SnapCenter Plug-in for Microsoft SQL Server をインストールする準備をします

SnapCenter Software 4.8

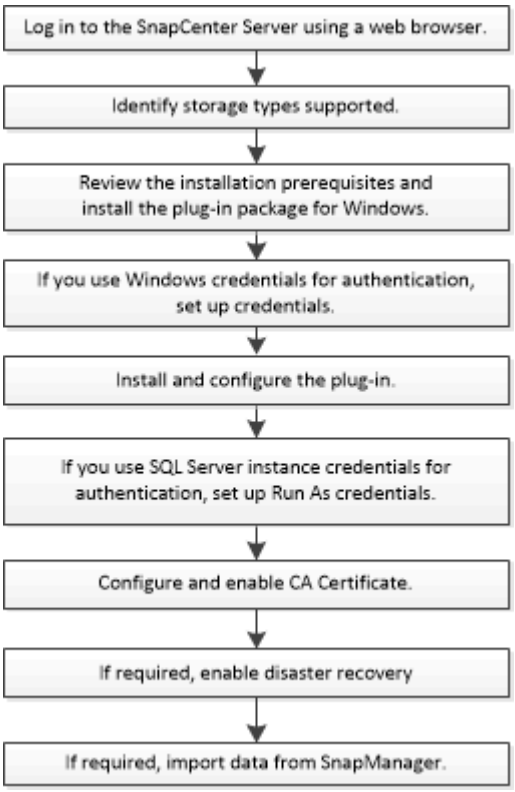
NetApp
January 18, 2024

目次

SnapCenter Plug-in for Microsoft SQL Server をインストールする準備をします

SnapCenter Plug-in for Microsoft SQL Server のインストールワークフロー

SQL Server データベースを保護する場合は、 SnapCenter Plug-in for Microsoft SQL Server をインストールしてセットアップする必要があります。



ホストを追加して SnapCenter Plug-in for Microsoft SQL Server をインストールするための前提条件

ホストを追加してプラグインパッケージをインストールする前に、すべての要件を満たしておく必要があります。

- iSCSI を使用している場合は、 iSCSI サービスが実行されている必要があります。
- リモートホストに対するローカルログイン権限を持つローカル管理者の権限を持つユーザが必要です。
- SnapCenter でクラスタノードを管理する場合は、クラスタ内のすべてのノードに対する管理者権限を持つユーザが必要です。
- SQL Server に対して sysadmin 権限を持つユーザが必要です。

  SnapCenter Plug-in for Microsoft SQL Server は Microsoft VDI Framework を使用しますが、これには sysadmin アクセスが必要です。

"Microsoft のサポート記事 2926557 ：「 SQL Server VDI backup and restore operations require Sysadmin privileges"

- Windows ホストにプラグインをインストールする場合、ビルトインでないクレデンシャルを指定する場合、またはユーザがローカルワークグループユーザに属している場合は、ホストで UAC を無効にする必要があります。
- SnapManager for Microsoft SQL Server がインストールされている場合は、サービスとスケジュールを停止または無効にしておく必要があります。

  バックアップジョブまたはクローンジョブを SnapCenter にインポートする予定の場合は、SnapManager for Microsoft SQL Server をアンインストールしないでください。

- ホストがサーバから完全修飾ドメイン名（ FQDN ）に解決できる必要があります。

  hosts ファイルが解決可能になるように変更され、短縮名と FQDN の両方が hosts ファイルに指定されている場合は、 SnapCenter hosts ファイルに <IP_address> <host_fqdn><host_name> の形式でエントリを作成します

SnapCenter Plug-ins Package for Windows をインストールするホストの要件

SnapCenter Plug-ins Package for Windows をインストールする前に、ホストシステムのいくつかの基本的なスペース要件とサイジング要件を確認しておく必要があります。

項目	要件
オペレーティングシステム	Microsoft Windows の場合 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。
ホスト上の SnapCenter プラグインの最小 RAM	1 GB
ホスト上の SnapCenter プラグインのインストールおよびログの最小スペース	5 GB 十分なディスクスペースを割り当て、logs フォルダによるストレージ消費を監視する必要があります。必要なログスペースは、保護するエンティティの数とデータ保護処理の頻度によって異なります。十分なディスクスペースがない場合、最近実行した処理に対してログは作成されません。

