# SnapCenter サーバのインストール

SnapCenter Software 5.0

NetApp
April 04, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/snapcenter/install/install_workflow.html on April 04, 2024. Always check docs.netapp.com for the latest.

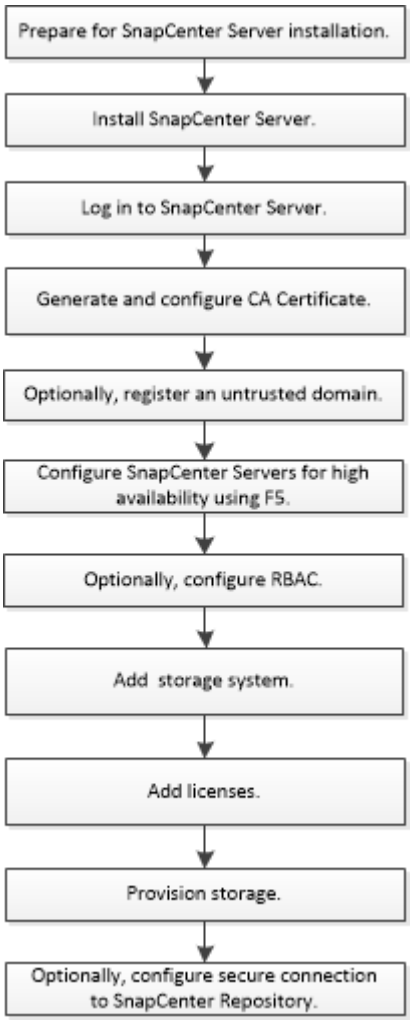
# 目次

SnapCenter サーバのインストール . . . 1
インストールワークフロー . . . 1
SnapCenter サーバをインストールする準備をします . . . 1
SnapCenter サーバをインストールします . . . 23
RBAC許可を使用してSnapCenter にログインします . . . 24
CA 証明書を設定します . . . 28
双方向SSL通信を設定して有効にします . . . 31
証明書ベースの認証を設定します . . . 36
Active Directory 、 LDAP 、 LDAPS を設定します . . . 39
ハイアベイラビリティを設定する . . . 41
ロールベースアクセス制御（ RBAC ）の設定 . . . 45
監査ログを設定します . . . 61
ストレージシステムを追加 . . . 62
SnapCenter の標準コントローラベースのライセンスを追加します . . . 66
SnapCenter の Standard 容量ベースのライセンスを追加 . . . 71
ストレージシステムをプロビジョニング . . . 75
SnapCenter サーバとの安全な MySQL 接続を設定します . . . 94
インストール中に Windows ホストで有効になる機能 . . . 100

# SnapCenter サーバのインストール

## インストールワークフロー

このワークフローでは、 SnapCenter サーバのインストールと設定に必要なさまざまなタスクについて説明します。




## SnapCenter サーバをインストールする準備をします

### ドメインとワークグループの要件

SnapCenter サーバは、ドメインまたはワークグループ内のシステムにインストールできます。インストールに使用するユーザには、ワークグループとドメインの両方の場合に、マシンに対する管理者権限が必要です。

Windows ホストに SnapCenter Server プラグインと SnapCenter プラグインをインストールするには、次のいずれかを使用する必要があります。

- * Active Directory ドメイン *

ローカル管理者の権限を持つドメインユーザ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 *

  ローカル管理者の権限がある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、 Microsoft の Active Directory ドメインと信頼関係に関するドキュメントを参照してください。

> SnapCenter サーバをインストールしたあとに、 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 サーバをインストールした時点のドメインから SnapCenter サーバホストを削除して、 SnapCenter サーバをアンインストールしようとすると、アンインストール処理は失敗します。

## スペースとサイジングの要件

SnapCenter サーバをインストールする前に、スペースとサイジングの要件を十分に理解しておく必要があります。また、利用可能なシステムおよびセキュリティの更新も適用する必要があります。

| 項目 | 要件 |
| --- | --- |
| オペレーティングシステム | Microsoft Windows の場合<br><br>サポートされているのは、英語版、ドイツ語版、日本語版、簡体字中国語版のオペレーティングシステムのみです。<br><br>サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。 |
| 最小 CPU 数 | 4 コア |
| 最小 RAM | 8 GB<br><br>MySQL Server のバッファプールでは、 RAM の合計の 20% が使用されます。 |
| SnapCenter サーバソフトウェアおよびログ用のハードドライブの最小容量 | 4 GB<br><br>SnapCenter サーバがインストールされているドライブに SnapCenter リポジトリがある場合は、 10GB にすることを推奨します。 |

| 項目 | 要件 |
| --- | --- |
| SnapCenter リポジトリ用のハードドライブの最小容量 | 6 GB<br>メモ： SnapCenter リポジトリがインストールされているドライブに SnapCenter サーバがある場合は、10GB にすることを推奨します。 |
| 必要なソフトウェアパッケージ | • Microsoft .NET Framework 4.7.2以降<br>• Windows Management Framework （ WMF ） 4.0 以降<br>• PowerShell 4.0 以降 |

## SAN ホストの要件

SnapCenter ホストが FC / iSCSI 環境に配置されている場合、 ONTAP ストレージへのアクセスを有効にするために、システムに追加のソフトウェアのインストールが必要になることがあります。

SnapCenter には、 Host Utilities と DSM は含まれていません。SnapCenter ホストが SAN 環境に配置されている場合は、次のソフトウェアのインストールと設定が必要になることがあります。

- Host Utilities のことです

  Host Utilities は FC および iSCSI をサポートしており、 Windows サーバ上で MPIO を使用することができます。詳細については、を参照してください "Host Utilities のマニュアル"。

- Microsoft DSM for Windows MPIO

  このソフトウェアは Windows MPIO ドライバと連携して、ネットアップと Windows のホストコンピュータ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、を参照してください "ONTAP DSM から Microsoft DSM への移行方法"。

## サポートされるストレージシステムおよびアプリケーション

サポートされるストレージシステム、アプリケーション、およびデータベースを確認しておく必要があります。

- SnapCenter では、データを保護するために ONTAP 8.3.0 以降がサポートされています。
- SnapCenter は、 ONTAP ソフトウェア 4.5 P1 パッチリリースからデータを保護するために、 NetApp SnapCenter 用の Amazon FSX をサポートしています。

NetApp ONTAP に Amazon FSX を使用している場合、データ保護処理を実行するには、 SnapCenter サーバホストプラグインを 4.5 P1 以降にアップグレードする必要があります。

NetApp ONTAP の Amazon FSX の詳細については、を参照してください "Amazon FSX for NetApp ONTAP のドキュメント"。

- SnapCenter では、さまざまなアプリケーションやデータベースの保護がサポートされます。

  サポートされているアプリケーションおよびデータベースの詳細については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

- SnapCenter 4.9 P1以降では、Amazon Web Services（AWS）のSoftware-Defined Data Center（SDDC）環境上のVMware Cloudで、OracleとMicrosoft SQLのワークロードの保護がサポートされます。

  詳細については、を参照してください "VMware Cloud on AWS SDDC環境でNetApp SnapCenterを使用してOracleやMS SQLのワークロードを保護"。

## サポートされているブラウザ

### SnapCenter ソフトウェアは、複数のブラウザで使用できます。

- クロム

  v66 を使用している場合、 SnapCenter GUI の起動に失敗することがあります。

- Internet Explorer の略

  IE 10 以前のバージョンを使用している場合、 SnapCenter UI が正しくロードされません。IE 11 にアップグレードする必要があります。

  - デフォルトレベルのセキュリティのみがサポートされています。

    Internet Explorer のセキュリティ設定を変更すると、ブラウザの表示に重大な問題が発生します。

  - Internet Explorer の互換表示を無効にする必要があります。

- Microsoft Edge の場合

サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

## 接続とポートの要件

### SnapCenter サーバとアプリケーションまたはデータベースのプラグインをインストールする前に、接続とポートの要件が満たされていることを確認する必要があります。

- アプリケーションはポートを共有できません。

  各ポートは、適切なアプリケーション専用にする必要があります。

- デフォルトのポートを使用しない場合は、インストール時にカスタムポートを選択できます。

プラグインポートは、インストール後にホストの変更ウィザードを使用して変更できます。

- 固定ポートの場合は、デフォルトのポート番号を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が接続を妨げないようにしてください。
  - SnapCenter のインストール時にカスタムポートを指定した場合は、プラグインホストに、SnapCenter Plug-in Loader のそのポート用のファイアウォールルールを追加する必要があります。

次の表に、各ポートとそのデフォルト値を示します。

| ポートのタイプ | デフォルトのポート |
|---|---|
| SnapCenter ポート | 8146 （ HTTPS ）、双方向、カスタマイズ可能。URL は、 https://server:8146_ を参照してください<br><br>SnapCenter クライアント（ SnapCenter ユーザ）と SnapCenter サーバ間の通信に使用されます。プラグインホストから SnapCenter サーバへの通信にも使用されます。<br><br>ポートをカスタマイズするには、を参照してください "インストールウィザードを使用してSnapCenterサーバをインストールします。" |
| SnapCenter SMCore の通信ポート | 8145 （ HTTPS ）、双方向、カスタマイズ可能<br><br>このポートは、 SnapCenter サーバと SnapCenter プラグインがインストールされているホストの間の通信に使用されます。<br><br>ポートをカスタマイズするには、を参照してください "インストールウィザードを使用してSnapCenterサーバをインストールします。" |
| MySQL ポート | 3306 （ HTTPS ）、双方向<br><br>このポートは、 SnapCenter と MySQL リポジトリデータベースの間の通信に使用されます。<br><br>SnapCenter サーバから MySQL サーバへのセキュアな接続を作成できます。 "詳細はこちら。"<br><br>ポートをカスタマイズするには、を参照してください "インストールウィザードを使用してSnapCenterサーバをインストールします。" |

| ポートのタイプ | デフォルトのポート |
| --- | --- |
| Windows プラグインホスト | 135 、 445 （ TCP ）<br><br>ポート 135 および 445 に加え、 Microsoft が指定したダイナミックポート範囲も開いている必要があります。リモートインストール操作では、このポート範囲を動的に検索する Windows Management Instrumentation （ WMI ）サービスを使用します。<br><br>サポートされているダイナミックポート範囲については、を参照してください "Windows のサービス概要とネットワークポート要件"<br><br>ポートは、 SnapCenter サーバとプラグインをインストールするホストとの間の通信に使用されます。プラグインパッケージのバイナリを Windows プラグインホストにプッシュするには、プラグインホストでのみポートを開く必要があります。このポートはインストール後に閉じることができます。 |
| Linux または AIX プラグインホスト | 22 （ SSH ）<br><br>ポートは、 SnapCenter サーバとプラグインをインストールするホストとの間の通信に使用されます。プラグインパッケージのバイナリを Linux または AIX プラグインのホストにコピーするために SnapCenter で使用されます。これらのポートを開いておくか、ファイアウォールまたは iptables から除外しておく必要があります。 |
| SnapCenter Plug-ins Package for Windows 、 SnapCenter Plug-ins Package for Linux または SnapCenter Plug-ins Package for AIX のいずれかです | 8145 （ HTTPS ）、双方向、カスタマイズ可能<br><br>ポートは、 SMCore とプラグインパッケージがインストールされているホストの間の通信に使用されます。<br><br>通信パスも、 SVM 管理 LIF と SnapCenter サーバの間で開いている必要があります。<br><br>ポートをカスタマイズするには、を参照してください "ホストを追加し、 SnapCenter Plug-in for Microsoft Windows をインストールします" または "ホストを追加してLinuxまたはAIX用のSnapCenter Plug-insパッケージをインストールします。" |

| ポートのタイプ | デフォルトのポート |
| --- | --- |
| SnapCenter Plug-in for Oracle Database | 27216 、カスタマイズ可能<br><br>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プラグイン for Oracle で使用されます。<br><br>ポートをカスタマイズするには、を参照してください "ホストを追加してLinuxまたはAIX用のSnapCenter Plug-insパッケージをインストールします。" |
| SnapCenter 用のカスタムプラグイン | 9090 （ HTTPS ）、固定<br><br>これはカスタムプラグインホストでのみ使用される内部ポートで、ファイアウォールの例外は不要です。<br><br>SnapCenter サーバとカスタム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 ）、双方向 80 （ HTTP ）、双方向<br><br>このポートは、 SnapCenter サーバを実行するホストと SVM の間の通信に SAL （ストレージ抽象化レイヤ）で使用されます。現時点では、 SnapCenter プラグインホストと SVM の間の通信に、 SnapCenter for Windows プラグインホストの SAL でもポートが使用されています。 |
| SnapCenter Plug-in for SAP HANA Database vCode スペルチェッカーポート | 3instance_number13 または 3instance_number15 、 HTTP または HTTPS 、双方向、カスタマイズ可能です<br><br>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は、ポート番号は 13 で終わり、 MDC 以外の場合はポート番号は 15 で終わります。<br><br>たとえば、 32013 はインスタンス 20 のポート番号で、 31015 はインスタンス 10 のポート番号です。<br><br>ポートをカスタマイズするには、を参照してください "ホストを追加し、プラグインパッケージをリモートホストにインストールする。" |

| ポートのタイプ | デフォルトのポート |
| --- | --- |
| ドメインコントローラの通信ポート | 認証が適切に機能するために、 Microsoft のマニュアルを参照して、ドメインコントローラのファイアウォールで開く必要があるポートを確認してください。<br><br>SnapCenter サーバ、プラグインホスト、またはその他の Windows クライアントがユーザを認証できるように、ドメインコントローラで Microsoft の必要なポートを開く必要があります。 |

