SnapCenterサーバーを構成する

SnapCenter software

NetApp
February 20, 2026

目次

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

データ保護とプロビジョニングの処理を実行するために、SnapCenterからONTAPストレージ、ASA R2システム、またはAmazon FSx for NetApp ONTAPへのアクセスを許可するストレージシステムをセットアップする必要があります。

スタンドアロンのSVMを追加することも、複数のSVMで構成されるクラスタを追加することもできます。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を追加するか、SnapCenterでFSx SVMを追加できます。

開始する前に

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

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

- ストレージシステム名は一意である必要があります。

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

- このタスクについて *
- ストレージシステムを設定する際に、イベント管理システム（EMS）およびAutoSupportの機能を有効にすることもできます。AutoSupportツールは、システムの健常性に関するデータを収集し、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、リストアまたはクローニング処理が正常に終了したとき、または処理が失敗したときに、SnapCenterからストレージシステムにAutoSupport情報が、ストレージシステムのsyslogにEMSメッセージが送信されます。

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

> ストレージシステムのパスワードを変更すると、スケジュールされたジョブ、オンデマンドバックアップ、およびリストア処理が失敗することがあります。ストレージ・システムのパスワードを変更した後、 Storage （ストレージ）タブで * Modify （変更） * をクリックしてパスワードを更新できます。

- 手順 *

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

フィールド	操作
ストレージシステム	ストレージシステムの名前またはIPアドレスを入力します。 ストレージシステム名は、ドメイン名を含めずに15文字以下にする必要があり、解決可能な名前である必要があります。15文字を超える名前のストレージシステム接続を作成するには、Add-SmStorageConnectionPowerShellコマンドレットを使用します。 MetroCluster構成（MCC）のストレージシステムでノンストップオペレーションを実現するには、ローカルクラスタとピアクラスタの両方を登録することを推奨します。 SnapCenter では、異なるクラスタにある同じ名前の SVM は複数サポートされません。SnapCenter でサポートされる SVM には、それぞれ一意の名前を付ける必要があります。 SnapCenter へのストレージ接続の追加後は、 ONTAP を使用して SVM またはクラスタの名前を変更しないでください。 SVM に短い名前または FQDN を追加した場合は、 SnapCenter とプラグインホストの両方から解決できる必要があります。
ユーザ名 / パスワード	ストレージシステム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
イベント管理システム（EMS）とAutoSupportの設定	保護が適用された場合、リストア処理が完了した場合、または処理が失敗した場合にEMSメッセージをストレージシステムのsyslogに送信したり、AutoSupportメッセージをストレージシステムに送信したりする場合は、該当するチェックボックスを選択します。 AutoSupport 通知を有効にするには AutoSupport メッセージが必要であるため、 ［* 失敗した処理に対する SnapCenter 通知をストレージ・システムに送信する *］ チェックボックスをオンにすると、 ［* サーバ・イベントを syslog に記録する *］ チェックボックスもオンになります。

4. プラットフォーム、プロトコル、ポート、およびタイムアウトに割り当てられたデフォルト値を変更する場合は、 [その他のオプション *] をクリックします。
   a. [プラットフォーム]で、ドロップダウンリストからいずれかのオプションを選択します。

      SVM がバックアップ関係のセカンダリストレージシステムの場合は、 * Secondary * チェックボックスを選択します。[* Secondary] オプションを選択すると、 SnapCenter はすぐにライセンスチェックを実行しません。

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

a. [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。

   通常はデフォルトのポート443を使用できます。

c. 通信の試行が停止するまでの経過時間を秒単位で入力します。

   デフォルト値は60秒です。

d. SVM に複数の管理インターフェイスがある場合は、「 * 優先 IP 」チェックボックスを選択し、 SVM 接続用の優先 IP アドレスを入力します。
e. [保存（ Save ）] をクリックします。
   1. [Submit （送信）] をクリックします。

- 結果 *

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

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

  FSx SVMを追加した場合は、ここにFSx SVMが表示されます。

- 追加されたすべてのクラスタを表示するには、「 * ONTAP クラスタ * 」を選択します。

  fsxadminを使用してFSxクラスタを追加した場合は、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、クラスタに含まれるすべての SVM が SVM セクションに表示されます。

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

- 終了後 *

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。そのためには、ストレージシステムのコマンドラインから次のコマンドを実行します。

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

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

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サーバと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

ストレージ接続により、SnapCenter ServerプラグインとSnapCenterプラグインはONTAPストレージにアクセスできます。これらの接続の設定には、AutoSupportおよびEvent Management System（EMS；イベント管理システム）機能の設定も含まれます。

クレデンシャル

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

- ローカル管理者（ワークグループのみ）

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

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

- 個 々 のリソースグループのクレデンシャル

  個 々 のリソースグループのクレデンシャルを設定し、ユーザ名に完全なadmin権限がない場合は、少なくともリソースグループとバックアップ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します。SnapCenter を使用して、 Windows ホストの igroup の作成、名前変更、変更、削除を行うことができます。

igroupを作成する

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

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

フィールド	操作
ストレージシステム	igroup にマッピングする LUN の SVM を選択します。
ホスト	igroupを作成するホストを選択します。
igroup名	igroupの名前を入力します。
イニシエータ	イニシエータを選択します。
タイプ	イニシエータタイプ、iSCSI、FCP、または混在（FCPとiSCSI）を選択します。

  5. 入力に問題がなければ、「 * OK * 」をクリックします。

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

igroupの名前を変更する

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

- 手順 *

1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
2. Hosts ページで、 * igroup * をクリックします。
3. イニシエータグループページで、 * Storage Virtual Machine * フィールドをクリックして使用可能な SVM のリストを表示し、名前を変更する igroup の SVM を選択します。
4. SVM の igroup のリストで、名前を変更する igroup を選択し、 * Rename * をクリックします。
5. igroup の名前変更ダイアログボックスで、 igroup の新しい名前を入力し、 * 名前の変更 * をクリックします。

igroupを変更する

SnapCenter を使用すると、既存の igroup にイニシエータを追加できます。igroupの作成時に追加できるホストは1つだけです。クラスタ用のigroupを作成する場合は、igroupを変更してそのigroupに他のノードを追加できます。

