SnapCenter Serverのインストールと構成

SnapCenter software

NetApp
November 06, 2025

目次

SnapCenter Serverのインストールと構成

SnapCenter Serverのインストールの準備

SnapCenter Server をインストールするための要件

Windows または Linux ホストにSnapCenter Server をインストールする前に、環境のすべての要件が満たされていることを確認する必要があります。

Windowsホストのドメインとワークグループの要件

SnapCenter Server は、ドメインまたはワークグループ内の Windows ホストにインストールできます。

管理者権限を持つユーザーは、 SnapCenterサーバーをインストールできます。

- Active Directory ドメイン: ローカル管理者権限を持つドメイン ユーザーを使用する必要があります。ドメイン ユーザは、Windowsホストのローカル管理者グループのメンバーである必要があります。
- ワークグループ: ローカル管理者権限を持つローカル アカウントを使用する必要があります。

ドメイン トラスト、マルチドメイン フォレスト、およびクロスドメイン トラストはサポートされていますが、クロスフォレスト ドメインはサポートされません。詳細については、Active Directoryドメインと信頼に関するMicrosoftのドキュメントを参照してください。

> SnapCenter Server をインストールした後は、 SnapCenterホストが配置されているドメインを変更しないでください。 SnapCenter Server がインストールされたときに存在していたドメインからSnapCenter Server ホストを削除し、その後SnapCenter Server をアンインストールしようとすると、アンインストール操作は失敗します。

スペースとサイジングの要件

スペースとサイズの要件をよく理解しておく必要があります。

項目	**Windows**ホストの要件	**Linux**ホストの要件
オペレーティング システム	Microsoft Windows サポートされているのは、英語版、ドイツ語版、日本語版、簡体字中国語版のみです。 サポートされているバージョンに関する最新情報については、https://imt.netapp.com/matrix/imt.jsp?components=121033;&solution=1258&isHWU&src=IMT["NetApp Interoperability Matrix Tool"^] 。	• Red Hat Enterprise Linux（RHEL）8および9 • SUSE Linux Enterprise Server（SLES）15 サポートされているバージョンに関する最新情報については、https://imt.netapp.com/matrix/imt.jsp?components=121032;&solution=1258&isHWU&src=IMT["NetApp Interoperability Matrix Tool"^] 。
最小CPU数	4	4

項目	**Windows**ホストの要件	**Linux**ホストの要件
最小RAM	8 GB MySQL Serverのバッファ プールがRAMの20%を使用します。	8 GB
最小ハード ドライブ スペース - SnapCenter Serverソフトウェアおよびログ用	7 GB SnapCenter Serverがインストールされているドライブと同じドライブにSnapCenterリポジトリがある場合は、15 GBを使用することを推奨します。	15 GB
最小ハード ドライブ スペース - SnapCenterリポジトリ用	8 GB 注意: SnapCenterリポジトリがインストールされているドライブと同じドライブにSnapCenter Server がある場合は、15 GB を用意することをお勧めします。	該当なし
必要なソフトウェア パッケージ	• ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドル • PowerShell 7.4.2以降	• .NET Framework 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) • PowerShell 7.4.2以降 • Nginxはリバース プロキシとして使用できるWebサーバ • Pam-devel PAM（Pluggable Authentication Modules）は、システム管理者が、認証を行うプログラムを再コンパイルすることなく認証ポリシーを設定できるようにするシステム セキュリティ ツールです。

ASP.NET コアでは、Windows 上のSnapCenter Server の一時ファイル システムにアクセスするために IIS_IUSRS が必要です。

SANホストの要件

SnapCenter にはホスト ユーティリティや DSM は含まれていません。 SnapCenterホストが SAN (FC/iSCSI) 環境の一部である場合は、 SnapCenter Server ホストに追加のソフトウェアをインストールして構成する必要がある場合があります。

- ホスト ユーティリティ: ホスト ユーティリティは FC と iSCSI をサポートしており、Windows サーバーで MPIO を使用できるようになります。 "詳細情報" 。
- Microsoft DSM for Windows MPIO: このソフトウェアは Windows MPIO ドライバーと連携して、 NetApp と Windows ホスト コンピューター間の複数のパスを管理します。ハイアベイラビリティ構成にはDSMが必要です。

ONTAP DSMを使用していた場合は、Microsoft DSMに移行する必要があります。詳細については、以下を参照してください。 "ONTAP DSMからMicrosoft DSMへの移行方法" 。

ブラウザの要件

SnapCenter softwareは、 Chrome 125 以降および Microsoft Edge 110.0.1587.17 以降をサポートしています。

ポート要件

SnapCenter softwareでは、異なるコンポーネント間の通信に異なるポートが必要です。

- 1つのポートを複数のアプリケーションで共有することはできません。
- デフォルト 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。
- 固定ポートの場合は、デフォルトのポート番号を受け入れる必要があります。
- 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 デバイスによって接続が妨げられないように注意してください。
  - SnapCenter をインストールするときにカスタム ポートを指定する場合は、 SnapCenterプラグイン ローダーのそのポートのファイアウォール ルールをLoader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まとめています。

ポート名	ポート番号	プロトコル	送受信方向	説明
SnapCenter Webポート	8146	HTTPS	双方向	このポートは、SnapCenterクライアント (SnapCenterユーザー) とSnapCenter Server 間の通信に使用され、プラグインホストからSnapCenter Server への通信にも使用されます。 ポート番号をカスタマイズできます。
SnapCenter SMCoreの通信ポート	8145	HTTPS	双方向	このポートは、SnapCenter ServerとSnapCenterプラグインがインストールされているホスト間の通信に使用されます。 ポート番号をカスタマイズできます。
スケジューラ サービス ポート	8154	HTTPS		このポートは、SnapCenter Serverホスト内で管理されるすべてのプラグインのSnapCenterスケジューラのワークフローを一元的にオーケストレーションするために使用されます。 ポート番号をカスタマイズできます。
RabbitMQ ポート	5672	TCP		これは RabbitMQ がリッスンするデフォルトのポートであり、Scheduler サービスとSnapCenter 間のパブリッシャー - サブスクライバーモデル通信に使用されます。

ポート名	ポート番号	プロトコル	送受信方向	説明
MySQLのポート	3306	HTTPS		このポートは、SnapCenterリポジトリ データベースとの通信に使用されます。 SnapCenter サーバーから MySQL サーバーへの安全な接続を作成できます。"詳細情報"
Windowsプラグイン ホスト	135, 445	TCP		このポートは、SnapCenter Server とプラグインがインストールされているホスト間の通信に使用されます。 Microsoft によって指定された追加の動的ポート範囲も開いている必要があります。
Linux / AIXプラグイン ホスト	22	SSH	一方向	このポートは、サーバからクライアント ホストに開始される、 SnapCenterサーバとホスト間の通信に使用されます。
Windows、Linux、AIX 用のSnapCenter プラグイン パッケージ	8145	HTTPS	双方向	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間の通信に使用されます。 カスタマイズ可能。 ポート番号をカスタマイズできます。
SnapCenter Plug-in for Oracle Database	27216			デフォルトのJDBC ポートは、Oracleデータベースに接続するためにOracle用プラグインで使用されます。

ポート名	ポート番号	プロトコル	送受信方向	説明
SnapCenter Plug-in for Exchange Database	909			デフォルトのNET.TCPポートは、Exchange VSSコールバックに接続するためにPlug-in for Windowsで使用されます。
NetAppでサポートされるSnapCenter用プラグイン	9090	HTTPS		これはプラグイン ホストでのみ使用される内部ポートであり、ファイアウォールの例外は必要ありません。 SnapCenterサーバーとプラグイン間の通信は、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の通信ポート	• 443（HTTPS） • 80（HTTP）	• HTTPS • HTTP	双方向	このポートは、SnapCenter Serverを実行するホストとSVMの間の通信のためにSAL（Storage Abstraction Layer）で使用されます。また、現在は、SnapCenterプラグイン ホストとSVMの間の通信のためにSnapCenter for Windowsプラグイン ホストのSALでも使用されます。
SnapCenter Plug-in for SAP HANA Database	• 3インスタンス番号13 • 3インスタンス番号15	• HTTPS • HTTP	双方向	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。 ポート番号をカスタマイズできます。

ポート名	ポート番号	プロトコル	送受信方向	説明
SnapCenter Plug-in for PostgreSQL	5432			このポートは、PostgreSQL 用プラグインが PostgreSQL クラスターと通信するために使用されるデフォルトの PostgreSQL ポートです。 ポート番号をカスタマイズできます。

SnapCenterソフトウェアにアクセスするための登録

Amazon FSx for NetApp ONTAPまたはAzure NetApp Filesを初めて使用し、既存のNetAppアカウントを持っていない場合は、 SnapCenter softwareにアクセスするために登録する必要があります。

開始する前に

- 会社のEメールIDにアクセスできる必要があります。
- Azure NetApp Filesを使用している場合は、AzureサブスクリプションIDが必要です。
- Amazon FSx for NetApp ONTAPを使用している場合は、FSx for ONTAPファイルシステムのファイルシステムIDが必要です。

タスク概要

登録には情報検証が必要であり、確認と新しいNetAppサポート サイト (NSS) アカウントの ゲスト アクセスから フル アクセスへのアップグレードには最大 1 日かかる場合があります。

手順

1. クリック https://mysupport.netapp.com/site/user/registration登録用。
2. 会社のメール ID を入力し、キャプチャを完了し、NetApp のプライバシー ポリシーに同意して、[送信] をクリックします。
3. メール ID に送信された OTP を入力して登録を認証し、「続行」をクリックします。
4. 登録完了ページで、以下の情報を入力して登録を完了します。
   a. * NetApp顧客/エンドユーザー* を選択します。
   b. [シリアル番号] フィールドに、 Azure NetApp Files を使用している場合は Azure サブスクリプション ID を入力し、 Amazon FSx for NetApp ONTAPを使用している場合はファイル システム ID を入力します。

チケットを申請するには https://mysupport.netapp.com/site/help登録中に問題が発生した場合、またはステータスを知りたい場合。

多要素認証（**MFA**）

多要素認証（**MFA**）の管理

Active Directoryフェデレーション サービス（AD FS）サーバとSnapCenter Serverで多要素認証（MFA）機能を管理できます。

多要素認証（**MFA**）の有効化

SnapCenter ServerのMFA機能は、PowerShellコマンドを使用して有効にできます。

タスク概要

- 同じAD FSに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。セキュリティ上の理由から、一部のAD FS構成では、AD FSセッションの永続化に応じて、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できるパラメータとその説明に関する情報は、以下を実行することで取得できます。 `Get-Help command_name` 。あるいは、 "SnapCenterソフトウェア コマンドレット リファレンス ガイド" 。

開始する前に

- Windows Active Directoryフェデレーション サービス（AD FS）が、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やCisco Duoなど、AD FSでサポートされている多要素認証サービスが必要です。
- SnapCenter Server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にする必要があります。
- SnapCenter Server用に、承認済みのCA証明書を取得して設定します。

  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とF5間の通信が切断されないようにします。
  - スタンドアロン構成または高可用性構成でのアップグレード、修復、ディザスタ リカバリ（DR）の実行中に自己署名証明書が再作成されないようにして、MFAの再設定を回避します。
  - 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ファイルの生成" 。

手順

1. Active Directoryフェデレーション サービス（AD FS）のホストに接続します。
2. AD FSフェデレーションメタデータファイルを以下からダウンロードします。"https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml" です。
3. ダウンロードしたファイルをSnapCenter Server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 Serverにログインします。
5. PowerShell セッションで、*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. SnapCenter ServerのMFAを有効にするには、 `Set-SmMultiFactorAuthentication`コマンドレット。
8. （オプション）MFAの構成ステータスと設定を確認するには、 `Get-SmMultiFactorAuthentication`コマンドレット。
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 > 個人 > 証明書 をクリックします。
   e. SnapCenterにバインドされた 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. アクセス許可ウィザードで、次の手順を実行します。
      i. *[追加]*をクリックします。
      ii. *場所*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。
      iii. *場所*ポップアップウィンドウで*OK*をクリックします。
      iv. 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。

      チェックが成功した場合は、[**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 > 証明書利用者信頼の追加 > 開始 を右クリック。
    b. 2 番目のオプションを選択し、 SnapCenter MFA メタデータ ファイルを参照して、[次へ] をクリックします。
    c. 表示名を指定して、[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. *クレーム発行ポリシーの編集*をクリックします。
    b. *ルールの追加*をクリックし、*次へ*をクリックします。
    c. 要求規則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*User-Principal-Name*を選択し、出力クレームの種類として*Name-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. [エンドポイント]、[識別子]、[署名]フィールドに値が入力されていることを確認します。

14. すべてのブラウザ タブを閉じ、ブラウザを再度開いて既存の、またはアクティブなセッションCookieをクリアし、再度ログインします。

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。

トラブルシューティング情報については、 "複数のタブで同時にログインしようとすると、MFAエラーが表示されます" 。

AD FS MFAメタデータの更新

アップグレード、CA証明書の更新、DRなど、AD FSサーバに何らかの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。

手順

1. AD FSフェデレーションメタデータファイルを以下からダウンロードします。"https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml"
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. すべてのブラウザ タブを閉じ、ブラウザを再度開いて既存の、またはアクティブなセッションCookieをクリアし、再度ログインします。

SnapCenter MFAメタデータの更新

修復、CA証明書の更新、DRなど、ADFSサーバに何らかの変更があった場合は、AD FSでSnapCenter MFAメタデータを更新する必要があります。

手順

1. 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*を選択します。

b. SnapCenter用に作成された証明書利用者信頼を右クリックし、[削除] を選択します。

証明書利用者信頼のユーザ定義名が表示されます。

c. 多要素認証（MFA）を有効にします。

見る"多要素認証を有効にする" 。

2. すべてのブラウザ タブを閉じ、ブラウザを再度開いて既存の、またはアクティブなセッションCookieをクリアし、再度ログインします。

多要素認証（**MFA**）の無効化

手順

1. MFAを無効にし、MFAが有効になったときに作成された構成ファイルをクリーンアップします。 `Set-SmMultiFactorAuthentication`コマンドレット。
2. すべてのブラウザ タブを閉じ、ブラウザを再度開いて既存の、またはアクティブなセッションCookieをクリアし、再度ログインします。

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

MFAログインは、ブラウザ、REST API、PowerShell、およびSCCLIでサポートされます。MFA は AD FS ID マネージャーを通じてサポートされます。GUI、REST API 、PowerShell、SCCLIを使用して、MFAの有効化、MFAの無効化、およびMFAの設定を行うことができます。

AD FSの**OAuth / OIDC**としてのセットアップ

Windows GUIウィザードを使用して**AD FS**を構成する

1. サーバー マネージャー ダッシュボード > ツール > **ADFS** 管理 に移動します。
2. **ADFS** > アプリケーション グループ に移動します。
   a. アプリケーション グループ を右クリックします。
   b. アプリケーション グループの追加 を選択し、アプリケーション名 を入力します。
   c. *サーバーアプリケーション*を選択します。
   d. *次へ*をクリックします。
3. *クライアント識別子*をコピーします。

   これがクライアントIDです。..[リダイレクトURI]にコールバックURL（SnapCenter ServerのURL）を追加します。..*次へ*をクリックします。

4. *共有シークレットの生成*を選択します。

   シークレット値をコピーします。これがクライアントのシークレットです。..*次へ*をクリックします。

5. *概要*ページで*次へ*をクリックします。
   a. *完了*ページで*閉じる*をクリックします。
6. 新しく追加された*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。

7. アプリのプロパティから*アプリケーションの追加*を選択します。
8. *アプリケーションを追加*をクリックします。

   Web APIを選択し、[次へ]をクリックします。

9. [Web APIの構成]ページで、SnapCenter ServerのURLと前の手順で作成したクライアントIDを[識別子]セクションに入力します。
   a. *[追加]*をクリックします。
   b. *次へ*をクリックします。
10. *アクセス制御ポリシーの選択*ページで、要件に基づいて制御ポリシーを選択し (たとえば、すべてのユーザーを許可し、MFA を要求する)、*次へ*をクリックします。
11. *アプリケーションの権限の構成*ページでは、デフォルトで openid がスコープとして選択されているので、*次へ*をクリックします。
12. *概要*ページで*次へ*をクリックします。

    *完了*ページで*閉じる*をクリックします。

13. サンプル アプリケーションのプロパティ ページで、**OK** をクリックします。
14. 承認サーバ（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」つまり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。

15. 選択したWebAPIを編集し、コールバックURL（SnapCenter Serverの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を設定します。

16. サーバー マネージャーの右上にある ツール メニューの下にある **AD FS** 管理 ツールを開きます。
    a. 左側のサイドバーから*アプリケーション グループ* フォルダを選択します。
    b. Web API を選択し、[編集] をクリックします。
    c. [発行変換規則]タブに移動します。
17. *ルールの追加*をクリックします。
    a. クレーム ルール テンプレートのドロップダウンで、**LDAP** 属性をクレームとして送信 を選択します。
    b. *次へ*をクリックします。
18. *クレームルール*の名前を入力します。
    a. 属性ストアのドロップダウンで*Active Directory*を選択します。
    b. **LDAP** 属性 ドロップダウンで **User-Principal-Name** を選択し、送信クレーム タイプ ドロップダウンで **UPN** を選択します。
    c. *[完了]*をクリックします。

PowerShellコマンドを使用したアプリケーション グループの作成

PowerShellコマンドを使用して、アプリケーション グループ、Web APIを作成し、スコープと要求を追加できます。これらのコマンドは、自動スクリプト形式で使用できます。詳細については、<KB 記事へのリンク>を参照してください。

1. 次のコマンドを使用して、AD FSに新しいアプリケーション グループを作成します。

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

   `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用の有効なURL

2. 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
   ```

3. ADFS 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"
   ```

4. クライアントIDとクライアント シークレットは1回しか表示されないため、次のコマンドの出力から取得します。

   ```
   "client_id = $identifier"

   "client_secret: "$($ADFSApp.ClientSecret)
   ```

5. AD FSアプリケーションにallatclaims権限とopenid権限を付与します。

   ```
   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);

"@
```

6. 変換規則ファイルを書き出します。

```
$transformrule |Out-File -FilePath .\issueancetransformrules.tmp -force
-Encoding ascii $relativePath = Get-Item .\issueancetransformrules.tmp
```

7. 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変換規則を定義します。

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API"
-TargetIdentifier

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

アクセス トークンの有効期限の更新

PowerShellコマンドを使用して、アクセス トークンの有効期限を更新できます。

このタスクについて

- アクセス トークンは、ユーザ、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、期限切れになるまで有効です。
- デフォルトでは、アクセス トークンの有効期間は60分です。最小値の有効期間でも十分な長さになるよう設定されています。現在進行中のビジネス クリティカルなジョブが妨げられないように、十分な値を指定する必要があります。

ステップ

アプリケーション グループWebAPIのアクセス トークンの有効期限を更新するには、AD FSサーバで次のコマンドを使用します。

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

AD FSからのBearerトークンの取得

RESTクライアント（Postmanなど）で以下のパラメータを入力する必要があります。RESTクライアントからユーザ クレデンシャル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には、2 要素認証 (ユーザーが所有している情報と、ユーザーが何者であるか) を入力する必要があります。

