



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

SnapCenter Software 4.8

NetApp
January 18, 2024

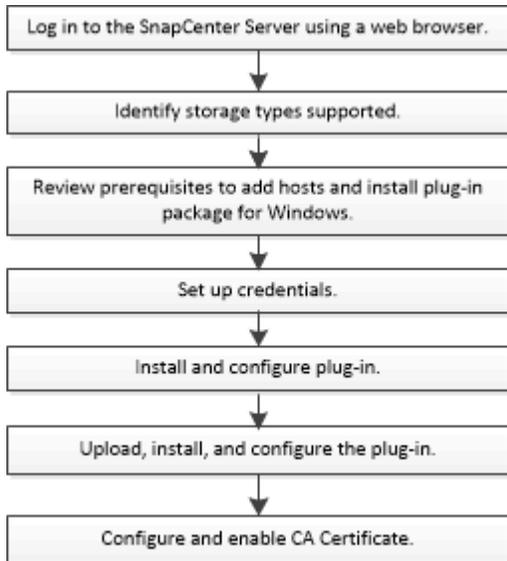
目次

SnapCenter Plug-in for Microsoft Exchange Server をインストールします	1
SnapCenter Plug-in for Microsoft Exchange Server のインストールワークフロー	1
ホストを追加して SnapCenter Plug-in for Microsoft Exchange Server をインストールするための前提条件	1
SnapCenter Plug-in for Windows のクレデンシャルを設定します	5
Windows Server 2012 以降で gMSA を構成します	6
ホストを追加し、 Plug-in for Exchange をインストールします	8
PowerShell コマンドレットを使用して、 SnapCenter サーバホストから Plug-in for Exchange をインストールします	12
コマンドラインから SnapCenter Plug-in for Exchange をサイレントにインストールします	13
SnapCenter プラグインパッケージのインストールステータスを監視する	15
CA 証明書を設定します	15
Exchange と SnapCenter が共存するように SnapManager 7.x を設定します	19

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

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

Exchange データベースを保護する場合は、SnapCenter Plug-in for Microsoft Exchange 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 Exchange 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。
- ローカル管理者権限を持つドメインユーザがあり、リモートホストに対してローカルログイン権限が付与されている必要があります。
- スタンドアロン構成およびデータベース可用性グループ構成で Microsoft Exchange Server 2013、2016、または 2019 を使用している必要があります。
- 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。
- 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。
- Exchange Server に対する管理者権限を持つユーザが必要です。
- SnapManager for Microsoft Exchange Server および SnapDrive for Windows がすでにインストールされている場合は、SnapDrive を使用してデータを確実に保護するために、同じ Exchange サーバに Plug-in for

Exchange をインストールする前に、SnapCenter for Windows で使用する VSS ハードウェアプロバイダの登録を解除する必要があります。

- SnapManager for Microsoft Exchange Server と Plug-in for Exchange が同じサーバにインストールされている場合は、SnapManager for Microsoft Exchange Server で作成されたすべてのスケジュールを Windows スケジューラから一時停止または削除する必要があります。
- 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 ファイルに次の形式でエントリを作成します： `_<IP_address>
<host_fqdn><host_name> _`。
- 次のポートがファイアウォールでブロックされていないことを確認してください。ブロックされていないとホストの追加操作が失敗します。この問題を解決するには、ダイナミックポート範囲を設定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 "Microsoft のドキュメント"](#)。
 - Windows 2016 および Exchange 2016 のポート範囲 50000 ~ 51000
 - Windows Server 2012 R2 および Exchange 2013 用のポート範囲 6000-6500
 - Windows 2019 のポート範囲は 49152~65536 です

ポート範囲を特定するには、次のコマンドを実行します。



- `netsh int ipv4 show dynamicport tcp`
- `netsh int ipv4 show dynamicport udp`
- `netsh int ipv6 show dynamicport tcp` を実行します
- `netsh int ipv6 show dynamicport udp`

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

項目	要件
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 <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>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。</p> </div>
必要なソフトウェアパッケージ	<ul style="list-style-type: none"> • Microsoft .NET Framework 4.7.2以降 • Windows Management Framework (WMF) 4.0 以降 • PowerShell 4.0 以降 <p>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"。</p>