- 手順 *

1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
2. Hosts ページで、 * igroup * をクリックします。
3. イニシエータグループページで、 * Storage Virtual Machine * フィールドをクリックして使用可能な SVM のドロップダウンリストを表示し、変更する igroup の SVM を選択します。
4. igroup のリストで igroup を選択し、 * イニシエータを igroup に追加 * をクリックします。
5. ホストを選択します。
6. イニシエータを選択し、 * OK * をクリックします。

igroupを削除する

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

- 手順 *

1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
2. Hosts ページで、 * igroup * をクリックします。
3. イニシエータグループページで、 * Storage Virtual Machine * フィールドをクリックして使用可能な SVM のドロップダウンリストを表示し、削除する igroup の SVM を選択します。
4. SVM の igroup のリストで、削除する igroup を選択し、 * Delete * をクリックします。
5. igroup の削除ダイアログボックスで、 * OK * をクリックします。

   SnapCenter によって igroup が削除されます。

ディスクの作成と管理

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はベーシックディスクのみをサポートします。ダイナミックディスクはサポートされていません。
- GPTの場合は1つのデータパーティションのみ、MBRの場合は1つのプライマリパーティションが許可されます。このパーティションには、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つのマウントパスがあります。
- サポートされるパーティションスタイル： GPT 、 MBR 。 VMware UEFI VM では、 iSCSI ディスクのみがサポートされます

SnapCenter では、ディスク名の変更はサポートされていません。SnapCenter で管理しているディスクの名前を変更すると、 SnapCenter 処理は正常に終了しません。

ホスト上のディスクの表示

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、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * Disks （ディスク） * をクリックします。
  3. [**Host**] ドロップダウン・リストからホストを選択します

     ディスクのリストが表示されます。

クラスタ化ディスクの表示

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

     ディスクのリストが表示されます。

iSCSIセッションを確立する

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ノードをiSCSIターゲットとして定義しておく必要があります。
- ストレージシステムでiSCSIサービスを開始しておく必要があります。 "詳細"
- 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両方が同じサブネット内にある場合にのみ使用できます。

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は、ホストを再起動する必要があります。

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

- 手順 *

1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
2. Hosts （ホスト）ページで、 * iSCSI Session （ iSCSI セッション） * をクリックします。
3. Storage Virtual Machine * ドロップダウンリストから、 iSCSI ターゲットの Storage Virtual Machine （ SVM ）を選択します。
4. [**Host**] ドロップダウン・リストから ' セッションのホストを選択します
5. [セッションの確立] をクリックします。

   セッションの確立ウィザードが表示されます。

6. Establish Session ウィザードで ' ターゲットを指定します

フィールド	入力するコマンド
ターゲットノード名	iSCSIターゲットのノード名 既存のターゲットノード名がある場合は、その名前が読み取り専用形式で表示されます。
ターゲットポータルアドレス	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. 入力が完了したら、 * 接続 * をクリックします。

   SnapCenter が iSCSI セッションを確立します。

8. この手順を繰り返して、ターゲットごとにセッションを確立します。

FC接続またはiSCSI接続のLUNまたはディスクを作成する

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

SnapCenter以外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は、ディスクを作成するホストにのみインストールする必要があります。
- このタスクについて *
- Windows Serverフェイルオーバークラスタ内のホストでLUNを共有しないかぎり、LUNを複数のホストに接続することはできません。
- Cluster Shared Volume（CSV；クラスタ共有ボリューム）を使用するWindows Serverフェイルオーバークラスタ内のホストでLUNを共有する場合は、クラスタグループを所有するホストにディスクを作成する必要があります。
- 手順 *

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

   Create Disk（ディスクの作成）ウィザードが開きます。

5. [LUN Name]ページで、LUNを特定します。

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

フィールド	操作
LUNラベル	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
専用ディスク	LUNにアクセスできるホストは1つだけです。 [* リソースグループ *] フィールドは無視してください。
共有ディスク	Windows Serverフェイルオーバークラスタ内のホストでLUNを共有します。 [* リソースグループ *] フィールドにクラスタリソースグループの名前を入力します。ディスクは、フェイルオーバークラスタ内の1つのホストにのみ作成する必要があります。
クラスタ共有ボリューム（CSV）	CSVを使用するWindows Serverフェイルオーバークラスタ内のホストでLUNを共有します。 [* リソースグループ *] フィールドにクラスタリソースグループの名前を入力します。ディスクを作成するホストがクラスタグループの所有者であることを確認します。

7. [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
マウントポイントを自動割り当て	SnapCenter では、システムドライブに基づいてボリュームマウントポイントが自動的に割り当てられます。 たとえば、システムドライブが C: の場合、自動割り当てでは C: ドライブ (C:\scmnpt) の下にボリュームマウントポイントが作成されます。自動割り当ては共有ディスクではサポートされません。
ドライブ文字の割り当て	ドロップダウンリストで選択したドライブにディスクをマウントします。

プロパティ	説明
ボリュームマウントポイントを使用する	フィールドで指定したドライブパスにディスクをマウントします。 ボリュームマウントポイントのルートは、ディスクを作成するホストが所有している必要があります。
ドライブレターまたはボリュームマウントポイントを割り当てない	Windowsでディスクを手動でマウントする場合は、このオプションを選択します。
LUNサイズ	LUNサイズを指定します（150MB以上）。 ドロップダウンリストでMB、GB、またはTBを選択します。
このLUNをホストするボリュームにシンプロビジョニングを使用する	LUNをシンプロビジョニングします。 シンプロビジョニングでは、一度に必要な量のストレージスペースのみが割り当てられるため、LUNは使用可能な最大容量まで効率的に拡張されます。 必要になると思われるすべてのLUNストレージを格納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。
パーティションタイプを選択	GUIDパーティションテーブルの場合はGPTパーティション、マスターブートレコードの場合はMBRパーティションを選択します。 MBRパーティションは、Windows Serverフェイルオーバークラスタでミスアライメントの問題を引き起こす可能性があります。 Unified Extensible Firmware Interface（UEFI）パーティションディスクはサポートされていません。

8. [Map LUN]ページで、ホスト上の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て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一覧から、イニシエータのホストを選択します。 このフィールドは、Windows Serverフェイルオーバークラスタ内のホストでLUNを共有している場合にのみ表示されます。
ホストイニシエータを選択	Fibre Channel * または * iSCSI * を選択し、ホスト上のイニシエータを選択します。 FCでMultipath I/O（MPIO；マルチパスI/O）を使用している場合は、FCイニシエータを複数選択できます。