+ ベアラー トークンの有効期間はアプリケーションごとに AD FS サーバーから構成可能で、デフォルトの有効期間は 60 分です。

フィールド	Value
助成金の種類	Authorization Code

Callback 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。
Auth URL	[adfsドメイン名]/adfs/oauth2/authorize
Access token URL	[adfsドメイン名]/adfs/oauth2/トークン
クライアントID	AD FSクライアントIDを入力します。
Client secret	AD FSクライアント シークレットを入力します。
Scope	OpenID
クライアント認証	Send as Basic AUTH Header
リソース	詳細オプション タブで、コールバック URL と同じ値を持つリソース フィールドを追加します。この値は、JWT トークンの "aud" 値として提供されます。

PowerShell、**SCCLI**、**REST API**を使用した**SnapCenter Server**での**MFA**の設定

PowerShell、SCCLI、およびREST APIを使用して、SnapCenter ServerでMFAを設定できます。

SnapCenter MFA CLI認証

PowerShellとSCCLIでは、既存のコマンドレット（Open-SmConnection）を「AccessToken」という追加のフィールドで拡張し、Bearerトークンを使用してユーザを認証します。

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

上記のコマンドレットを実行すると、それぞれのユーザがSnapCenterコマンドレットを実行できるようにセッションが作成されます。

SnapCenter MFA REST API認証

REST API クライアント (Postman や swagger など) で *Authorization=Bearer <access token>* の形式のベアラー トークンを使用し、ヘッダーにユーザーの RoleName を指定して、 SnapCenterから正常な応答を取得します。

MFA REST APIのワークフロー

MFAがAD FSで設定されている場合、REST APIを使用してSnapCenterアプリケーションにアクセスするには、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。

このタスクについて

- Postman、Swagger UI、FireCampなど、任意のRESTクライアントを使用できます。
- 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、任意の処理を実行します。

手順

AD FS MFA 経由で認証するには

1. AD FSエンドポイントを呼び出してアクセス トークンを取得するようにRESTクライアントを設定します。

   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ます。そのページでADクレデンシャルを入力してMFAで認証する必要があります。1.AD FS SSOページで、[Username]テキスト ボックスにユーザ名または電子メールを入力します。

   + ユーザー名は、user@domain または domain\user の形式にする必要があります。

2. [Password]テキスト ボックスにパスワードを入力します。
3. *ログイン*をクリックします。
4. サインイン オプション セクションから認証オプションを選択し、認証します (構成によって異なります)。
   - プッシュ: 携帯電話に送信されるプッシュ通知を承認します。
   - 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確認コードを入力します。
   - ワンタイム パスワード: トークンのワンタイム パスワードを入力します。
5. 認証が成功すると、アクセス、ID、およびリフレッシュ トークンを含むポップアップが表示されます。

   アクセス トークンをコピーし、SnapCenter REST APIで使用して操作を実行します。

6. REST APIのヘッダー 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. AD FSから取得したこのアクセス トークンをSnapCenterが検証します。

   有効なトークンである場合、SnapCenterはそのトークンをデコードし、ユーザ名を取得します。

8. SnapCenterがユーザ名とロール名を使用して、API実行のためにユーザ認証を行います。

   認証に成功した場合、SnapCenterは結果を返します。失敗した場合は、エラー メッセージが表示されます。

REST API、**CLI**、**GUI**の**SnapCenter MFA**機能の有効化または無効化

GUI

手順

1. SnapCenter管理者としてSnapCenter Serverにログインします。
2. 設定 > グローバル設定 > *多要素認証(MFA)設定*をクリックします

3. インターフェイス（GUI / RST API / CLI）を選択してMFAログインを有効または無効にします。

PowerShell インターフェース

手順

1. GUI、REST API、PowerShell、SCCLIのMFAを有効にするためのPowerShellコマンドまたはCLIコマンドを実行します。

   ```
   Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled
   -IsCliMFAEnabled -Path
   ```

   pathパラメータには、AD FS MFAメタデータxmlファイルの場所を指定します。

   SnapCenter GUI、REST API、PowerShell、およびSCCLIが、指定したAD FSメタデータ ファイル パスを使用して設定され、MFAが有効になります。

2. MFAの構成ステータスと設定を確認するには、 `Get-SmMultiFactorAuthentication`コマンドレット。

SCCLIインターフェース

手順

1. ```
   # sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true
   -IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path
   "C:\ADFS_metadata\abc.xml"
   ```
2. ```
   # sccli Get-SmMultiFactorAuthentication
   ```

REST API

1. GUI、REST API、PowerShell、SCCLIのMFAを有効にするには、次のPOST APIを実行します。

パラメータ	Value
要求のURL	/api/4.9/settings/multifactorauthentication
HTTPメソッド	投稿
要求の本文	{ "IsGuiMFAEnabled": false、 "IsRestApiMFAEnabled": true、 "IsCliMFAEnabled": false、 "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml" }
応答の本文	{ "MFAConfiguration": { "IsGuiMFAEnabled": false、 "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": null、 "IsRestApiMFAEnabled": true、 "IsCliMFAEnabled": false、 "ADFSHostName": "win-adfs-sc49.winscedom2.com" } }

2. 次のAPIを使用して、MFAのステータスと設定を確認します。

パラメータ	Value
要求のURL	/api/4.9/settings/multifactorauthentication
HTTPメソッド	Get
応答の本文	{ "MFAConfiguration": { "IsGuiMFAEnabled": false、 "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": null、 "IsRestApiMFAEnabled": true、 "IsCliMFAEnabled": false、 "ADFSHostName": "win-adfs-sc49.winscedom2.com" } }

SnapCenter Serverのインストール

WindowsホストへのSnapCenter Serverのインストール

SnapCenter Serverインストーラの実行ファイルを使用して、SnapCenter Serverをインストールできます。

必要に応じて、PowerShellコマンドレットを使用して複数のインストール手順や設定手順を実行することもできます。PowerShell 7.4.2 以降を使用する必要があります。

コマンドラインからのSnapCenter Serverのサイレント インストールは、サポートされていません。

開始する前に

- SnapCenter ServerホストにWindowsの最新の更新プログラムが適用されていて、システムの再起動が完了している必要があります。
- SnapCenter Serverをインストールするホストに MySQL Serverがインストールされていないことを確認しておく必要があります。
- Windowsインストーラのデバッグを有効にしておく必要があります。

  有効化の詳細については、MicrosoftのWebサイトを参照してください。 "Windowsインストーラのログ" 。

  Microsoft Exchange Server、Active Directory、またはドメイン ネーム サーバが配置されたホストには、SnapCenter Serverをインストールしないでください。

手順

1. SnapCenter Serverのインストールパッケージを以下からダウンロードします。 "NetAppサポート サイト" 。

2. ダウンロードした.exeファイルをダブルクリックして、SnapCenter Serverのインストールを開始します。

   インストールを開始すると、すべての事前確認が実行されます。最小要件を満たしていない場合は、対応するエラーまたは警告メッセージが表示されます。

   警告メッセージは無視してインストールを続行できますが、エラーは修正する必要があります。

3. SnapCenter Serverのインストールに必要な入力済みの値を確認し、必要に応じて変更します。

   MySQL Serverリポジトリ データベースのパスワードを指定する必要はありません。SnapCenter Serverのインストール時には、パスワードが自動生成されます。

   > 特殊文字「`%`" is not supported in the custom path for the repository database. If you include "`パスに「%」が含まれていると、インストールは失敗します。

4. *今すぐインストール*をクリックします。

   無効な値を指定すると、対応するエラー メッセージが表示されます。値を再入力してからインストールを開始してください。

   > *キャンセル*ボタンをクリックすると、実行中のステップが完了し、ロールバック操作が開始されます。SnapCenter Serverはホストから完全に削除されます。

   ただし、「SnapCenter Server サイトの再起動」または「 SnapCenter Server の起動を待機中」の操作の実行中に [キャンセル] をクリックすると、操作はキャンセルされずにインストールが続行されます。

   ログ ファイルは常にadminユーザの%temp%フォルダに（古い順に）表示されます。ログの場所をリダイレクトする場合は、次のコマンドを実行して、コマンド プロンプトからSnapCenter Server のインストールを開始します。`C:\installer_location\installer_name.exe /log"C:\"`

インストール中に **Windows** ホストで有効になる機能

SnapCenter Serverインストーラでのインストール中、WindowsホストでWindowsの機能とロールが有効になります。これらは、ホスト システムのトラブルシューティングと保守に役立つ可能性があります。

カテゴリ	特徴
Webサーバー	• インターネット インフォメーション サービス • World Wide Webサービス • HTTP共通機能 ◦ 既定のドキュメント ◦ ディレクトリの参照 ◦ HTTPエラー ◦ HTTPリダイレクション ◦ 静的なコンテンツ ◦ WebDAV発行 • 状態と診断 ◦ カスタム ログ ◦ HTTPログ ◦ ログ ツール ◦ 要求監視 ◦ トレース • パフォーマンス機能 ◦ 静的なコンテンツの圧縮 • セキュリティ ◦ IPセキュリティ ◦ 基本認証 ◦ 一元的なSSL証明書のサポート ◦ クライアント証明書マッピング認証 ◦ IIS クライアント証明書マッピング認証 ◦ IPおよびドメインの制限 ◦ 要求フィルター ◦ URL承認 ◦ Windows認証 • アプリケーション開発機能 ◦ .NET拡張機能4.5 ◦ アプリケーションの初期化 ◦ ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドル ◦ サーバー側インクルード WebSocketプロトコル
	管理ツール

カテゴリ	特徴
IIS管理スクリプトおよびツール	• IIS管理サービス • Web管理ツール
.NET Framework 8.0.12 の機能	• ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドル • Windows Communication Foundation (WCF) HTTP Activation45 ◦ TCPアクティブ化 ◦ HTTPアクティブ化
Windowsプロセス アクティブ化サービス	プロセス モデル
構成API	All

Linuxホストへの**SnapCenter Server**のインストール

SnapCenter Serverインストーラの実行ファイルを使用して、SnapCenter Serverをインストールできます。

開始する前に

- SnapCenterをインストールするための十分な権限がないroot以外のユーザを使用してSnapCenter Serverをインストールする場合は、NetAppサポート サイトからsudoersチェックサム ファイルを入手します。Linuxのバージョンに基づいて適切なチェックサム ファイルを使用する必要があります。
- SUSE Linuxでsudoパッケージを使用できない場合は、認証の失敗を回避するためにsudoパッケージをインストールします。
- SUSE Linuxの場合は、インストールの失敗を回避するためにホスト名を設定します。
- 次のコマンドを実行して、Linuxのセキュアステータスを確認します。 `sestatus` 。 *SELinux* ステータスが「有効」で、現在のモード が「強制」の場合は、次の操作を実行します。
  - 次のコマンドを実行します。 `sudo semanage port -a -t http_port_t -p tcp <WEBAPP_EXTERNAL_PORT_>`

    _WEBAPP_EXTERNAL_PORT_のデフォルト値は8146です。
  - ファイアウォールがポートをブロックしている場合は、 `sudo firewall-cmd --add-port <WEBAPP_EXTERNAL_PORT_>/tcp`

    _WEBAPP_EXTERNAL_PORT_のデフォルト値は8146です。
  - 読み取りおよび書き込み権限があるディレクトリから、次のコマンドを実行します。
    - `sudo ausearch -c 'nginx' --raw | audit2allow -M my-nginx`

      コマンドから「nothing to do」が返された場合は、SnapCenter Serverのインストール後にコマン

ドを再実行します。

- コマンドによって *my-nginx.pp* が作成された場合は、次のコマンドを実行してポリシー パッケージをアクティブにします。 `sudo semodule -i my-nginx.pp`

◦ MySQL PID ディレクトリに使用されるパスは */var/opt/mysqld* です。次のコマンドを実行して、MySQLインストールの権限を設定します。

- `mkdir /var/opt/mysqld`
- `sudo semanage fcontext -a -t mysqld_var_run_t "/var/opt/mysqld(/.*)?"`
- `sudo restorecon -Rv /var/opt/mysqld`

◦ MySQL データ ディレクトリに使用されるパスは、*/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL/* です。次のコマンドを実行して、MySQL データ ディレクトリの権限を設定します。

- `mkdir -p /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`
- `sudo semanage fcontext -a -t mysqld_db_t "/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL(/.*)?"`
- `sudo restorecon -Rv /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`

タスク概要

- SnapCenter ServerをLinuxホストにインストールすると、MySQL、RabbitMQ、Errlangなどのサードパーティ サービスがインストールされます。これらはアンインストールしないでください。
- LinuxホストにインストールされているSnapCenter Serverは、以下をサポートしていません。
  - 高可用性
  - Windowsプラグイン
  - Active Directory（ローカル ユーザ[クレデンシャルを持つrootユーザおよびroot以外のユーザ]のみをサポート）
  - SnapCenterへのログインに使用するキーベースの認証
- .NET ランタイムのインストール中に、*libicu* ライブラリの依存関係を解決できない場合は、次のコマンドを実行して *libicu* をインストールします。 `yum install -y libicu`
- *Perl* が利用できないためにSnapCenter Server のインストールが失敗する場合は、次のコマンドを実行して *Perl* をインストールします。 `yum install -y perl`

手順

1. 以下からダウンロードしてください "NetAppサポート サイト"*/home* ディレクトリ へ。
   - SnapCenter Server インストール パッケージ - **snapcenter-linux-server-(el8/el9/sles15).bin**
   - 公開鍵ファイル - **snapcenter_public_key.pub**
   - それぞれの署名ファイル - **snapcenter-linux-server-(el8/el9/sles15).bin.sig**
2. 署名ファイルを検証します。 `$openssl dgst -sha256 -verify snapcenter_public_key.pub -signature <path to signature file> <path to bin file>`
3. 非ルート ユーザーによるインストールの場合は、.bin インストーラーに付属する **snapcenter_server_checksum_(el8/el9/sles15).txt** に指定されている visudo コンテンツを追加します。

4. .bin インストーラーの実行権限を割り当てます。 `chmod +x snapcenter-linux-server-(el8/el9/sles15).bin`
5. いずれかの操作を実行して、SnapCenter Serverをインストールします。

実行する処理	操作
対話型インストール	`./snapcenter-linux-server-(el8/el9/sles15).bin` 次の情報を入力するように求められます。 • Linuxホスト外部のSnapCenter Serverにアクセスするために使用されるWebApp外部ポート。デフォルト値は8146です。 • SnapCenter Serverをインストールするユーザ。 • パッケージがインストールされるインストールディレクトリ。

実行する処理	操作
非対話型インストール	`sudo ./snapcenter-linux-server-(el8/el9/sles15).bin -i silent -DWEBAPP_EXTERNAL_PORT=<port> -DWEBAPP_INTERNAL_PORT=<port> -DSMCORE_PORT=<port> -DSCHEDULER_PORT=<port> -DSNAPCENTER_SERVER_USER=<user> -DUSER_INSTALL_DIR=<dir> -DINSTALL_LOG_NAME=<filename>` 例: sudo ./snapcenter_linux_server.bin -i silent -DWEBAPP_EXTERNAL_PORT=8146 -DSNAPCENTER_SERVER_USER=root -DUSER_INSTALL_DIR=/opt -DINSTALL_LOG_NAME=InstallerLog.log ログは */var/opt/snapcenter/logs* に保存されます。 SnapCenter Serverをインストールするために渡されるパラメータ： • DWEBAPP_EXTERNAL_PORT: Linux ホスト外部のSnapCenter Server にアクセスするために使用される Web アプリケーション外部ポート。デフォルト値は8146です。 • DWEBAPP_INTERNAL_PORT: Linux ホスト内のSnapCenter Server にアクセスするために使用される Web アプリケーションの内部ポート。デフォルト値は8147です。 • DSMCORE_PORT: smcore サービスが実行されている SMCore ポート。デフォルト値は8145です。 • DSCHEDULER_PORT: スケジューラ サービスが実行されているスケジューラ ポート。デフォルト値は8154です。 • DSNAPCENTER_SERVER_USER: SnapCenter Server をインストールするSnapCenter Server ユーザー。*DSNAPCENTER_SERVER_USER* の場合、デフォルトはインストーラーを実行しているユーザーです。 • DUSER_INSTALL_DIR: パッケージがインストールされるインストール ディレクトリ。*DUSER_INSTALL_DIR* の場合、デフォルトのインストール ディレクトリは */opt* です。 • DINSTALL_LOG_NAME: インストール ログが保存されるログ ファイル名。これはオプションパラメータで、指定した場合はコンソールにログが表示されなくなります。このパラメータを指定しない場合は、ログがコンソールに表示され、デフォルトのログ ファイルにも保存されます。

次の手順

- *SELinux* ステータス が「有効」で、現在のモード が「強制」の場合、**nginx** サービスは起動に失敗します。次のコマンドを実行する必要があります。
  a. ホーム ディレクトリに移動します。
  b. 次のコマンドを実行します。 `journalctl -x|grep nginx`
  c. WebApp内部ポート（8147）でリッスンできない場合は、次のコマンドを実行します。
     - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
     - `semodule -i my-nginx.pp`
  d. 走る `setsebool -P httpd_can_network_connect on`

- DSELINUX: *SELinux* ステータス が「有効」で、現在のモード が「強制」であり、「開始する前に」セクションで説明したコマンドを実行した場合は、このパラメータを指定して値を 1 に割り当てる必要があります。デフォルト値は0です。
- DUPGRADE: デフォルト値は 0 です。SnapCenter Serverをアップグレードするには、このパラメータに0以外の任意の整数を指定します。

インストール中に**Linux**ホストで有効になる機能

SnapCenter Server は、ホスト システムのトラブルシューティングとメンテナンスに役立つ以下のソフトウェア パッケージをインストールします。

- Rabbitmq
- Erlang

SnapCenterを登録する

NetApp製品を初めて使用し、既存のNetAppアカウントを持っていない場合は、サポートを有効にするためにSnapCenterを登録する必要があります。

手順

1. SnapCenterをインストールした後、*ヘルプ > バージョン情報*に移動します。
2. [SnapCenter について] ダイアログ ボックスで、971 で始まる 20 桁の番号であるSnapCenterインスタンスをメモします。
3. クリック https://register.netapp.com。
4. 私は**NetApp**の登録顧客ではありません をクリックします。
5. ご自身の情報を指定して、登録します。
6. [NetApp Reference SN]フィールドは空白のままにします。
7. 製品ラインドロップダウンから* SnapCenter*を選択します。
8. 課金プロバイダを選択します。
9. 20桁のSnapCenterインスタンスIDを入力します。
10. *送信*をクリックします。

RBAC許可を使用した**SnapCenter**へのログイン

SnapCenterでは、ロールベース アクセス制御（RBAC）がサポートされています。SnapCenter管理者は、SnapCenter RBACを使用して、ロールとリソースをワークグループ / Active Directory内のユーザまたはActive Directory内のグループに割り当てま

