SnapCenterサーバのインストール

SnapCenter Software 6.0

NetApp
September 23, 2024

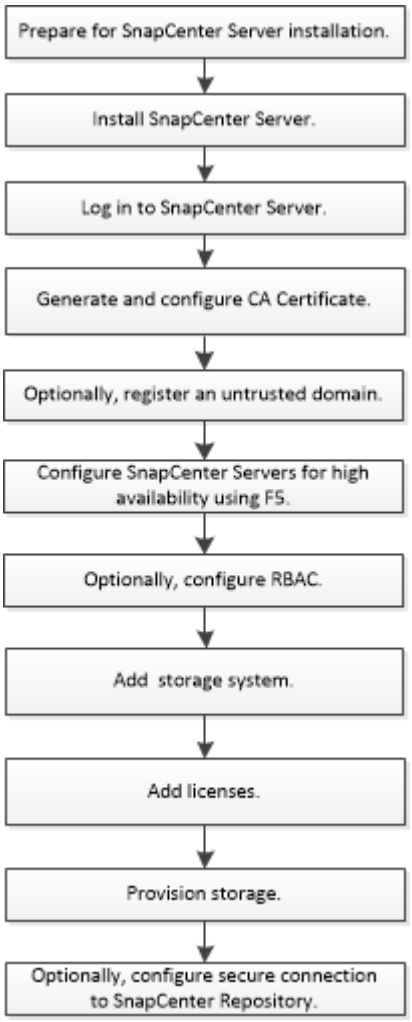
目次

SnapCenterサーバのインストール . . . 1
- インストールワークフロー . . . 1
- SnapCenterサーバのインストールの準備 . . . 1
- WindowsホストへのSnapCenterサーバのインストール . . . 24
- LinuxホストへのSnapCenterサーバのインストール . . . 26
- RBAC許可を使用したSnapCenterへのログイン . . . 30
- WindowsホストのCA証明書の設定 . . . 34
- LinuxホストのCA証明書の設定 . . . 38
- Windowsホストで双方向SSL通信を設定して有効にする . . . 39
- Linuxホストでの双方向SSL通信の設定と有効化 . . . 43
- 証明書ベースの認証の設定 . . . 45
- Active Directory、LDAP、LDAPSの設定 . . . 48
- ハイアベイラビリティの設定 . . . 51
- ロールベースアクセス制御（RBAC）の設定 . . . 54
- 監査ログの設定 . . . 72
- ストレージシステムを追加する . . . 73
- SnapCenter Standardコントローラベースライセンスを追加 . . . 77
- ストレージシステムのプロビジョニング . . . 82
- SnapCenterサーバとのセキュアなMySQL接続の設定 . . . 101
- インストール時にWindowsホストで有効になる機能 . . . 107
- インストルチユウニLinuxホストテユウコウニナルキノウ . . . 110

SnapCenterサーバのインストール

インストールワークフロー

このワークフローは、SnapCenterサーバのインストールと設定に必要なさまざまなタスクを示しています。



SnapCenterサーバのインストールの準備

ドメインとワークグループの要件

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

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

- * Active Directory ドメイン *

ローカル管理者の権限を持つドメインユーザを使用する必要があります。ドメインユーザは、Windowsホストのローカル管理者グループのメンバーである必要があります。

- * ワークグループ *

  ローカル管理者の権限を持つローカルアカウントを使用する必要があります。

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

SnapCenter サーバをインストールしたあとに、 SnapCenter ホストが配置されているドメインを変更しないでください。SnapCenter サーバをインストールした時点のドメインから SnapCenter サーバホストを削除して、 SnapCenter サーバをアンインストールしようとすると、アンインストール処理は失敗します。

スペースとサイジングの要件

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

項目	**Windows**ホストノヨウケン	**Linux** ホストの要件
オペレーティングシステム	Microsoft Windows 英語版、ドイツ語版、日本語版、簡体字中国語版のみがサポートされています。 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool"。	• Red Hat Enterprise Linux（RHEL）8および9 • SUSE Linux Enterprise Server（SLES）15 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool"。
最小CPU数	4コア	4コア
最小RAM	8GB MySQL Serverのバッファプールは、RAMの合計容量の20%を使用します。	8GB

項目	**Windows**ホストノヨウケン	**Linux** ホストの要件
SnapCenter サーバソフトウェアおよびログ用のハードドライブの最小容量	7GB SnapCenterサーバがインストールされているドライブと同じドライブにSnapCenterリポジトリがある場合は、15 GBを使用することを推奨します。	15GB
SnapCenterリポジトリ用の最小ハードドライブ容量	8GB メモ： SnapCenter リポジトリがインストールされているドライブに SnapCenter サーバがある場合は、15GB にすることを推奨します。	該当なし
必要なソフトウェアパッケージ	• Microsoft .NET Framework 4.7.2以降 • ASP。 Net Core Hosting Bundle（8.0.5以降） • PowerShell 7.4.2以降 用。 NET固有のトラブルシューティング情報。を参照してください。 "インターネットに接続されていないレガシーシステムでは、SnapCenter のアップグレードまたはインストールが失敗します"	• ASP。 Net Core Runtime 8.0.5以降 • PowerShell 7.4.2以降 • nginxはリバースプロキシとして使用できるWebサーバ • PAM -デベル PAM（Pluggable Authentication Modules）は、システム管理者が認証を行うプログラムを再コンパイルすることなく認証ポリシーを設定できるシステムセキュリティツールです。

SANホストの要件

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

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

- ホストユーティリティ

  Host UtilitiesはFCとiSCSIをサポートしており、WindowsサーバでMPIOを使用できます。詳細については、を参照してください "Host Utilities のマニュアル"。

- Microsoft DSM for Windows MPIO

  このソフトウェアは、Windows MPIOドライバと連携して、NetAppとWindowsホストコンピュータ間の複数のパスを管理します。

  ハイアベイラビリティ構成にはDSMが必要です。

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

サポートされるストレージシステムとアプリケーション

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

- SnapCenterは、データを保護するためにONTAP 9 12.1以降をサポートしています。
- SnapCenterはAmazon FSx for NetApp ONTAPをサポートしており、SnapCenterソフトウェア4.5 P1パッチリリースからデータを保護します。

  Amazon FSx for NetApp ONTAPを使用している場合は、データ保護処理を実行するために、SnapCenterサーバホストプラグインを4.5 P1以降にアップグレードしてください。

  Non-Volatile Memory Express（NVMe）over Transport Control Protocol（TCP）をサポートします。

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

- SnapCenterは、さまざまなアプリケーションやデータベースの保護をサポートしています。

  サポートされているアプリケーションとデータベースの詳細については、を参照してください "NetApp Interoperability Matrix Tool"。

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

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

サポートされるブラウザ

SnapCenterソフトウェアは複数のブラウザで使用できます。

- Chromeバージョン125以降
- Microsoft Edge 110.0.1587.17以降

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

接続とポートの要件

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

- アプリケーションは1つのポートを共有できません。

  各ポートは、適切なアプリケーション専用にする必要があります。

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

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

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

次の表に、各ポートとそのデフォルト値を示します。

ポートのタイプ	デフォルトポート
SnapCenterポート	8146（HTTPS）、URL _\https://server:8146_のように双方向、カスタマイズ可能 SnapCenter クライアント（ SnapCenter ユーザ）と SnapCenter サーバ間の通信に使用されます。プラグインホストから SnapCenter サーバへの通信にも使用されます。 ポートをカスタマイズするには、を参照してください。 "インストールウィザードを使用してSnapCenterサーバをインストールします。"
SnapCenter SMCore通信ポート	8145（HTTPS）、双方向、カスタマイズ可能 このポートは、 SnapCenter サーバと SnapCenter プラグインがインストールされているホストの間の通信に使用されます。 ポートをカスタマイズするには、を参照してください。 "インストールウィザードを使用してSnapCenterサーバをインストールします。"

ポートのタイプ	デフォルトポート
スケジューラサービスポート	8154（HTTPS） このポートは、SnapCenterサーバホスト内で管理されるすべてのプラグインのSnapCenterスケジューラワークフローを一元的にオーケストレーションするために使用されます。 ポートをカスタマイズするには、を参照してください。 "インストールウィザードを使用してSnapCenterサーバをインストールします。"
RabbitMQポート	5672（TCP） これはRabbitMQがリッスンするデフォルトポートで、スケジューラサービスとSnapCenter間のパブリッシャ/サブスクライバモデル通信に使用されます。
MySQLのポート	3306（HTTPS）、双方向、カスタマイズ可能 このポートは、SnapCenterとMySQLリポジトリデータベースの間の通信に使用されます。 SnapCenterサーバからMySQLサーバへのセキュアな接続を確立できます。 "詳細" ポートをカスタマイズするには、を参照してください。 "インストールウィザードを使用してSnapCenterサーバをインストールします。"
Windowsプラグインホスト	135、445（TCP） ポート135と445に加えて、Microsoftが指定したダイナミックポート範囲もオープンにする必要があります。リモートインストール操作では、このポート範囲を動的に検索するWindows Management Instrumentation（WMI）サービスを使用します。 サポートされるダイナミックポート範囲については、を参照してください。 "Windows のサービス概要とネットワークポート要件" ポートは、 SnapCenter サーバとプラグインをインストールするホストとの間の通信に使用されます。プラグインパッケージのバイナリをWindowsプラグインホストにプッシュするには、プラグインホストでのみポートを開く必要があり、インストール後に閉じることができます。

ポートのタイプ	デフォルトポート
LinuxまたはAIXプラグインホスト	22（SSH） ポートは、 SnapCenter サーバとプラグインをインストールするホストとの間の通信に使用されます。プラグインパッケージのバイナリを Linux または AIX プラグインのホストにコピーするために SnapCenter で使用されます。これらのポートを開いておくか、ファイアウォールまたは iptables から除外しておく必要があります。
SnapCenter Plug-ins Package for Windows 、SnapCenter Plug-ins Package for Linux 、SnapCenter Plug-ins Package for AIX	8145（HTTPS）、双方向、カスタマイズ可能 このポートは、SMCoreとプラグインパッケージがインストールされているホストの間の通信に使用されます。 通信パスも、 SVM 管理 LIF と SnapCenter サーバの間で開いている必要があります。 ポートをカスタマイズするには、またはを参照してください。 "ホストを追加してSnapCenter Plug-in for Microsoft Windowsをインストールする" "ホストを追加してLinuxまたはAIX用のSnapCenter Plug-insパッケージをインストールします。"
SnapCenter Plug-in for Oracle Database	27216、カスタマイズ可能 デフォルトのJDBCポートは、Oracleデータベースへの接続にOracle用プラグインで使用されます。 ポートをカスタマイズするには、を参照してください。 "ホストを追加してLinuxまたはAIX用のSnapCenter Plug-insパッケージをインストールします。"
SnapCenter Plug-in for Exchangeデータベース	909、カスタマイズ可能 デフォルトのNETです。 TCPポートは、Plug-in for WindowsでExchange VSSコールバックに接続するために使用されます。 ポートをカスタマイズするには、を参照してください "ホストを追加してPlug-in for Exchangeをインストールする"。