項目	要件
必要なソフトウェアパッケージ	• Microsoft .NET Framework 4.7.2以降 • Windows Management Framework （ WMF ） 4.0 以降 • PowerShell 4.0 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 で確認できます"。

SnapCenter Plug-ins Package for Windows のクレデンシャルを設定します

SnapCenter は、クレデンシャルを使用して SnapCenter 処理を実行するユーザを認証しますSnapCenter プラグインのインストールに必要なクレデンシャル、およびデータベースや Windows ファイルシステムでデータ保護処理を実行するための追加のクレデンシャルを作成する必要があります。

- 必要なもの *
- プラグインのインストール前に Windows クレデンシャルをセットアップする必要があります。
- リモートホストに対する管理者権限を含む、管理者権限でクレデンシャルを設定する必要があります。
- Windows ホストでの SQL 認証

  プラグインのインストール後に SQL クレデンシャルを設定する必要があります。

  SnapCenter Plug-in for Microsoft SQL Server を導入する場合は、プラグインのインストール後に SQL クレデンシャルを設定する必要があります。このクレデンシャルは、 SQL Server の sysadmin 権限を持つユーザに対して設定します。

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

- 手順 *
  1. 左側のナビゲーションペインで、 * 設定 * をクリックします。
  2. [設定] ページで、 [* 資格情報] をクリックします。
  3. [新規作成（ New ）] をクリックする。
  4. [Credential] ページで、クレデンシャルの設定に必要な情報を指定します。

フィールド	手順
クレデンシャル名	クレデンシャルの名前を入力します。
ユーザ名 / パスワード	認証に使用するユーザ名とパスワードを入力します。 • ドメイン管理者 SnapCenter プラグインをインストールするシステムのドメイン管理者を指定します。Username フィールドの有効な形式は次のとおりです。 ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` • 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次のとおりです。 `UserName` パスワードに二重引用符（"）またはバックティック（`）を使用しないでください。 小なり（<）と感嘆符（！）は使用しないでください。 パスワードに記号を追加します。たとえば、lessthan <！10、lessthan10 <！、backtick 12とします。
認証モード	使用する認証モードを選択します。SQL 認証モードを選択した場合は、 SQL Server インスタンスとその SQL インスタンスのホストも指定する必要があります。

5. [OK] をクリックします。

クレデンシャルの設定が完了したら、 [ユーザとアクセス（ User and Access ）] ページで、ユーザまたはユーザグループにクレデンシャルのメンテナンスを割り当てることができます。

個々の SQL Server リソースのクレデンシャルを設定する

クレデンシャルを設定して、各ユーザに対して個々の SQL Server リソースに対してデ

ータ保護ジョブを実行することができます。クレデンシャルはグローバルに設定することもできますが、必要に応じて特定のリソースに対してのみ設定することもできます。

このタスクについて

- Windows クレデンシャルを認証に使用している場合は、プラグインのインストール前にクレデンシャルを設定する必要があります。

  ただし、 SQL Server インスタンスを認証に使用している場合は、プラグインのインストール後にクレデンシャルを追加する必要があります。

- クレデンシャルの設定時に SQL 認証を有効にしている場合は、検出されたインスタンスまたはデータベースに赤色の南京錠のアイコンが表示されます。

  南京錠のアイコンが表示された場合は、インスタンスまたはデータベースのクレデンシャルを指定して、インスタンスまたはデータベースをリソースグループに追加する必要があります。

- 次の条件に該当する場合、 sysadmin アクセスがないロールベースアクセス制御（ RBAC ）ユーザにクレデンシャルを割り当てる必要があります。
  - SQL インスタンスに資格情報が割り当てられます。
  - SQL インスタンスまたはホストが RBAC ユーザに割り当てられている。