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

選択するオプション	状況
選択したイニシエータ用に新しいigroupを作成	選択したイニシエータ用に新しいigroupを作成します。
選択したイニシエータ用に既存のigroupを選択するか、新しいigroupを指定する	選択したイニシエータ用に既存のigroupを指定するか、指定した名前で新しいigroupを作成します。 igroup name * フィールドに igroup 名を入力します。既存のigroup名の最初の数文字を入力すると、このフィールドに自動的に入力されます。

10. [概要] ページで選択内容を確認し、 [完了] をクリックします。

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

ディスクのサイズ変更

ストレージシステムのニーズの変化に応じて、ディスクのサイズを増減できます。

- 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（ボリューム内の利用可能なサイズ）が最大サイズとして表示されます。
- MBRパーティション形式のLUNのサイズの上限は2TBです。

- GPTパーティション形式のLUNのストレージシステムサイズの上限は16TBです。
- LUNのサイズを変更する前にSnapshotを作成しておくことを推奨します。
- LUNのサイズ変更前に作成されたSnapshotからLUNをリストアする必要がある場合は、SnapCenterによってLUNのサイズがSnapshotのサイズに自動的に変更されます。

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

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * Disks （ディスク） * をクリックします。
  3. [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. [ディスクのサイズ変更]ダイアログボックスで、スライダツールを使用してディスクの新しいサイズを指定するか、[サイズ]フィールドに新しいサイズを入力します。

     サイズを手動で入力する場合は、[縮小]または[展開]ボタンを適切に有効にする前に、[サイズ]フィールドの外側をクリックする必要があります。また、単位を指定するには、 MB 、 GB 、または TB をクリックする必要があります。

  6. 入力内容に問題がなければ、必要に応じて、 [* 縮小（ * Shrink ）] または [* 展開（ * Expand ）] をクリックします。

     SnapCenter はディスクのサイズを変更します。

ディスクの接続

[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LUNを共有しないかぎり、LUNを複数のホストに接続することはできません。
- Cluster Shared Volume（CSV；クラスタ共有ボリューム）を使用するWindows Serverフェイルオーバークラスタ内のホストでLUNを共有する場合は、クラスタグループを所有するホストにディスクを接続する必要があります。
- Plug-in for Windows をインストールする必要があるのは、ディスクを接続するホストだけです。
- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。

2. Hosts （ホスト）ページで、 * Disks （ディスク） * をクリックします。
3. [**Host**] ドロップダウン・リストからホストを選択します
4. [接続] をクリックします。

   [Connect Disk]ウィザードが開きます。

5. [LUN Name]ページで、接続先のLUNを特定します。

フィールド	操作
ストレージシステム	LUN の SVM を選択します。
LUNパス	[* Browse] をクリックして、 LUN を含むボリュームの完全パスを選択します。
LUN名	LUN の名前を入力します。
クラスタサイズ	クラスタのLUNブロック割り当てサイズを選択します。 クラスタのサイズは、オペレーティングシステムとアプリケーションによって異なります。
LUNラベル	必要に応じて、LUNの説明を入力します。

6. [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
専用ディスク	LUNにアクセスできるホストは1つだけです。
共有ディスク	Windows Serverフェイルオーバークラスタ内のホストでLUNを共有します。 ディスクはフェイルオーバークラスタ内の1つのホストにのみ接続する必要があります。
クラスタ共有ボリューム（CSV）	CSVを使用するWindows Serverフェイルオーバークラスタ内のホストでLUNを共有します。 ディスクに接続するホストがクラスタグループの所有者であることを確認します。

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

プロパティ	説明
自動割り当て	システムドライブに基づいて、 SnapCenter で自動的にボリュームマウントポイントを割り当てます。 たとえば、システムドライブが C: の場合、自動割り当てプロパティは C: ドライブ (C:\scmnpt) の下にボリュームマウントポイントを作成します。自動割り当てプロパティは共有ディスクではサポートされていません。
ドライブ文字の割り当て	ドロップダウンリストで選択したドライブにディスクをマウントします。
ボリュームマウントポイントを使用する	フィールドで指定したドライブパスにディスクをマウントします。 ボリュームマウントポイントのルートは、ディスクを作成するホストが所有している必要があります。
ドライブレターまたはボリュームマウントポイントを割り当てない	Windowsでディスクを手動でマウントする場合は、このオプションを選択します。

8. [Map LUN]ページで、ホスト上の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て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うち、イニシエータに使用するホストを選択します。 このフィールドは、Windows Serverフェイルオーバークラスタ内のホストでLUNを共有している場合にのみ表示されます。
ホストイニシエータを選択	Fibre Channel * または * iSCSI * を選択し、ホスト上のイニシエータを選択します。 FCでMPIOを使用している場合は、FCイニシエータを複数選択できます。

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

選択するオプション	状況
選択したイニシエータ用に新しいigroupを作成	選択したイニシエータ用に新しいigroupを作成します。
選択したイニシエータ用に既存のigroupを選択するか、新しいigroupを指定する	選択したイニシエータ用に既存のigroupを指定するか、指定した名前で新しいigroupを作成します。 igroup name * フィールドに igroup 名を入力します。既存のigroup名の最初の数文字を入力すると、自動的に入力されます。

10. [概要] ページで選択内容を確認し、 [完了] をクリックします。

    SnapCenter は、ホスト上の指定したドライブまたはドライブパスに LUN を接続します。

ディスクの切断

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

開始する前に

- LUNがどのアプリケーションでも使用されていないことを確認します。
- LUNが監視ソフトウェアで監視されていないことを確認します。
- LUN が共有されている場合は、 LUN からクラスタリソースの依存関係を解除し、クラスタ内のすべてのノードの電源がオンで正常に機能しており、 SnapCenter からアクセスできることを確認します。
- このタスクについて *

SnapCenter が作成した FlexClone ボリュームの LUN を切断した場合、そのボリュームに他の LUN が接続されていなければ、 SnapCenter はボリュームを削除します。この場合、 LUN が切断される前に、 FlexClone ボリュームが削除される可能性があることを警告するメッセージが SnapCenter に表示されます。

FlexCloneボリュームが自動的に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する必要があります。ボリュームの名前を変更するときは、最後の文字だけでなく、複数の文字を変更してください。