ポートのタイプ	デフォルトポート
NetAppでサポートされるSnapCenter用プラグイン	9090（HTTPS）、固定 カスタムプラグインホストでのみ使用される内部ポートです。ファイアウォールの例外は必要ありません。 SnapCenterサーバとカスタムプラグインの間の通信は、ポート8145を介してルーティングされます。
ONTAPクラスタまたはSVMの通信ポート	443（HTTPS）、bidirectional80（HTTP）、bidirectional このポートは、SnapCenterサーバを実行するホストとSVMの間の通信にSAL（ストレージ抽象化レイヤ）で使用されます。現在、このポートは、SnapCenterプラグインホストとSVMの間の通信にSnapCenter for Windows Plug-inホストの SALでも使用されています。
SnapCenter Plug-in for SAP HANA Database vCodeのスペルチェックポート	3instance_number13または3instance_number15、HTTPまたはHTTPS、双方向、カスタマイズ可能 マルチテナントデータベースコンテナ（MDC）のシングルテナントの場合、ポート番号は13で終わります。MDC以外の場合、ポート番号は15で終わります。 たとえば、32013はインスタンス20のポート番号で、31015はインスタンス10のポート番号です。 ポートをカスタマイズするには、を参照してください。 "ホストを追加し、プラグインパッケージをリモートホストにインストールする。"
ドメインコントローラの通信ポート	認証が正しく機能するためにドメインコントローラのファイアウォールで開く必要があるポートについては、Microsoftのドキュメントを参照してください。 SnapCenter サーバ、プラグインホスト、またはその他の Windows クライアントがユーザを認証できるように、ドメインコントローラで Microsoft の必要なポートを開く必要があります。

ポートの詳細を変更するには、を参照してください "プラグインホストの変更"。

SnapCenterライセンス

SnapCenterでは、アプリケーション、データベース、ファイルシステム、仮想マシンの

データ保護を実現するために複数のライセンスが必要です。インストールする SnapCenter ライセンスのタイプは、ストレージ環境および使用する機能によって異なります。

ライセンス	必要な場合
SnapCenter Standard（コントローラベース）	FAS、AFF、オールSANアレイ（ASA）に必要 SnapCenter Standardライセンスはコントローラベースのライセンスで、Premium Bundleに含まれています。SnapManager Suiteライセンスをお持ちの場合は、SnapCenter Standardライセンスの使用権も取得できます。FAS、AFF、またはASAストレージにSnapCenterの試用版をインストールする場合は、営業担当者に連絡してPremium Bundleの評価ライセンスを取得してください。 SnapCenterは、Data Protection Bundleの一部としても提供されます。A400以降を購入済みの場合は、Data Protection Bundleを購入する必要があります。
SnapMirrorまたはSnapVault	ONTAP SnapCenterでレプリケーションが有効になっている場合は、SnapMirrorまたはSnapVaultのいずれかのライセンスが必要です。
SnapRestore	バックアップのリストアと検証に必要です。 フライマリストレエシシステム • リモート検証を実行し、バックアップからのリストアを実行するには、SnapVaultデスティネーションシステムに必要です。 • リモート検証を実行するには、SnapMirrorデスティネーションシステムに必要です。

ライセンス	必要な場合
FlexClone	データベースのクローニングおよび検証処理に必要です。 フライマリストレシシステムトセカンタリストレシシステム • セカンダリバックアップからクローンを作成するには、SnapVaultデスティネーションシステムに必要です。 • セカンダリSnapMirrorバックアップからクローンを作成するには、SnapMirrorデスティネーションシステムに必要です。
プロトコル	• LUNのiSCSIまたはFCライセンス • SMB共有用のCIFSライセンス • NFSタイプのVMDK用のNFSライセンス • VMFSタイプのVMDK用のiSCSIまたはFCライセンス ソースボリュームを使用できない場合にデータを提供するには、SnapMirrorデスティネーションシステムに必要です。
SnapCenter Standardライセンス（オプション）	セカンダリデスティネーション セカンダリデスティネーションにSnapCenter Standardライセンスを追加することを推奨しますが、必須ではありません。セカンダリデスティネーションでSnapCenter Standardライセンスが有効になっていない場合、フェイルオーバー処理の実行後にSnapCenterを使用してセカンダリデスティネーションでリソースをバックアップすることはできません。ただし、クローニング処理と検証処理を実行するには、セカンダリデスティネーションに FlexClone ライセンスが必要です。

SnapCenter Advanced および SnapCenter NAS ファイルサービスのライセンスは廃止され、現在は提供されていません。Amazon FSx for NetApp ONTAPおよびCloud Volumes ONTAPでは、容量ベースのライセンスは不要になりました。Azure NetApp Filesには標準ライセンスと容量ベースライセンスは必要ありません。

1つ以上のSnapCenterライセンスをインストールする必要があります。ライセンスの追加方法については、を

参照してください "SnapCenter Standardコントローラベースライセンスを追加"。

Single Mailbox Recovery（SMBR）ライセンス

SnapCenter Plug-in for Exchangeを使用してMicrosoft Exchange Serverデータベースおよび Single Mailbox Recovery（SMBR）を管理する場合は、SMBR用の追加ライセンスが必要です。このライセンスはユーザのメールボックスに基づいて別途購入する必要があります。

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

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

登録して**SnapCenter**ソフトウェアにアクセス

Amazon FSx for NetApp ONTAPまたはAzure NetApp Filesを初めて使用し、既存のNetAppアカウントを持っていない場合は、SnapCenterソフトウェアにアクセスできます。

開始する前に

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

タスクの内容

登録には情報が検証される必要があります。新しいNetAppサポートサイト（NSS）アカウントの確認とアップグレードが完了するまで、「ゲスト」から「フル」アクセスになるまで、最大1日かかる場合があります。

手順

1. をクリックし https://mysupport.netapp.com/site/user/registration て登録します。
2. 会社のEメールアドレスを入力し、キャプチャを完了してネットアップのプライバシーポリシーに同意し、*[送信]*をクリックします。
3. EメールIDに送信されたOTPを入力して登録を認証し、* Continue *をクリックします。
4. 登録完了ページで、以下の詳細を入力して登録を完了します。
   a. NetApp Customer/End User *を選択します。
   b. [Serial Number]フィールドに、次のいずれかを入力します。
      - Azure NetApp Filesを使用している場合はAzureサブスクリプションID。
      - ファイルシステムID（Amazon FSx for NetApp ONTAPを使用している場合）。

登録中に問題が発生した場合、またはステータスを確認する場合は、でチケットを発行できます https://mysupport.netapp.com/site/help 。

クレデンシャルの認証方式

クレデンシャルで使用される認証方法は、アプリケーションや環境に応じて異なります。クレデンシャルで認証されたユーザは、 SnapCenter の処理を実行できます。プラグインのインストールに使用するクレデンシャルとデータ保護処理に使用するクレデンシャルをそれぞれ1組ずつ作成する必要があります。

Windows認証

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

信頼されていないドメイン認証

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

ローカルワークグループ認証

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

SQL Server認証

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

Linux認証

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

AIX認証

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

Oracleデータベース認証

Oracleデータベース認証方式は、Oracleデータベースに照らして認証します。データベースホストでオペレー

ティングシステム（OS）認証が無効になっている場合は、Oracleデータベースで処理を実行するためにOracleデータベース認証が必要になります。そのため、Oracleデータベースのクレデンシャルを追加する前に、Oracleデータベースでsysdba権限を持つOracleユーザを作成しておく必要があります。

Oracle ASM認証

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

RMANカタログ認証

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

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。

- * 資格情報 *

  - ドメイン管理者または管理者グループの任意のメンバー

    ドメイン管理者またはSnapCenterプラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。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。

多要素認証（MFA）

多要素認証（**MFA**）を管理します。

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

多要素認証（**MFA**）を有効にする

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

タスクの内容

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

開始する前に

- Windows Active Directoryフェデレーションサービス（AD FS）がそれぞれのドメインで稼働している必要があります。
- Azure MFA、Cisco Duoなど、AD FSがサポートする多要素認証サービスが必要です。
- SnapCenterサーバとAD FSサーバのタイムスタンプは、タイムゾーンに関係なく同じにする必要があります。
- SnapCenterサーバ用に許可されたCA証明書を取得して設定します。

  CA証明書は、次の理由で必須です。

  - 自己署名証明書はノードレベルで一意であるため、ADFS-F5通信が切断されないようにします。
  - スタンドアロン構成またはハイアベイラビリティ構成でのアップグレード、修復、またはディザスタリカバリ（DR）中に自己署名証明書が再作成されないようにすることで、MFAの再設定を回避します。
  - IP-FQDNの解決を保証します。

    CA証明書の詳細については、を参照してください "CA証明書CSRファイルの生成"。

手順

1. Active Directoryフェデレーションサービス（AD FS）ホストに接続します。
2. FQDN >/FederationMetadata/2007-06/FederationMetadata.xmlからAD FSフェデレーションメタデータファイルをダウンロードし "https://<host ます。
3. ダウンロードしたファイルをSnapCenterサーバにコピーして、MFA機能を有効にします。
4. PowerShellを使用して、SnapCenter管理者ユーザとしてSnapCenterサーバにログインします。

