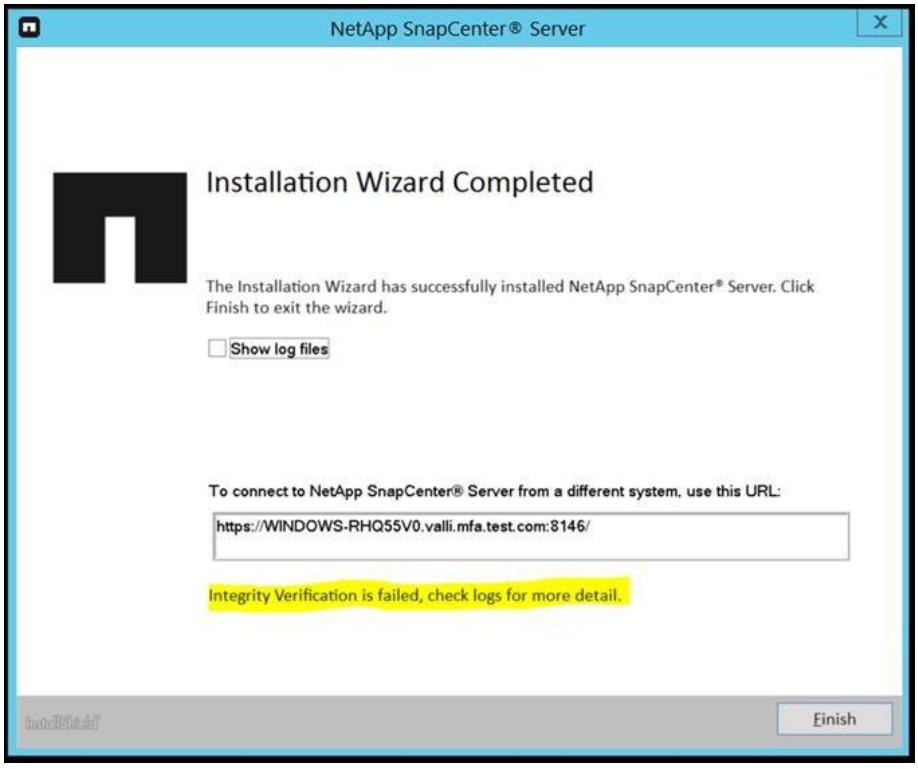
これらのガイドラインとツールは、Windowsサーバー上で実行されるSnapCenterサーバーとプラグインを安全に強化し、ハッキングを防止するために提供されています。これには、脆弱性の排除または軽減が含まれます。脆弱性という用語は、システムの実装、構成、設計、または管理で発生する可能性のあるソフトウェアの欠陥および弱点を指します。セキュリティ強化技術では、通常、運用機能とセキュリティのバランスを取るために設定をロックダウンすることが必要です。このガイドでは、NetApp 解決策 に不可欠な機密性、整合性、および可用性を使用して、オペレータと管理者がそのタスクを実行できるように支援します。

インストールと導入の

整合性の検証

SnapCenterサーバのインストールが終了すると、整合性検証機能は2つのチェックを実行します。最初のチェックでは、サードパーティ製ファイルやネットアップ所有のファイルを含むすべてのファイルのチェックサム検証が行われます。次に、NetAppバイナリファイル（実行可能ファイルおよびダイナミックリンクライブラリ（DLL））のデジタル署名検証を実行します。チェックサムとデジタル署名の検証に不一致がある場合は、次のスクリーンショットに示すように、インストーラの最後に報告されます。

図1）整合性の検証



どちらのチェックも、Windowsプラグインが個別にインストールされている場合にも実行されます。

整合性検証は、製品の新規インストール時または以前のリリースからの製品アップグレード時にのみ実行されます。

詳細については、次のログを参照してください。

- SnapCenterログパス：一時ディレクトリ `(%temp%)\IntegrityVerifier_<time_stamp>.log`
- Windowsプラグインログのパス：`C:\Windows\SnapCenter Plugin\<Job Name>\Integrity_Verifier.log`

整合性検証機能ログに「file hash not matched」または「file has invalid digital signature」というエラーメッセージが記録されている場合は、ファイルコピーエラーを回避するために、ソフトウェアパッケージを新規ダウンロードしてSnapCenterソフトウェアを再インストールする必要があります。同じファイルでもエラーが解決しない場合は、テクニカルサポートにお問い合わせください。

注: ファイルが見つからない場合やファイルビジーエラーが表示された場合は、除外することができます。

SnapCenterサーババイナリの保護

デフォルトでは、SnapCenterサーバはインストール時にカスタムアプリケーションプールを作成します。このローカルユーザアカウントの名前は、インターネットインフォメーションサービス（IIS）AppPool\\SnapCenterです。セキュリティを強化し、他のユーザのSnapCenterファイルへのアクセスを容易に管理するには、次の手順を実行してデフォルトユーザから優先ドメインまたはローカルワークグループユーザに変更します。

1. SnapCenterがインストールされているWindows ServerでIISマネージャを開きます。
2. 左側のナビゲーションペインで、**[アプリケーションプール]**をクリックします。
3. [アプリケーションプール]リストで[SnapCenter]を選択し、[操作]ペインで[詳細設定]をクリックします。
4. **[ID]**を選択し、[...]をクリックします。）をクリックして、SnapCenterアプリケーションプールIDを編集します。
5. [Custom Account]フィールドに、Active Directoryの読み取り権限を持つドメインユーザまたはドメイン管理者アカウントの名前を入力します。
6. **[OK]**をクリックします。

カスタムアカウントは、SnapCenterアプリケーションプールの組み込みのApplicationPoolIdentityアカウントを置き換えます。

ポートとプロトコル

SnapCenterサーバとプラグインホスト、ストレージシステム、およびその他のコンポーネントの間で通信を行うには、必要なポートとプロトコルを使用します。

- SnapCenterサーバおよびアプリケーションプラグインまたはデータベースプラグインをインストールする前に、接続とポートの要件が満たされていることを確認してください。
- アプリケーションは1つのポートを共有できません。
- 各ポートは、適切なアプリケーション専用にする必要があります。
- デフォルトのポートを使用しない場合は、インストール時にカスタムポートを選択できます。プラグインポートは、インストール後にホスト変更ウィザードを使用して変更できます。
- 固定ポートの場合は、デフォルトのポート番号をそのまま使用する必要があります。

ファイアウォール

ファイアウォール、プロキシ、またはその他のネットワークデバイスが接続に干渉しないようにしてください。SnapCenterのインストール時にカスタムポートを指定した場合は、SnapCenter Plug-in Loader用にそのポートのファイアウォールルールをプラグインホストに追加する必要があります。

次の表に、各ポートとそのデフォルト値を示します。

表1）SnapCenter接続とポートの要件

ポートのタイプ	デフォルト ポート
SnapCenterポート	**8146** （HTTPS）、双方向、カスタマイズ可能、URL： `https://server:8146` SnapCenterクライアント（SnapCenterユーザ）とSnapCenterサーバ間の通信に使用されます。プラグインホストからSnapCenterサーバへの通信にも使用されます。
SnapCenter SMCoreの通信ポート	**8145**（HTTPS）、双方向、カスタマイズ可能 このポートは、SnapCenterサーバとSnapCenterプラグインがインストールされているホストの間の通信に使用されます。
MySQLのポート	**3306** （HTTPS）、双方向 このポートは、SnapCenterとMySQLリポジトリデータベースの間の通信に使用されます。SnapCenterサーバからMySQLサーバへのセキュアな接続を確立できます。詳細はこちら。
Windowsプラグインホスト	**135**、**445**（TCP） ポート135と445に加えて、Microsoftが指定する動的ポート範囲も開いておく必要があります。リモート インストールではWindows Management Instrumentation（WMI）サービスを使用しますが、WMIサービスはこのポート範囲を検索します。 サポートされるダイナミックポート範囲については、「Windowsのサービスの概要とネットワークポートの要件」を参照してください。 これらのポートは、SnapCenterサーバとプラグインがインストールされているホストの間の通信に使用されます。プラグインパッケージのバイナリをWindowsプラグインホストにプッシュするには、プラグインホストでのみポートを開く必要があり、インストール後に閉じることができます。
LinuxまたはAIXプラグインホスト	**22** （SSH） このポートは、SnapCenterサーバとプラグインがインストールされているホストの間の通信に使用されます。プラグインパッケージのバイナリをLinuxまたはAIXのプラグインホストにコピーするためにSnapCenterで使用されます。このポートを開いておくか、ファイアウォールまたはiptablesから除外しておく必要があります。
SnapCenter Plug-ins Package for Windows、SnapCenter Plug-ins Package for Linux、SnapCenter Plug-ins Package for AIX	**8145** （HTTPS）、双方向、カスタマイズ可能 このポートは、SMCoreとプラグイン パッケージがインストールされているホストの間の通信に使用されます。 通信パスは、Storage VM（Storage Virtual Machine、略称SVM）の管理LIFとSnapCenterサーバの間でも開いている必要があります。
SnapCenter Plug-in for Oracle Database	**27216**、カスタマイズ可能 デフォルトのJDBCポートは、Oracleデータベースへの接続にOracle用プラグインで使用されます。
SnapCenter用のカスタムプラグイン	**9090** （HTTPS）、固定 カスタムプラグインホストでのみ使用される内部ポートです。ファイアウォールの例外は必要ありません。 SnapCenterサーバとカスタムプラグインの間の通信は、ポート8145を介してルーティングされます。
ONTAPクラスタまたはSVM通信ポート	**443** （HTTPS）、双方向 **80** （HTTP）、双方向 このポートは、SnapCenterサーバを実行するホストとSVMの間の通信にストレージ抽象化レイヤ（SAL）で使用されます。現在は、SnapCenterプラグインホストとSVMの間の通信にSnapCenter for Windows Plug-inホストのSALでも使用されています。
SnapCenter Plug-in for SAP HANA Database	**3instance_number13** または **3instance_number15**、HTTPまたはHTTPS、双方向、カスタマイズ可能

ポートのタイプ	デフォルト ポート
vCodeスペル チェッカーポート	マルチテナントデータベースコンテナ（MDC）のシングルテナントの場合、ポート番号は **13**で終わります。MDC以外の場合、ポート番号は **15**で終わります。 たとえば、32013はインスタンス20のポート番号で、31015はインスタンス10のポート番号です。
ドメインコントローラの通信ポート	認証が正しく機能するためにドメインコントローラのファイアウォールで開く必要があるポートについては、Microsoftのドキュメントを参照してください。 SnapCenterサーバ、プラグインホスト、またはその他のWindowsクライアントがユーザを認証できるように、Microsoftが必要とするポートをドメインコントローラで開く必要があります。

認証とログイン

多要素認証（MFA）

MFAは、セキュリティレイヤを強化するためにSnapCenter 4.7で導入されました。MFA機能は、Active Directoryフェデレーションサービス（AD FS）アイデンティティマネージャと呼ばれるMicrosoftベースの標準解決策で動作します。SnapCenterはAD FSマネージャのクライアントとして機能し、SnapCenterログインページはAD FSログインページにリダイレクトされます。また、AD FSは、SnapCenterユーザのログイン、ログアウト、およびセッションタイムアウトも行います。
Security Assertion Markup Language（SAML）2.0プロトコルは、SnapCenterサーバとAD FSアイデンティティマネージャの間の通信を有効にするために使用されます。

MFA機能を有効にするには、AD FSサーバとSnapCenterサーバでいくつかの手順を実行する必要があります。MFAを設定する前に、次の点を確認してください。

- AD FSは、それぞれのドメインで稼働している必要があります。
- Azure MFA、Cisco Duoなど、AD FSでサポートされているMFAサービスが必要です。
- SnapCenterとAD FSサーバのタイムスタンプは、タイムゾーンに関係なく同じである必要があります。
- SnapCenterサーバの認証局（CA）証明書を取得して設定しておきます。

CA証明書は、次の理由で必須です。

- 自己署名証明書はノードレベルで一意であるため、ADFS-F5通信は中断できません。
- スタンドアロン構成またはハイアベイラビリティ構成でのアップグレード、修復、またはディザスタリカバリ（DR）の実行中は、自己署名証明書が再作成されないため、MFAの再設定が回避されます。
- IP-FQDNの解決を保証します。

CA証明書の詳細については、「CA証明書CSRの生成」を参照してください。

- 同じAD FSで他のアプリケーションが設定されている場合、SnapCenterはSSOベースのログインをサポートします。一部のAD FS構成では、AD FSセッションの持続性に応じて、セキュリティ上の理由からSnapCenterでユーザ認証が必要になる場合があります。
- コマンドレットで使用するパラメータとその説明は、Get-Helpで確認 `command_name`できます。また、『SnapCenterソフトウェア コマンドレットリファレンスガイド』も参照してください。

SnapCenter MFA機能を有効にする方法

1. AD FSホストに接続します。
2. からAD FSフェデレーションメタデータファイルをダウンロードし `https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml`ます。
3. ダウンロードしたファイルをSnapCenterサーバにコピーして、MFA機能を有効にします。

4. PowerShellを使用して、SnapCenter管理者ユーザとしてSnapCenterサーバにログインします。
5. PowerShellセッションを使用して、 `New- SmMultifactorAuthenticationMetadata -path` コマンドレットを使用してSnapCenter MFAメタデータファイルを生成します。pathパラメータには、SnapCenter ServerのホストにMFAメタデータ ファイルを保存するためのパスを指定します。
6. 生成されたファイルをAD FSのホストにコピーし、SnapCenterをクライアント エンティティとして設定します。
7. Set-SmMultiFactorAuthenticationコマンドレットを使用して、SnapCenterサーバのMFAを有効にします。pathパラメータは、手順3でSnapCenterサーバーにコピーしたAD FS MFAメタデータXMLファイルの場所を指定します。
8. （オプション）`Get- SmMultiFactorAuthentication` コマンドレットを使用して、MFAの設定ステータスと設定を確認します。
9. Microsoft管理コンソール（MMC）に移動し、次の手順を実行します。

a. [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] > [パーソナル] > [証明書]をクリックします。
e. SnapCenterにバインドされている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。
f. Permissionsウィザードで、次の手順を実行します。

– [追加]をクリックします。
– [Locations]をクリックし、該当するホスト（階層の最上位）を選択します。
– [場所]ポップアップ ウィンドウで、[OK]をクリックします。
– [オブジェクト名]フィールドに「IIS_IUSRS」と入力し、[名前の確認]をクリックして[OK]をクリックします。確認が問題なく完了したら、[OK]をクリックします。

10. AD FSホストでAD FS管理ウィザードを開き、次の手順を実行します。

a. [証明書利用者信頼]を右クリックし、[証明書利用者信頼の追加] > [開始]をクリックします。
b. 2つ目のオプションを選択し、SnapCenter MFAメタデータ ファイルを参照したら、[次へ]をクリックします。
c. 表示名を指定し、[次へ]をクリックします。
d. 必要に応じてアクセス制御ポリシーを選択し、[次へ]をクリックします。
e. 次のタブの設定をデフォルトに設定します。
f. [完了]をクリックします。

SnapCenterが、指定した表示名の証明書利用者として反映されます。

11. 名前を選択し、次の手順を実行します。

a. [要求発行ポリシーの編集]をクリックします。
b. [規則の追加]をクリックし、[次へ]をクリックします。
c. クレームルールの名前を指定します。
d. 属性ストアとして[Active Directory]を選択します。
e. 属性として[ユーザー プリンシパル名]を選択し、発信要求タイプとして[名前ID]を選択します。
f. [完了]をクリックします。

12. ADFSサーバで次のPowerShellコマンドを実行します。

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >' -
SigningCertificateRevocationCheck None
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >' -
EncryptionCertificateRevocationCheck None
```

13. 次の手順を実行して、メタデータがインポートされたことを確認します。

a. 証明書利用者信頼を右クリックし、[プロパティ]を選択します。

b. [Endpoints]、[Identifier]、および[Signature]フィールドに値が入力されている

ことSnapCenterのMFA機能は、REST APIを使用して有効にすることもできます。

SnapCenterでMFA設定を有効化、更新、または無効化したら、すべてのブラウザタブを閉じてブラウザを再度開いて再度ログインします。これにより、既存の、またはアクティブなセッションCookieがクリアされます。

アップグレード、CA証明書の更新、ディザスタリカバリ（DR）など、AD FSサーバで変更があった場合は、SnapCenterでAD FS MFAメタデータを更新する必要があります。

AD FS MFAメタデータを更新する方法

1. からAD FSフェデレーションメタデータファイルをダウンロードし `https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml`ます。
2. ダウンロードしたファイルをSnapCenter Serverにコピーして、MFAの設定を更新します。
3. 次のコマンドレットを実行して、SnapCenterでAD FSメタデータを更新します。