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

     ディスクのリストが表示されます。

  4. 切断するディスクを選択し、 * 切断 * をクリックします。
  5. [ディスクの切断] ダイアログボックスで、 [OK] をクリックします。

SnapCenter によってディスクが切断されます。

ディスクの削除

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、 * Hosts * （ホスト）をクリックします。
  2. Hosts （ホスト）ページで、 * Disks （ディスク） * をクリックします。
  3. [**Host**] ドロップダウン・リストからホストを選択します

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

     SnapCenter によってディスクが削除されます。

SMB共有の作成と管理

Storage Virtual Machine（SVM）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します。

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

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

必要に応じて、提供されているモデルに従って独自のテンプレートを作成できます。カスタムテンプレートを作成する前に、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共有ページを使用して、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のサポートはプロビジョニングのみに限定されます。

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

[新しい共有] ダイアログが開きます。

5. [新しい共有] ダイアログで、共有を定義します。

フィールド	操作
説明	共有の説明を入力します。
共有名	共有名を入力します（例：test_share）。 入力した共有名は、ボリューム名としても使用されます。 共有名： • UTF-8文字列である必要があります。 • 次の文字は使用できません：0x00～0x1Fの制御文字（両方を含む）、0x22（二重引用符）、および特殊文字 `\ / [ ] : (vertical bar) < > + = ; , ?`
共有パス	• フィールド内をクリックして、新しいファイルシステムパス（ / など）を入力します。 • フィールドをダブルクリックして、既存のファイルシステムパスのリストから選択します。

6. 入力に問題がなければ、「 * OK * 」をクリックします。

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

SMB共有を削除する

不要になったSMB共有は削除できます。

- 手順 *
  1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
  2. ホストページで、 * 共有 * をクリックします。
  3. 共有ページで、 * Storage Virtual Machine * フィールドをクリックして、ドロップダウンと使用可能な Storage Virtual Machine （ SVM ）のリストを表示し、削除する共有の SVM を選択します。
  4. SVM 上の共有のリストから削除する共有を選択し、 * Delete * をクリックします。
  5. 共有の削除ダイアログボックスで、 * OK * をクリックします。

     SnapCenter によって SVM から SMB 共有が削除されます。

ストレージシステム上のスペースの再生

ファイルが削除または変更されると、NTFSはLUN上の使用可能なスペースを追跡しますが、新しい情報はストレージシステムには報告しません。新しく解放されたブロックがストレージで使用可能と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PowerShellコマンドレットを実行します。

コマンドレットをリモートのプラグインホストで実行する場合は、SnapCenterOpen-SMConnectionコマンドレットを実行してSnapCenterサーバへの接続を確立しておく必要があります。

開始する前に

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

  NTFSファイルシステム全体がスキャンされていることを確認する必要があります。

- このタスクについて *
- 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ホストの使用率が低いときに処理を実行することを推奨します。
- スペース再生では、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。

  再利用プロセスに時間がかかることがあります。

- ステップ *

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

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

drive_pathは、LUNにマッピングされたドライブパスです。

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 Open-SMConnectionコマンドレットを実行してSnapCenterサーバへの接続を確立する必要があります。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

SnapDrive for Windowsがサーバから削除されたためにSnapCenter PowerShellコマンドレットが破損した場

合は、を参照してください "SnapDrive コマンドレットは、 SnapCenter for Windows をアンインストールすると解除されます"。

VMware環境でのストレージのプロビジョニング

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

サポートされるVMwareゲストOSプラットフォーム

- サポートされているバージョンのWindows Server
- Microsoftクラスタ構成

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

- RDM LUN

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

  VMware準仮想SCSIコントローラをサポートします。RDMディスクでは256本のディスクをサポートできます。

VMware ESXiサーバ関連の制限事項

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

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

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

SnapCenter RDMの処理に必要な最小限のvCenter権限

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

- データストア：ファイルを削除します
- ホスト： [Configuration] > [Storage Partition] の順に選択します
- 仮想マシン：構成

これらの権限は、Virtual Center Serverレベルのロールに割り当てる必要があります。これらの権限を割り当てたロールを、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**を管理します。

Plug-in for Windowsを使用して、FC RDM LUNを使用するMicrosoftクラスタを管理できますが、まず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する必要があります。

ESXi 5.5以降では、ESX iSCSIおよびFCoEハードウェアを使用してMicrosoftクラスタを管理することもできます。Plug-in for Windows では、設定作業なしで Microsoft クラスタがサポートされます。

要件

Plug-in for Windows では、特定の構成要件を満たしていれば、 2 つの異なる ESX サーバまたは ESXi サーバに属する 2 台の仮想マシンで構成された Microsoft クラスタで FC RDM LUN の使用がサポートされます。この構成は、クラスタ全体のボックスとも呼ばれます。

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

  必要に応じて、共有データストアをiSCSI経由で作成することもできます。

- 共有RDM LUNが物理互換モードになっている必要があります。
- 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。

- SCSIコントローラは、クラスタ内の各仮想マシンで物理互換モードで構成する必要があります。

  Windows Server 2008 R2では、各仮想マシンで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コントローラのタイプが1つしかなく、すでにC：ドライブに接続されている場合、共有LUNで既存のLSI Logic SASコントローラを使用することはできません。

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

  物理互換モードで仮想マシン上の共有 LUN に SCSI コントローラを追加する場合は、 VMware Infrastructure Client の * Create a new disk* オプションではなく、 * Raw Device Mappings * （ RDM ）オプションを選択する必要があります。

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

  共有クラスタディスクとして使用するRDM LUNを作成する前に、すべてのESXiホストのイニシエータを

含むigroupをストレージコントローラ上に作成する必要があります。

- 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を使用して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のどちらかである必要があります。両方は使用できません。
- 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ていません。
- 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には、まず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する必要があります。

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。

関連情報

"Broadcom技術ドキュメント"を参照し、物理ホスト間での仮想マシンのクラスタリングと、Microsoft クラスタ用の共有 FC RDM LUN の作成に関するドキュメントを検索します。

SnapCenter Standardコントローラベースライセンスを追加

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。

- Premium Bundle または Flash Bundle （ベースパックには含まれません）の購入に SnapCenter Standard のライセンスが含まれます。
- 無制限のストレージ使用量
- 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ロックされています