5. PowerShellセッションを使用して、_New-SmMultifactorAuthenticationMetadata-path_cmdletを使用して、SnapCenter MFAメタデータファイルを生成します。

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

6. 生成されたファイルをAD FSホストにコピーして、SnapCenterをクライアントエンティティとして設定します。
7. コマンドレットを使用して、SnapCenterサーバのMFAを有効にします `Set-SmMultiFactorAuthentication` 。
8. （オプション）コマンドレットを使用して、MFAの設定ステータスと設定を確認します `Get-SmMultiFactorAuthentication` 。
9. Microsoft管理コンソール（MMC）に移動し、次の手順を実行します。
   a. [ファイル>*スナップインの追加と削除*]をクリックします。
   b. [スナップインの追加と削除] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
   c. [証明書] スナップインウィンドウで、 [**Computer account**] オプションを選択し、 [完了 *] をクリックします。
   d. ［コンソールルート］>［証明書–ローカルコンピューター］>［個人］>［証明書］の順にクリックします。
   e. SnapCenter にバインドされているCA証明書を右クリックし、すべてのタスク>*秘密鍵の管理*を選択します。
   f. Permissionsウィザードで、次の手順を実行します。
      i. [追加]*をクリックします。
      ii. [場所]*をクリックし、該当するホスト（階層の最上位）を選択します。
      iii. 「場所」ポップアップウィンドウで「* OK」をクリックします。
      iv. [オブジェクト名]フィールドに「IIS_IUSRS」と入力し、[名前の確認]をクリックして、[OK]をクリックします。

      チェックが正常に終了したら、* OK *をクリックします。

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

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

11. 名前を選択し、次の手順を実行します。

a. ［クレーム発行ポリシーの編集］をクリックします。

b. [ルールの追加]をクリックし、[次へ]をクリックします。

c. クレームルールの名前を指定します。

d. 属性ストアとして「* Active Directory *」を選択します。

e. 属性として「* User-Principal-Name 」を選択し、発信クレームタイプとして「 Name-ID *」を選択します。

f. [完了] をクリックします。

12. ADFSサーバで次のPowerShellコマンドを実行します。

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

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

13. メタデータがインポートされたことを確認するには、次の手順を実行します。

a. 証明書利用者信頼を右クリックし、* Properties *を選択します。

b. [Endpoints]、[Identifiers]、および[Signature]フィールドに値が入力されていることを確認します。

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

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

トラブルシューティング情報については、を参照してください "複数のタブで同時にログインを試行すると、MFAエラーが表示されます"。

AD FS MFAメタデータの更新

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

手順

1. FQDN >/FederationMetadata/2007-06/FederationMetadata.xmlからAD FSフェデレーションメタデータファイルをダウンロードし "https://<host ます。"

2. ダウンロードしたファイルをSnapCenterサーバにコピーして、MFA設定を更新します。

3. 次のコマンドレットを実行して、SnapCenterでAD FSメタデータを更新します。

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

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

SnapCenter MFAメタデータの更新

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

手順

1. AD FSホストでAD FS管理ウィザードを開き、次の手順を実行します。
   a. [証明書利用者信頼]をクリックします。
   b. SnapCenter 用に作成された証明書利用者信頼を右クリックし、*削除*をクリックします。

      証明書利用者信頼のユーザ定義名が表示されます。

   c. 多要素認証（MFA）を有効にします。

      を参照して "多要素認証を有効にします"

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

多要素認証（**MFA**）を無効にする

手順

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

REST API、**PowerShell**、**SCCLI**を使用して多要素認証（**MFA**）を管理

MFAログインは、ブラウザ、REST API、PowerShell、およびSCCLIからサポートされます。MFAは、AD FSアイデンティティマネージャを介してサポートされます。GUI、REST API、PowerShell、SCCLIを使用して、MFAの有効化、MFAの無効化、およびMFAの設定を行うことができます。

AD FSを**OAuth/OIDC**としてセットアップします

- Windows GUIウィザードを使用してAD FSを構成します*
  1. Server Manager Dashboard **>** Tools **>** ADFS Management *に移動します。
  2. **>**[アプリケーショングループ]*に移動します。
     a. [アプリケーショングループ]を右クリックします。
     b. を選択し、[アプリケーション名]*と入力します。
     c. [サーバーアプリケーション]*を選択します。
     d. 「 * 次へ * 」をクリックします。
  3. コピー*クライアントID *。

     これはクライアントIDです。..リダイレクトURLにコールバックURL（SnapCenterサーバURL）を追加します。..「 * 次へ * 」をクリックします。

  4. [Generate shared secret]*を選択します。

     シークレット値をコピーします。これはクライアントの秘密です。..「 * 次へ * 」をクリックします。

5. [概要]ページで、*[次へ]*をクリックします。
   a. [完了]ページで、*[閉じる]*をクリックします。
6. 新しく追加した*アプリケーショングループ*を右クリックし、*プロパティ*を選択します。
7. [アプリケーションのプロパティ]から*[アプリケーションの追加]*を選択します。
8. [アプリケーションの追加]*をクリックします。

   [Web API]を選択し、*[Next]*をクリックします。

9. [Web APIの構成]ページで、前の手順で作成したSnapCenterサーバのURLとクライアント識別子を[識別子]セクションに入力します。
   a. [追加]*をクリックします。
   b. 「 * 次へ * 」をクリックします。
10. [Choose Access Control Policy]ページで、要件に基づいて制御ポリシーを選択し（[Permit Everyone and Require MFA]など）、*[Next]*をクリックします。
11. [アプリケーション権限の設定]ページでは、デフォルトでOpenIDがスコープとして選択されており、*[次へ]*をクリックします。
12. [概要]ページで、*[次へ]*をクリックします。

    [完了]ページで、*[閉じる]*をクリックします。

13. [サンプルアプリケーションのプロパティ]ページで、*[OK]*をクリックします。
14. 承認サーバー(AD FS)によって発行され、リソースによって消費されることを意図したJWTトークン。

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

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

    ユーザー名を要求として提供するようにOpenID Connectを設定します。

16. サーバーマネージャの右上にある* Tools メニューの下にある AD FS Management *ツールを開きます。
    a. 左側のサイドバーから* Application Groups *フォルダを選択します。
    b. Web APIを選択し、* edit *をクリックします。
    c. [発行トランスフォームルール]タブに移動します
17. [* ルールの追加 *] をクリックします。
    a. [Claim rule template]ドロップダウンで、*[Send LDAP Attributes as Claims]*を選択します。
    b. 「 * 次へ * 」をクリックします。
18. [Claim rule]*の名前を入力します。
    a. [属性ストア]ドロップダウンで*[Active Directory]*を選択します。
    b. [LDAP Attribute]ドロップダウンで*を選択し、**[O*utgoing Claim Type]***ドロップダウンで[UPN]*を選択します。

c. [完了] をクリックします。

PowerShellコマンドを使用してアプリケーショングループを作成します

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

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

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

`ClientRoleIdentifier` アプリケーショングループの名前

`redirectURL` 許可後のリダイレクションの有効なURL

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

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

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

```
$identifier = (New-Guid).Guid

Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier
-Name "App Web API"

-Identifier $identifier -AccessControlPolicyName "Permit everyone"
```

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

```
"client_id = $identifier"

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

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

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

$transformrule = @"

@RuleTemplate = "LdapClaims"

@RuleName = "AD User properties and Groups"

c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
```

```
Issuer ==

"AD AUTHORITY"]

⇒ issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);

"@
```

6. 変換ルールファイルを書き出します。

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

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

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

アクセストークンの有効期限を更新します

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

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

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

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

AD FSからBearerトークンを取得します

RESTクライアント（Postmanなど）で以下のパラメータを入力する必要があり、ユーザクレデンシャルを入力するように求められます。さらに、ベアラートークンを取得するには、第2要素認証(あなたが持っているものとあなたがいるもの)を入力する必要があります。

+ベアラートークンの有効期間は、アプリケーションごとにAD FSサーバから設定できます。デフォルトの有効期間は60分です。

フィールド	値
付与タイプ	承認コード
コールバックURL	コールバックURLがない場合は、アプリケーションのベースURLを入力します。
認証URL	[ADFS-domain-name]/ADFS/OAuth2/authorize
アクセストークンURL	[ADFS-domain-name]/ADFS/OAuth2/token
クライアントID	AD FSクライアントIDを入力します
クライアントシークレット	AD FSクライアントシークレットを入力します
適用範囲	OpenID
クライアント認証	基本認証ヘッダーとして送信します
リソース	[詳細オプション]タブで、[コールバックURL]と同じ値を持つ[リソース]フィールドを追加します。この値は、JWTトークンでは「AUD」値として表示されます。

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

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

SnapCenter MFA CLI認証

PowerShellとSCCLIでは、既存のコマンドレット（Open-SmConnection）を「AccessToken」というもう1つのフィールドで拡張し、ベアラートークンを使用してユーザを認証します。

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

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

SnapCenter MFA REST API認証

REST <access token>クライアント(Postmanやswaggerなど)でBearerトークンを_Authorization = Bearer _の形式で使用し、ヘッダーにユーザRoleNameを指定すると、SnapCenterからの応答が成功します。

MFA REST APIワークフロー

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

は、アクセス（Bearer）トークンを使用して認証する必要があります。

- このタスクについて *
- Postman、Swagger UI、FireCampなど、任意のRESTクライアントを使用できます。
- アクセストークンを取得し、それを使用して以降の要求（SnapCenter REST API）を認証し、あらゆる処理を実行します。
- 手順 *
- AD FS MFAを介して認証する場合*

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

   ボタンを押してアプリケーションのアクセストークンを取得すると、AD FS SSOページにリダイレクトされ、ADクレデンシャルを入力してMFAで認証する必要があります。1.[AD FS SSO]ページで、[Username]テキストボックスにユーザ名または電子メールを入力します。

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

1. [パスワード]テキストボックスにパスワードを入力します。
2. *ログイン*をクリックします。
3. [サインインオプション]*セクションで、認証オプションを選択し、（設定に応じて）認証します。
   - プッシュ：電話機に送信されるプッシュ通知を承認します。
   - QRコード: AUTH Pointモバイルアプリを使用してQRコードをスキャンし、アプリに表示される認証コードを入力します
   - ワンタイムパスワード:トークンのワンタイムパスワードを入力します。
4. 認証が成功すると、Access、ID、およびRefresh Tokenを含むポップアップが開きます。