```
Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
```

4. SnapCenterでMFA設定を有効化、更新、または無効化したら、すべてのブラウザタブを閉じ、ブラウザを再度開いて再度ログインします。これにより、既存またはアクティブなセッションCookieがクリアされます。

SnapCenter MFAメタデータの更新

AD FSサーバに修復、CA証明書の更新、DRなどの変更がある場合は、AD FSでSnapCenter MFAメタデータを更新する必要があります。

AD FSホストで、AD FS管理ウィザードを開き、次の手順を実行します。

1. **[証明書利用者信頼]**をクリックします。
2. SnapCenter用に作成した証明書利用者信頼を右クリックし、**[削除]**をクリックします。
3. 証明書利用者信頼のユーザ定義の名前が表示されます。
4. 多要素認証（MFA）を有効にします。

詳細については、「多要素認証の有効化」を参照してください。

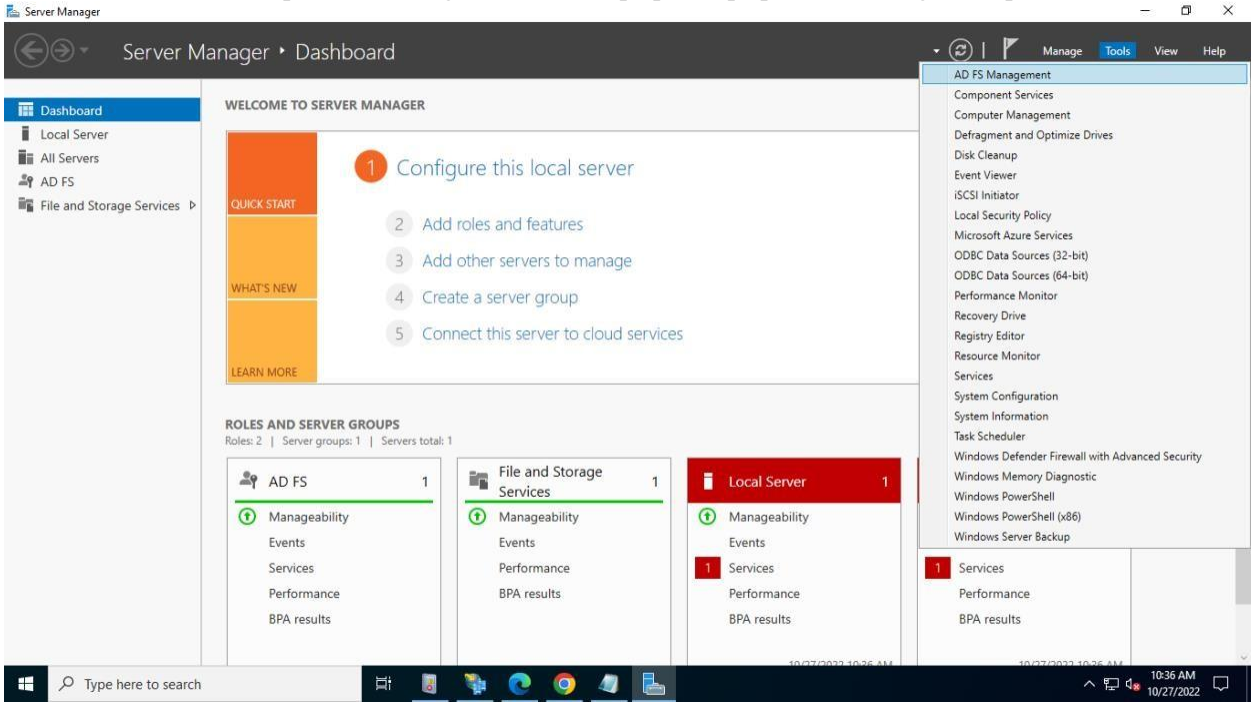
SnapCenterでMFA設定を有効化、更新、または無効化したら、すべてのブラウザタブを閉じ、ブラウザを再度開いて再度ログインします。これにより、既存またはアクティブなセッションCookieがクリアされます。

REST API、PowerShell、SCCLIを使用した多要素認証（MFA）の管理

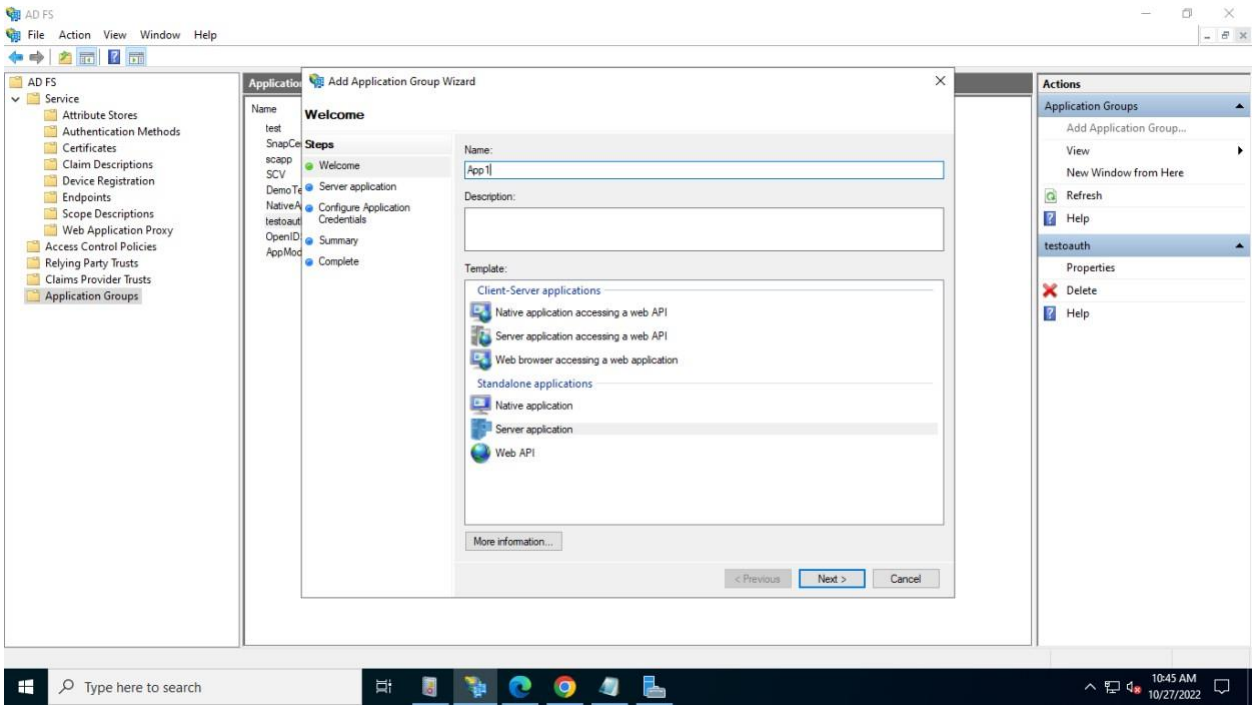
前のセクションで説明したように、MFAはSnapCenter 4.7で導入され、SnapCenterのGUIインターフェイスのセキュリティレイヤを強化しました。SnapCenter 4.9では、MFA機能が拡張され、RestAPI、PowerShell、およびSCCLIインターフェイスと連携できるようになりました。

Active Directoryフェデレーションサービス（AD FS）をOAuth/OpenID Connect（OIDC）としてセットアップする

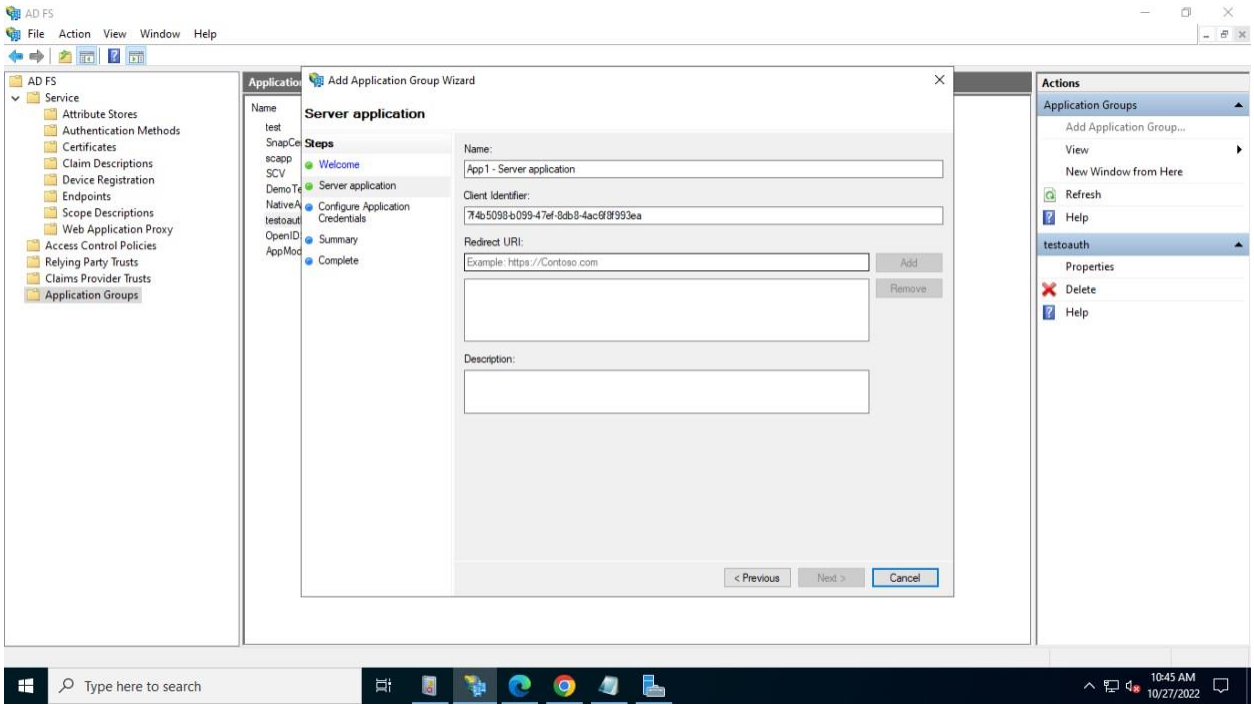
- AD FSホストに接続し、**[Server Manager Dashboard]->[Tools]->[AD FS Management]**の順に選択します。

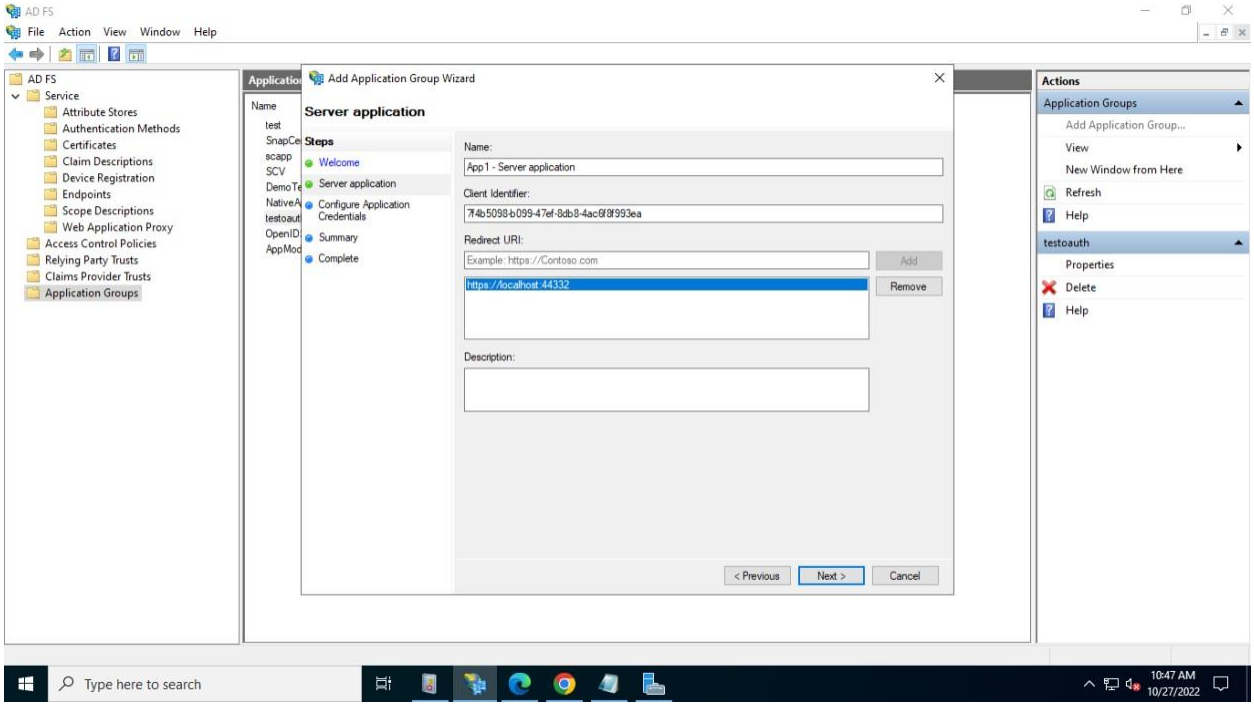


- **[AD FS]->[アプリケーショングループ]**に移動します。**[アプリケーショングループ]**を右クリックして**[アプリケーショングループの追加]**をクリックし、**[アプリケーション名]**を入力します。**[Server Application]**を選択し、**[Next]**をクリックします。

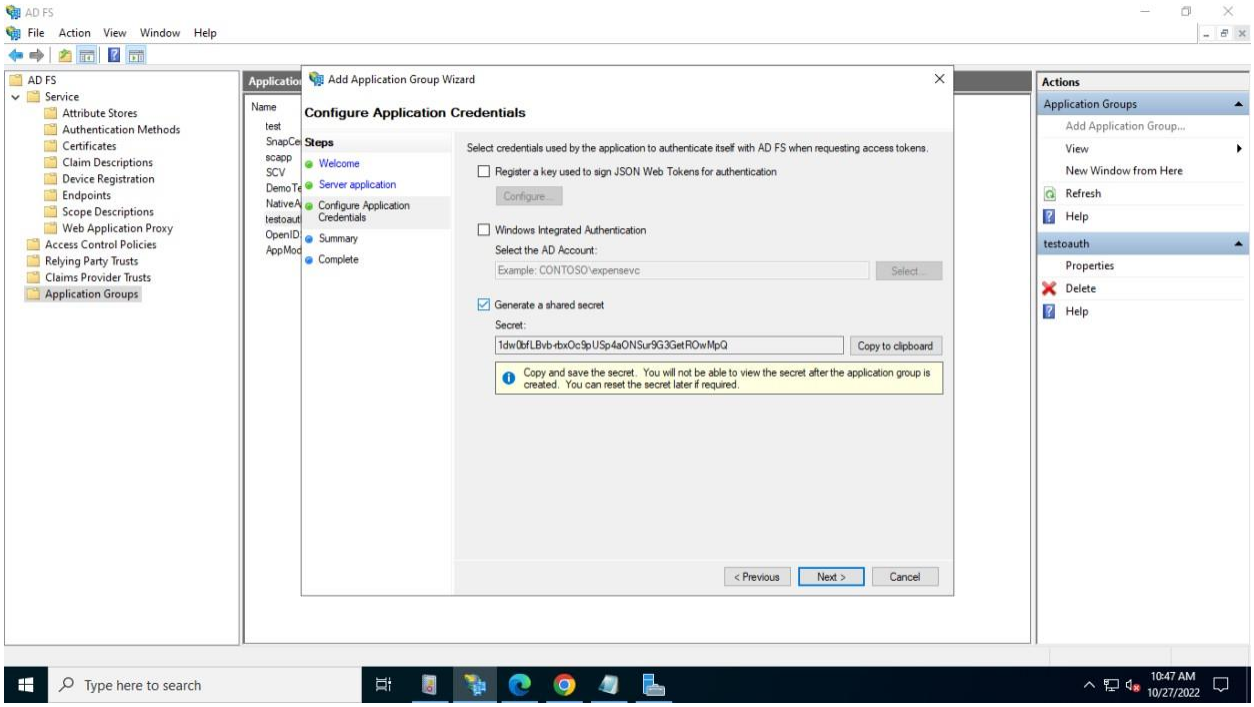


- **クライアントID**をコピーします。これは**クライアントID**です。**リダイレクトURL**に**コールバックURL**（SnapCenterサーバURL）を追加します。**[次へ]**をクリックします。

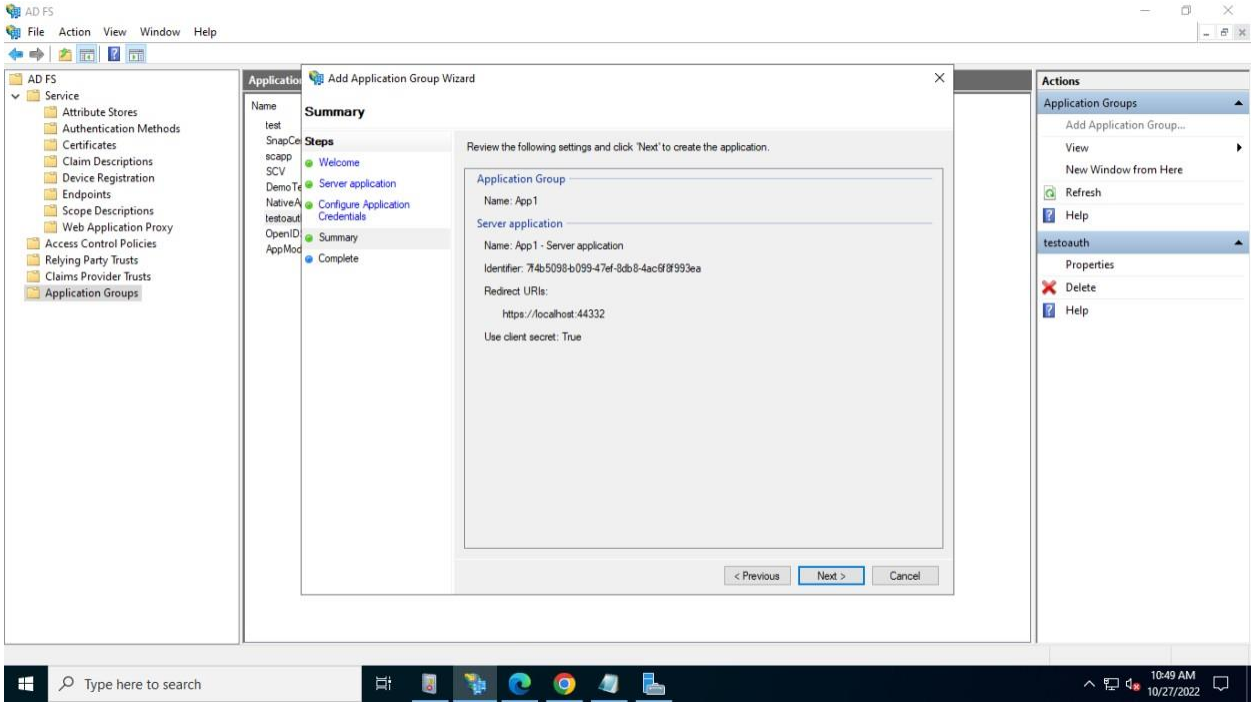




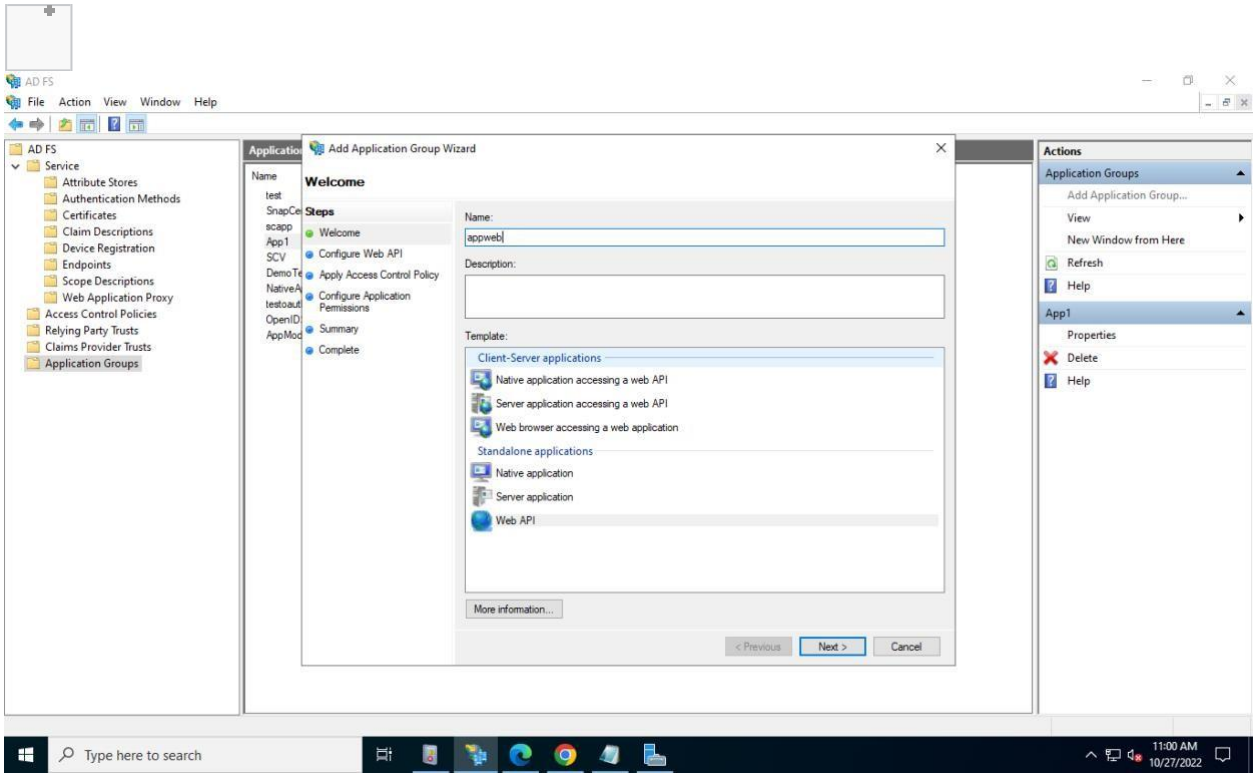
- **[Generate shared secret]**をクリックします。**[Secret]の値**をコピーします。これが**クライアントの秘密**です。**[次へ]**をクリックします。



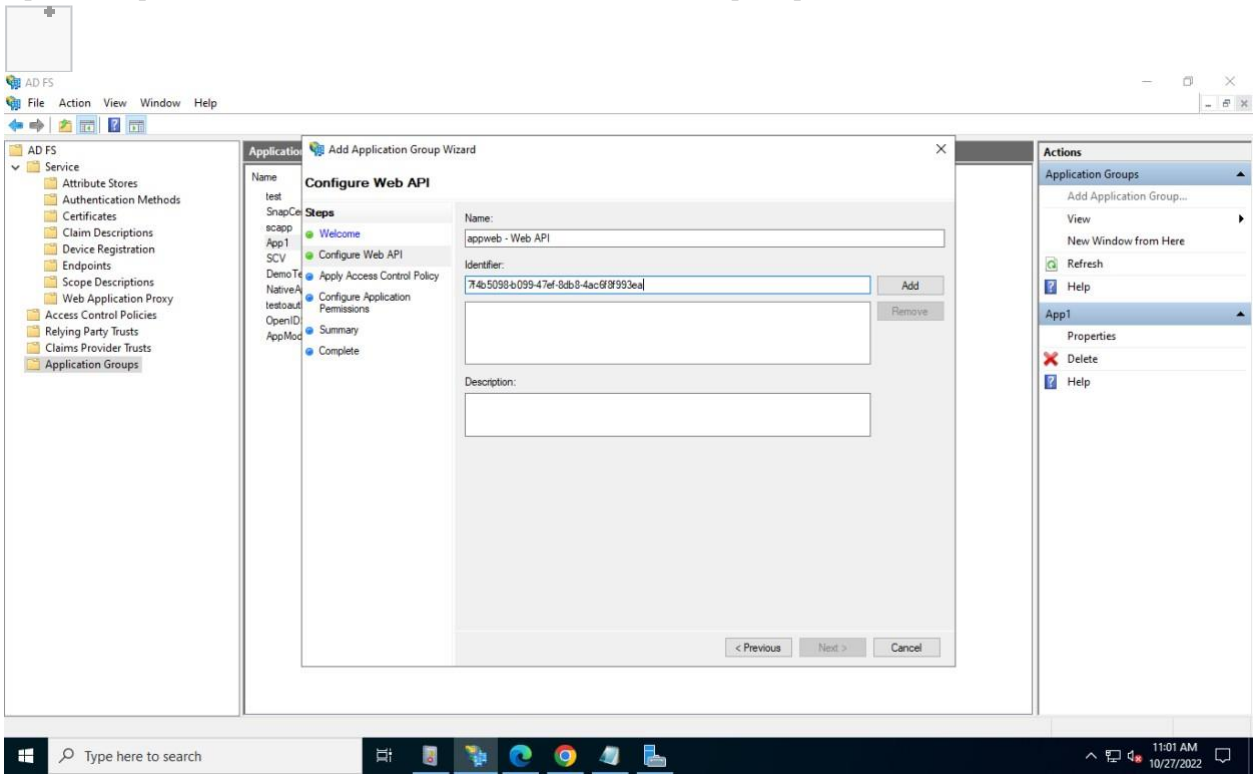
- **[Summary]**画面で、**[Next]**をクリックします。**[Complete]**画面で、**[Close]**をクリックします。



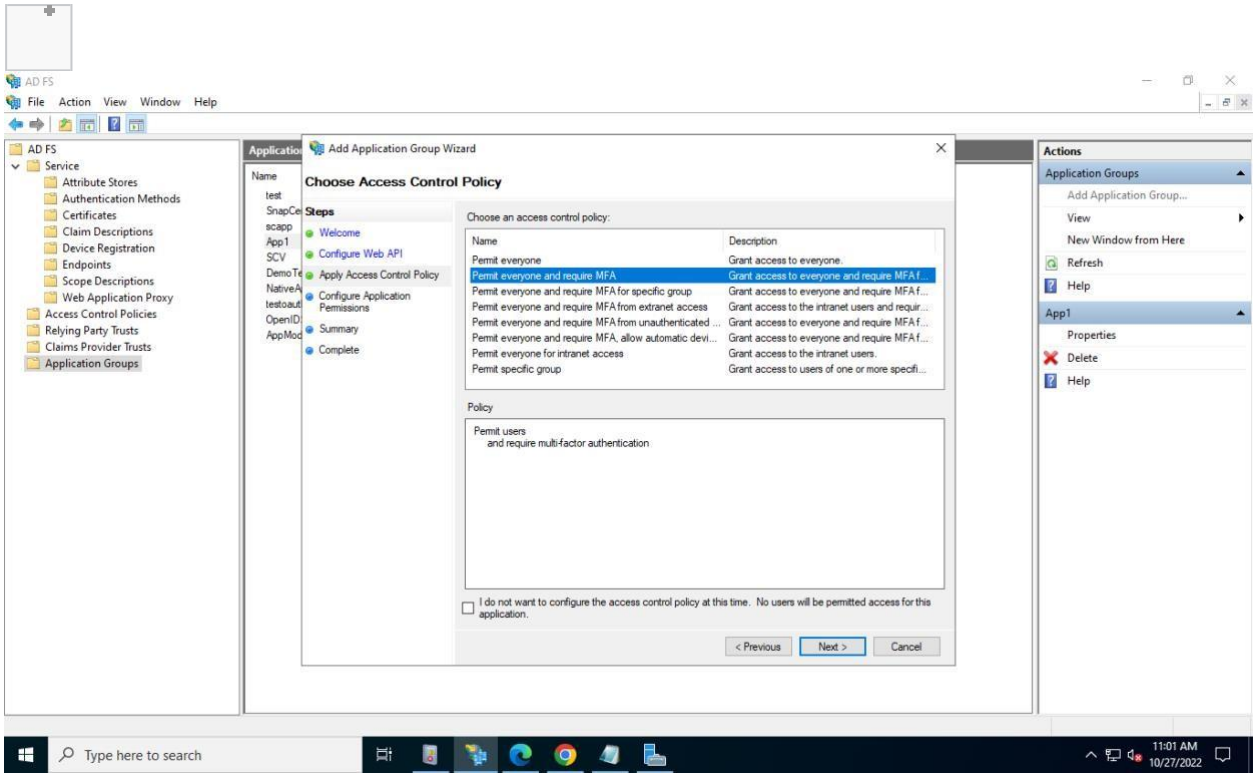
- 次に、新しく追加したアプリケーショングループを右クリックし、**[プロパティ]**を選択します。
- **[アプリケーションのプロパティ]**から**[アプリケーションの追加]**をクリックします。
- **[追加]**アプリケーションをクリックします。次に、**[Web API]**を選択し、**[Next]**をクリックします。



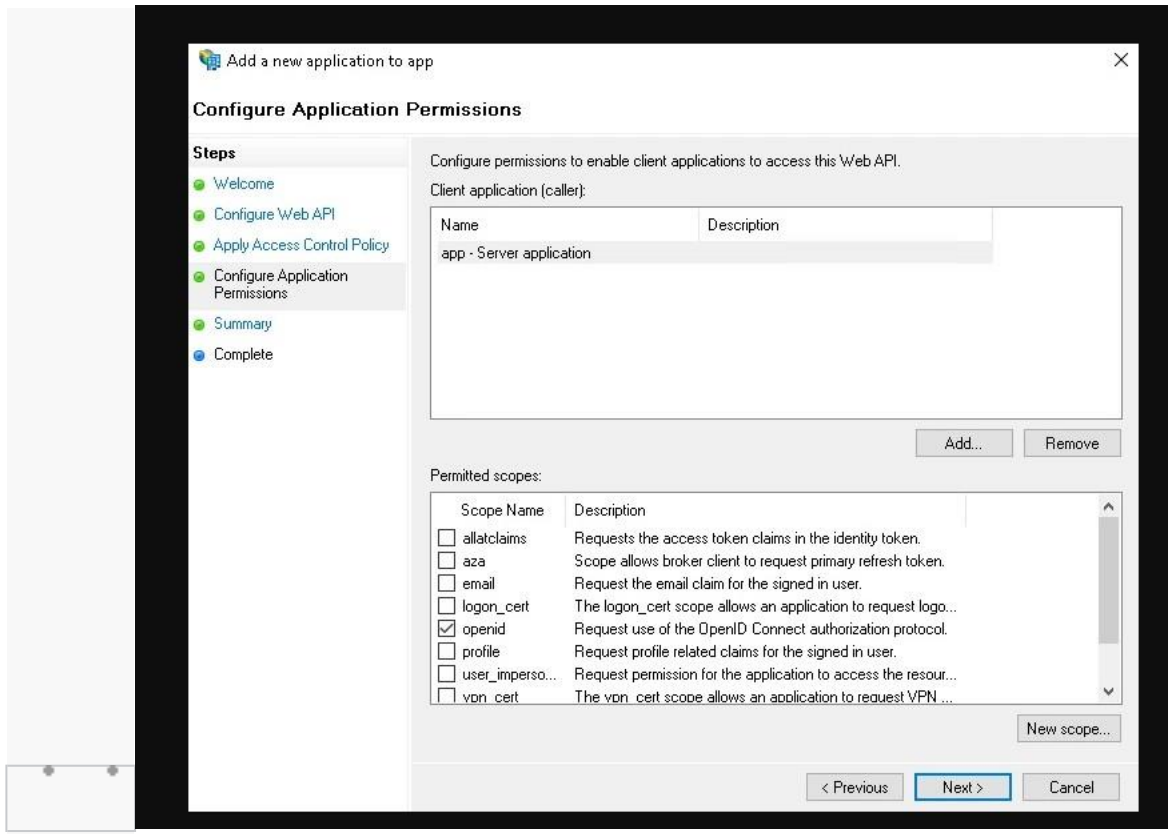
- **[Web APIの設定]**画面で、 前の手順で作成した**SnapCenterサーバのURL**とクライアント識別子を**[Identifier]**セクションに入力します。**追加**をクリックします。**[Next]**をクリックします。



- **[Choose Access Control Policy]**画面で、要件に基づいて制御ポリシーを選択し（例：**Permit Everyoneand Require MFA**）、**[Next]**をクリックします。

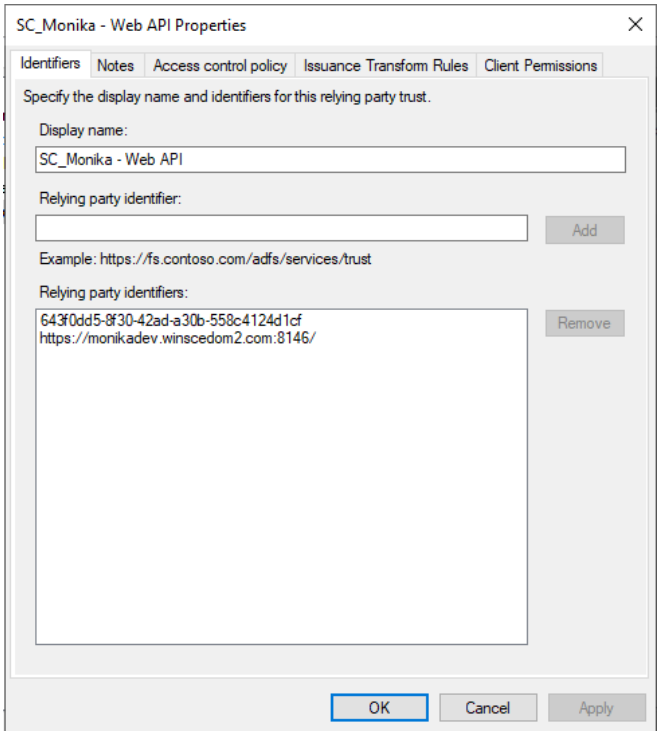


- **[アプリケーションの設定]**権限では、デフォルトで**OpenID**がスコープとして選択され、[次へ]をクリックします。



- **[Summary]**画面で、**[Next]**をクリックします。**[Complete]**画面で、**[Close]**をクリックします。
- **[Sample Application Properties]**で**[OK]**をクリックします。

- 承認サーバー(AD FS)によって発行され、リソースによって消費されることを意図したJWTトークン。このトークンの「AUD」またはオーディエンス要求は、リソースまたはWeb APIの識別子と一致している必要があります。
- 選択したWebAPIを編集し、コールバックURL（**SnapCenterサーバURL**）と**クライアント識別子**が正しく追加されていることを確認します。

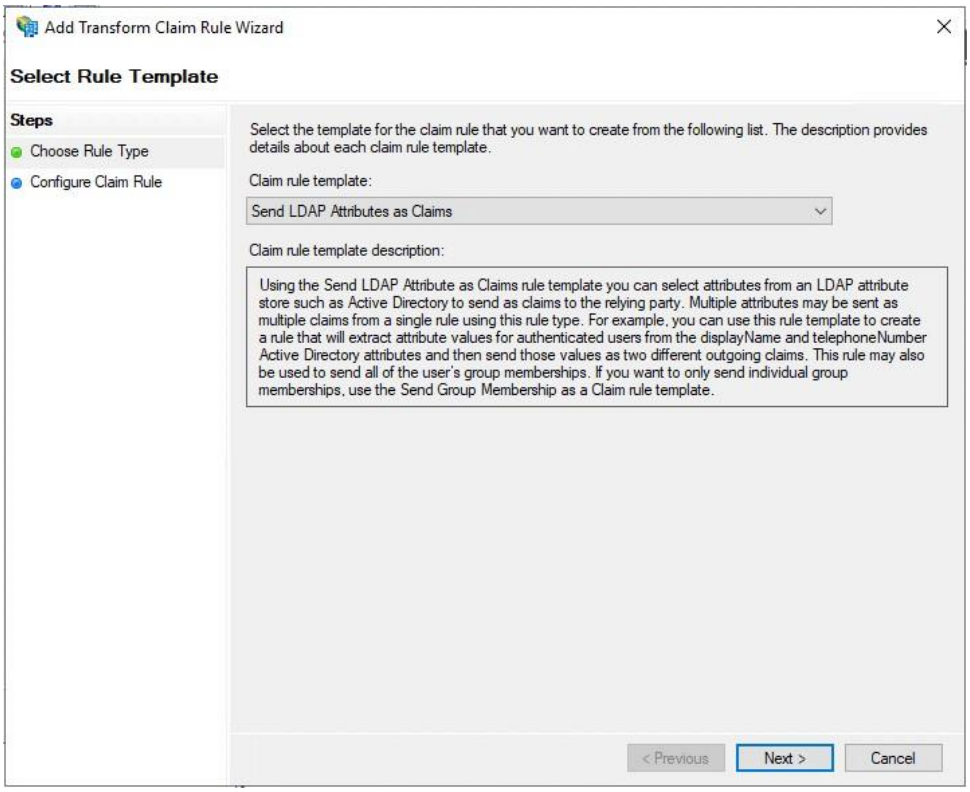


ユーザ名を要求として提供するようにOpenID Connect（OIDC）を設定します。

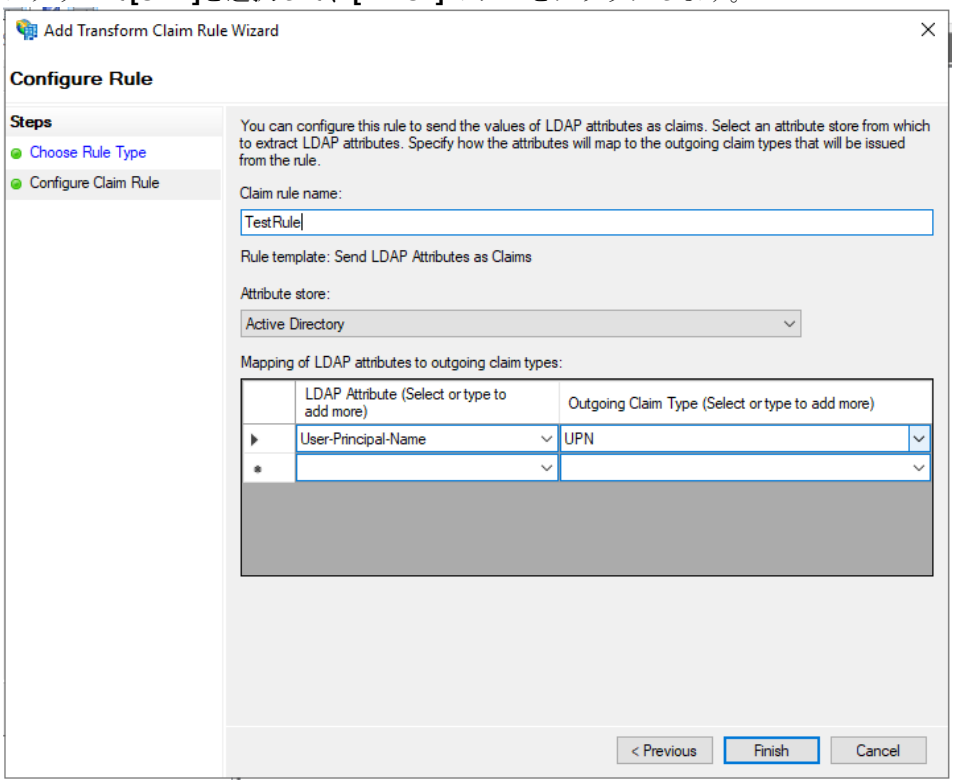
OpenID Connect（OIDC）は、OAuth 2.0認可プロトコルを拡張し、追加の認証プロトコルとして使用します。OIDCを使用すると、セキュリティトークンを使用して、OAuth対応アプリケーション間のシングルサインオン（SSO）を有効にできます。

サーバーマネージャの右上にある[ツール]メニューの下にある[AD FS管理]ツールを開きます。

- 左側のサイドバーの「アプリケーショングループ」フォルダ項目を選択します。
- **Web API**を選択し、**編集**ボタンをクリックします。
- 次に、**[発行トランスフォームルール]**タブに移動します。
- **[Add Rule]** ボタンをクリックし、[Claim rule template]ドロップダウンで**[Send LDAP Attributes as Claims]**を選択し、**[Next]**をクリックします。



次に、**要求ルール**名を入力し、**[属性ストア（Attribute store）]**ドロップダウンで[Active Directory]を選択します。次に、[LDAP Attribute]ドロップダウンで**[User-Principal-Name]**を選択し、[Outgoing Claim Type]ドロップダウンで**[UPN]**を選択して、**[Finish]** ボタンをクリックします。



PowerShellによるアプリケーショングループの自動作成

アプリケーショングループ、Web APIを作成し、スコープとクレームを追加するために使用されるコマンドの概要を次に示します。

• AD FSで新しいアプリケーショングループを作成します。
'ClientRoleIdentifier'アプリケーショングループの名前'redirectURL"承認後のリダイレクトの有効なURL