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

手順1：SnapManager Suiteライセンスがインストールされているかどうかを確認します

SnapCenter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、追加したすべての SVM またはクラスタを表示するかどうかを選択します。
   - 追加されたすべての SVM を表示するには、 * ONTAP SVM * を選択します。
   - 追加されたすべてのクラスタを表示するには、 * ONTAP クラスタ * を選択します。

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

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

   - FAS、AFF、またはASAプライマリストレージシステムにSnapManager Suiteライセンスがインストールされていることを示します。
   - FAS、AFF、またはASAプライマリストレージシステムにSnapManager Suiteライセンスがインストールされていないことを示します。
   - [Not Applicable]は、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ストレージコントローラがあるため、SnapManager Suiteライセンスが適用されないことを示します。

手順2：コントローラにインストールされているライセンスを特定します

ONTAPコマンドラインを使用して、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、 SnapManagerSuite ライセンスをインストールするため、 SnapCenter の追加ライセンスは必要ありません。

手順3：コントローラのシリアル番号を取得します

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、出力を確認してコントローラのシリアル番号を特定します。

   出力例

```
cluster1::> system show -instance

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

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

3. シリアル番号を記録します。

手順4：コントローラベースライセンスのシリアル番号を取得します

FAS、 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

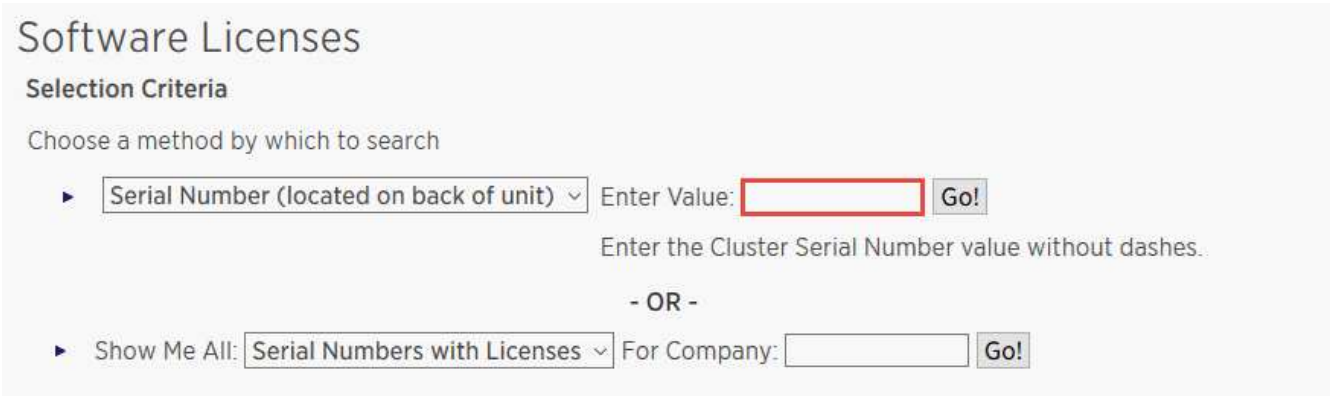
- NetAppサポートサイトの有効なログインクレデンシャルが必要です。

  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. にログインし "NetAppサポートサイト"ます。
2. [システム] 、 [* ソフトウェアライセンス] の順に移動します。
3. [Selection Criteria]領域で、[Serial Number（located on back of unit）]が選択されていることを確認し、コントローラのシリアル番号を入力して*[Go ！]*を選択します。



   指定したコントローラのライセンスのリストが表示されます。

4. SnapCenter Standard または SnapManagerSuite ライセンスを探して記録します。

手順5：コントローラベースのライセンスを追加する

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

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。

タスクの内容

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

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

手順

1. ONTAP コマンドラインを使用してネットアップクラスタにログインします。
2. 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ていることを確認します。

```
license show
```

ステップ6:試用版ライセンスを削除します

コントローラベースのSnapCenter 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。

トライアルライセンスを手動で削除する必要があるのは、 SnapCenter の標準コントローラベースのライセンスを使用している場合のみです。

手順

1. SnapCenterサーバで、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';
```

ハイアベイラビリティの設定

高可用性を実現するための**SnapCenter**サーバの設定

WindowsまたはLinuxで実行されているSnapCenterでハイアベイラビリティ（HA）をサポートするには、F5ロードバランサをインストールします。F5を使用すると、SnapCenterサーバは、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サーバを設定し、F5ロードバランサを設定する必要があります。

ネットワークロードバランシング（NLB）を設定してSnapCenterハイアベイラビリティを設定することもできます。ハイアベイラビリティ構成にするには、SnapCenterのインストールとは別にNLBを手動で設定する

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ロードバランサを使用して高可用性を設定できます。

F5を使用してハイアベイラビリティを設定する

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 サーバのハイアベイラビリティを設定する方法" 。

次のコマンドレットを使用してF5クラスタを追加および削除するには、（SnapCenterAdminロールが割り当てられていることに加えて）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
- アドSmServer
- 削除- SmServerCluster

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

追加情報

- SnapCenter をインストールしてハイアベイラビリティ用に設定したら、 F5 クラスタ IP を指すように SnapCenter デスクトップのショートカットを編集します。
- SnapCenterサーバ間でフェールオーバーが発生し、既存のSnapCenterセッションも存在する場合は、ブラウザを閉じてSnapCenterに再度ログオンする必要があります。
- ロードバランサのセットアップ（NLBまたはF5）で、NLBまたはF5ホストによって部分的に解決されたホストを追加し、SnapCenterホストがこのホストにアクセスできない場合は、SnapCenterホストページでホストの停止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ホストの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コマンドを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は、監査ログの設定が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、監査ログの設定を手動で繰り返す必要があります。

Network Load Balancing（**NLB**）を使用したハイアベイラビリティの設定

SnapCenterハイアベイラビリティを設定するには、ネットワークロードバランシング（NLB）を設定します。ハイアベイラビリティ構成にするには、SnapCenterのインストールとは別にNLBを手動で設定する必要があります。

SnapCenterを使用したネットワークロードバランシング（NLB）の設定方法については、を参照してください "NLB に SnapCenter を設定する方法"。