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

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

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

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

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

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

- GUI *
- 手順 *

1. SnapCenter管理者としてSnapCenterサーバにログインします。
2. **>**[グローバル設定]**>**[MultiFactorAuthentication（MFA）設定]*をクリックします

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

- PowerShellインターフェイス*
- 手順 *

1. PowerShellまたはCLIコマンドを実行して、GUI、REST API、PowerShell、SCCLIのMFAを有効にします。

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

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

指定したAD FSメタデータファイルパスを使用して設定されたSnapCenter GUI、REST API、PowerShell、およびSCCLIのMFAを有効にします。

1. コマンドレットを使用して、MFAの設定ステータスと設定を確認します `Get-SmMultiFactorAuthentication` 。

- SCCLIインターフェイス*
- 手順 *

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

- REST API *

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

パラメータ	値
要求されたURL	/api/4.9/settings/multifactorauthentication
HTTPメソッド	投稿
リクエストボディ	{"IsGuiMFAEnabled"：false、"IsRestApiMFAEnabled"：true、"IsCliMFAEnabled"：false、"ADFSConfigFilePath"："C:\\ADFS_METADATA\\abc.xml"}
応答本文	{"MFAConfiguration"： {"IsGuiMFAEnabled "：false、"ADFSConfigFilePath"："C：\\ADFS_METADATA\\abc.xml"、"SCConfigFilePath"：null、"IsRestApiMFAEnabled"：true、"IsCliMFAEnabled"：false、 "ADFSHostName"：" win-adfs-sc49.winscedom2.com}

2. 以下のAPIを使用してMFA構成のステータスと設定を確認します。

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

WindowsホストへのSnapCenterサーバのインストール

SnapCenterサーバインストーラの実行可能ファイルを実行して、SnapCenterサーバをインストールできます。

必要に応じて、PowerShellコマンドレットを使用して、いくつかのインストールと設定の手順を実行できます。

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

開始する前に

- SnapCenterサーバホストにWindowsの更新プログラムが適用されていて、システムの再起動が保留されていないことが必要です。
- SnapCenterサーバをインストールするホストにMySQLサーバがインストールされていないことを確認しておく必要があります。
- Windowsインストーラのデバッグを有効にしておく必要があります。

  を有効にする方法については、MicrosoftのWebサイトを参照して "Windows インストーラのログ"ください。

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

- 手順 *

1. からSnapCenterサーバインストールパッケージをダウンロードし "NetAppサポートサイト"ます。
2. ダウンロードした.exeファイルをダブルクリックして、SnapCenterサーバのインストールを開始します。

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

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

3. SnapCenterサーバのインストールに必要な値があらかじめ入力されていることを確認し、必要に応じて変更します。

   MySQL Serverリポジトリデータベースのパスワードを指定する必要はありません。SnapCenterサーバのインストール中に、パスワードが自動的に生成されます。

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

4. [今すぐインストール] をクリックします。

   無効な値を指定した場合は、該当するエラーメッセージが表示されます。値を再入力してからインストールを開始してください。

   > [Cancel] * ボタンをクリックすると、実行中のステップが完了し、ロールバック操作が開始されます。SnapCenter サーバがホストから完全に削除されます。

   ただし、「 SnapCenter サーバサイトの再起動」または「 SnapCenter サーバの起動を待機中」の処理が実行されているときに「 * キャンセル」をクリックすると、処理はキャンセルされずにインストールが続行されます。

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

製品を登録してサポートを有効にする

NetApp製品を初めてご利用になり、既存のNetAppアカウントをお持ちでない場合は、製品を登録してサポートを有効にする必要があります。

手順

1. SnapCenterのインストール後、*[ヘルプ]>[バージョン情報]*に移動します。
2. [_About SnapCenter _]ダイアログボックスで、971で始まる20桁のSnapCenterインスタンスをメモします。
3. をクリックします https://register.netapp.com
4. [* I am not a registered NetApp Customer*] をクリックします。
5. 自分自身を登録するには、詳細を指定してください。
6. NetApp Reference SNフィールドは空白のままにします。
7. [Product Line]ドロップダウンから[* SnapCenter *]を選択します。
8. 課金プロバイダを選択します。
9. 20桁のSnapCenterインスタンスIDを入力します。
10. [Submit （送信）] をクリックします。

LinuxホストへのSnapCenterサーバのインストール

SnapCenterサーバインストーラの実行可能ファイルを実行して、SnapCenterサーバをインストールできます。

開始する前に

- SnapCenterをインストールするための十分な権限がないroot以外のユーザを使用してSnapCenterサーバをインストールする場合は、NetAppサポートサイトからsudoersチェックサムファイルを入手してください。Linuxのバージョンに基づいて適切なチェックサムファイルを使用する必要があります。
- のインストール中。 NETランタイム。インストール時に_libicu_libraryの依存関係の解決に失敗した場合は、次のコマンドを実行してinstall_libicu_を実行します。 `yum install -y libicu`
- _perl_が使用できないためにSnapCenterサーバのインストールが失敗した場合は、次のコマンドを実行してinstall_perl_をインストールします。 `yum install -y perl`
- SUSE Linuxでsudoパッケージを使用できない場合は、認証エラーを回避するためにsudoパッケージをインストールします。
- SUSE Linuxの場合は、インストールの失敗を回避するためにホスト名を設定します。
- コマンドを実行して、セキュアなLinuxのステータスを確認します `sestatus`。SELinux status_が「enabled」で、_current mode_が「enforcing」の場合は、次の手順を実行します。
  - 次のコマンドを実行します。 `sudo semanage port -a -t http_port_t -p tcp <WEBAPP_EXTERNAL_PORT_>`

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

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

      コマンドから「Nothing to do」が返された場合は、SnapCenterサーバのインストール後にコマンドを再実行します。
    - コマンドがcreates_my-nginx.pp_を作成する場合は、コマンドを実行してポリシーパッケージをアクティブにします。 `sudo semodule -i my-nginx.pp`
  - MySQL PIDディレクトリに使用されるパスは_/ var/opt/mysqld_です。次のコマンドを実行して、MySQLインストールの権限を設定します。
    - `mkdir /var/opt/mysqld`
    - `sudo semanage fcontext -a -t mysqld_var_run_t "/var/opt/mysqld(/.*)?"`
    - `sudo restorecon -Rv /var/opt/mysqld`
  - MySQLのデータディレクトリのパスは、_/ INSTALL_DIR /NetApp/snapcenter/SnapManagerWeb/Repository/mysql/_です。次のコマンドを実行して、MySQLのデータディレクトリの権限を設定します。

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

タスクの内容

- SnapCenterサーバをLinuxホストにインストールすると、MySQL、RabbitMQ、Errlangなどのサードパーティサービスがインストールされます。アンインストールしないでください。
- LinuxホストにインストールされているSnapCenterサーバは、次の機能をサポートしていません。
  - 高可用性
  - Windowsプラグイン
  - Active Directory（Credを使用するrootユーザとroot以外のユーザの両方で、ローカルユーザのみをサポート）
  - SnapCenterへのログインに使用するキーベースの認証

手順

1. 次のファイルをから_/ホームディレクトリ_にダウンロードし "NetAppサポートサイト" ます。
   - SnapCenterサーバインストールパッケージ-* snapcenter-linux-server-(el8/el9/sles15).bin*
   - 公開キーファイル-* snapcenter_public_key.pub *
   - それぞれのシグネチャファイル-* snapcenter-linux-server-(el8/el9/sles15).bin.sig*
2. 署名ファイルを検証します。 `$openssl dgst -sha256 -verify snapcenter_public_key.pub -signature <path to signature file> <path to bin file>`
3. root以外のユーザをインストールする場合は、.binインストーラとともに* snapcenter_server_checksum_（el8/el9/sles15）.txt *で指定したvisudoコンテンツを追加します。
4. .binインストーラの実行権限を割り当てます。 `chmod +x snapcenter-linux-server-(el8/el9/sles15).bin`
5. いずれかの操作を実行して、SnapCenterサーバをインストールします。

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

実行する処理	操作
非対話型インストール	`sudo ./snapcenter-linux-server-(el8/el9/sles15).bin -i silent -DWEBAPP_EXTERNAL_PORT=<port> -DWEBAPP_INTERNAL_PORT=<port> -DSMCORE_PORT=<port> -DSCHEDULER_PORT=<port> -DSNAPCENTER_SERVER_USER=<user> -DUSER_INSTALL_DIR=<dir> -DINSTALL_LOG_NAME=<filename>` 例：sudo ./ snapcenter_linux_server.bin -i silent -dwebapp_external_port=8146 -DSNAPCENTER_SERVER_USER=root -Duser_install_DIR=/opt -DINSTALL_LOG_NAME=InstallerLog.log ログは_/var/opt/snapcenter/logs _に保存されます。 SnapCenterサーバをインストールするために渡されるパラメータ： • DWEBAPP_EXTERNAL_PORT：Linuxホスト外のSnapCenterサーバにアクセスするために使用されるwebapp外部ポート。デフォルト値は8146です。 • DWEBAPP_INTERNAL_PORT：Linuxホスト内のSnapCenterサーバへのアクセスに使用されるwebapp内部ポート。デフォルト値は8147です。 • DSMCORE_PORT：smcoreサービスが実行されているSMCoreポート。デフォルト値は8145です。 • DSCHEDULER_PORT：スケジューラサービスが実行されているスケジューラポート。デフォルト値は8154です。 • DSNAPCENTER_SERVER_USER ：SnapCenterサーバをインストールするSnapCenterサーバユーザ。DSNAPCENTER_SERVER_USER_の場合、デフォルトはインストーラを実行しているユーザです。 • DUSER_INSTALL_DIR:パッケージがインストールされるインストールディレクトリ。*DUSER_INSTALL_DIR_*の場合、デフォルトのインストールディレクトリは/ opt_です。 • DINSTALL_LOG_NAME：インストールログを格納するログファイルの名前。これはオプションパラメータで、指定するとログはコンソールに表示されません。 このパラメータを指定しない場合、ログはコンソールに表示され、デフォルトのログファイルにも格納されます。 DSELINUX：_SELinux STATUS_が「

次の手順

- _SELinux status_が「enabled」で、_current mode_が「enforcing」の場合、*nginx*サービスは起動しません。次のコマンドを実行する必要があります。
  a. ホームディレクトリに移動します。
  b. コマンドを実行します `journalctl -x|grep nginx`。
  c. webapp内部ポート（8147）がリッスンできない場合は、次のコマンドを実行します。
     - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
     - `semodule -i my-nginx.pp`
  d. 実行 `setsebool -P httpd_can_network_connect on`