す。RBACユーザは、割り当てられたロールを使用してSnapCenterにログインできるようになりました。

開始する前に

- Windowsサーバ マネージャでWindowsプロセス アクティブ化サービス（WAS）を有効にする必要があります。
- Internet Explorerをブラウザとして使用してSnapCenter Serverにログインする場合は、Internet Explorerの保護モードが無効になっていることを確認する必要があります。
- SnapCenter ServerがLinuxホストにインストールされている場合は、SnapCenter Serverのインストールに使用したユーザ アカウントを使用してログインする必要があります。

このタスクについて

インストール時には、SnapCenter Serverのインストール ウィザードによってショートカットが作成され、SnapCenterがインストールされているホストのデスクトップと[スタート]メニューに配置されます。また、インストールが終了すると、インストール ウィザードに、インストール時に指定した情報に基づいてSnapCenterのURLが表示されます。リモート システムからログインする場合は、このURLをコピーして使用できます。

Webブラウザで複数のタブを開いている場合は、SnapCenterのブラウザ タブだけを閉じてもSnapCenterからはログアウトされません。SnapCenterとの接続を終了するには、[サインアウト] ボタンをクリックするか、Web ブラウザ全体を閉じて、 SnapCenterからログアウトする必要があります。

ベスト プラクティス: セキュリティ上の理由から、ブラウザでSnapCenter のパスワードを保存しないようにすることをお勧めします。

デフォルトの GUI URL は、 SnapCenter Server がインストールされているサーバーのデフォルト ポート 8146 への安全な接続です (*https://server:8146*)。SnapCenterのインストール時に別のサーバ ポートを指定した場合は、そのポートが代わりに使用されます。

高可用性 (HA) 展開の場合、仮想クラスター IP *https://Virtual_Cluster_IP_or_FQDN:8146* を使用してSnapCenterにアクセスする必要があります。 Internet Explorer (IE) で *https://Virtual_Cluster_IP_or_FQDN:8146* に移動してもSnapCenter UI が表示されない場合は、各プラグインホストの IE で仮想クラスタの IP アドレスまたは FQDN を信頼済みサイトとして追加するか、各プラグインホストで IE セキュリティ強化を無効にする必要があります。詳細については、以下を参照してください。 "ネットワーク外からクラスタIPアドレスにアクセスできない" 。

SnapCenter GUIに加えて、PowerShellコマンドレットを使用してスクリプトを作成し、設定、バックアップ、リストアの各処理を実行できます。一部のコマンドレットは、SnapCenterの各リリースで変更されている場合があります。その "SnapCenterソフトウェア コマンドレット リファレンス ガイド"詳細が記載されています。

SnapCenterへの初回ログイン時は、インストール プロセスで指定したクレデンシャルを使用してログインする必要があります。

手順

1. ローカル ホストのデスクトップに表示されたショートカット、インストールの終了時に表示されたURL、またはSnapCenter管理者から受け取ったURLを使用して、SnapCenterを起動します。

2. ユーザ クレデンシャルを入力します。

指定する項目	使用する形式
ドメイン管理者	• NetBIOS\UserName • UserName@UPN suffix 例：username@netapp.com • Domain FQDN\UserName
ローカル管理者	UserName

3. 複数のロールが割り当てられている場合は、このログイン セッションで使用するロールを[ロール]ボックスから選択します。

   ログインすると、SnapCenterの右上に現在のユーザとそのロールが表示されます。

結果

[Dashboard]ページが表示されます。

サイトにアクセスできないというエラーでログ記録が失敗した場合は、SSL 証明書をSnapCenterにマップする必要があります。 "詳細情報"

終わったら

SnapCenter Serverに初めてRBACユーザとしてログインしたら、リソース リストを更新します。

SnapCenterでサポート対象にする信頼されないActive Directoryドメインがある場合は、信頼されないドメインのユーザにロールを設定する前に、それらのドメインをSnapCenterに登録する必要があります。"詳細情報"。

Linux ホスト上で実行されているSnapCenterにプラグイン ホストを追加する場合は、*/opt/NetApp/snapcenter/SnapManagerWeb/Repository* の場所からチェックサム ファイルを取得する必要があります。

6.0リリース以降では、デスクトップにSnapCenter PowerShellのショートカットが作成されます。ショートカットを使用すると、SnapCenter PowerShellコマンドレットに直接アクセスできます。

多要素認証（**MFA**）を使用した**SnapCenter**へのログイン

SnapCenter Serverは、Active Directoryに含まれているドメイン アカウントのMFAをサポートしています。

開始する前に

MFAを有効にしておく必要があります。MFAを有効にする方法については、以下を参照してください。"多要素認証を有効にする"

このタスクについて

- FQDNのみがサポートされます。

- ワークグループ ユーザとクロスドメイン ユーザは、MFAを使用したログインはできません。

手順

1. ローカル ホストのデスクトップに表示されたショートカット、インストールの終了時に表示されたURL、またはSnapCenter管理者から受け取ったURLを使用して、SnapCenterを起動します。
2. AD FSのログイン ページで、ユーザ名とパスワードを入力します。

   AD FSのページに、ユーザ名またはパスワードが無効だというエラー メッセージが表示された場合は、次の点を確認してください。

   - 有効なユーザ名とパスワードであるかどうか

     ユーザ アカウントがActive Directory（AD）に存在している必要があります。

   - ADで設定された最大試行回数を超えていないかどうか
   - ADとAD FSが稼働中かどうか

SnapCenterのデフォルトの**GUI**セッション タイムアウトの変更

SnapCenter GUIのセッション タイムアウト時間を、デフォルトのタイムアウト時間である20分から変更できます。

セキュリティ機能として、デフォルトでは、操作を行わないまま15分が経過すると、5分後にSnapCenterのGUIセッションからログアウトすることを示す警告が表示されます。また、操作を行わないまま20分が経過すると、SnapCenterのGUIセッションからログアウトされ、再度ログインが必要になります。

手順

1. 左側のナビゲーション ペインで、[設定] > [グローバル設定] をクリックします。
2. [グローバル設定]ページで、[構成設定]をクリックします。
3. [セッション タイムアウト] フィールドに新しいセッション タイムアウトを分単位で入力し、[保存] をクリックします。

SSL 3.0の無効化による**SnapCenter Web**サーバの保護

SnapCenter WebサーバでSecure Socket Layer（SSL）3.0プロトコルが有効になっている場合は、セキュリティ上の理由からMicrosoft IISで無効にする必要があります。

SSL 3.0プロトコルには欠陥があり、攻撃者が悪用して接続エラーを引き起こしたり、中間者攻撃を実行したり、Webサイトと訪問者の間の暗号化トラフィックを監視したりすることができます。

手順

1. SnapCenter Web サーバー ホストでレジストリ エディターを起動するには、[スタート] > [実行] をクリックし、「regedit」と入力します。
2. レジストリ エディタで、HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\に移動します。

- サーバー キーがすでに存在する場合:
  i. 有効な DWORD を選択し、[編集] > [変更] をクリックします。
  ii. 値を 0 に変更し、[OK] をクリックします。
- サーバーキーが存在しない場合は:
  i. 編集 > 新規 > キー をクリックし、キーに Server という名前を付けます。
  ii. 新しいサーバー キーを選択した状態で、[編集] > [新規] > [DWORD] をクリックします。
  iii. 新しいDWORDに「Enabled」という名前を付け、値として「0」を入力します。

3. レジストリ エディタを閉じます。

SnapCenterサーバーを構成する

ストレージシステムの追加とプロビジョニング

ストレージシステムを追加する

データ保護およびプロビジョニング操作を実行するには、 SnapCenter がONTAPストレージ、 ASA r2 システム、またはAmazon FSx for NetApp ONTAPにアクセスできるようにストレージ システムをセットアップする必要があります。

スタンドアロンのSVMを追加するか、複数のSVMで構成されるクラスタを追加できます。Amazon FSx for NetApp ONTAPを使用している場合は、fsxadminアカウントを使用して複数のSVMで構成されるFSx管理LIFを追加したり、SnapCenterでFSx SVMを追加したりできます。

開始する前に

- ストレージ接続を作成するには、Infrastructure Adminロールの権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

  ストレージ システム接続の追加中は、ホスト プラグインのインストールが進行中であってはなりません。ホスト キャッシュが更新されず、 SnapCenter GUI にデータベースのステータスが「バックアップに使用できません」または「 NetAppストレージ上にありません」と表示される可能性があるためです。

- ストレージ システムの名前は一意である必要があります。

  SnapCenterでは、別々のクラスタに属している場合でも、複数のストレージ システムに同じ名前を付けることはサポートされません。SnapCenterでサポートする各ストレージ システムには、一意な名前とデータLIFの一意なIPアドレスが必要です。

このタスクについて

- ストレージ システムの設定時に、イベント管理システム（EMS）とAutoSupportの機能を有効にすることもできます。AutoSupportツールは、システムの健全性に関するデータを収集し、そのデータをシステムのトラブルシューティング用にNetAppテクニカル サポートに自動的に送信します。

  これらの機能を有効にすると、リソースが保護されたとき、リストアやクローンの処理が完了したとき、または処理が失敗したときに、SnapCenterからストレージ システムにAutoSupport情報が、ストレージ システムのsyslogにEMSメッセージが送信されます。

- SnapMirrorデスティネーションまたはSnapVaultデスティネーションにSnapshotをレプリケートする場合は、デスティネーションSVM / クラスタとソースSVM / クラスタへのストレージ システム接続をセットアップする必要があります。

ストレージ システムのパスワードを変更すると、スケジュール済みジョブ、オンデマンド バックアップ、およびリストア処理が失敗する場合があります。ストレージ システムのパスワードを変更した後、[ストレージ] タブで [変更] をクリックしてパスワードを更新できます。

手順

1. 左側のナビゲーション ペインで、[ストレージ システム] をクリックします。
2. ストレージ システム ページで、[新規] をクリックします。
3. [Add Storage System]ページで、次の情報を入力します。

フィールド	操作
Storage System	ストレージ システムの名前またはIPアドレスを入力します。 ストレージ システム名（ドメイン名は含めない）は15文字以下にする必要があります。解決可能な名前を使用してください。15文字を超える名前のストレージ システム接続を作成する場合は、Add-SmStorageConnectionPowerShellコマンドレットを使用します。 MetroCluster 構成（MCC）のストレージ システムでノンストップ オペレーションを実現するには、ローカル クラスタとピア クラスタの両方を登録することを推奨します。 SnapCenterでは、別々のクラスタに属している場合でも、複数のSVMに同じ名前を付けることはサポートされません。SnapCenterでサポートするSVMには、すべて一意の名前を付ける必要があります。 SnapCenterにストレージ接続を追加したあとで、ONTAPを使用してSVMまたはクラスタの名前を変更しないでください。 SVMに短縮名またはFQDNを追加した場合は、その名前がSnapCenterとプラグイン ホストの両方から解決できる必要があります。

フィールド	操作
ユーザー名/パスワード	ストレージ システムへのアクセスに必要な権限を持つストレージ ユーザのクレデンシャルを入力します。
Event Management System (EMS) & AutoSupport Settings	保護が適用されたとき、リストア処理が完了したとき、または処理が失敗したときにEMSメッセージをストレージ システムのsyslogに送信、またはAutoSupportメッセージをストレージ システムに送信するには、該当するチェックボックスをオンにします。 失敗した操作に関する**AutoSupport**通知をストレージ システムに送信する チェックボックスをオンにすると、 AutoSupport通知を有効にするには EMS メッセージングが必要であるため、* SnapCenter Server イベントを syslog に記録する* チェックボックスもオンになります。

4. プラットフォーム、プロトコル、ポート、タイムアウトに割り当てられたデフォルト値を変更する場合は、[その他のオプション] をクリックします。

   a. [Platform]で、ドロップダウン リストから次のいずれかのオプションを選択します。

      SVM がバックアップ関係におけるセカンダリ ストレージ システムである場合は、[セカンダリ] チェックボックスをオンにします。 セカンダリ オプションを選択すると、 SnapCenter はライセンス チェックをすぐに実行しません。

   SnapCenterでSVMを追加した場合は、ドロップダウンからプラットフォーム タイプを手動で選択する必要があります。

   a. [Protocol]で、SVMまたはクラスタのセットアップ時に設定したプロトコル（通常はHTTPS）を選択します。

   b. ストレージ システムが受け入れるポートを入力します。

      通常はデフォルト ポート443を使用します。

   c. 接続を試行する時間（秒）を入力します。

      デフォルト値は60秒です。

   d. SVM に複数の管理インターフェイスがある場合は、[優先 **IP**] チェックボックスをオンにし、SVM 接続の優先 IP アドレスを入力します。

   e. *保存*をクリックします。

5. *送信*をクリックします。

結果

[ストレージ システム] ページの [タイプ] ドロップダウンから、次のいずれかのアクションを実行します。

- 追加されたすべての SVM を表示する場合は、* ONTAP SVM* を選択します。

  FSx SVMを追加した場合は、ここにFSx SVMが表示されます。

- 追加されたすべてのクラスタを表示する場合は、* ONTAPクラスタ* を選択します。

  fsxadminを使用してFSxクラスタを追加した場合は、ここにFSxクラスタが表示されます。

  クラスタ名をクリックすると、そのクラスタに含まれるすべてのSVMが[Storage Virtual Machine]セクションに表示されます。

  ONTAP GUI を使用してONTAPクラスタに新しい SVM が追加された場合は、[再検出] をクリックして新しく追加された SVM を表示します。

終わったら

SnapCenterがアクセスできるすべてのストレージ システムからEメール通知を送信するには、クラスタ管理者が各ストレージ システム ノードでAutoSupportを有効にする必要があります。ストレージ システムのコマンドラインで次のコマンドを実行してください。

```
autosupport trigger modify -node nodename -autosupport-message client.app.info
-to enable -noteto enable
```

Storage Virtual Machine（SVM）管理者にはAutoSupportへのアクセス権はありません。

ストレージ接続とクレデンシャル

データ保護処理を実行する前に、ストレージ接続をセットアップし、SnapCenter ServerとSnapCenterプラグインで使用するクレデンシャルを追加する必要があります。

ストレージ接続

SnapCenter ServerとSnapCenterプラグインは、ストレージ接続を通じてONTAPストレージにアクセスします。SVM接続を設定するには、AutoSupport機能およびイベント管理システム（EMS）機能も設定する必要があります。

Credentials

- ドメイン管理者または管理者グループの任意のメンバー

  ドメイン管理者またはSnapCenterプラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。ユーザ名フィールドの有効な形式は次のとおりです。

  - *NetBIOS*\ユーザー名
  - ドメイン*FQDN*\ユーザー名
  - ユーザー名@*upn*

- ローカル管理者（ワークグループの場合のみ）

  ワークグループに属するシステムの場合は、SnapCenterプラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザ アカウントに昇格された権限がある場合、またはホスト シス

テムでユーザ アクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカル ユーザ アカウントを指定できます。

ユーザー名フィールドの有効な形式は次のとおりです: *UserName*

- 個々のリソース グループのクレデンシャル

  個々のリソース グループのクレデンシャルを設定する場合で、ユーザ名に完全なadmin権限が割り当てられていない場合は、少なくともリソース グループとバックアップの権限を割り当てる必要があります。

Windowsホストでのストレージのプロビジョニング

igroupの作成と管理

イニシエータ グループ（igroup）を作成して、ストレージ システム上の特定のLUNにアクセスできるホストを指定することができます。SnapCenterを使用して、Windows ホスト上の igroup を作成、名前変更、変更、または削除できます。

igroupの作成

SnapCenterを使用して、Windows ホスト上に igroup を作成できます。 igroup を LUN にマップすると、ディスクの作成ウィザードまたはディスクの接続ウィザードで igroup が使用できるようになります。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、**Igroup** をクリックします。
3. イニシエーター グループ ページで、[新規] をクリックします。
4. [igroup の作成] ダイアログ ボックスで、igroup を定義します。

フィールド	操作
Storage System	igroup にマップする LUN の SVM を選択します。
ホスト	igroupを作成するホストを選択します。
グループ名	igroupの名前を入力します。
イニシエーター	イニシエータを選択します。
タイプ	イニシエータ タイプとして、iSCSI、FCP、または混在（FCPとiSCSI）のいずれかを選択します。

5. 入力内容に満足したら、「**OK**」をクリックします。

   SnapCenter はストレージ システム上に igroup を作成します。

igroupの名前の変更

SnapCenterを使用して、既存の igroup の名前を変更できます。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、**Igroup** をクリックします。
3. [イニシエータ グループ] ページで、[ストレージ仮想マシン] フィールドをクリックして使用可能な SVM のリストを表示し、名前を変更する igroup の SVM を選択します。
4. SVM の igroup のリストで、名前を変更する igroup を選択し、「名前の変更」をクリックします。
5. 「igroup の名前変更」ダイアログ ボックスで、igroup の新しい名前を入力し、「名前の変更」をクリックします。

igroupの変更

SnapCenter を使用して、既存の igroup に igroup イニシエーターを追加できます。igroupの作成時に追加できるホストは1つだけです。クラスタに対してigroupを作成するには、既存のigroupを変更して他のノードを追加します。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、**Igroup** をクリックします。
3. [イニシエータ グループ] ページで、[ストレージ仮想マシン] フィールドをクリックして使用可能な SVM のドロップダウン リストを表示し、変更する igroup の SVM を選択します。
4. igroup のリストで igroup を選択し、「**igroup** にイニシエータを追加」をクリックします。
5. ホストを選択します。
6. イニシエーターを選択し、[**OK**] をクリックします。

igroupを削除する

不要になった igroup は、 SnapCenterを使用して削除できます。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、**Igroup** をクリックします。
3. [イニシエータ グループ] ページで、[ストレージ仮想マシン] フィールドをクリックして使用可能な SVM のドロップダウン リストを表示し、削除する igroup の SVM を選択します。
4. SVM の igroup のリストで、削除する igroup を選択し、[削除] をクリックします。
5. 「igroup の削除」ダイアログボックスで、「**OK**」をクリックします。

   SnapCenter はigroup を削除します。

Windowsホストは、ストレージ システム上のLUNを仮想ディスクとして認識します。SnapCenterを使用して、FC接続LUNまたはiSCSI接続LUNを作成および設定できます。

- SnapCenterでサポートされるのは、ベーシック ディスクのみです。ダイナミック ディスクはサポートされていません。
- GPTでは1つのデータ パーティションのみ、MBRではNTFSまたはCSVFSでフォーマットされた1つのボリュームと1つのマウント パスを持つ1つのプライマリ パーティションのみを含めることができます。
- サポートされているパーティション スタイル: GPT、MBR。VMware UEFI VM では、iSCSI ディスクのみがサポートされます。

SnapCenterでは、ディスクの名前を変更することはできません。SnapCenterで管理しているディスクの名前が変更された場合、SnapCenterの処理は正常に実行されません。

ホスト上のディスクの表示

SnapCenterで管理している各Windowsホスト上のディスクを表示できます。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[ディスク] をクリックします。
3. *ホスト*ドロップダウンリストからホストを選択します。

