# SnapCenterサーバーを構成する

SnapCenter software

NetApp
November 06, 2025

# 目次


SnapCenterサーバーを構成する 1
ストレージシステムの追加とプロビジョニング 1
ストレージシステムを追加する 1
ストレージ接続とクレデンシャル 4
Windowsホストでのストレージのプロビジョニング 5
VMware環境でのストレージのプロビジョニング 20
SnapCenter Standardコントローラベース ライセンスの追加 23
ステップ1: SnapManager Suiteライセンスがインストールされているかどうかを確認する 23
ステップ2: コントローラにインストールされているライセンスを識別する 24
ステップ3: コントローラーのシリアル番号を取得する 25
ステップ4: コントローラベースのライセンスのシリアル番号を取得する 26
ステップ5: コントローラベースのライセンスを追加する 27
ステップ6: 試用ライセンスを削除する 28
高可用性の設定 28
SnapCenterサーバを高可用性向けに構成する 28
SnapCenter MySQLリポジトリの高可用性 33
ロールベース アクセス制御（RBAC）の設定 33
ロールの作成 33
セキュリティ ログイン コマンドを使用してNetApp ONTAP RBAC ロールを追加する 34
最小権限でのSVMロールの作成 36
ASA r2 システムの SVM ロールを作成する 41
最小権限でのONTAPクラスタ ロールの作成 46
ASA r2システム用のONTAPクラスタロールを作成する 52
ユーザまたはグループの追加と、ロールとアセットの割り当て 59
監査ログの設定 62
SnapCenter ServerとのセキュアなMySQL接続の設定 63
スタンドアロンSnapCenter Server構成用のセキュアなMySQL接続の設定 63
HA構成用のセキュアなMySQL接続の設定 65

# SnapCenterサーバーを構成する

## ストレージシステムの追加とプロビジョニング

### ストレージシステムを追加する

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

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

開始する前に

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

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

- ストレージ システムの名前は一意である必要があります。

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

このタスクについて

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

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

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

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

手順

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

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

| フィールド | 操作 |
| --- | --- |
| Event Management System (EMS) & AutoSupport Settings | 保護が適用されたとき、リストア処理が完了したとき、または処理が失敗したときにEMSメッセージをストレージ システムのsyslogに送信、またはAutoSupportメッセージをストレージ システムに送信するには、該当するチェックボックスをオンにします。<br><br>失敗した操作に関する**AutoSupport**通知をストレージ システムに送信する チェックボックスをオンにすると、 AutoSupport通知を有効にするには EMS メッセージングが必要であるため、* SnapCenter Server イベントを syslog に記録する* チェックボックスもオンになります。 |

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

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

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

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

   a. [Protocol]で、SVMまたはクラスタのセットアップ時に設定したプロトコル（通常はHTTPS）を選択します。
   b. ストレージ システムが受け入れるポートを入力します。

      通常はデフォルト ポート443を使用します。

   c. 接続を試行する時間（秒）を入力します。

      デフォルト値は60秒です。

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

5. *送信*をクリックします。

結果

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

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

  FSx SVMを追加した場合は、ここにFSx SVMが表示されます。

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

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

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

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

終わったら

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

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

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

## ストレージ接続とクレデンシャル

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

ストレージ接続

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

**Credentials**

- ドメイン管理者または管理者グループの任意のメンバー

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

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

- ローカル管理者（ワークグループの場合のみ）

  ワークグループに属するシステムの場合は、SnapCenterプラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザ アカウントに昇格された権限がある場合、またはホスト システムでユーザ アクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカル ユーザ アカウントを指定できます。