```
New-AdfsApplicationGroup -Name $ClientRoleIdentifier -
ApplicationGroupIdentifier $ClientRoleIdentifier
```

• AD FSサーバアプリケーションを作成し、クライアントシークレットを生成します。

```
Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app" -
ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri
$redirectURL   -Identifier $identifier -GenerateClientSecret
```

• AD FS Web APIアプリケーションを作成し、使用するポリシー名を設定します。

```
  $identifier = (New-Guid).Guid
  Add-AdfsWebApiApplication -ApplicationGroupIdentifier
 $ClientRoleIdentifier   -Name "App Web API" -Identifier $identifier -
 AccessControlPolicyName "Permit everyone"
```

• クライアントIDとクライアントシークレットは一度しか表示されないため、この出力から取得します。

```
"client_id = $identifier"
"client_secret: "$($ADFSApp.ClientSecret)
```

• AD FSアプリケーションにallatclaims権限とOpenID権限を付与する

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier -
 ServerRoleIdentifier $identifier -ScopeNames @('openid')

$transformrule = @"
@RuleTemplate = "LdapClaims"
@RuleName = "AD User properties and Groups"
c:[Type ==
 "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
 , Issuer == "AD AUTHORITY"]
=> issue(store = "Active Directory", types =
 ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
 ";userPrincipalName;{0}", param = c.Value);
"@
```

• 変換ルールファイルを書き出す

```
$transformrule |Out-File -FilePath .\issueancetransformrules.tmp -force -
 Encoding ascii

$relativePath = Get-Item .\issueancetransformrules.tmp
```

- Web APIアプリケーションに名前を付け、外部ファイルを使用してその発行トランスフォームルールを定義します。

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API" -
 TargetIdentifier $identifier -Identifier $identifier,$redirectURL -
 IssuanceTransformRulesFile $relativePath
```

PowerShellスクリプトファイル

コマンドプロンプトまたはPowerShellで簡単なコマンドを使用してAD FSでアプリケーショングループを設定する方法については、以下のナレッジベースの記事を参照してください。

ADFSのアプリケーショングループとしてのSnapCenterの設定

アクセストークンの有効期限の更新

- アクセストークンは、ユーザー、クライアント、およびリソースの特定の組み合わせに対してのみ使用できます。アクセストークンは無効にすることはできず、有効期限が切れるまで有効です。
- In Access Tokenデフォルトの有効期限は60分です。この最小限のトークンライフタイムは十分で拡張可能です。継続的なビジネスクリティカルなジョブを回避するためには、十分な価値を提供する必要があります。
  アプリケーショングループWebAPIのトークンライフタイムを変更するには、次の手順を実行します。

```
Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName " <Web API> "
```

注:ターゲット名は、そのアプリケーショングループのWeb APIに対して指定した表示名です。

AD FSからベアラートークンを取得する

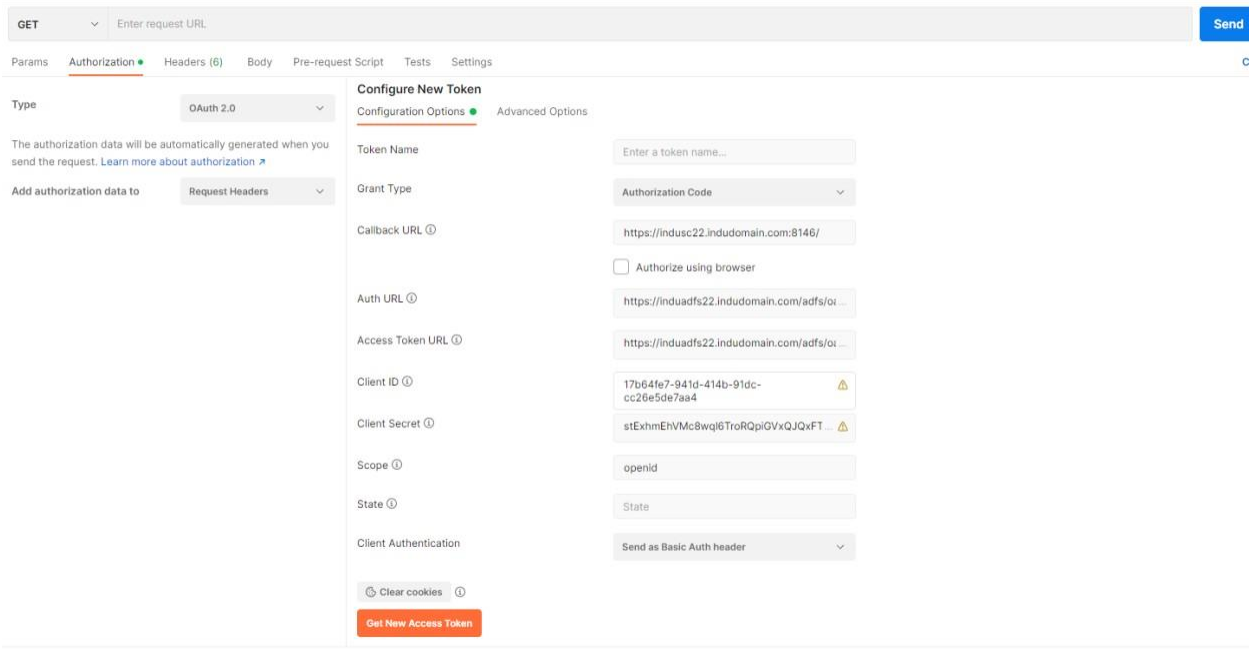
RESTクライアント(Postmanなど)で以下のすべてのパラメータを入力する必要があります。また、関係するユーザー資格情報を入力するように求められます。さらに、ベアラートークンを取得するために、セカンドファクタ認証(あなたが持っているものとあなたがいるもの)を要求します。
Bearerトークンの有効期間は、アプリケーションごとにADFSサーバーから設定でき、デフォルトの有効期間は60分です。

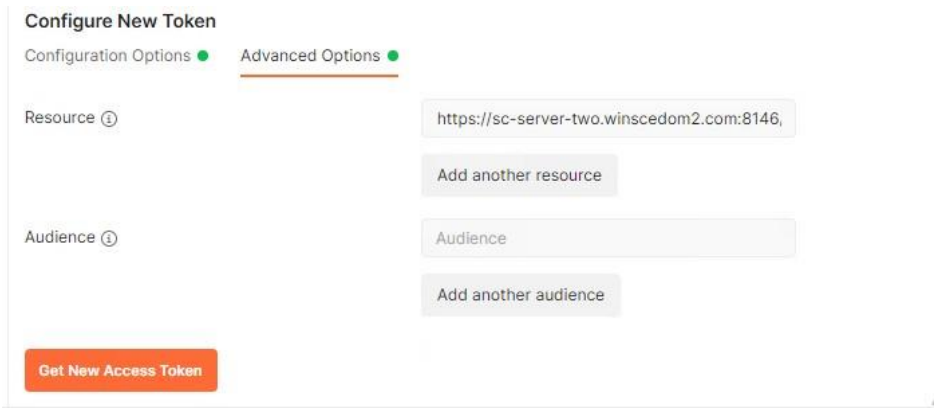
フィールド	Value
付与タイプ	認証コード
コールバックURL	コールバックURLがない場合は、アプリケーションのベースURLを入力します。
認証URL	[ADFS-domain-name]/ADFS/OAuth2/authorize
アクセストークンURL	[adfs-domain-name]/adfs/oauth2/token
クライアントID	ADFSクライアントIDの入力
クライアントシークレット	ADFSクライアントシークレットの入力
スコープ	OpenID
クライアント認証	基本認証ヘッダーとして送信

例: postmanを使用してアクセストークンを取得します。

- Postmanアプリケーションを開きます。
- [Authorization]タブに移動します。

- ドロップダウンからタイプとしてOAuth 2.0を選択し、Get access tokenをクリックします。
- 上記の表から次の情報を追加します。
- [Advance Options]タブで、[Resource]フィールドに、コールバックURLと同じ値を追加します。この値は、JWTトークンの「AUD」値として返されます。
- postmanは認証フローを開始し、アクセストークンを使用するように要求します。
- [Add token to the header]を選択します。
- 唯一のアクセストークンのコピー





構成（SC構成とホスト構成）

SnapCenter MFA CLI認証

PowerShellとSCCLIでは、既存のコマンドレットに「**AccessToken**」というフィールドを1つ追加して拡張し、Bearerトークンを使用して関係するユーザを認証しました。

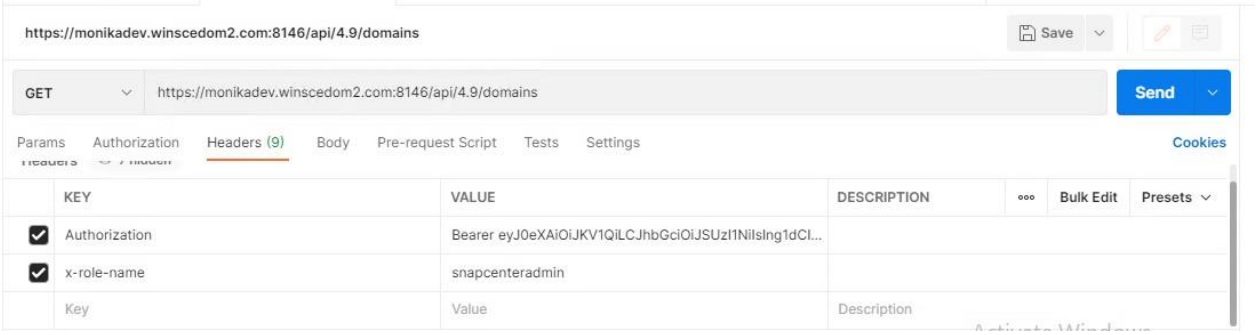
SYNTAX

```
Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port
<String>] [-RoleName <String>] [ -AccessToken <string>]
```

応答:このコマンドレットを実行するには、各ユーザのセッションを作成して、さらにSnapCenterコマンドレットを実行してください。

SnapCenter MFA RestAPI認証

Bearerトークンを***Authorization**の形式で使用し*、次の画像に示すように、REST APIクライアントで***type=Bearer トークン***を使用して(Postmanやswaggerなど)、ヘッダーにuser RoleNameを指定して、SnapCenterからの成功応答を取得します。



MFA REST APIのワークフロー

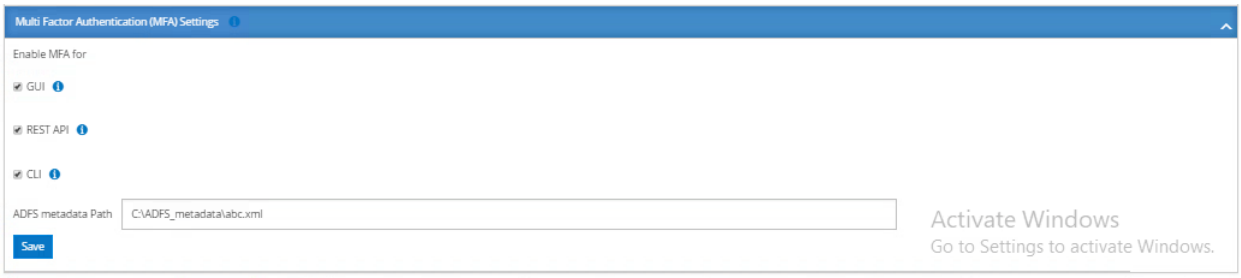
MFAがAD FSで構成されている場合、ユーザがREST APIを使用してSnapCenterアプリケーションにアクセスするときは、アクセス（Bearer）トークンを使用して認証する必要があります。
以下は、アクセストークンを取得し、それを使用して以降の要求（SnapCenter REST API）を認証して処理を実行する手順です。
AD FS MFAで認証するには、次の手順に従います。

1. Postman、Swagger UI、FireCampなどのRESTクライアントを使用する必要がある
2. アクセストークンを取得するためにAD FSエンドポイントを呼び出すようにPostmanを設定します。
3. ユーザーがボタンを押してアプリケーションのアクセストークンを取得すると、AD FS SSOページにリダイレクトされ、そこでAD資格情報を入力してMFAで認証する必要があります。
    1. AD FS SSOページにリダイレクトされます。
    2. [ユーザー名]テキストボックスに、ユーザー名または電子メールを入力します。ユーザ名は、user@domainまたはdomain\userの形式で指定する必要があります。
    3. [パスワード]テキストボックスにパスワードを入力します。
    4. [Log In]をクリックします。
    5. [サインインオプション]セクションで、認証オプションを選択し、（お客様の設定に応じて）認証します。
        1. [Push]：電話機に送信されるプッシュ通知を承認します。
        2. QRコード–Auth Pointモバイルアプリを使用してQRコードをスキャンし、アプリに表示される認証コードを入力します。
        3. [One-Timeime Password]：トークンのワンタイムパスワードを入力します。
4. サインイン/承認が成功した後。Access、ID、Refresh Tokenを含むポップアップが開きます。
5. このアクセストークンをコピーする必要があり、このアクセストークンをSnapCenter REST APIで使用して処理を実行します。
6. REST APIでは、ヘッダーセクションでアクセストークンとロール名を渡す必要があります。
7. SCはADFSからこのアクセストークンを検証します。有効なトークンの場合、SCはそれをデコードしてユーザー名を取得します。
8. [Username]と[Role Name]を使用して、SCはAPI実行のためにユーザを認証します。有効である場合は、結果を返します。そうでない場合は、エラーメッセージが返されます。

GUI、SCCLI、RestAPIの**SnapCenter MFA機能を有効または無効にする方法**

GUIインターフェイス

a. SnapCenter管理者としてSnapCenterサーバにログインします。
b. [設定]->[グローバル設定]->[MultiFactorAuthentication（MFA）設定]をクリックします。
c. MFAログインの有効化/無効化に必要なインターフェイス（GUI / RST API / CLI）を選択します。



PowerShellインターフェイス

GUI、REST API、PowerShell、およびscclでMultiFactorAuthenticationを有効にするには、次のPowerShell / CLIコマンドを実行します。

この構文例では、指定したAD FSメタデータファイルパスを使用してSnapCenter GUI、REST API、PowerShell、およびSCCLIConfiguredのMFAを有効にします。

```
C:\PS>Set-SmMultiFactorAuthentication -IsGuiMFAEnabled $true -
IsRestApiMFAEnabled     $true -IsCliMFAEnabled      $true -Path
C:\ADFS_metadata\FederationMetadata.xml
      IsGuiMFAEnabled = True
      ADFSConfigFilePath = C:\\ADFS_metadata\\FederationMetadata.xml
      SCConfigFilePath = c:\ProgramData\NetApp\SnapCenter\Package
Repository\SnapCenterMFAMetadata.xml
      IsRestApiMFAEnabled   = True
      IsCliMFAEnabled   =  True
      ADFSHostName = adfs19.ad19domain.com

 - IsGuiMFAEnabled: To enable GUI MFA Login. Value-> $true/$false
 - IsRestApiMFAEnabled: To enable RestAPI MFA Login. Value-> $true/$false
 - IsCliMFAEnabled: To enable PowerShell and sccli MFA Login. Value->
$true/$false
 -Path - The path parameter specifies the location of the AD FS MFA metadata XML
file.
```

GetSmMultiFactorAuthenticationコマンドレットを使用して、MFA構成のステータスと設定を確認します。

この構文例では、SnapCenter GUI、REST API、PowerShell、SCCLIのMFA設定を取得します。

```
C:\PS>Get-SmMultiFactorAuthentication

    IsGuiMFAEnabled = true
```

```
    ADFSConfigFilePath = C:\\ADFS_metadata\\FederationMetadata.xml
    SCConfigFilePath = c:\ProgramData\NetApp\SnapCenter\Package
    Repository\SnapCenterMFAMetadata.xml
    IsRestApiMFAEnabled   = false
    IsCliMFAEnabled   = false ADFSHostName
    = adfs19.ad19domain.com
```

SCCLIインターフェイス

```
# sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true -
IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path
"C:\ADFS_metadata\abc.xml"
  INFO: The command 'Set-SmMultiFactorAuthentication' executed successfully.
```