- Enabled」、_CURRENT MODE_が Enforcing」で、「Before You Begin」セクションで説明したコマンドを実行した場合は、このパラメータを指定して値を1に割り当てる必要があります。デフォルト値は0です。
- UPGRADE コマンドを実行します。値は0です。SnapCenterサーバをアップグレードするには、このパラメータと0以外の任意の整数を指定します。

製品を登録してサポートを有効にする

NetAppを初めてご利用になり、NetAppアカウントをお持ちでない場合は、製品を登録してサポートを有効にする必要があります。

手順

1. SnapCenterのインストール後、*[ヘルプ]>[バージョン情報]*に移動します。
2. [_About SnapCenter _]ダイアログボックスで、971で始まる20桁のSnapCenterインスタンスをメモします。
3. をクリックします https://register.netapp.com
4. [* I am not a registered NetApp Customer*] をクリックします。
5. 自分自身を登録するには、詳細を指定してください。
6. NetApp Reference SNフィールドは空白のままにします。
7. [Product Line]ドロップダウンから[* SnapCenter *]を選択します。
8. 課金プロバイダを選択します。
9. 20桁のSnapCenterインスタンスIDを入力します。
10. [Submit （送信）] をクリックします。

RBAC許可を使用したSnapCenterへのログイン

SnapCenterはロールベースアクセス制御（RBAC）をサポートしています。SnapCenter管理者は、SnapCenter RBACを使用して、ワークグループまたはActive Directory内のユーザ、またはActive Directory内のグループにロールとリソースを割り当てます。これで、RBACユーザは割り当てられたロールを使用してSnapCenterにログインできるようになります。

開始する前に

- Windows Server ManagerでWindowsプロセスアクティブ化サービス（WAS）を有効にする必要があります。
- Internet Explorerをブラウザとして使用してSnapCenterサーバーにログインする場合は、Internet Explorerの保護モードが無効になっていることを確認する必要があります。

- SnapCenterサーバがLinuxホストにインストールされている場合は、SnapCenterサーバのインストールに使用したユーザアカウントを使用してログインする必要があります。
- このタスクについて *

インストール中に、SnapCenterサーバーインストールウィザードによってショートカットが作成され、SnapCenterがインストールされているホストのデスクトップおよび[スタート]メニューに配置されます。また、インストールの最後に、インストールウィザードには、インストール中に指定した情報に基づいてSnapCenter URLが表示されます。リモートシステムからログインする場合は、このURLをコピーできます。

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

* ベストプラクティス：セキュリティ上の理由から、ブラウザで SnapCenter パスワードを保存しないことを推奨します。

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

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

SnapCenter GUIに加えて、PowerShellコマンドレットを使用してスクリプトを作成し、設定、バックアップ、リストアの各処理を実行できます。一部のコマンドレットは、SnapCenterのリリースごとに変更されている場合があります。詳細については、を "SnapCenter ソフトウェアコマンドレットリファレンスガイド" 参照してください。

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

- 手順 *

1. ローカルホストのデスクトップにあるショートカット、インストールの終了時に表示された URL 、または SnapCenter 管理者から提供された URL から、 SnapCenter を起動します。
2. ユーザー資格情報を入力します。

指定する項目	使用する形式
ドメイン管理者	• NetBIOS\ユーザ名 • ユーザ名@UPNサフィックス 例：username@netapp.com • ドメインFQDN\ユーザ名
ローカル管理者	ユーザ名

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

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

- 結果 *

[Dashboard]ページが表示されます。

サイトに到達できないというエラーが表示されてロギングが失敗した場合は、SSL証明書をSnapCenterにマッピングする必要があります。 "詳細"

- 終了後 *

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

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

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

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

多要素認証（MFA）を使用したSnapCenterへのログイン

SnapCenterサーバは、Active Directoryの一部であるドメインアカウントに対してMFAをサポートしています。

開始する前に

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

- このタスクについて *
- FQDNのみがサポートされます。
- ワークグループユーザとクロスドメインユーザはMFAを使用してログインできない

- 手順 *

1. ローカルホストのデスクトップにあるショートカット、インストールの終了時に表示された URL 、または SnapCenter 管理者から提供された URL から、 SnapCenter を起動します。
2. AD FSログインページで、[Username]と[Password]を入力します。

   AD FSページにユーザ名またはパスワードが無効であるというエラーメッセージが表示された場合は、次の点を確認する必要があります。

   - ユーザ名またはパスワードが有効かどうか

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

   - ADで設定された最大試行回数を超えたかどうか
   - AD FSとAD FSが稼働しているかどうか

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

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

セキュリティ機能として、デフォルトでは、操作を行わないまま 15 分が経過すると、 SnapCenter は GUI セッションから 5 分後にログアウトすることを警告するメッセージを表示します。デフォルトでは、操作を行わないまま 20 分が経過すると SnapCenter によって GUI セッションからログアウトされ、再度ログインする必要があります。

- 手順 *

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

SSL 3.0を無効にしてSnapCenter Webサーバを保護する

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

SSL 3.0プロトコルには、接続障害を引き起こしたり、中間者攻撃を実行したり、Webサイトと訪問者間の暗号化トラフィックを観察したりするために攻撃者が使用できる欠陥があります。

- 手順 *

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

   - サーバキーがすでに存在する場合：

     i. 有効な DWORD を選択し、 * 編集 * > * 変更 * をクリックします。

ii. 値を 0 に変更し、 * OK * をクリックします。

- サーバキーが存在しない場合は、次の手順を実行します。
  i. [* 編集 *] 、 [* 新規 *] 、 [* キー *] の順にクリックし、キーサーバーに名前を付けます。
  ii. 新しいサーバーキーを選択した状態で、 * 編集 * > * 新規 * > * DWORD * をクリックします。
  iii. 新しいDWORDにenabledという名前を付け、値として0を入力します。

3. レジストリエディタを閉じます。

WindowsホストのCA証明書の設定

CA証明書CSRファイルの生成

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

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

CA証明書RSAキーの長さは3072ビット以上にする必要があります。

CSRを生成する方法については、を参照してください "CA 証明書 CSR ファイルの生成方法"。

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

クラスタ構成の場合、クラスタ名（仮想クラスタFQDN）、およびそれぞれのホスト名がCA証明書に記載されている必要があります。証明書を更新するには、証明書を取得する前に Subject Alternative Name （ SAN ）フィールドに値を入力します。ワイルドカード証明書（ * .domain.company.com ）の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

CA証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenterサーバおよびWindowsホストプラグインにCA証明書をインポートする必要があります。

手順

1. Microsoft 管理コンソール (MMC) に移動し、 [* ファイル *] 、 [スナップインの追加と削除] の順にクリックします。
2. [スナップインの追加と削除] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
3. [証明書] スナップインウィンドウで、 [**Computer account**] オプションを選択し、 [完了 *] をクリックします。
4. [* コンソールルート **>** 証明書–ローカルコンピュータ **>** 信頼されたルート証明機関 **>** 証明書 *] をクリックします。
5. [信頼されたルート証明機関] フォルダを右クリックし、 [すべてのタスク **>*Import**] を選択してインポ

ートウィザードを開始します。

6. 次の手順でウィザードを完了します。

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

証明書のインポートは、秘密鍵にバンドルされている必要があります（サポートされている形式は、**.pfx**、.p12、および*.p7b）。

7. 「Personal」フォルダに対して手順5を繰り返します。

CA証明書サムプリントの取得

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

手順

1. GUIで次の手順を実行します。
   a. 証明書をダブルクリックします。
   b. [証明書] ダイアログボックスで、 [* 詳細 *] タブをクリックします。
   c. フィールドのリストをスクロールし、 [**Thumbprint**] をクリックします。
   d. ボックスから16進数の文字をコピーします。
   e. 16進数の間のスペースを削除します。

      たとえば、サムプリントが「 A9 09 50 2D d8 2a 14 33 e6 F8 38 86 b0 0d 42 77 A3 2a 7b 」の場合、スペースを削除すると、「 a909502dd82ae41433e6f83886b00d4277a32a7b 」となります。

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

      Get-ChildItem - パス証明書： *\localmachine\My*

   b. サムプリントをコピーします。

Windowsホストプラグインサービスでの**CA**証明書の設定

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

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

手順

1. 次のコマンドを実行して、SMCoreのデフォルトポート8145を使用して既存の証明書バインディングを削除します。

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

   例：

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

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

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

   例：

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

SnapCenterサイトで**CA**証明書を設定

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

- 手順 *
  1. SnapCenter がインストールされている Windows サーバーで IIS マネージャーを開きます。
  2. 左側のナビゲーションペインで、 * 接続 * をクリックします。
  3. サーバー名と * Sites * を展開します。
  4. SSL証明書をインストールするSnapCenter Webサイトを選択します。
  5. [* アクション * （ Actions * ）] > [* サイトの編集 * （ * Edit Site * ）] に移動し、 [* バインド * （

Bind

6. バインディングページで、「 https * のバインディング」を選択します。
7. [編集（ Edit ）] をクリックします。
8. [SSL証明書]ドロップダウンリストから、最近インポートしたSSL証明書を選択します。
9. [OK]*をクリックします。

SnapCenterスケジューラサイト（デフォルトポート：8154、HTTPS）には自己署名証明書が設定されています。このポートはSnapCenterサーバホスト内で通信しており、CA証明書を使用してを設定する必要はありません。ただし、CA証明書の使用が必要な環境の場合は、SnapCenterスケジューラサイトを使用して手順5から9を繰り返します。

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

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

SnapCenterのCA証明書を有効にする

CA証明書を設定し、SnapCenterサーバに対してCA証明書の検証を有効にする必要があります。

開始する前に

- CA証明書を有効または無効にするには、Set-SmCertificateSettingsコマンドレットを使用します。
- SnapCenterサーバの証明書のステータスは、Get-SmCertificateSettingsコマンドレットを使用して表示できます。

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

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

[管理対象ホスト]タブのホストには南京錠が表示され、南京錠の色はSnapCenterサーバとプラグインホスト間の接続のステータスを示します。

- * 🔒 *は、有効になっているかプラグインホストに割り当てられているCA証明書がないことを示します。
- ** 🔒 は、CA証明書が正常に検証されたことを示します。
- ** 🔒 は、CA証明書を検証できなかったことを示します。