ポートの詳細を変更する手順については、を参照してください "プラグインホストを変更します"。

## SnapCenter ライセンス

SnapCenter では、アプリケーション、データベース、ファイルシステム、および仮想マシンのデータを保護するために、複数のライセンスが必要になります。インストールする SnapCenter ライセンスのタイプは、ストレージ環境および使用する機能によって異なります。

| 使用許諾 | 必要に応じて |
| --- | --- |
| SnapCenter 標準のコントローラベース | FAS、AFF、オールSANアレイ（ASA）に必要<br><br>SnapCenter Standard ライセンスはコントローラベースのライセンスで、 Premium Bundle に含まれています。SnapManager スイートのライセンスをお持ちの場合は、 SnapCenter Standard のライセンスもご利用いただけます。FAS、AFF、またはASAストレージにSnapCenterの試用版をインストールする場合は、営業担当者に連絡してPremium Bundleの評価ライセンスを取得してください。<br><br>SnapCenter は、データ保護バンドルの一部としても提供されます。A400 以降を購入している場合は、データ保護バンドルを購入する必要があります。 |

| 使用許諾 | 必要に応じて |
| --- | --- |
| SnapCenter - 容量ベース | ONTAP Select および Cloud Volumes ONTAP で必要です<br><br>Cloud Volumes ONTAP または ONTAP Select を使用している場合は、 SnapCenter で管理するデータに基づいて、容量ベースのライセンスを 1TB 単位で購入する必要があります。デフォルトでは、 SnapCenter には 90 日間の 100TB SnapCenter の標準容量ベースの試用版ライセンスが組み込まれています。その他の詳細については、営業担当者にお問い合わせください。 |
| SnapMirror または SnapVault | ONTAP<br><br>SnapCenter でレプリケーションを有効にする場合は、 SnapMirror または SnapVault のライセンスが必要です。 |
| SnapRestore | バックアップのリストアおよび検証に必要です。<br><br>プライマリストレージシステム<br><br>• リモート検証に加えてバックアップからのリストアを実行するには、 SnapVault デスティネーションシステムに必要です。<br>• リモート検証を実行する場合は、 SnapMirror デスティネーションシステムに必要です。 |
| FlexClone | データベースのクローニングおよび検証処理に必要です。<br><br>プライマリストレージシステムおよびセカンダリストレージシステム。<br><br>• セカンダリ SnapVault バックアップからクローンを作成する場合、 SnapVault デスティネーションシステムに必要です。<br>• セカンダリ SnapMirror バックアップからクローンを作成するには、 SnapMirror デスティネーションシステムに必要です。 |

| 使用許諾 | 必要に応じて |
| --- | --- |
| プロトコル | • LUN 用の iSCSI または FC ライセンス<br>• SMB 共有の CIFS ライセンス<br>• NFS タイプの VMDK 用の NFS ライセンスです<br>• VMFS タイプの VMDK 用の iSCSI または FC ライセンス<br><br>ソースボリュームを利用できない場合に SnapMirror デスティネーションシステムからデータを提供するには、 SnapMirror デスティネーションシステムに必要です。 |
| SnapCenter 標準ライセンス（オプション） | セカンダリデスティネーション<br><br>セカンダリデスティネーションに SnapCenter Standard ライセンスを追加することを推奨しますが、必須ではありません。セカンダリデスティネーションで SnapCenter 標準ライセンスが有効になっていない場合、フェイルオーバー処理の実行後に、SnapCenter を使用してセカンダリデスティネーションのリソースをバックアップすることはできません。ただし、クローニング処理と検証処理を実行するには、セカンダリデスティネーションに FlexClone ライセンスが必要です。 |

SnapCenter Advanced および SnapCenter NAS ファイルサービスのライセンスは廃止され、現在は提供されていません。

1 つ以上の SnapCenter ライセンスをインストールする必要があります。ライセンスの追加方法については、を参照してください "SnapCenter の標準コントローラベースのライセンスを追加します" または "SnapCenter の Standard 容量ベースのライセンスを追加"。

**Single Mailbox Recovery （ SMBR ）**ライセンス

SnapCenter Plug-in for Exchange を使用して Microsoft Exchange Server データベースと Single Mailbox Recovery （ SMBR ）を管理している場合は、 SMBR のライセンスが追加で必要です。 SMBR の場合は、ユーザのメールボックスに基づいて別途購入する必要があります。

NetApp®Single Mailbox Recoveryは、2023年5月12日に販売終了（EOA）になりました。詳細については、を参照してください "CPC-00507"。NetAppは、2020年6月24日に導入されたマーケティング用パーツ番号を通じて、メールボックスの容量、メンテナンス、サポートを購入したお客様をサポート対象期間中も引き続きサポートします。

NetApp Single Mailbox Recoveryは、Ontrackが提供するパートナー製品です。Ontrack PowerControlsに

は、NetApp Single Mailbox Recoveryと同様の機能が用意されています。お客様は、新しいOntrack PowerControlsソフトウェアライセンスとOntrack PowerControlsメンテナンスおよびサポートの更新をOntrackから（licensingteam@ontrack.com経由で）調達し、2023年5月12日のEOA日以降にメールボックスをきめ細かくリカバリできます。

## クレデンシャルの認証方式を指定します

クレデンシャルは、アプリケーションや環境に応じて異なる認証方式を使用します。クレデンシャルで認証されたユーザは、 SnapCenter の処理を実行できます。プラグインのインストール用とデータ保護処理用に 1 組のクレデンシャルを作成する必要があります。

### **Windows** 認証

Windows 認証方式は、 Active Directory に照らして認証します。Windows 認証の場合、 Active Directory は SnapCenter の外部で設定されます。SnapCenter の認証に追加の設定は必要ありません。Windows クレデンシャルは、ホストの追加、プラグインパッケージのインストール、ジョブのスケジュール設定などのタスクを実行する際に必要になります。

#### 信頼されないドメイン認証です

SnapCenter では、信頼されていないドメインに属するユーザとグループを使用して Windows クレデンシャルを作成できます。認証を成功させるには、信頼されていないドメインを SnapCenter に登録する必要があります。

#### ローカルワークグループ認証

SnapCenter では、ローカルのワークグループユーザとグループを使用して Windows クレデンシャルを作成できます。ローカルワークグループのユーザとグループの Windows 認証は、 Windows クレデンシャルの作成時には行われませんが、ホストの登録やその他のホスト処理が実行されるまで保留されます。

### **SQL Server** 認証

SQL 認証方式は、 SQL Server インスタンスに照らして認証します。つまり、 SnapCenter で SQL Server インスタンスが検出されている必要があります。そのため、 SQL クレデンシャルを追加する前に、ホストの追加とプラグインパッケージのインストールを行って、リソースを更新しておく必要があります。SQL Server 認証は、 SQL Server でのスケジュールの設定やリソースの検出などの処理を実行する際に必要になります。

### **Linux** 認証

Linux 認証方式は、 Linux ホストに照らして認証します。Linux 認証は、 SnapCenter の GUI からリモートで Linux ホストを追加して SnapCenter Plug-ins Package for Linux をインストールする最初のステップで必要になります。

### **AIX** 認証

AIX 認証方式は、 AIX ホストに照らして認証します。AIX 認証は、 SnapCenter の GUI からリモートで AIX ホストを追加して SnapCenter Plug-ins Package for AIX をインストールする最初のステップで必要になります。

**Oracle** データベース認証

Oracle データベース認証方式は、 Oracle データベースに照らして認証します。データベースホストでオペレーティングシステム（ OS ）認証が無効な場合、 Oracle データベースに対して処理を実行するには、 Oracle データベース認証が必要です。そのため、 Oracle データベースのクレデンシャルを追加する前に、 Oracle データベースで sysdba 権限を持つ Oracle ユーザを作成しておく必要があります。

**Oracle ASM** 認証

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

**RMAN** カタログ認証

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

## ストレージ接続およびクレデンシャル

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 サーバおよび 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 *

  ストレージ接続を使用すると、 SnapCenter サーバおよび SnapCenter プラグインから ONTAP ストレージにアクセスできるようになります。この接続のセットアップには、 AutoSupport 機能と Event Management System （ EMS ；イベント管理システム）機能の設定も含まれます。

- * 資格情報 *

  - 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。Username フィールドの有効な形式は次のとおりです。

    - NETBIOS_USERNAME_
    - _ ドメイン FQDN\ ユーザ名 _
    - *Username@UPN*

  - ローカル管理者（ワークグループのみ）

    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。

  Username フィールドの有効な形式は、 *username* です

- 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していて、ユーザ名にフル管理者権限がない場合は、少なくともリソースグループとバックアップ権限をユーザ名に割り当てる必要があります。

## 多要素認証（ **MFA** ）

多要素認証（**MFA**）を管理します。

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

#### 多要素認証（**MFA**）を有効にする

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

このタスクについて

- SnapCenter は、他のアプリケーションが同じAD FSで構成されている場合にSSOベースのログインをサポートします。AD FSの構成によっては、AD FSセッションの持続性に応じて、セキュリティ上の理由からSnapCenter でユーザ認証が必要になる場合があります。
- コマンドレットで使用できるパラメータとその説明は、を実行して確認できます `Get-Help command_name`。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

作業を開始する前に

- 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、Cisco Duoなど、AD FSがサポートする多要素認証サービスが必要です。
- SnapCenter およびAD FSサーバのタイムスタンプは、タイムゾーンに関係なく同じである必要があります。
- SnapCenter サーバの認証済み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-F5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ハイアベイラビリティ構成でのアップグレード、修復、またはディザスタリカバリ（DR）の実行時に、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、を参照してください "CA 証明書 CSR ファイルを生成します"。

手順

1. Active Directoryフェデレーションサービス（AD FS）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からダウンロードします "https://<host Fqdn>/FederationMetadata/2007-06/FederationMetadata.xml」を参照してください。

3. ダウンロードしたファイルをSnapCenter サーバにコピーしてMFA機能を有効にします。
4. PowerShellを使用して、SnapCenter 管理者ユーザとしてSnapCenter サーバにログインします。
5. PowerShellセッションを使用して、_New-SmMultifactorAuthenticationMetadata-path_cmdletを使用して、SnapCenter MFAメタデータファイルを生成します。

   pathパラメータでは、SnapCenter サーバホストにMFAメタデータファイルを保存するパスを指定します。

6. 生成されたファイルをAD FS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. を使用して、SnapCenter サーバのMFAを有効にします `Set-SmMultiFactorAuthentication` コマンドレット。
8. （オプション）を使用して、MFAの設定のステータスと設定を確認します `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、 [**Certificates**] を選択し、 [**Add**] をクリックします。
   c. [ 証明書 ] スナップインウィンドウで、 [**Computer account**] オプションを選択し、 [ 完了 *] をクリックします。
   d. ［コンソールルート］>［証明書**–**ローカルコンピューター］>［個人］>［証明書］の順にクリックします。
   e. SnapCenter にバインドされているCA証明書を右クリックし、すべてのタスク>*秘密鍵の管理*を選択します。
   f. 許可ウィザードで、次の手順を実行します。
      i. [ 追加（ Add ） ] 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。

      チェックが正常に終了したら、* OK *をクリックします。

10. AD FSホストで、AD FS管理ウィザードを開き、次の手順を実行します。
    a. [証明書利用者信頼（Rel証明 書利用者信頼）]>[証明書利用者信頼の追加（Add Rel証明 書利用者信頼）]>[開始
    b. 2番目のオプションを選択してSnapCenter MFAメタデータファイルを参照し、*次へ*をクリックします。
    c. 表示名を指定し、*次へ*をクリックします。
    d. 必要に応じてアクセス制御ポリシーを選択し、*[Next]*をクリックします。
    e. 次のタブでデフォルトに設定を選択します。
    f. [ 完了 ] をクリックします。

指定した表示名の証明書利用者としてSnapCenter が反映されるようになりました。

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. クレームルールの名前を指定します。
    d. 属性ストアとして「* Active Directory *」を選択します。
    e. 属性として「* User-Principal-Name 」を選択し、発信クレームタイプとして「 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. メタデータが正常にインポートされたことを確認するには、次の手順を実行します。
    a. 証明書利用者信頼を右クリックし、* Properties *を選択します。
    b. [エンドポイント]、[識別子]、および[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、を参照してください "複数のタブで同時にログインを試行すると、MFAエラーが表示されます"。

#### AD FS MFAメタデータを更新します

AD FSサーバでアップグレード、CA証明書の更新、DRなどの変更が行われた場合は、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 サーバにコピーしてMFA設定を更新します。
3. 次のコマンドレットを実行して、SnapCenter 内の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メタデータを更新します

ADFSサーバで修復、CA証明書の更新、DRなどに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]をクリックします。
   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*をクリックします。

      ユーザが定義した証明書利用者信頼の名前が表示されます。

   c. 多要素認証（MFA）を有効にします。

      を参照してください "多要素認証を有効にします"。

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）を無効にする

手順

1. MFAを無効にし、を使用してMFAを有効にし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を使用して多要素認証（MFA）を管理

MFAログインは、ブラウザ、REST API、PowerShell、およびSCCLIからサポートされます。MFAは、AD FSアイデンティティマネージャを介し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をOAuth/OIDCとしてセットアップします

- Windows GUIウィザードを使用してAD FSを構成します*
  1. Server Manager Dashboard **>** Tools **>** ADFS Management *に移動します。
  2. **>**[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. を選択し、[アプリケーション名]*と入力します。
     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. コピー*クライアントID *。

     これはクライアントIDです。 。リダイレクトURLにコールバックURL（SnapCenterサーバURL）を追

加します。 。「 * 次へ * 」をクリックします。

4. [Generate shared secret]*を選択します。

   シークレット値をコピーします。これはクライアントの秘密です。 。「 * 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. 新しく追加した*アプリケーショングループ*を右クリックし、*プロパティ*を選択します。
7. [アプリケーションのプロパティ]から*[アプリケーションの追加]*を選択します。
8. [アプリケーションの追加]*をクリックします。

   [Web API]を選択し、*[Next]*をクリックします。

9. [Web APIの構成]ページで、前の手順で作成したSnapCenterサーバのURLとクライアント識別子を[識別子]セクションに入力します。
   a. [ 追加（ Add ） ] をクリックします。
   b. 「 * 次へ * 」をクリックします。
10. [Choose Access Control Policy]ページで、要件に基づいて制御ポリシーを選択し（[Permit Everyone and Require MFA]など）、*[Next]*をクリックします。
11. [アプリケーション権限の設定]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おり、*[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. 承認サーバー(AD FS)によって発行され、リソースによって消費されることを意図したJWTトークン。

    このトークンの「AUD」またはオーディエンス要求は、リソースまたはWeb APIの識別子と一致している必要があります。

15. 選択したWebAPIを編集し、コールバックURL（SnapCenterサーバURL）とクライアント識別子が正しく追加されていることを確認します。

    ユーザー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の右上にある* Tools メニューの下にある AD FS Management *ツールを開きます。
    a. 左側のサイドバーから* Application Groups *フォルダを選択します。
    b. Web APIを選択し、* edit *をクリックします。
    c. [発行トランスフォームルール]タブに移動します
17. [ * ルールの追加 * ] をクリックします。
    a. [Claim rule template]ドロップダウンで、*[Send LDAP Attributes as Claims]*を選択します。

b. 「 * 次へ * 」をクリックします。

18. [Claim rule]*の名前を入力します。

    a. [属性ストア]ドロップダウンで*[Active Directory]*を選択します。

    b. [LDAP Attribute]ドロップダウンで*を選択し、**[O*utgoing Claim Type]***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コマンドを使用してアプリケーショングループを作成します

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、<link to KB article>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` 許可後のリダイレクションの有効な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. 変換ルール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トランスフォームルールを定義します。

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

アクセストークンの有効期限を更新します

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

- このタスクについて *
- アクセストークンは、ユーザー、クライアント、およびリソースの特定の組み合わせに対してのみ使用できます。アクセストークンは無効にすることはできず、有効期限が切れるまで有効です。
- デフォルトでは、アクセストークンの有効期限は60分です。 この最小限の有効期限は十分であり、拡張されています。ビジネスクリティカルなジョブが継続的に発生しないように、十分な価値を提供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Bearerトークンを取得します

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、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、第2要素認証(あなたが持っているものとあなたがいるもの)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サーバから設定できます。デフォルトの有効期間は60分です。

| フィールド | 価値 |
|---|---|
| 許可タイプ | 承認コード |
| コールバックURL | コールバックURLがない場合は、アプリケーションのベースURLを入力します。 |
| 認証URL | [ADFS-domain-name]/ADFS/OAuth2/authorize |
| アクセストークンURL | [ADFS-domain-name]/ADFS/OAuth2/token |
| クライアント ID | AD FSクライアントIDを入力します |
| クライアントシークレット | AD FSクライアントシークレットを入力します |
| 適用範囲 | OpenID |
| クライアント認証 | 基本認証ヘッダーとして送信します |
| 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トークンでは「AUD」値として表示されます。 |