    ユーザにはリソースグループとバックアップの両方の権限が必要です。

手順1：クレデンシャルを追加して設定します

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、 [* 資格情報] をクリックします。
   a. 新しい資格情報を追加するには、 * New * をクリックします。
   b. [Credential] ページで、クレデンシャルを設定します。

フィールド	手順
クレデンシャル名	クレデンシャルの名前を入力します。

フィールド	手順
ユーザ名	SQL Server 認証に使用するユーザ名を入力します。 • ドメイン管理者または管理者グループの任意のメンバー ドメイン管理者、または SnapCenter プラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。[**Username**] フィールドの有効な形式は次のとおりです。 ◦ NETBIOS_USERNAME_ ◦ _ ドメイン FQDN\ ユーザ名 _ • 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またはユーザがある場合は、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 ホストシステムでアクセス制御機能が無効になっています。[* ユーザー名 *] フィールドの有効な形式は、 *username* です
パスワード	認証に使用するパスワードを入力します。
認証モード	SQL Server 認証モードを選択します。 SQL Server に対する sysadmin 権限がある Windows ユーザの場合は、 Windows 認証を選択することもできます。
ホスト	ホストを選択します。
SQL Serverインスタンス	SQL Server インスタンスを選択します。

c. [OK] をクリックしてクレデンシャルを追加します。

ステップ**2**：インスタンスを構成します

1. 左側のナビゲーションペインで、 * リソース * をクリックします。
2. [リソース] ページで、 [* 表示 *] リストから [* インスタンス *] を選択します。
   a. をクリックします をクリックし、ホスト名を選択してインスタンスをフィルタリングします。
   b. をクリックします をクリックしてフィルタペインを閉じます。
3. Instance Protect （インスタンス保護）ページで、インスタンスを保護し、必要に応じて、 Configure Credentials （資格情報の設定） * をクリックします。

   SnapCenter サーバにログインしているユーザが SnapCenter プラグイン for Microsoft SQL Server にアクセスできない場合は、そのユーザがクレデンシャルを設定する必要があります。

   クレデンシャルオプションは、データベースおよび可用性グループには適用されません。

4. [リソースの更新] をクリックします。

Windows Server 2012 以降で gMSA を構成します

Windows Server 2012 以降では、管理ドメインアカウントからサービスアカウントパスワードの自動管理を提供するグループマネージドサービスアカウント（ gMSA ）を作成できます。

- 必要なもの *
- Windows Server 2012 以降のドメインコントローラが必要です。
- ドメインのメンバーである Windows Server 2012 以降のホストが必要です。
- 手順 *

1. GMSA のオブジェクトごとに固有のパスワードを生成するには、 KDS ルートキーを作成します。
2. ドメインごとに、 Windows ドメインコントローラから次のコマンドを実行します。 Add-KDSRootKey -EffectiveImmedient
3. GMSA を作成して構成します。
   a. 次の形式でユーザグループアカウントを作成します。

```
 domainName\accountName$
.. グループにコンピュータオブジェクトを追加します。
.. 作成したユーザグループを使用して gMSA を作成します。
```