   ディスクのリストが表示されます。

クラスタ ディスクの表示

SnapCenterで管理しているクラスタ上のクラスタ ディスクを表示できます。クラスタ ディスクは、[Hosts]ドロップダウンからクラスタを選択した場合にのみ表示されます。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[ディスク] をクリックします。
3. ホスト ドロップダウン リストからクラスターを選択します。

   ディスクのリストが表示されます。

iSCSIセッションの確立

iSCSIを使用してLUNに接続する場合は、LUNを作成して通信を有効にする前に、iSCSIセッションを確立する必要があります。

始める前に

- ストレージ システムのノードをiSCSIターゲットとして定義しておく必要があります。
- ストレージ システムで iSCSI サービスを開始する必要があります。 "詳細情報"

このタスクについて

iSCSIセッションは、同じバージョンのIP間（IPv6とIPv6またはIPv4とIPv4）でのみ確立できます。

リンクローカルIPv6アドレスは、iSCSIセッションの管理や、ホストとターゲットの間の通信（ホストとターゲットが両方とも同じサブネット内に存在する場合）に使用できます。

iSCSIイニシエータの名前を変更すると、iSCSIターゲットへのアクセスに影響します。名前を変更した場合、新しい名前が認識されるように、イニシエータがアクセスするターゲットの再設定が必要になることがあります。iSCSIイニシエータの名前を変更した場合、ホストを必ず再起動してください。

ホストに複数の iSCSI インターフェイスがある場合、最初のインターフェイスの IP アドレスを使用してSnapCenterへの iSCSI セッションを確立すると、別の IP アドレスを持つ別のインターフェイスから iSCSI セッションを確立することはできません。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[iSCSI セッション] をクリックします。
3. ストレージ仮想マシン ドロップダウン リストから、iSCSI ターゲットのストレージ仮想マシン (SVM) を選択します。
4. *ホスト*ドロップダウンリストから、セッションのホストを選択します。
5. *セッションの確立*をクリックします。

   セッションの確立ウィザードが表示されます。

6. セッションの確立ウィザードで、ターゲットを特定します。

フィールド	入力する内容
ターゲットノード名	iSCSIターゲットのノード名 既存のターゲット ノードがある場合、表示されるノード名は変更できません。
ターゲットポータルアドレス	ターゲット ネットワーク ポータルのIPアドレス
ターゲットポータルポート	ターゲット ネットワーク ポータルのTCPポート
イニシエーターポータルアドレス	イニシエータ ネットワーク ポータルのIPアドレス

7. 入力内容に満足したら、「接続」をクリックします。

   SnapCenter はiSCSI セッションを確立します。

8. 同じ手順を繰り返して各ターゲットのセッションを確立します。

FC接続または**iSCSI**接続の**LUN**またはディスクの作成

Windowsホストは、ストレージ システム上のLUNを仮想ディスクとして認識します。SnapCenterを使用して、FC接続LUNまたはiSCSI接続LUNを作成および設定できます。

SnapCenterの外部でディスクを作成してフォーマットする場合は、NTFSファイルシステムとCSVFSファイルシステムのみがサポートされます。

開始する前に

- ストレージ システム上にLUN用のボリュームを作成しておく必要があります。

  このボリュームには、SnapCenterで作成したLUNのみを格納します。

  SnapCenterで作成したクローン ボリュームには、クローンがすでにスプリットされている場合を除き、LUNを作成することはできません。

- ストレージ システムでFCサービスまたはiSCSIサービスを開始しておく必要があります。
- iSCSIを使用している場合は、ストレージ システムとのiSCSIセッションを確立しておく必要があります。
- SnapCenter Plug-ins Package for Windowsをインストールする必要があるのは、ディスクを作成するホストだけです。

このタスクについて

- Windows Serverフェイルオーバー クラスタ内のホストで共有する場合を除き、LUNを複数のホストに接続することはできません。
- Cluster Shared Volume（CSV;クラスタ共有ボリューム）を使用したWindows Serverフェイルオーバー クラスタ内のホストでLUNを共有する場合、クラスタ グループを所有するホストにディスクを作成する必要があります。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[ディスク] をクリックします。
3. *ホスト*ドロップダウンリストからホストを選択します。
4. *新規*をクリックします。

   [Create Disk]ウィザードが開きます。

5. [LUN Name]ページで、LUNの情報を指定します。

フィールド	操作
Storage System	LUNのSVMを選択します。

フィールド	操作
LUN path	参照 をクリックして、LUN を含むフォルダーの完全なパスを選択します。
LUN名	LUNの名前を入力します。
Cluster size	クラスタのLUNのブロック割り当てサイズを選択します。 クラスタのサイズは、オペレーティング システムおよびアプリケーションによって異なります。
LUN label	必要に応じて、LUNの説明を入力します。

6. [Disk Type]ページで、ディスク タイプを選択します。

選択するオプション	状況
Dedicated disk	LUNにアクセスできるホストは1つだけです。 リソース グループ フィールドは無視します。
共有ディスク	Windows Serverフェイルオーバー クラスタ内のホストでLUNを共有します。 リソース グループ フィールドにクラスター リソース グループの名前を入力します。ディスクはフェイルオーバー クラスタ内の1つのホストだけに作成します。
Cluster Shared Volume (CSV)	CSVを使用するWindows Serverフェイルオーバー クラスタ内のホストでLUNを共有します。 リソース グループ フィールドにクラスター リソース グループの名前を入力します。ディスクはクラスタ グループを所有するホストに作成する必要があります。

7. [Drive Properties]ページで、ドライブのプロパティを指定します。

プロパティ	説明
マウントポイントの自動割り当て	システム ドライブに基づいて、SnapCenterで自動的にボリューム マウント ポイントを割り当てます。 たとえば、システム ドライブがC:であれば、C:ドライブにボリューム マウント ポイント（C:\scmnpt\）が作成されます。自動割り当ては共有ディスクではサポートされません。
Assign drive letter	ドロップダウン リストで選択したドライブにディスクをマウントします。
Use volume mount point	フィールドで指定したドライブ パスにディスクをマウントします。 ボリューム マウント ポイントのルートは、ディスクを作成するホストが所有している必要があります。
Do not assign drive letter or volume mount point	ディスクをWindowsで手動でマウントする場合に選択します。
LUN size	LUNサイズ（150MB以上）を指定します。 ドロップダウン リストで単位（MB、GB、またはTB）を選択します。
Use thin provisioning for the volume hosting this LUN	LUNをシンプロビジョニングします。 シンプロビジョニングでは、ストレージ スペースが必要なときに必要な分だけ割り当てられるため、LUNは使用可能な最大容量まで効率的に拡張されます。 必要になるすべてのLUNストレージに対応できるだけの十分なスペースがボリュームにあることを確認してください。

プロパティ	説明
Choose partition type	GUIDパーティション テーブルの場合はGPTパーティション、マスター ブート レコードの場合はMBRパーティションを選択します。 MBRパーティションをWindows Serverフェイルオーバー クラスタで使用した場合、ミスアライメントが発生することがあります。 Unified Extensible Firmware Interface（UEFI）パーティション ディスクはサポートされていません。

8. [Map LUN]ページで、ホストのiSCSIイニシエータまたはFCイニシエータを選択します。

フィールド	操作
ホスト	クラスタ グループ名をダブルクリックし、ドロップダウン リストに表示されたクラスタに属するホストの中から、イニシエータに指定するホストを選択します。 このフィールドは、Windows Serverフェイルオーバー クラスタ内のホストでLUNを共有する場合にのみ表示されます。
Choose host initiator	ファイバー チャネル または **iSCSI** を選択し、ホスト上のイニシエーターを選択します。 FCでマルチパスI/O（MPIO）を使用する場合は、FCイニシエータを複数選択できます。

9. [Group Type]ページで、既存のigroupをLUNにマッピングするか新しいigroupを作成するかを指定します。

選択するオプション	状況
選択したイニシエータの新しい igroup を作成する	選択したイニシエータ用に新しいigroupを作成します。
Choose an existing igroup or specify a new igroup for selected initiators	選択したイニシエータ用に既存のigroupを指定するか、指定した名前で新しいigroupを作成します。 **igroup** 名 フィールドに igroup 名を入力します。既存のigroup名の最初の数文字を入力すると、残りの文字が自動的に入力されます。

10. 概要ページで選択内容を確認し、「完了」をクリックします。

SnapCenterにより、LUNが作成され、ホスト上の指定したドライブまたはドライブ パスに接続されま

す。

ディスクのサイズ変更

ストレージ システムのニーズの変化に応じて、ディスクのサイズを拡張または縮小することができます。

このタスクについて

- シンプロビジョニングLUNの場合、ONTAP LUNのジオメトリのサイズが最大サイズとして表示されます。
- シックプロビジョニングLUNの場合、拡張可能なサイズ（ボリューム内の使用可能なサイズ）が最大サイズとして表示されます。
- MBRパーティション方式を使用したLUNの場合、最大サイズは2TBです。
- GPTパーティション方式を使用したLUNの場合、ストレージ システムの最大サイズは16TBです。
- LUNのサイズを変更する前にSnapshotを作成しておくことを推奨します。
- LUNのサイズの変更前に作成されたSnapshotからLUNをリストアすると、SnapCenterによってLUNのサイズがSnapshotのサイズに自動的に変更されます。

  リストア処理のあと、サイズ変更後にLUNに追加されたデータを、サイズ変更後に作成されたSnapshotからリストアする必要があります。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[ディスク] をクリックします。
3. [Host]ドロップダウン リストからホストを選択します。

   ディスクのリストが表示されます。

4. サイズを変更するディスクを選択し、「サイズ変更」をクリックします。
5. [Resize Disk]ダイアログ ボックスで、スライダ ツールを使用してディスクの新しいサイズを指定するか、[Size]フィールドに新しいサイズを入力します。

   サイズを手動で入力した場合は、入力後に[Size]フィールド以外の部分をクリックすると、[Shrink]ボタンまたは[Expand]ボタンが有効になります。また、[MB]、[GB]、または[TB]のいずれかをクリックして単位を指定する必要があります。

6. 入力内容に問題がなければ、必要に応じて 縮小 または 拡大 をクリックします。

   SnapCenterによって、ディスクのサイズが変更されます。

ディスクの接続

[Connect Disk]ウィザードを使用して、既存のLUNをホストに接続したり、切断されたLUNを再接続したりできます。

開始する前に

- ストレージ システムでFCサービスまたはiSCSIサービスを開始しておく必要があります。
- iSCSIを使用している場合は、ストレージ システムとのiSCSIセッションを確立しておく必要があります。
- Windows Serverフェイルオーバー クラスタ内のホストで共有する場合を除き、LUNを複数のホストに接続することはできません。
- クラスタ共有ボリューム（CSV）を使用するWindows Serverフェイルオーバー クラスタ内のホスト間でLUNを共有する場合、クラスタ グループを所有するホストにディスクを接続する必要があります。
- Plug-in for Windowsをインストールする必要があるのは、ディスクを接続するホストだけです。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[ディスク] をクリックします。
3. *ホスト*ドロップダウンリストからホストを選択します。
4. *接続*をクリックします。

   [Connect Disk]ウィザードが開きます。

5. [LUN Name]ページで、接続するLUNの情報を指定します。

フィールド	操作
Storage System	LUNのSVMを選択します。
LUN path	参照 をクリックして、LUN を含むボリュームの完全なパスを選択します。
LUN名	LUNの名前を入力します。
Cluster size	クラスタのLUNのブロック割り当てサイズを選択します。 クラスタのサイズは、オペレーティング システムおよびアプリケーションによって異なります。
LUN label	必要に応じて、LUNの説明を入力します。

6. [Disk Type]ページで、ディスク タイプを選択します。

選択するオプション	状況
Dedicated disk	LUNにアクセスできるホストは1つだけです。

選択するオプション	状況
共有ディスク	Windows Serverフェイルオーバー クラスタ内のホストでLUNを共有します。 ディスクはフェイルオーバー クラスタ内の1つのホストだけに接続します。
Cluster Shared Volume (CSV)	CSVを使用するWindows Serverフェイルオーバー クラスタ内のホストでLUNを共有します。 ディスクはクラスタ グループを所有するホストに接続する必要があります。

7. [Drive Properties]ページで、ドライブのプロパティを指定します。

プロパティ	説明
自動割り当て	システム ドライブに基づいて、SnapCenterで自動的にボリューム マウント ポイントを割り当てます。 たとえば、システム ドライブがC:であれば、C:ドライブにボリューム マウント ポイント（C:\scmnpt\）が作成されます。自動割り当ては共有ディスクではサポートされません。
Assign drive letter	ドロップダウン リストで選択したドライブにディスクをマウントします。
Use volume mount point	フィールドで指定したドライブ パスにディスクをマウントします。 ボリューム マウント ポイントのルートは、ディスクを作成するホストが所有している必要があります。
Do not assign drive letter or volume mount point	ディスクをWindowsで手動でマウントする場合に選択します。

8. [Map LUN]ページで、ホストのiSCSIイニシエータまたはFCイニシエータを選択します。

フィールド	操作
ホスト	クラスタ グループ名をダブルクリックし、ドロップダウン リストに表示されたクラスタに属するホストの中から、イニシエータに指定するホストを選択します。 このフィールドは、Windows Serverフェイルオーバー クラスタ内のホストでLUNを共有する場合にのみ表示されます。
Choose host initiator	ファイバー チャネル または **iSCSI** を選択し、ホスト上のイニシエーターを選択します。 FCでMPIOを使用している場合は、FCイニシエータを複数選択できます。

9. [Group Type]ページで、既存のigroupをLUNにマッピングするか新しいigroupを作成するかを指定します。

選択するオプション	状況
選択したイニシエータの新しい igroup を作成する	選択したイニシエータ用に新しいigroupを作成します。
Choose an existing igroup or specify a new igroup for selected initiators	選択したイニシエータ用に既存のigroupを指定するか、指定した名前で新しいigroupを作成します。 **igroup** 名 フィールドに igroup 名を入力します。既存のigroup名の最初の数文字を入力すると、残りの文字が自動的に入力されます。

10. 概要ページで選択内容を確認し、「完了」をクリックします。

    SnapCenterにより、ホスト上の指定したドライブまたはドライブ パスにLUNが接続されます。

ディスクの切断

LUN の内容に影響を与えずにホストから LUN を切断できますが、1 つの例外があります: クローンを分割する前に切断すると、クローンの内容が失われます。

開始する前に

- LUNを使用しているアプリケーションがないことを確認します。
- LUNが監視ソフトウェアで監視されていないことを確認します。
- LUNが共有されている場合は、LUNからクラスタ リソースの依存関係を解除し、クラスタ内のすべてのノードの電源がオンで正常に動作しており、SnapCenterからアクセスできることを確認します。

このタスクについて

SnapCenterで作成したFlexCloneボリュームのLUNを切断した場合、そのボリュームに他のLUNが接続されて

いなければSnapCenterはボリュームも削除します。この場合、LUNが切断される前に、FlexCloneボリュームが削除される可能性があることを警告するメッセージがSnapCenterに表示されます。

FlexCloneボリュームが自動で削除されないようにするには、最後のLUNを切断する前にボリュームの名前を変更します。ボリュームの名前を変更する際は、最後の1文字だけでなく複数の文字を変更してください。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[ディスク] をクリックします。
3. *ホスト*ドロップダウンリストからホストを選択します。

   ディスクのリストが表示されます。
4. 切断するディスクを選択し、「切断」をクリックします。
5. [ディスクの切断] ダイアログ ボックスで、[**OK**] をクリックします。

   SnapCenterによってディスクが切断されます。

ディスクの削除

不要になったディスクは削除できます。削除したディスクは復元できません。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[ディスク] をクリックします。
3. *ホスト*ドロップダウンリストからホストを選択します。

   ディスクのリストが表示されます。
4. 削除するディスクを選択し、「削除」をクリックします。
5. [ディスクの削除] ダイアログボックスで、[**OK**] をクリックします。

   SnapCenterによってディスクが削除されます。

SMB共有の作成と管理

Storage Virtual Machine（SVM）上にSMB3共有を設定するには、SnapCenterユーザ インターフェイスまたはPowerShellコマンドレットを使用できます。

ベスト プラクティス: コマンドレットを使用すると、 SnapCenterに用意されているテンプレートを利用して共有構成を自動化できるため、コマンドレットの使用をお勧めします。

テンプレートには、ボリュームおよび共有の設定に関するベストプラクティスが組み込まれています。テンプレートは、SnapCenter Plug-ins Package for Windowsのインストール フォルダのTemplatesフォルダにあります。

必要に応じて、提供されるモデルに従って独自のテンプレートを作成することもできます。カスタム テンプレートを作成する場合は、コマンドレットのドキュメントでパラメータを確認してください。

SMB共有を作成する

SnapCenterの[Shares]ページを使用して、Storage Virtual Machine（SVM）にSMB3共有を作成できます。

SnapCenterを使用して SMB 共有上のデータベースをバックアップすることはできません。SMBでサポートされるのはプロビジョニングのみです。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[共有] をクリックします。
3. *ストレージ仮想マシン*ドロップダウンリストから SVM を選択します。
4. *新規*をクリックします。

   [新しい共有] ダイアログが開きます。

5. [新しい共有] ダイアログで、共有を定義します。

フィールド	操作
説明	共有の説明を入力します。
シェア名	共有の名前を入力します（例：test_share）。 ここで入力した共有の名前はボリューム名としても使用されます。 共有名には次のルールが適用されます。 • UTF-8文字列である必要があります。 • 以下の文字を含めることはできません: 0x00から0x1Fまでの制御文字(両端を含む)、0x22(二重引用符)、および特殊文字 `\ / [ ] : (vertical bar) < > + = ; , ?`
パスを共有	• フィールドをクリックして、新しいファイル システム パス (例: /) を入力します。 • フィールドをダブルクリックし、既存のファイル システム パスのリストから選択します。

6. 入力内容に満足したら、「**OK**」をクリックします。

   SnapCenter はSVM 上に SMB 共有を作成します。

SMB共有を削除する

不要になったSMB共有は削除できます。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[共有] をクリックします。
3. [共有] ページで、[ストレージ仮想マシン] フィールドをクリックして、使用可能なストレージ仮想マシン (SVM) のリストを含むドロップダウンを表示し、削除する共有の SVM を選択します。
4. SVM 上の共有リストから、削除する共有を選択し、[削除] をクリックします。
5. [共有の削除] ダイアログボックスで、[**OK**] をクリックします。

   SnapCenter はSVM から SMB 共有を削除します。

ストレージ システムでのスペースの再生

ファイルが削除または変更された場合、NTFSはLUN上の使用可能なスペースを追跡しますが、この情報はストレージ システムには報告されません。新たに解放されたブロックがストレージで空きスペースとしてマークされるようにするには、Plug-in for Windows ホストでスペース再生用のPowerShellコマンドレットを実行します。

リモートのプラグイン ホストでコマンドレットを実行する場合は、SnapCenterOpen-SMConnectionコマンドレットを実行してSnapCenter Serverへの接続を確立する必要があります。