AWS Elastic Load Balancing（**ELB**）を使用してハイアベイラビリティを設定

Amazon Web Services（AWS）でハイアベイラビリティSnapCenter環境を設定するには、別 々 のアベイラビリティゾーン（AZ）に2台のSnapCenterサーバをセットアップし、自動フェイルオーバーを設定します。この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、およびアクティブMySQLデータベースとスタンバイ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を設定します。詳細については、を参照して "仮想プライベートオーバーレイIPの設定"ください。
2. Windowsホストの準備
   a. IPv4を強制的にIPv6よりも優先します。
      - 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設定経由で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設定されていないことを確認します。
   d. Active Directoryを使用しないセットアップを使用する場合は、両方のWindows Serverで管理者パスワードが同じで、サーバが1つのドメインにないことを確認してください。
   e. 両方のWindowsサーバに仮想IPを追加します。
3. SnapCenterクラスタを作成
   a. PowerShellを起動し、SnapCenterに接続します。 `Open-SmConnection`
   b. クラスタを作成 `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip> -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator`
   c. セカンダリサーバを追加します。 `Add-SmServer -ServerName <server_name> -ServerIP <server_ip> -CleanUpSecondaryServer -Verbose -Credential administrator`
   d. 高可用性の詳細をご確認ください。 `Get-SmServerConfig`
4. AWS CloudWatchで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備えて、Lamda関数を作成してルーティングテーブルを調整します。詳細については、を参照して "Lambda関数の作成"ください。
5. CloudWatchでモニターを作成して、SnapCenterエンドポイントの可用性を監視します。エンドポイントに到達できない場合にLambda機能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、トラフィックをアクティブなSnapCenterサーバにリダイレクトするようにルーティングテーブルを調整します。詳細については、を参照して "合成カナリアの作成"ください。
6. CloudWatchモニタリングの代わりにSTEP機能を使用してワークフローを実装し、フェールオーバー時間を短縮します。このワークフローには、SnapCenter URLをテストするためのLambdaプローブ関数、失敗カウントを保存するためのDynamoDBテーブル、およびStep関数自体が含まれています。
   a. lambda関数を使用してSnapCenter URLを調べます。詳細については、を参照して "ラムダ関数の作成"ください。
   b. 2つのステップ関数イテレーション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、を参照して "DynamoDBテーブルの使用を開始する"ください。
   c. ステップ機能を作成します。詳細については、を参照して "STEP関数のドキュメント"ください。
   d. 1つ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関数の実行を許可する権限を調整します。

g. ステップ機能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、を参照して "Amazon EventBridge Schedulerを使用したステップ関数の開始"ください。

Azureロードバランサを使用して高可用性を設定する

Azureロードバランサを使用して高可用性SnapCenter環境を構成できます。

手順

1. Azure portal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仮想マシンのスケールセットでは、負荷分散された仮想マシンのグループを作成および管理できます。仮想マシンインスタンスの数は、要求や定義されたスケジュールに応じて自動的に増減できます。詳細については、を参照して "Azure portalを使用してスケールセットに仮想マシンを作成する"ください。
2. 仮想マシンを設定したら、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サーバをインストールします。
3. ホスト1にクラスタを作成します。 `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <specify the load balancer front end virtual ip> -PrimarySCServerIP <ip address> -Verbose -Credential <credentials>`
4. セカンダリサーバを追加します。 `Add-SmServer -ServerName <name of node2> -ServerIP <ip address of node2> -Verbose -Credential <credentials>`
5. ハイアベイラビリティ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`

== NLBからF5に切り替えて高可用性を実現

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

- 手順 *

1. F5を使用して高可用性を実現するようにSnapCenterサーバを設定します。 "詳細"です。
2. SnapCenterサーバホストで、PowerShellを起動します。
3. Open-SmConnectionコマンドレットを使用してセッションを開始し、クレデンシャルを入力します。
4. 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サーバを更新します。

   コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

SnapCenter MySQL リポジトリの高可用性

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

SnapCenter は、マスターリポジトリに対して読み取りまたは書き込み操作を実行し、マスターリポジトリに障害が発生した場合はスレーブリポジトリに接続をルーティングします。その後、スレーブリポジトリがマスターリポジトリになります。SnapCenter は逆方向のレプリケーションもサポートしており、これはフェイルオーバー時にのみ有効になります。

MySQLのハイアベイラビリティ（HA）機能を使用する場合は、1つ目のノードでNetwork Load Balancer（NLB）を設定する必要があります。MySQLリポジトリは、インストール時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場合は、1つ目のノードのF5に参加し、2つ目のノードにMySQLリポジトリのコピーを作成する必要があります。

SnapCenter には、 MySQL レプリケーションを管理するための _Get-SmRepositoryConfig_and _Set -SmRepositoryConfig_PowerShell コマンドレットが用意されています。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

MySQL HA 機能に関連する次の制限事項を確認しておく必要があります。

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

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

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

  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つ目のノードにフェイルオーバーすると、以降のジョブはすべて正常に実行されます。

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

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 ロールに加えて、独自のロールを作成して権限をカスタマイズでき

ます。

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

   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が表示されないようにするには、このオプションの選択を解除してください。

   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するユーザにオブジェクトまたはリソースへのアクセス権を割り当てる必要はありません。

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

security login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clustered ONTAPを実行している場合は、security login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（あるいはその両方）に権限を付与します。

  各コマンド/コマンドディレクトリには、フルアクセスと読み取り専用の2つのアクセスレベルがあります。

  フルアクセス権限は必ず最初に割り当てる必要があります。

- ユーザにロールを割り当てます。
- SnapCenter プラグインがクラスタ全体の 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。

タスクの内容

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 Privilegesの正しく設定を自動的に処理します。たとえば、RBAC User Creator for NetApp ONTAPツールでは、フルアクセスのPrivilegesが最初に表示されるように、Privilegesが正しい順序で自動的に追加されます。最初に読み取り専用Privilegesを追加してからフルアクセスPrivilegesを追加すると、ONTAPはフルアクセスPrivilegesを重複としてマークし、無視します。

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

ONTAP RBACロールの設定の詳細については、を参照してください "ONTAP 9管理者認証とRBACパワーガイド"。

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。空白のままにすると、デフォルトでクラスタ管理者が設定されます。
   - role_nameは、ロールに指定する名前です。
   - commandはONTAP機能です。