ユーザー名フィールドの有効な形式は次のとおりです: *UserName*

- 個々のリソース グループのクレデンシャル

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

## Windowsホストでのストレージのプロビジョニング

### igroupの作成と管理

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

#### igroupの作成

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

手順

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

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

5. 入力内容に満足したら、「**OK**」をクリックします。

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

#### igroupの名前の変更

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

手順

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

#### igroupの変更

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

手順

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

#### igroupを削除する

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

手順

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

   SnapCenter はigroup を削除します。

ディスクの作成と管理

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

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

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

### ホスト上のディスクの表示

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

手順

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

   ディスクのリストが表示されます。

### クラスタ ディスクの表示

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

手順

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

   ディスクのリストが表示されます。

### **iSCSI**セッションの確立

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

始める前に

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

このタスクについて

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

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

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

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

手順

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

   セッションの確立ウィザードが表示されます。

6. セッションの確立ウィザードで、ターゲットを特定します。

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

7. 入力内容に満足したら、「接続」をクリックします。

   SnapCenter はiSCSI セッションを確立します。

8. 同じ手順を繰り返して各ターゲットのセッションを確立します。

#### FC接続またはiSCSI接続のLUNまたはディスクの作成

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

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

開始する前に

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

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

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

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

このタスクについて

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

手順

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

   [Create Disk]ウィザードが開きます。

5. [LUN Name]ページで、LUNの情報を指定します。

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

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

6. [Disk Type]ページで、ディスク タイプを選択します。

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

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

| プロパティ | 説明 |
| --- | --- |
| マウントポイントの自動割り当て | システム ドライブに基づいて、SnapCenterで自動的にボリューム マウント ポイントを割り当てます。<br><br>たとえば、システム ドライブがC:であれば、C:ドライブにボリューム マウント ポイント（C:\scmnpt\）が作成されます。自動割り当ては共有ディスクではサポートされません。 |
| Assign drive letter | ドロップダウン リストで選択したドライブにディスクをマウントします。 |
| Use volume mount point | フィールドで指定したドライブ パスにディスクをマウントします。<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。 |
| Do not assign drive letter or volume mount point | ディスクをWindowsで手動でマウントする場合に選択します。 |
| LUN size | LUNサイズ（150MB以上）を指定します。<br><br>ドロップダウン リストで単位（MB、GB、またはTB）を選択します。 |
| Use thin provisioning for the volume hosting this LUN | LUNをシンプロビジョニングします。<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 | 説明 |
| --- | --- |
| Choose partition type | GUIDパーティション テーブルの場合はGPTパーティション、マスター ブート レコードの場合はMBRパーティションを選択します。<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、ミスアライメントが発生することがあります。<br><br>Unified Extensible Firmware Interface（UEFI）パーティション ディスクはサポートされていません。 |

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

| フィールド | 操作 |
| --- | --- |
| ホスト | クラスタ グループ名をダブルクリックし、ドロップダウン リストに表示されたクラスタに属するホストの中から、イニシエータに指定するホストを選択します。<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。 |
| Choose host initiator | ファイバー チャネル または **iSCSI** を選択し、ホスト上のイニシエーターを選択します。<br><br>FCでマルチパスI/O（MPIO）を使用する場合は、FCイニシエータを複数選択できます。 |

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

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

10. 概要ページで選択内容を確認し、「完了」をクリックします。

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

す。

### ディスクのサイズ変更

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

このタスクについて

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

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

手順

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

   ディスクのリストが表示されます。

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

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

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

   SnapCenterによって、ディスクのサイズが変更されます。

### ディスクの接続

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

開始する前に

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

手順

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

   [Connect Disk]ウィザードが開きます。

5. [LUN Name]ページで、接続するLUNの情報を指定します。

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

6. [Disk Type]ページで、ディスク タイプを選択します。

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

| 選択するオプション | 状況 |
| --- | --- |
| 共有ディスク | Windows Serverフェイルオーバー クラスタ内のホストでLUNを共有します。<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) | 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>ディスクはクラスタ グループを所有するホストに接続する必要があります。 |

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

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

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

| フィールド | 操作 |
| --- | --- |
| ホスト | クラスタ グループ名をダブルクリックし、ドロップダウン リストに表示されたクラスタに属するホストの中から、イニシエータに指定するホストを選択します。<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。 |
| Choose host initiator | ファイバー チャネル または **iSCSI** を選択し、ホスト上のイニシエーターを選択します。<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の新しい igroup を作成する | 選択したイニシエータ用に新しいigroupを作成します。 |
| Choose an existing igroup or specify a new igroup for selected initiators | 選択したイニシエータ用に既存のigroupを指定するか、指定した名前で新しいigroupを作成します。<br><br>**igroup** 名 フィールドに igroup 名を入力します。既存のigroup名の最初の数文字を入力すると、残りの文字が自動的に入力されます。 |