   例：

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName
<fqdn> -PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. を実行します `Get-ADServiceAccount`
サービスアカウントを確認するコマンド。
```

4. ホストで gMSA を設定します。
   a. gMSA アカウントを使用するホストで、 Windows PowerShell 用の Active Directory モジュールを有効にします。

      そのためには、 PowerShell から次のコマンドを実行します。

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                                Name                Install State
------------                                ----                -------------
[ ] Active Directory Domain Services   AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. ホストを再起動します。

b. PowerShellコマンドプロンプトから次のコマンドを実行して、ホストにgMSAをインストールします。 `Install-AdServiceAccount <gMSA>`

c. 次のコマンドを実行して'gMSAアカウントを確認します `Test-AdServiceAccount <gMSA>`

1. ホスト上で設定されている gMSA に管理者権限を割り当てます。
2. SnapCenter サーバで設定済みの gMSA アカウントを指定して、 Windows ホストを追加します。

   SnapCenter サーバーは選択されたプラグインをホストにインストールし、指定された gMSA はプラグインのインストール時にサービスログオンアカウントとして使用されます。

SnapCenter Plug-in for Microsoft SQL Server をインストールします

ホストを追加し、 SnapCenter Plug-ins Package for Windows をインストールします

ホストの追加およびプラグインパッケージのインストールには、 SnapCenter * ホストの追加ページを使用する必要があります。プラグインは、自動的にリモートホストにインストールされます。

- 必要なもの *
- SnapCenter Admin ロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが必要です。
- Windows ホストにプラグインをインストールするときに、ビルトインでないクレデンシャルを指定する場合は、ホストで UAC を無効にします。
- メッセージキューイングサービスが実行中状態であることを確認する必要があります。

- Group Managed Service Account （ gMSA ；グループ管理サービスアカウント）を使用している場合は、管理者権限を持つ gMSA を設定する必要があります。

  "Windows Server 2012 以降で SQL 用のグループマネージドサービスアカウントを設定します"

- このタスクについて *

SnapCenter サーバをプラグインホストとして別の SnapCenter サーバに追加することはできません。

ホストの追加とプラグインパッケージのインストールは、個々のホストまたはクラスタに対して実行できます。クラスタまたは Windows Server Failover Clustering （ WSFC ）にプラグインをインストールする場合、プラグインはクラスタのすべてのノードにインストールされます。

ホストの管理の詳細については、を参照してください "ホストを管理します"。

- 手順 *

1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
2. 上部で [Managed Hosts] タブが選択されていることを確認します。
3. [追加（ Add ）] をクリックします。
4. Hosts ページで、次の手順を実行します。

フィールド	手順
ホストタイプ	ホストタイプとして Windows を選択します。 SnapCenter サーバによってホストが追加され、ホストに Plug-in for Windows がインストールされていない場合はインストールされます。 [プラグイン] ページで [Microsoft SQL Server] オプションを選択すると、 SnapCenter サーバによって Plug-in for SQL Server がインストールされます。
ホスト名	ホストの完全修飾ドメイン名（ FQDN ）または IP アドレスを入力します。 信頼されていないドメインホストの IP アドレスは、 FQDN に解決される場合にのみサポートされます。 SnapCenter は、 DNS の適切な設定によって異なります。そのため、 FQDN を入力することを推奨します。 次のいずれかの IP アドレスまたは FQDN を入力できます。 • スタンドアロンホスト • WSFC SnapCenter を使用してホストを追加する際、ホストがサブドメインの一部である場合は、 FQDN を指定する必要があります。

フィールド	手順
クレデンシャル	作成したクレデンシャルの名前を選択するか、新しいクレデンシャルを作成します。 このクレデンシャルには、リモートホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。 クレデンシャルの詳細を表示するには、指定したクレデンシャル名にカーソルを合わせます。 クレデンシャル認証モードは、ホストの追加ウィザードで指定したホストタイプによって決まります。

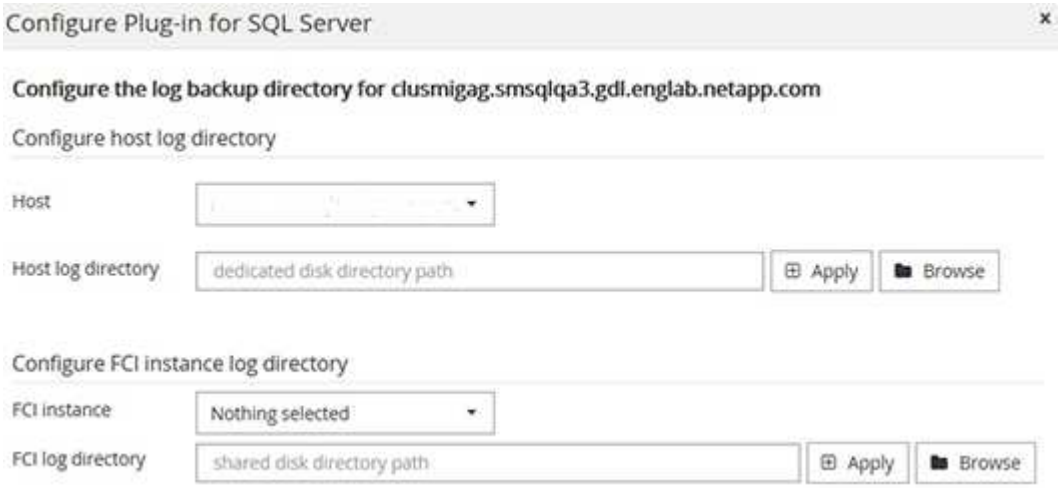
5. [インストールするプラグインを選択してください *] セクションで、インストールするプラグインを選択します。
6. [* その他のオプション *] をクリックします。

フィールド	手順
ポート	デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。 デフォルトのポート番号は 8145 です。SnapCenter サーバがカスタムポートにインストールされている場合は、そのポート番号がデフォルトポートとして表示されます。 プラグインを手動でインストールし、カスタムポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理は失敗します。
インストールパス	デフォルトパスは C ： \Program Files\NetApp\SnapManager です。必要に応じて、パスをカスタマイズできます。