Exchange Server の権限が必要です

SnapCenter で Exchange サーバまたは DAG を追加し、ホストまたは DAG に SnapCenter Plug-in for Microsoft Exchange Server をインストールできるようにするには、最小限の権限と権限を持つユーザのクレデンシャルを SnapCenter に設定する必要があります。

ローカル管理者の権限を持つドメインユーザと、リモート Exchange ホストに対するローカルログイン権限、および DAG 内のすべてのノードに対する管理権限を持つドメインユーザが必要です。ドメインユーザには、次の最小権限が必要です。

- Add-MailboxDatabaseCopy を追加します
- dismount - データベース
- Get-AdServerSettings
- Get-DatabaseAvailabilityGroup」を参照してください
- Get-ExchangeServer
- MailboxDatabase を取得します
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistics を実行します
- Get-PublicFolderDatabase を参照してください
- MOVE - ActiveMailboxDatabase
- move-DatabasePath-ConfigurationOnly:\$true

- mount - データベース
- New-MailboxDatabase
- 新規 - PublicFolderDatabase
- MailboxDatabase を削除します
- MailboxDatabaseCopy を削除します
- -PublicFolderDatabase を削除します
- 履歴書 -MailboxDatabaseCopy
- 「設定」 - 「サーバ設定
- MailboxDatabase-allowfilerestore を \$true に設定します
- MailboxDatabaseCopy を設定します
- 「 - PublicFolderDatabase 」を設定します
- Suspend-MailboxDatabaseCopy を実行します
- Update-MailboxDatabaseCopy

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 <div style="display: flex; align-items: center;">  <p>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。</p> </div>

項目	要件
必要なソフトウェアパッケージ	<ul style="list-style-type: none"> • Microsoft .NET Framework 4.7.2以降 • Windows Management Framework (WMF) 4.0 以降 • PowerShell 4.0 以降 <p>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"。</p>

SnapCenter Plug-in 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。プラグインパッケージをインストールするためのクレデンシャル、およびデータベース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。

- このタスクについて *

Windows ホストにプラグインをインストールするためのクレデンシャルを設定する必要があります。ホストを導入してプラグインをインストールしたあとに Windows のクレデンシャルを作成することもできますが、SVM を追加したあとで、ホストを導入してプラグインをインストールする前にクレデンシャルを作成することを推奨します。

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します。

個々のリソースグループのクレデンシャルを設定していて、ユーザ名にフル管理者権限がない場合は、少なくともリソースグループとバックアップ権限をユーザ名に割り当てる必要があります。

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

[資格情報] ウィンドウが表示されます。

4. [クレデンシャル] ページで、次の操作を実行します。

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	<p>認証に使用するユーザ名を入力します。</p> <ul style="list-style-type: none"> 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 <p>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。</p> <ul style="list-style-type: none"> ◦ NetBIOS\UserName ◦ Domain FQDN\UserName <ul style="list-style-type: none"> ローカル管理者（ワークグループのみ） <p>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せん。Username フィールドの有効な形式は次のとおりです。UserName</p>
パスワード	<p>認証に使用するパスワードを入力します。</p>
認証	<p>認証モードとして Windows を選択します。</p>

5. [OK] 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 -Effectivelmmedient
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。

ホストを追加し、 **Plug-in for Exchange** をインストールします

SnapCenter のホストの追加ページを使用して、Windows ホストを追加できます。指定したホストに Plug-in for Exchange が自動的にインストールされます。これはプラグインのインストールに推奨される方法です。ホストを追加してプラグインをインストールするには、個々のホストまたはクラスタを使用します。

- 必要なもの *
- SnapCenter Admin 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。
- メッセージキューサービスが実行されている必要があります。
- 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。詳細については、[を参照してください "Microsoft Exchange Server 2012 以降で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。
- Exchange ノードが DAG の一部である場合、SnapCenter サーバに追加できるノードは 1 つだけです。
- クラスタ (Exchange DAG) にプラグインをインストールする場合は、ネットアップ LUN 上にデータベースがないノードがある場合でも、クラスタのすべてのノードにインストールされます。