10. 概要ページで選択内容を確認し、「完了」をクリックします。

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

ディスクの切断

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

開始する前に

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

このタスクについて

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

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

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

手順

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

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

   SnapCenterによってディスクが切断されます。

ディスクの削除

不要になったディスクは削除できます。削除したディスクは復元できません。

手順

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

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

   SnapCenterによってディスクが削除されます。

**SMB**共有の作成と管理

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

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

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

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

**SMB**共有を作成する

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

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

手順

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

   [新しい共有] ダイアログが開きます。

5. [新しい共有] ダイアログで、共有を定義します。

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

6. 入力内容に満足したら、「**OK**」をクリックします。

   SnapCenter はSVM 上に SMB 共有を作成します。

### SMB共有を削除する

不要になったSMB共有は削除できます。

手順

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

   SnapCenter はSVM から SMB 共有を削除します。

### ストレージ システムでのスペースの再生

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

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

開始する前に

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

  NTFSファイルシステム全体がスキャンされたことを確認してください。

このタスクについて

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

  再生プロセスの実行速度が低下する可能性があります。

ステップ

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

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

drive_pathは、LUNにマッピングされているドライブのパスです。

#### PowerShellコマンドレットを使用したストレージのプロビジョニング

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

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

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

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

## VMware環境でのストレージのプロビジョニング

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

#### サポートされるVMwareゲストOSプラットフォーム

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

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

- RDM LUN

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

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

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

#### VMware ESXiサーバ関連の制限事項

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

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

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

#### SnapCenterのRDMの処理に必要な最小限のvCenter権限

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

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

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

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

### MicrosoftクラスタのFC RDM LUNの管理

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

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

#### 要件

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

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

  共有データストアは、必要に応じてiSCSIで作成することもできます。

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

  共有ストレージに仮想ディスクを使用することはできません。

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

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

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

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

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

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

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

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

#### 制限事項

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

この機能は、ESX 5.5iよりも前のリリースではサポートされていません。

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

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

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

#### 共有**FC RDM LUN**の作成

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

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

# SnapCenter Standardコントローラベース ライセンスの追加

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

コントローラベース ライセンスには次のような特徴があります。

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

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

- コントローラのシリアル番号に紐付けられます。

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

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

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

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

手順

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

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

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

   -

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

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

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

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

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

手順

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

出力例

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

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

Serial Number: 1-81-0000000000000000000000000xx
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、SnapManager Suiteライセンスがインストールされているため、SnapCenterライセンスを設定する必要はありません。