     > このコマンドは権限ごとに繰り返す必要があります。フルアクセスコマンドは、読み取り専用コマンドの前に指定する必要があります。

   権限のリストについては、を参照してください "ロールの作成と権限の割り当てに使用するONTAP CLIコマンド"。

2. 次のコマンドを入力して、ユーザ名を作成します。

   ```
   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、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 で作成したユーザの名前です。このコマンドでは、ロールに関連付けるユー

ザを変更できます。

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

4. 次のコマンドを入力して、ユーザが正しく作成されたことを確認します。

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

user_nameは、手順3で作成したユーザの名前です。

最小限の権限で**SVM**ロールを作成する

ONTAP で新しい SVM ユーザのロールを作成する場合、実行する必要がある ONTAP CLI コマンドがいくつかあります。ONTAP 内の SVM を SnapCenter で使用するように設定し、 vsadmin ロールを使用したくない場合、このロールが必要です。

- 手順 *

1. ストレージシステムで、ロールを作成し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繰り返す必要があります。

1. ユーザを作成し、そのユーザにロールを割り当てます。

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

2. ユーザのロックを解除します。

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

SVMロールの作成と権限の割り当て用の**ONTAP CLI**コマンド

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

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

"job 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システム用のSVMロールの作成

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繰り返す必要があります。

1. ユーザを作成し、そのユーザにロールを割り当てます。

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

2. ユーザのロックを解除します。

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

SVMロールの作成と権限の割り当て用のONTAP CLIコマンド

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

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

最小限の権限で**ONTAP**クラスタロールを作成する

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

- 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繰り返す必要があります。

1. ユーザを作成し、そのユーザにロールを割り当てます。

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

2. 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用の**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があるONTAP CLIコマンドがいくつかあります。

- `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クラスタロールの作成

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

- 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繰り返す必要があります。

1. ユーザを作成し、そのユーザにロールを割り当てます。

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

2. 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用の**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があるONTAP CLIコマンドがいくつかあります。

- `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を追加してロールとアセットを割り当てる

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。ロールによって、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で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を使用してこれらのアカウントを作成することはできません。

ユーザ名とグループ名に使用できる特殊文字は、スペース（）、ハイフン（-）、アンダースコア（_）、コロン（:）です。

- SnapCenter には、事前定義されたロールが複数あり

  これらのロールをユーザに割り当てるか、新しいロールを作成できます。

- SnapCenter RBACに追加する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。
- 適切な権限が割り当てられたユーザまたはグループにロールを割り当てたら、ホストやストレージ接続などの SnapCenter アセットへのユーザアクセスを割り当てる必要があります。

これにより、ユーザは自分に割り当てられているアセットに対して権限のある操作を実行できます。

- RBACの権限と効率性を活用するには、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。
- 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、 ユーザまたはグループの作成時のユーザに対するクレデンシャル。
- 特定の処理を実行するためにユーザに割り当てる必要がある最小アセットは次のとおりです。

操作	アセットの割り当て
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
リソースグループを作成	ホスト

- WindowsクラスタまたはDAG（Exchange Server Database Availability Group）アセットに新しいノードを追加したときに、この新しいノードがユーザに割り当てられている場合は、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ユーザまたはグループをクラスタまたはDAGに再割り当てして、新しいノードをRBACユーザまたはグループに追加する必要があります。たとえば、2ノードクラスタにRBACユーザまたはグループを割り当てているとします。クラスタに別のノードを追加した場合は、RBACユーザまたはグループをクラスタに再割り当てして、RBACユーザまたはグループに新しいノードを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ボリュームとデスティネーションボリュームの両方に対するストレージ接続を割り当てる必要があります。

  ユーザにアクセスを割り当てる前にアセットを追加する必要があります。

SnapCenter Plug-in for VMware vSphereの機能を使用してVM、VMDK、またはデータストアを保護する場合は、VMware vSphere GUIを使用してSnapCenter Plug-in for VMware vSphereロールにvCenterユーザを追加する必要があります。VMware vSphereのロールについては、を参照してください "SnapCenter Plug-in for VMware vSphereに付属の事前定義されたロール"。

- 手順 *

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. [設定]ページで、**[ユーザーとアクセス]>**をクリックします。
3. [Add Users/Groups from Active Directory or Workgroup] ページで、次の手順を実行します。

フィールド	操作
アクセスタイプ	[ドメイン]または[ワークグループ]を選択します。 [ドメイン]認証タイプの場合は、ロールにユーザを追加するユーザまたはグループのドメイン名を指定する必要があります。 デフォルトでは、ログインしているドメイン名があらかじめ入力されています。 信頼されていないドメインは、 [* 設定 * > * グローバル設定 * > * ドメイン設定 * （ * Settings * > * Global Settings * ）] ページで登録する必要があります。
タイプ	[ユーザ]または[グループ]を選択します SnapCenter でサポートされるのはセキュリティグループのみで、配信グループはサポートされません。
ユーザー名	a. 部分的なユーザー名を入力し、 * 追加 * をクリックします。 ユーザ名では大文字と小文字が区別されます。 b. 検索リストからユーザ名を選択します。 別のドメインまたは信頼されていないドメインのユーザを追加する場合は、ドメイン間ユーザの検索リストがないため、ユーザ名を完全に入力する必要があります。 この手順を繰り返して、選択したロールにユーザまたはグループを追加します。
役割	ユーザを追加するロールを選択します。

4. [**Assign**] をクリックし、 [Assign Assets] ページで次の手順を実行します。
   a. [* アセット *] ドロップダウン・リストからアセットのタイプを選択します。
   b. [アセット]テーブルで、アセットを選択します。

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

c. 必要なすべてのアセットについて、この手順を繰り返します。

d. [保存（ Save ）] をクリックします。

5. [Submit （送信）] をクリックします。

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

監査ログの設定

監査ログは、SnapCenterサーバのすべてのアクティビティについて生成されます。デフォルトでは、監査ログはインストールされているデフォルトの場所である_ C：\Program Files\NetApp\Virtual \SnapCenter WebApp\audit_にあります。

監査ログは、すべての監査イベントに対してデジタル署名されたダイジェストを生成して保護することで保護され、不正な変更から保護されます。生成されたダイジェストは別の監査チェックサムファイルで保持され、その下ではコンテンツの整合性を保証するために定期的な整合性チェックが行われます。

「SnapCenterAdmin」ロールでログインしておく必要があります。

タスクの内容

- 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スケジュールまたはsyslogサーバが有効または無効になっています
  - 監査ログの整合性チェック、監査ログ、またはsyslogサーバログの障害
  - ディスクスペースが少ない
- 整合性チェックに失敗した場合にのみEメールが送信されます。
- 監査ログディレクトリと監査チェックサムログディレクトリの両方のパスを同時に変更する必要があります。いずれか1つだけを変更することはできません。
- 監査ログディレクトリと監査チェックサムログディレクトリのパスを変更すると、以前の場所にある監査ログで整合性チェックを実行できません。
- 監査ログディレクトリと監査チェックサムログディレクトリのパスは、SnapCenterサーバのローカルドライブに配置する必要があります。

  共有ドライブまたはネットワークマウントドライブはサポートされていません。

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

  コマンドレットで使用できるパラメータとその説明は、Get-Help Command_nameを実行して確認できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

手順

1. [設定]ページで、[設定]>[グローバル設定]>[監査ログ設定]の順に選択します。
2. [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*および*監査チェックサム・ログ・ディレクトリ*を入力します
   a. 最大ファイルサイズを入力します
   b. ログファイルの最大数を入力
   c. アラートを送信するためのディスクスペース使用量のパーセンテージを入力します
4. （任意）*Log UTC time *をイネーブルにします。
5. （オプション）* Audit Log Integrity Check Schedule を有効にし、 Start Integrity Check * for On Demand integrity checkをクリックします。

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

6. （オプション）リモートsyslogサーバへの転送監査ログを有効にし、syslogサーバの詳細を入力します。

   TLS 1.2プロトコルの場合、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サーバホストの入力
   b. syslogサーバポートの入力
   c. syslogサーバプロトコルの入力
   d. RFC形式の入力
7. [保存（ Save ）] をクリックします。
8. 監査整合性チェックとディスク領域チェックは、* Monitor **>** Jobs *をクリックすると表示できます。

SnapCenterサーバとのセキュアなMySQL接続の設定

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

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

SnapCenter サーバと MySQL サーバ間の通信を保護する場合は、 Secure Sockets Layer （ SSL ）証明書およびキーファイルを生成できます。証明書とキーファイルは MySQL Server と SnapCenter Server で設定する必要があります。

次の証明書が生成されます。

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

  1. opensslコマンドを使用して、Windows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。

詳しくは、を参照してください。 "MySQL バージョン 5.7 ： openssl を使用した SSL 証明書およびキーの作成"

> サーバ証明書、クライアント証明書、およびキーファイルに使用される共通名の値は、それぞれCA証明書に使用される共通名の値と異なる必要があります。共通名の値が同じ場合、OpenSSLを使用してコンパイルされたサーバの証明書とキーファイルは失敗します。

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

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

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

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

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

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

   MySQL サーバ構成ファイル（ my.in ）の [client] セクションで、 CA 証明書、クライアントパブリック証明書、およびクライアント秘密鍵のパスを指定する必要があります。

   次の例では、デフォルトフォルダ内のmy.iniファイルの[mysqld]セクションに証明書とキーファイルがコピーされ `C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data`ています。

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

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

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

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

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

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

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

4. インターネットインフォメーションサーバー (IIS) で SnapCenter サーバーの Web アプリケーションを停止します。
5. MySQLサービスを再起動します。
6. MySQLProtocolキーの値をSnapManager .Web.UI.dll.configファイルで更新します。

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

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

7. my.iniファイルの[client]セクションに指定されているパスを使用して、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" />
```