### PowerShell、SCCLI、REST APIを使用してSnapCenterサーバでMFAを設定します

SnapCenter Serverでは、PowerShell、SCCLI、およびREST APIを使用して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」というもう1つのフィールドで拡張し、ベアラー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 <access token>クライアント(Postmanやswaggerなど)でBearerトークンを_Authorization = Bearer _の形式で使用し、ヘッダーにユーザRoleNameを指定すると、SnapCenterからの応答が成功します。

#### MFA REST API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、あらゆる処理を実行します。
- 手順 *
- AD FS MFAを介して認証する場合*

  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、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、[ユーザー名]テキストボックスにユーザー名または電子メールを入力します。

[+] ユーザ名は、user@domainまたはdomain\userの形式で指定する必要があります。

1. [パスワード]テキストボックスにパスワードを入力します。
2. *ログイン*をクリックします。
3. [サインインオプション]*セクションで、認証オプションを選択し、（設定に応じて）認証します。
   - プッシュ：電話機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認証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。
4. 認証が成功すると、Access、ID、およびRefresh Tokenを含むポップアップが開きます。

   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。

5. REST APIでは、ヘッダーセクションでアクセストークンとロール名を渡す必要があります。
6. SnapCenterは、AD FSからこのアクセストークンを検証します。

   有効なトークンである場合、SnapCenterはそれをデコードし、ユーザー名を取得します。

7. SnapCenterは、ユーザ名とロール名を使用して、API実行のためにユーザを認証します。

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

**REST API、CLI、GUIのSnapCenter MFA機能を有効または無効にします**

- GUI *
- 手順 *
  1. SnapCenter管理者としてSnapCenterサーバにログインします。
  2. **>**[グローバル設定]**>**[MultiFactorAuthentication（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インターフェイス*
- 手順 *
  1. PowerShellまたはCLIコマンドを実行して、GUI、REST API、PowerShell、SCCLIのMFAを有効にします。

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

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

  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たSnapCenter GUI、REST API、PowerShell、およびSCCLIのMFAを有効にします。

  1. を使用して、MFAの設定のステータスと設定を確認します `Get-SmMultiFactorAuthentication` コマンドレット。
- SCCLIインターフェイス*
- 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でMFAを有効にするには、次のPOST APIを実行します。

| パラメータ | 価値 |
|---|---|
| 要求されたURL | /api/4.9/settings/multifactorauthentication |
| HTTP メソッド | ポスト |
| リクエストボディ | { "IsGuiMFAEnabled"：false、"IsRestApiMFAEnabled"：true、"IsCliMFAEnabled"：false、"ADFSConfigFilePath"："C：\\ADFS_METADATA\\abc.xml" } |

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

2. 以下のAPIを使用してMFA構成のステータスと設定を確認します。

| パラメータ | 価値 |
|---|---|
| 要求されたURL | /api/4.9/settings/multifactorauthentication |
| HTTP メソッド | ゲット |
| 応答本文 | { "MFAConfiguration"：{ "IsGuiMFAEnabled"：false、 "ADFSConfigFilePath"："C：\\ADFS_METADATA\\abc.xml"、 "SCConfigFilePath"：null、 "IsRestApiMFAEnabled"：true、 "IsCliMFAEnabled"：false、 "ADFSHostName"："win-adfs-sc49.winscedom2.com } } |

# SnapCenter サーバをインストールします

SnapCenter サーバインストーラの実行ファイルを実行して、 SnapCenter サーバ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ができます。

> コマンドラインからの SnapCenter サーバのサイレントインストールはサポートされていません。

作業を開始する前に

- SnapCenter サーバホストは、保留中のシステムの再起動がない Windows アップデートで最新の状態になっている必要があります。
- SnapCenter サーバをインストールするホストに MySQL サーバ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。

  有効にする方法については、 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"。

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

- 手順 *

1. から SnapCenter Server インストールパッケージをダウンロードします "ネットアップサポートサイト"。
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。

   インストールの開始後、すべての事前確認が実行され、最小要件を満たしていない場合には、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、エラーは修正しておく必要があります。

3. SnapCenter サーバのインストールに必要な設定済みの値を確認し、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 サーバのインストール時に、パスワードは自動生成されます。

   > リポジトリ・データベースのカスタム・パスでは ' 特殊文字 “%” はサポートされていませんパスに "%" を含めると ' 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、該当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。

   > [Cancel] * 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 サーバがホストから完全に削除されます。

   ただし、「 SnapCenter サーバサイトの再起動」または「 SnapCenter サーバの起動を待機中」の処理が実行されているときに「 * キャンセル」をクリックすると、処理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% フォルダに古いものから順番に表示されます。ログの場所をリダイレクトする場合は 'C:\installer_location\installer_name.exe /log"C:\"`` 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

# RBAC許可を使用してSnapCenter にログインします

SnapCenter では、 Role-Based Access Control （ RBAC ；ロールベースアクセス制御）がサポートされています。SnapCenter 管理者が、 SnapCenter RBAC を使用して、ロールとリソースをワークグループまたは 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。

作業を開始する前に

- Windows Server Manager で Windows Process Activation Service （ 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 サーバ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。
- このタスクについて *

インストール中に、 SnapCenter サーバー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 ] メニューに表示されます。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。この URL は、リモートシステムからログインする場合にコピーできます。

> Web ブラウザで複数のタブを開いている場合は、 SnapCenter ブラウザの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 パスワードを保存しないことを推奨します。

GUI のデフォルトの URL は、 SnapCenter サーバがインストールされているサーバのデフォルトポート 8146 へのセキュアな接続です（ \\ 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。

ハイアベイラビリティ（ HA ）構成の場合は、仮想クラスタ 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で IE の信頼済みサイトに仮想クラスタの IP アドレスまたは FQDN を追加するか、あるいは各プラグインホストで IE のセキュリティ強化オプションを無効にする必要があります。詳細については、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ません"。

PowerShell コマンドレットを使用すると、 SnapCenter GUI に加え、設定、バックアップ、リストアの各処理を実行するスクリプトを作成できます。一部のコマンドレットは、各 SnapCenter リリースで変更された可能性があります。。 "SnapCenter ソフトウェアコマンドレットリファレンスガイド" に詳細を示します。

> 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あるショートカット、インストールの終了時に表示された URL 、または SnapCenter 管理者から提供された URL から、 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 | 次のいずれかの形式を使用 ... |
| --- | --- |
| ドメイン管理者 | • NETBIOs\ ユーザー名<br>• ユーザー名 @UPN サフィックス<br>たとえば、「 username@netapp.com 」と入力します<br>• ドメイン FQDN\ ユーザ名 |
| ローカル管理者 | ユーザ名 |

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

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

- 結果 *

ダッシュボードページが表示されます。

ログにサイトにアクセスできないというエラーが表示されて失敗した場合は、 SSL 証明書を SnapCenter にマッピングする必要があります。 "詳細はこちら。"

- 終了後 *

SnapCenter サーバに初めて RBAC ユーザとしてログインしたあと、リソースのリストを更新します。

SnapCenter でサポートされる信頼されていない Active Directory ドメインがある場合は、信頼されてい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。 "詳細はこちら。"

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

SnapCenter サーバでは、Active Directoryに含まれるドメインアカウントに対してMFAがサポートされます。

作業を開始する前に

- 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、を参照してください "多要素認証を有効にします"

- 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を使用してログインできません
- 手順 *

1. ローカルホストのデスクトップにあるショートカット、インストールの終了時に表示された URL 、または SnapCenter 管理者から提供された URL から、 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ページにユーザ名またはパスワードが無効であることを示す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。

   - ユーザ名またはパスワードが有効かどうか

     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たかどうか
   - ADおよびAD FSが稼働しているかどうか

## SnapCenter のデフォルトの GUI セッションタイムアウトを変更します

SnapCenter GUI のセッションタイムアウト時間を変更して、デフォルトのタイムアウト時間である 20 分以上に設定できます。

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、 SnapCenter は GUI セッションから 5 分後にログアウトすることを警告するメッセージを表示します。デフォルトでは、操作を行わないまま 20 分が経過すると SnapCenter によって GUI セッションからログアウトされ、再度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 * > * 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. [Session Timeout] 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、 [**Save**] をクリックします。

## SSL 3.0 を無効にして、 SnapCenter Web サーバを保護します

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

SSL 3.0 プロトコルに脆弱性が存在します。攻撃者はこの脆弱性を悪用して、原因接続に失敗したり、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できます。

- 手順 *

  1. SnapCenter Web サーバ・ホストでレジストリ・エディタを起動するには、 [ スタート **>*Run**] 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\SOFTWARE\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\ に移動します。

     - サーバ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。

     - サーバキーが存在しない場合は、次の手順を実行します。

i. [ * 編集 * ] 、 [ * 新規 * ] 、 [ * キー * ] の順にクリックし、キーサーバーに名前を付けます。
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 に有効という名前を付け、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。

# CA 証明書を設定します

## CA 証明書 CSR ファイルを生成します

証明書署名要求（ CSR ）を生成し、生成された CSR を使用して認証局（ CA ）から取得できる証明書をインポートできます。証明書には秘密鍵が関連付けられます。

CSR はエンコードされたテキストブロックであり、認証された証明書ベンダーに提供されて署名済み CA 証明書を取得します。

CA証明書RSAキーの長さは3072ビット以上にする必要があります。

CSR の生成方法については、を参照してください "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、 CA 証明書 CSR ファイルの生成を省略できます。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は、クラスタ名（仮想クラスタ FQDN ）とそれぞれのホスト名を CA 証明書に記載する必要があります。証明書を更新するには、証明書を取得する前に Subject Alternative Name （ SAN ）フィールドに値を入力します。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 証明書をインポートする

Microsoft の管理コンソール（ MMC ）を使用して、 SnapCenter サーバと 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 ] の順にクリックします。
2. [ スナップインの追加と削除 ] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
3. [ 証明書 ] スナップインウィンドウで、 [**Computer account**] オプションを選択し、 [ 完了 *] をクリックします。
4. [ * コンソールルート **>** 証明書–ローカルコンピュータ **>** 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 **>*Import** ] を選択してインポートウィザードを開始します。
6. 次の手順でウィザードを完了します。

| ウィザードウィンドウ | 実行する処理 |
| --- | --- |
| 秘密鍵をインポートします | オプション * はい * を選択し、秘密鍵をインポートして、 * 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、 * Next * をクリックします。 |
| 証明書のインポートウィザードを完了しています | 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。 |

証明書のインポートは、秘密鍵に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）。

7. 「 Personal 」フォルダについて、手順 5 を繰り返します。

## CA 証明書のサムプリントを取得します

証明書のサムプリントは、証明書を識別する 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、 [**Thumbprint**] をクリックします。
   d. ボックスから 16 進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、サムプリントが「 A9 09 50 2D d8 2a 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 」となります。

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一覧表示し、最近インストールされた証明書を件名で識別します。

      *Get-ChildItem* - パス証明書： *\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を使用して CA 証明書を設定する

CA 証明書に Windows ホストプラグインサービスを設定して、インストールされたデジ

タル証明書をアクティブ化する必要があります。

SnapCenter サーバおよび 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、 SMCore のデフォルトポート 8145 にバインドされている既存の証明書を削除します。

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

   例：

   ```
    > 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にバインドします。
   ```

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

   例：

   ```
   > $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 CA 証明書を設定します

CA 証明書は、 Windows ホスト上で SnapCenter サイトを使用して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 サーバーで IIS マネージャーを開きます。
  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. サーバー名と * Sites * を展開します。
  4. SSL 証明書をインストールする SnapCenter Web サイトを選択します。
  5. [* アクション * （ Actions * ） ] > [* サイトの編集 * （ * Edit Site * ） ] に移動し、 [ * バインド * （ Bind
  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（ Edit ） ] 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。

> 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。

> 証明書が次のパスを使用して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 > 信頼されたルート証明機関 > 証明書 * 。

### SnapCenter の CA 証明書を有効にします

CA 証明書を設定し、 SnapCenter サーバの CA 証明書検証を有効にする必要があります。

作業を開始する前に

- CA 証明書は、 Set-SmCertificateSettings コマンドレットを使用して有効または無効にできます。
- Get-SmCertificateSettings コマンドレットを使用すると、 SnapCenter サーバの証明書のステータスを表示できます。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、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"。

- 手順 *
  1. 設定ページで、 * 設定 * > * グローバル設定 * > * CA 証明書設定 * と進みます。
  2. [ 証明書の検証を有効にする ] を選択します。
  3. [ 適用（ Apply ） ] をクリックします。
- 終了後 *

管理対象ホストタブのホストには鍵が表示され、 SnapCenter サーバとプラグインホストの間の接続のステータスが南京錠の色で示されます。

- ：有効な CA 証明書がないか、プラグインホストに割り当てられていないことを示します。
- 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。
- 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ときは、データ保護処理が正常に完了しています。

## 双方向SSL通信を設定して有効にします

## 双方向SSL通信を設定します

SnapCenterサーバとプラグイン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。

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

  詳細については、を参照してください "CA証明書の設定セクション"

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

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

- 手順 *

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

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

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

   例：

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

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

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

   ```
   > $cert = “<CA_certificate thumbprint>”

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

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

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

   例：

   ```
   > $cert = “abc123abc123abc123abc123”
   ```

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

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

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

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

> netsh http show sslcert ipport=0.0.0.0:8146

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

2. CA証明書の権限にアクセスするには、次の手順を実行して新しく取得したCA証明書にアクセスし、SnapCenterのデフォルトのIIS Webサーバユーザ「* IIS AppPool\SnapCenter *」を証明書の権限のリストに追加します。
   a. Microsoft管理コンソール（MMC）に移動し、**[**ファイル**]**>*[SnapInの追加と削除]*をクリックします。
   b. [ スナップインの追加と削除 ] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
   c. [ 証明書 ] スナップインウィンドウで、 [**Computer account**] オプションを選択し、 [ 完了 *] をクリックします。
   d. ［コンソールルート］>［証明書**–**ローカルコンピューター］>［個人］>［証明書］の順にクリックします。
   e. SnapCenter証明書を選択します。
   f. ユーザー/権限の追加ウィザードを開始するには、CA証明書を右クリックし、**[**すべてのタスク**]**>*[秘密鍵の管理]*を選択します。
   g. [追加]*をクリックし、[ユーザーとグループの選択]ウィザードで場所をローカルコンピュータ名（階層の最上位）に変更します。
   h. IIS AppPool\SnapCenterユーザを追加し、フルコントロール権限を付与します。
3. CA証明書IIS権限*の場合、次のパスからSnapCenterサーバーに新しいDWORDレジストリキーエントリを追加します。

   Windowsレジストリエディタで、次のパスに移動します。

   ```
   HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\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プラグインを設定します

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

- 始める前に *

CA証明書サムプリントが使用可能であることを確認します。

- 手順 *

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

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

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

   例：

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

   b. 新しく取得したCA証明書をSMCoreポートにバインドします。

   ```
   > $cert = “<CA_certificate thumbprint>”

