SnapCenter Plug-in for Microsoft SQL Serverのインストールの準備

SnapCenter Software 5.0

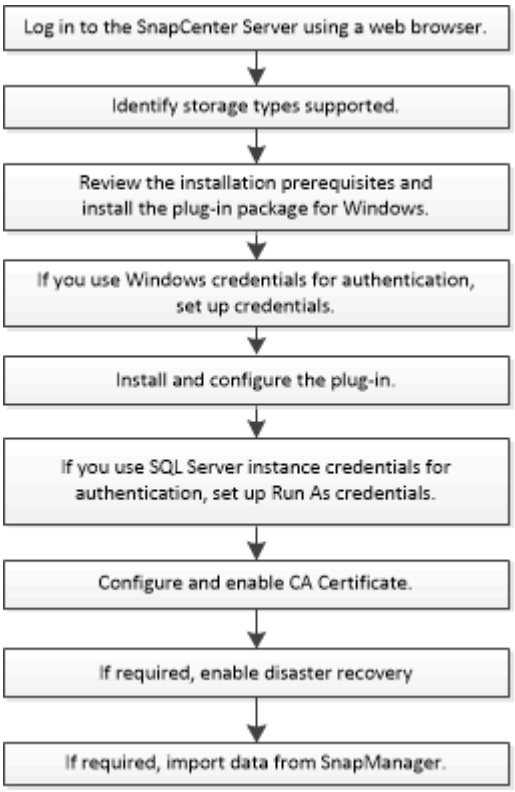
NetApp
July 18, 2024

目次

SnapCenter Plug-in for Microsoft SQL Serverのインストールの準備

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に対する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ときに、組み込みでないクレデンシャルを指定した場合やユーザがローカルワークグループに属している場合は、ホストの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。

- ホストを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、基本的なホストシステムのスペース要件とサイジング要件を理解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 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 "NetApp Interoperability Matrix Tool" ください。
ホスト上のSnapCenterプラグイン用の最小RAM	1 GB
ホスト上のSnapCenterプラグインのインストールと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量を監視する必要があります。必要なログスペースは、保護対象の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、最近実行した処理の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 "NetApp Interoperability Matrix Tool" ください。 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従来型システムでは、SnapCenter のアップグレードまたはインストールが失敗します。"

SnapCenter Plug-ins Package for Windowsのクレデンシャルを設定する

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。

開始する前に

- プラグインをインストールする前にWindows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には、管理者権限（リモートホストに対する管理者権限を含む）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。SQL Serverのsysadmin権限を持つユーザのクレデンシャルを設定します。

  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完了し、リソースを更新する必要があります。SQL Server認証は、リソースのスケジュール設定や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. [クレデンシャル]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	操作
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インスタンスとそれが配置されている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、必要に応じて[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の設定

各ユーザの個 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ためのクレデンシャルを設定できます。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。

タスクの内容

- 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認証を有効にした場合は、検出されたインスタンスまたはデータベースに赤い南京錠のアイコンが表示されます。

  南京錠アイコンが表示された場合、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には、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する必要があります。

- 次の条件に該当する場合は、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。
  - クレデンシャルがSQLインスタンスに割り当てられます。
  - 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]*を選択します。
2. [設定]ページで、*[クレデンシャル]*を選択します。
   a. 新しいクレデンシャルを追加するには、*[New]*を選択します。
   b. [クレデンシャル]ページで、クレデンシャルを設定します。

フィールド	操作
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	操作
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は、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または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 _ • ローカル管理者（ワークグループの場合のみ）ワークグループに属するシステムの場合は、SnapCenterプラグインをインストールするシステムのビルトインローカル管理者を指定します。 ユーザアカウントに昇格された権限がある場合、またはホストシステムでユーザアクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカルユーザアカウントを指定できます。[* ユーザー名 *] フィールドの有効な形式は、 *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。WindowsユーザにSQL Serverに対するsysadmin権限がある場合は、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]*を選択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]*を選択します。
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. を選択し [フィルタアイコン]、ホスト名を選択してインスタンスをフィルタします。
   b. フィルタペインを閉じる場合に選択し [フィルタアイコン] ます。
3. [インスタンスの保護]ページで、インスタンスを保護し、必要に応じて*[クレデンシャルの設定]*を選択します。