開始する前に

- リストア処理を実行する前に必ずスペース再生プロセスを完了しておく必要があります。
- Windows Serverフェイルオーバー クラスタ内のホストでLUNを共有している場合は、クラスタ グループを所有するホストでスペース再生を実行する必要があります。
- ストレージのパフォーマンスを最適化するには、できるだけ頻繁にスペース再生を実行します。

  NTFSファイルシステム全体がスキャンされたことを確認してください。

このタスクについて

- スペース再生には時間がかかり、CPUを大量に消費するため、通常はストレージ システムとWindowsホストがあまり使用されていない時間帯に実行することを推奨します。
- 使用可能なほぼすべてのスペースが再生されますが、100%ではありません。
- スペース再生の実行中にディスクのデフラグは実行しないでください。

  再生プロセスの実行速度が低下する可能性があります。

ステップ

アプリケーション サーバのコマンド プロンプトで、次のPowerShellコマンドを入力します。

```
Invoke-SdHostVolumeSpaceReclaim -Path drive_path
```

drive_pathは、LUNにマッピングされているドライブのパスです。

PowerShellコマンドレットを使用したストレージのプロビジョニング

SnapCenter GUI を使用してホストのプロビジョニングおよびスペース再利用ジョブを実行しない場合、PowerShell コマンドレットを使用できます。コマンドレットは直接使用できるほか、スクリプトに追加することもできます。

リモートのプラグイン ホストでコマンドレットを実行する場合は、SnapCenterのOpen-SMConnectionコマンドレットを実行してSnapCenter Serverへの接続を確立する必要があります。

コマンドレットで使用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、 "SnapCenterソフトウェア コマンドレット リファレンス ガイド" 。

SnapDrive for Windowsをサーバーから削除したためにSnapCenter PowerShellコマンドレットが機能しなくなった場合は、 "SnapDrive for Windows をアンインストールするとSnapCenterコマンドレットが壊れる" 。

VMware環境でのストレージのプロビジョニング

SnapCenter Plug-in for Microsoft Windowsは、VMware環境でのLUNの作成と管理やSnapshotの管理に使用できます。

サポートされるVMwareゲストOSプラットフォーム

- サポート対象バージョンのWindows Server
- Microsoftクラスタ構成

  VMware上でサポートされるノードは、Microsoft iSCSI Software Initiatorを使用する場合は最大16、FCを使用する場合は最大2つです。

- RDM LUN

  通常のRDMSでは、最大56のRDM LUNと4つのLSI Logic SCSIコントローラがサポートされます。VMware VM MSCSのボックスツーボックスのPlug-in for Windows構成では、最大42のRDM LUNと3つのLSI Logic SCSIコントローラがサポートされます。

  VMware ParaVirtual SCSIコントローラがサポートされます。RDMディスクでは、256台のディスクがサポートされます。

サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool" 。

VMware ESXiサーバ関連の制限事項

- 仮想マシンで構成されたMicrosoftクラスタにPlug-in for Windowsをインストールする場合、ESXiクレデンシャルは使用できません。

  クラスタ化された仮想マシンにPlug-in for Windowsをインストールする場合、vCenterのクレデンシャルを使用する必要があります。

- クラスタ化されたすべてのノードで、同じクラスタ ディスクには同じ（仮想SCSIアダプタ上の）ターゲットIDを使用する必要があります。
- Plug-in for Windowsを使用せずにRDM LUNを作成した場合、プラグイン サービスを再起動し、作成したディスクを認識させる必要があります。
- VMwareゲストOSでiSCSIイニシエータとFCイニシエータを同時に使用することはできません。

SnapCenterのRDMの処理に必要な最小限のvCenter権限

ゲストOSでRDM処理を実行するには、ホストに対する次のvCenter権限が必要です。

- データストア: ファイルの削除
- ホスト: 構成 > ストレージパーティション構成
- 仮想マシン: 構成

これらの権限を、仮想センター サーバ レベルのロールに割り当てる必要があります。これらの権限を割り当てたロールをroot権限を持たないユーザに割り当てることはできません。

これらの権限を割り当てたら、ゲストOSにPlug-in for Windowsをインストールできます。

Microsoftクラスタの FC RDM LUNの管理

Plug-in for Windowsを使用して、FC RDM LUNを使用するMicrosoftクラスタを管理するには、プラグインの外部で共有RDMクォーラムと共有ストレージを作成し、クラスタ内の仮想マシンにディスクを追加しておく必要があります。

ESXi 5.5以降、ESXのiSCSIハードウェアやFCoEハードウェアを使用したMicrosoftクラスタの管理も可能となりました。Plug-in for Windowsでは、設定作業なしでMicrosoftクラスタがサポートされます。

要件

Plug-in for Windowsでは、一定の構成要件を満たしていれば、2つの異なるESXまたはESXiサーバに属する2台の仮想マシン上のFC RDM LUNを使用したMicrosoftクラスタ（筐体間クラスタ）がサポートされます。

- 各仮想マシン（VM）が同じバージョンのWindows Serverを実行している必要があります。
- 各VMware親ホストのESX / ESXiサーバのバージョンが同じである必要があります。
- 各親ホストに少なくとも2つのネットワーク アダプタが必要です。
- 2台のESX / ESXiサーバ間でVMware Virtual Machine File System（VMFS）データストアを少なくとも1つ共有している必要があります。
- VMwareでは、共有データストアをFC SANで作成することを推奨しています。

  共有データストアは、必要に応じてiSCSIで作成することもできます。

- 共有RDM LUNが物理互換モードである必要があります。
- 共有RDM LUNは、Plug-in for Windowsの外部で手動で作成する必要があります。

  共有ストレージに仮想ディスクを使用することはできません。

- クラスタ内の各仮想マシンに、SCSIコントローラが物理互換モードで構成されている必要があります。

Windows Server 2008 R2の場合、各仮想マシンにLSI Logic SAS SCSIコントローラを構成する必要があります。LSI Logic SASタイプのコントローラが1台しかなく、すでにC:ドライブに接続されている場合、そのコントローラを共有LUNで使用することはできません。

準仮想化タイプのSCSIコントローラはVMware Microsoftクラスタではサポートされていません。

物理互換モードの仮想マシン上の共有 LUN に SCSI コントローラを追加する場合は、VMware Infrastructure Client で 新しいディスクの作成 オプションではなく、**Raw** デバイス マッピング (RDM) オプションを選択する必要があります。

- Microsoft仮想マシン クラスタをVMwareクラスタに含めることはできません。
- Microsoftクラスタに属する仮想マシンにPlug-in for Windowsをインストールする場合は、ESXまたはESXiのクレデンシャルではなくvCenterのクレデンシャルを使用する必要があります。
- Plug-in for Windowsでは、複数のホストのイニシエータを含むigroupを作成することはできません。

  共有クラスタ ディスクとして使用するRDM LUNを作成する前に、すべてのESXiホストのイニシエータを含むigroupをストレージ コントローラ上に作成しておく必要があります。

- ESXi 5.0では、FCイニシエータを使用してRDM LUNを作成します。

  RDM LUNを作成すると、ALUAでイニシエータ グループが作成されます。

制限事項

Plug-in for Windowsでは、異なるESXサーバまたはESXiサーバに属する異なる仮想マシン上のFC / iSCSI RDM LUNを使用するMicrosoftクラスタがサポートされます。

この機能は、ESX 5.5iよりも前のリリースではサポートされていません。

- Plug-in for Windowsでは、ESX iSCSIおよびNFSデータストア上のクラスタはサポートされません。
- Plug-in for Windowsでは、クラスタ環境でのイニシエータの混在はサポートされません。

  イニシエータはFCとMicrosoft iSCSIのどちらか一方にする必要があります。

- ESX iSCSIイニシエータとHBAはMicrosoftクラスタ内の共有ディスクではサポートされません。
- Plug-in for Windowsでは、Microsoftクラスタに属する仮想マシンのvMotionによる移行はサポートされません。
- Plug-in for Windowsでは、Microsoftクラスタ内の仮想マシンでのMPIOはサポートされません。

共有**FC RDM LUN**の作成

FC RDM LUNを使用してMicrosoftクラスタ内のノード間でストレージを共有する場合、事前に共有クォーラム ディスクと共有ストレージ ディスクを作成し、それらをクラスタ内の両方の仮想マシンに追加しておく必要があります。

共有ディスクの作成にPlug-in for Windowsは使用しません。共有LUNを作成し、クラスタ内の各仮想マシンに追加する必要があります。詳細については、 "物理ホスト間で仮想マシンをクラスタ化する" 。

SnapCenter Standardコントローラベース ライセンスの追加

FAS、 AFF、またはASAストレージ コントローラを使用している場合は、 SnapCenter Standard コントローラ ベースのライセンスが必要です。

コントローラベース ライセンスには次のような特徴があります。

- SnapCenter Standardライセンスは、Premium BundleまたはFlash Bundleに含まれています（Base Packには含まれていません）。
- ストレージ容量に制限はありません。
- ONTAP System Manager またはONTAP CLI を使用して、 FAS、 AFF、またはASAストレージ コントローラに直接追加されます。

> SnapCenterコントローラベースのライセンスについては、 SnapCenterユーザー インターフェイスにライセンス情報を入力しません。

- コントローラのシリアル番号に紐付けられます。

必要なライセンスについては、以下を参照してください。"SnapCenterのライセンス" 。

ステップ**1: SnapManager Suite**ライセンスがインストールされているかどうかを確認する

SnapCenterユーザー インターフェイスを使用して、 SnapManager Suite ライセンスがFAS、 AFF、またはASAプライマリ ストレージ システムにインストールされているかどうかを確認し、ライセンスが必要なシステムを特定できます。SnapManager Suiteライセンスは、プライマリ ストレージ システム上のFAS、AFF、およびASA SVM / クラスタにのみ適用されます。

> コントローラにすでにSnapManager Suite ライセンスがある場合、 SnapCenter は標準コントローラベースのライセンス権限を自動的に提供します。SnapManager Suiteライセンスとの SnapCenter Standardコントローラベース ライセンスは同じライセンスを表しています。

手順

1. 左側のナビゲーション ペインで、*ストレージ システム*を選択します。
2. [ストレージ システム] ページの [タイプ] ドロップダウンから、追加されたすべての SVM またはクラスターを表示するかどうかを選択します。
   - 追加されたすべての SVM を表示するには、* ONTAP SVM* を選択します。
   - 追加されたすべてのクラスターを表示するには、* ONTAPクラスター* を選択します。

     クラスタ名を選択すると、そのクラスタに含まれるすべてのSVMが[Storage Virtual Machine]セクションに表示されます。
3. [ストレージ接続]リストの[コントローラ ライセンス]列を確認します。

   [Controller License]列には、次のステータスが表示されます。

   - ✔ SnapManager Suite ライセンスがFAS、 AFF、またはASAプライマリ ストレージ システムにインストールされていることを示します。

-  SnapManager Suite ライセンスがFAS、 AFF、またはASAプライマリ ストレージ システムにインストールされていないことを示します。
- [Not Applicable]は、ストレージ コントローラがAmazon FSx for NetApp ONTAP、Cloud Volumes ONTAP、ONTAP Select、またはセカンダリ ストレージ プラットフォーム上にあるため、SnapManager Suiteライセンスが適用されないことを示します。

ステップ**2:** コントローラにインストールされているライセンスを識別する

ONTAPコマンドラインを使用して、コントローラにインストールされているすべてのライセンスを表示できます。FAS、AFF、またはASAシステムのクラスタ管理者である必要があります。

コントローラには、 SnapCenter Standard コントローラ ベースのライセンスが SnapManagerSuite ライセンスとして表示されます。

手順

1. ONTAPコマンドラインを使用してNetAppコントローラにログインします。
2. license show コマンドを入力し、出力を表示して SnapManagerSuite ライセンスがインストールされているかどうかを確認します。

出力例

```
cluster1::> license show
(system license show)

Serial Number: 1-80-0000xx
Owner: cluster1
Package           Type     Description              Expiration
----------------- -------- ---------------------    ---------------
Base              site     Cluster Base License     -

Serial Number: 1-81-00000000000000000000000xx
Owner: cluster1-01
Package           Type     Description              Expiration
----------------- -------- ---------------------    ---------------
NFS               license  NFS License              -
CIFS              license  CIFS License             -
iSCSI             license  iSCSI License            -
FCP               license  FCP License              -
SnapRestore       license  SnapRestore License      -
SnapMirror        license  SnapMirror License       -
FlexClone         license  FlexClone License        -
SnapVault         license  SnapVault License        -
SnapManagerSuite  license  SnapManagerSuite License -
```

この例では、SnapManager Suiteライセンスがインストールされているため、SnapCenterライセンスを設定する必要はありません。

ステップ**3:** コントローラーのシリアル番号を取得する

ONTAPコマンドラインを使用してコントローラのシリアル番号を取得します。コントローラベースのライセンスのシリアル番号を取得するには、 FAS、 AFF、またはASAシステムのクラスタ管理者である必要があります。

手順

1. ONTAPコマンドラインを使用してコントローラにログインします。
2. system show -instanceコマンドを入力し、その出力でコントローラのシリアル番号を確認します。

出力例

```
cluster1::> system show -instance

Node: fasxxxx-xx-xx-xx
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234511
Asset Tag: -
Uptime: 143 days 23:46
NVRAM System ID: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false

Node: fas8080-41-42-02
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234512
Asset Tag: -
Uptime: 144 days 00:08
NVRAM System ID: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false
2 entries were displayed.
```

3. シリアル番号をメモします。

ステップ**4:** コントローラベースのライセンスのシリアル番号を取得する

FAS、 ASA、またはAFFストレージを使用している場合は、 ONTAPコマンドラインを使用してインストールする前に、 NetAppサポート サイトからSnapCenterコントローラベースのライセンスを取得できます。

開始する前に

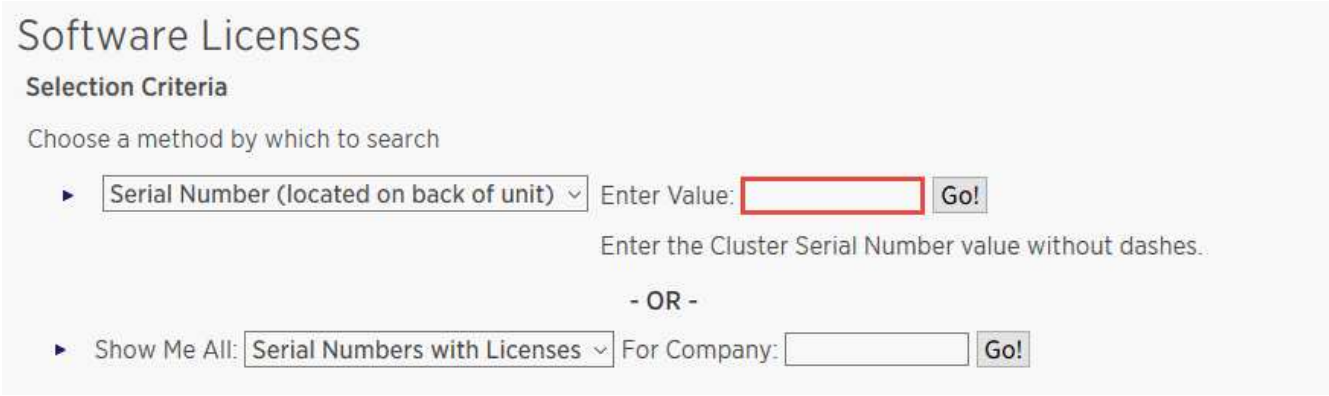
- NetAppサポート サイトの有効なログイン クレデンシャルが必要です。

有効な資格情報を入力しない場合は、検索に対して情報が返されません。

- コントローラのシリアル番号が必要です。

手順

1. ログイン "NetAppサポート サイト"。
2. システム > ソフトウェア ライセンス に移動します。
3. [選択基準] 領域で、[シリアル番号] (ユニットの背面にあります) が選択されていることを確認し、コントローラーのシリアル番号を入力して、[Go!] を選択します。



指定したコントローラのライセンスのリストが表示されます。

4. SnapCenter StandardまたはSnapManager Suiteのライセンスをメモします。

ステップ**5:** コントローラベースのライセンスを追加する

FAS、AFF、またはASAシステムを使用していて、SnapCenter StandardまたはSnapManager Suiteのライセンスがある場合は、ONTAPコマンドラインを使用してSnapCenterコントローラベース ライセンスを追加できます。

開始する前に

- FAS、AFF、またはASAシステムのクラスタ管理者である必要があります。
- SnapCenter StandardまたはSnapManager Suiteのライセンスが必要です。

タスク概要

FAS、AFF、またはASAストレージにSnapCenterの試用版をインストールしたい場合は、Premium Bundleの評価版ライセンスを入手してコントローラにインストールできます。

SnapCenterの試用版をインストールする場合は、営業担当者からPremium Bundleの評価版ライセンスを入手してコントローラにインストールする必要があります。

手順

1. ONTAPコマンドラインを使用してNetAppクラスタにログインします。
2. SnapManager Suiteライセンス キーを追加します。

```
system license add -license-code license_key
```

このコマンドは、admin権限レベルで使用できます。

3. SnapManager Suiteライセンスがインストールされたことを確認します。

```
license show
```

ステップ**6:** 試用ライセンスを削除する

コントローラベースのSnapCenter Standard ライセンスを使用しており、容量ベースの試用ライセンス (シリアル番号が「50」で終わる) を削除する必要がある場合は、MySQL コマンドを使用して試用ライセンスを手動で削除する必要があります。試用ライセンスは、 SnapCenterユーザー インターフェイスを使用して削除することはできません。

試用版ライセンスを手動で削除する必要があるのは、SnapCenter Standardコントローラベース ライセンスを使用している場合のみです。

手順

1. SnapCenter Serverで、PowerShellウィンドウを開いてMySQLパスワードをリセットします。
   a. Open-SmConnection コマンドレットを実行して、SnapCenterAdmin アカウントのSnapCenter Server との接続を確立します。
   b. Set-SmRepositoryPasswordを実行してMySQLパスワードをリセットします。

      コマンドレットの詳細については、以下を参照してください。 "SnapCenterソフトウェア コマンドレット リファレンス ガイド" 。

2. コマンド プロンプトを開き、mysql -u root -pを実行してMySQLにログインします。

   パスワードの入力を求められます。パスワードのリセット時に指定したクレデンシャルを入力します。

3. データベースから試用版ライセンスを削除します。

```
use nsm;DELETE FROM nsm_License WHERE nsm_License_Serial_Number='510000050';
```

高可用性の設定

SnapCenterサーバを高可用性向けに構成する

Windows または Linux 上で実行されているSnapCenterで高可用性 (HA) をサポートするには、F5 ロード バランサをインストールできます。F5により、SnapCenter Serverは、同じ場所にある最大2つのホストでアクティブ / パッシブ構成をサポートできます。SnapCenterでF5ロード バランサを使用するには、SnapCenter Serverを設定し、F5 ロード バランサを設定する必要があります。