SnapCenter 4.6 以降では、SCE はマルチテナンシーをサポートしており、次の方法を使用してホストを追加できます。

ホスト追加処理	4.5以前	4.6以降
IP なしの DAG をクロスドメインまたは別のドメインに追加	サポート対象外	サポートされます
同じドメインまたはクロスドメインにそれぞれ固有の名前を持つ複数の IP DAG を追加します	サポートされます	サポートされます

ホスト追加処理	4.5以前	4.6以降
クロスドメインに、ホスト名と DB 名が同じ IP DAG または IP レス DAG を複数追加する	サポート対象外	サポートされます
同じ名前でクロスドメインに属する IP/IP を行わない DAG を複数追加します	サポート対象外	サポートされます
同じ名前とクロスドメインを持つ複数のスタンドアロンホストを追加します	サポート対象外	サポートされます

Plug-in for Exchange は Windows 用 SnapCenter プラグインパッケージによって異なり、バージョンも同じである必要があります。Plug-in for Exchange のインストール時に、デフォルトで SnapCenter Plug-ins Package for Windows が選択され、VSS Hardware Provider とともにインストールされます。

SnapManager for Microsoft Exchange Server と SnapDrive for Windows がすでにインストールされている場合は、同じ Exchange サーバに Plug-in for Exchange をインストールする場合は、Plug-in for Exchange および SnapCenter Plug-ins Package for Windows と互換性がないため、SnapDrive for Windows で使用する VSS ハードウェアプロバイダの登録を解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 "[Data ONTAP VSS ハードウェアプロバイダを手動で登録する方法](#)"。

• 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] 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	<p>ホストタイプとして * windows * を選択します。</p> <p>SnapCenter サーバによってホストが追加され、Plug-in for Windows と Plug-in for Exchange がまだインストールされていない場合はホストにインストールされます。</p> <p>Plug-in for Windows および Plug-in for Exchange のバージョンが同じである必要があります。以前に別のバージョンの Plug-in for Windows がインストールされていた場合、SnapCenter のインストール時にこのバージョンが更新されます。</p>

フィールド	手順
ホスト名	<p>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。</p> <p>SnapCenter は、DNS の適切な設定によって異なります。そのため、ベストプラクティスは Fully Qualified Domain Name（FQDN；完全修飾ドメイン名）を入力することです。</p> <p>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。</p> <p>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。</p> <p>次のいずれかの IP アドレスまたは FQDN を入力できます。</p> <ul style="list-style-type: none"> • スタンドアロンホスト • Exchange DAG <p>Exchange DAG の場合、次の操作を実行できます。</p> <ul style="list-style-type: none"> ◦ DAG 名、DAG の IP アドレス、ノード名、またはノードの IP アドレスを指定して DAG を追加します。 ◦ DAG クラスタのいずれかのノードの IP アドレスまたは FQDN を指定して、IP なしの DAG クラスタを追加します。 ◦ 同じドメインまたは別のドメインに属する IP なしの DAG を追加します。同じ名前前でドメインが異なる複数の IP/IP が少ない DAG を追加することもできます。 <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> スタンドアロンホストまたは Exchange DAG（クロスドメインまたは同じドメイン）の場合は、ホストまたは DAG の FQDN または IP アドレスを指定することを推奨します。</p> </div>

フィールド	手順
クレデンシャル	<p>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。</p> <p>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。</p> <p>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。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  資格情報認証モードは、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。 </div>

5. インストールするプラグインの選択セクションで、インストールするプラグインを選択します。

Plug-in for Exchange を選択すると、SnapCenter Plug-in for Microsoft SQL Server の選択が自動的に解除されます。Microsoft では、Exchange で必要とされるメモリの使用量やその他のリソースの使用量が原因で、SQL Server と Exchange サーバを同じシステムにインストールしないことを推奨しています。

6. (オプション) * 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	<p>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。</p> <p>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。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  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。 </div>
インストールパス	<p>デフォルトパスは <code>C:\Program Files\NetApp\SnapCenter</code> です。</p> <p>必要に応じて、パスをカスタマイズできます。</p>
DAG 内のすべてのホストを追加します	<p>DAG を追加する場合は、このチェックボックスを選択します。</p>

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	<p>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。</p> <p>gMSA 名を <code>domainName\accountName\$</code> の形式で指定します。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>gMSA は、SnapCenter Plug-in for Windows サービスのログオンサービスアカウントとしてのみ使用されます。</p> </div>