クラスタ内のすべてのホストを追加します	WSFC または SQL 可用性グループ内のすべてのクラスタノードを追加するには、このチェックボックスを選択します。 クラスタ内の複数の使用可能な SQL 可用性グループを管理および識別するには、 GUI で適切なクラスタチェックボックスを選択して、すべてのクラスタノードを追加する必要があります。

フィールド	手順
インストール前のチェックをスキップします	プラグインを手動でインストール済みで、プラグインのインストール要件をホストが満たしているかどうかを検証しない場合は、このチェックボックスを選択します。
プラグインサービスを実行するには、 Group Managed Service Account （ gMSA ；グループ管理サービスアカウント）を使用します	グループ管理サービスアカウント（ GMSA ）を使用してプラグインサービスを実行する場合は、このチェックボックスをオンにします。 gMSA 名を domainName\accountName$ の形式で指定します。 ホストが gMSA とともに追加され 'gMSA にログイン権限と sys 管理権限がある場合は 'gMSA を使用して SQL インスタンスに接続します

7. [Submit （送信）] をクリックします。
8. SQL Plug-in の場合、ログディレクトリを設定するホストを選択します。
   a. ログディレクトリの設定 * をクリックし、ホストログディレクトリの設定ページで * 参照 * をクリックして、次の手順を実行します。

      ネットアップ LUN （ドライブ）のみが選択対象として表示されます。SnapCenter は、バックアップ処理の一環として、ホストログディレクトリをバックアップしてレプリケートします。



      i. ホストログを格納するホスト上のドライブレターまたはマウントポイントを選択します。
      ii. 必要に応じてサブディレクトリを選択します。
      iii. [保存（ Save ）] をクリックします。
9. [Submit （送信）] をクリックします。

[事前確認をスキップ] チェックボックスをオンにしていない場合、プラグインをインストールするための要件をホストが満たしているかどうかが検証されます。ディスクスペース、 RAM 、 PowerShell

のバージョン、 .NET のバージョン、場所（ Windows プラグインの場合）、および Java のバージョン（ Linux プラグインの場合）が、最小要件に照らして検証されます。最小要件を満たしていない場合は、対応するエラーまたは警告メッセージが表示されます。

エラーがディスクスペースまたは RAM に関連している場合は、 C ： \Program Files\NetApp\SnapManager WebApp にある web.config ファイルを更新してデフォルト値を変更することができます。エラーが他のパラメータに関連している場合は、問題を修正する必要があります。

HA セットアップで web.config ファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

1. インストールの進行状況を監視します。

コマンドレットを使用して、複数のリモートホストに **SnapCenter Plug-in for Microsoft SQL Server** をインストールします

SmHostPackage PowerShell コマンドレットを使用して、複数のホストに SnapCenter Plug-in for Microsoft SQL Server を同時にインストールできます。

- 必要なもの *

プラグインパッケージをインストールする各ホストで、ローカル管理者の権限を持つドメインユーザとして SnapCenter にログインしている必要があります。

- 手順 *

1. PowerShell を起動します。
2. SnapCenter サーバホストで、 Open-SmConnection コマンドレットを使用してセッションを確立し、クレデンシャルを入力します。
3. Install-SmHostPackage コマンドレットと必要なパラメータを使用して、複数のリモートホストに SnapCenter Plug-in for Microsoft SQL Server をインストールします。

   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"。

プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、 -skipprecheck オプションを使用できます。

1. リモートインストールのクレデンシャルを入力します。

コマンドラインから **SnapCenter Plug-in for Microsoft SQL Server** をサイレントインストールします

SnapCenter Plug-in for Microsoft SQL Server は、 SnapCenter ユーザインターフェイス内からインストールする必要があります。ただし、何らかの理由でインストールできない場合は、 Windows のコマンドラインから、 Plug-in for SQL Server のインストールプログラムをサイレントモードで自動的に実行できます。

- 必要なもの *
- をインストールする前に、以前のバージョンの SnapCenter Plug-in for Microsoft SQL Server を削除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 "SnapCenter Plug-in をプラグインホストから手動で直接インストールする方法"。

- 手順 *

1. C ： \temp フォルダがプラグインホストに存在し、ログインしているユーザにそのフォルダへのフルアクセス権があるかどうかを確認してください。
2. C ： \ProgramData\NetApp\SnapCenter \Package Repository から Plug-in for SQL Server ソフトウェアをダウンロードします。

   このパスには、 SnapCenter サーバがインストールされているホストからアクセスできます。

3. プラグインをインストールするホストにインストールファイルをコピーします。
4. ローカルホストの Windows コマンドプロンプトで、プラグインのインストールファイルを保存したディレクトリに移動します。
5. Plug-in for SQL Server ソフトウェアをインストールします。

   ```
   "snapcenter_windows_host_plugin.exe"/silent /debuglog"Debug_Log_Path"
   /log"Log_Path" BI_SNAPCENTER_PORT=Num
   SUITE_INSTALLDIR="Install_Directory_Path"
   BI_SERVICEACCOUNT=domain\\administrator BI_SERVICEPWD=password
   ISFeatureInstall=SCW,SCSQL