ネットワーク負荷分散 (NLB) を構成して、 SnapCenter の高可用性を設定することもできます。高可用性を実現するには、 SnapCenterインストールの外部で NLB を手動で構成する必要があります。

クラウド環境では、Amazon Web Services (AWS) Elastic Load Balancing (ELB) と Azure ロードバランサーのいずれかを使用して高可用性を構成できます。

F5を使用した高可用性の設定

F5ロードバランサを使用して高可用性を実現するSnapCenterサーバの構成手順については、以下を参照してください。 "F5 ロードバランサを使用してSnapCenterサーバを高可用性に構成する方法" 。

次のコマンドレットを使用してF5クラスタを追加および削除するには、（SnapCenterAdminロールが割り当てられた）SnapCenter Serverのローカル管理者グループのメンバーである必要があります。

- Add-SmServerCluster
- Add-SmServer
- Remove-SmServerCluster

> https://docs.netapp.com/us-en/snapcenter-cmdlets/index.html["SnapCenterソフトウェア コマンドレット リファレンス ガイド"^] 。

追加情報

- SnapCenterをインストールして高可用性を実現するための設定を行ったあとで、F5クラスタのIPを指すようにSnapCenterデスクトップのショートカットを編集します。
- SnapCenter Server間のフェイルオーバーが発生し、SnapCenterの既存のセッションも存在する場合は、ブラウザを閉じてからSnapCenterに再度ログオンする必要があります。
- ロード バランサ セットアップ (NLB または F5) で、NLB または F5 ホストによって部分的に解決されるホストを追加し、 SnapCenterホストがこのホストにアクセスできない場合、 SnapCenterホスト ページでは、ホストのダウン状態と実行状態が頻繁に切り替わります。この問題を解決するには、両方のSnapCenterホストが NLB または F5 ホストでホストを解決できることを確認する必要があります。
- MFA 設定用のSnapCenterコマンドは、すべてのホストで実行する必要があります。証明書利用者の設定は、F5クラスタの詳細を使用してActive Directoryフェデレーション サービス（AD FS）サーバで行う必要があります。 MFA を有効にすると、ホスト レベルのSnapCenter UI アクセスがブロックされます。
- フェイルオーバー中、監査ログ設定は 2 番目のホストに反映されません。したがって、F5 パッシブホストがアクティブになったときに、監査ログ設定を手動で繰り返す必要があります。

ネットワーク負荷分散 **(NLB)** を使用して高可用性を構成する

ネットワーク負荷分散 (NLB) を構成して、 SnapCenter の高可用性を設定できます。高可用性を実現するには、 SnapCenterインストールの外部で NLB を手動で構成する必要があります。

SnapCenterでネットワーク負荷分散（NLB）を構成する方法については、以下を参照してください。 "SnapCenterでNLBを構成する方法" 。

AWS Elastic Load Balancing (ELB) を使用して高可用性を構成する

2 台のSnapCenterサーバーを別々のアベイラビリティーゾーン (AZ) に設定し、自動フェイルオーバーを構成することで、Amazon Web Services (AWS) で高可用性SnapCenter環境を構成できます。アーキテクチャには、仮想プライベート IP アドレス、ルーティング テーブル、アクティブおよびスタンバイ MySQL データベース間の同期が含まれます。

手順

1. AWS で仮想プライベートオーバーレイ IP を構成します。詳細については、 "仮想プライベートオーバーレイIPを構成する" 。
2. Windowsホストを準備する
   a. IPv4 を IPv6 よりも優先させる:
      - 場所: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
      - キー: DisabledComponents
      - タイプ: REG_DWORD
      - 値: 0x20
   b. 完全修飾ドメイン名が DNS またはローカル ホスト構成を介して IPv4 アドレスに解決できることを確認します。
   c. システム プロキシが構成されていないことを確認してください。
   d. Active Directory のないセットアップを使用し、サーバーが同じドメインにない場合は、両方の Windows Server で管理者パスワードが同じであることを確認します。
   e. 両方の Windows サーバーに仮想 IP を追加します。
3. SnapCenterクラスターを作成します。
   a. Powershell を起動し、 SnapCenterに接続します。 `Open-SmConnection`
   b. クラスターを作成します。 `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip> -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator`
   c. セカンダリ サーバーを追加します。 `Add-SmServer -ServerName <server_name> -ServerIP <server_ip> -CleanUpSecondaryServer -Verbose -Credential administrator`
   d. 高可用性の詳細を取得します。 `Get-SmServerConfig`
4. AWS CloudWatch によって監視されている仮想プライベート IP エンドポイントが使用できなくなった場合にルーティング テーブルを調整する Lambda 関数を作成します。詳細については、 "Lambda関数を作成する" 。
5. SnapCenterエンドポイントの可用性を監視するために、CloudWatch でモニターを作成します。エンドポイントに到達できない場合に Lambda 関数をトリガーするようにアラームが設定されています。 Lambda 関数はルーティング テーブルを調整して、トラフィックをアクティブなSnapCenterサーバーにリダイレクトします。詳細については、 "合成カナリアを作成する" 。
6. CloudWatch モニタリングの代替としてステップ関数を使用してワークフローを実装し、フェイルオーバー時間を短縮します。ワークフローには、 SnapCenter URL をテストするための Lambda プローブ関数、失敗数を保存するための DynamoDB テーブル、および Step Function 自体が含まれています。
   a. SnapCenter URL を調査するには、Lambda 関数を使用します。詳細については、 "Lambda関数を作成する" 。
   b. 2 回の Step Function 反復間の失敗回数を保存するための DynamoDB テーブルを作成します。詳細については、 "DynamoDBテーブルを使い始める" 。
   c. ステップ関数を作成します。詳細については、 "Step Function ドキュメント" 。
   d. 単一のステップをテストします。

e. 完全な機能をテストします。

f. IAM ロールを作成し、Lambda 関数を実行できるように権限を調整します。

g. Step Function をトリガーするスケジュールを作成します。詳細については、 "Amazon EventBridge Scheduler を使用して Step Functions を開始する" 。

Azure ロード バランサーを使用して高可用性を構成する

Azure ロード バランサーを使用して、高可用性SnapCenter環境を構成できます。

手順

1. Azure ポータルを使用してスケール セット内に仮想マシンを作成します。 Azure 仮想マシン スケール セットを使用すると、負荷分散された仮想マシンのグループを作成して管理できます。仮想マシン インスタンスの数は、需要または定義されたスケジュールに応じて自動的に増加または減少します。詳細については、 "Azure ポータルを使用してスケール セットに仮想マシンを作成する" 。
2. 仮想マシンを構成した後、VM セット内の各仮想マシンにログインし、両方のノードにSnapCenter Server をインストールします。
3. ホスト 1 にクラスターを作成します。 `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <specify the load balancer front end virtual ip> -PrimarySCServerIP <ip address> -Verbose -Credential <credentials>`
4. セカンダリ サーバーを追加します。 `Add-SmServer -ServerName <name of node2> -ServerIP <ip address of node2> -Verbose -Credential <credentials>`
5. 高可用性の詳細を取得します。 `Get-SmServerConfig`
6. 必要に応じて、セカンダリ ホストを再構築します。 `Set-SmRepositoryConfig -RebuildSlave -Verbose`
7. 2 番目のホストにフェイルオーバーします。 `Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose`

== 高可用性のために NLB から F5 に切り替える

SnapCenterのHA構成を、ネットワーク負荷分散（NLB）からF5ロード バランサに変更できます。

手順

1. F5 を使用して、高可用性を実現するSnapCenterサーバーを構成します。 "詳細情報" 。
2. SnapCenter Serverホストで、PowerShellを起動します。
3. Open-SmConnectionコマンドレットを使用してセッションを開始し、クレデンシャルを入力します。
4. Update-SmServerClusterコマンドレットを使用して、F5クラスタのIPアドレスを指すようにSnapCenter Serverを更新します。

   コマンドレットで使用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、 "SnapCenterソフトウェア コマンドレット リファレンス ガイド" 。

SnapCenter MySQLリポジトリの高可用性

MySQL Serverの機能であるMySQLレプリケーションを使用すると、MySQLデータベース サーバ（マスター）から別のMySQLデータベース サーバ（スレーブ）へ、データをレプリケートできます。SnapCenterでは、ネットワーク負荷分散（NLB）が有効な2つのノード間でのみ、高可用性実現のためにMySQLレプリケーションをサポートしています。

SnapCenterは、マスター リポジトリに対して読み取りまたは書き込みの処理を実行し、マスター リポジトリで障害が発生した場合はスレーブ リポジトリへ接続をルーティングします。この場合、スレーブ リポジトリがマスター リポジトリになります。SnapCenterでは逆方向のレプリケーションもサポートされており、これはフェイルオーバー時にのみ有効になります。

MySQL高可用性（HA）機能を使用する場合は、1つ目のノードにネットワーク ロード バランサ（NLB）を設定する必要があります。MySQLリポジトリは、インストール中にこのノードにインストールされます。2つ目のノードにSnapCenterをインストールするときは、1つ目のノードのF5に追加して、2つ目のノードにMySQLリポジトリのコピーを作成する必要があります。

SnapCenter は、MySQL レプリケーションを管理するための *Get-SmRepositoryConfig* および *Set-SmRepositoryConfig* PowerShell コマンドレットを提供します。

コマンドレットで使用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、 "SnapCenterソフトウェア コマンドレット リファレンス ガイド" 。

MySQL HA機能に関連する次の制限事項を理解しておく必要があります。

- NLBとMySQL HAがサポートされるのは、2つのノードまでです。
- SnapCenterスタンドアロン インストールからNLBインストールまたはその逆の切り替えや、MySQLスタンドアロン セットアップからMySQL HAへの切り替えはサポートされていません。
- スレーブ リポジトリのデータがマスター リポジトリのデータと同期されていない場合、自動フェイルオーバーはサポートされません。

  Set-SmRepositoryConfig コマンドレットを使用して強制フェールオーバーを開始できます。

- フェイルオーバーが開始されると、実行中のジョブが失敗する場合があります。

  MySQL ServerまたはSnapCenter Serverがダウンしたためにフェイルオーバーが発生した場合、実行中のすべてのジョブが失敗する可能性があります。2つ目のノードへのフェイルオーバー後、後続のすべてのジョブは正常に実行されます。

高可用性の構成については、以下を参照してください。 "SnapCenterでNLBとARRを構成する方法" 。

ロールベース アクセス制御（**RBAC**）の設定

ロールの作成

既存のSnapCenterロールを使用するだけでなく、独自のロールを作成し、権限をカスタマイズすることもできます。

独自のロールを作成するには、「SnapCenterAdmin」ロールとしてログインする必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. 設定ページで、「ロール」をクリックします。
3. クリック。
4. 新しいロールの名前と説明を指定します。

   ユーザー名とグループ名には、スペース ( )、ハイフン (-)、アンダースコア (_)、コロン (:) の特殊文字のみを使用できます。

5. このロールのすべてのメンバーが他のメンバーのオブジェクトを表示できる を選択すると、ロールの他のメンバーは、リソース リストを更新した後にボリュームやホストなどのリソースを表示できるようになります。

   このロールのメンバーに他のメンバーが割り当てられているオブジェクトを表示しない場合は、このオプションをオフにします。

   このオプションを有効にすると、オブジェクトまたはリソースを作成したユーザと同じロールに属しているユーザにオブジェクトまたはリソースへのアクセスを割り当てる必要がなくなります。

6. 「権限」ページで、ロールに割り当てる権限を選択するか、「すべて選択」をクリックしてロールにすべての権限を付与します。
7. *送信*をクリックします。

セキュリティ ログイン コマンドを使用して**NetApp ONTAP RBAC** ロールを追加する

ストレージ システムでクラスタ化されたONTAP を実行している場合は、セキュリティ ログイン コマンドを使用してNetApp ONTAP RBAC ロールを追加できます。

開始する前に

- 実行するタスク (1 つまたは複数) と、それらのタスクを実行するために必要な権限を特定します。
- コマンドおよびコマンド ディレクトリ、またはそのいずれかに権限を付与します。

  コマンドおよびコマンド ディレクトリのアクセス権限には、フルアクセスと読み取り専用の2つのレベルがあります。

  フルアクセス権限は、常に最初に付与する必要があります。

- ユーザにロールを割り当てます。
- SnapCenterプラグインがクラスタ全体の Cluster Administrator IP に接続されているか、クラスタ内の SVM に直接接続されているかに応じて構成を識別します。

タスク概要

ストレージ システムでのこれらのロールの構成を簡素化するには、 NetAppコミュニティ フォーラムに掲載されているNetApp ONTAPツール用の RBAC User Creator を使用できます。

このツールは、ONTAPの権限の適切な設定を自動的に処理します。たとえば、 NetApp ONTAPツールの

RBAC User Creator は、すべてのアクセス権限が最初に表示されるように、権限を正しい順序で自動的に追加します。読み取り専用権限を最初に追加し、次にフルアクセス権限を追加すると、ONTAPはフルアクセス権限を重複するものとしてマーキングし、無視します。

> 後でSnapCenterまたはONTAPをアップグレードする場合は、 NetApp ONTAPツールの RBAC User Creator を再実行して、以前に作成したユーザー ロールを更新する必要があります。前のバージョンのSnapCenterまたはONTAP用に作成したユーザ ロールは、アップグレード後のバージョンでは正常に機能しません。ツールを再度実行すると、アップグレードが自動的に処理されます。ロールを再作成する必要はありません。

ONTAP RBACロールの設定の詳細については、 "ONTAP 9 管理者認証および RBAC パワーガイド" 。

手順

1. ストレージ システムで、次のコマンドを入力して新しいロールを作成します。

```
security login role create <role_name\> -cmddirname "command" -access all
-vserver <svm_name\>
```

   - svm_nameには、SVMの名前を指定します。これを空白のままにした場合、デフォルトでクラスタ管理者が指定されます。
   - role_nameは、ロールに指定する名前です。
   - commandは、ONTAPの機能です。

   > このコマンドは、権限ごとに実行する必要があります。フルアクセス コマンドは、読み取り専用コマンドの前にリストする必要があります。

   権限のリストについては、以下を参照してください。"ロールの作成と権限の割り当てのためのONTAP CLIコマンド" 。

2. 次のコマンドを入力して、ユーザ名を作成します。

```
security login create -username <user_name\> -application ontapi -authmethod
<password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment
"user_description"
```

   - user_nameは、作成するユーザの名前です。
   - <password> はあなたのパスワードです。パスワードを指定しないと、パスワードの入力を求めるプロンプトが表示されます。
   - svm_nameには、SVMの名前を指定します。

3. 次のコマンドを入力して、ユーザにロールを割り当てます。

```
security login modify username <user_name\> -vserver <svm_name\> -role
<role_name\> -application ontapi -application console -authmethod <password\>
```

   - <user_name> は、手順 2 で作成したユーザーの名前です。このコマンドでは、ロールに関連付けるユーザを変更できます。
   - <svm_name> は SVM の名前です。
   - <role_name> は、手順 1 で作成したロールの名前です。

◦ <password> はあなたのパスワードです。パスワードを指定しないと、パスワードの入力を求めるプロンプトが表示されます。

4. 次のコマンドを入力して、ユーザが正しく作成されたことを確認します。

```
security login show -vserver <svm_name\> -user-or-group-name <user_name\>
```

user_nameは、手順3で作成したユーザ名です。

最小権限での**SVM**ロールの作成

ONTAP内の新しいSVMユーザにロールを作成する場合、複数のONTAP CLIコマンドを実行する必要があります。ONTAP内のSVMをSnapCenterで使用するように設定し、vsadminロールを使用したくない場合、このロールが必要です。

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\>
```

このコマンドは、権限ごとに実行する必要があります。

2. ユーザを作成して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\>
```

3. 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

SVMロールを作成して権限を割り当てるために実行する必要のあるONTAP CLIコマンドがあります。

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -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 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 -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

"volume online" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_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 modify-snaplock-expiry-time" -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 snapshot show-delta" -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
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname

"nvme namespace modify" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all

ASA r2 システムの SVM ロールを作成する

ASA r2 システムで新しい SVM ユーザーのロールを作成するには、いくつかのONTAP CLI コマンドを実行する必要があります。このロールは、 ASA r2 システムで SVM をSnapCenterで使用するように構成し、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\>
   ```

   このコマンドは、権限ごとに実行する必要があります。

2. ユーザを作成してロールを割り当てます。

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

3. 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

SVMロールを作成して権限を割り当てるために実行する必要のあるONTAP CLIコマンドがあります。

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -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 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 -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_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 modify-snaplock-expiry-time" -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 snapshot show-delta" -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
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "storage-unit show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "consistency-group" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror protect" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume delete" -access all`
- `security login create -user-or-group-name user_name -application http -authentication-method password -role SVM_Role_Name -vserver SVM_Name`
- `security login create -user-or-group-name user_name -application ssh -authentication-method password -role SVM_Role_Name -vserver SVM_Name`

最小権限での**ONTAP**クラスタ ロールの作成

最小権限でONTAPクラスタ ロールを作成し、ONTAP adminロールを使用しなくてもSnapCenterで処理を実行できるようにする必要があります。いくつかのONTAP CLIコマンドを実行して、ONTAPクラスタ ロールを作成し、最小権限を割り当てることができます。

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 <cluster_name\>- role <role_name\>
   -cmddirname <permission\>
   ```

   このコマンドは、権限ごとに実行する必要があります。

2. ユーザを作成してロールを割り当てます。

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

3. 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

クラスタ ロールを作成して権限を割り当てるために実行する必要のあるONTAP CLIコマンドがあります。

- `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 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 "nvme subsystem map" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all
- 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 snapshot modify-snaplock-expiry-time" -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 snapshot show-delta" -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

ASA r2システム用の**ONTAP**クラスタロールを作成する

最小権限でONTAPクラスタ ロールを作成し、ONTAP adminロールを使用しなくてもSnapCenterで処理を実行できるようにする必要があります。いくつかのONTAP CLIコマンドを実行して、ONTAPクラスタ ロールを作成し、最小権限を割り当てることができます。