7. [Submit (送信)] をクリックします。

Skip ケーブルの事前確認チェックボックスを選択しなかった場合は、プラグインのインストール要件を満たすかどうかをホストが検証されます。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、にあるweb.configファイルを更新できます C:\Program Files\NetApp\SnapCenter Webappを使用して、デフォルト値を変更します。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。

PowerShell コマンドレットを使用して、SnapCenter サーバホストから Plug-in for Exchange をインストールします

Plug-in for Exchange は SnapCenter の GUI からインストールする必要があります。GUI を使用しない場合は、SnapCenter サーバホストまたはリモートホストで PowerShell コマンドレットを使用できます。

- 必要なもの *
- SnapCenter サーバがインストールおよび設定されている必要があります。
- ホストのローカル管理者または管理者権限を持つユーザである必要があります。
- SnapCenter Admin など、プラグイン、インストール、および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

- Plug-in for Exchange をインストールする前に、サポートされている構成のインストール要件と種類を確認しておく必要があります。
- Plug-in for Exchange をインストールするホストには Windows ホストを使用する必要があります。
- 手順 *

 1. SnapCenter サーバホストで、 `_Open-SmConnection_cmdlet` 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。
 2. Plug-in for Exchange をインストールするホストを追加するには、 `_Add-SmHost_cmdlet` と必要なパラメータを使用します。

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](#)"。

ホストは、スタンドアロンホストでも DAG ホストでもかまいません。DAG を指定する場合は、 `-IsDAG_parameter` が必要です。

1. 必要なパラメータを指定して、 `_Install-SmHostPackage_cmdlet` を使用し、 Plug-in for Exchange をインストールします。

このコマンドは、指定したホストに Plug-in for Exchange をインストールし、 SnapCenter にプラグインを登録します。

コマンドラインから SnapCenter Plug-in for Exchange をサイレントにインストールします

Plug-in for Exchange は、 SnapCenter ユーザー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 Exchange 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 *
- Microsoft Exchange Server リソースをバックアップしておく必要があります。
- SnapCenter プラグインパッケージをインストールしておく必要があります。
- をインストールする前に、以前のリリースの 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. プラグインホストに `_C : \temp_folder` が存在し、ログインしているユーザにフルアクセス権があるかどうかを確認します。
 2. `C : \ProgramData\NetApp\SnapCenter \Package_Repository` から SnapCenter Plug-in for Microsoft Windows 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. 次のコマンドを入力して、プラグインをインストールします。

```
_snapcenter_windows_host_plugin.exe "/silent/debuglog "<Debug_Log_Path>" /log" <Log_Path>"  
b_SNAPCENTER_port=<Num>Suite_INSTALLDIR="<Install_Directory_Path>"  
BV_ServiceAccount=<domain\administrator> BV_SERVICEPCPWD = <SCW> インストール、 ISW>
```

例：

```
C : \ProgramData\NetApp\SnapCenter \Package Repository_snapcenter_windows_host_plugin.exe  
"/silent/debuglog" C : \HPPW_SCSQL_Install.log "/log" C : \temp\temp\b_SNAPCENTER_PORT =  
8145 Suite_INSTALLDIR=" C : \Program Files\NetApp\SnapManager SnapCenter \BIT_VISPRI 管理  
者パスワードです
```



Plug-in for Exchange 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。

変数には次の値を入力します。

変数 (Variable)	価値
	インストーラのログファイルの名前と場所を次のように指定します。 <i>Setup.exe /debuglog "C:\PathToLog\setupexe.log</i>
BI _SNAPCENTER_PORT	SnapCenter が SMCORE と通信するポートを指定します。
SUITE_INSTALLDIR	ホストのプラグインパッケージのインストールディレクトリを指定します。
BY_ServiceAccount の場合	SnapCenter Plug-in for Microsoft Windows の Web サービスアカウントを指定します。
BI_SERVVICEPWD	SnapCenter Plug-in for Microsoft Windows の Web サービスアカウントのパスワードを指定します。
ISFeatureInstall	SnapCenter によってリモートホストに導入される解決策を指定します。

