



はじめに

SnapCenter Plug-in for VMware vSphere 5.0

NetApp
July 18, 2024

目次

はじめに.....	1
導入の概要.....	1
既存ユーザ向けの導入ワークフロー.....	1
SCVの導入要件.....	2
Open Virtual Appliance（OVA；オープン仮想アプライアンス）のダウンロード.....	9
SnapCenter Plug-in for VMware vSphereの導入.....	10
導入後に必要な処理と問題.....	14
SnapCenter VMware vSphere Clientにログインします。.....	16

はじめに

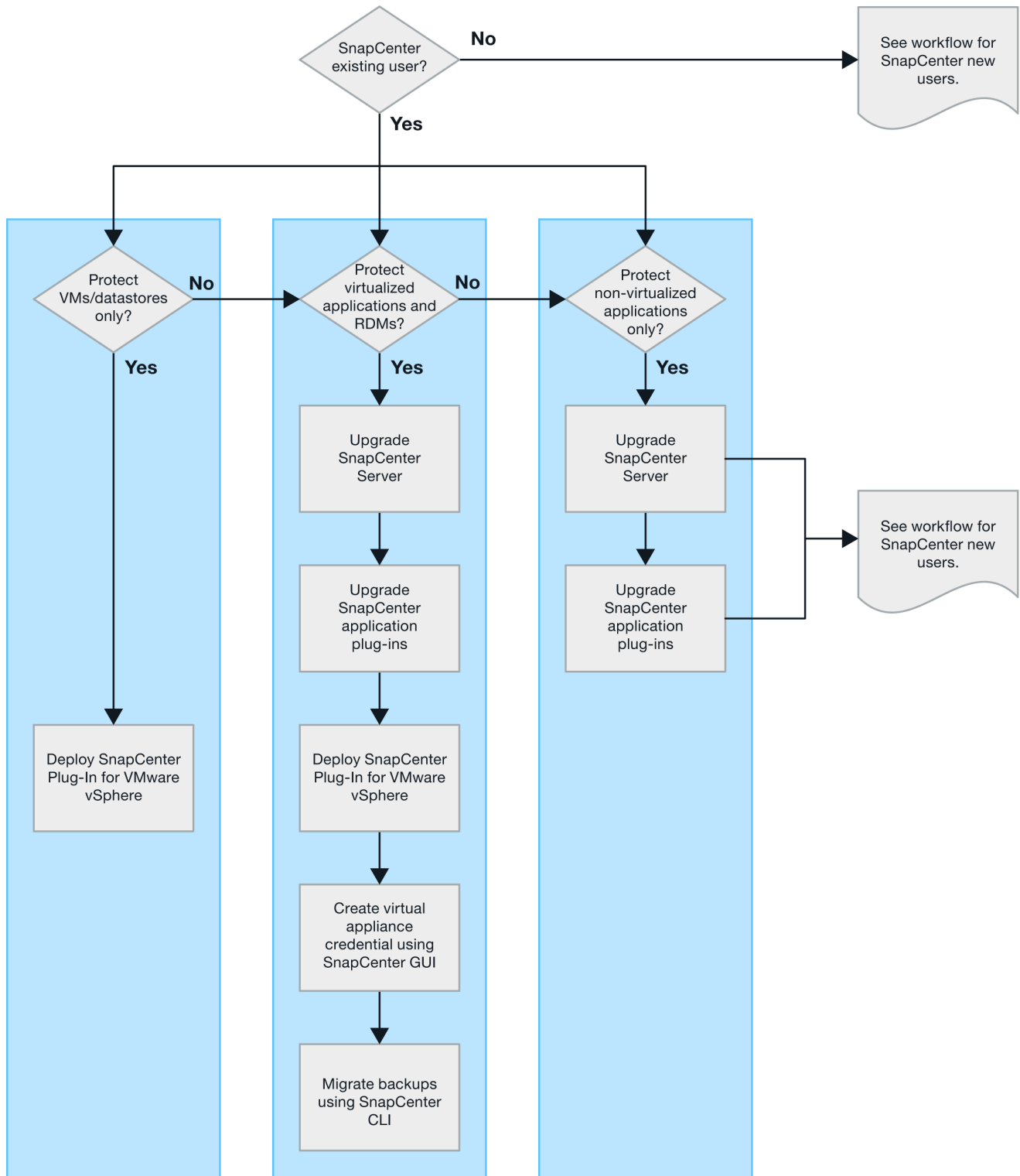
導入の概要

SnapCenterの機能を使用して仮想マシン上のVM、データストア、アプリケーションと整合性のあるデータベースを保護するには、SnapCenter Plug-in for VMware vSphereを導入する必要があります。

既存のSnapCenterユーザは、新しいSnapCenterユーザとは別の導入ワークフローを使用する必要があります。

既存ユーザ向けの導入ワークフロー

SnapCenterユーザでSnapCenterバックアップを作成している場合は、次のワークフローを使用して作業を開始してください。



SCVの導入要件

導入の計画と要件

仮想アプライアンスを導入する前に、導入要件を確認しておく必要があります。導入要

件を次の表に示します。

ホストの要件

SnapCenter Plug-in for VMware vSphere (SCV) の導入を開始する前に、ホストの要件を確認しておく必要があります。

- SnapCenter VMwareプラグインは、プラグインを使用してWindowsシステムとLinuxシステムのどちらのデータを保護するかに関係なく、Linux VMとして導入されます。
- vCenter ServerにSnapCenter VMwareプラグインを導入する必要があります。