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

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

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

   例：

   ```
   > $cert = “abc123abc123abc123abc123”

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

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

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

## 双方向SSL通信を有効にします

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

- 始める前に *

すべてのプラグインとSMCoreエージェントのコマンドを最初に実行し、次にサーバのコマンドを実行します。

- 手順 *

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

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

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

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

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

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

双方向**SSL**通信を無効にします

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

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

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

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

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

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

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

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

# 証明書ベースの認証を設定します

## SnapCenterサーバから認証局（CA）証明書をエクスポートします

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

作業を開始する前に

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 ] の順にクリックします。
  2. [ スナップインの追加と削除 ] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
  3. [証明書スナップイン]ウィンドウで*オプションを選択し、[完了]*をクリックします。
  4. **>**[証明書-ローカルコンピュータ]**>**[個人]**>**[証明書]*をクリックします。
  5. SnapCenterサーバーで使用される調達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開始します。
  6. ウィザードで次の操作を実行します。

| オプション | 実行する処理 |
|---|---|
| 秘密鍵をエクスポートします | を選択し、[次へ]*をクリックします。 |
| エクスポートファイル形式（ Export File Format ） | 「 * 次へ * 」をクリックします。 |
| ファイル名（ File Name ） | 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。

## 認証局（**CA**）証明書を**Windows**プラグインホストにインポートします

エクスポートしたSnapCenterサーバ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 ] の順にクリックします。
  2. [ スナップインの追加と削除 ] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
  3. [証明書スナップイン]ウィンドウで*オプションを選択し、[完了]*をクリックします。
  4. **>**[証明書-ローカルコンピュータ]**>**[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開始します。
  6. ウィザードで次の操作を実行します。

| オプション | 実行する処理 |
|---|---|
| ストアの場所 | 「 * 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サーバ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。 |

## **CA**証明書を**UNIX**ホストプラグインにインポートし、ルート証明書または中間証明書を**SPL trust-store**に設定します

### **CA**証明書を**UNIX**プラグインホストにインポートします

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、秘密鍵に関連付けられているすべてのエイリアスパスワードは同じである必要があります。
- 手順 *
  1. SPL プロパティファイルから SPL キーストアのデフォルトパスワードを取得できます。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、キーストアに使用されているパスワードと同じパスワードに変更します。 `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
4. SPL_KEYSTORE_PASS INキーについても同じ内容を更新します `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てください。

ルート証明書または中間証明書を **SPL** の信頼ストアに設定します

## ルート証明書または中間証明書をspl trust-storeに設定する必要があります。ルート CA 証明書、中間 CA 証明書の順に追加する必要があります。

- 手順 *

1. SPLキーストアが格納されているフォルダに移動します。 `/var/opt/snapcenter/spl/etc`。
2. ファイルを探します `keystore.jks`。
3. キーストアに追加された証明書を表示します。 `$ 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 の信頼ストアにルート証明書または中間証明書を設定したら、サービスを再起動します。

**CA** 署名キーペアを **SPL** の信頼ストアに設定します

SPL trust-storeに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のキーストアが格納されているフォルダに移動します `/var/opt/snapcenter/spl/etc`。
2. ファイルを探します `keystore.jks`。
3. キーストアに追加された証明書を表示します。 `$ keytool -list -v -keystore keystore.jks`
4. 秘密鍵と公開鍵の両方を含む 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表示します。 `$ keytool -list -v -keystore keystore.jks`
6. キーストアに、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含まれていることを確認します。
7. CA 証明書用に追加された秘密鍵のパスワードをキーストアのパスワードに変更します。

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

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

keystore.jks`

1. CA 証明書のエイリアス名が長く、スペースまたは特殊文字（「*」、「」）が含まれている場合は、エイリアス名を単純な名前に変更します。 `$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
2. にある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。 この値をキー SPL の certificate_alias に更新します。
3. CA 署名済みキーペアを SPL 信頼ストアに設定したら、サービスを再起動します。

### 証明書ベースの認証を有効にします

SnapCenter ServerおよびWindowsプラグインホストに対して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には：

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

- クライアント証明書ベースの認証を無効にするには：

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

## Active Directory 、 LDAP 、 LDAPS を設定します

### 信頼できない **Active Directory** ドメインを登録します

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 サーバに登録する必要があります。

作業を開始する前に

- LDAP および LDAPS プロトコル *
- LDAP または LDAPS プロトコルを使用して、信頼されていない Active Directory ドメインを登録できます。
- プラグインホストと SnapCenter サーバ間の双方向通信を有効にしておく必要があります。
- DNS 解決は、 SnapCenter サーバからプラグインホスト、およびその逆にセットアップする必要があります。
- LDAP プロトコル *
- Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を SnapCenter サーバ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 に登録できます。FQDN を SnapCenter サーバ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。これは、 SnapCenter サーバが解決できる必要があります。

- LDAPS プロトコル *
- Active Directory 通信でエンドツーエンドの暗号化を行うには、 LDAPS で CA 証明書が必要です。

  "LDAPS の CA クライアント証明書を設定します"

- ドメインコントローラのホスト名（ DCHostName ）に SnapCenter サーバからアクセス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を登録するには、 SnapCenter ユーザインターフェイス、 PowerShell コマンドレット、または REST API を使用します。
- 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. をクリックします + 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、 LDAP の信頼されていないドメインを登録するために必要な情報を指定します。

| フィールド | 手順 |
|---|---|
| ドメイン名（ Domain Name ） | ドメインの NetBIOS 名を指定します。 |
| ドメイン FQDN | FQDN を指定し、 * resolve * 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 FQDN を SnapCenter サーバ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 1 つ以上指定します。<br><br>詳細については、を参照してください "GUI から信頼できないドメインのドメインコントローラ IP を追加します"。 |

     b. 「 * LDAPS * 」を選択した場合は、 LDAPS の信頼されていないドメインの登録に必要な情報を指定します。

| フィールド | 手順 |
|---|---|
| ドメイン名（ Domain Name ） | 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。 |

| フィールド | 手順 |
| --- | --- |
| ドメインコントローラ名 | 1 つまたは複数のドメインコントローラ名を指定し、 * Resolve.* 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が SnapCenter サーバ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。

### **LDAPS** の **CA** クライアント証明書を設定します

Windows Active Directory LDAPS に CA 証明書が設定されている場合は、 SnapCenter サーバで 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 ] の順にクリックします。
2. [ スナップインの追加と削除 ] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
3. [ 証明書 ] スナップインウィンドウで、 [**Computer account**] オプションを選択し、 [ 完了 *] をクリックします。
4. [ * コンソールルート **>** 証明書–ローカルコンピュータ **>** 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 **>*Import** ] を選択してインポートウィザードを開始します。
6. 次の手順でウィザードを完了します。

| ウィザードウィンドウ | 実行する処理 |
| --- | --- |
| ウィザードの 2 ページ目に表示されます | [ * 参照 ] をクリックし、 *Root Certificate* 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を完了しています | 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. 中間証明書について、手順 5 と 6 を繰り返します。

## ハイアベイラビリティを設定する

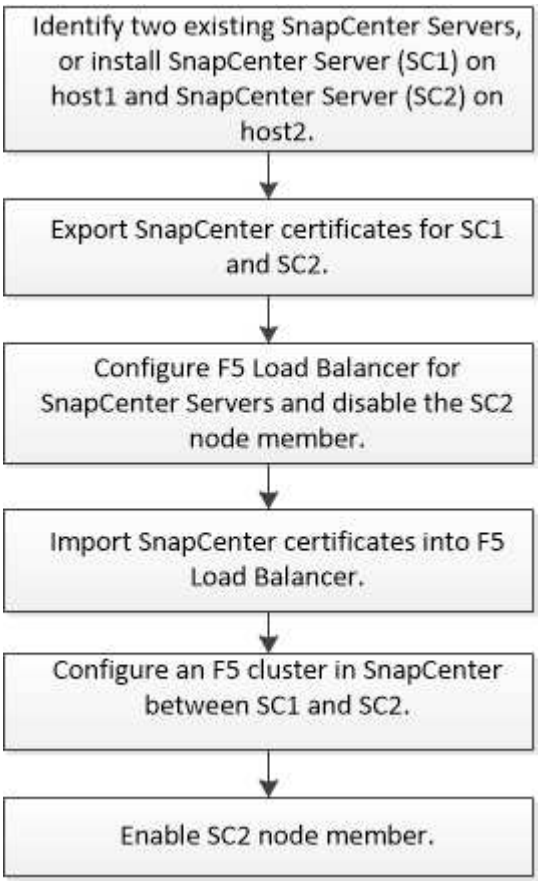
### **F5** を使用して **SnapCenter** サーバのハイアベイラビリティを構成します

SnapCenter でハイアベイラビリティ（ 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します。F5 によって、 SnapCenter サーバは、同じ場所にある最大 2 台

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 サーバを設定し、 F5 ロードバランサを設定する必要があります。

> SnapCenter 4.2.x からアップグレードし、以前に Network Load Balancing （ NLB ）を使用していた場合は、引き続きその構成を使用するか、 F5 に切り替えることができます。

ワークフローイメージには、 F5 ロードバランサを使用して SnapCenter サーバのハイアベイラビリティを設定する手順が記載されています。詳細な手順については、を参照してください "F5 ロードバランサを使用して SnapCenter サーバのハイアベイラビリティを設定する方法"。




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、 SnapCenter サーバ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（ SnapCenterAdmin ロールに割り当てられることに加えて）。

- Add - SmServerCluster をクリックします
- add-SmServer
- remove-SmServerCluster を実行しました

  詳細については、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"。

**F5** のその他の設定情報

- SnapCenter をインストールしてハイアベイラビリティ用に設定したら、 F5 クラスタ 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 サーバ間でフェイルオーバーが発生し、既存の SnapCenter セッションも存在する場合は、ブラウザを閉じてから再度 SnapCenter にログオンする必要があります。
- ロードバランサのセットアップ（ NLB または F5 ）で、 NLB ノードまたは F5 ノードによって一部解決されているノードを追加し、 SnapCenter ノードがこのノードに到達できない場合、 SnapCenter ホストページでホストが停止して実行中の状態になる頻度が高くなります。この問題を解決するには、両方の SnapCenter ノードが NLB ノードまたは F5 ノード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設定のSnapCenter コマンドは、すべてのノードで実行する必要があります。証明書利用者設定は、Active Directoryフェデレーションサービス（AD FS）サーバで、F5クラスタの詳細を使用して行う必要があります。ノードレベルのSnapCenter UIアクセスはMFAが有効になったあとはブロックされます。
- フェイルオーバー時、監査ログの設定が2つ目のノードに反映されません。このため、F5パッシブノードがアクティブになった場合は、そのノードで監査ログ設定を手動で繰り返してください。

## Microsoft Network Load Balancer を手動で設定します

SnapCenter ハイアベイラビリティを設定するには、 Microsoft Network Load Balancing （ NLB ）を設定します。SnapCenter 4.2 以降では、高可用性を実現するために、SnapCenter 以外のインストール環境で NLB を手動で設定する必要があります。

SnapCenter でネットワーク負荷分散 (NLB) を構成する方法の詳細については、を参照してください "NLB に SnapCenter を設定する方法"。

> SnapCenter 4.1.1 以前では、 SnapCenter のインストール時にネットワーク負荷分散 (NLB) の構成がサポートされていました。

## NLB から F5 に切り替えて高可用性を実現します

SnapCenter HA 構成を Network Load Balancing （ NLB ）から変更して、 F5 ロードバランサを使用することができます。

- 手順 *
  1. F5 を使用して SnapCenter サーバのハイアベイラビリティを設定します。 "詳細はこちら。"。
  2. SnapCenter サーバホストで、 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. SnapCenter サーバを更新して、 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ついては、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "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）にデータを

レプリケートできます。SnapCenter では、 Network Load Balancing （ 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操作を実行し、マスターリポジトリに障害が発生した場合はスレーブリポジトリに接続をルーティングします。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 は逆方向のレプリケーションもサポートしており、これはフェイルオーバー時にのみ有効になります。

MySQL の高可用性（ HA ）機能を使用する場合は、 1 つ目のノードに Network Load Balancer （ 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 に参加して、 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 には、 MySQL レプリケーションを管理するための _Get-SmRepositoryConfig_and _Set -SmRepositoryConfig_PowerShell コマンドレットが用意されています。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "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確認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。

  強制フェイルオーバーを開始するには、 _Set-SmRepositoryConfig_cmdlet を使用します。

- 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可能性があります。

  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。

ハイアベイラビリティの設定については、を参照してください "SnapCenter で NLB と ARR を設定する方法"。

## SnapCenter 証明書をエクスポートする

- 手順 *
  1. Microsoft 管理コンソール (MMC) に移動し、 [ * ファイル * ] 、 [ * スナップインの追加と削除 ] の順にクリックします。
  2. [ スナップインの追加と削除 ] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
  3. [ 証明書 ] スナップインウィンドウで、 [ マイ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 **>*Certificates - Current User**>*Trusted Root Certification

Authorities*>*Certificates* ] をクリックします。

5. SnapCenter フレンドリ名が表示されている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完了します。

| ウィザードウィンドウ | 実行する処理 |
|---|---|
| 秘密鍵をエクスポートします | [ はい ] を選択し、秘密鍵 * をエクスポートして、 [ 次へ ] をクリックします。 |
| エクスポートファイル形式（ Export File Format ） | 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、 * Next * をクリックします。 |
| エクスポートするファイル | エクスポートされた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。 |

- 結果 *

証明書は .pfx 形式でエクスポートされます。

# ロールベースアクセス制御（ RBAC ）の設定

## ユーザまたはグループを追加し、ロールとアセットを割り当てます

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。

作業を開始する前に

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

SnapCenter 4.5 では、ユーザ名とグループ名に次の特殊文字のみを使用できます。スペース（）、ハイフン（ - ）、アンダースコア（ _ ）、コロン（ : ）。これらの特殊文字を使用して以前のリリースの SnapCenter で作成したロールを使用する場合は、 SnapCenter WebApp がインストールされている web.config ファイルで「 isableSQLInjionValidation 」パラメータの値を true に変更することで、ロール名の検証を無効にできます。値を変更した場合、サービスを再起動する必要はありません。

- SnapCenter には、事前定義されたロールが複数あり

  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 に追加される AD ユーザと AD グループには、 Active Directory 内の 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。
- 適切な権限が割り当てられたユーザまたはグループにロールを割り当てたら、ホストやストレージ接続などの SnapCenter アセットへのユーザアクセスを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ます。

- RBAC の権限と効率性を利用するには、いずれかの時点でロールをユーザまたはグループに割り当てる必要があります。
- ホスト、リソースグループ、ポリシー、ストレージ接続、プラグインなどのアセットを割り当てることができます。 ユーザまたはグループの作成時にユーザにクレデンシャルを付与する必要があります。
- 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。

| 操作 | 資産の割り当て |
|---|---|
| リソースを保護 | 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 |
| リソースグループを作成します | 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）のアセットに新しいノードを追加したときに、その新しいノードをユーザに割り当てた場合は、新しいノードを追加するアセットをユーザまたはグループに再割り当てする必要があります。

  RBAC ユーザまたはグループをクラスタまたは DAG に再割り当てして、新しいノードを RBAC ユーザまたはグループに追加する必要があります。たとえば、 2 ノードクラスタで RBAC ユーザまたはグループをクラスタに割り当てているとします。クラスタに別のノードを追加した場合は、 RBAC のユーザまたはグループをクラスタに再割り当てして、 RBAC ユーザまたはグループの新しいノードを追加します。

- 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ボリュームとデスティネーションボ

リュームの両方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く必要があります。

> 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 のロールについては、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. [Add Users/Groups from Active Directory or Workgroup] ページで、次の手順を実行します。

| フィールド | 手順 |
| --- | --- |
| アクセスタイプ | ドメインまたはワークグループのいずれかを選択します<br><br>ドメイン認証タイプには、ロールにユーザを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。<br><br>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。<br><br>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 * （ * Settings * > * Global Settings * ） ] ページで登録する必要があります。 |
| を入力します | [ ユーザー ] または [ グループ ] を選択します<br><br>SnapCenter でサポートされるのはセキュリティグループのみで、配信グループはサポートされません。 |

| フィールド | 手順 |
| --- | --- |
| ユーザ名 | a. 部分的なユーザー名を入力し、 * 追加 * をクリックします。<br>ユーザ名では大文字と小文字が区別されます。<br>b. 検索リストからユーザ名を選択します。<br>別のドメインまたは信頼されていないドメインのユーザを追加する場合は、ユーザ名を完全に入力する必要があります。これは、クロスドメインユーザの検索リストがないためです。<br>この手順を繰り返して、選択したロールに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. [**Assign**] をクリックし、 [Assign Assets] ページで次の手順を実行します。
   a. [* アセット * ] ドロップダウン・リストからアセットのタイプを選択します。
   b. [ アセット ] リストで、アセットを選択します。

      アセットは、ユーザが SnapCenter にアセットを追加した場合にのみ表示されます。

   c. 必要なすべてのアセットについて、この手順を繰り返します。
   d. [ 保存（ Save ） ] をクリックします。
5. [Submit （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、リソースのリストを更新します。

## ロールを作成します

### 既存の SnapCenter ロールに加えて、独自のロールを作成して権限をカスタマイズできます。

「 SnapCenterAdmin 」ロールで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、 * 役割 * をクリックします。
3. をクリックします 。

4. [Add Role] ページで、新しいロールの名前と概要を指定します。

> SnapCenter 4.5 では、ユーザ名とグループ名に次の特殊文字のみを使用できます。スペース（）、ハイフン（ - ）、アンダースコア（ _ ）、コロン（ : ）。これらの特殊文字を使用して以前のリリースの SnapCenter で作成したロールを使用する場合は、SnapCenter WebApp がインストールされている web.config ファイルで「 isableSQLInjionValidation 」パラメータの値を true に変更することで、ロール名の検証を無効にできます。値を変更した場合、サービスを再起動する必要はありません。

5. このロールのすべてのメンバーは、他のメンバーのオブジェクトを表示できます * を選択すると、そのロールの他のメンバーは、リソースリストの更新後にボリュームやホストなどのリソースを参照できます。

   他のメンバーが割り当てられているオブジェクトをこのロールのメンバーに表示しないようにするには、このオプションを選択解除する必要があります。

> 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ユーザが属している場合に、オブジェクトまたはリソースへのアクセスをユーザに割り当てる必要がなくなります。

1. [ アクセス許可 ] ページで、そのロールに割り当てるアクセス許可を選択するか、 [ すべて選択 ] をクリックしてそのロールにすべてのアクセス許可を付与します。
2. [Submit （送信） ] をクリックします。

## security login コマンドを使用して、 ONTAP RBAC ロールを追加します

ストレージシステムで clustered ONTAP を実行している場合、 security login コマンドを使用して ONTAP RBAC ロールを追加できます。

作業を開始する前に

- clustered ONTAP を実行しているストレージシステム用に ONTAP RBAC ロールを作成する前に、次の項目について確認しておく必要があります。
  - 実行するタスク
  - これらのタスクを実行するために必要な権限
- RBAC ロールを設定するには、次の操作を実行する必要があります。
  - コマンドおよびコマンドディレクトリ、またはその両方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、常に最初に割り当てる必要があります。

  - 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クラスタ管理者 IP に接続されているか、またはクラスタ内の SVM に直接接続されているかに応じて、設定は異なります。
- このタスクについて *

RBAC User Creator for Data ONTAP ツールを使用して、これらのロールのストレージシステムへの設定を簡素化することができます。このツールは、ネットアップコミュニティフォーラムに掲載されています。

このツールは、 ONTAP 権限の適切な設定を自動的に処理します。たとえば、 Data ONTAP フルアクセス権限が最初に表示されるように、権限が自動的に正しい順序で追加されます。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。

> SnapCenter または ONTAP をあとからアップグレードする場合は、 RBAC User Creator for Data ONTAP ツールを再度実行して、以前に作成したユーザロールを更新する必要があります。以前のバージョンの 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、を参照してください "ONTAP 9 管理者認証と RBAC パワーガイド"。