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

HA構成用のセキュアなMySQL接続の設定

SnapCenterサーバとMySQLサーバ間の通信を保護する場合は、高可用性（HA）ノードの両方に対してSecure Sockets Layer（SSL）証明書とキーファイルを生成できます。証明書とキーファイルは、MySQLサーバとHAノードで設定する必要があります。

次の証明書が生成されます。

- CA証明書

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

- 両方のHAノードのサーバパブリック証明書とサーバ秘密鍵ファイル
- 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サーバとクライアントのSSL証明書とキーファイルを設定します。

   詳しくは、を参照してください。 "MySQL バージョン 5.7 ： openssl を使用した SSL 証明書およびキーの作成"

   > サーバ証明書、クライアント証明書、およびキーファイルに使用される共通名の値は、それぞれCA証明書に使用される共通名の値と異なる必要があります。共通名の値が同じ場合、OpenSSLを使用してコンパイルされたサーバの証明書とキーファイルは失敗します。

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

2. SSL証明書とキーファイルをMySQL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.in）で、CA証明書、サーバパブリック証明書、クライアントパブリック証明書、サーバ秘密鍵、およびクライアント秘密鍵のパスを更新します。

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

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

   MySQL サーバ構成ファイル（ my.in ）の [client] セクションで、 CA 証明書、クライアントパブリック証明書、およびクライアント秘密鍵のパスを指定する必要があります。

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

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

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

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

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

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

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

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

4. 2つ目のHAノードで、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ノードで生成されたCA証明書を2つ目のNLB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証明書は今後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、およびクライアント秘密鍵ファイルのみを作成する必要があります。

   b. 1つ目のHAノードで、openssl コマンドを使用して、WindowsのMySQLサーバとクライアントの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 証明書およびキーの作成"

      サーバ証明書、クライアント証明書、およびキーファイルに使用される共通名の値は、それぞれCA証明書に使用される共通名の値と異なる必要があります。共通名の値が同じ場合、OpenSSLを使用してコンパイルされたサーバの証明書とキーファイルは失敗します。

      サーバ証明書の共通名としてサーバの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.in）で、CA証明書、サーバパブリック証明書、クライアントパブリック証明書、サーバ秘密鍵、およびクライアント秘密鍵のパスを更新します。

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

MySQL サーバ構成ファイル（ my.in ）の [client] セクションで、 CA 証明書、クライアントパブリック証明書、およびクライアント秘密鍵のパスを指定する必要があります。

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

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

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

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

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

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

+

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

+

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

5. 両方のHAノードのインターネットインフォメーションサーバ（IIS）でSnapCenterサーバWebアプリケーションを停止します。
6. 両方のHAノードでMySQLサービスを再起動します。
7. 両方のHAノードのMySQLProtocolキーの値をSnapManager .Web.UI.dll.configファイルで更新します。

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

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

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

1. 両方のHAノードのIISでSnapCenterサーバWebアプリケーションを起動します。
2. 一方のHAノードでSet-SmRepositoryConfig -RebuildSlave -Force PowerShellコマンドレットに-Forceオプションを指定して使用し、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。

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