```
# sccli Get-SmMultiFactorAuthentication
 IsGuiMFAEnabled | IsRestApiMFAEnabled | IsCliMFAEnabled |
ADFSConfigFilePath     | SCConfigFilePath | ADFSHostName          |
false      | false        | true       | C:\ADFS_metadata\abc.xml   |          | win-
adfs-sc49.winscedom2.com |
```

REST API：

a. GUI、REST API、PowerShell、およびscclでMultiFactorAuthenticationを有効にするには、次のPOST APIを実行します。

パラメータ	Value
要求されたURL	/api/4.9/settings/multifactorauthentication
HTTPメソッド	投稿

リクエスト本文	{
	"IsGuiMFAEnabled": false,
	"IsRestApiMFAEnabled": true,
	"IsCliMFAEnabled": false,
	"ADFSConfigFilePath":
	"C:\\ADFS_METADATA\\abc.xml"
	}

応答本文	{
	"MFAConfiguration": {
	"IsGuiMFAEnabled": false,
	"ADFSConfigFilePath":
	"C:\\ADFS_METADATA\\abc.xml",
	"SCConfigFilePath": null,
	"IsRestApiMFAEnabled": true,
	"IsCliMFAEnabled": false,
	"ADFSHostName": "win-adfs-
	sc49.winscedom2.com"
	}
	}

b. 以下のGET APIを使用して、MFA構成のステータスと設定を確認してください。

パラメータ	Value
要求されたURL	/api/4.9/settings/multifactorauthentication
HTTPメソッド	取得

応答本文	{
	"MFAConfiguration": {
	"IsGuiMFAEnabled": false,
	"ADFSConfigFilePath": "C:\\ADFS_METADATA\\abc.xml",
	"SCConfigFilePath": null,
	"IsRestApiMFAEnabled": true,
	"IsCliMFAEnabled": false,
	"ADFSHostName": "win-adfs-sc49.winscedom2.com"
	}
	}

証明書ベースの認証

証明書ベースの認証は、デジタル証明書を使用した認証を改善するセキュリティ機能です。証明書ベースの認証は、従来のユーザー名/パスワード認証よりも強力なセキュリティを提供します。暗号鍵とデジタル証明書に依存しているため、権限のないユーザーが有効なユーザーになりすましにくくなります。証明書ベースの認証は、SnapCenterプラグインホストにアクセスしようとする各ユーザの信頼性を検証します。秘密鍵なしでSnapCenterサーバ証明書をエクスポートし、プラグインホストの信頼されたストアにインポートする必要があります。この機能は、双方向SSLが設定されたシステム上で動作します。

SnapCenterサーバからCA証明書をエクスポートします。

Microsoft管理コンソール（MMC）を使用して、SnapCenterサーバからプラグインホストにCA証明書をエクスポートする必要があります。

前提条件：双方向SSLが設定されている必要があります。

手順

1. 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]**の順にクリックします。
2. [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。
3. [証明書スナップイン]ウィンドウで、**[コンピュータアカウント]**オプションを選択し、**[完了]**をクリックします。
4. **[コンソールルート] > [証明書-ローカルコンピュータ] > [個人] > [証明書]** の順にクリックします。
5. SnapCenterサーバで使用される調達CA証明書を右クリックし、**[All Tasks] > [Export]**を選択してエクスポートウィザードを開始します。
6. 次の手順でウィザードを完了します。

このウィザードウィンドウでは...	操作
秘密キーのエクスポート	[**いいえ**、秘密鍵をエクスポートしない]オプションを選択し、**[次へ]**をクリックします。
エクスポートファイル形式	変更しないで、**[次へ]をクリックします**。
ファイル名	**[参照]**をクリックし、証明書を保存するファイルパスを指定して、**[次へ]**をクリックします。
証明書のエクスポートウィザードの完了	概要を確認し、**[Finish]**をクリックしてエクスポートを開始します。

注：SnapCenter HA構成はサポートされません。

WindowsホストプラグインへのCA証明書のインポート

エクスポートされたSnapCenterサーバCA証明書の使用Microsoft管理コンソール(MMC)を使用して、問題の証明書をSnapCenter Windowsホストプラグインにインポートする必要があります。

手順

1. 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]**の順にクリックします。
2. [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**。
3. [証明書スナップイン]ウィンドウで、**[コンピュータアカウント]**オプションを選択し、**[完了]**をクリックします。
4. **[コンソールルート] > [証明書-ローカルコンピュータ] > [個人] > [証明書]**の順にクリックします。
5. 「**個人**」フォルダを右クリックし、**[すべてのタスク] > [インポート]**を選択してインポートウィザードを開始します。
6. 次の手順でウィザードを完了します。

このウィザードウィンドウでは...	操作
店舗の場所	変更しないで、**[次へ]をクリックします**。
インポートするファイル	.cerファイル形式で終了するSnapCenterサーバ証明書を選択します。
証明書ストア	変更しないで、**[次へ]をクリックします**。
証明書のインポート ウィザードの完了	概要を確認し、**[Finish]をクリックし**てインポートを開始します。

証明書ベースの認証を有効または無効にするPowerShellコマンドレット

- クライアント証明書ベースの認証を有効にするには：

```
Set-SmConfigSettings -Agent -configSettings
@{"EnableClientCertificateAuthentication"="true"} -HostName <<hostname>>
```

- クライアント証明書ベースの認証を無効にするには：

```
Set-SmConfigSettings -Agent -configSettings
@{"EnableClientCertificateAuthentication"="false"} -HostName <<hostname>>
```

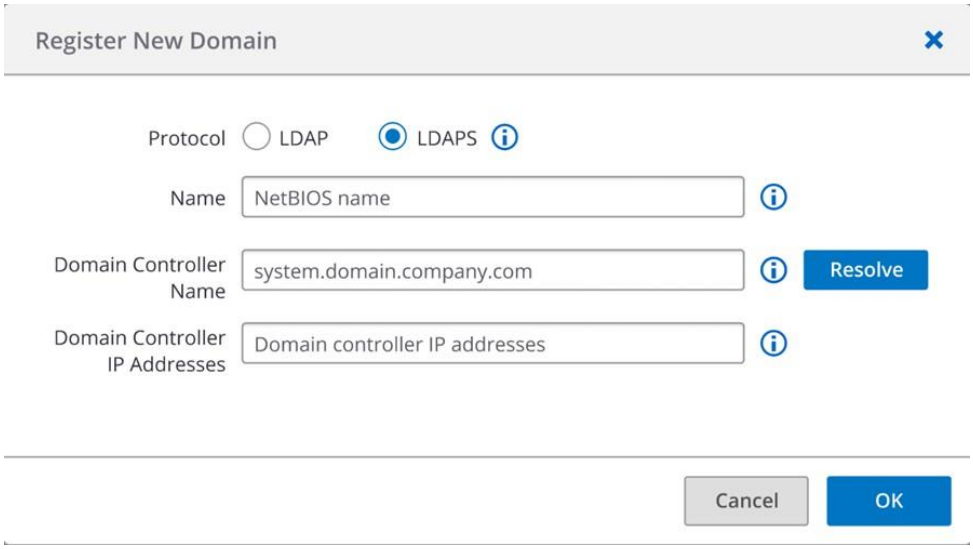
LDAPS

SnapCenterは、Windows Active Directoryとの通信にLDAPS（LDAP over SSL）プロトコルをサポートしています。許可されたCA証明書は、セキュアな通信のためにバックエンドで使用されます。

スタンドアロンActive Directory

- セキュアなActive Directory接続を選択するには、LDAPSオプションを明示的に選択する必要があります。
- 既存のドメイン名（domain.com）ユーザー入力フィールドをドメインコントローラ名（system.domain.company.com）に置き換えます。これは、Active Directoryとの通信を開始するための必須入力です。
- ドメインコントローラ名は、DNSまたは `etc/hosts` エントリを介して解決される必要があります。
- 自動解決IPアドレスは、IPv4およびIPv6（64ビット）の形式でサポートされます。
- IPアドレスの手動入力はサポートされていません。自動的に解決されます。ドメインコントローラのIPアドレスフィールドは編集できません。
- 指定したドメインコントローラ名は、次のチェックに対して検証されます。
  - Active Directoryホストに到達できるかどうか。
  - Active Directoryホストまたは通常のWindowsサーバで動作しているActive Directory以外のホストとして検出できます。
  - LDAPSポートと通信できるかどうか。

図2）[New domain registration]ダイアログボックス



ハイアベイラビリティ（HA）Active Directory

上記のスタンドアロンの手順はすべて適用できます。

- HA Active Directoryをサポートするために、ユーザ入力[Domain Controller Name]はカンマで区切った値として入力を受け取り、複数のドメインコントローラ名を1つのエントリとして格納します。
- ユーザ入力の例は、dc01.domain.company.com、dc02.domain.company.comです。
- いずれかのノードで検証に失敗すると、エンドユーザにエラーがスローされます。

カスタムポートのサポート

- デフォルトのLDAPSポートは **636**です。
- SnapCenterサーバ `web.config` ファイルに新しいキーと値のペアを手動で追加して、カスタムポートのサポートを拡張することもできます。

  注： web.configの場所（デフォルトのパス）：`C:\Program Files\NetApp\SnapCenter WebApp\App_Data\Web.config`

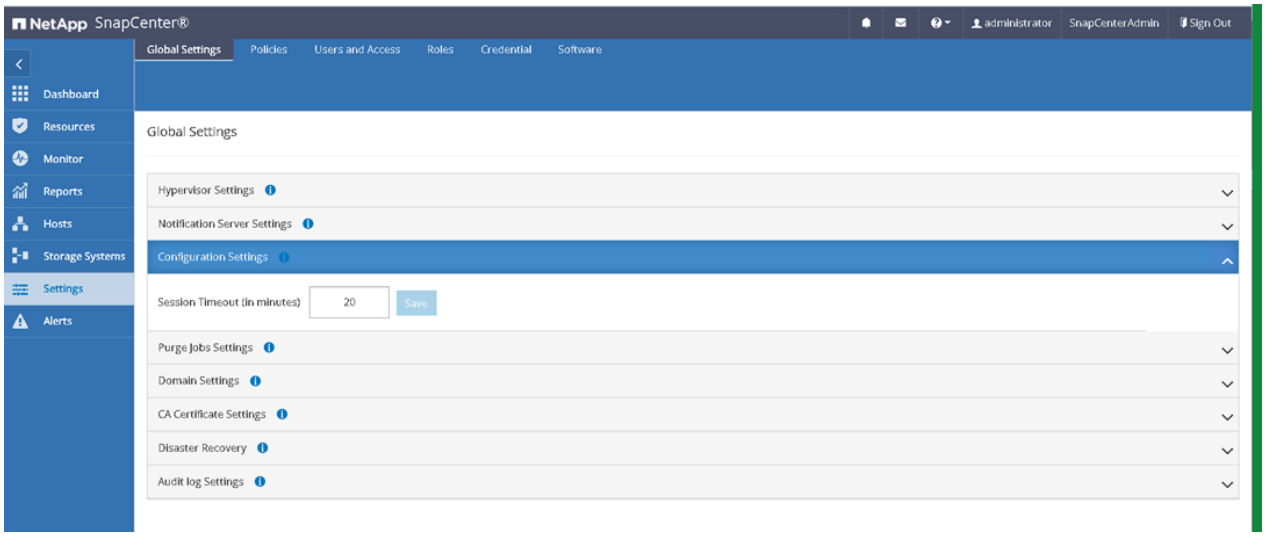
注: キーと値のペア:<を`add key="LDAPSPort" value="3269" />` appsettingセクションに追加する必要があります。

- 更新された値は、SnapCenterサーバをアップグレードまたは修復したあとも維持されます。
- LDAPS GC（グローバルカタログ）ポートは **3269**です。
- Active Directory GCサーバには、親ドメインやすべてのサブドメイン（子ドメイン）オブジェクトなど、Active Directoryツリー内のすべてのオブジェクトのコピーがあります。
- カスタムポートを設定したら、新しいドメインの登録を続行できます。
- でデフォルトのLDAPS通信ポートを変更したあとも、サービスを再起動する必要はありません`web.config`。

非アクティブまたはタイムアウト

非アクティブなWebページのデフォルトのセッションタイムアウトは20分です。この値は設定可能です。

図3）SnapCenterのデフォルトのセッションタイムアウトのダイアログボックス



監査ログ

監査ログは、SnapCenterサーバのアクティビティごとに生成されます。監査ログは、デフォルトでインストールされた場所で保護され`C:\Program Files\NetApp\SnapCenter WebApp\audit\`ます。

このセクションでは、UIからの監査ログの設定、整合性チェック、およびsyslogサーバへの転送について説明します。

監査ログの保護

監査ログは、監査イベントごとにデジタル署名されたダイジェストが生成され、不正な変更から保護されます。生成されたダイジェストは別の監査チェックサムファイルに保持され、コンテンツの整合性を保証するために定期的な整合性チェックが行われます。

構成

監査ログの設定は、UIおよびPowerShellコマンドレットを使用して行うことができます。監査の整合性チェックスケジュールを有効または無効にすることもできます。

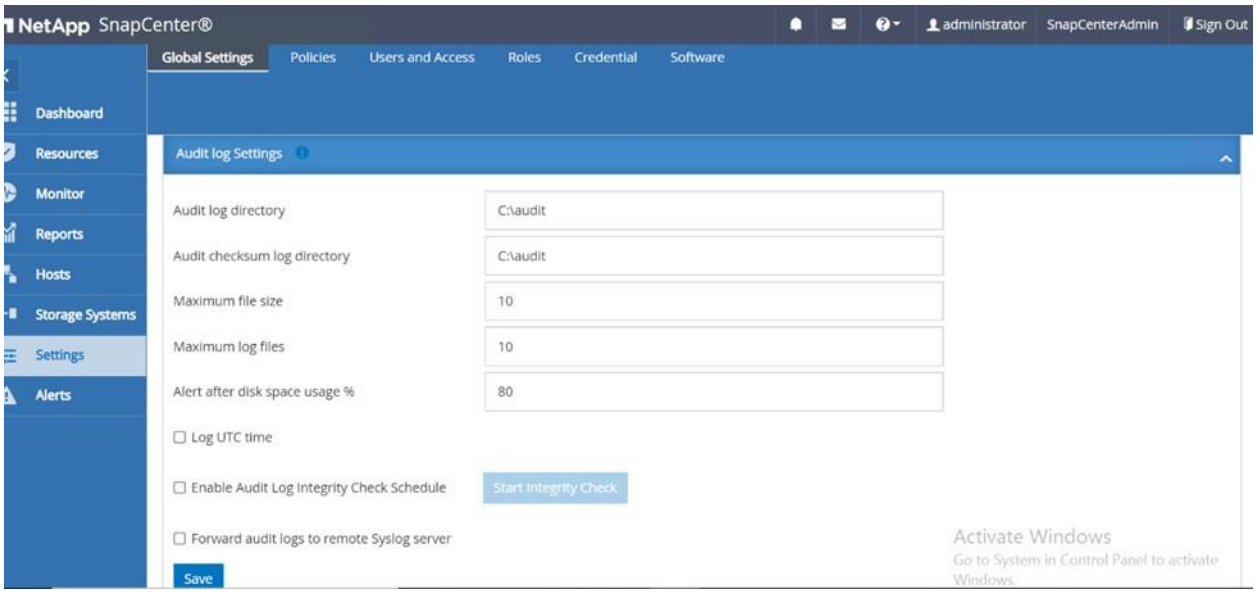
監査ログディレクトリと監査チェックサムログディレクトリは、SnapCenterサーバのローカルドライブにのみ配置できます。共有ドライブまたはネットワークマウントドライブはサポートされていません。

監査の整合性チェックが有効または無効になると、SnapCenterアラートが生成されて管理者に通知されます。

UI

監査設定は、 **SnapCenter > Global Settings > Audit Log Settings**のUIで設定できます。

図4）監査ログの設定



PowerShellコマンド

監査設定は、PSコマンドレット、`Get-SmAuditSettings` およびを使用して構成できます `Set- SmAuditSettings`。

UIおよびPSのコマンドレットを使用して、監査ログの設定と取得を行うことができます。

```
MaxFileSize, MaxSizeRollBackups, UniversalTime, LogDirectory and DiskSpaceLimitPercentage
```

```
PS C:\Users\Administrator> Set-SmAuditSettings

cmdlet Set-SmAuditSettings at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
MaxFileSize: 10
MaxSizeRollBackups: 2
AuditLogDirectory: C:\SC_Aduit\audit
AuditChecksumLogDirectory: C:\SC_Audit\checksum
DiskSpaceLimitPercentage: 80
EnableAuditIntegrityCheckSchedule: true
EnableSyslogServer: true
SyslogProtocol: TCP
SyslogServerHost: 1.1.1.1
SyslogServerPort: 111
RfcFormat: RFC5424


MaxFileSize                       : 10
MaxSizeRollBackups                : 2
UniversalTime                     : False
AuditLogDirectory                 : C:\SC_Aduit\audit
AuditChecksumLogDirectory         : C:\SC_Audit\checksum
DiskSpaceLimitPercentage          : 80
EnableSyslogServer                : True
SyslogProtocol                    : TCP
SyslogServerHost                  : 1.1.1.1
SyslogServerPort                  : 111
RfcFormat                         : RFC5424
EnableAuditIntegrityCheckSchedule : True


PS C:\Users\Administrator> Get-SmAuditSettings


MaxFileSize                       : 10
MaxSizeRollBackups                : 2
UniversalTime                     : False
AuditLogDirectory                 : C:\SC_Aduit\audit
AuditChecksumLogDirectory         : C:\SC_Audit\checksum
DiskSpaceLimitPercentage          : 80
EnableSyslogServer                : True
SyslogProtocol                    : TCP
SyslogServerHost                  : 1.1.1.1
SyslogServerPort                  : 111
RfcFormat                         : RFC5424
EnableAuditIntegrityCheckSchedule : True
```

注: これらの設定はJSONファイルとして保存され -\SnapCenter WebApp\Audit_LogSettings.jsonます。

通知

次の場合、SnapCenterアラートを発行して管理者に通知できます。

- Audit integrity checks enabledアラート
- Audit Integrity Checks disabledアラート
- Low disk spaceアラート
- Audit integrity check failureアラート
- Audit failureアラート

E メール アラート

整合性検証に失敗した場合は、Eメール通知が送信されてSnapCenter管理者に通知されます。

監査ログの送信

監査ログをsyslogサーバに安全に送信して、監査ログファイルの機密性と整合性を保護できます。SnapCenter UIまたはPowerShellで次の手順を実行することで、監査ログを安全に送信できます。

各監査レコードはsyslogサーバにリアルタイムで送信され、整合性検証のためにセカンダリコピーが保持されます。

構成

監査ログの設定は、UIおよびPSのコマンドレットを使用して実行できます。監査設定にsyslogサーバの新しいフィールドが追加されます。

表2）監査ログの設定時に考慮すべきパラメータ

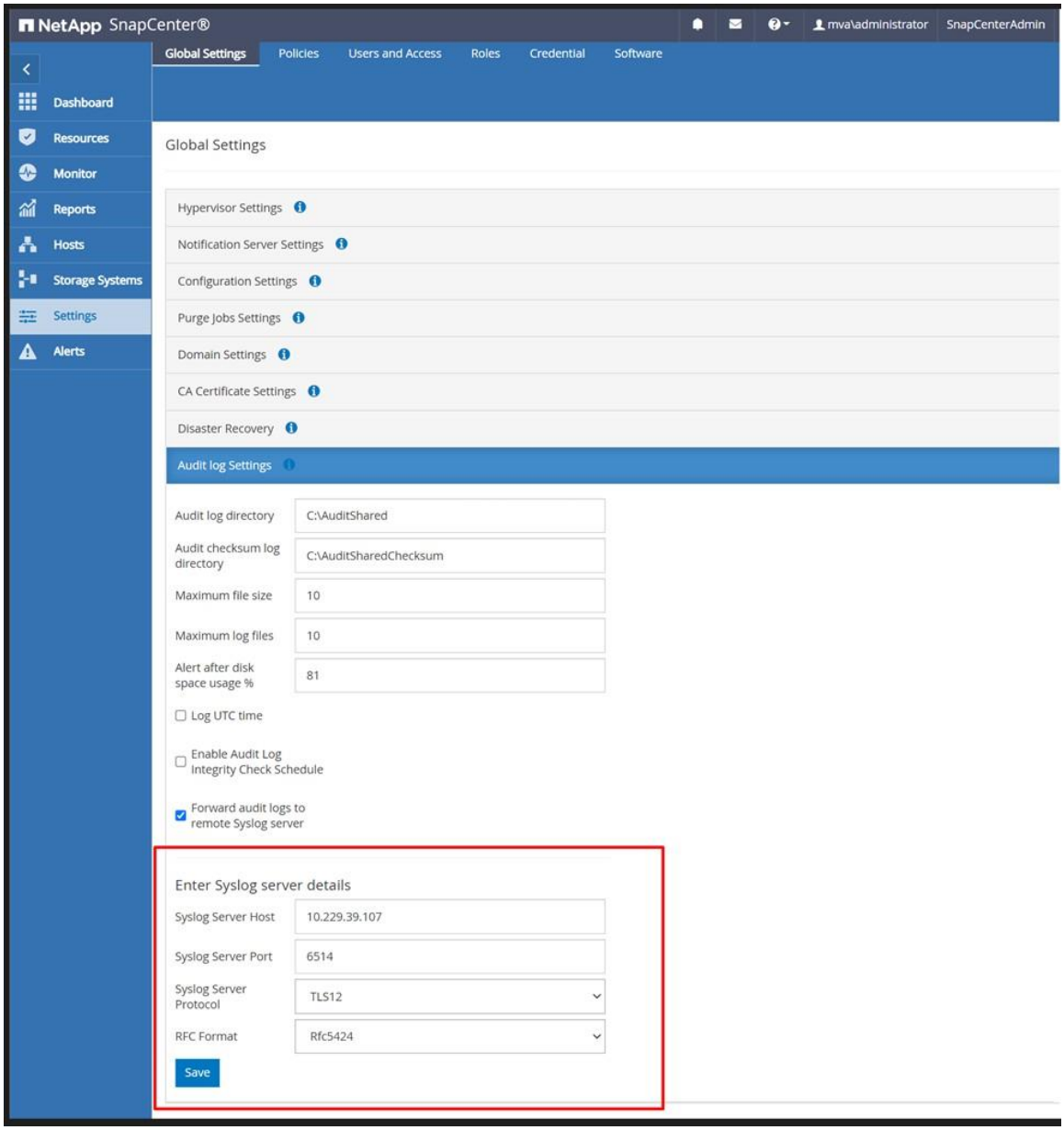
パラメータ	詳細
SyslogServerPort	syslogサーバのポート（0 ~ 65535）
SyslogServerHost	リモートsyslogサーバのIP
SyslogProtocol（SyslogProtocol）	許可されているプロトコル。サポートされる値：UDP、TCP、またはTransport Layer Security（TLS）1.2、TLS 1.3（UDPはRFC3164でのみサポートされます）
SyslogFormat	Rfc5424またはRfc3164
EnableSyslogServer	syslogへのログの転送を有効または無効にするように指定するPowerShellスイッチパラメータ

注: これらの設定はJSONファイルとして保存され `-\SnapCenter WebApp\Audit_LogSettings.json`ます。

UI

監査設定は、 **SnapCenter** > **Global Settings** > **Audit log SettingsのUIで設定できます**。

図5）syslogサーバの設定



PowerShellコマンド

syslogサーバの監査設定は、PSコマンドレット：を使用して構成できます。`Set-SmAuditSettings`監査設定はPSコマンドレットで確認できます `Get-SmAuditSettings`。

```
PS C:\Users\Administrator> Set-SmAuditSettings

cmdlet Set-SmAuditSettings at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
MaxFileSize: 10
MaxSizeRollBackups: 2
AuditLogDirectory: C:\SC_Aduit\audit
AuditChecksumLogDirectory: C:\SC_Audit\checksum
DiskSpaceLimitPercentage: 80
EnableAuditIntegrityCheckSchedule: true
EnableSyslogServer: true
SyslogProtocol: TCP
SyslogServerHost: 1.1.1.1
SyslogServerPort: 111
RfcFormat: RFC5424


MaxFileSize                       : 10
MaxSizeRollBackups                : 2
UniversalTime                     : False
AuditLogDirectory                 : C:\SC_Aduit\audit
AuditChecksumLogDirectory         : C:\SC_Audit\checksum
DiskSpaceLimitPercentage          : 80
EnableSyslogServer                : True
SyslogProtocol                    : TCP
SyslogServerHost                  : 1.1.1.1
SyslogServerPort                  : 111
RfcFormat                         : RFC5424
EnableAuditIntegrityCheckSchedule : True