> SnapCenter のドキュメントではロールに割り当てる要素を「権限」と呼びますが、OnCommand システムマネージャGUIでは、_privilegeではなく、TERM_attribute__が使用されます。ONTAP RBACロールを設定する場合は、この2つの用語は同じ意味です。

- 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。

   「 securitylogin role create <role_name\> -cmddirname 」「 command 」 -access all – vserver <svm_name\> 」のように指定します

   - svm_name は、 SVM ユーザの名前です。空白のままにすると、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、を参照してください "ロールの作成および権限の割り当てに使用する 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。

   「 securitylogin create -username <user_name\> -application ontapi -authmethod <password\> -role <name_on_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、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 は、 SVM ユーザの名前です。

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。

「 securitylogin modify username <user_name> – vserver <svm_name> -role <role_name\> -application ontapi -application console -authmethod <password\> 」の形式で指定します

- <user_name> は、手順 2 で作成したユーザの名前です。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、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。

   「 securitylogin show – vserver <svm_name> -user-or -group-name <user_name\>

user_name は、手順 3 で作成したユーザの名前です。

## 最小権限を持つ **SVM** ロールを作成します

ONTAP で新しい SVM ユーザのロールを作成する場合、実行する必要がある ONTAP CLI コマンドがいくつかあります。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、そのロールに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。

1. ユーザを作成し、そのユーザにロールを割り当てます。

   「 security login create -user <user_name\> -vserver <svm_name> -application ontapi -authmethod password -role <svm_Role_Name\>` 」のように設定します

2. ユーザのロックを解除します。

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

**SVM** ロールの作成および権限の割り当てに使用する **ONTAP CLI** コマンド

SVM ロールを作成して権限を割り当てるには、いくつかの ONTAP CLI コマンドを実行する必要があります。

- `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 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 を指定します
- 「 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 」に設定されています
- 「 security login role create -vserver svm_name -role SVM_Role_Name -cmddirname 」 volume clone split stop 「 -access all 」に設定されています
- 「 security login role create -vserver svm_name -role SVM_Role_Name -cmddirname 」 volume create コマンド -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 」に設定されています
- 「 security login role create -vserver svm_name -role SVM_Role_Name -cmddirname 」 volume modify コマンド -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 コマンド「-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 rename 「-access all
- 「security login role create -vserver svm_name -role SVM_Role_Name -cmddirname」 volume snapshot restore コマンド -access all
- 「security login role create -vserver svm_name -role SVM_Role_Name -cmddirname」 volume snapshot restore -file 「-access all
- 「security login role create -vserver svm_name -role SVM_Role_Name -cmddirname」 volume snapshot show 「-access all
- 「security login role create -vserver svm_name -role SVM_Role_Name -cmddirname」 volume unmount 「-access all
- 「security login role create -vserver svm_name -role SVM_Role_Name -cmddirname」 vserver cifs share create 「-access all
- 「security login role create -vserver svm_name -role SVM_Role_Name -cmddirname」 vserver cifs share delete 「-access all
- 「security login role create -vserver svm_name -role SVM_Role_Name -cmddirname」 vserver cifs share show 「-access all
- 「security login role create -vserver svm_name -role SVM_Role_Name -cmddirname」 vserver cifs show 「-access all
- 「security login role create -vserver svm_name -role SVM_Role_Name -cmddirname」 vserver export-policy create 「-access all
- 「security login role create -vserver svm_name -role SVM_Role_Name -cmddirname」 vserver export-

policy delete 「 -access all

- 「 security login role create -vserver svm_name -role SVM_Role_Name -cmddirname 」 vserver export-policy rule create 「 -access all
- 「 security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname 」 vserver export-policy rule show 「 -access all 」
- 「security login role create -vserver svm_name -role SVM_Role_Name -cmddirname」vserver export-policy show「-access all
- 「security login role create -vserver svm_name -role SVM_Role_Name -cmddirname」vserver iscsi connection show「-access all」
- 「 security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname 」 vserver 「 -access readonly
- 「 security login role create -vserver svm_name -role SVM_Role_Name -cmddirname 」 vserver export-policy 「 -access all
- 「 security login role create -vserver svm_name -role SVM_Role_Name -cmddirname 」 vserver iscsi 「 -access all
- 「security login role create -vserver svm_name -role SVM_Role_Name -cmddirname」volume clone split status「-access all」を指定します
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all`

## 最小限の権限で **ONTAP** クラスタロールを作成します

最小限の権限で ONTAP クラスタロールを作成して、 SnapCenter の admin ロールを使用して ONTAP で処理を実行する必要がないようにする必要があります。ONTAP のいくつかの CLI コマンドを実行して、 ONTAP クラスタロールを作成し、最小限の権限を割り当てることができます。

- 手順 *

1. ストレージシステムで、ロールを作成し、そのロールに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。

1. ユーザを作成し、そのユーザにロールを割り当てます。

   「 securitylogin create -user <user_name\> -vserver <cluster_name\> -application ontapi -authmethod password -role <role_name\> 」のようになります

2. ユーザのロックを解除します。

   「 securitylogin unlock -user <user_name\\> -vserver <cluster_name\\> 」のようになります

クラスタロールの作成および権限の割り当てに使用する **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。

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all`
- security login role create -vserver cluster_name -role Role_Name -cmddirname " job history show " -access all `
- security login role create -vserver cluster_name -role Role_Name -cmddirname "job stop " -access all `
- 「 security login role create -vserver cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver cluster_name -role Role_Name -cmddirname "lun create " -access all `
- security login role create -vserver cluster_name -role Role_Name -cmddirname "lun delete " -access all `
- 「 security login role create -vserver cluster_name -role Role_Name -cmddirname 」「 lun igroup add 」 -access all
- 「 security login role create -vserver cluster_name -role Role_Name -cmddirname 」「 lun igroup create 」 -access all
- 「 security login role create -vserver cluster_name -role Role_Name -cmddirname 」「 lun igroup delete 」 -access all
- 「 security login role create -vserver cluster_name -role Role_Name -cmddirname 」「 lun igroup modify 」 -access all 」を参照してください
- 「 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 コマンド -access all 」を参照してください
- 「 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 」を参照してください
- 「 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 コマンド -access readonly 」を参照してください
- 「 security login role create -vserver cluster_name -role Role_Name -cmddirname 」 network interface delete 「 -access readonly 」
- 「 security login role create -vserver cluster_name -role Role_Name -cmddirname 」 network interface modify 「 -access readonly
- 「 security login role create -vserver cluster_name -role Role_Name -cmddirname 」 network interface show 「 -access readonly 」
- security login role create -vserver cluster_name -role Role_Name -cmddirname "security login" -access readonly `
- 「 security login role create -role Role_Name -cmddirname 」「 snapmirror create 」 -vserver cluster_name -access all 」を参照してください
- 「 security login role create -role Role_Name -cmddirname 」 snapmirror list -destinations 「 -vserver cluster_name -access all 」を指定します
- 「 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 」を参照してください
- 「 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 」を参照してください
- 「 security login role create -vserver cluster_name -role Role_Name -cmddirname 」 system node modify コマンド -access all `
- 「 security login role create -vserver cluster_name -role Role_Name -cmddirname 」 system node show 「 -access all 」を参照してください
- 「 security login role create -vserver cluster_name -role Role_Name -cmddirname 」 system status show 「 -access all 」を参照してください
- 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 コマンド -access all `
- 「 security login role create -vserver cluster_name -role Role_Name -cmddirname 」 volume clone show 「 -access all 」を参照してください
- 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 コマンド -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 」を参照してください
- security login role create -vserver cluster_name -role Role_Name -cmddirname " volume modify " -access all `
- security login role create -vserver cluster_name -role Role_Name -cmddirname " volume offline " -access all `
- security login role create -vserver cluster_name -role Role_Name -cmddirname " volume online " -access all `
- 「 security login role create -vserver cluster_name -role Role_Name -cmddirname 」 volume qtree create コマンド -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 コマンド -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 コマンド -access all `
- 「 security login role create -vserver cluster_name -role Role_Name -cmddirname 」 volume snapshot promote 「 -access all 」を参照してください
- security login role create -vserver cluster_name -role Role_Name -cmddirname " volume snapshot rename " -access all `
- security login role create -vserver cluster_name -role Role_Name -cmddirname " volume snapshot restore " -access all `
- 「 security login role create -vserver cluster_name -role Role_Name -cmddirname 」 volume snapshot restore -file 「 -access all
- security login role create -vserver cluster_name -role Role_Name -cmddirname " volume snapshot show " -access all `
- 「 security login role create -vserver cluster_name -role Role_Name -cmddirname 」 volume unmount 「 -access all
- 「 security login role create -vserver cluster_name -role Role_Name -cmddirname 」「 vserver 」 -access all
- 「 security login role create -vserver cluster_name -role Role_Name -cmddirname 」 vserver cifs create 「

-access all

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

### Active Directory の読み取り権限を有効にするように IIS アプリケーションプールを設定します

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、カスタムの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 サーバーで IIS マネージャーを開きます。
  2. 左側のナビゲーションペインで、 * アプリケーションプール * をクリックします。
  3. ［アプリケーションプール］ リストで ［SnapCenter］ を選択し、 ［アクション］ ペインで ［* 詳細設定 *］ をクリックします。
  4. [ID] を選択し、 [*...] をクリックして 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に組み込まれている ApplicationPoolIdentity アカウントに代わるものです。

## 監査ログを設定します

監査ログは、SnapCenter サーバ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、監査ログはインストールされているデフォルトの場所である_ C：\Program Files\NetApp\Virtual \SnapCenter WebApp\audit_にあります。

監査ログは、各監査イベントに対してデジタル署名されたダイジェストを生成することで保護され、不正な変更から保護されます。生成されたダイジェストは個別の監査チェックサムファイルに保持され、の定期的な整合性チェックでコンテンツの整合性を確保します。

「 SnapCenterAdmin 」ロールでログインする必要があります。

- このタスクについて *
- 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サーバが有効または無効になっています
  - 監査ログの整合性チェック、監査ログ、またはsyslogサーバのログに障害が発生しました
  - ディスクスペースが不足しています
- 整合性チェックが失敗した場合にのみ、電子メールが送信されます。
- 監査ログディレクトリと監査チェックサムログディレクトリの両方のパスを一緒に変更する必要があります。変更できるのはどちらか一方だけです。
- 監査ログディレクトリと監査チェックサムログディレクトリのパスが変更された場合、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することはできません。

- 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のパスは、SnapCenter サーバのローカルドライブにある必要があります。

  共有ドライブまたはネットワークマウントドライブはサポートされません。

- syslogサーバ設定でUDPプロトコルが使用されている場合、ポートが停止しているか使用できないことによるエラーは、SnapCenter ではエラーまたはアラートとしてキャプチャできません。
- Set-SmAuditSettingsコマンドとGet-SmAuditSettingsコマンドを使用して、監査ログを構成できます。

  コマンドレットで使用できるパラメータとその説明については、 Get-Help コマンドレットを実行して確認できます。または、を参照することもできます "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]の順に選択します。
  2. 監査ログセクションに詳細を入力します。
  3. 監査ログ・ディレクトリ*および*監査チェックサム・ログ・ディレクトリ*を入力します
     a. 最大ファイルサイズを入力します
     b. 最大ログファイル数を入力します
     c. アラートを送信するためのディスクスペース使用率を入力します
  4. （任意）*Log UTC time *をイネーブルにします。
  5. （オプション）* Audit Log Integrity Check Schedule を有効にし、 Start Integrity Check * for On Demand integrity checkをクリックします。

     また、*Start-SmAuditIntegrityCheck*コマンドを実行して、必要に応じて整合性チェックを開始することもできます。

  6. （任意）転送された監査ログをリモートsyslogサーバに対してイネーブルにし、Syslogサーバの詳細を入力します。

     syslogサーバからTLS 1.2プロトコルの「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 Server Host」と入力します
     b. 「Syslog Server Port」と入力します
     c. 「Syslog Server Protocol」と入力します
     d. RFC形式を入力します
  7. [ 保存（ Save ） ] をクリックします。
  8. 監査整合性チェックとディスク領域チェックは、* Monitor > Jobs *をクリックすると表示できます。

# ストレージシステムを追加

データ保護処理とプロビジョニング処理を実行するためには、 ONTAP ストレージまたは NetApp ONTAP 用の Amazon FSX に SnapCenter アクセスを付与するストレージシ

## 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 を追加したり、複数の SVM で構成されるクラスタを追加したりできます。NetApp ONTAP に Amazon FSX 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 を追加するか、 SnapCenter に FSX SVM を追加できます。

作業を開始する前に

- ストレージ接続を作成するには、 Infrastructure Admin ロールに必要な権限が必要です。
- 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。

  ホスト・プラグインのインストールは ' ストレージ・システム接続の追加中は実行しないでくださいホスト・キャッシュが更新されず ' データベース・ステータスが SnapCenter GUI に表示される場合がありますこれは ' バックアップには使用できませんまたは NetApp ストレージには使用できません

- ストレージシステム名は一意である必要があります。

  SnapCenter では、異なるクラスタに同じ名前のストレージシステムを複数配置することはサポートされていません。SnapCenter でサポートされるストレージシステムには、それぞれ一意の名前およびデータ LIF の IP アドレスを割り当てる必要があります。

- このタスクについて *
- ストレージシステムを設定する際に、 Event Management System （ EMS ；イベント管理システム）と AutoSupport の機能を有効にすることもできます。AutoSupport ツールは、システムの健常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ネットアップ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、リストアまたはクローニング処理が正常に完了したとき、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またはデスティネーションクラスタとソースSVMまたは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、スケジュールされたジョブ、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、 Storage （ストレージ）タブで * Modify （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、 [ 新規作成 ] をクリックします。
  3. Add Storage System （ストレージシステムの追加）ページで、次の情報を入力します。

| フィールド | 手順 |
| --- | --- |
| ストレージシステム | 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。<br><br>ストレージシステム名は、ドメイン名を含めずに15文字以下にする必要があり、解決可能な名前である必要があります。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には、 Add-SmStorageConnectionPowerShell コマンドレットを使用します。<br><br>MetroCluster 構成（ MCC ）を使用するストレージシステムでは、ノンストップオペレーションを実現するために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。<br><br>SnapCenter では、異なるクラスタにある同じ名前の SVM は複数サポートされません。SnapCenter でサポートされる SVM には、それぞれ一意の名前を付ける必要があります。<br><br>SnapCenter へのストレージ接続の追加後は、 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。<br><br>SVM に短い名前または FQDN を追加した場合は、 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。 |
| ユーザ名 / パスワード | ストレージシステムにアクセスするため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。 |

| フィールド | 手順 |
| --- | --- |
| Event Management System （ EMS ；イベント管理システム）および AutoSupport の設定 | 保護適用、リストア処理の完了、または処理の失敗のために AutoSupport メッセージをストレージシステムに送信する場合は、該当するチェックボックスを選択します。<br><br>AutoSupport 通知を有効にするには AutoSupport メッセージが必要であるため、 ［ * 失敗した処理に対する SnapCenter 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、 ［ * サーバ・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、および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. プラットフォームで、ドロップダウンリストから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のセカンダリストレージシステムの場合は、 * Secondary * チェックボックスを選択します。[* Secondary] オプションを選択すると、 SnapCenter はすぐにライセンスチェックを実行しません。

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. プロトコルで、 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、デフォルトポート 443 は使用可能です。

   c. 通信が中断されるまでの経過時間を秒単位で入力します。

      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選択し、 SVM 接続用の優先 IP アドレスを入力します。
   e. [ 保存（ Save ） ] をクリックします。
      1. [Submit （送信） ] をクリックします。

- 結果 *

Storage Systems （ストレージシステム）ページの * Type （タイプ） * ドロップダウンから、次のいずれかの操作を実行します。

- 追加されたすべての ONTAP を表示する場合は、「 * SVM 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には、「 * 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、 FSX クラスタがここに表示されます。

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

ONTAP の GUI を使用して ONTAP クラスタに新しい SVM を追加した場合は、 * Rediscover* をクリックすると、新しく追加した SVM が表示されます。

> FASまたはAFFストレージシステムをオールSANアレイ（ASA）にアップグレードした場合は、SnapCenterサーバのストレージ接続を更新して、SnapCenterの新しいストレージタイプを反映する必要があります。

- 終了後 *

クラスタ管理者は、ストレージシステムのコマンドラインから次のコマンドを実行して、各ストレージシステムノードで AutoSupport を有効にし、 SnapCenter がアクセス可能な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必要があります。