- ** は、接続情報を取得できなかったことを示します。

ステータスが黄色または緑の場合は、データ保護処理が正常に完了しています。

LinuxホストのCA証明書の設定

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

nginx証明書の設定

手順

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

監査ログ証明書の設定

手順

1. viまたは任意のテキストエディタを使用して_install_DIR /NetApp/snapcenter/SnapManagerWeb/SnapManagerWeb.UI.dll.config_を開きます。

   *INSTALL_DIR_IS_*のデフォルト値は/ opt_です。

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

   監査ログ証明書では、_.pfx_formatのみがサポートされます。

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

SnapCenterサービス証明書の設定

手順

1. viまたは任意のテキストエディタを使用して、次の設定ファイルを開きます。
   - *INSTALL_DIR /NetApp/snapcenter/SnapManagerWeb/SnapManagerWeb.UI.dll.config*
   - *INSTALL_DIR /NetApp/snapcenter/SMCore/SMCoreServiceHost.dll.config*
   - *install_DIR /NetApp/snapcenter/Scheduler/Scheduler.api.dll.config*

*INSTALL_DIR_IS_*のデフォルト値は/ opt_です。

2. SERVICE_CERTIFICATE_PATH キーと SERVICE_CERTIFICATE_PASSWORD *キーを編集して、CA証明書のパスとパスワードをそれぞれ追加します。

   SnapCenterサービス証明書では、_.pfx_formatのみがサポートされます。

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

Windowsホストで双方向SSL通信を設定して有効にする

Windowsホストでの双方向SSL通信の設定

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

開始する前に

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

  詳細については、を参照してください。 "CA証明書の設定セクション"

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

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

手順

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

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

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

      例えば、

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

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

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

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

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

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

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

例えば、

```
> $cert = "abc123abc123abc123abc123"

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

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

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

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

> netsh http show sslcert ipport=0.0.0.0:8146

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

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

Windowsレジストリエディタで、次のパスに移動します。

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

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

```
SendTrustedIssuerList = 0

ClientAuthTrustMode = 2
```

双方向SSL通信用のSnapCenter Windowsプラグインを設定します

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

開始する前に

CA証明書サムプリントが使用可能であることを確認します。

手順

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

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

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

   例えば、

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

   b. 新しく取得したCA証明書をSMCoreポートにバインドします。

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

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

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

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

   例えば、

   ```
   > $cert = "abc123abc123abc123abc123"

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

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

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

Windowsホストで双方向SSL通信を有効にする

PowerShellコマンドを使用して、Windowsホスト上のSnapCenterサーバとプラグインの間の相互通信を保護するために、双方向SSL通信を有効にすることができます。

- 始める前に *

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

- 手順 *

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

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

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

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

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

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

双方向SSL通信を無効にします

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

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

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

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

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

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

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

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

Linuxホストでの双方向SSL通信の設定と有効化

Linuxホストでの双方向SSL通信の設定

双方向SSL通信を設定して、Linuxホスト上のSnapCenterサーバとプラグインの間の相互通信を保護する必要があります。

開始する前に

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

手順

1. certificate.pem *を_/etc/pki/ca-trust/source/anchors/_にコピーします。
2. Linuxホストの信頼リストに証明書を追加します。
   - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
   - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
   - `update-ca-trust extract`
3. 証明書が信頼リストに追加されたかどうかを確認します。 `trust list | grep "<CN of your certificate>"`
4. SnapCenter * nginx ファイルの ssl_certificate と ssl_certificate_key *を更新して再起動してください。
   - `vim /etc/nginx/conf.d/snapcenter.conf`
   - `systemctl restart nginx`
5. SnapCenterサーバGUIリンクを更新します。
6. */<installation path>/NetApp/snapcenter/SnapManagerWeb_*および* *SMCoreServiceHost.dll.config* *（/<installation path>/NetApp/snapcenter/SMCore_）で次のキーの値を更新します。
   - <add key="SERVICE_CERTIFICATE_PATH" value="<path of certificate.pfx>" />
   - <add key="SERVICE_CERTIFICATE_PASSWORD" value="<password>"/>

7. 次のサービスを再起動します。
   - `systemctl restart smcore.service`
   - `systemctl restart snapmanagerweb.service`
8. 証明書がSnapManager Webポートに接続されていることを確認します。 `openssl s_client -connect localhost:8146 -brief`
9. 証明書がsmcoreポートに接続されていることを確認します。 `openssl s_client -connect localhost:8145 -brief`
10. SPLキーストアとエイリアスのパスワードを管理します。
    a. SPLプロパティファイルの* spl_keystore_pass *キーに割り当てられたSPLキーストアのデフォルトパスワードを取得します。
    b. キーストアのパスワードを変更します。 `keytool -storepasswd -keystore keystore.jks`
    c. 秘密鍵エントリのすべてのエイリアスのパスワードを変更します。 `keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
    d. _spl.properties_のキー* spl_keystore_pass *と同じパスワードを更新します。
    e. サービスを再起動します。
11. プラグインLinuxホストで、SPLプラグインのキーストアにルート証明書と中間証明書を追加します。
    - `keytool -import -trustcacerts -alias <any preferred alias name> -file <path of root-ca.pem> -keystore <path of keystore.jks mentioned in spl.properties file>`
    - `keytool -importkeystore -srckeystore <path of certificate.pfx> -srcstoretype pkcs12 -destkeystore <path of keystore.jks mentioned in spl.properties file> -deststoretype JKS`
      i. keystore.jksのエントリを確認します。 `keytool -list -v -keystore <path to keystore.jks>`
      ii. 必要に応じてエイリアスの名前を変更します。 `keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas`
12. _spl.properties_ファイルの* spl_certificate_alias の値を**_keystore.jks_**に格納されている certificate.pfx * のエイリアスで更新し、SPLサービスを再起動します。 `systemctl restart spl`
13. 証明書がsmcoreポートに接続されていることを確認します。 `openssl s_client -connect localhost:8145 -brief`

Linuxホストで**SSL**通信を有効にする

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

ステップ

1. 一方向SSL通信を有効にするには、次の手順を実行します。
   a. SnapCenter GUIにログインします。

b. >[グローバル設定]をクリックし、[SnapCenterサーバーで証明書の検証を有効にする]*を選択します。

c. >[管理対象ホスト]*をクリックし、一方向SSLを有効にするプラグインホストを選択します。

d. アイコンをクリックし  、*[証明書の検証を有効にする]*をクリックします。

2. SnapCenterサーバLinuxホストからの双方向SSL通信を有効にします。

   ◦ `Open-SmConnection`

   ◦ `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName <Plugin Host Name>`

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

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

証明書ベースの認証の設定

SnapCenterサーバから認証局（CA）証明書をエクスポートします

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

開始する前に

双方向SSLを設定しておく必要があります。

- 手順 *

1. Microsoft 管理コンソール (MMC) に移動し、 [* ファイル *] 、 [スナップインの追加と削除] の順にクリックします。
2. [スナップインの追加と削除] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
3. [証明書スナップイン]ウィンドウで*オプションを選択し、[完了]*をクリックします。
4. >[証明書-ローカルコンピュータ]>[個人]>[証明書]*をクリックします。
5. SnapCenterサーバーで使用される調達CA証明書を右クリックし、**[**すべてのタスク**]**>*[エクスポート]*を選択してエクスポートウィザードを開始します。
6. ウィザードで次の操作を実行します。

オプション	操作
秘密キーのエクスポート	を選択し、[次へ]*をクリックします。
エクスポートファイル形式	「 * 次へ * 」をクリックします。
ファイル名	をクリックし、証明書を保存するファイルパスを指定して[次へ]*をクリックします。

オプション	操作
証明書のエクスポートウィザードの完了	概要を確認し、 * 完了 * をクリックしてエクスポートを開始します。

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

認証局（CA）証明書をWindowsプラグインホストにインポートします

エクスポートしたSnapCenterサーバCA証明書を使用するには、Microsoft管理コンソール（MMC）を使用して、関連する証明書をSnapCenter Windowsプラグインホストにインポートする必要があります。

- 手順 *

1. Microsoft 管理コンソール (MMC) に移動し、 [* ファイル *] 、 [スナップインの追加と削除] の順にクリックします。
2. [スナップインの追加と削除] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
3. [証明書スナップイン]ウィンドウで*オプションを選択し、[完了]*をクリックします。
4. **>**[証明書-ローカルコンピュータ]**>**[個人]**>**[証明書]*をクリックします。
5. 「個人」フォルダを右クリックし、すべてのタスク>*インポート*を選択してインポートウィザードを開始します。
6. ウィザードで次の操作を実行します。

オプション	操作
ストアの場所	「 * 次へ * 」をクリックします。
インポートするファイル	拡張子.cerで終わるSnapCenterサーバ証明書を選択します。
証明書ストア	「 * 次へ * 」をクリックします。
証明書のエクスポートウィザードの完了	概要を確認し、 [完了] をクリックしてインポートを開始します。

UNIXホストプラグインにCA証明書をインポートし、SPL trust-storeにルート証明書または中間証明書を設定する

CA証明書をUNIXプラグインホストにインポートします

CA証明書をUNIXプラグインホストにインポートする必要があります。

- このタスクについて *

- SPLキーストアのパスワード、および使用中のCA署名キーペアのエイリアスを管理できます。
- SPLキーストアのパスワードと、秘密鍵に関連付けられているすべてのエイリアスパスワードは同じである必要があります。
- 手順 *
  1. SPLキーストアのデフォルトパスワードは、SPLプロパティファイルから取得できます。キーに対応する値です `SPL_KEYSTORE_PASS`。
  2. キーストアのパスワードを変更します。 `$ keytool -storepasswd -keystore keystore.jks`
  3. キーストア内の秘密鍵エントリのすべてのエイリアスのパスワードを、キーストアと同じパスワードに変更します。 `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
  4. ファイルのSPL_KEYSTORE_PASSキーについても同じ内容を更新し `spl.properties` ます。
  5. パスワードを変更したら、サービスを再起動します。

spl trust-storeに対するルート証明書または中間証明書の設定

ルート証明書または中間証明書をspl trust-storeに設定する必要があります。ルートCA証明書のあとに中間CA証明書を追加する必要があります。

- 手順 *
  1. SPLキーストアが格納されているフォルダに移動します `/var/opt/snapcenter/spl/etc`。
  2. ファイルを探します `keystore.jks`。
  3. キーストアに追加された証明書を一覧表示します。 `$ keytool -list -v -keystore keystore.jks`
  4. ルート証明書または中間証明書を追加します。 `$ keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
  5. spl trust-storeにルート証明書または中間証明書を設定したら、サービスを再起動します。