   ```

   プレースホルダの値をデータに置き換えます

   - debug_log_Path は、スイートインストーラログファイルの名前と場所です。
   - LOG_Path はプラグインコンポーネント（ SCW 、 SCSQL 、および SMCore ）のインストールログの場所です。
   - num は、 SnapCenter が SMCore と通信するポートです
   - install_Directory_Path は、ホストプラグインパッケージのインストールディレクトリです。
   - domain\administrator は、 SnapCenter Plug-in for Microsoft Windows の Web サービスアカウントです。
   - password は、 SnapCenter Plug-in for Microsoft Windows Web サービスアカウントのパスワードです。 [+] `"snapcenter_windows_host_plugin.exe"/silent /debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145 SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter" BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password ISFeatureInstall=SCW,SCSQL`

   Plug-in for SQL Server のインストール時に渡されるすべてのパラメータでは、大文字と小文字が区別されます。

1. Windows タスクスケジューラ、メインインストールログファイル C:\Installdebug.log 、および C:\Temp 内の追加インストールファイルを監視します。

2. %temp% ディレクトリを監視して、 msiexe.exe インストーラがエラーなしでソフトウェアをインストールしていることを確認します。

Plug-in for SQL Server をインストールすると、 SnapCenter Server ではなくホストにプラグインが登録されます。SnapCenter サーバにプラグインを登録するには、 SnapCenter GUI または PowerShell コマンドレットを使用してホストを追加します。ホストを追加すると、プラグインが自動的に検出されます。

Plug-in for SQL Server のインストールのステータスを監視します

SnapCenter プラグインパッケージのインストールの進捗状況は、 Jobs ページで監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題があるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- 手順 *
  1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
  2. [モニター] ページで、 [* ジョブ *] をクリックします。
  3. [ジョブ] ページで、プラグインのインストール操作だけが表示されるようにリストをフィルタリングするには、次の手順を実行します。
     a. [* フィルタ * （ Filter * ）] をクリック
     b. オプション：開始日と終了日を指定します。
     c. タイプドロップダウンメニューから、 * プラグインインストール * を選択します。
     d. Status ドロップダウンメニューから、インストールステータスを選択します。
     e. [適用（ Apply ）] をクリックします。
  4. インストールジョブを選択し、 ［ * 詳細 * ］ をクリックしてジョブの詳細を表示します。
  5. ［ ジョブの詳細 ］ ページで、 ［ * ログの表示 * ］ をクリックします。

CA 証明書を設定します

CA 証明書 CSR ファイルを生成します

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

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

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

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

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

CA 証明書をインポートする

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

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

ウィザードウィンドウ	実行する処理
秘密鍵をインポートします	オプション * はい * を選択し、秘密鍵をインポートして、 * 次へ * をクリックします。
インポートファイル形式	変更せずに、 * 次へ * をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、 * Next * をクリックします。

ウィザードウィンドウ	実行する処理
証明書のインポートウィザードを完了しています	概要を確認し、 [完了] をクリックしてインポートを開始します。

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

7. 「 Personal 」フォルダについて、手順 5 を繰り返します。

CA 証明書のサムプリントを取得します

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

- 手順 *

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

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

2. PowerShell で次の手順を実行します。
   a. 次のコマンドを実行して、インストールされている証明書のサムプリントを一覧表示し、最近インストールされた証明書を件名で識別します。

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

   b. サムプリントをコピーします。

Windows ホストプラグインサービスを使用して CA 証明書を設定する

CA 証明書に Windows ホストプラグインサービスを設定して、インストールされたデジタル証明書をアクティブ化する必要があります。

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

- 手順 *

1. 次のコマンドを実行して、 SMCore のデフォルトポート 8145 にバインドされている既存の証明書を削除します。