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 <cluster_name\>- role <role_name\>
-cmddirname <permission\>
```

このコマンドは、権限ごとに実行する必要があります。

2. ユーザを作成してロールを割り当てます。

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

3. 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

クラスタ ロールを作成して権限を割り当てるために実行する必要のあるONTAP CLIコマンドがあります。

- `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 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 "nvme subsystem map" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all
- 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 snapshot modify-snaplock-expiry-time" -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 snapshot show-delta" -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
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "storage-unit show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "consistency-group" show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror protect" show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume delete" show" -access all

ユーザまたはグループの追加と、ロールとアセットの割り当て

SnapCenterユーザのロールベース アクセス制御を設定するには、ユーザまたはグループを追加してロールを割り当てます。ロールに基づいて、SnapCenterユーザがアクセスできるオプションが決まります。

開始する前に

- 「SnapCenterAdmin」ロールでログインする必要があります。
- オペレーティング システムまたはデータベースのActive Directoryにユーザまたはグループのアカウントを作成しておく必要があります。SnapCenterでこれらのアカウントを作成することはできません。

  ユーザー名とグループ名には、スペース ( )、ハイフン (-)、アンダースコア (_)、コロン (:) の特殊文字のみを含めることができます。

- SnapCenterには、事前定義されたロールが複数あります。

  これらのロールをユーザに割り当てるか、新しいロールを作成できます。

- SnapCenter RBACに追加するADユーザとADグループには、Active DirectoryのUsersコンテナとComputersコンテナに対する読み取り権限が必要です。
- まず適切な権限を含むロールをユーザまたはグループに割り当ててから、SnapCenterのアセット（ホストやストレージ接続など）へのアクセスをそのユーザに割り当てる必要があります。

  これにより、ユーザは、自身に割り当てられたアセットに対して、権限のある処理を実行できるようになります。

- RBACの権限と効率性を活用するためには、いずれかの時点でユーザまたはグループにロールを割り当てる必要があります。

- ユーザまたはグループの作成時に、ホスト、リソース グループ、ポリシー、ストレージ接続、プラグイン、クレデンシャルなどのアセットをユーザに割り当てることができます。
- 特定の処理を実行するためにユーザに割り当てる必要がある最小アセットは次のとおりです。

処理	割り当てるアセット
リソースの保護	ホスト、ポリシー
バックアップ	ホスト、リソース グループ、ポリシー
リストア	ホスト、リソース グループ
クローン	ホスト、リソース グループ、ポリシー
クローンのライフサイクル	ホスト
リソース グループの作成	ホスト

- WindowsクラスタまたはDAG（Exchange Serverデータベース可用性グループ）アセットに新しいノードが追加され、そのノードがユーザに割り当てられた場合は、アセットをユーザまたはグループに再割り当てして、新しいノードをユーザまたはグループに追加する必要があります。

  RBACユーザ / グループをクラスタ / DAGに再割り当てして、新しいノードをRBACユーザ / グループに追加する必要があります。たとえば、2ノード クラスタにRBACユーザまたはグループを割り当てたとします。このクラスタに別のノードを追加した場合は、RBACユーザ / グループをクラスタに再割り当てして、新しいノードをRBACユーザ / グループに追加する必要があります。

- Snapshotをレプリケートする場合は、処理を実行するユーザにソースとデスティネーションの両方のボリュームに対するストレージ接続を割り当てる必要があります。

  ユーザにアクセスを割り当てる前にアセットを追加しておいてください。

SnapCenter Plug-in for VMware vSphereの機能を使用してVM、VMDK、またはデータストアを保護している場合は、VMware vSphere GUIを使用してSnapCenter Plug-in for VMware vSphereロールにvCenterユーザを追加する必要があります。VMware vSphere のロールの詳細については、以下を参照してください。 "SnapCenter Plug-in for VMware vSphereに組み込みの事前定義のロール" 。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. 設定ページで、ユーザーとアクセス > *をクリックします。 *。
3. [Active Directory またはワークグループからユーザ / グループを追加]ページで次の操作を実行します。

フィールド	操作
アクセスタイプ	[Domain]または[workgroup]を選択します。 ドメイン認証タイプの場合は、ロールに追加するユーザまたはグループのドメイン名を指定する必要があります。 デフォルトでは、ログインしているドメイン名があらかじめ入力されています。 信頼されていないドメインは、設定 > グローバル設定 > ドメイン設定 ページで登録する必要があります。
タイプ	[User]または[Group]を選択します。 SnapCenterでサポートされるのはセキュリティ グループのみです。配信グループはサポートされません。
ユーザ名	a. ユーザー名の一部を入力し、[追加] をクリックします。 ユーザ名では大文字と小文字が区別されます。 b. 検索リストからユーザ名を選択します。 別のドメインまたは信頼されないドメインからユーザを追加する場合、ドメインをまたぐユーザの検索リストはないため、完全なユーザ名を入力する必要があります。 同じ手順を繰り返して、選択したロールに必要なユーザまたはグループを追加します。
ロール	ユーザを追加するロールを選択します。

4. *割り当て*をクリックし、資産の割り当てページで次の操作を行います。
   a. *資産*ドロップダウンリストから資産の種類を選択します。
   b. 資産テーブルで、資産を選択します。

      リストには、ユーザがSnapCenterに追加したアセットだけが表示されます。

   c. 必要なすべてのアセットについて、同じ手順を繰り返します。

d. *保存*をクリックします。

5. *送信*をクリックします。

ユーザまたはグループを追加してロールを割り当てたら、リソース リストを更新します。

監査ログの設定

監査ログは、SnapCenter Serverのすべてのアクティビティについて生成されます。デフォルトでは、監査ログはデフォルトのインストール場所 *C:\Program Files\ NetApp\ SnapCenter WebApp\audit* に保存されます。

監査ログのセキュリティは、すべての監査イベントについて、不正な変更ができないようにデジタル署名が付いたダイジェストを生成することで確保されます。生成されたダイジェストは、独立した監査チェックサム ファイルに保持され、コンテンツの整合性を確認するために定期的な整合性チェックが実行されます。

「SnapCenterAdmin」ロールでログインする必要があります。

タスク概要

- アラートは、次のシナリオで送信されます。
  - 監査ログの整合性チェックのスケジュールまたはsyslogサーバが有効化 / 無効化された
  - 監査ログの整合性チェック、監査ログ、またはsyslogサーバ ログに問題がある
  - ディスク スペースが不足している
- 整合性チェックに失敗した場合のみ、Eメールが送信されます。
- 監査ログのディレクトリと監査チェックサム ログのディレクトリのパスは、両方とも変更する必要があります。片方だけを変更することはできません。
- 監査ログのディレクトリと監査チェックサム ログのディレクトリのパスを変更すると、以前の場所にある監査ログに対して整合性チェックを実行できなくなります。
- 監査ログのディレクトリと監査チェックサム ログのディレクトリのパスは、SnapCenter Serverのローカル ドライブ上である必要があります。

  共有ドライブやネットワーク マウント ドライブは、サポートされていません。

- syslogサーバの設定でUDPプロトコルを使用している場合、ポートが停止している、または使用できないことによるエラーは、SnapCenterでエラーまたはアラートとして取得できません。
- 監査ログを構成するには、Set-SmAuditSettings コマンドと Get-SmAuditSettings コマンドを使用できます。

  コマンドレットで使用できるパラメータとその説明は、Get-Help command_nameを実行して確認できます。あるいは、 "SnapCenterソフトウェア コマンドレット リファレンス ガイド" 。

手順

1. 設定*ページで、*設定 > グローバル設定 > *監査ログ設定*に移動します。
2. [Audit log]セクションで、詳細を入力します。
3. *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*を入力します。

a. [Maximum file size]を入力します。

b. [Maximum log files]を入力します。

c. アラートが送信されるディスク スペース使用量を割合（%）で入力します。

4. (オプション) **UTC** 時間のログ を有効にします。

5. (オプション) 監査ログ整合性チェックスケジュール を有効にし、オンデマンド整合性チェックを実行するために 整合性チェックの開始 をクリックします。

   Start-SmAuditIntegrityCheck コマンドを実行して、オンデマンドの整合性チェックを開始することもできます。

6. （オプション）[Forwarded audit logs to remote syslog server]を有効にし、syslogサーバの詳細を入力します。

   TLS 1.2プロトコルについては、syslogサーバから「信頼されたルート」に証明書をインポートする必要があります。

   a. syslogサーバのホストを入力します。

   b. syslogサーバのポートを入力します。

   c. syslogサーバのプロトコルを入力します。

   d. RFCの形式を入力します。

7. *保存*をクリックします。

8. モニター > ジョブ をクリックすると、監査整合性チェックとディスク容量チェックを確認できます。

SnapCenter ServerとのセキュアなMySQL接続の設定

スタンドアロン構成またはNetwork Load Balancing（NLB）構成でSnapCenter ServerとMySQLサーバの間の通信を保護する場合は、Secure Sockets Layer（SSL）証明書とキー ファイルを生成します。

スタンドアロンSnapCenter Server構成用のセキュアなMySQL接続の設定

SnapCenter ServerとMySQLサーバの間の通信を保護するには、Secure Sockets Layer（SSL）証明書とキー ファイルを生成します。証明書とキー ファイルは、MySQLサーバとSnapCenter Serverで設定する必要があります。

次の証明書が生成されます。

- CA証明書
- サーバのパブリック証明書と秘密鍵ファイル
- クライアントのパブリック証明書と秘密鍵ファイル

手順

1. opensslコマンドを使用して、WindowsのMySQLサーバおよびクライアントのSSL証明書とキー ファイルを設定します。

詳細については、 "MySQL バージョン 5.7: openssl を使用した SSL 証明書とキーの作成"

> サーバ証明書、クライアント証明書、およびキー ファイルに使用する共通名は、それぞれCA証明書の共通名と異なる必要があります。共通名が同じ場合、それらの証明書とキーファイルはOpenSSLを使用してコンパイルされたサーバでエラーになります。

ベスト プラクティス: サーバー証明書の共通名として、サーバーの完全修飾ドメイン名 (FQDN) を使用する必要があります。

2. SSL証明書とキー ファイルをMySQLのデータ フォルダにコピーします。

   デフォルトのMySQLデータフォルダのパスは `C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\`。

3. MySQLサーバ構成ファイル（my.ini）で、CA証明書、サーバ パブリック証明書、クライアント パブリック証明書、サーバ秘密鍵、およびクライアント秘密鍵のパスを更新します。

   デフォルトのMySQLサーバー設定ファイル（my.ini）のパスは `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini`。

   > MySQL サーバー構成ファイル (my.ini) の [mysqld] セクションで、CA 証明書、サーバー公開証明書、およびサーバー秘密キーのパスを指定する必要があります。

   MySQL サーバー構成ファイル (my.ini) の [client] セクションで、CA 証明書、クライアント公開証明書、およびクライアント秘密キーのパスを指定する必要があります。

   次の例は、デフォルトフォルダのmy.iniファイルの[mysqld]セクションにコピーされた証明書とキーファイルを示しています。 `C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data` 。

   ```
   ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
   ```

   ```
   ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
   ```

   ```
   ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
   ```

   次の例は、my.ini ファイルの [client] セクションで更新されたパスを示しています。

   ```
   ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
   ```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-
key.pem"
```

4. Internet Information Server（IIS）でSnapCenter Server Webアプリケーションを停止します。
5. MySQLサービスを再起動します。
6. SnapManager.Web.UI.dll.configファイルのMySQLProtocolキーの値を更新します。

   次の例では、SnapManager.Web.UI.dll.configファイルのMySQLProtocolキーの値が更新されています。

```
<add key="MySQLProtocol" value="SSL" />
```

7. my.ini ファイルの [client] セクションで指定されたパスを使用して、 SnapManager.Web.UI.dll.config ファイルを更新します。

   次の例は、my.ini ファイルの [client] セクションで更新されたパスを示しています。

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

8. IISでSnapCenter Server Webアプリケーションを起動します。

HA構成用のセキュアな**MySQL**接続の設定

SnapCenter ServerとMySQLサーバの間の通信を保護する場合は、両方の高可用性（HA）ノード用にSecure Sockets Layer（SSL）証明書とキー ファイルを生成します。証明書とキー ファイルは、MySQLサーバとHAノードで設定する必要があります。

次の証明書が生成されます。

- CA証明書

  一方のHAノードでCA証明書を生成し、もう一方のHAノードにコピーします。

- 両方のHAノードのサーバ パブリック証明書とサーバ秘密鍵ファイル
- 両方のHAノードのクライアント パブリック証明書とクライアント秘密鍵ファイル

手順

1. 1つ目のHAノードで、openssl コマンドを使用して、WindowsのMySQLサーバおよびクライアントのSSL証明書とキー ファイルを設定します。

   詳細については、 "MySQL バージョン 5.7: openssl を使用した SSL 証明書とキーの作成"

   > サーバ証明書、クライアント証明書、およびキー ファイルに使用する共通名は、それぞれCA証明書の共通名と異なる必要があります。共通名が同じ場合、それらの証明書とキー ファイルはOpenSSLを使用してコンパイルされたサーバでエラーになります。

   ベスト プラクティス: サーバー証明書の共通名として、サーバーの完全修飾ドメイン名 (FQDN) を使用する必要があります。

2. SSL証明書とキー ファイルをMySQLのデータ フォルダにコピーします。

   MySQLのデータ フォルダのデフォルト パスは、C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\です。

3. MySQLサーバ構成ファイル（my.ini）で、CA証明書、サーバ パブリック証明書、クライアント パブリック証明書、サーバ秘密鍵、およびクライアント秘密鍵のパスを更新します。

   MySQLサーバ構成ファイル（my.in）のデフォルト パスは、C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.iniです

   > MySQL サーバー構成ファイル (my.ini) の [mysqld] セクションで、CA 証明書、サーバー公開証明書、およびサーバー秘密キーのパスを指定する必要があります。

   MySQL サーバー構成ファイル (my.ini) の [client] セクションで、CA 証明書、クライアント公開証明書、およびクライアント秘密キーのパスを指定する必要があります。

   次の例は、デフォルト フォルダ C:/ProgramData/ NetApp/ SnapCenter/MySQL Data/Data にある my.ini ファイルの [mysqld] セクションにコピーされた証明書とキー ファイルを示しています。

   ```
   ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
   ```

   ```
   ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
   ```

   ```
   ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
   ```

次の例は、my.ini ファイルの [client] セクションで更新されたパスを示しています。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem"
```

4. 2つ目のHAノードで、次の手順に従ってCA証明書をコピーし、サーバ パブリック証明書、サーバ秘密鍵ファイル、クライアント パブリック証明書、およびクライアント秘密鍵ファイルを生成します。

   a. 1つ目のHAノードで生成したCA証明書を2つ目のHAノードのMySQLのデータ フォルダにコピーします。

      MySQLのデータ フォルダのデフォルト パスは、C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\です。

      CA証明書は新しく作成しないでください。サーバ パブリック証明書、クライアント パブリック証明書、サーバ秘密鍵ファイル、クライアント秘密鍵ファイルのみを作成します。

   b. 1つ目のHAノードで、openssIコマンドを使用して、WindowsのMySQLサーバおよびクライアントのSSL証明書とキー ファイルを設定します。

      "MySQL バージョン 5.7: openssl を使用した SSL 証明書とキーの作成"

      サーバ証明書、クライアント証明書、およびキー ファイルに使用する共通名は、それぞれCA証明書の共通名と異なる必要があります。共通名が同じ場合、それらの証明書とキー ファイルはOpenSSLを使用してコンパイルされたサーバでエラーになります。

      サーバ証明書の共通名としてサーバのFQDNを使用することを推奨します。

   c. SSL証明書とキー ファイルをMySQLのデータ フォルダにコピーします。

   d. MySQLサーバ構成ファイル（my.ini）で、CA証明書、サーバ パブリック証明書、クライアント パブリック証明書、サーバ秘密鍵、およびクライアント秘密鍵のパスを更新します。

      MySQL サーバー構成ファイル (my.ini) の [mysqld] セクションで、CA 証明書、サーバー公開証明書、およびサーバー秘密キーのパスを指定する必要があります。

      MySQL サーバー構成ファイル (my.ini) の [client] セクションで、CA 証明書、クライアント公開証明書、およびクライアント秘密キーのパスを指定する必要があります。

      次の例は、デフォルト フォルダ C:/ProgramData/ NetApp/ SnapCenter/MySQL Data/Data にある my.ini ファイルの [mysqld] セクションにコピーされた証明書とキー ファイルを示しています。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

次の例は、my.ini ファイルの [client] セクションで更新されたパスを示しています。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

+

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

+

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

5. 両方のHAノードのInternet Information Server（IIS）でSnapCenter Server Webアプリケーションを停止します。
6. 両方のHAノードで、MySQLサービスを再起動します。
7. 両方のHAノードで、SnapManager.Web.UI.dll.configファイルのMySQLProtocolキーの値を更新します。

   次の例では、SnapManager.Web.UI.dll.configファイルのMySQLProtocolキーの値が更新されています。

   ```
   <add key="MySQLProtocol" value="SSL" />
   ```

8. 両方の HA ノードの my.ini ファイルの [client] セクションで指定したパスを使用して、SnapManager.Web.UI.dll.config ファイルを更新します。

   次の例は、my.ini ファイルの [client] セクションで更新されたパスを示しています。

   ```
   <add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem" />
   ```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

9. 両方のHAノードのIISでSnapCenter Server Webアプリケーションを起動します。
10. 一方のHAノードで、PowerShellのSet-SmRepositoryConfig -RebuildSlave -Forceコマンドレット（-Force オプションを指定）を使用して、両方のHAノードにセキュアなMySQLレプリケーションを確立します。

    レプリケーションが健全な状態であっても、-Forceオプションを指定するとスレーブ リポジトリを再構築できます。

証明書ベースの認証を構成する

証明書ベースの認証は、 SnapCenterサーバーとプラグイン ホストの両方の ID を検証することでセキュリティを強化し、安全で暗号化された通信を保証します。

証明書ベースの認証の有効化

SnapCenter ServerおよびWindowsプラグイン ホストの証明書ベースの認証を有効にするには、次のPowerShellコマンドレットを実行します。Linuxプラグイン ホストで双方向SSLを有効にすると、証明書ベースの認証が有効になります。

- クライアント証明書ベースの認証を有効にする：

  ```
  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：

  ```
  Set-SmConfigSettings -Agent –configSettings
  @{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
  ```

SnapCenter Serverからの認証局（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 Server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。

開始する前に

双方向SSLを設定しておく必要があります。

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] をクリックしま

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。
4. コンソール ルート > 証明書 - ローカル コンピューター > 個人 > 証明書 をクリックします。
5. SnapCenter Server に使用される取得した CA 証明書を右クリックし、[すべてのタスク] > [エクスポート] を選択してエクスポート ウィザードを起動します。
6. ウィザードで次の操作を実行します。

オプション	操作
秘密キーのエクスポート	*いいえ、秘密キーをエクスポートしません*を選択し、*次へ*をクリックします。
エクスポート ファイルの形式	*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、[完了] をクリックしてエクスポートを開始します。

証明書ベースの認証は、SnapCenter HA構成およびSnapCenter Plug-in for VMware vSphereではサポートされません。

Windowsプラグインホストに**CA**証明書をインポートする

エクスポートしたSnapCenter Server CA証明書を使用するには、Microsoft管理コンソール（MMC）を使用して、関連する証明書をSnapCenter Windowsプラグイン ホスト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] をクリックします。
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。
4. コンソール ルート > 証明書 - ローカル コンピューター > 個人 > 証明書 をクリックします。
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 ウィザードを起動します。
6. ウィザードで次の操作を実行します。

オプション	操作
保存場所	*次へ*をクリックします。
インポートするファイル	拡張子.cerで終わるSnapCenter Server証明書を選択します。
証明書ストア	*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、[完了] をクリックしてインポートを開始します。

UNIXプラグイン ホストへのCA証明書のインポート

CA証明書をUNIXプラグイン ホストにインポートする必要があります。

このタスクについて

- 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、秘密キーに関連付けられているエイリアス パスワードをすべて同じにする必要があります。