## ステップ**3:** コントローラーのシリアル番号を取得する

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

手順

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

出力例

```
cluster1::> system show -instance

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

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

3. シリアル番号をメモします。

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

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

開始する前に

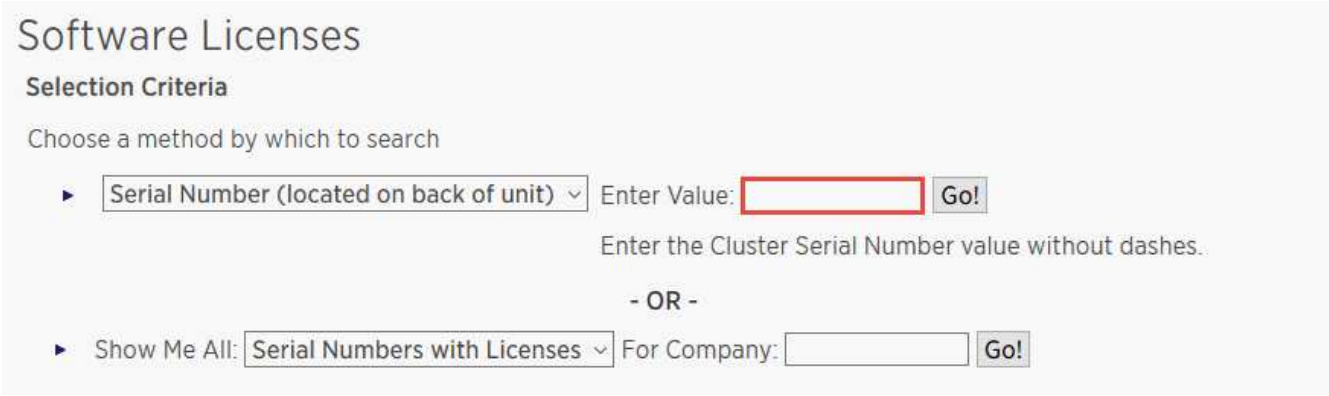
- NetAppサポート サイトの有効なログイン クレデンシャルが必要です。

有効な資格情報を入力しない場合は、検索に対して情報が返されません。

- コントローラのシリアル番号が必要です。

手順

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




指定したコントローラのライセンスのリストが表示されます。

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

## ステップ**5:** コントローラベースのライセンスを追加する

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

開始する前に

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

タスク概要

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

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

手順

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

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

このコマンドは、admin権限レベルで使用できます。

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