PS C:\Users\Administrator> Get-SmAuditSettings


MaxFileSize                       : 10
MaxSizeRollBackups                : 2
UniversalTime                     : False
AuditLogDirectory                 : C:\SC_Aduit\audit
AuditChecksumLogDirectory         : C:\SC_Audit\checksum
DiskSpaceLimitPercentage          : 80
EnableSyslogServer                : True
SyslogProtocol                    : TCP
SyslogServerHost                  : 1.1.1.1
SyslogServerPort                  : 111
RfcFormat                         : RFC5424
EnableAuditIntegrityCheckSchedule : True
```

syslogサーバを確認しました

SnapCenterは、syslogサーバのSplunkとsyslogウォッチャーで検証されます。SnapCenterでは、次の形式のsyslogサーバがサポートされます。

- BSDおよびRFC 5424タイプ
- Syslog-over-TCP-over-TLSおよびUDP
- TLSシンプル
- TLS over TCP（TLSにはルート証明書が必要です）

通知

syslogサーバへの監査レコードの送信に失敗した場合に管理者に通知するために、次のSnapCenterアラートが生成されます。

- Syslog server enabledアラート

- Syslog server disabledアラート
- syslog server failureアラートへの監査ログ

MySQLリポジトリ・データベースの保護

SnapCenterは独自のMySQLリポジトリを使用してメタデータを格納します。製品のインストールを安全かつ簡単に行うために、複雑な文字セットを使用してMySQLパスワードが自動的に生成されます。

カスタムMySQLパスワードを設定する

コンプライアンス要件がないかぎり、パスワードをリセットしてMySQLデータベースにアクセスする必要はありません。リポジトリデータベースへの変更は、テクニカルサポートの慎重な観察の下で行う必要があります。

ユーザパスワードポリシーの推奨事項に基づいてMySQLパスワードを更新するには、次の手順を実行します。

1. SnapCenterサーバで管理者としてPowerShellを起動します。
2. と入力し `Open-SmConnection`ます。
3. SnapCenterAdminロールを持つユーザのクレデンシャルを入力します。
4. と入力し `Set-SmRepositoryPassword`ます。
5. 新しいパスワードを設定し、パスワードを再入力してパスワードが一致していることを確認します。

SnapCenterリポジトリのリモートアクセスの制限

この手順は、ファイアウォールルールを追加してMySQLポートのインバウンド通信を制限することで、SnapCenterリポジトリのセキュリティレベルを強化します。

1. システム構成（パブリック、プライベート、またはドメイン）に基づいて、それぞれのレベルのWindowsファイアウォールを有効にします。
2. 次のPowerShellコマンドを実行して古いファイアウォールルールを削除し、実行時のファイアウォール優先順位の問題を回避します。

```
Remove-NetFirewallRule -DisplayName "Port 3306"
```

3. SnapCenterサーバの設定を確認します。
   - スタンドアロンのSnapCenter構成の場合は、次のPowerShellコマンドを実行します。

```
New-NetFirewallRule -DisplayName "Port 3306" -Direction Inbound -LocalPort 3306 -Protocol TCP -
Action Block
```

   - クラスタSnapCenter構成の場合は、各ノードで次のPowerShellコマンドを実行します。

```
Node1: New-NetFirewallRule -DisplayName "Port 3306" -Direction Inbound -LocalPort 3306 -Protocol
TCP -Action Allow -RemoteAddress <Node2_IP_address>
Node2: New-NetFirewallRule -DisplayName "Port 3306" -Direction Inbound -LocalPort 3306 -Protocol
TCP -Action Allow -RemoteAddress <Node1_IP_address>
```

ストレージ設定

このセクションでは、SnapCenterにONTAPストレージを追加し、両者の間にセキュアな接続を確立するために必要な最小限の権限について説明します。接続されると、SnapCenterはデータベースまたはアプリケーションリソースをホストするストレージレイアウトを検出します。

SnapCenterおよびONTAPがCA証明書を使用して通信する場合は、次の手順を実行します。

4. クラスタまたはSVMの.pemファイルをONTAPからダウンロードし、.crtファイルに変換します（OpenSSLを使用）。
5. SnapCenterサーバ、および信頼されたルート証明機関内のプラグインマシンまたはプラグインマシンにCA証明書をインストールします。

6. SnapCenterサーバでCA証明書を有効にします。
7. `SMCoreServiceHost.exe.Config` SnapCenterサーバおよびプラグインマシンのファイルに次のキーを追加します。

```
<add key="EnableSSLValicationWithPSTKCommand" value="true" />
```

- クラスタまたはSVMの詳細をホストファイルに追加します。
- SnapCenterサーバとプラグインマシンでSMCoreサービスを再起動します。
- 完全修飾ドメイン名（FQDN）を使用してクラスタまたはSVMを追加します。

最小権限を持つSVMロールの作成

ONTAPで新しいSVMユーザのロールを作成するときは、ONTAP CLIコマンドをいくつか実行する必要があります。このロールは、ONTAPのSVMをSnapCenterで使用するように設定し、vsadminロールを使用しない場合に必要です。

手順

1. ストレージシステムで、ロールを作成してすべての権限を割り当てます。

```
security login role create -vserver <svm_name\>- role <SVM_Role_Name\> -cmddirname <permission\>
```

2. 権限ごとにこのコマンドを繰り返します。
3. ユーザを作成し、そのユーザにロールを割り当てます。

```
security login create -user <user_name\> -vserver <svm_name\> -application ontapi -authmethod
password -role <SVM_Role_Name\>
```

4. ユーザのロックを解除します。

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

SVMロールの作成と権限の割り当てのためのONTAP CLIコマンド

次のONTAP CLIコマンドを実行して、SVMロールを作成し、権限を割り当てます。

- `security login role create -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -vserver SVM_Name -access all`
- `security login role create -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -vserver SVM_Name -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all`

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all`

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all`
- `security login role create -vserver SVM_name cmddirname "volume modify" -access all`
- `security login role create -vserver SVM_name cmddirname "volume offline" -access all`
- `security login role create -vserver SVM_name cmddirname "volume online" -access all`
- `security login role create -vserver SVM_name cmddirname "volume qtree create" -access all`
- `security login role create -vserver SVM_name cmddirname "volume qtree delete" -access all`
- `security login role create -vserver SVM_name cmddirname "volume qtree modify" -access all`
- `security login role create -vserver SVM_name cmddirname "volume qtree show" -access all`
- `security login role create -vserver SVM_name cmddirname "volume restrict" -access all`
- `security login role create -vserver SVM_name cmddirname "volume show" -access all`
- `security login role create -vserver SVM_name cmddirname "volume snapshot create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all`

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname “volume managed-feature” -access all`

最小権限を持つONTAPクラスタロールの作成

SnapCenterで処理を実行するときにONTAP管理者ロールを使用する必要がないように、最小限の権限でONTAPクラスタロールを作成する必要があります。複数のONTAP CLIコマンドを実行して、ONTAPクラスタロールを作成し、最小限の権限を割り当てることができます。

1. ストレージシステムで、ロールを作成してすべての権限を割り当てます。

```
security login role create -vserver <cluster_name\>- role <role_name\> -cmddirname <permission\>
```

2. 権限ごとにこのコマンドを繰り返します。

3. ユーザを作成し、そのユーザにロールを割り当てます。

```
security login create -user <user_name\> -vserver <cluster_name\> -application ontapi -authmethod
password -role <role_name\>
```

4. ユーザのロックを解除します。

```
security login unlock -user <user_name\> -vserver <cluster_name\>
```

クラスタ ロールの作成と権限の割り当てのためのONTAP CLIコマンド

次のONTAP CLIコマンドを実行して、クラスタロールを作成し、権限を割り当てます。

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly`
- `security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all`
- `security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all`

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all`

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all`
- `security login role create -vserver Cluster_name -role Role Name -cmddirname "volume file show-disk-usage" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all`

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all`

暗号の設定

デフォルトでは、SnapCenterはTLS1.3、TLS1.2、TLS1.1、およびTLS1.0プロトコルをサポートしています。Windows Server 2012 OSでは、TLS1.0の拡張サポートのみを提供しています。

TLS 1.0を無効にする

TLS 1.0プロトコルを無効にするには、SnapCenterサーバおよびプラグインホストで次のコマンドレットを実行します。パラメータ名は、 `DisableTLS1.0` プロトコルスコープを有効または無効にします。

```
Open-SmConnection -Credential <user_credentilas> -RoleName <only if user has multiple role>
Set-SmConfigSettings -Server -configSettings @{"DisableTLS1.0"="True";}
```

```
Set-SmConfigSettings -Agent -HostName <Plugin Host Name> -configSettings
@{"DisableTLS1.0"="True";}
```

Windows用の強化された暗号スイート

SnapCenterサーバーが実行されているオペレーティングシステム(OS)に基づいて、Windowsはネットワーク通信全体のセキュリティを提供するために特定のSSL暗号スイートのセットをサポートしています。

Windows Server 2008およびWindows Server 2012用のSSL暗号スイートの設定手順

1. コマンドプロンプトでと入力し `gpedit.msc`、**Enter**キーを押します。ローカルグループポリシーエディタが表示されます。
2. **[コンピュータの構成] > [管理用テンプレート] > [ネットワーク] > [SSL設定]**の順に移動し、**[SSL Cipher Suite Order]**をダブルクリックします。
3. [SSL Cipher Suite Order]ウィンドウで、**[Enabled]**をクリックします。
4. [Options]ペインで、[SSL Cipher Suites]テキストボックスの内容全体を次の暗号リストに置き換えます。

```
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
```

5. システムを再起動します。

Windows Server 2016以降でSSL暗号スイートを設定する手順

最新のOSバージョンでは、推奨されないプロトコル、暗号、ハッシュ、およびキー交換を無効にしてから、推奨される設定を有効にすることで、SChannelレジストリキー設定を使用して暗号スイートの構成を直接制御できます。

手動のレジストリキー設定または IISCryptoツール2.0(またはそれ以上)を使用して、必要なSChannel設定のセットを選択および選択解除できます。デフォルトでは、SChannel設定エントリはレジストリに存在しません。必要なコンポーネントを無効または有効にするには、強制的に作成する必要があります。

表3）WindowsのSChannel設定

SChannel	有効にする	無効にする
サーバプロトコル（クライアントとサーバ）	TLS 1.2、TLS 1.3	• マルチプロトコルUnified Hello • PCT 1.0 • SSL 2.0 • SSL 3.0 • TLS 1.0 • TLS 1.1
暗号	• AES 128 • AES 256	• NULL • DES 56 • RC2 40/128 • RC2 56/128 • RC2 128 • RC4 40/128 • RC4 56/128

SChannel	有効にする	無効にする
		• RC4 64/128 • RC4 128 • トリプルDES 168
ハツシユ	• SHA 256 • SHA 384 • SHA 512	• MD5 • SHA
キーエクスチェンジ	• Diffie-Hellam • ECDH	• PKCS

これらの設定を変更したら、システムを再起動します。

例1：TLS 1.2プロトコルを有効にするためのレジストリ設定

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProv iders\SCHANNEL\Protocols\TLS
1.2\Client] "DisabledByDefault"=dword:00000000 "Enabled"=dword: ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvi ders\SCHANNEL\Protocols\TLS
1.2\Server] "DisabledByDefault"=dword:00000000 "Enabled"=dword: ffffffff
```

例2: IISCryptoツールv2.0以上の使用

- IISCryptoツールv2.0以降では、ツールで選択した内容に基づいてレジストリキーの設定が自動的に更新されます。
- システムを再起動して、設定済みのSChannel設定を有効にします。

証明書-一方向および相互SSL

SnapCenterでは、サーバとプラグインホストの間のクロス通信用にCA証明書がサポートされています。

一方向SSL

このセクションでは、Microsoft Certreqを使用して署名付きSSL証明書を生成する方法について説明します。これは、次の点で役立ちます。

- 証明書署名要求（CSR）の生成
- 生成されたCSRを使用してCAから取得した証明書のインポート

このプロセスでは、証明書に秘密鍵が関連付けられていることが保証されます。Microsoft Certreqツールは、Windows Server 2008 R2システムでデフォルトで使用できるため、CSRを生成できます。

注：

- ツールは構成ファイルを使用して証明書要求を生成します。
- 同じサーバで完全な手順に従っていることを確認してください。

構成request.inファイルを作成します。

1. 次の内容を使用して、構成request.inファイルを作成します。

```
;----------------------------------- request.inf ----------------------------------------
[Version]
Signature="$Windows NT$"
[NewRequest]
Subject = "CN=View_Server_FQDN, OU=Organizational_Unit_Name, O=Organization_Name, L=City_Name,
S=State_Name, C=Country_Name"
; replace the attributes appropriately in the above line, refer example in the next step.
KeySpec = 1
KeyLength = 2048 ; Can be 2048, 4096 or 8192 - Larger key sizes are more secure
HashAlgorithm = SHA256 ; Can be SHA256, SHA384, SHA512 - Higher values are more secure
KeyUsage = 0xA0 ; Digital Signature, Key Encipherment
```

```
MachineKeySet = TRUE ; The key belongs to the local computer account
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
Exportable = TRUE
SMIME = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderType = 12
RequestType = PKCS10
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1 ; this is for Server Authentication
[RequestAttributes]
; SAN= dns=FQDN_you_require&dns=other_FQDN_you_require
;-----------------------------------------------------------------------------------------------
```

2. 必要に応じて、次の変更を適用します。
3. 例：

```
Subject = "CN=view.company.com , OU=IT, O=ABCCompany, L=Sunnyvale, S=California, C=US
```

4. Subject Alternative Name（SAN）を使用している場合は、この行のコメントを解除し、SAN属性をFQDNで更新します。
5. 例：

```
SAN= dns= server1.domain.com&dns= server2.domain.com&dns= server3.domain.com&dns=
server4.domain.com&dns= server5.domain.com
```

6. request.inファイルを保存して閉じます。

構成ファイルを使用して**CSR**を生成する手順

1. **cmd.exe**を右クリックして **[管理者として実行]**を選択し、コマンドプロンプトを開きます。
2. request.inファイルが保存されている場所にディレクトリを変更します。

例：

```
cd C:\certificates
```

3. CSRファイルを生成するには、このコマンドを実行します。

```
certreq.exe -new request.inf certreq.csr
```

4. 生成されたcertreq.csrCSRファイルをテキストエディタで開き、ファイルのテキストをコピーするか、CSRファイルを直接アップロードしてCAに送信し、CAから署名済み証明書を取得します。

   注： 必要に応じて、CAから署名済み証明書、ルートCA証明書、および中間CA証明書が提供されます。CAによってフォーマットのリストが異なります。

5. 証明書テキストを新しいファイルに保存するか、cert.cer証明書要求が生成されたサーバにCERファイルという名前の証明書をダウンロードします。
6. ルート root.cer intermediate.cer 証明書と中間CA証明書を、という名前のファイルと、証明書要求が生成されたサーバ上のファイルに保存します。異なるCAのファイル形式は .cer、またはのいずれかに .crtなります。

署名済み証明書のインポート

1. **cmd.exe**を右クリックして **[管理者として実行]**を選択し、コマンドプロンプトを開きます。
2. cert.cerファイルが保存されている場所にディレクトリを変更します。
3. 例：

```
cd C:\certificates
```

4. 署名済み証明書をインポートするには、次のコマンドを実行します。

```
certreq.exe -accept -machine root.cer
```

```
certreq.exe -accept -machine intermediate.cer
certreq.exe -accept -machine cert.cer
```

5. インポートが完了すると、証明書がローカルマシンの個人証明書ストアにインポートされます。
6. 管理者としてMMCを開きます。
7. **[ファイル]**、**[スナップインの追加と削除]**の順にクリックするか、**Ctrl**キーを押しながら**M**キーを押します。
   a. 使用可能なスナップインで証明書を選択し、**[追加]**をクリックします。必ずコンピュータアカウントを選択してください。
   b. **[次へ]**、**[完了]**の順にクリックします
8. **Personal** > **Certificates**フォルダをダブルクリックし、最近インポートしたSSL Certificateをその名前で選択します。
9. 最近調達したCA証明書を右クリックし、**All Tasks** > **Export**を選択し、**Export with Private Key**オプションを選択してウィザードを続行します。次に、デフォルトのオプションに進みます。
10. MMCウィザードで、**Trusted Root Certification Authorities** フォルダを右クリックし、**All Tasks** > **Import**を選択します。
    a. インポートする証明書には秘密鍵がバンドルされている必要があります（サポートされている形式は`*.pfx`、`*p12`、`*.p7b`です）。秘密鍵が証明書にバンドルされていない場合は、秘密鍵をSnapCenterサーバに使用することはできません。
    b. 秘密鍵のパスワードを入力し、デフォルトのオプションに進みます。次に[Finish]をクリックします。

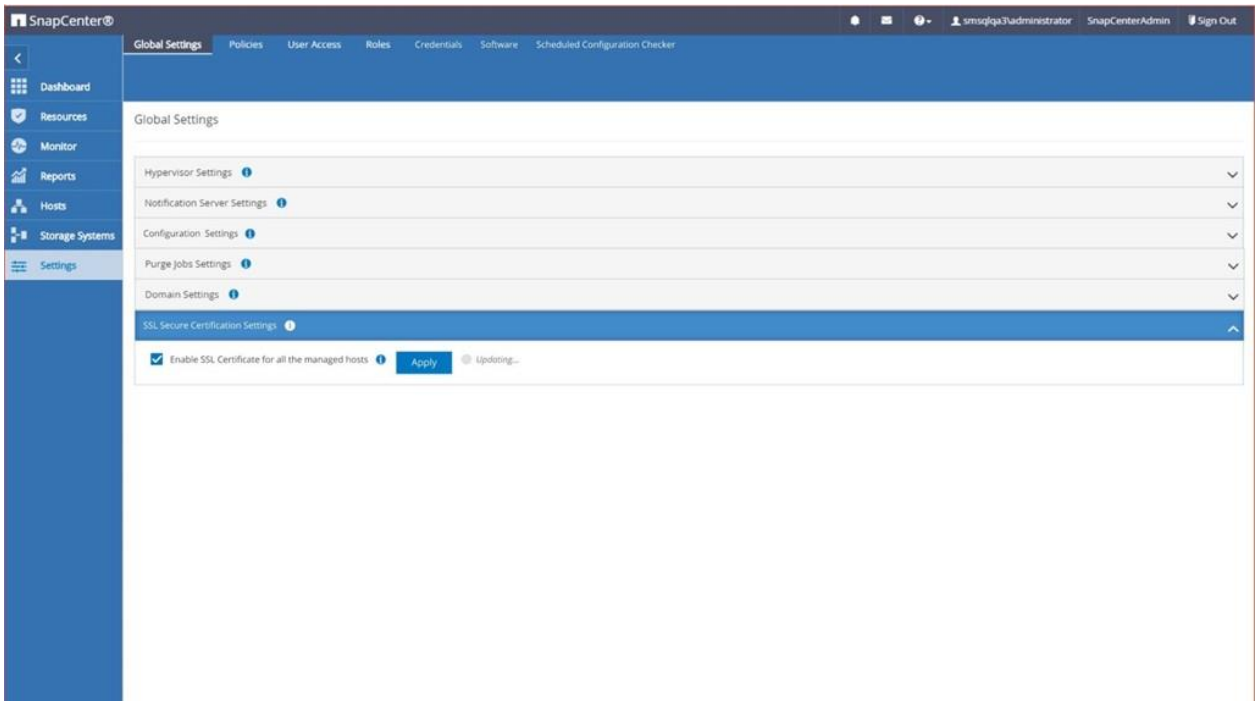
ルートCA証明書と中間CA証明書について手順8と9を繰り返します。これらの証明書には秘密鍵オプションは使用できません。

SnapCenterサーバのCA証明書を有効にする

認証局は、Secure Sockets Layer（SSL）証明書を発行する信頼されたエンティティです。これらのデジタル証明書は、暗号化によってエンティティを公開鍵とリンクするために使用されるデータファイルです。SnapCenterでは、許可されたCA証明書を使用したサーバとプラグインの相互通信がサポートされるようになりました。すべてのHTTPS呼び出しは、セキュアなSSL標準に基づいて検証されます。

GUIのグローバル設定ページには、SnapCenterレベルでCA証明書機能をイネーブルにするオプション（チェックボックス）があり、各ホストのセキュリティレベルを表すロックパッドアイコンが管理対象ホストページに表示されます。

図6）SSL Secure証明書の設定

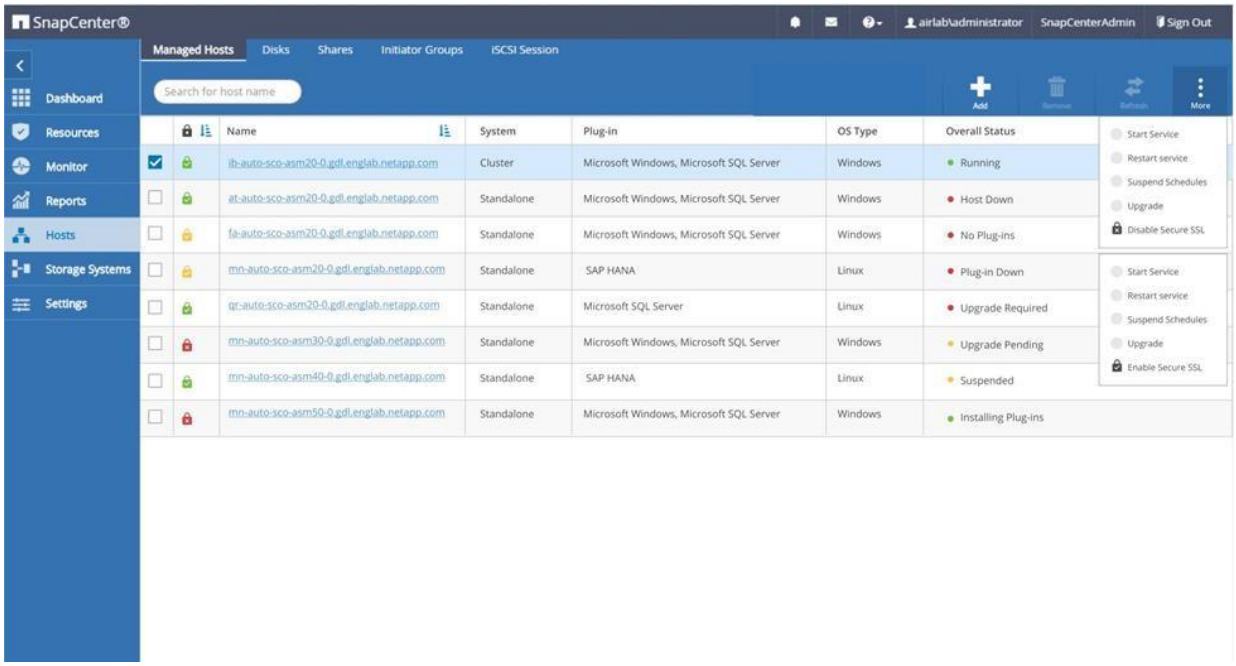


SnapCenterプラグインのCA証明書を有効にする

管理対象ホストページのメニューには、プラグインホストレベルのSSLセキュア検証を有効または無効にする追加オプションがあります。

プラグインホストでCA証明書を設定したあとに、このオプションを有効にする必要があります。

図7）プラグインホストのセキュリティステータス

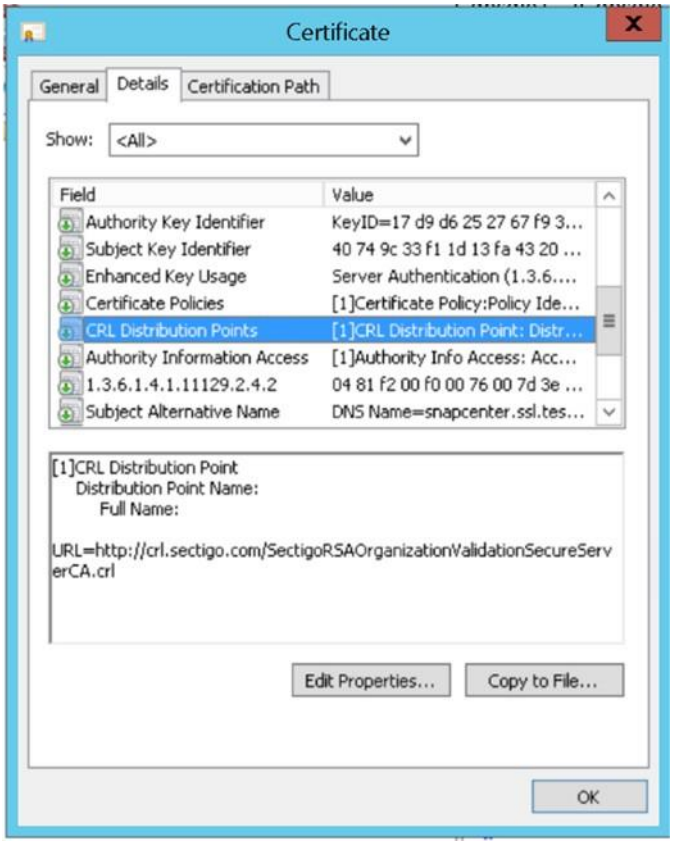


証明書失効リスト（CRL）

次の手順では、SnapCenter CA証明書のCRLファイルを更新する方法について説明します。

モード：UI

1. 最新のCRLファイルを取得します。
2. 管理者としてMMCを開きます。
3. **[ファイル]**、**[スナップインの追加と削除]**、または **Ctrl+M**をクリックします。
4. 利用可能なスナップインで、**[証明書]**を選択し、**[追加]**をクリックします。また、**[コンピュータアカウント]**を選択していることを確認してください。
5. **[次へ]**、**[完了]**の順に選択します。
6. Trusted Root Certification Authoritiesフォルダで、サーバー証明書をダブルクリックします。
7. [Certificate]ダイアログボックスで、**[Details]** タブを選択し、**[CRL Distribution Points]**を選択します。