   SnapCenterサーバにログインしているユーザがSnapCenter Plug-in for Microsoft SQL Serverにアクセスできない場合は、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. [リソースを更新]を選択します。

Windows Server 2012以降でのgMSAの設定

Windows Server 2012以降では、管理対象ドメインアカウントからサービスアカウントのパスワードを自動管理するグループ管理サービスアカウント（gMSA）を作成できます。

開始する前に

- 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. KDSルートキーを作成して、gMSA内のオブジェクトごとに一意のパスワードを生成します。
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を作成して設定します。
   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$
      ```

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

      例えば、

      ```
      New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
      -PrincipalsAllowedToRetrieveManagedPassword <group>
      -ServicePrincipalNames <SPN1,SPN2,…>
      ```

      .. コマンドを実行し `Get-ADServiceAccount` てサービスアカウントを確認します。

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Active Directoryモジュールを有効にします。

      これを行うには、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で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>`

5. ホスト上の設定済みgMSAに管理者権限を割り当てます。

6. 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。

   選択したプラグインがSnapCenterサーバにインストールされ、指定したgMSAがプラグインのインストール時にサービスの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のインストール

ホストを追加して**SnapCenter Plug-ins Package for Windows**をインストールする

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。プラグインはリモートホストに自動的にインストールされます。

開始する前に

- 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。
- 組み込みでないクレデンシャルを指定してWindowsホストにプラグインをインストールする場合は、ホストのUACを無効にする必要があります。
- メッセージキューサービスがrunning状態であることを確認する必要があります。
- グループ管理サービスアカウント（gMSA）を使用する場合は、管理者権限で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"

タスクの内容

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、ホストごとまたはクラスタごとに実行できます。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。

ホストの管理については、を参照してください "ホストの管理"。

手順

1. 左側のナビゲーションペインで、 **Hosts** を選択します。
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」を選択します。
4. [Hosts]ページで、次の手順を実行します。

フィールド	操作
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。 [Plug-ins]ページで[Microsoft SQL Server]オプションを選択すると、SnapCenter Server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ときに、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	操作
クレデンシャ	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。 指定したクレデンシャルの名前にカーソルを合わせると、クレデンシャルの詳細を確認できます。 クレデンシャルの認証モードは、ホスト追加ウィザードで指定するホストタイプによって決まります。

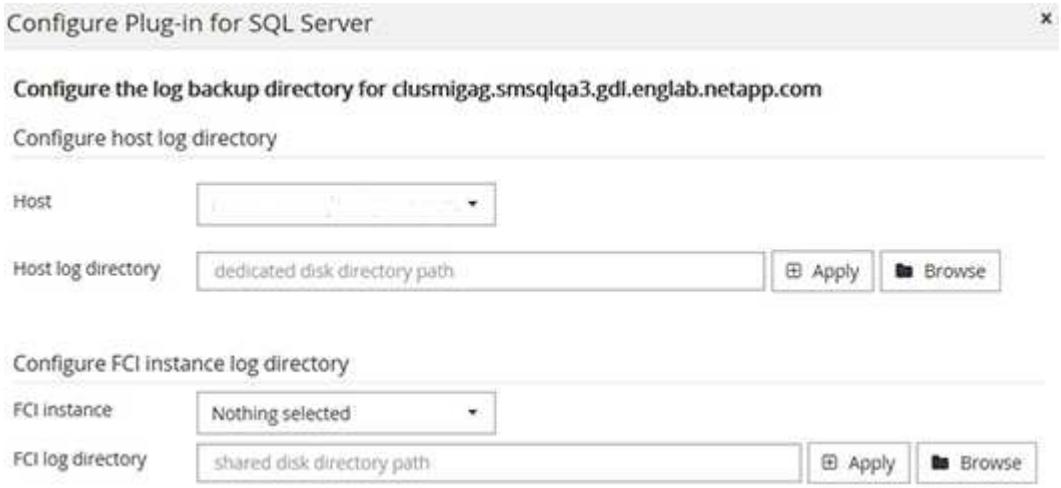
5. [インストールするプラグインを選択してください *] セクションで、インストールするプラグインを選択します。
6. [* その他のオプション *] を選択します。