```
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。

# SnapCenter の標準コントローラベースのライセンスを追加します

## FAS、AFF、またはオールSANアレイ（ASA）ストレージコントローラを使用している場合は、コントローラベースのSnapCenterライセンスが必要です。

コントローラベースのライセンスには次のような特徴があります。

- Premium Bundle または Flash Bundle （ベースパックには含まれません）の購入に SnapCenter Standard のライセンスが含まれます。
- 無制限のストレージ使用
- ONTAP System Managerまたはストレージクラスタのコマンドラインを使用して、FAS、AFF、またはASAのストレージコントローラに直接追加して有効にします

  > SnapCenter コントローラベースのライセンスについては、 SnapCenter GUI 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ロックされています

必要なライセンスの詳細については、を参照してください "SnapCenter ライセンス"。

### 手順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します

SnapCenter GUI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、SnapManager Suiteライセンスが必要なストレージシ

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、ASA SVMまたはクラスタにのみ適用されます。

> お使いのコントローラにすでに SnapManagerSuite ライセンスがある場合は、 SnapCenter の標準コントローラベースのライセンス使用権が自動的に提供されます。SnapManagerSuite ライセンスと SnapCenter 標準のコントローラベースのライセンスは同じ意味で使用されますが、同じライセンスを指します。

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、追加したすべての SVM またはクラスタ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を表示するには、 * ONTAP クラスタ * 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で、コントローラライセンス列を探します。

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

   - ✔ FAS、AFF、またはASAプライマリストレージシステムにSnapManager Suiteライセンスがインストールされていることを示します。
   - ⊘ FAS、AFF、またはASAプライマリストレージシステムにSnapManager Suiteライセンスがインストールされていないことを示します。
   - 該当しない場合は、ストレージコントローラが 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 スイートのライセンスは適用されません。

## 手順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特定します

ONTAP コマンドラインを使用すると、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。

> SnapCenter の標準コントローラベースのライセンスが、 SnapManagerSuite ライセンスとしてコントローラに表示されます。

手順

1. ONTAP コマンドラインを使用してネットアップ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: 1-81-0000000000000000000000000xx
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、 SnapManagerSuite ライセンスをインストールするため、 SnapCenter の追加ライセンスは必要ありません。

## 手順3：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、コントローラのシリアル番号が必要です。ONTAP コマンドラインを使用すると、コントローラのシリアル番号を取得できます。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。

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、出力を確認して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. シリアル番号を記録します。

## 手順4：コントローラベースライセンスのシリアル番号を取得します

FAS または AFF ストレージを使用している場合、ネットアップ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してから、 ONTAP コマンドラインを使用してインストールできます。

作業を開始する前に

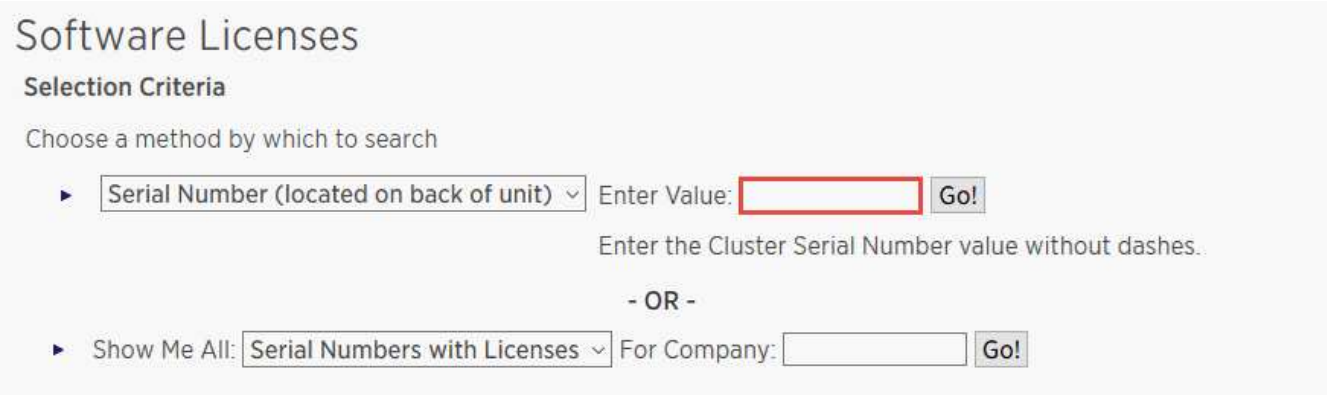
- 有効なネットアップサポートサイトのログインクレデンシャルが必要です。

有効なクレデンシャルを入力しないと、検索結果は返されません。

- コントローラのシリアル番号を確認しておく必要があります。

手順

1. にログインします "ネットアップサポートサイト"。
2. [ システム ] 、 [ * ソフトウェアライセンス ] の順に移動します。
3. [Selection Criteria]領域で、[Serial Number（located on back of unit）]が選択されていることを確認し、コントローラ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 SnapManagerSuite ライセンスを探して記録します。

## 手順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。

作業を開始する前に

- 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 SnapManagerSuite のライセンスが必要です。

このタスクについて

FAS、AFF、またはASAストレージにSnapCenterの試用版をインストールする場合は、Premium Bundleの評価版ライセンスを取得してコントローラにインストールできます。

SnapCenter を試用版としてインストールする場合は、営業担当者にお問い合わせいただき、 Premium Bundle 評価ライセンスを取得してコントローラにインストールしてください。

手順

1. ONTAP コマンドラインを使用してネットアップクラスタにログインします。
2. SnapManagerSuite 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. SnapManagerSuite ライセンスがインストールされていることを確認します。

   「 license show 」を参照してください

### ステップ6:試用版ライセンスを削除します

コントローラベースの SnapCenter 標準ライセンスを使用していて、容量ベースの試用版ライセンス ( シリアル番号は「 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、試用版ライセンスを手動で削除する必要があります。SnapCenter GUI でトライアルライセンスを削除することはできません。

> トライアルライセンスを手動で削除する必要があるのは、 SnapCenter の標準コントローラベースのライセンスを使用している場合のみです。SnapCenter の Standard 容量ベースのライセンスを調達し、 SnapCenter の GUI に追加すると、試用版ライセンスが自動的に上書きされます。

手順

1. SnapCenter サーバで、 PowerShell ウィンドウを開き、 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 サーバとの接続セッションを開始します。
   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、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るプロンプトが MySQL から表示されます。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。

   「 nsm を使用」「 nsm ライセンスから削除」。ここで、 NSM_License_Serial_number='510000050';'

# SnapCenter の Standard 容量ベースのライセンスを追加

## ONTAP Select 標準容量ライセンスは、 Cloud Volumes ONTAP プラットフォームと SnapCenter プラットフォームのデータを保護するために使用します。

容量ライセンスには次のような特徴があります。

- 51xxxxxxx の形式の 9 桁のシリアル番号で構成されます

  SnapCenter GUI を使用してライセンスを有効にするには、ライセンスのシリアル番号と有効なネットアップサポートサイトのログインクレデンシャルを使用します。

- 個別の永続ライセンスとして提供され、使用済みストレージ容量または保護するデータのサイズのいずれか小さい方に基づくコストと、データは SnapCenter によって管理されます

- テラバイトあたりの利用可能容量

  たとえば、 1TB 、 2TB 、 4TB などの容量ベースのライセンスを取得できます。

- 100TB の容量が使用可能な 90 日間の試用版ライセンスです

  必要なライセンスの詳細については、を参照してください "SnapCenter ライセンス"。

SnapCenter は、管理対象の ONTAP Select および Cloud Volumes ONTAP ストレージ上で、 1 日に 1 回、午前 0 時に使用容量を自動的に計算します。Standard 容量ライセンスを使用している場合、 SnapCenter は、ライセンスで許可された合計容量から、すべてのボリュームの使用済み容量を差し引くことによって、未使用の容量を計算します。使用容量がライセンスで許可された容量を超えた場合、 SnapCenter ダッシュボードに警告が表示されます。SnapCenter で容量のしきい値と通知を設定している場合は、使用容量が指定したしきい値に達すると E メールが送信されます。

ステップ**1**：必要な容量を計算する

SnapCenter の容量ベースのライセンスを取得する前に、 SnapCenter で管理するホストの容量を計算する必要があります。

Cloud Volumes ONTAP または ONTAP Select システムのクラスタ管理者である必要があります。

このタスクについて

SnapCenter は、使用済み容量を計算します。ファイルシステムまたはデータベースのサイズが 1TB で、使用スペースが 500GB の場合、 SnapCenter は 500GB の使用容量を計算します。重複排除と圧縮のあとにボリューム容量が計算され、ボリューム全体の使用容量に基づいて算出されます。

手順

1. ONTAP コマンドラインを使用してネットアップコントローラにログインします。
2. 使用済みボリューム容量を表示するには、コマンドを入力します。

```
select::> vol show -fields used -volume Engineering,Marketing
vserver volume       used
------- ------       ------
VS1     Engineering  2.13TB
VS1     Marketing    2.62TB

2   entries were displayed.
```

   2 つのボリュームの使用済み容量の合計が 5TB 未満であるため、 5TB のデータをすべて保護する場合は、 SnapCenter の容量ベースの最小ライセンス要件は 5TB です。

   ただし、合計で 5TB の使用容量のうち 2TB しか保護しない場合は、 2TB の容量ベースライセンスを取得できます。

手順**2**：容量ベースライセンスのシリアル番号を取得します

SnapCenter の容量ベースのライセンスのシリアル番号は、注文の確認やドキュメントパッケージに記載され

ています。このシリアル番号がない場合は、ネットアップサポートサイトから取得できます。

有効なネットアップサポートサイトのログインクレデンシャルが必要です。

手順

1. にログインします "ネットアップサポートサイト"。
2. [ システム ] 、 [ * ソフトウェアライセンス ] の順に移動します。
3. [ 選択基準 ] 領域で、 [ すべてを表示：シリアル番号とライセンス ] ドロップダウンメニューから **SC_standard** を選択します。