8. URLをコピーし、最新のCRLファイルをダウンロードします。

SnapCenterサーバおよびWindowsホストのCA証明書の設定

モード：UI

1. MMCの左ペインの[証明書スナップイン]で、**[証明書(ローカルコンピュータ)]** ノードを展開します。
2. **[信頼されたルート証明機関]**ノードを展開し、**[証明書]**サブフォルダを右クリックして **[すべてのタスク]**を選択し、**[インポート]**を選択します。
3. 証明書のインポートウィザードの[ようこそ]ページで、**[次へ]**を選択します。
4. [インポートするファイル]ページで、**[参照]**を選択します。

5. [File Type]フィールドで、**[Certificate Revocation List]** （*）を選択します。crl）。
6. .crl ファイルの場所を参照し、ファイルを選択して**[開く]**を選択します。
7. [インポートするファイル]ページで、**[次へ]**を選択します。
8. [証明書ストア]ページで、デフォルトの選択を受け入れ、**[次へ]**を選択します。
9. [Certificate Import Wizard]ページを完了したら、**[Finish]**を選択します。
10. [**信頼されたルート認証局**]ノードを選択し、**スナップインを更新します**。

新しいを含む証明書失効リストフォルダ。crl ファイルが作成されました。

WindowsホストでのSnapCenterカスタムプラグイン用のCRLの設定

SnapCenterカスタムプラグインは、事前設定されたディレクトリでCRLファイルを検索します。SnapCenterカスタムプラグインのCRLファイルのデフォルトディレクトリはです C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\ etc\crl。

1. agent.properties ファイルのデフォルトディレクトリを変更し、キーに対して更新し CRL_PATHます。
2. このディレクトリに複数のCRLファイルを配置します。

受信証明書は、各CRLに対して検証されます。

SnapCenter Plug-in for VMware vSphere用のCRLの設定

SnapCenter Plug-in for VMware vSphereは、設定済みのディレクトリでCRLファイルを検索します。SnapCenter Plug-in for VMware vSphereのCRLファイルのデフォルトディレクトリは、です /opt/netapp/config/crl。このディレクトリには、複数のCRLファイルを格納できます。着信証明書は、各CRLに対して検証されます。

双方向SSL（相互認証）

上記の一方向SSLの手順に加えて、次の手順を実行して、SnapCenterサーバとプラグイン通信間の相互認証を有効にすることができます。この機能はSnapCenter 4.9以降で導入されました。

前提条件*：*

- 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、「CA証明書の設定」セクションを参照してください。
- 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。

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

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>

For example,

> 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サーバおよび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
```

例えば、

```
> $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、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、新しく取得したCA証明書にアクセスします。

    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]**の順にクリックします。

    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] > [個人] [証明書]**の順にクリックします。

    e. SnapCenter証明書を選択します。

    f. TADD USER\Permissionウィザードを起動するには、CA証明書を右クリックし、**All Tasks** > **Manage Private Keys**の順に選択します。

    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（階層の一番上）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**を取得するには、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、以下のパス

HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProvders\SCHANNELに移動します。

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

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。

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>
For example,
> 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>
```

たとえば、

```
> $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
```

双方向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、SnapCenterサーバとプラグインの間の相互通信を保護できます。

開始する前に

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"}
```

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。
>再起動- WebAppPool -名前「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。

タスク概要

- 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"}
```

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
```

サービスの設定

SnapCenterサーバでは、SnapCenterログインおよびプラグイン管理用に、ローカルワークグループおよびドメインのユーザアカウントがサポートされます。このセクションでは、アカウントのパスワードを更新し、サービスの所有権をサービスアカウントに変更して、サービスをユーザアカウントから分離する方法について説明します。

SnapCenterサービスアカウントのパスワード

Active Directoryでサービスアカウントのパスワードが変更された場合、手動でトリガーされるまでサービスがパスワードの変更を更新しないため、バックアップが失敗する可能性があります。

SnapCenter Plug-in for Windowsを実行しているホストで、次の手順を実行します。

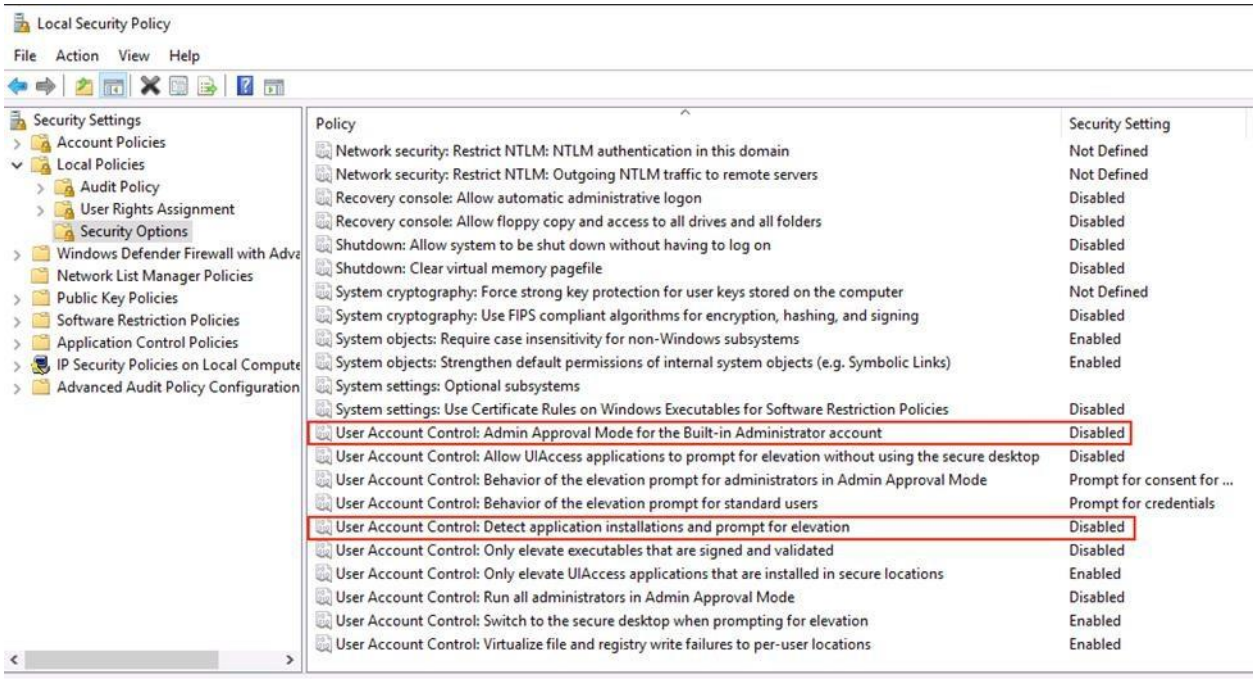
1. プラグインを一時停止します（バックアップが実行されていない場合）。
2. Active DirectoryでSnapCenterサービスアカウントのパスワードを変更します。
3. SnapCenter UIおよびSnapCenter Plug-in for VMwareの設定（およびそのドメインアカウントが使用されている任意の場所）でクレデンシャルのパスワードを更新します。
4. SnapCenter UIでプラグインの一時停止を解除します。
5. 影響を受けるホストでPlug-in for WindowsサービスおよびSnapCenter SMCoreサービスを再起動します。
6. テストバックアップを実行します。

SnapCenterプラグインホストの権限設定

Windows 2016および2019には、追加のユーザアクセス制御（UAC）とリモートPowerShell Windows Management Instrumentation（WMI）のセキュリティ設定があり、インストーラが自己定義のローカルユーザで実行されないようにします。

インストーラを実行するには、ホストのローカル管理者アカウントを使用するか、ローカルセキュリティポリシーでUACを完全に無効にします。

1. プラグインホストのリモートセッションを開くには、**[Start]**をクリックして **[Local Security Policy]** `(secpol.msc)` を開きます。
2. **[Security Settings]** > **[Local Policies]** > **[Security Options]**に移動します。
3. 次の両方のパラメータを **[Disabled]**に設定します。
   a. ユーザーアカウント制御:アプリケーションのインストールを検出し、昇格のプロンプトを表示します。
   b. ユーザーアカウント制御:管理者承認モードですべての管理者を実行します。



4. PowerShellセッションを開き、次のコマンドを実行します。

```
Get-Service winrm
Enable-PSRemoting -force
winrm s winrm/config/client '@{TrustedHosts="SNAPCENTER_HOSTNAME/IP"}'
```

   - `SNAPCENTER_HOSTNAME` = SnapCenterサーバのホスト名
   - `IP` = SnapCenterサーバのIPアドレス

```
winrm quickconfig
```

5. 必要に応じて、`winrm` 最後のコマンドのステータスに基づいてを設定します。

```
PS C:\Users\Administrator.DEMO> Get-Service winrm

Status   Name               DisplayName
------   ----               -----------
Running  winrm              Windows Remote Management (WS-Manag...


PS C:\Users\Administrator.DEMO> Enable-PSRemoting -force
PS C:\Users\Administrator.DEMO> winrm s winrm/config/client '@{TrustedHosts="MAIL/192.168.0.89"}'
Client
    NetworkDelayms = 5000
    URLPrefix = wsman
    AllowUnencrypted = false
    Auth
        Basic = true
        Digest = true
        Kerberos = true
        Negotiate = true
        Certificate = true
        CredSSP = false
    DefaultPorts
        HTTP = 5985
        HTTPS = 5986
    TrustedHosts = MAIL/192.168.0.89

PS C:\Users\Administrator.DEMO> winrm quickconfig
WinRM service is already running on this machine.
WinRM is already set up for remote management on this computer.
PS C:\Users\Administrator.DEMO>
```

6. サーバをリブートします（UACの変更を適用する場合）。

7. 必要に応じて、他のプラグインホストでも同じ手順を繰り返します。

グループ管理サービスアカウント（gMSA）

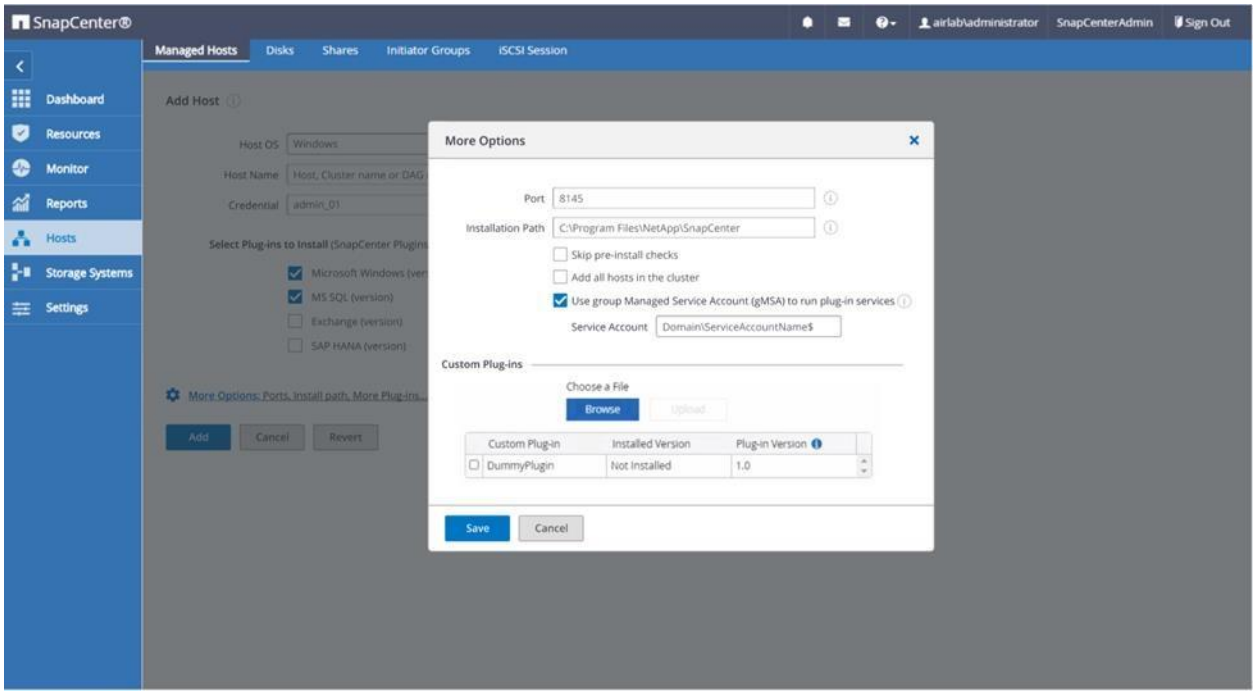
SnapCenterソフトウェアでは、実際のユーザに関連付けられていないgMSAを使用したSnapCenterプラグインサービスの実行がサポートされ、パスワードの自動管理が可能です。gMSAアカウントは、SnapCenter Plug-in for WindowsおよびSnapCenter Plug-in for SQL Serverサービスでのみサポートされます。

gMSAは次のオプションを使用して設定できます。

ホストまたはクラスタを追加

ホストの登録時に、プラグインサービスを実行するgMSAアカウントを指定することもできます。gMSAを有効にするには、**SnapCenter > Hosts > Add Host > More Options**に移動します。

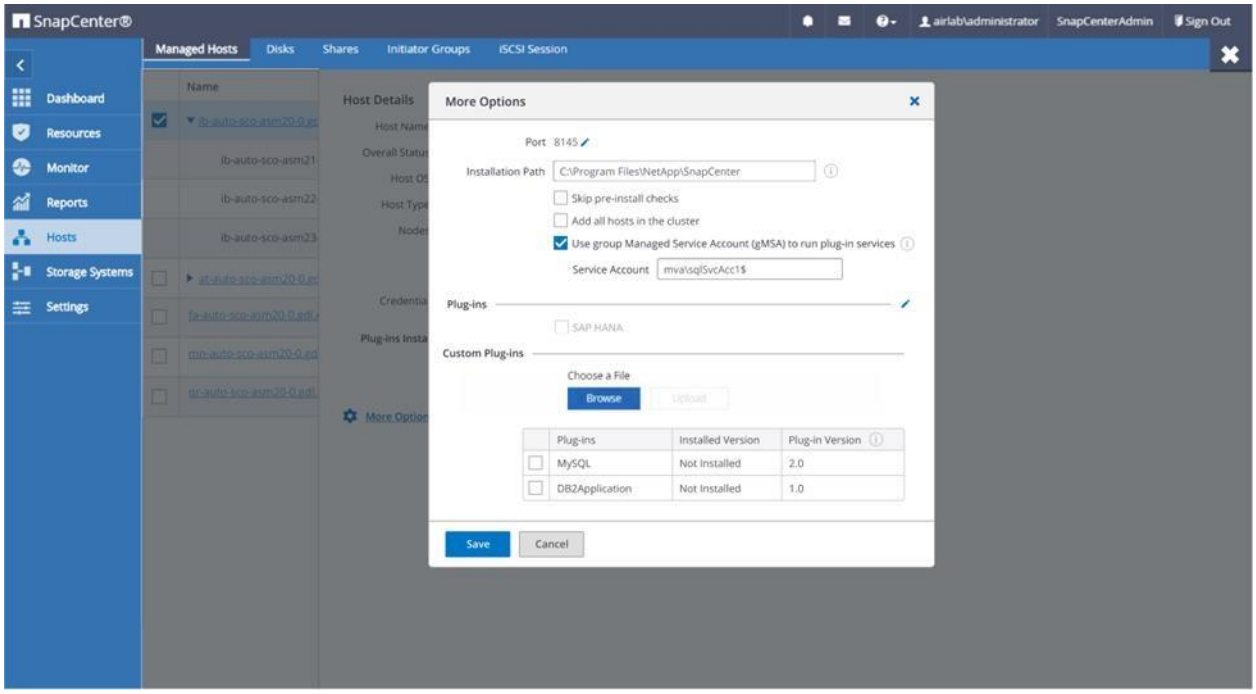
図8）gMSAのダイアログボックス



ホストまたはクラスタを変更する

gMSAを指定せずにプラグインがすでにインストールされている場合は、ホスト変更UIでgMSAアカウントを指定してプラグインサービスアカウントとして使用できます。

これを行うには 、**SnapCenter**に移動し、ホスト名をクリックし、**[More options]**をクリックします。



PowerShellコマンドレットの使用

コマンドレットを使用してgMSAを設定するには、次の手順を実行します。

1. 走れ `Install-SmHostPackage`。

   例：

```
Install-SmHostPackage -HostNames <hostname> -PluginCodes SCW,SCSQL -GMSAName <gMSA_Name>
```

2. 走れ `Set-SmHost`。

   例：

```
Set-SmHost -HostName <hostname> -UseGMSA:$true -GMSAName <gMSA_Name>
```

ポリシー設定

プリスクリプトとポストスクリプト

SnapCenterでは、処理ワークフローの実行時にプリスクリプトまたはポストスクリプトを実行するオプションが用意されています。Windowsプラグインの場合、ワークフロー中にプリスクリプトまたはポストスクリプトを実行するには、の定義済みディレクトリにスクリプトファイルを保存する必要があります。

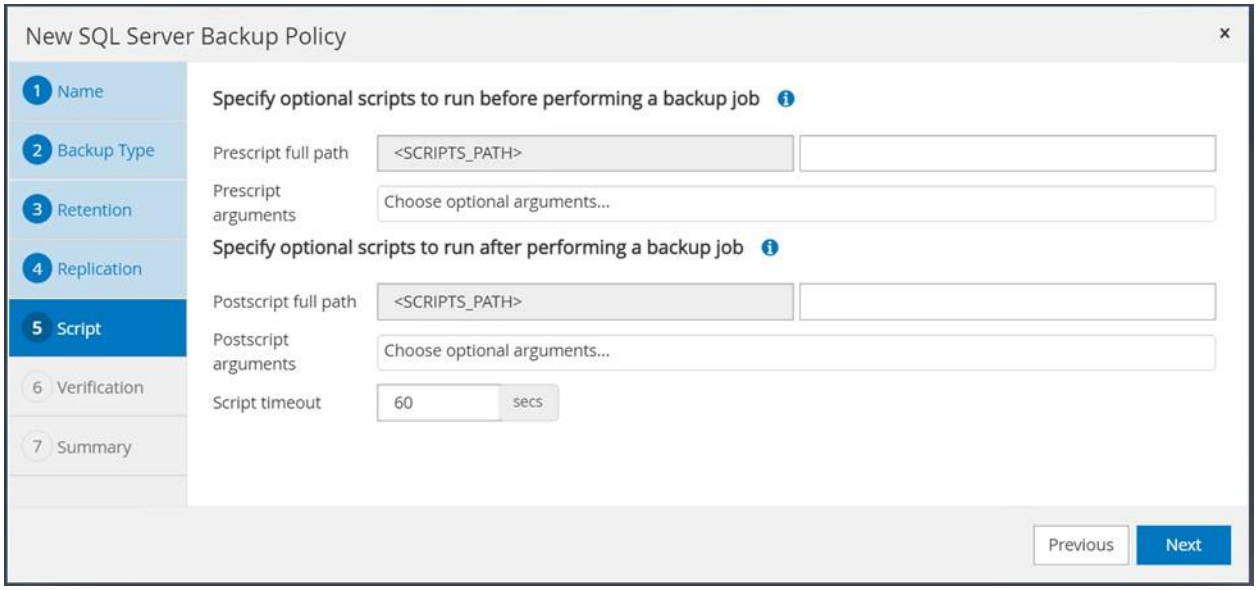
```
C:\Program Files\NetApp\SnapCenter\SMCore\Scripts\
```

カスタムスクリプトディレクトリ

カスタムディレクトリを使用する場合は `C:\Program Files\NetApp\SnapCenter\SMCore\SMCoreServiceHost.exe.Config`、ファイルからを設定する必要があります。キーの値を変更し `PredefinedWindowsScriptsDirectory`ます。デフォルトのキー値はです `PredefinedWindowsScriptsDirectory - C:\Program Files\NetApp\SnapCenter\SMCore\Scripts\`。

UI

テキストボックスに指定したパスが、スクリプトディレクトリのパスに追加されます。たとえば、というパスを入力する `MyScripts\TestScripts.cmd`と、SnapCenterはでスクリプトを検索します `C:\Program Files\NetApp\SnapCenter\SMCore\Scripts\MyScripts\TestScripts.cmd`。



LinuxおよびAIXサーバで実行されるSnapCenterプラグインの強化

このセクションでは、LinuxサーバまたはAIXサーバでOracle用SnapCenterプラグインを使用する場合と、LinuxホストでSAP HANA用SnapCenterプラグインを使用する場合に必要なセキュリティ強化手順について説明します。

Secure Shell（SSH）設定Secure Shell（SSH）セッテイ

SSHセッションの確立中、サーバとクライアント間の通信はFederal Information Processing Standard（FIPS；連邦情報処理標準）140-2に準拠しています。エンドポイント間のすべての通信はTLS 1.2とTLS 1.3を介して行われる

許可される暗号は次のとおりです。暗号ブロックチェーン（CBC）ベースの暗号は、TLS 1.2およびTLS 1.3と組み合わせても脆弱ではありません。

- AES128-CTR
- AES192-CTR
- AES256-CTR
- AES128-CBC
- AES192-CBC
- AES256-CBC
- 3DES-CBC

メッセージ認証コードでサポートされるアルゴリズムは次のとおりです。

- Linuxの場合は、MAC HMAC-sha2-256およびMAC HMAC-sha2-512をに追加します `/etc/ssh/sshd_config`。
- AIXの場合は、MAC HMAC-sha1をに追加します `/etc/ssh/sshd_config`。

使用される鍵交換アルゴリズム：

```
Diffie-hellman-group-exchange-sha256
```

オペレーティングシステムのセキュリティ保護とファイアウォールの設定

Port security

使用されていないネットワークポートは閉じる必要があります。特に、Telnet接続用のポート23などの脆弱なポートは、すべてのシステムで閉じる必要があります。Linuxシステムに必要な次のポートが開いている必要があります。

- デフォルトでは、SPL_PORTとSNAPCENTER_SERVER_PORTは それぞれ8145と8146に設定する必要があります。ただし、これらのポート値は、ファイルで定義されている設定可能なパラメータを使用して設定できます `/var/opt/snapcenter/spl/etc/spl.properties`。
- ポート **22**（SSH）を有効にしてプラグインをインストールします。ただし、Linuxホストに手動でインストールすることで、ファイアウォールリストからポート22をスキップできます。
- ポート **27216**を有効にします。このデフォルトのJDBCポートは、Oracleデータベースへの接続にOracle用プラグインで使用されます。

リスニングポートのリストを確認するには、次のコマンドを使用します。

```
netstat -tulpn
```

この情報を使用して、必要なリスニングポートと無効にするポートを判断できます。

開いたままにしておく残りのポートを保護するには、ポートアクセスを特定のホストIPアドレスに制限します。

SELinux

セキュリティ強化Linuxは、アクセス制御セキュリティポリシーをサポートするカーネルセキュリティメカ

ニズムです。次のコマンドを実行して、現在のSELinuxモードを確認します。

```
sestatus
```

SnapCenter Plug-ins Package for Linuxが処理を実行できるように、SELinuxをPermissiveに設定する必要があります。そうしないと、インストールに失敗する可能性があります。

Rootログインのセキュリティ

ルートログインの無効化または制限には、複数の利点があります。ユーザにsudoコマンドを強制的に使用して管理レベルのコマンドを実行させると、複数のユーザがrootとしてログインして同じタスクを実行している場合、存在しないレベルの監査が作成されます。

最も安全なプロセスは、SnapCenter Plug-ins Package for Linuxをroot以外のユーザとしてインストールして、すべてのルートアクセスを無効にすることです。

ファイアウォール

Iptablesは、Linuxカーネルが提供するファイアウォールを設定するためのユーザ空間アプリケーションプログラムです。ファイアウォールルールは、「ポートセキュリティ」セクションに記載されているポートをブロックしないようにし、ホストIPとポートをリスンするために開いておく必要があります。