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*、およびその他のインストールファイルを *C:\Temp* で監視します。
2. *%temp%* ディレクトリを監視して、*_msiexe.exe_installers* がエラーなしでソフトウェアをインスト

ールしているかどうかを確認します。



Plug-in for Exchange をインストールすると、SnapCenter サーバ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。

SnapCenter プラグインパッケージのインストールステータスを監視する

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 : \ocalmachine\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。

Exchange と SnapCenter が共存するように SnapManager 7.x を設定します

SnapCenter Plug-in for Microsoft Exchange Server を SnapManager for Microsoft Exchange Server と共存できるようにするには、SnapManager for Microsoft Exchange Server がインストールされている Exchange Server と同じ Exchange Server に SnapCenter Plug-in for Microsoft Exchange Server をインストールし、SnapManager for Exchange のスケジュールを無効にする必要があります。および SnapCenter Plug-in for Microsoft Exchange Server を使用して新しいスケジュールとバックアップを設定します。

- 必要なもの *
- SnapManager for Microsoft Exchange Server と SnapDrive for Windows がすでにインストールされており、システムおよび SnapInfo ディレクトリに SnapManager for Microsoft Exchange Server のバックアップが存在します。
- SnapManager for Microsoft Exchange Server で作成された不要なバックアップを削除または再利用しておく必要があります。
- SnapManager for Microsoft Exchange Server で作成されたすべてのスケジュールを、Windows スケジューラから一時停止または削除しておく必要があります。
- SnapManager Plug-in for Microsoft Exchange Server と SnapCenter for Microsoft Exchange Server は同じ Exchange サーバ上に共存できますが、既存の SnapManager for Microsoft Exchange Server を SnapCenter にアップグレードすることはできません。

SnapCenter には、アップグレードのオプションはありません。

- SnapCenter では、SnapManager for Microsoft Exchange Server バックアップからの Exchange データベースのリストアはサポートされていません。

SnapCenter Plug-in for Microsoft Exchange Server のインストール後に SnapManager for Microsoft Exchange Server をアンインストールしないで、SnapManager for Microsoft Exchange Server のバックアップをリストアする場合は、追加の手順を実行する必要があります。

- 手順 *

1. すべての DAG ノードで PowerShell を使用して、SnapDrive for Windows VSS ハードウェアプロバイ

ダが登録されているかどうかを確認します。 *vssadmin list providers*

```
C:\Program Files\NetApp\SnapDrive>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
Provider type: Hardware
Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
Version: 7. 1. 4. 6845
```

2. SnapDrive ディレクトリから、SnapDrive for Windows から VSS ハードウェアプロバイダの登録を解除します。 *navssprv.exe -r service -u*
3. VSS ハードウェアプロバイダが削除されたことを確認します。 *vssadmin list providers*
4. SnapCenter に Exchange ホストを追加し、SnapCenter Plug-in for Microsoft Windows および SnapCenter Plug-in for Microsoft Exchange Server をインストールします。
5. すべての DAG ノードの SnapCenter Plug-in for Microsoft Windows ディレクトリで、VSS ハードウェアプロバイダが登録されていることを確認します： *vssadmin list providers*

```
[PS] C:\Windows\system32>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
Provider type: Hardware
Provider Id: {31fca584-72be-45b6-9419-53a3277301d1}
Version: 7. 0. 0. 5561
```

6. SnapManager for Microsoft Exchange Server のバックアップスケジュールを停止します。
7. SnapCenter GUI を使用して、オンデマンドバックアップの作成、スケジュールされたバックアップの設定、保持の設定を行います。
8. SnapManager for Microsoft Exchange Server をアンインストールします。

SnapManager for Microsoft Exchange Server を今すぐアンインストールしないで、SnapManager for Microsoft Exchange Server のバックアップをリストアする場合は、次の手順を実行します。

- a. すべての DAG ノードから SnapCenter Plug-in for Microsoft Exchange Server の登録を解除します。 *_navssprv.exe -r service -u _*

```
C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for
Microsoft Windows>navssprv.exe -r service -u
```

- b. C : \Program Files\NetApp\SnapManager \SnapDrive_directory から、すべての DAG ノードに SnapDrive for Windows を登録します。 `_navssprv.exe -r service -c hostname \username -p password_`

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。