4. 会社名を入力し、* Go！*を選択します。

   SnapCenter ライセンスの 9 桁のシリアル番号が 51xxxxxxx の形式で表示されます。

5. シリアル番号を記録します。

ステップ**3**：ネットアップライセンスファイルを生成する

NetApp Support Site のクレデンシャルとSnapCenter ライセンスのシリアル番号をSnapCenter のGUIに入力しない場合や、SnapCenter からNetApp Support Site にインターネットアクセスできない場合は、ネットアップライセンスファイル（NLF）を生成できます。その後、SnapCenter ホストからアクセスできる場所にファイルをダウンロードして格納できます。

作業を開始する前に

- SnapCenter を ONTAP Select または Cloud Volumes ONTAP で使用する必要があります。
- 有効なネットアップサポートサイトのログインクレデンシャルが必要です。
- ライセンスの 9 桁のシリアル番号を 51xxxxxxx の形式で用意しておく必要があります。

手順

1. に移動します "ネットアップライセンスファイルジェネレータ"。
2. 必要な情報を入力します。
3. [ 製品ライン ] フィールドで、プルダウンメニューから **SnapCenter Standard (capacity based-)** を選択します。
4. [ 製品シリアル番号 ] フィールドに、 SnapCenter ライセンスのシリアル番号を入力します
5. ネットアップのデータプライバシーポリシーを読んで同意し、*[送信]*を選択します。

6. ライセンスファイルを保存し、ファイルの場所を記録します。

手順**4**：容量ベースのライセンスを追加する

SnapCenter を ONTAP Select プラットフォームまたは Cloud Volumes ONTAP プラットフォームで使用している場合は、 1 つ以上の SnapCenter 容量ベースのライセンスをインストールする必要があります。

作業を開始する前に

- SnapCenter 管理者ユーザとしてログインする必要があります。
- 有効なネットアップサポートサイトのログインクレデンシャルが必要です。
- ライセンスの 9 桁のシリアル番号を 51xxxxxxx の形式で用意しておく必要があります。

  ネットアップライセンスファイル（ NLF ）を使用してライセンスを追加する場合は、ライセンスファイルの場所を確認しておく必要があります。

このタスクについて

設定ページでは、次のタスクを実行できます。

- ライセンスを追加します
- ライセンスの詳細を表示して、各ライセンスに関する情報を簡単に確認できます。
- ライセンス容量を更新したり、しきい値通知の設定を変更したりする場合など、既存のライセンスを置き換えるときにライセンスを変更します。
- 既存のライセンスを置き換える場合やライセンスが不要になった場合は、ライセンスを削除します。

> トライアルライセンス（ 50 で終わるシリアル番号）は、 SnapCenter GUI では削除できません。購入した SnapCenter Standard 容量ベースのライセンスを追加すると、試用版ライセンスが自動的に上書きされます。

手順

1. 左側のナビゲーションペインで、*[設定]*を選択します。
2. [設定]ページで、*[ソフトウェア]*を選択します。
3. [Software]ページの[License]セクションで、**[Add]**（を選択します ＋ ）。
4. SnapCenter ライセンスの追加ウィザードで、次のいずれかの方法を選択して、追加するライセンスを取得します。

| フィールド | 手順 |
| --- | --- |
| ライセンスをインポートするには、ネットアップサポートサイト（ NSS ）のログインクレデンシャルを入力します | a. NSS のユーザ名を入力します。<br>b. NSS パスワードを入力します。<br>c. コントローラベースのライセンスのシリアル番号を入力します。 |

| フィールド | 手順 |
| --- | --- |
| ネットアップライセンスファイル | a. ライセンスファイルの場所を参照し、選択します。<br>b. 「 * 開く * 」を選択します。 |

5. 通知ページで、 SnapCenter が E メール、 EMS 、および AutoSupport 通知を送信する容量のしきい値を入力します。

   デフォルトのしきい値は 90% です。

6. Eメール通知に使用するSMTPサーバを設定するには、**[設定]>*>**[通知サーバ設定]*を選択し、次の詳細を入力します。

| フィールド | 手順 |
| --- | --- |
| E メール設定 | 「 * Always * 」または「 * Never * 」のいずれかを選択します。 |
| E メールの設定を指定します | [* 常に * （ Always * ） ] を選択した場合は、次のように指定します<br>• 送信者の E メールアドレス<br>• 受信者の E メールアドレス<br>• オプション：デフォルトの件名を編集します<br>デフォルトの件名は「 SnapCenter ライセンス容量通知」です。 |

7. 処理に失敗した場合に Event Management System （ EMS ；イベント管理システム）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選択します。AutoSupport を有効にすると、発生する可能性のある問題のトラブルシューティングに役立つことを推奨します。
8. 「 * 次へ * 」を選択します。
9. 概要を確認し、*[終了]*を選択します。

# ストレージシステムをプロビジョニング

## **Windows** ホストでストレージをプロビジョニングする

### **LUN** ストレージを設定します

SnapCenter を使用して、 FC 接続 LUN または iSCSI 接続 LUN を設定できます。SnapCenter を使用して、既存の LUN を Windows ホストに接続することもできます。

LUN は、 SAN 構成におけるストレージの基本単位です。Windows ホストは、システム上の LUN を仮想ディスクとして認識します。詳細については、を参照してください "ONTAP 9 SAN 構成ガイド"。

**iSCSI** セッションを確立します

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 サービスを開始しておく必要があります。 "詳細はこちら。"
- このタスクについて *

iSCSI セッションは、 IPv6 と IPv6 のどちらか、または IPv4 と IPv4 の同じ IP バージョンの間でのみ確立できます。

iSCSI セッションの管理、およびホストとターゲットの間の通信には、両方が同じサブネット内にある場合にのみ、リンクローカル IPv6 アドレスを使用できます。

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で IP アドレスを使用して SnapCenter への iSCSI セッションを確立したあとで、別の IP アドレスを使用して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、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * iSCSI Session （ iSCSI セッション） * をクリックします。
  3. Storage Virtual Machine * ドロップダウンリストから、 iSCSI ターゲットの Storage Virtual Machine （ SVM ）を選択します。
  4. [**Host**] 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. Establish Session ウィザードで ' ターゲットを指定します

| フィールド | 入力するコマンド |
|---|---|
| ターゲットノード名 | iSCSI ターゲットのノード名<br><br>既存のターゲットノード名がある場合は、その名前が読み取り専用形式で表示されます。 |
| ターゲットポータルのアドレス | ターゲットネットワークポータルの IP アドレス |

| フィールド | 入力するコマンド |
| --- | --- |
| 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 |
| イニシエータポータルのアドレス | イニシエータネットワークポータルの IP アドレス |

7. 入力が完了したら、 * 接続 * をクリックします。

   SnapCenter が iSCSI セッションを確立します。

8. この手順を繰り返して、各ターゲットのセッションを確立します。

#### iSCSI セッションを切断します

複数のセッションを実行しているターゲットから iSCSI セッションを切断しなければならない場合があります。

- 手順 *

1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
2. Hosts （ホスト）ページで、 * iSCSI Session （ iSCSI セッション） * をクリックします。
3. Storage Virtual Machine * ドロップダウンリストから、 iSCSI ターゲットの Storage Virtual Machine （ SVM ）を選択します。
4. [**Host**] 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. iSCSI セッションのリストから、切断するセッションを選択し、 * セッションの切断 * をクリックします。
6. [ セッションの切断 ] ダイアログボックスで、 [OK] をクリックします。

   SnapCenter によって iSCSI セッションが切断されます。

### igroup を作成して管理します

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します。SnapCenter を使用して、 Windows ホストの igroup の作成、名前変更、変更、削除を行うことができます。

#### igroup を作成

SnapCenter を使用して、 Windows ホスト上に igroup を作成できます。igroup を LUN にマッピングすると、ディスクの作成ウィザードまたはディスク接続ウィザードでこの igroup を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、 * Hosts * （ホスト）をクリックします。
2. Hosts 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、 [* 新規作成 ] 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 | 手順 |
| --- | --- |
| ストレージシステム | igroup にマッピングする 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。 |
| igroup 名 | igroup の名前を入力します。 |
| イニシエータ | イニシエータを選択します。 |
| を入力します | 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. 入力に問題がなければ、「 * OK * 」をクリックします。

   SnapCenter により、ストレージシステムに igroup が作成されます。

#### igroup の名前を変更する

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、 * Hosts * （ホスト）をクリックします。
  2. Hosts 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、 * Storage Virtual Machine * 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、 * Rename * 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 を変更する

SnapCenter を使用すると、既存の igroup にイニシエータを追加できます。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、 igroup を変更して他のノードをその igroup に追加します。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. Hosts 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、 * Storage Virtual Machine * 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、 * イニシエータを igroup に追加 * をクリックします。
5. ホストを選択します。
6. イニシエータを選択し、 * OK * をクリックします。

#### igroup を削除する

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

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. Hosts 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、 * Storage Virtual Machine * 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、 * Delete * 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 によって igroup が削除されます。

### ディスクを作成および管理する

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 では基本ディスクのみがサポートされます。ダイナミックディスクはサポートされていません。
- GPT には、 NTFS または CSVFS でフォーマットされたボリュームとマウントパスが 1 つのボリュームを含むデータパーティションと MBR 1 つのプライマリパーティションのみが許可されます。
- サポートされ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、ディスク名の変更はサポートされていません。SnapCenter で管理しているディスクの名前を変更すると、 SnapCenter 処理は正常に終了しません。

#### ホスト上のディスクを表示します

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、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * Disks （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。

クラスタディスクを表示します

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。クラスタ化されたディスクは、Hosts （ホスト）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、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * Disks （ディスク） * をクリックします。
  3. [**Host**] ドロップダウン・リストからクラスタを選択します

     ディスクのリストが表示されます。

**FC** 接続または **iSCSI** 接続の **LUN** またはディスクを作成します

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 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 と CSVFS ファイルシステムのみがサポートされます。

作業を開始する前に

- 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 は、ディスクを作成するホストにのみインストールする必要があります。
- 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、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * Disks （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
  4. [ 新規作成（ New ） ] をクリックする。

Create Disk （ディスクの作成）ウィザードが開きます。

5. LUN Name ページで、 LUN を特定します。

| フィールド | 手順 |
| --- | --- |
| ストレージシステム | LUN の SVM を選択します。 |
| LUN パス | 「 * Browse * 」をクリックして、 LUN を含むフォルダのフルパスを選択します。 |
| LUN 名 | LUN の名前を入力します。 |
| クラスタサイズ | クラスタの LUN のブロック割り当てサイズを選択します。<br><br>クラスタのサイズは、オペレーティングシステムとアプリケーションによって異なります。 |
| LUN ラベル | 必要に応じて、 LUN の説明を入力します。 |

6. ディスクタイプページで、ディスクタイプを選択します。

| 選択するオプション | 状況 |
| --- | --- |
| 専用ディスク | LUN にアクセスできるホストは 1 つだけです。<br><br>[* リソースグループ * ] フィールドは無視してください。 |
| 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。<br><br>[ * リソースグループ * ] フィールドにクラスタ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する必要があります。 |
| Cluster Shared Volume （ CSV ；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で LUN を共有します。<br><br>[ * リソースグループ * ] フィールドにクラスタリソースグループの名前を入力します。ディスクを作成するホストがクラスタグループの所有者であることを確認します。 |

7. ドライブのプロパティページで、ドライブのプロパティを指定します。

| プロパティ（ **Property** ） | 説明 |
| --- | --- |
| マウントポイントの自動割り当て | SnapCenter では、システムドライブに基づいてボリュームマウントポイントが自動的に割り当てられます。<br><br>たとえば、システムドライブが C: の場合、自動割り当てでは C: ドライブ (C:\scmnpt) の下にボリュームマウントポイントが作成されます。自動割り当ては共有ディスクではサポートされません。 |
| ドライブ文字を割り当てます | 隣接する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。 |
| ボリュームマウントポイントを使用する | 隣接する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。<br><br>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。 |
| ドライブレターまたはボリュームマウントポイントを割り当てないでください | ディスクを Windows で手動でマウントする場合は、このオプションを選択します。 |
| LUN サイズ | LUN のサイズを 150MB 以上指定します。<br><br>ドロップダウンリストから MB 、 GB 、または TB を選択します。 |
| この LUN をホストしているボリュームにシンプロビジョニングを使用します | LUN をシンプロビジョニングします。<br><br>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。<br><br>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（ **Property** ） | 説明 |
| --- | --- |
| パーティションタイプを選択します | 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。<br><br>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、原因のミスアライメントが発生することがあります。<br><br>UEFI （ Unified Extensible Firmware Interface ）パーティションディスクはサポートされていません。 |

8. LUN のマッピングページで、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 | 手順 |
| --- | --- |
| 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。<br><br>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。 |
| ホストイニシエータを選択します | Fibre Channel * または * iSCSI * を選択し、ホスト上のイニシエータを選択します。<br><br>FC で Multipath I/O （ MPIO ；マルチパス I/O ）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用に新しい igroup を作成します | 選択したイニシエータ用に新しい igroup を作成します。 |

| 選択するオプション | 状況 |
| --- | --- |
| 既存の igroup を選択するか、選択したイニシエータ用に新しい igroup を指定します | 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。<br><br>igroup name * 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 によって 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できます。

- このタスクについて *
- シンプロビジョニングされた LUN の場合、 ONTAP の LUN ジオメトリサイズは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のサイズ変更前に作成されたSnapshotからLUNをリストアする必要がある場合は、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。

  リストア処理後、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、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * Disks （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. 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. ディスクのサイズ変更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、サイズ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する場合は、 [ 縮小 ] または [ 展開 ] ボタンを適切に有効にする前に、 [ サイズ ] フィールドの外側をクリックする必要があります。また、単位を指定するには、 MB 、 GB 、または TB をクリック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（ * Shrink ） ] または [ * 展開（ * Expand ） ] をクリックします。

   SnapCenter はディスクのサイズを変更します。

ディスクを接続します

ディスク接続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。

作業を開始する前に

- 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。
- Cluster Shared Volume （ CSV ；クラスタ共有ボリューム）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、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * Disks （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
  4. [ 接続 ] をクリックします。

     ディスクの接続ウィザードが開きます。

  5. LUN Name ページで、接続先の LUN を特定します。

| フィールド | 手順 |
|---|---|
| ストレージシステム | LUN の SVM を選択します。 |
| LUN パス | [* Browse] をクリックして、 LUN を含むボリュームの完全パスを選択します。 |
| LUN 名 | LUN の名前を入力します。 |

| フィールド | 手順 |
| --- | --- |
| クラスタサイズ | クラスタの LUN のブロック割り当てサイズを選択します。<br><br>クラスタのサイズは、オペレーティングシステムとアプリケーションによって異なります。 |
| LUN ラベル | 必要に応じて、 LUN の説明を入力します。 |

6. ディスクタイプページで、ディスクタイプを選択します。

| 選択するオプション | 状況 |
| --- | --- |
| 専用ディスク | LUN にアクセスできるホストは 1 つだけです。 |
| 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。<br><br>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 ；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で LUN を共有します。<br><br>ディスクを接続するホストがクラスタグループの所有者であることを確認します。 |