次の例は、SUSE Linux Enterprise Serverを設定する方法を示しています。

1. SnapCenter Plug-in Loader（SPL）ポートをiptablesに追加します。
   - `/usr/sbin/iptables -A INPUT -p tcp -m tcp --dport 8145 -j ACCEPT`

- `/usr/sbin/iptables -A OUTPUT -p tcp -m tcp --dport 8145 -j ACCEPT`

2. `/etc/sysconfig/SuSEfirewall2` ファイルで次のパラメータを変更して、SPLポートをファイアウォールスクリプトに追加します。
   - `FW_SERVICES_EXT_TCP="22 8145" <==== Add SSH and SPL ports`
   - `FW_SERVICES_EXT_UDP="22 8145"`
3. SLESのバージョンに応じて、次のコマンドを実行します。

   SLES 11の場合は、次のコマンドを実行します。

   a. `service SuSEfirewall2_setup stop`

   b. `service SuSEfirewall2_setup start`

   SLES 12の場合は、次のコマンドを実行します。

   a. `systemctl stop SuSEfirewall2`

   b. `systemctl start SuSEfirewall2`

一定期間（3時間など）後にネットワーク接続を終了する会社全体のポリシーがある場合は、SnapCenterアプリケーションでネットワーク接続をオフにする必要があります。そうしないと、処理が失敗し始めます。

レート制限は、DOSおよびDDoS攻撃に対するメカニズムを提供します。悪意のある攻撃を防ぐために、OSネットワークファイアウォールを介して新しい接続のIPアドレスを送信元ごとにレート制限できます。Red Hat Enterprise Linux（RHEL）では `iptables` 、コマンドを使用してレートリミッタを設定できます。次のコマンドを使用して、`n` 1秒あたりの要求で新しい接続をレート制限します。

```
iptables -A INPUT -m conntrack --ctstate NEW -m hashlimit --hashlimit-above 10/sec --hashlimit-burst 5 --hashlimit-mode srcip --hashlimit-name conn-rate-limit -j DROP
```

認証とログイン

証明書ベースの認証

証明書ベースの認証は、デジタル証明書を使用した認証を改善するセキュリティ機能です。証明書ベースの認証は、従来のユーザー名/パスワード認証よりも強力なセキュリティを提供します。暗号鍵とデジタル証明書に依存しているため、権限のないユーザーが有効なユーザーになりすましにくくなります。証明書ベースの認証は、SnapCenterプラグインホストにアクセスしようとする各ユーザの信頼性を検証します。秘密鍵なしでSnapCenterサーバ証明書をエクスポートし、プラグインホストの信頼されたストアにインポートする必要があります。この機能は、双方向SSLが設定されたシステム上で動作します。

SnapCenterサーバからのCA証明書のエクスポート

Microsoft管理コンソール（MMC）を使用して、SnapCenterサーバからプラグインホストにCA証明書をエクスポートする必要があります。

前提条件：双方向SSLが設定されている必要があります。

手順

7. 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]**の順にクリックします。
8. [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。
9. [証明書スナップイン]ウィンドウで、**[コンピュータアカウント]**オプションを選択し、**[完了]**をクリックします。
10. **[コンソールルート] > [証明書-ローカルコンピュータ] > [個人] > [証明書]** の順にクリックします。

11. SnapCenterサーバで使用される調達CA証明書を右クリックし、**[All Tasks] > [Export]**を選択してエクスポートウィザードを開始します。
12. 次の手順でウィザードを完了します。

このウィザードウィンドウでは...	操作
秘密キーのエクスポート	**[いいえ**、秘密鍵をエクスポートしない]オプションを選択し、**[次へ]**をクリックします。
エクスポートファイル形式	変更しないで、**[次へ]**をクリックします。
ファイル名	**[参照]**をクリックし、証明書を保存するファイルパスを指定して、**[次へ]**をクリックします。
証明書のエクスポートウィザードの完了	概要を確認し、**[Finish]**をクリックしてエクスポートを開始します。

注：SnapCenter HA構成はサポートされません。

UNIXホストプラグインへのCA証明書のインポート

- SPLキーストアのパスワード、および使用中のCA署名キーペアのエイリアスを管理できます。
- 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は同じである必要があります。

手順

1. SPLキーストアのデフォルト パスワードは、SPLプロパティ ファイルから取得できます。キーに対応する値です `'SPL_KEYSTORE_PASS'`。
2. キーストアのパスワードを変更します。
```
$ keytool -storepasswd -keystore keystore.jks
```
3. 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、 キーストアと同じパスワードに変更します。
```
$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```
4. `SPL_KEYSTORE_PASS` spl.propertiesファイル内のキーについても同じ内容を更新します。
5. パスワードを変更したら、サービスを再起動します。

ルート証明書または中間証明書をSPL trust-storeに設定します。

ルート証明書または中間証明書をspl trust-storeに設定する必要があります。ルートCA証明書のあとに中間CA証明書を追加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. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。
```
$ keytool -list -v -keystore keystore.jks
```
4. ルート証明書か中間証明書を追加します。
```
$ keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported> -file
/<CertificatePath> -keystore keystore.jks
```
5. SPLトラストストアへの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。

SPLトラストストアに対するCA署名付きキー ペアの設定

注：ルートCA証明書のあとに中間CA証明書を追加する必要があります。

手順

1. SPLのキーストア/var/opt/snapcenter/spl/etcが格納されているフォルダに移動します。
2. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

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

4. 秘密キーと公開キーの両方が設定されたCA証明書を追加します。

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

5. キーストアに追加された証明書の一覧を表示します。

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

6. 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 キーストアに含まれていることを確認します。
7. CA証明書に追加した秘密キーのパスワードを、キーストアのパスワードに変更します。
   SPLキーストアのデフォルトのパスワードは、spl.propertiesファイルのキーSPL_KEYSTORE_PASSの値です。

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

8. 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 "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
```

9. 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。
   SPL_CERTIFICATE_ALIASキーに対するこの値を更新します。
10. SPLトラストストアにCA署名キー ペアを設定したら、サービスを再起動します。

証明書-一方向および相互SSL

Linuxホスト上のSnapCenter Plug-in for SAP HANA DatabaseおよびSnapCenter Plug-in Loaderサービス用のCA証明書の設定

カスタムプラグインでは、ファイルを使用し keystore.jksます。このファイルは /opt/NetApp/snapcenter/scc/etc、信頼ストアとキーストアの両方にあります。

カスタムプラグインキーストアのパスワードと、使用中のCA署名キーペアのエイリアスを管理します。

カスタムプラグインキーストアのデフォルトパスワードは、カスタムプラグインエージェントプロパティファイルから取得できます。キーKEYSTORE_PASSに対応する値です。

1. キーストアのパスワードを変更します。

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

2. 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、キーストアと同じパスワードに変更します。

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

3. agent.properties ファイルのキーkeystore_passについても同じ内容を更新します。
4. パスワードを変更したら、サービスを再起動します。

注： カスタムプラグイン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は同じである必要があります。

カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定

ルート証明書または中間証明書は、カスタムプラグインの信頼ストアに秘密鍵なしで設定する必要があります。

1. カスタム プラグイン キーストアが格納されているフォルダ、「/opt/NetApp/snapcenter/scc/etc」
2. ファイルを探します keystore.jks。
3. キーストアに追加された証明書を一覧表示します。

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

4. ルート証明書または中間証明書を追加します。

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore
keystore.jks
```

5. カスタムプラグイン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。

   注： ルートCA証明書のあとに中間CA証明書を追加する必要があります。

カスタムプラグインの信頼ストアへのCA署名キーペアの設定

CA署名キーペアをカスタムプラグインの信頼ストアに設定する必要があります。

1. カスタムプラグインキーストアが格納されているフォルダに移動します。「/opt/NetApp/snapcenter/scc/etc」
2. ファイルを探します keystore.jks。
3. キーストアに追加された証明書を一覧表示します。

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

4. 秘密鍵と公開鍵の両方が設定されたCA証明書を追加します。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype
pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. キーストアに追加された証明書を一覧表示します。

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

6. 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、キーストアに含まれていることを確認します。
7. CA証明書に追加し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。
8. デフォルトのカスタムプラグインキーストアパスワードは agent.properties、ファイル内のキーkeystore_passの値です。

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore keystore.jks
```

9. 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 "long_alias_name" -destalias "simple_alias" -keystore keystore.jks
```

10. agent.properties ファイルのCA証明書からエイリアス名を設定します。

11. この値を、キーSCC_CERTIFICATE_ALIASに対して更新します。
12. カスタムプラグインの信頼ストアにCA署名キーペアを設定したら、サービスを再起動します。

SnapCenterカスタムプラグインのCRLを設定

- SnapCenterカスタムプラグインは、事前設定されたディレクトリでCRLファイルを検索します。
- SnapCenterカスタムプラグインのCRLファイルのデフォルトディレクトリはです `opt/NetApp/snapcenter/scc/etc/crl`。
- `agent.properties` CRL_PATHキーに対して、ファイル内のデフォルトディレクトリを変更および更新できます。
- このディレクトリには、複数のCRLファイルを格納できます。着信証明書は、各CRLに対して検証されます。

LinuxホストでのSnapCenter Plug-in Loaderサービスを使用したCA証明書の実装

SnapCenter Plug-in Loader（SPL）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。SPL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。SPLでは、ファイルが `keystore.jks/var/opt/snapcenter/spl/etc` 信頼ストアとキーストアの両方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署名キー ペアのエイリアスの管理

SPLキーストアのデフォルトパスワードは、SPLプロパティファイルから取得できます。これは、SPL_KEYSTORE_PASSキーに対応する値です。

1. キーストアのパスワードを変更します。

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

2. キーストア内の秘密キー エントリのすべてのエイリアスのパスワードを、キーストアと同じパスワードに変更します。

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

3. `spl.properties` ファイルのSPL_KEYSTORE_PASSキーについても同じ内容を更新します。
4. パスワードを変更したら、サービスを再起動します。

注：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は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のSPLトラストストアへの設定

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。

1. SPLキーストアが格納されているフォルダに移動し `/var/opt/snapcenter/spl/etc`ます。
2. ファイルを探します `keystore.jks`。
3. キーストアに追加された証明書を一覧表示します。

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

4. ルート証明書または中間証明書を追加します。

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

5. SPLトラストストアへの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。
6. ルートCA証明書を追加してから、中間CA証明書を追加する必要があります。

SPL信頼ストアへのCA署名キーペアの設定

SPL信頼ストアにCA署名キーペアを設定するには、次の手順を実行します。

1. SPLキーストアが格納されているフォルダに移動し `/var/opt/snapcenter/spl/etc`ます。
2. ファイルを探します `keystore.jks`。
3. キーストアに追加された証明書を一覧表示します。

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

4. 秘密鍵と公開鍵の両方を持つCA証明書を追加します。

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

5. キーストアに追加された証明書を一覧表示します。

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

6. 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、キーストアに含まれていることを確認します。
7. CA証明書に追加し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`、ファイルのSPL_KEYSTORE_PASSキーの値です。

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

8. 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 "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore
keystore.jks
```

9. `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。

   SPL_CERTIFICATE_ALIASキーに対するこの値を更新します。
10. SPLトラストストアにCA署名キー ペアを設定したら、サービスを再起動します。

SPLの証明書失効リストを設定する

SPLのCRLを設定する必要があります。

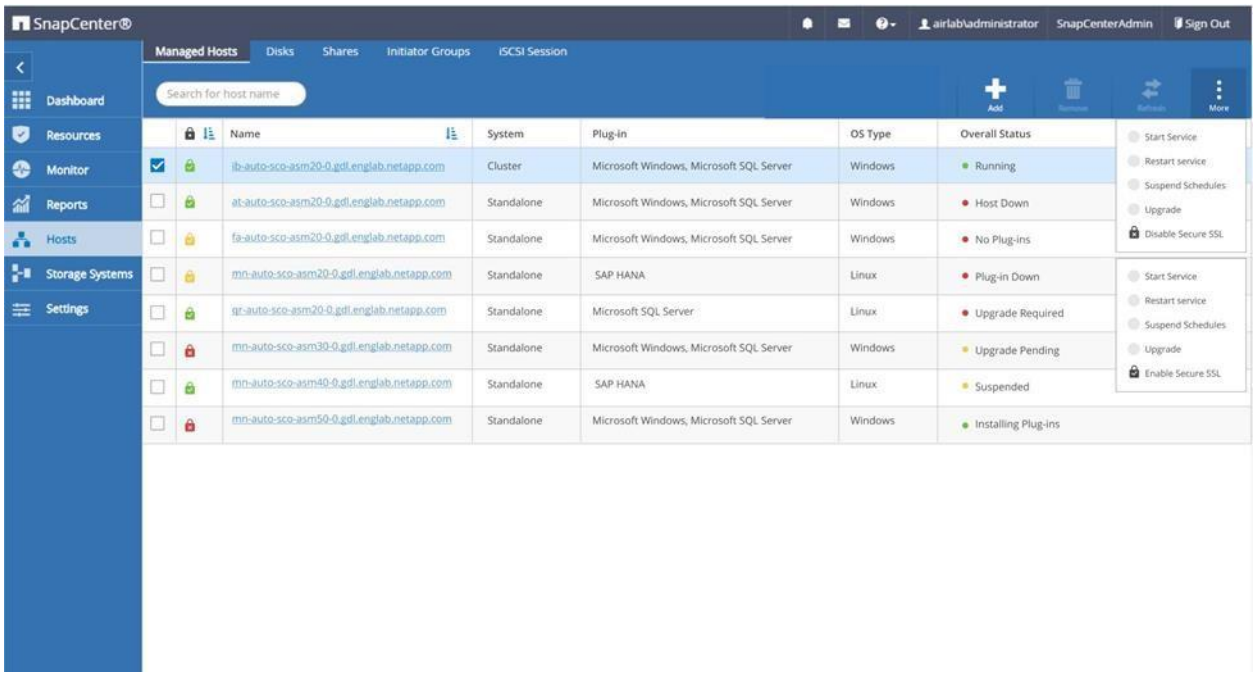
- SPLは、事前設定されたディレクトリでCRLファイルを検索します。
- SPLのCRLファイルのデフォルトディレクトリはです `/var/opt/snapcenter/spl/etc/crl`。

1. `spl.properties` ファイルのデフォルトディレクトリを変更し、キーに対して更新し `SPL_CRL_PATH`ます。
2. このディレクトリに複数のCRLファイルを配置します。

受信証明書は、各CRLに対して検証されます。

SnapCenterプラグインのCA証明書を有効にする

CA証明書機能は、グローバル設定ページでSnapCenterレベルでイネーブルにする必要があります。その後、SnapCenterの管理対象ホストページのメニューに、プラグインホストレベルのSSLセキュア検証を有効または無効にする追加オプションが表示されます。プラグインホストでCA証明書を設定したあとに、このオプションを有効にする必要があります。緑色の南京錠は、CA証明書が正常に検証されたことを示します。



相互SSL

追加の手順は必要ありません。一方向通信のSSL設定手順は有効なままです。[LinuxホストでSnapCenter Plug-in Loader（SPL）サービスを使用してCA証明書を設定します]。

暗号の設定SPL

サポートされる暗号

SPLでは、サーバとLinuxクライアントの間の通信でAES128暗号とAES256暗号のみがサポートされます。

```
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-SHA256
AES256-GCM-SHA384
AES256-SHA256
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-SHA256
AES128-GCM-SHA256
AES128-SHA256
```

Remote Support Agentキー

Linuxプラグインホスト（SPL / SCC）でのSSL/TLS証明書の検証時にSSL/TLS証明書で許可されるRemote Support Agent（RSA）の最小公開鍵長（ビット） `RSA_KEY_MINLENGTH`を設定するには、パラメータの値を指定する必要があります。

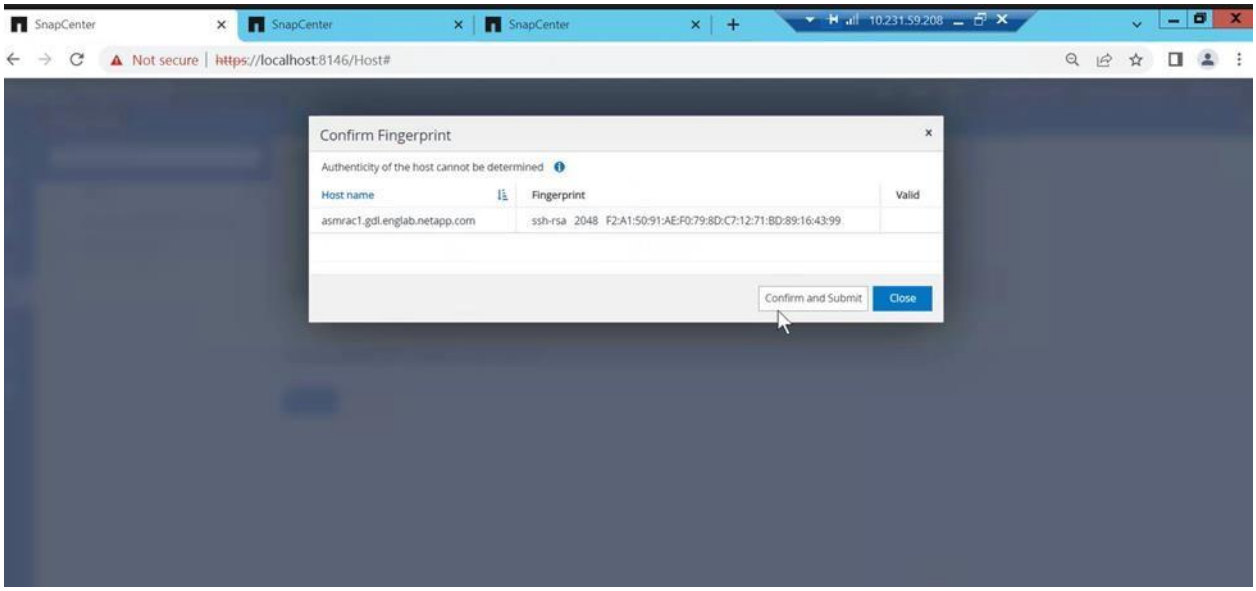
```
RSA_KEY_MINLENGTH=3072
```

SPLの場合は `spl.properties` `/var/opt/snapcenter/spl/etc/spl.properties`、`agent.properties` `<user_install_path>/NetApp/snapcenter/scc/etc/agent.properties`（SCCの場合は）（Linuxの場合は）にあるファイルで、このパラメータを指定できます。

プラグインのインストールの保護

プッシュインストールでのフィンガープリント検証

インストール処理の一環として、パッケージをホストにプッシュする前に、 次のスクリーンショットに示すように、ホストに対して視覚的に確認することで、フィンガープリントを検証し、[Confirm fingerprint]をクリックする必要があります。クラスタセットアップでは、クラスタ内の各ノードのフィンガープリントを確認する必要があります。フィンガープリントの最小長は2048です。そうしないと、インストールは続行されません。



Javaパスの可用性

プラグインのインストール中に、製品をインストールしようとするユーザーに設定されたJavaパスが自動的に解決されます。

sudo設定（ルート以外の場合）

root以外のユーザにSnapCenter for Linuxプラグインをインストールするには `oracle_checksum.txt` 、にあるファイルの内容を追加する必要があり `C:\ProgramData\NetApp\SnapCenter\Package Repository` ます。このファイルには、これらの処理の実行に必要なチェックサムとパス関連の情報が格納されています。

1.8.7以上のsudoバージョンのsudoersファイルのサンプルコンテンツ

```
# ===== sudo user rules to be added on the Linux plug-in host if sudo package version is 1.8.7 or
later =====
# ===== Replace USER_HOME_DIRECTORY with the path of the home directory of the user who will
deploy the plug-in. =====
# ===== Replace LINUXUSER with the OS username identified for deploying the plug-in. =====
# ===== Replace /opt with the custom location where the plug-in will be installed. =====
Cmnd_Alias HPPLCMD = sha224:+GfDlO9XjgxmOqWhB2WRjwdqbu7ZskMYaFigdg==
/<USER_HOME_DIRECTORY>/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall, /opt/NetApp/snapcenter/spl/bin/spl,
/opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:ir9Km4ctOavgJ60Fbbmmpx7a6dJ68FiQIXHdyw==
/<USER_HOME_DIRECTORY>/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:HQukzZNynG+nugzScFnHuccouOL75sZ1RRDaNg==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config_Check.sh
```

```
Cmnd_Alias SCCMD = sha224:GHupVXP5krvae06pNNxjvhZcM5VfRkOvc86Ibw==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR = sha224:Z/y0i1kAYtuWf/uOExqlnBOPVufF8samQPEE7g==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
<LINUXUSER> ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD, CONFIGCHECKCMD, SCCCMDEXECUTOR,
SCCMD
Defaults:<LINUXUSER> !visiblepw
Defaults:<LINUXUSER> !requiretty
```

1.8.7より前のsudoバージョンのsudoersファイルのサンプルコンテンツ

```
# ===== sudo user rules to be added on the Linux plug-in host if sudo package version is below
1.8.7 =====
# ===== Replace USER_HOME_DIRECTORY with the path of the home directory of the user who will
deploy the plug-in. =====
# ===== Replace LINUXUSER with the OS username identified for deploying the plug-in. =====
# ===== Replace /opt with the custom location where the plug-in will be installed. =====
<LINUXUSER> ALL=(ALL) NOPASSWD:SETENV:
/<USER_HOME_DIRECTORY>/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall, /opt/NetApp/snapcenter/spl/bin/spl,
/opt/NetApp/snapcenter/scc/bin/scc, /<USER_HOME_DIRECTORY>/.sc_netapp/Linux_Prechecks.sh,
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config_Check.sh,
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
Defaults:<LINUXUSER> !visiblepw
Defaults:<LINUXUSER> !requiretty
```

手動インストール-署名検証手順

SnapCenter Plug-in for Oracleを手動でインストールした場合は `snapcenter_public_key.pub`、（にある `C:\ProgramData\NetApp\SnapCenter\Package Repository`）キーを使用してバイナリパッケージの署名を検証する必要があります。そのためには、次のコマンドを実行します。

```
openssl dgst -sha256 -verify snapcenter_public_key.pub -signature
snapcenter_linux_host_plugin.bin.sig snapcenter_linux_host_plugin.bin
```

前提条件

- OpenSSL：OpenSSL 1.0.2G

インストールされているコンポーネントのチェックサム検証

インストールの一環として、インストールされているすべてのコンポーネントのチェックサム検証は、まず製品のマニフェストファイルに対して検証されます。チェックサムの不一致が検出されると、インストールは中止され、パッケージはアンインストールされます。次に、NetApp所有のすべてのJARのデジタル署名も検証され、不一致が検出されるとSPLサービスは開始されず、インストールは中止されます。

ストレージ設定

ストレージエクスポートポリシーにホストの優先IPアドレスを設定する

scclicmdletを使用して、マウント処理とクローン処理用にストレージエクスポートポリシーに追加するホストのIPアドレスを選択または制御します `Set-PreferredHostIPsInStorageExportPolicy`。デフォルトでは、SnapCenterによってホストのすべてのIPアドレスがストレージエクスポートポリシーに追加されます。

次に、IPアドレスを設定する例を示します。

```
# sccli Set-PreferredHostIPsInStorageExportPolicy -IpAddresses '192.168.1.1, 192.168.1.2, 192.168.1.3, 192.168.1.4'
Are you sure you want to overwrite the existing preferred IP addresses of the host for storage export policy?
Enter either [Y] Yes or [N] No (default is 'N'): Y
INFO: Preferred IP addresses of the host for storage export policy are updated successfully.
INFO: The command 'Set-PreferredHostIPsInStorageExportPolicy' executed successfully.
```

SnapCenter Plug-in for Oracleのセキュリティ保護

すべてのOracleスクリプト（プリスクリプトまたはポストスクリプト）をディレクトリに配置する必要があります `/var/opt/snapcenter/spl/scripts/`。このディレクトリには、rootユーザのみがアクセスできます。

Oracle認証

データベース認証

Oracleデータベース認証方式は、Oracleデータベースに照らして認証します。データベースホストでオペレーティングシステム認証が無効になっている場合は、Oracleデータベースで処理を実行するためにOracleデータベース認証が必要になります。そのため、Oracleデータベースのクレデンシャルを追加する前に、Oracleデータベースでsysdba権限を持つOracleユーザを作成しておく必要があります。

ASM認証

Oracle ASM認証方式は、Oracle Automatic Storage Management（ASM）インスタンスに照らして認証します。Oracle ASMインスタンスにアクセスする必要があり、データベースホストでオペレーティングシステムのOS認証が無効になっている場合は、Oracle ASM認証が必要です。そのため、Oracle ASMのクレデンシャルを追加する前に、ASMインスタンスでSYSASM権限を持つOracleユーザを作成しておく必要があります。