```
> netsh http delete 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 ホストプラグインサービスにバインドします。

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

例：

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

プラグインの CA 証明書を有効にします

CA 証明書を設定し、 SnapCenter サーバと対応するプラグインホストに CA 証明書を導入する必要があります。 プラグインの CA 証明書検証を有効にする必要があります。

- 必要なもの *
- CA 証明書を有効または無効にするには、 run_Set-SmCertificateSetting_cmdlet を使用します。
- このプラグインの証明書ステータスは、 *Get-SmCertificateSettings* 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. 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、 [*Managed Hosts] をクリックします。
  3. 1 つまたは複数のプラグインホストを選択します。
  4. [* その他のオプション *] をクリックします。
  5. [証明書の検証を有効にする] を選択します。
- 終了後 *

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

- は、 CA 証明書が有効になっておらず、プラグインホストにも割り当てられていないことを示します。
- CA 証明書が正常に検証されたことを示します。
- は、 CA 証明書を検証できなかったことを示します。
- 接続情報を取得できなかったことを示します。

ステータスが黄色または緑のときは、データ保護処理が正常に完了しています。

ディザスタリカバリを設定

SnapCenter Plug-in for SQL Server のディザスタリカバリ

SnapCenter Plug-in for SQL Serverが停止した場合は、次の手順を実行して別のSQLホストに切り替え、データをリカバリします。

必要なもの

- セカンダリホストのオペレーティングシステム、アプリケーション、およびホスト名は、プライマリホストと同じにする必要があります。
- [ホストの追加] または [ホストの変更] ページを使用して、 SnapCenter Plug-in for SQL Server を別のホストにプッシュします。を参照してください "ホストを管理します" を参照してください。

手順

1. [*Hosts] ページからホストを選択して、 SnapCenter Plug-in for SQL Server を変更およびインストールします。
2. （オプション） SnapCenter Plug-in for SQL Server の構成ファイルをディザスタリカバリ（ DR ）バックアップから新しいマシンに置き換えます。
3. Windows スケジュールと SQL スケジュールを、 DR バックアップから SnapCenter Plug-in for SQL Server フォルダからインポートします。