7. ドライブのプロパティページで、ドライブのプロパティを指定します。

| プロパティ（ **Property** ） | 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。<br><br>たとえば、システムドライブが C: の場合、自動割り当てプロパティは C: ドライブ (C:\scmnpt) の下にボリュームマウントポイントを作成します。自動割り当てプロパティは共有ディスクではサポートされません。 |
| ドライブ文字を割り当てます | 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。 |

| プロパティ（ **Property** ） | 説明 |
| --- | --- |
| ボリュームマウントポイントを使用する | 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。<br><br>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。 |
| ドライブレターまたはボリュームマウントポイントを割り当てないでください | ディスクを Windows で手動でマウントする場合は、このオプションを選択します。 |

8. LUN のマッピングページで、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 | 手順 |
| --- | --- |
| 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。<br><br>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。 |
| ホストイニシエータを選択します | Fibre Channel * または * iSCSI * を選択し、ホスト上のイニシエータを選択します。<br><br>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用に新しい igroup を作成します | 選択したイニシエータ用に新しい igroup を作成します。 |
| 既存の igroup を選択するか、選択したイニシエータ用に新しい igroup を指定します | 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。<br><br>igroup name * 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 は、ホスト上の指定したドライブまたはドライブパスに LUN を接続します。

ディスクの切断

LUN は内容を残したままホストから切断できます。ただし、スプリットせずにクローンを切断した場合、クローンの内容は失われます。

作業を開始する前に

- 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機能しており、 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 が作成した 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 はボリュームを削除します。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ときは、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、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * Disks （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. 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。

ディスクを削除します

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、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * Disks （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. 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** 共有を作成および管理する

## 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： * SnapCenter に付属のテンプレートを利用して共有の設定を自動化できるため、コマンドレットの使用を推奨します。

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、提供されているモデルに従って独自のテンプレートを作成できます。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

SnapCenter 共有ページを使用すると、 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 のサポートはプロビジョニングのみに限定されます。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （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. Storage Virtual Machine * ドロップダウンリストから SVM を選択します。
  4. [ 新規作成（ New ） ] をクリックする。

     [ 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 | 手順 |
|---|---|
| 説明 | 共有の説明を入力します。 |
| 共有名 | 共有名を入力します（例： test_share ）。<br><br>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。<br><br>共有名：<br><br>• UTF-8 文字列である必要があります。<br>• 0x00 から 0x1F までの制御文字、 0x22 （二重引用符）、および特殊文字の「 \ / [ ] ：（縦棒） <> + = ；、 ？」は使用できません |

| フィールド | 手順 |
| --- | --- |
| 共有パス | • フィールド内をクリックして、新しいファイルシステムパス（ / など）を入力します。<br>• フィールドをダブルクリックして、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. 入力に問題がなければ、「 * OK * 」をクリックします。

   SnapCenter により、 SVM に SMB 共有が作成されます。

#### 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、 * Hosts * （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、 * Storage Virtual Machine * フィールドをクリックして、ドロップダウンと使用可能な Storage Virtual Machine （ SVM ）のリストを表示し、削除する共有の SVM を選択します。
  4. SVM 上の共有のリストから削除する共有を選択し、 * Delete * 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 によって SVM から SMB 共有が削除されます。

### ストレージシステム上のスペースを再生する

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 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 サーバへの接続を確立する必要があります。

作業を開始する前に

- リストア処理を実行する前に、スペース再生プロセスが完了していることを確認する必要があります。
- 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 PowerShell コマンドプロンプトで、次のコマンドを入力します。

「 Invoke-NaSdHostVolumeSpaceReclaim - Path drive_path 」です

drive_path は、 LUN にマッピングされているドライブパスです。

**PowerShell** コマンドレットを使用してストレージをプロビジョニング

SnapCenter GUI を使用してホストのプロビジョニングやスペース再生のジョブを実行しない場合は、 SnapCenter Plug-in for Microsoft Windows から提供される 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 Open-SMConnection コマンドレットを実行して SnapCenter サーバ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ついては、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "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 をサーバから削除したために SnapCenter PowerShell コマンドレットが破損した場合は、を参照してください "SnapDrive コマンドレットは、 SnapCenter for Windows をアンインストールすると解除されます"。

## **VMware** 環境でストレージをプロビジョニング

VMware環境では、SnapCenter Plug-in for Microsoft Windowsを使用して、LUNの作成と管理やSnapshotの管理を行うことができます。

サポートされている **VMware** ゲスト **OS** プラットフォーム

- サポートされている Windows Server のバージョン
- 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 準仮想 SCSI コントローラをサポートします。RDM ディスクでは 256 本のディスクをサポートできます。

サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

#### VMware ESXi サーバ関連の制限事項

- ESXi クレデンシャルを使用して仮想マシン上の Microsoft クラスタに Plug-in for Windows をインストールすることはできません。

  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て、新しく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 RDM の処理に必要な最小限の vCenter 権限

ゲスト OS で RDM の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：ファイルを削除します
- ホスト： [Configuration] > [Storage Partition] の順に選択します
- 仮想マシン：構成

これらの権限は、 Virtual Center Server 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るロールは、 root 権限を持たないユーザには割り当てることができません。

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 クラスタで FC RDM LUN を管理します

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ことができます。そのためには、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 以降では、 ESX の iSCSI ハードウェアや FCoE ハードウェアを使用して Microsoft クラスタを管理することもできます。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、特定の構成要件を満たしていれば、 2 つの異なる ESX サーバまたは ESXi サーバに属する 2 台の仮想マシンで構成された Microsoft クラスタで FC RDM LUN の使用がサポートされます。この構成は、クラスタ全体のボックスとも呼ばれます。

- 仮想マシン（ VM ）で同じバージョンの Windows Server を実行している必要があります。
- ESX サーバまたは ESXi サーバのバージョンが VMware の各親ホストで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 サーバまたは ESXi サーバ間で VMFS （ VMware Virtual Machine File System ）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 上に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設定されている必要があります。

  Windows Server 2008 R2 では、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。

  > 物理互換モードで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 の * Create a new disk* オプションではなく、 * Raw Device Mappings * （ 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 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

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** を作成

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、を参照してください "物理ホスト間で仮想マシンをクラスタ化します"。

# SnapCenter サーバとの安全な MySQL 接続を設定します

SnapCenter サーバと MySQL サーバ間の通信をスタンドアロン構成または Network Load Balancing （ NLB ）構成で保護する場合は、 Secure Sockets Layer （ SSL ）証明書とキーファイルを生成できます。

## スタンドアロン SnapCenter サーバ構成用にセキュアな MySQL 接続を設定します

SnapCenter サーバと MySQL サーバ間の通信を保護する場合は、 Secure Sockets Layer （ SSL ）証明書およびキーファイルを生成できます。証明書とキーファイルは MySQL Server 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 上の 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セットアップします。

   詳細については、を参照してください "MySQL バージョン 5.7 ： openssl を使用した SSL 証明書およびキーの作成"

   > 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される共通名の値は、CA 証明書に使用される共通名の値と異なる必要があります。共通名の値が同じ場合、OpenSSL を使用してコンパイルされたサーバーの証明書とキーファイルは失敗します。

* ベストプラクティス： * サーバ証明書の共通名として、サーバの Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を使用してください。

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

   デフォルトの MySQL Data フォルダパスは、 C ： \ProgramData\NetApp\SnapCenter \MySQL Data\Data\`` です。

3. MySQL サーバ構成ファイル（ my.in ）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 サーバ構成ファイル（ my.in ）のパスは「 C ： \ProgramData\NetApp\SnapCenter \MySQL Data\my.ini` 」です。

   MySQL サーバ構成ファイル（ my.in ）の [mysqld] セクションで、 CA 証明書、サーバパブリック証明書、サーバ秘密鍵のパスを指定する必要があります。

   MySQL サーバ構成ファイル（ my.in ）の [client] セクションで、 CA 証明書、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のパスを指定する必要があります。

   次の例は、 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デフォルトフォルダ「 C ： /ProgramData\NetApp/SnapCenter /MySQL Data\Data] に示しています。

```
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. インターネットインフォメーションサーバー (IIS) で SnapCenter サーバーの 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. web.config ファイルで MySQLProtocol キーの値を更新します。

   次の例は、 web.config ファイルで更新された MySQLProtocol キーの値を示しています。

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

7. my.ini ファイルの [client] セクションに指定されたパスで web.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" />
```

1. IIS で SnapCenter サーバー Web アプリケーションを起動します。

## HA 構成用にセキュアな MySQL 接続を設定します

SnapCenter サーバと MySQL サーバ間の通信を保護する場合は、ハイアベイラビリティ（ HA ）ノードの両方について Secure Sockets Layer （ SSL ）証明書とキーファイルを生成できます。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

  いずれかの HA ノードで CA 証明書が生成され、この CA 証明書がもう一方の HA ノードにコピーされます。

- 両方の HA ノードのサーバパブリック証明書とサーバの秘密鍵ファイル
- 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. 最初の HA ノードに対して、 openssl コマンドを使用して、 Windows 上の 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セットアップします。

   詳細については、を参照してください "MySQL バージョン 5.7 ： openssl を使用した SSL 証明書およびキーの作成"

   > 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される共通名の値は、CA 証明書に使用される共通名の値と異なる必要があります。共通名の値が同じ場合、OpenSSL を使用してコンパイルされたサーバーの証明書とキーファイルは失敗します。

   * ベストプラクティス： * サーバ証明書の共通名として、サーバの Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を使用してください。

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

   MySQL のデフォルトのフォルダパスは、 C ： \ProgramData\NetApp\SnapCenter \MySQL Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\\です 。

3. MySQL サーバ構成ファイル（ my.in ）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 サーバ構成ファイル（ my.in l ）のパスは、 C ： \ProgramData\NetApp\SnapCenter \MySQL Data\my.in です

   > MySQL サーバ構成ファイル（ my.in ）の [mysqld] セクションで、 CA 証明書、サーバパブリック証明書、サーバ秘密鍵のパスを指定する必要があります。

   MySQL サーバ構成ファイル（ my.in ）の [client] セクションで、 CA 証明書、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のパスを指定する必要があります。

   次の例は、 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。このデフォルトフォルダは C ： /ProgramData\NetApp/SnapCenter /MySQL Data\Data です。

   ```
   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 ノードについて、 CA 証明書をコピーし、サーバのパブリック証明書、サーバの秘密鍵ファイル、クライアントのパブリック証明書、およびクライアントの秘密鍵ファイルを生成します。次の手順を実行します。

   a. 1 つ目の HA ノードで生成された CA 証明書を、 2 つ目の NLB ノードの MySQL Data フォルダにコピーします。

      MySQL のデフォルトのフォルダパスは、 C ： \ProgramData\NetApp\SnapCenter \MySQL Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\Data\\です 。

      > 再度 CA 証明書を作成することはできません。作成するのは、サーバのパブリック証明書、クライアントのパブリック証明書、サーバの秘密鍵ファイル、およびクライアントの秘密鍵ファイルだけにしてください。

   b. 最初の HA ノードに対して、 openssl コマンドを使用して、 Windows 上の 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セットアップします。

      "MySQL バージョン 5.7 ： openssl を使用した SSL 証明書およびキーの作成"

      > 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される共通名の値は、 CA 証明書に使用される共通名の値と異なる必要があります。共通名の値が同じ場合、 OpenSSL を使用してコンパイルされたサーバーの証明書とキーファイルは失敗します。

      サーバ証明書の共通名としてサーバ 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 Data フォルダにコピーします。

   d. MySQL サーバ構成ファイル（ my.in ）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 [mysqld] セクションで、 CA 証明書、サーバパブリック証明書、サーバ秘密鍵のパスを指定する必要があります。

      MySQL サーバ構成ファイル（ my.in ）の [client] セクションで、 CA 証明書、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のパスを指定する必要があります。

      次の例は、 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。このデフォルトフォルダは C ： /ProgramData\NetApp/SnapCenter /MySQL Data\Data です。

```
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 ノードのインターネットインフォメーションサーバ (IIS) で、 SnapCenter サーバ 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 ノードについて、 web.config ファイルで MySQLProtocol キーの値を更新します。

   次の例は、 web.config ファイルで更新された MySQLProtocol キーの値を示しています。

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

8. 両方の HA ノードについて、 my.ini ファイルの [client] セクションで指定したパスで web.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" />
```

1. 両方の HA ノードの IIS で SnapCenter サーバー Web アプリケーションを起動します。
2. いずれかの HA ノードで Set-SmRepositoryConfig-RebuildSlave -Force PowerShell コマンドレットを使用して、両方の HA ノードでセキュアな MySQL レプリケーションを確立します。

   レプリケーションステータスが正常であっても、 -Force オプションを使用してスレーブリポジトリを再構築できます。

# インストール中に **Windows** ホストで有効になる機能

SnapCenter Server インストーラを使用すると、インストール中に Windows ホストで Windows の機能とロールが有効になります。これらの情報は、トラブルシューティングやホストシステムのメンテナンスに役立つ場合があります。

| カテゴリ | フィーチャー（ **Feature** ） |
| --- | --- |
| Web サーバ | • インターネットインフォメーションサービス<br>• World Wide Web Services の略<br>• Common HTTP Features （共通 HTTP 機能）<br>　◦ 既定のドキュメント<br>　◦ ディレクトリの参照<br>　◦ HTTP エラー<br>　◦ HTTP リダイレクション<br>　◦ 静的なコンテンツ<br>　◦ WebDAV 発行<br>• 正常性と診断<br>　◦ カスタムログ<br>　◦ HTTP ログ<br>　◦ ログツール<br>　◦ Request Monitor サービスの略<br>　◦ トレース<br>• パフォーマンス機能<br>　◦ 静的なコンテンツの圧縮<br>• セキュリティ<br>　◦ IP セキュリティ<br>　◦ Basic Authentication の略<br>　◦ 一元的な SSL 証明書のサポート<br>　◦ クライアント証明書マッピング認証<br>　◦ IIS クライアント証明書マッピング認証<br>　◦ IP およびドメインの制限<br>　◦ 要求フィルタリング<br>　◦ URL 承認<br>　◦ Windows 認証<br>• アプリケーション開発機能<br>　◦ .NET 拡張機能 4.5<br>　◦ アプリケーションの初期化<br>　◦ ASP.NET 4.7.2.<br>　◦ サーバー側インクルード<br>　◦ WebSocket プロトコル<br>管理ツール<br>　IIS Management Console の略 |

| カテゴリ | フィーチャー（ **Feature** ） |
| --- | --- |
| IIS 管理スクリプトおよびツール | • IIS 管理サービス<br>• Web 管理ツール |
| .NET Framework 4.7.2の機能 | • .NET Framework 4.7.2<br>• ASP.NET 4.7.2.<br>• Windows Communication Foundation (WCF) HTTP Activation 45<br>◦ TCP のアクティブ化<br>◦ HTTP アクティブ化<br>◦ メッセージキュー（ MSMQ ）のアクティブ化 |
| メッセージキュー | • メッセージキューサービス<br>SnapCenter が作成および管理する MSMQ サービスを他のアプリケーションが使用していないことを確認します。<br>• MSMQ サーバ |
| Windows プロセスアクティブ化サービス | • プロセスモデル |
| 設定 API | すべて |

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。