SPL trust-storeへの**CA**署名済みキーペアの設定

SPL trust-storeにCA署名付きキーペアを設定する必要があります。

- 手順 *
  1. SPLのキーストアが格納されているフォルダに移動し `/var/opt/snapcenter/spl/etc` ます。
  2. ファイルを探します `keystore.jks`。
  3. キーストアに追加された証明書を一覧表示します。 `$ keytool -list -v -keystore keystore.jks`
  4. 秘密鍵と公開鍵の両方が設定されたCA証明書を追加します。 `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS`
  5. キーストアに追加された証明書を一覧表示します。 `$ keytool -list -v -keystore keystore.jks`

6. キーストアに追加された新しいCA証明書に対応するエイリアスがキーストアに含まれていることを確認します。
7. CA証明書に追加した秘密鍵のパスワードをキーストアのパスワードに変更します。

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

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

1. CA証明書のエイリアス名が長く、スペースまたは特殊文字（"*"、"、"、"）が含まれている場合は、エイリアス名を単純な名前に変更します。 `$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
2. ファイルにあるキーストアからエイリアス名を設定し `spl.properties` ます。この値をSPL_CERTIFICATE_ALIASキーに対して更新します。
3. SPL trust-storeにCA署名キーペアを設定したら、サービスを再起動します。

証明書ベースの認証を有効にします

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

- クライアント証明書ベースの認証を有効にするには：

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

- クライアント証明書ベースの認証を無効にするには：

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

Active Directory、LDAP、LDAPSの設定

信頼されていない**Active Directory**ドメインの登録

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

開始する前に

- LDAP および LDAPS プロトコル *
- 信頼されていないActive Directoryドメインは、LDAPまたはLDAPSプロトコルを使用して登録できます。
- プラグインホストとSnapCenterサーバの間の双方向の通信を有効にしておく必要があります。
- DNSによる解決は、SnapCenterサーバからプラグインホストへ（またはその逆）設定する必要があります。

- LDAPプロトコル*
- 完全修飾ドメイン名（FQDN）をSnapCenterサーバから解決できる必要があります。

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

- LDAPSプロトコル*
- CA証明書は、Active Directory通信中にLDAPSでエンドツーエンドの暗号化を提供するために必要です。

  "LDAPS用のCAクライアント証明書の設定"

- ドメインコントローラのホスト名（DCHostName）にSnapCenterサーバから到達できる必要があります。
- このタスクについて *
- 信頼されていないドメインは、SnapCenterユーザインターフェイス、PowerShellコマンドレット、またはREST APIを使用して登録できます。
- 手順 *
  1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
  2. 設定ページで、 * グローバル設定 * をクリックします。
  3. [グローバル設定] ページで、 [* ドメイン設定 *] をクリックします。
  4. をクリックして新しいドメインを登録します。
  5. [新しいドメインの登録] ページで、 **LDAP** または *LDAPS * のいずれかを選択します。
     a. 「 * ldap * 」を選択した場合は、 LDAP の信頼されていないドメインを登録するために必要な情報を指定します。

フィールド	操作
ドメイン名	ドメインのNetBIOS名を指定します。
ドメインFQDN	FQDN を指定し、 * resolve * をクリックします。
ドメインコントローラのIPアドレス	ドメイン FQDN を SnapCenter サーバから解決できない場合は、ドメインコントローラの IP アドレスを 1 つ以上指定します。 詳細については、を参照してください "GUI から信頼できないドメインのドメインコントローラ IP を追加します"。

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

フィールド	操作
ドメイン名	ドメインのNetBIOS名を指定します。
ドメインFQDN	FQDNを指定します。
トメインコントロオラメイ	1 つまたは複数のドメインコントローラ名を指定し、 * Resolve.* をクリックします。
ドメインコントローラのIPアドレス	ドメインコントローラ名をSnapCenterサーバから解決できない場合は、DNSの解決を修正する必要があります。

6. [OK]*をクリックします。

LDAPS用のCAクライアント証明書の設定

Windows Active Directory LDAPSにCA証明書が設定されている場合は、SnapCenterサーバでLDAPSのCAクライアント証明書を設定する必要があります。

- 手順 *

1. Microsoft 管理コンソール (MMC) に移動し、 [* ファイル *] 、 [スナップインの追加と削除] の順にクリックします。
2. [スナップインの追加と削除] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
3. [証明書] スナップインウィンドウで、 [**Computer account**] オプションを選択し、 [完了 *] をクリックします。
4. [* コンソールルート **>** 証明書–ローカルコンピュータ **>** 信頼されたルート証明機関 **>** 証明書 *] をクリックします。
5. [信頼されたルート証明機関] フォルダを右クリックし、 [すべてのタスク **>*Import**] を選択してインポートウィザードを開始します。
6. 次の手順でウィザードを完了します。

ウィザードウィンドウ	操作
ウィザードの2ページ目	[* 参照] をクリックし、 *Root Certificate* を選択して、 [* 次へ *] をクリックします。
証明書のインポートウィザードの完了	概要を確認し、 [完了] をクリックしてインポートを開始します。

7. 中間証明書について、手順 5 と 6 を繰り返します。

ハイアベイラビリティの設定

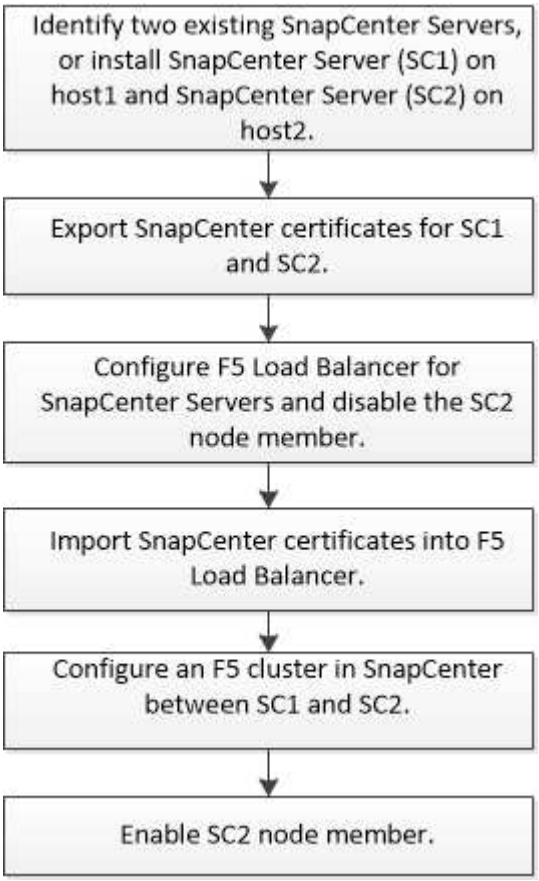
F5を使用した高可用性のためのSnapCenterサーバの設定

SnapCenter でハイアベイラビリティ（ HA ）をサポートするには、 F5 ロードバランサをインストールします。F5 によって、 SnapCenter サーバは、同じ場所にある最大 2 台のホストでアクティブ / パッシブ構成をサポートできます。SnapCenterでF5ロードバランサを使用するには、SnapCenterサーバを設定し、F5ロードバランサを設定する必要があります。

SnapCenterは、AWS Elastic Load Balancing（ELB）とAzureのロードバランシングもサポートしています。

以前にネットワークロードバランシング（NLB）を使用していたSnapCenter 4.2.xからアップグレードした場合は、引き続きその構成を使用するか、F5に切り替えることができます。

ワークフロー図は、F5ロードバランサを使用してSnapCenterサーバーを高可用性に設定する手順を示しています。詳細については、を参照してください "F5 ロードバランサを使用して SnapCenter サーバのハイアベイラビリティを設定する方法"。



次のコマンドレットを使用してF5クラスタを追加および削除するには、（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"。

F5のその他の設定情報

- SnapCenter をインストールしてハイアベイラビリティ用に設定したら、 F5 クラスタ IP を指すように SnapCenter デスクトップのショートカットを編集します。
- SnapCenterサーバ間でフェ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）では、NLBまたはF5ノードによって部分的に解決されたノードを追加し、SnapCenterノードがこのノード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ノードがNLBノードまたはF5ノード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ノード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、ノードレベルの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、2つ目のノードに監査ログの設定が反映されません。そのため、監査ログの設定は、F5パッシブノードがアクティブになったときに手動で繰り返す必要があります。

Microsoft Network Load Balancerの手動設定

Microsoftネットワークロードバランシング（NLB）を設定して、SnapCenterの高可用性をセットアップできます。SnapCenter 4.2以降では、高可用性を実現するために、SnapCenterインストールの外部で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"。

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

NLBからF5に切り替えて高可用性を実現

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"。

SnapCenter証明書のエクスポート

- 手順 *

1. Microsoft 管理コンソール (MMC) に移動し、 [* ファイル *] 、 [* スナップインの追加と削除] の順にクリックします。
2. [スナップインの追加と削除] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
3. [証明書] スナップインウィンドウで、 [マイユーザーアカウント *] オプションを選択し、 [完了 *] をクリックします。
4. [* コンソールルート **>*Certificates - Current User**>*Trusted Root Certification Authorities*>*Certificates*] をクリックします。
5. SnapCenter フレンドリ名が表示されている証明書を右クリックし、 * すべてのタスク * > * エクスポート * を選択してエクスポートウィザードを開始します。
6. 次の手順でウィザードを完了します。

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

- 結果 *

証明書は.pfx形式でエクスポートされます。

ロールベースアクセス制御（**RBAC**）の設定

ユーザまたはグループを追加し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。

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

- SnapCenter には、事前定義されたロールが複数あり

  これらのロールをユーザに割り当てるか、新しいロールを作成できます。

- SnapCenter RBACに追加する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。

フィールド	操作
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。

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。

「SnapCenterAdmin」ロールでログインしておく必要があります。

- 手順 *

1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
2. 設定ページで、 * 役割 * をクリックします。
3. をクリックします 