フィールド	操作
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	デフォルトのパスはC：\Program Files\NetApp\SnapCenter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	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オンにします。クラスタ内で使用可能な複数のSQL可用性グループを管理および識別する場合は、GUIで該当するクラスタの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。
インストール前チェックをスキップ	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、このチェックボックスを選択します。

フィールド	操作
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	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選択します。 gMSA名をdomainName\accountName$の形式で指定してください。 gMSAでホストを追加し、gMSAにログイン権限とsys admin権限がある場合は、gMSAを使用してSQLインスタンスに接続されます。

7. [送信] を選択します。
8. SQL Plug-inの場合は、ログディレクトリを設定するホストを選択します。
   a. を選択し、**[**ホストログディレクトリの設定**]**ページで[参照]*を選択して、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 ）] を選択します。
9. [送信] を選択します。

[インストール前チェックをスキップ]*チェックボックスを選択していない場合は、プラグインをインストールするための要件を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バージョン、場所（Windowsプラグインの場合）、およびJava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、該当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\SnapCenter WebAppにあるweb.configファイルを更新してデフォルト値を変更できます。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。

10. 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た複数のリモートホストへの**SnapCenter Plug-in for Microsoft SQL Server**のインストール

PowerShellコマンドレットInstall-SmHostPackageを使用すると、SnapCenter Plug-in for Microsoft SQL Serverを複数のホストに同時にインストールできます。

開始する前に

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。

4. 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の**SnapCenter Plug-in for Microsoft SQL Server**のサイレントインストール

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。

開始する前に

- 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があるかどうかを検証します。
2. Plug-in for SQL ServerソフトウェアをC：\ProgramData\NetApp\SnapCenter\Package Repositoryから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。
6. 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。
7. %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く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 GUIまたはPowerShellコマンドレットを使用してホストを追加することで、SnapCenterサーバにプラグインを登録できます。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のインストールステータスの監視

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発生していないかどうかを確認できます。

タスクの内容

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
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み

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. [* Monitor*] ページで、 [* Jobs] 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処理のみ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"
```

プラグインに対して**CA**証明書を有効にする

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、 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. プラグインホストを1つまたは複数選択します。
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、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。
- ** 🔒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。

ディザスタリカバリの設定

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、次の手順に従って別のSQLホストに切り替えてデータをリカバリします。

開始する前に

- 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である必要があります。
- [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。詳細については、を参照してください "ホストの管理" 。

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およびSQLスケジュールを、DRバックアップのSnapCenter Plug-in for SQL Serverフォルダからインポートします。

関連情報

ビデオを参照してください "ディザスタリカバリ API" 。

SnapCenter Plug-in for SQL Server向けストレージディザスタリカバリ（DR）

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。

開始する前に

- プラグインがメンテナンスモードであることを確認します。
- SnapMirror / SnapVault関係を解除 "SnapMirror関係の解除"
- セカンダリのLUNを同じドライブレターでホストマシンに接続します。
- すべてのディスクが、DRの前に使用していたのと同じドライブレターを使用して接続されていることを確認します。
- MSSQLサーバー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。

タスクの内容

VMDKおよびRDM構成ではディザスタリカバリ（DR）はサポートされません。

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じように動作し続けます。

- DRモードで作成された新しいバックアップは、[Topology]ページの[SnapMirror]またはSnapVault（secondary）]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、これらのバックアップがDRモード中に作成されたことを示します。

- フェイルオーバー中に作成された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に一部のリソースをDR以外のモードにする場合は、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 "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。

- 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。

開始する前に

- 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、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、関係の方向がフェイルオーバー前と同じであることを確認します。

  逆再同期処理の実行後もプライマリストレージとセカンダリストレージのロールを保持するには、逆再同期処理をもう一度実行します。

  詳細については、 "ミラー関係を逆再同期しています"

- MSSQLサーバー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中、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、次回のホスト更新処理で更新されます。

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

フェイルオーバー中に作成された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