```
license show
```

### ステップ6: 試用ライセンスを削除する

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

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

手順

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

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

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

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

3. データベースから試用版ライセンスを削除します。

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

# 高可用性の設定

## SnapCenterサーバを高可用性向けに構成する

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

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

クラウド環境では、Amazon Web Services (AWS) Elastic Load Balancing (ELB) と Azure ロードバランサーの

いずれかを使用して高可用性を構成できます。

#### F5を使用した高可用性の設定

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

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

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

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

追加情報

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

#### ネットワーク負荷分散 **(NLB)** を使用して高可用性を構成する

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

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

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

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

手順

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

e. 完全な機能をテストします。

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

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

**Azure** ロード バランサーを使用して高可用性を構成する

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

手順

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

== 高可用性のために NLB から F5 に切り替える

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

手順

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

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

### SnapCenter MySQLリポジトリの高可用性

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

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

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

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

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

MySQL HA機能に関連する次の制限事項を理解しておく必要があります。

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

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

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

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

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

# ロールベース アクセス制御（RBAC）の設定

## ロールの作成

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

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

手順

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

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

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

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

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

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

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

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

開始する前に

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

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

  フルアクセス権限は、常に最初に付与する必要があります。

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

タスク概要

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

このツールは、ONTAPの権限の適切な設定を自動的に処理します。たとえば、 NetApp ONTAPツールの RBAC User Creator は、すべてのアクセス権限が最初に表示されるように、権限を正しい順序で自動的に追加します。読み取り専用権限を最初に追加し、次にフルアクセス権限を追加すると、ONTAPはフルアクセス権限を重複するものとしてマーキングし、無視します。

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

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

手順

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

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

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

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

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

2. 次のコマンドを入力して、ユーザ名を作成します。

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

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

3. 次のコマンドを入力して、ユーザにロールを割り当てます。

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

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

- <role_name> は、手順 1 で作成したロールの名前です。
- <password> はあなたのパスワードです。パスワードを指定しないと、パスワードの入力を求めるプロンプトが表示されます。

4. 次のコマンドを入力して、ユーザが正しく作成されたことを確認します。

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

   user_nameは、手順3で作成したユーザ名です。

## 最小権限での**SVM**ロールの作成

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

手順

1. ストレージ システムで、ロールを作成してすべての権限を割り当てます。

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

   このコマンドは、権限ごとに実行する必要があります。

2. ユーザを作成してロールを割り当てます。

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

3. ユーザのロックを解除します。

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

### **SVM**ロールの作成と権限の割り当てのための**ONTAP CLI**コマンド

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

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

"job stop" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

"volume offline" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname

"nvme namespace delete" -access all

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

## ASA r2 システムの SVM ロールを作成する

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

手順

1. ストレージ システムで、ロールを作成してすべての権限を割り当てます。

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

   このコマンドは、権限ごとに実行する必要があります。

2. ユーザを作成してロールを割り当てます。

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

3. ユーザのロックを解除します。

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

### SVMロールの作成と権限の割り当てのためのONTAP CLIコマンド

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

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

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

"snapmirror policy add-rule" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname`

"vserver export-policy create" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all

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

## 最小権限での**ONTAP**クラスタ ロールの作成

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

手順

1. ストレージ システムで、ロールを作成してすべての権限を割り当てます。

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

   このコマンドは、権限ごとに実行する必要があります。

2. ユーザを作成してロールを割り当てます。

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

3. ユーザのロックを解除します。

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

### クラスタ ロールの作成と権限の割り当てのための**ONTAP CLI**コマンド

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

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`

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

"lun mapping delete" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"system license add" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"vserver cifs share modify" -access all

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

## ASA r2システム用のONTAPクラスタロールを作成する

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

手順

1. ストレージ システムで、ロールを作成してすべての権限を割り当てます。

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

   このコマンドは、権限ごとに実行する必要があります。

2. ユーザを作成してロールを割り当てます。

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

3. ユーザのロックを解除します。

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

クラスタ ロールの作成と権限の割り当てのための**ONTAP CLI**コマンド

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

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

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"network interface create" -access readonly

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all

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

"volume clone split start" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"vserver export-policy rule modify" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "storage-unit show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "consistency-group" show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror protect" show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume delete" show" -access all

## ユーザまたはグループの追加と、ロールとアセットの割り当て

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

開始する前に

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

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

- SnapCenterには、事前定義されたロールが複数あります。

  これらのロールをユーザに割り当てるか、新しいロールを作成できます。

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

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

- RBACの権限と効率性を活用するためには、いずれかの時点でユーザまたはグループにロールを割り当てる必要があります。
- ユーザまたはグループの作成時に、ホスト、リソース グループ、ポリシー、ストレージ接続、プラグイン、クレデンシャルなどのアセットをユーザに割り当てることができます。
- 特定の処理を実行するためにユーザに割り当てる必要がある最小アセットは次のとおりです。

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

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

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

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

  ユーザにアクセスを割り当てる前にアセットを追加しておいてください。

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

手順

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

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

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

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

   c. 必要なすべてのアセットについて、同じ手順を繰り返します。

d. *保存*をクリックします。

5. *送信*をクリックします。

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

# 監査ログの設定

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

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

「SnapCenterAdmin」ロールでログインする必要があります。

タスク概要

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

  共有ドライブやネットワーク マウント ドライブは、サポートされていません。
- syslogサーバの設定でUDPプロトコルを使用している場合、ポートが停止している、または使用できないことによるエラーは、SnapCenterでエラーまたはアラートとして取得できません。
- 監査ログを構成するには、Set-SmAuditSettings コマンドと Get-SmAuditSettings コマンドを使用できます。

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

手順

1. 設定*ページで、*設定 > グローバル設定 > *監査ログ設定*に移動します。
2. [Audit log]セクションで、詳細を入力します。
3. *監査ログディレクトリ*と*監査チェックサムログディレクトリ*を入力します。

a. [Maximum file size]を入力します。

b. [Maximum log files]を入力します。

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

4. (オプション) **UTC** 時間のログ を有効にします。

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

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

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

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

   a. syslogサーバのホストを入力します。

   b. syslogサーバのポートを入力します。

   c. syslogサーバのプロトコルを入力します。

   d. RFCの形式を入力します。

7. *保存*をクリックします。

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

# SnapCenter ServerとのセキュアなMySQL接続の設定

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

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

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

次の証明書が生成されます。

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

手順

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## HA構成用のセキュアなMySQL接続の設定

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

次の証明書が生成されます。

- CA証明書

一方のHAノードでCA証明書を生成し、もう一方のHAノードにコピーします。

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

手順

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

+

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

+

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

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

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

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

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

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

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

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

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

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

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

## 著作権に関する情報



## 商標に関する情報