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

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

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

   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。

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

security loginコマンドを使用してONTAP RBACロールを追加する

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ONTAP RBACロールを追加できます。

開始する前に

- clustered ONTAPを実行するストレージシステム用にONTAP RBACロールを作成する前に、次の項目について確認しておく必要があります。
  - 実行するタスク（複数可）
  - これらのタスクの実行に必要な権限
- RBACロールを設定するには、次の操作を実行する必要があります。
  - コマンドおよびコマンドディレクトリ（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クラスタ管理者 IP に接続されているか、またはクラスタ内の SVM に直接接続されているかに応じて、設定は異なります。
- このタスクについて *

これらのロールをストレージシステムで簡単に設定するには、NetAppコミュニティフォーラムに掲載されているRBAC User Creator for Data ONTAPツールを使用します。

このツールは、ONTAP権限の適切な設定を自動的に処理します。たとえば、RBAC User Creator for Data ONTAPツールでは、フルアクセス権限が最初に表示されるように、権限が正しい順序で自動的に追加されます。読み取り専用権限を最初に追加してからフルアクセス権限を追加すると、ONTAPはフルアクセス権限を重複としてマークし、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 Data ONTAP ツールを再度実行して、以前に作成したユーザロールを更新する必要があります。以前のバージョンの SnapCenter または ONTAP 用に作成したユーザロールは、アップグレード後のバージョンでは正常に機能しません。ツールを再実行すると、アップグレードが自動的に処理されます。ロールを再作成する必要はありません。

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

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

- 手順 *

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

   ```
   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。

5.0以降では、SVM管理者ユーザはREST APIでのみサポートされます。SVM管理者以外を使用してロールを作成する場合は、ZAPIを使用してください。

- `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

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 -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。

SnapCenter 5.0以降では、クラスタ管理者ユーザはREST APIでのみサポートされます。クラスタ管理者以外のユーザを使用してロールを作成する場合は、ZAPIを使用してください。

- `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 "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`

Active Directoryの読み取り権限を有効にするように**IIS**アプリケーションプールを構成する

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

- 手順 *
  1. SnapCenter がインストールされている Windows サーバーで IIS マネージャーを開きます。
  2. 左側のナビゲーションペインで、 * アプリケーションプール * をクリックします。
  3. ［アプリケーションプール］リストで［SnapCenter］を選択し、［アクション］ペインで［*詳細設定 *］をクリックします。
  4. [ID] を選択し、 [*...] をクリックして SnapCenter アプリケーションプール ID を編集します。
  5. [カスタムアカウント] フィールドに、 Active Directory の読み取り権限を持つドメインユーザーまたはドメイン管理者アカウント名を入力します。
  6. [OK] をクリックします。

     カスタムアカウントは、 SnapCenter アプリケーションプールに組み込まれている ApplicationPoolIdentity アカウントに代わるものです。

監査ログの設定

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。

- このタスクについて *
- アラートは次のシナリオで送信されます。
  - 監査ログの整合性チェック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。

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。

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

- 終了後 *

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。

SnapCenter Standardコントローラベースライセンスを追加

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

コントローラベース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またはストレージクラスタのコマンドラインを使用して、FAS、AFF、またはASAのストレージコントローラに直接追加して有効にします

  SnapCenter コントローラベースのライセンスについては、 SnapCenter GUI にライセンス情報を入力しません。

- コントローラのシリアル番号にロックされています

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

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

SnapCenter GUIを使用して、SnapManager SuiteライセンスがFAS、AFF、またはASAプライマリストレージ

システムにインストールされているかどうかを確認し、SnapManager Suiteライセンスが必要なストレージシステムを特定できます。SnapManager Suiteライセンスは、プライマリストレージシステム上のFAS、AFF、ASA SVMまたはクラスタにのみ適用されます。

コントローラにSnapManager Suiteライセンスがすでにある場合は、SnapCenter Standardコントローラベースライセンスが自動的に提供されます。SnapManagerSuite ライセンスと SnapCenter 標準のコントローラベースのライセンスは同じ意味で使用されますが、同じライセンスを指します。

手順

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

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

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

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

コントローラでは、SnapCenter Standardコントローラベースライセンスが 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、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。

出力例

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

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

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

この例では、 SnapManagerSuite ライセンスをインストールするため、 SnapCenter の追加ライセンスは必要ありません。

手順3：コントローラのシリアル番号を取得します

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

手順

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

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 または AFF ストレージを使用している場合、NetApp Support Siteから SnapCenter コントローラベースのライセンスを取得してから、 ONTAP コマンドラインを使用してインストールできます。

開始する前に

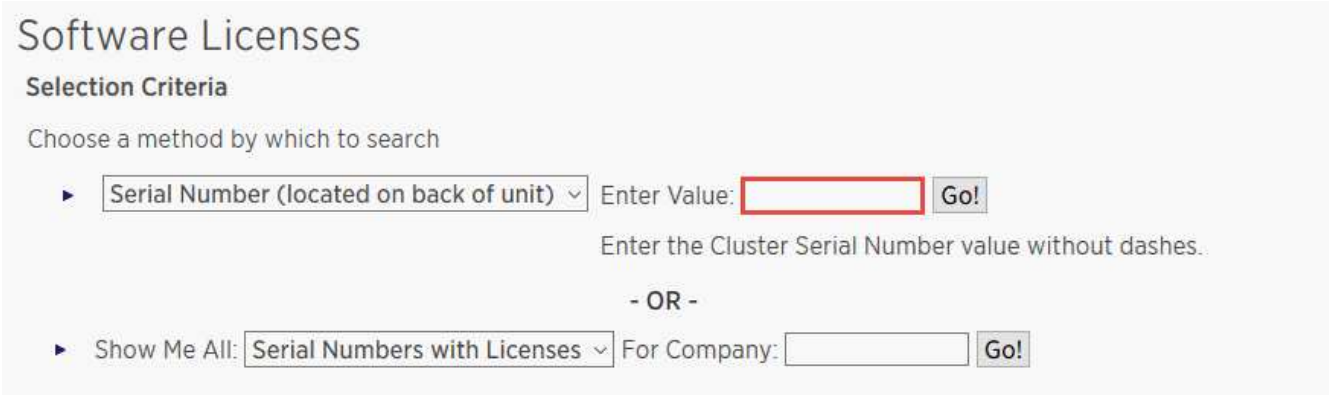
- NetAppサポートサイトの有効なログインクレデンシャルが必要です。

有効なクレデンシャルを入力しないと、検索のための情報は返されません。

- 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 標準ライセンスを使用していて、容量ベースの試用版ライセンス (シリアル番号は「 50 」で終わる) を削除する必要がある場合は、 MySQL コマンドを使用して、試用版ライセンスを手動で削除する必要があります。試用版ライセンスは、SnapCenter GUIでは削除できません。

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. SnapCenterAdminアカウントのSnapCenterサーバとの接続セッションを開始するには、Open-SmConnectionコマンドレットを実行します。
   b. Set-SmRepositoryPasswordを実行してMySQLパスワードをリセットします。

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

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

   パスワードの入力を求められます。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';
```

ストレージシステムのプロビジョニング

Windowsホストでのストレージのプロビジョニング

LUNストレージの設定

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

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

iSCSIセッションを確立する

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。

iSCSIセッションの切断

複数のセッションを使用しているターゲットからiSCSIセッションの切断が必要になる場合があります。

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

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

igroup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。

フィールド	操作
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。

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。

フィールド	操作
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。
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。
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。

プロパティ	説明
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。

選択するオプション	状況
共有ディスク	Windows Serverフェイルオーバークラスタ内のホストでLUNを共有します。 ディスクはフェイルオーバークラスタ内の1つのホスト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

ホストのプロビジョニングやスペース再生のジョブにSnapCenter GUIを使用しない場合は、SnapCenter Plug-in for Microsoft Windowsに付属のPowerShellコマンドレットを使用します。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。

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

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。詳細については、を参照してください "物理ホスト間で仮想マシンをクラスタ化します"。

SnapCenterサーバとのセキュアな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。

インストール時に**Windows**ホストで有効になる機能

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

カテゴリ	機能
Webサーバ	• インターネットインフォメーションサービス • World Wide Webサービス • 一般的なHTTP機能 ◦ 既定のドキュメント ◦ ディレクトリの参照 ◦ HTTPエラー ◦ HTTPリダイレクション ◦ 静的なコンテンツ ◦ WebDAV発行 • 健全性と診断 ◦ カスタムログ ◦ HTTPロギング ◦ ログツール ◦ リクエストモニター ◦ トレース • パフォーマンス機能 ◦ 静的なコンテンツの圧縮 • セキュリティ ◦ IPセキュリティ ◦ Basic Authentication の略 ◦ 一元化されたSSL証明書のサポート ◦ クライアント証明書マッピング認証 ◦ IIS クライアント証明書マッピング認証 ◦ IPおよびドメインの制限 ◦ 要求フィルタリング ◦ URL認証 ◦ Windows認証 • アプリケーション開発機能 ◦ です。 NET拡張性4.5 ◦ アプリケーションの初期化 ◦ ASP。 Net Core Hosting Bundle（8.0.5以降） ◦ サーバー側インクルード ◦ WebSocketプロトコル 管理ツール
	IIS管理コンソール

カテゴリ	機能
IIS管理スクリプトとツール	• IIS管理サービス • Web管理ツール
.NET Framework 8.0.5の機能	• .NET Framework 8.0.5 • ASP。 正味8.0.5 • Windows Communication Foundation (WCF) HTTPアクティブ化45 ◦ TCPのアクティブ化 ◦ HTTPアクティブ化 用。 NET固有のトラブルシューティング情報。を参照してください。 "インターネットに接続されていないレガシーシステムでは、SnapCenter のアップグレードまたはインストールが失敗します"
メッセージキュー	• メッセージキューサービス SnapCenter が作成および管理する MSMQ サービスを他のアプリケーションが使用していないことを確認します。 • RabbitMQ
Windowsプロセスアクティブ化サービス	• プロセスモデル
セツテイAPI	すべて

インストルチユウニLinuxホストテユウコウニナルキノウ

SnapCenterサーバは以下のソフトウェアパッケージをインストールします。これらのパッケージは、トラブルシューティングやホストシステムのメンテナンスに役立ちます。

- RabbitMQ
- nginx
- アーラン
- .NET Framework 8.0.5
- PAM -デベル
- PowerShell