RMANカタログ認証

RMANカタログ認証方式は、Oracle Recovery Manager（RMAN）カタログデータベースに照らして認証します。外部カタログメカニズムを設定し、データベースをカタログデータベースに登録した場合は、RMANカタログ認証を追加する必要があります。

SnapCenterカスタムプラグインの保護

sudo構成（root以外のユーザ用）

SnapCenter 4.8以降のリリースでは、SnapCenterカスタムプラグインをroot以外のユーザとして実行できます。

SnapCenterカスタムプラグインをroot以外のユーザとして実行するには、SnapCenterカスタムプラグインをインストールする前に次の手順を実行する必要があります。

1. Linuxホストでroot以外のユーザを作成します。
2. sudoersファイルを適切なコンテンツで更新して、root以外のユーザに適切なsudo権限を付与します `oracle_checksum` （インストールされているSnapCenterサーバのファイルを参照してください `C:\ProgramData\NetApp\SnapCenter\Package Repository\oracle_checksum`）。
3. このホストのSnapCenter UIからSnapCenterカスタムプラグイン（SCC）をインストールするか、root以外のユーザを設定してこのホストから手動でインストールします。

プリスクリプトまたはポストスクリプト

SnapCenterカスタムプラグインのクローニングまたはリストアのワークフローでのプリスクリプトまたはポストスクリプトの手順のセキュリティを強化するために、`allowed_commands.config` LinuxホストまたはWindowsホストへのプラグインのインストール時にファイルが配布されます。`allowed_commands.config` ファイルに書き込むことができるのは、Windowsの管理者またはLinuxのルートだけです。

ワークフローの実行前または実行後にホストでコマンドを実行する必要がある場合は、`allowed_commands.config` ファイルにコマンドを含めることで明示的に許可する必要があります。このファイルに書き込むことができるのは、Windowsの管理者またはLinuxのルートだけです。

`allowed_commands.config` ホスト上ののパスは次のとおりです。

Linuxホスト

- デフォルト：/opt/NetApp/snapcenter/scc/etc/allowed_commands.config
- カスタムパス：
  <Custome_Directory>/NetApp/snapcenter/scc/etc/allowed_commands.config

Windowsホスト

- デフォルト：C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config
- カスタムパス：<Custome_Directory>\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config

にコマンドを追加するには allowed_commands.config、allowed_commands.config エディターでを開きます。各コマンドは、コマンドプロンプトでコマンドを入力する場合とまったく同じように、専用の行で入力します。
ケースは重要です。

例：

```
command: mount
command: umount
command: "C:\Software\New command\commandLists\scripts\abc.bat"
command: "c:\a b\c.bat"
command: echo
```

必ず完全修飾パス名を指定してください。パス名にスペースが含まれている場合は、パス名を引用符で囲みます。

例：

```
command: "C:\Program Files\NetApp\SnapCreator commands\sdcli.exe"
command: myscript.bat
```

注： セキュリティ上の理由から、ワイルドカードエントリ（*）を使用してすべてのコマンドを許可しないでください。

カスタム プラグイン

ホストにカスタムプラグインをインポートすると、SnapCenterはプラグインzipファイルのSHA512ハッシュが custom_plugin_checksum_list ホスト上のファイルに存在するかどうかを確認します。

この custom_plugin_checksum_list ファイルは、SnapCenterからホストへのカスタムプラグインインストールの一部として出荷されます。NetAppで作成されたカスタムプラグインのSHA512ハッシュが含まれます。custom_plugin_checksum_list ファイルに書き込むことができるのは、Windowsの管理者またはLinuxのrootだけです。

Linuxホスト上のチェックサムファイルの場所は次のとおりです。

```
/var/opt/snapcenter/scc/custom_plugin_checksum_list.txt
```

同様に、Windowsホストでは、ファイルのデフォルトの場所は次のとおりです。

```
C:\Program Files\NetApp\SnapCenter Plug-in Creator\etc\custom_plugin_checksum_list.txt
```

カスタムインストールパスが次の場所で使用されている場合、デフォルトの場所は上記と同じです。

```
<custom path>\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\custom_plugin_checksum_list.txt
```

自分で作成したカスタムプラグインをインポートするには、プラグインのzipファイルのSHA512チェックサムを custom_plugin_checksum_list ホスト上のに追加する必要があります。これには、次の手順を実行します。

1. プラグインのzipファイルのSHA512ハッシュを生成します。https://emn178.github.io/online-tools/sha512_file_hash.htmlやLinux上のSHA512ツールのような任意のオンラインツールを使用できます。certutilを使用することもできます

Windowsでは、`certutil -hashfile "<plugin_zipfile>"` 次のようにコマンドSHA512を使用してツールを実行します。

```
C:\Users\Administrator\Desktop>certutil -hashfile "MySQL_plugin.zip" SHA512
SHA512 hash of file MySQL_plugin.zip:
8befbe32c97dee430edd212edc4119a28e52c29a7978d702139b73f4a7481e2381c71d9c8995034eda3cb5c44b5bb14a690e23c073afde41e55b9b182a01fc5a
CertUtil: -hashfile command completed successfully.
```

2. `custom_plugin_checksum_list` ホスト管理者（Linuxの場合はroot）に問い合わせて、生成されたSHA512ハッシュをホスト上のファイルに別の行に追加します。ハッシュが属するプラグインを識別するために、#記号で始まるコメントをファイルに追加できます。Windowsでは、このファイルの編集にワードパッドを使用することをお勧めします。

   次のチェックサムファイルのサンプルエントリを参照してください。

```
#ORASCPM 0.1
03721f567a1e4a1cb5569066b9a58af619ee12b1f8713108f81b696cfbdb81c25232fa63d6e6777a2b2a1ec068bb0a93a
59a8ade71587182f8bccbe81f7e0ba6
```

3. カスタムプラグインをインポートします。

監査

SPLまたはSCCがrootとして実行されている場合は `<user_install_dir>/Netapp/snapcenter/scc/logs/audit.log`、次のようににににある監査ログに記録されます。

```
06-12-2022 19:45:59: SPL process with pid 21234 is running as root
06-12-2022 19:45:59: SCC process with pid 21595 is running as root
```

この監査ファイルを使用して、SCC / SPLが特権ユーザ（root）として実行されているかどうかを監視できます。ロギングは、SPL / SCC run-asユーザがrootに切り替えられたときにのみ実行されます。

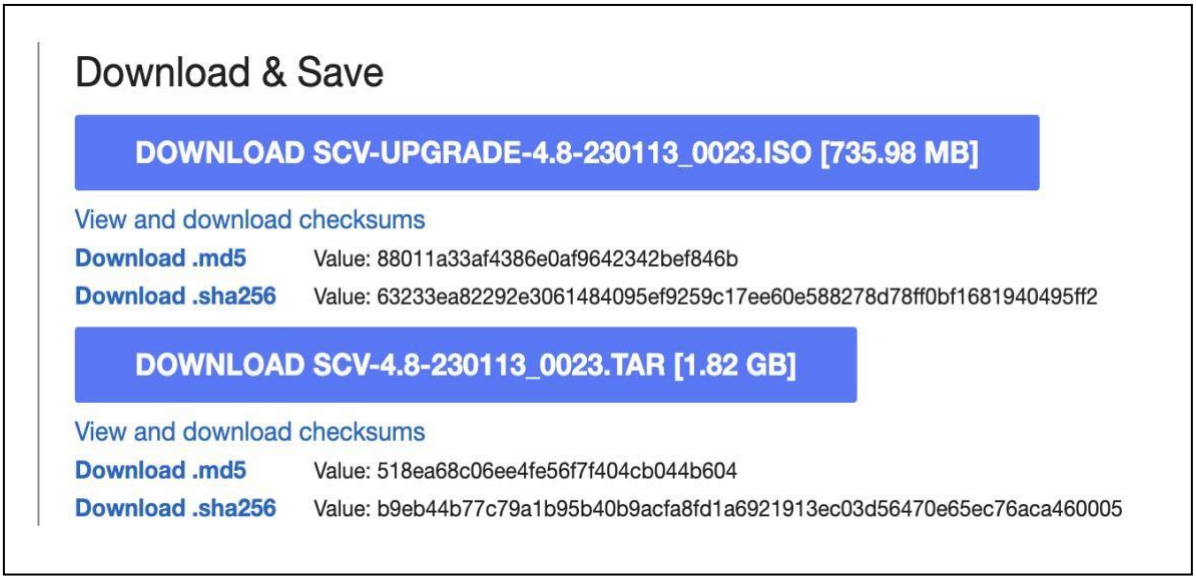
VMware vSphere用SnapCenterプラグインの強化

SnapCenter Plug-in for VMware vSphere

NetAppのダウンロードの整合性検証

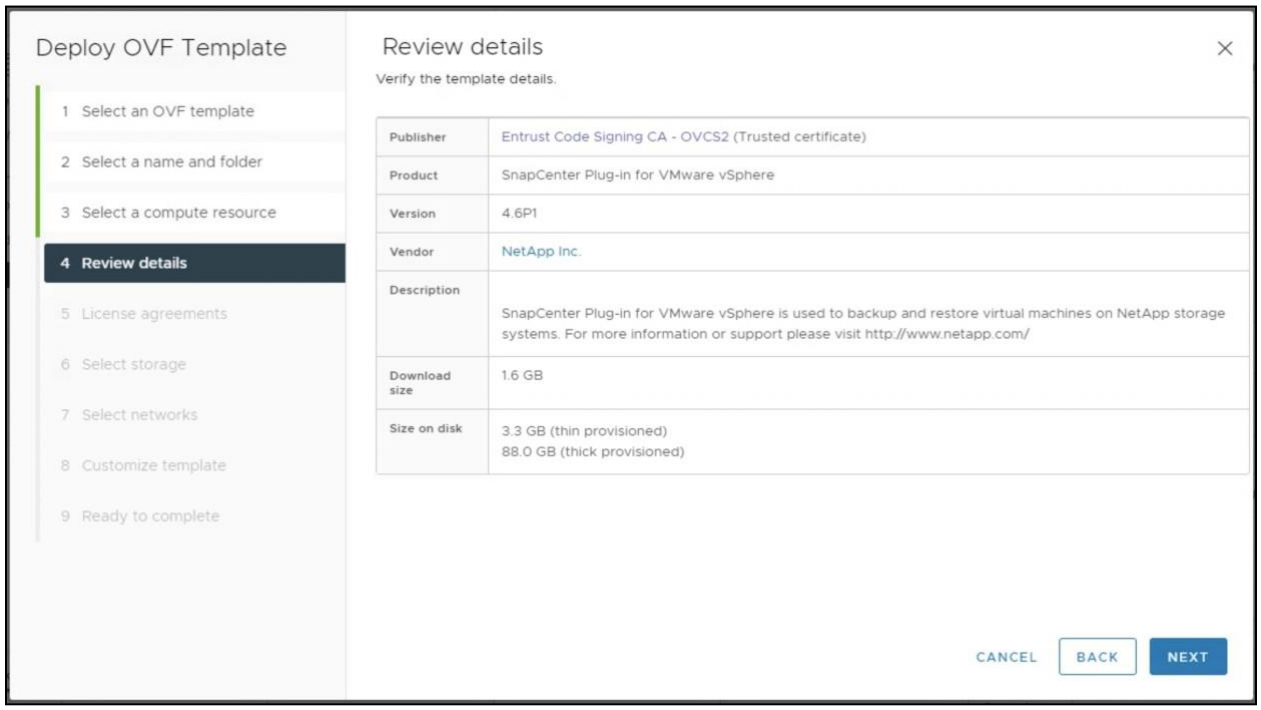
NetAppのダウンロードページから製品をダウンロードする場合は、NetApp MD5チェックサムとSHA256チェックサムをメモして、ダウンロードしたファイルが改ざんされていないことを確認することをお勧めします。製品を導入する前に、標準のチェックサム検証ツールを使用してチェックサムを検証できます。この手順は、ダウンロードしたファイルの整合性と信頼性を確保し、悪意のあるソフトウェアパッケージや破損したソフトウェアパッケージのインストールを防止するのに役立ちます。

tarファイルには、OVA（Open Virtual Appliance）とcertsフォルダが含まれています。このフォルダには、OVAおよびISOの整合性と信頼性を検証するための証明書が含まれています。

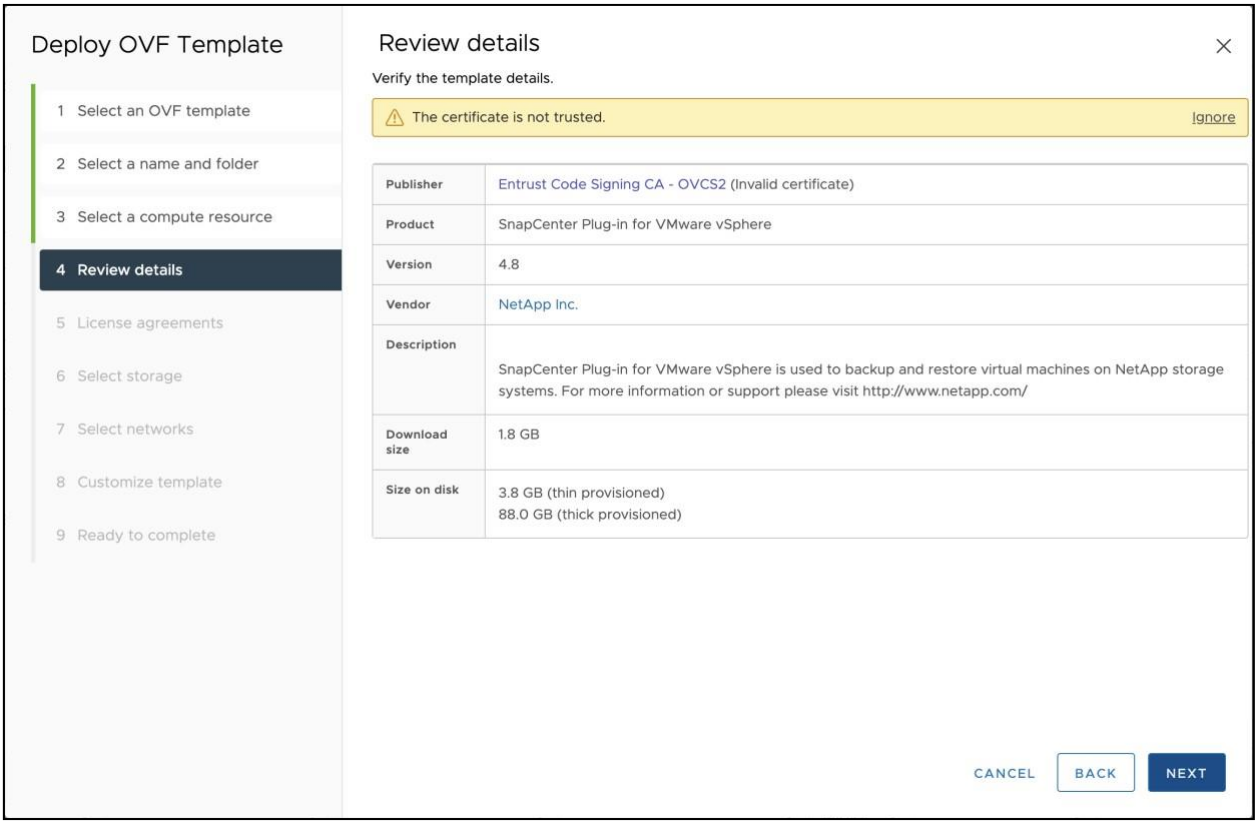


VMware vCenterへのOVAの導入

SnapCenter Plug-in for VMware vSphereは、vCenterに導入可能なOVAファイルとして出荷されます。導入プロセスでは、vCenterによってOVAファイルの整合性が検証され、ファイルが改ざんされておらず、インストールしても安全であることが確認されます。



既知の問題が原因で、次の図に示すように、VC 7.0.3ではOVA整合性検証が正常に機能しない可能性があります。



OVAファイルの整合性検証を有効にするには、このリンクの手順に従って、証明書をvCenter（7.0U3E以降）にインポートする必要があります。

vCenterでのSnapCenter Plug-in for VMware vSphereアプライアンスの保護

vCenterでのvCenter Manageアプライアンス

vCenterにアプライアンスを導入したら、vCenterでアプライアンスに割り当てられているアクセス許可を確認します。アクセス権を持つユーザまたはグループを確認し、適切なアクセス制御を行うために必要な変更を行います。

必要なRBAC権限

SnapCenter Plug-in for VMware vSphereの導入、アップグレード、および使用に必要なRBAC権限については、NetAppのドキュメントページで確認できます。このページには、vCenterでユーザまたはグループに必要な権限を割り当てる手順も記載されています。

vCenterの権限については、NetAppのドキュメントを参照してください。最小限必要な権限が記載されています。

CA署名証明書の有効化

SnapCenter VMwareプラグインは、クライアントブラウザとのセキュアな通信を実現するために、SSL（Secure Socket Layer）暗号化を採用しています。この方法ではネットワーク全体でデータを暗号化できますが、新しい自己署名証明書を作成するか、独自の認証局（CA）インフラまたはサードパーティのCAを使用することで、証明書が環境に固有のものになります。追加情報の場合は、このリンクをクリックしてください。

ソフトウェアコンポーネント

アプライアンスに導入および使用されているすべてのNetAppコンポーネントとサードパーティコンポーネントのチェックサムが検証されます。安全な開発活動については、NetAppのドキュメントを参照してください。

表4）組み込みユーザ

ユーザ	説明
メンテナンスコンソールユーザ	メンテナンスコンソールの操作を実行します。 資格情報を変更するには： 1. メンテナンスコンソールのウィンドウにアクセスします。 2. システム設定に「2」と入力します。 3. maintユーザのパスワードを変更するには、「3」と入力します。 4. 新しいパスワードを入力します。
管理ユーザ	管理UIを使用して クレデンシャルを変更します。 1. メンテナンスコンソールのウィンドウにアクセスする 2. アプリケーション設定に「1」を入力します。 3. ユーザ名またはパスワードを変更するには、「4」と入力します。 4. 新しいパスワードを入力します。
vCenterユーザ	vSphere ClientとREST APIを使用したプラグインの処理 vCenterのドキュメントに従ってクレデンシャルを変更します。
MySQLユーザ	アプライアンスのMySQLインスタンスを管理します。資格情報を変更するには： 1. メンテナンスコンソールウィンドウへのアクセス 2. アプリケーション設定に「1」を入力します。 3. 「5」と入力してMySQLパスワードを変更します。 4. 新しいパスワードを入力します。
diagユーザ	リモート診断を実行します。 リモート診断を有効にするときは、diagユーザのパスワードを設定する必要があります。

ポートとプロトコル

表5）ポートとプロトコル

ポートのタイプ	事前設定済みポート
VMware ESXi Serverのポート	**443**（HTTPS）、双方向 ゲスト ファイルのリストア機能では、このポートが使用されます。
SnapCenter Plug-in for VMware vSphereのポート	**8144**（HTTPS）、双方向 このポートはVMware vSphere ClientおよびSnapCenter Serverからの通信用です。 **8080**、双方向

ポートのタイプ	事前設定済みポート
	このポートは仮想アプライアンスの管理に使用します。 **注：** ポート設定は変更できません。
VMware vSphere vCenter Serverのポート	VVol VMを保護する場合は、ポート443を使用する必要があります。
ストレージ クラスタまたはStorage VMのポート	**443**（HTTPS）、双方向 **80**（HTTP）、双方向 このポートは、仮想アプライアンスと、Storage VMまたはStorage VMを含むクラスタとの間の通信に使用されます。

監査ログ

監査ログは、システムアクティビティを時系列で記録したもので、システムで実行されたイベントやアクションの記録を提供します。セキュリティとコンプライアンスを目的としたアクティビティの監視とレビューに使用されます。監査ログファイルはに生成され `/var/log/netapp/audit`ます。NetAppでは、定期的に監査ログを確認して、イベントの追跡、問題のトラブルシューティング、ユーザアクティビティの監視を行うことを推奨しています。追加情報は、NetAppのドキュメントページにあります。

MySQLリポジトリデータベース

デフォルト設定の保護

SnapCenter Plug-in for VMware vSphereアプライアンスにはMySQLが導入され、MySQL rootユーザのパスワードが自動生成されます。これは複雑なパスワードです。パスワードは、MySQLデータを検査する場合にのみ変更してください。MySQLパスワードは次のように変更できます。

1. メンテナンスコンソールのウィンドウを開きます。メンテナンスコンソールにアクセスします。
2. メインメニューから、オプション **1）Application Configuration**と入力します。
3. [Application Configuration Menu]から、オプション **5）[Change MySQL password]**を入力します。
4. ガイドラインを確認し、新しい複雑なパスワードを設定します。

ストレージ設定

必要なONTAP権限については、NetAppのドキュメントを参照してください。

ニンショウホウシキ

SnapCenter Plug-in for VMware vSphereには、ストレージを管理するための2つの認証モード（クレデンシャルベースと証明書ベース）があります。

クレデンシャルベースの認証は、認証のためにユーザ名とパスワードの組み合わせに依存します。ただし、セキュリティと相互認証を強化するために、NetAppでは証明書ベースの認証の使用を推奨しています。要件に応じて、CA署名証明書または認証用の自己署名証明書のいずれかの手順を実行できます。

Transport Layer Security（TLS）の設定

SnapCenter Plug-in for VMware vSphereアプライアンスでは、セキュリティを強化するためにデフォルトでTLS v1.0およびTLS v1.1が無効になっています。つまり、TLS v1.2とTLS v1.3のみが有効になっており、通信でサポートされています。

TLS設定の確認

SnapCenter Plug-in for VMware vSphereアプライアンスでTLSのバージョンを無効にしたり確認したりする方法については、こちらの技術情報アーティクルを参照してください。

弱い暗号の無効化

SnapCenterは、暗号がWindows構成の一部であるWindowsサーバにインストールされます。デフォルトでは、弱い暗号は手動設定が完了するまで有効になります。そのため、SCVでは弱い暗号を使用する必要があります。弱い暗号を無効にするには、`disable.weakCiphers scbr.override` ファイルのプロパティのデフォルト値を上書きします。手順については、NetAppのドキュメントを参照してください。

DoS攻撃

DebianシステムをDoS攻撃から保護するには、iptablesと呼ばれる組み込みのファイアウォールツールを使用します。iptablesを使用すると、送受信ネットワークトラフィックを制限および制御するためのさまざまなルールを設定できます。

iptablesを使用したDoS攻撃を防ぐ1つの方法は、特定のIPアドレスまたはネットワークからのトラフィックのレートを制限することです。この手法はレート制限と呼ばれ、トラフィックでネットワークをフラッディングする攻撃を軽減するのに効果的です。トラフィックのレートを制限することで、DoS攻撃の影響を最小限に抑え、正当なトラフィックが引き続き通過できるようにします。

```
iptables -A INPUT -m conntrack --ctstate NEW -m hashlimit --hashlimit-above 10/sec --hashlimit-burst 5 --hashlimit-mode srcip --hashlimit-name conn-rate-limit -j DROP
```

このコマンドは、ファイアウォールの入力チェーンに新しいルールを追加します。これにより、各送信元IPアドレスからの着信接続のレートが、最大5つの接続のバーストで1秒あたり10個以下に制限されます。このルールは、新しい接続の一部である着信トラフィックだけを照合し、接続レート制限を超えた着信パケットをドロップします。これにより、単一の送信元IPアドレスから生成できるトラフィックの量を制限することで、DoS攻撃を防ぐことができます。

詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、以下のドキュメントやWebサイトを確認してください。

- SnapCenterソフトウェアのドキュメント リソース
  https://www.netapp.com/cyber-resilience/data-protection/snapcenter/documentation/
- NetApp SnapCenterを使用したMicrosoft SQL Serverのベストプラクティス
  https://www.netapp.com/pdf.html?item=/media/12400-tr4714.pdf
- NetApp SnapCenterでOracleプラグインを使用する場合のベストプラクティス
  https://www.netapp.com/pdf.html?item=/media/12403-tr4700.pdf
- SnapCenterプラグインVMware vSphere -製品のセキュリティ
  https://docs.netapp.com/us-en/netapp-solutions/virtualization/scvmware-security-secure-development-activities.html

バージョン履歴

バージョン	日付	ドキュメントの改訂履歴
バージョン1.0	2023年3月	最初のドキュメントリリース。
バージョン2.0	2023年4月	追加されたSCVコンテンツ。

本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、NetApp サポート サイトで Interoperability Matrix Tool (IMT)を参照してください。NetApp IMT には、NetApp がサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

商標に関する情報

TR-4957-0323-JP

NetApp