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、キーストアで使用されているものと同じパスワードに変更します。 `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
4. キーSPL_KEYSTORE_PASSも同様に更新します。 `spl.properties``ファイル。
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のSPLトラストストアへの設定

ルート証明書または中間証明書をSPLトラストストアに設定する必要があります。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。

手順

1. SPL キーストアが含まれているフォルダーに移動します。 `/var/opt/snapcenter/spl/etc` 。
2. ファイルを見つける `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。

SPLトラストストアに対する**CA**署名付きキー ペアの設定

SPLトラストストアに対してCA署名付きキー ペアを設定する必要があります。

手順

1. SPLのキーストアを含むフォルダに移動します `/var/opt/snapcenter/spl/etc`。
2. ファイルを見つける `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。

   デフォルトのSPLキーストアのパスワードは、SPL_KEYSTORE_PASSキーの値です。 `spl.properties`ファイル。

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

8. CA 証明書のエイリアス名が長く、スペースや特殊文字 (「*」、「」) 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. 以下のキーストアからエイリアス名を設定します。 `spl.properties`ファイル。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。

SnapCenter証明書のエクスポート

SnapCenter証明書を .pfx 形式でエクス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] をクリックします。
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、[ユーザー アカウント] オプションを選択し、[完了] をクリックしま

す。

4. コンソール ルート > 証明書 - 現在のユーザー > 信頼されたルート証明機関 > 証明書 をクリックします。
5. SnapCenterフレンドリ名を持つ証明書を右クリックし、[すべてのタスク] > [エクスポート] 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実行します。

ウィザード ウィンドウ	操作
秘密キーのエクスポート	*はい、秘密キーをエクスポートします*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 ファイルの形式	変更せずに、[次へ] をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、[次へ] をクリックします。
エクスポートするファイル	エクスポートする証明書のファイル名を指定し (.pfx を使用する必要があります)、[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、[完了] をクリックしてエクスポートを開始します。

WindowsホストのCA証明書の設定

CA証明書CSRファイルの生成

証明書署名要求（CSR）を生成し、生成したCSRを使用して認証局（CA）から取得した証明書をインポートできます。証明書には秘密キーが関連付けられます。

CSRはエンコードされたテキストのブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。

CA 証明書の RSA キーの長さは最低 3072 ビットである必要があります。

CSRを生成するための情報については、 "CA証明書CSRファイルの生成方法" 。

ドメイン (*.domain.company.com) またはシステム (machine1.domain.company.com) の CA 証明書を所有している場合は、CA 証明書 CSR ファイルの生成をスキップできます。SnapCenterを使用して、既存のCA証明書を導入できます。

クラスタ構成の場合、クラスタ名（仮想クラスタFQDN）と、それぞれのホスト名がCA証明書に記載されている必要があります。証明書を取得する前に、サブジェクト別名 (SAN) フィールドに入力することで証明書を更新できます。ワイルド カード証明書 (*.domain.company.com) の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

CA証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenter ServerとWindowsホスト プラグインにCA証明書を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] をクリックします。
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。
4. コンソール ルート > 証明書 - ローカル コンピューター > 信頼されたルート証明機関 > 証明書 をクリックします。
5. 「信頼されたルート証明機関」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 ウィザードを起動します。
6. 次の手順でウィザードを実行します。

ウィザード ウィンドウ	操作
秘密キーのインポート	*はい*オプションを選択し、秘密キーをインポートして、*次へ*をクリックします。
インポート ファイル形式	変更せずに、[次へ] をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、[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、[完了] をクリックしてインポートを開始します。

インポートする証明書は秘密キーと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、および *.p7b です)。

7. 「個人用」フォルダに対して手順5を繰り返します。

CA証明書のサムプリントの取得

証明書サムプリントは、証明書を識別するための16進数の文字列です。サムプリントは、サムプリント アルゴリズムを使用して証明書の内容から計算されます。

手順

1. GUIで次の手順を実行します。
   a. 証明書をダブルクリックします。
   b. [証明書] ダイアログボックスで、[詳細] タブをクリックします。

c. フィールドのリストをスクロールして、「拇印」をクリックします。

d. ボックスから16進数の文字をコピーします。

e. 16進数の間のスペースを削除します。

たとえば、拇印が「a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b」の場合、スペースを削除すると「a909502dd82ae41433e6f83886b00d4277a32a7b」になります。

2. PowerShellで、次の手順を実行します。

a. 次のコマンドを実行して、インストールされている証明書のサムプリントを表示し、最近インストールされた証明書をサブジェクト名で識別します。

Get-ChildItem -Path 証明書*:\LocalMachine\My*

b. サムプリントをコピーします。

Windowsホスト プラグイン サービスでのCA証明書の設定

インストールされているデジタル証明書をアクティブ化するには、Windowsホスト プラグイン サービスを使用してCA証明書を設定する必要があります。

SnapCenter Serverと、CA証明書がすでに導入されているすべてのプラグイン ホストで、次の手順を実行します。

手順

1. 次のコマンドを実行して、既存の証明書とSMCoreのデフォルト ポート8145とのバインドを削除します。

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

例えば：

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

. 次のコマンドを実行して、新しくインストールした証明書をWindowsホスト プラグイン サービスとバインドします。

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

例えば：

```
> $cert = “a909502dd82ae41433e6f83886b00d4277a32a7b”
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

SnapCenterサイトでのCA証明書の設定

Windowsホスト上のSnapCenterサイトでCA証明書を設定する必要があります。

手順

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、[接続] をクリックします。
3. サーバーの名前と*サイト*を展開します。
4. SSL証明書をインストールするSnapCenterのWebサイトを選択します。
5. アクション > サイトの編集 に移動し、バインド をクリックします。
6. [バインディング] ページで、*https のバインディング*を選択します。
7. *編集*をクリックします。
8. [SSL certificate]ドロップダウン リストから、最近インポートしたSSL証明書を選択します。
9. [OK]をクリックします。

SnapCenter Scheduler サイト (デフォルト ポート: 8154、HTTPS) は、自己署名証明書で構成されています。このポートはSnapCenter Serverホスト内で通信しており、CA証明書を使用した設定は必須ではありません。ただし、CA証明書の使用が必要な環境の場合は、SnapCenterスケジューラ サイトを使用して手順5から9を繰り返します。

最近導入したCA証明書がドロップダウン メニューに表示されない場合は、CA証明書が秘密鍵に関連付けられているかどうかを確認します。

次のパスを使用して証明書が追加されていることを確認します: コンソール ルート **>** 証明書 **-** ローカル コンピューター **>** 信頼されたルート証明機関 **>** 証明書。

SnapCenterのCA証明書の有効化

CA証明書を設定し、SnapCenter ServerのCA証明書の検証を有効にする必要があります。

開始する前に

- CA証明書を有効または無効にするには、Set-SmCertificateSettingsコマンドレットを使用します。
- SnapCenter Serverの証明書のステータスを表示するには、Get-SmCertificateSettingsコマンドレットを使用します。

コマンドレットで使用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。または、 "SnapCenterソフトウェア コマンドレット リファレンス ガイド" 。

手順

1. 設定ページで、設定 > グローバル設定 > **CA** 証明書設定 に移動します。
2. *証明書の検証を有効にする*を選択します。
3. *適用*をクリックします。

終わったら

[Managed Hosts]タブのホストに鍵マークが表示されます。この鍵マークの色は、SnapCenter Serverとプラグイン ホスト間の接続のステータスを示します。

- * * は、プラグイン ホストに有効化されているか割り当てられている CA 証明書がないことを示します。
- * * は CA 証明書が正常に検証されたことを示します。
- * * は、CA 証明書を検証できなかったことを示します。
- * * は接続情報を取得できなかったことを示します。

ステータスが黄色または緑の場合は、データ保護処理が正常に完了しています。

LinuxホストのCA証明書の設定

LinuxにSnapCenter Serverをインストールすると、インストーラによって自己署名証明書が作成されます。このCA証明書を使用する場合は、nginxリバース プロキシ、監査ログ、およびSnapCenterサービスの証明書を設定する必要があります。

nginx証明書の設定

手順

1. */etc/nginx/conf.d* に移動します。 `cd /etc/nginx/conf.d`
2. vi または任意のテキスト エディターを使用して **snapcenter.conf** を開きます。
3. 構成ファイルのserverセクションに移動します。
4. CA 証明書を指すように *ssl_certificate* と *ssl_certificate_key* のパスを変更します。
5. ファイルを保存して、閉じます。
6. nginx をリロードします: `$nginx -s reload`

監査ログ証明書の設定

手順

1. vi または任意のテキスト エディターを使用して、*INSTALL_DIR/ NetApp/snapcenter/SnapManagerWeb/ SnapManager.Web.UI.dll.config* を開きます。

INSTALL_DIR のデフォルト値は */opt* です。

2. **AUDILOG_CERTIFICATE_PATH** キーと **AUDILOG_CERTIFICATE_PASSWORD** キーを編集して、それぞれ CA 証明書パスとパスワードを含めます。

   監査ログ証明書では *.pfx* 形式のみがサポートされます。

3. ファイルを保存して、閉じます。
4. **snapmanagerweb** サービスを再起動します。 `$ systemctl restart snapmanagerweb`

SnapCenterサービス証明書の設定

手順

1. viまたは任意のテキスト エディタを使用して、次の構成ファイルを開きます。
   - *INSTALL_DIR/ NetApp/snapcenter/SnapManagerWeb/ SnapManager.Web.UI.dll.config*
   - *INSTALL_DIR/ NetApp/snapcenter/SMCore/SMCoreServiceHost.dll.config*
   - *INSTALL_DIR/ NetApp/snapcenter/Scheduler/Scheduler.Api.dll.config*

     INSTALL_DIR のデフォルト値は */opt* です。

2. **SERVICE_CERTIFICATE_PATH** キーと **SERVICE_CERTIFICATE_PASSWORD** キーを編集して、それぞれ CA 証明書パスとパスワードを含めます。

   SnapCenterサービス証明書では、*.pfx* 形式のみがサポートされます。

3. ファイルを保存して閉じます。
4. すべてのサービスを再起動します。
   - `$ systemctl restart snapmanagerweb`
   - `$ systemctl restart smcore`
   - `$ systemctl restart scheduler`

Windowsホストでの双方向SSL通信の設定と有効化

Windowsホストでの双方向SSL通信の設定

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

開始する前に

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

詳細については、 "CA 証明書セクションを構成します。"

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

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

手順

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

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

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

      次に例を示します。

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

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

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

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

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

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

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

      次に例を示します。

      ```
      > $cert = "abc123abc123abc123abc123"

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

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

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

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

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

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

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

   Windowsレジストリ エディタで次のパスに移動します。

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

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

   ```
   SendTrustedIssuerList = 0

   ClientAuthTrustMode = 2
   ```

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

PowerShellコマンドを使用して、SnapCenter Windowsプラグインで双方向SSL通信を使用できるように設定する必要があります。

開始する前に

CA証明書サムプリントが使用可能であることを確認します。

手順

1. ポートをバインドするには、Windowsプラグイン ホストでSMCoreポート8145（デフォルト）に対して次の操作を実行します。
   a. 次のPowerShellコマンドを使用して、既存のSnapCenter自己署名証明書のポート バインドを削除します。

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

      次に例を示します。

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

b. 新しく取得したCA証明書をSMCoreポートにバインドします。

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

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

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

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

次に例を示します。

```
> $cert = "abc123abc123abc123abc123"

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

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

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

Windowsホストでの双方向SSL通信の有効化

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

始める前に

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

手順

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

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

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

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

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

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

双方向**SSL**通信の無効化

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

このタスクについて

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

手順

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

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

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

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

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

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

Linuxホストでの双方向**SSL**通信の設定と有効化

Linuxホストでの双方向**SSL**通信の設定

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

開始する前に

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

手順

1. **certificate.pem** を */etc/pki/ca-trust/source/anchors/* にコピーします。

2. Linuxホストの信頼リストに証明書を追加します。
   - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
   - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
   - `update-ca-trust extract`
3. 証明書が信頼リストに追加されたかどうかを確認します。 `trust list | grep "<CN of your certificate>"`
4. SnapCenter **nginx** ファイル内の **ssl_certificate** と **ssl_certificate_key** を更新して再起動します。
   - `vim /etc/nginx/conf.d/snapcenter.conf`
   - `systemctl restart nginx`
5. SnapCenter Server GUIリンクを更新します。
6. */<インストール パス>/ NetApp /snapcenter/SnapManagerWeb* にある * SnapManager .Web.UI.dll.config* と */<インストール パス>/ NetApp/snapcenter/SMCore* にある **SMCoreServiceHost.dll.config** の次のキーの値を更新します。
   - <add key="SERVICE_CERTIFICATE_PATH" value="<certificate.pfx のパス>" />
   - <キーを追加="SERVICE_CERTIFICATE_PASSWORD" 値="<パスワード>"/>
7. 次のサービスを再起動します。
   - `systemctl restart smcore.service`
   - `systemctl restart snapmanagerweb.service`
8. 証明書がSnapManager Web ポートに接続されていることを確認します。 `openssl s_client -connect localhost:8146 -brief`
9. 証明書が smcore ポートに接続されていることを確認します。 `openssl s_client -connect localhost:8145 -brief`
10. SPLキーストアとエイリアスのパスワードを管理します。
    a. SPL プロパティ ファイルの **SPL_KEYSTORE_PASS** キーに割り当てられた SPL キーストアのデフォルト パスワードを取得します。
    b. キーストアのパスワードを変更します。 `keytool -storepasswd -keystore keystore.jks`
    c. すべての秘密鍵エントリのエイリアスのパスワードを変更します。 `keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
    d. *spl.properties* のキー **SPL_KEYSTORE_PASS** の同じパスワードを更新します。
    e. サービスを再起動します。
11. プラグインのLinuxホストで、SPLプラグインのキーストアにルート証明書と中間証明書を追加します。
    - `keytool -import -trustcacerts -alias <any preferred alias name> -file <path of root-ca.pem> -keystore <path of keystore.jks mentioned in spl.properties file>`
    - `keytool -importkeystore -srckeystore <path of certificate.pfx> -srcstoretype pkcs12 -destkeystore <path of keystore.jks mentioned in spl.properties file> -deststoretype JKS`
      i. keystore.jks 内のエントリを確認します。 `keytool -list -v -keystore <path to`

keystore.jks>

ii. 必要に応じてエイリアスの名前を変更します。 `keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas`

12. *spl.properties* ファイルの **SPL_CERTIFICATE_ALIAS** の値を、*keystore.jks* に保存されている **certificate.pfx** のエイリアスで更新し、SPL サービスを再起動します。 `systemctl restart spl`

13. 証明書が smcore ポートに接続されていることを確認します。 `openssl s_client -connect localhost:8145 -brief`

Linuxホストでの**SSL**通信の有効化

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

手順

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

Active Directory、LDAP、LDAPSの設定

信頼されていない**Active Directory**ドメインの登録

信頼されていない複数のActive Directoryドメインのホスト、ユーザ、およびグループを管理するには、Active DirectoryをSnapCenter Serverに登録する必要があります。

開始する前に

LDAP および **LDAPS** プロトコル

- 信頼されていないActive Directoryドメインは、LDAPプロトコルまたはLDAPSプロトコルを使用して登録できます。
- プラグイン ホストとSnapCenter Serverの間の双方向の通信を有効にしておく必要があります。

- SnapCenter Serverとプラグイン ホストの間でDNS解決が設定されている必要があります。

LDAPプロトコル

- 完全修飾ドメイン名（FQDN）をSnapCenter Serverから解決できる必要があります。

  信頼されていないドメインはFQDNを使用して登録できます。FQDNをSnapCenter Serverから解決できない場合は、ドメイン コントローラのIPアドレスを使用して登録できます。このアドレスは、SnapCenter Serverから解決できるものである必要があります。

LDAPSプロトコル

- Active Directoryとの通信中にLDAPSでエンドツーエンドの暗号化を提供するためには、CA証明書が必要です。

  "LDAPS用のCAクライアント証明書の設定"

- ドメイン コントローラのホスト名（DCHostName）にSnapCenter Serverから到達できる必要があります。

このタスクについて

- 信頼されていないドメインは、SnapCenterユーザ インターフェイス、PowerShellコマンドレット、REST APIのいずれかを使用して登録できます。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[グローバル設定]をクリックします。
3. [グローバル設定]ページで、[ドメイン設定]をクリックします。
4. をクリックし て新しいドメインを登録します。
5. 「新しいドメインの登録」ページで、**LDAP** または **LDAPS** のいずれかを選択します。
   a. **LDAP** を選択した場合は、信頼されていないドメインを LDAP に登録するために必要な情報を指定します。

フィールド	操作
ドメイン名	ドメインのNetBIOS名を指定します。
ドメインFQDN	FQDN を指定して、[解決] をクリックします。
ドメインコントローラのIPアドレス	ドメインのFQDNをSnapCenter Serverから解決できない場合、ドメイン コントローラのIPアドレスを1つ以上指定します。 詳細については、以下を参照してください。 "GUIから信頼されていないドメインのドメインコントローラIPを追加する" 。

b. **LDAPS** を選択した場合は、信頼されていないドメインを LDAPS に登録するために必要な情報を指定します。

フィールド	操作
ドメイン名	ドメインのNetBIOS名を指定します。
ドメインFQDN	FQDNを指定します。
Domain controller Names	1 つ以上のドメイン コントローラー名を指定し、[解決] をクリックします。
ドメインコントローラのIPアドレス	ドメイン コントローラ名をSnapCenter Serverから解決できない場合は、DNS解決を修正する必要があります。

6. [OK]をクリックします。

Active Directoryの読み取り権限を有効にするためのIISアプリケーション プールの設定

SnapCenterの Active Directory 読み取り権限を有効にする必要がある場合は、Windows Server でインターネット インフォメーション サービス (IIS) を構成してカスタム アプリケーション プール アカウントを作成できます。

手順

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 ウィンドウで、[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、操作ウィンドウで 詳細設定 をクリックします。
4. [ID] を選択し、[...] をクリックしてSnapCenterアプリケーション プール ID を編集します。
5. [カスタム アカウント] フィールドに、Active Directory の読み取り権限を持つドメイン ユーザーまたはドメイン管理者のアカウント名を入力します。
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 ApplicationPoolIdentity アカウントを置き換えます。

LDAPS用のCAクライアント証明書の設定

Windows Active Directory LDAPSにCA証明書が設定されている場合は、SnapCenter ServerにLDAPSのCAクライアント証明書を設定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] をクリックしま

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。
4. コンソール ルート > 証明書 - ローカル コンピューター > 信頼されたルート証明機関 > 証明書 をクリックします。
5. 「信頼されたルート証明機関」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 ウィザードを起動します。
6. 次の手順でウィザードを実行します。

ウィザード ウィンドウ	操作
ウィザードの2番目のページ	*参照*をクリックし、_ルート証明書_を選択して*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、[完了] をクリックしてインポートを開始します。

7. 中間証明書に対して手順 5 と 6 を繰り返します。

著作権に関する情報

商標に関する情報