を参照してください。

を参照してください "ディザスタリカバリ API" ビデオ：

SnapCenter Plug-in for SQL Server の Storage Disaster Recovery （ DR ；ストレージディザスタリカバリ）

SnapCenter Plug-in for SQL Server ストレージをリカバリするには、グローバル設定ページでストレージの DR モードを有効にします。

- 必要なもの *
- プラグインがメンテナンスモードになっていることを確認します。
- SnapMirror / SnapVault 関係を解除 "SnapMirror 関係を解除します"

- セカンダリの LUN を、同じドライブレターを使用してホストマシンに接続します。
- DR の前に使用したのと同じドライブレターを使用して、すべてのディスクが接続されていることを確認してください。
- MSSQL サーバサービスを再起動します。
- SQL リソースがオンラインに戻っていることを確認します。
- このタスクについて *

ディザスタリカバリ（ DR ）は、 VMDK 構成と RDM 構成ではサポートされていません。

- 手順 *
  1. 設定ページで、 * 設定 * > * グローバル設定 * > * ディザスタ・リカバリ * と進みます。
  2. [Enable Disaster Recovery] を選択します。
  3. [適用（ Apply ）] をクリックします。
  4. DR ジョブが有効になっているかどうかを確認するには、 * Monitor * > * Jobs * をクリックします。
- 終了後 *
- フェイルオーバー後に新しいデータベースが作成されると、データベースは非 DR モードになります。

  新しいデータベースは、フェイルオーバー前と同様に動作します。

- DR モードで作成された新しいバックアップは、トポロジページの SnapMirror または SnapVault （セカンダリ）の下に表示されます。

  新しいバックアップの横に「 i 」アイコンが表示され、 DR モードで作成されたバックアップであることが示されます。

- フェイルオーバー時に作成されたSnapCenter Plug-in for SQL Serverのバックアップは、UIまたは次のコマンドレットを使用して削除できます。 `Remove-SmBackup`
- フェイルオーバー後、一部のリソースをDR以外のモードにするには、次のコマンドレットを使用します。 `Remove-SmResourceDRMode`

  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"。

- SnapCenter サーバは、 DR モードまたは非 DR モードの個々のストレージリソース（ SQL データベース）を管理しますが、 DR モードまたは非 DR モードのストレージリソースを含むリソースグループは管理しません。

SnapCenter Plug-in for SQL Server のセカンダリストレージからプライマリストレージへのフェイルバック

SnapCenter Plug-in for SQL Server のプライマリストレージがオンラインに戻ったら、プライマリストレージにフェイルバックする必要があります。

- 必要なもの *
- Managed Hosts ページから SnapCenter Plug-in for SQL Server を * Maintenance * モードにします。
- セカンダリストレージをホストから切断して、プライマリストレージから接続します。

- プライマリストレージにフェイルバックするには、逆再同期処理を実行して、フェイルオーバー前と同じ関係の方向が維持されることを確認します。

  逆再同期処理後もプライマリストレージとセカンダリストレージの役割を維持するには、逆再同期処理をもう一度実行します。

  詳細については、を参照してください "ミラー関係を逆再同期しています"

- MSSQL サーバサービスを再起動します。
- SQL リソースがオンラインに戻っていることを確認します。

> プラグインのフェイルオーバーまたはフェイルバックの実行中は、プラグインの全体的なステータスはすぐには更新されません。ホストおよびプラグインの全体的なステータスは、以降のホスト更新処理中に更新されます。

- 手順 *
  1. 設定ページで、 * 設定 * > * グローバル設定 * > * ディザスタ・リカバリ * と進みます。
  2. [Enable Disaster Recovery] を選択解除します。
  3. [適用（ Apply ）] をクリックします。
  4. DR ジョブが有効になっているかどうかを確認するには、 * Monitor * > * Jobs * をクリックします。
- 終了後 *
- フェイルオーバー時に作成されたSnapCenter Plug-in for SQL Serverのバックアップは、UIまたは次のコマンドレットを使用して削除できます。 `Remove-SmDRFailoverBackups`

著作権に関する情報

商標に関する情報