バックアップ スケジュールは、SnapCenter VMwareプラグインが導入されているタイムゾーンで実行されます。vCenterは、vCenterが配置されているタイムゾーンでデータをレポートします。そのため、SnapCenter VMwareプラグインとvCenterが異なるタイムゾーンにある場合は、SnapCenter VMwareプラグインのダッシュボードのデータがレポートのデータと異なることがあります。

- 名前と特殊文字が含まれるフォルダにはSnapCenter VMwareプラグインを導入しないでください。

フォルダ名には、\$! @ # % ^ & () _ + { } ' ; , * ? " < > | という特殊文字は使用できません

- vCenter Serverごとに、固有のSnapCenter VMwareプラグインインスタンスを個別に導入して登録する必要があります。
 - 各vCenter Serverは、リンクモードかどうかに関係なく、SnapCenter VMwareプラグインの個別のインスタンスとペアリングする必要があります。
 - SnapCenter VMwareプラグインの各インスタンスを個別のLinux VMとして導入する必要があります。

たとえば、6つの異なるvCenter Serverインスタンスからバックアップを実行する場合は、6つのホストにSnapCenter VMwareプラグインを導入し、各vCenter ServerをSnapCenter VMwareプラグインの固有のインスタンスとペアリングする必要があります。

- VVOL VM (VMware VVOLデータストア上のVM) を保護するには、最初にONTAP tools for VMware vSphereを導入する必要があります。ONTAP toolsは、ONTAPおよびVMware WebクライアントでVVOL用のストレージをプロビジョニングおよび設定します。

詳細については、を参照してください。 ["VMware vSphere向けONTAPツール"](#)

サポートされているONTAP toolsの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。

- SnapCenter VMwareプラグインでは、Storage vMotionをサポートする仮想マシンの制限により、共有PCIデバイスまたはPCIeデバイス (NVIDIA Grid GPUなど) のサポートが制限されます。詳細については、ベンダーのドキュメント『VMware導入ガイド』を参照してください。

- サポート内容：

リソースグループの作成

VMの整合性を伴わないバックアップの作成

すべてのVMDKがNFSデータストアにあり、プラグインでStorage vMotionを使用する必要がない場合の、VM全体のリストア

VMDKの接続と接続解除

データストアのマウントとアンマウント

ゲストファイルのリストア

◦ サポートされていないもの：

VM整合性を維持したバックアップの作成

VMFSデータストア上に1つ以上のVMDKがある場合のVM全体のリストア

- SnapCenter VMware プラグインの制限事項の詳細については、を参照してください "[SnapCenter Plug-in for VMware vSphere リリースノート](#)".

ライセンス要件

次のライセンスを提供する必要があります。	ライセンス要件
ONTAP	いずれか：SnapMirrorまたはSnapVault（関係のタイプに関係なくセカンダリデータ保護用）
その他の製品	vSphere Standard、Enterprise、またはEnterprise Plus リストア処理（Storage vMotionを使用）を実行するには、vSphere ライセンスが必要です。vSphere Essentials または Essentials Plus ライセンスには、Storage vMotion は含まれていません。
プライマリデスティネーション	SnapCenter Standard：VMware SnapRestore を介したアプリケーションベースの保護を実行する場合に必要：VMware の VM およびデータストアのみ FlexClone のリストア処理を実行する場合に必要：VMware の VM およびデータストアのみのマウント処理と接続処理に使用
セカンダリデスティネーション	SnapCenter Standard：VMware FlexClone を介したアプリケーションベースの保護のフェイルオーバー処理に使用：VMware の VM およびデータストアのみのマウント処理と接続処理に使用されます

ソフトウェアのサポート

項目	サポートされるバージョン
vCenter vSphere	7.0U1以上
ESXi	7.0U1以上
IPアドレス	IPv4、IPv6
VMware TLS	1.2、1.3
SnapCenterサーバ上のTLS	1.2、1.3 SnapCenter サーバでは、VMDKを介したアプリケーションのデータ保護処理のために、これを使用してSnapCenter VMwareプラグインと通信しません。

項目	サポートされるバージョン
VMwareアプリケーションvStorage API for Array Integration (VAAI)	SnapCenter Plug-in for VMware vSphereは、この設定を使用してリストア処理のパフォーマンスを向上させます。また、NFS環境でのパフォーマンスも向上します。
VMware向けONTAPツール	SnapCenter Plug-in for VMware vSphereは、このを使用してVVolデータストア（VMwareの仮想ボリューム）を管理します。サポートされているバージョンについては、を参照してください " NetApp Interoperability Matrix Tool "。

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。

スペースとサイジングの要件

項目	要件
オペレーティングシステム	Linux
最小CPU数	4コア
最小RAM	最小構成：12 GB推奨：16 GB
SnapCenter Plug-in for VMware vSphere、□ グ、MySQLデータベース用の最小ハードドライブスペース	100 GB

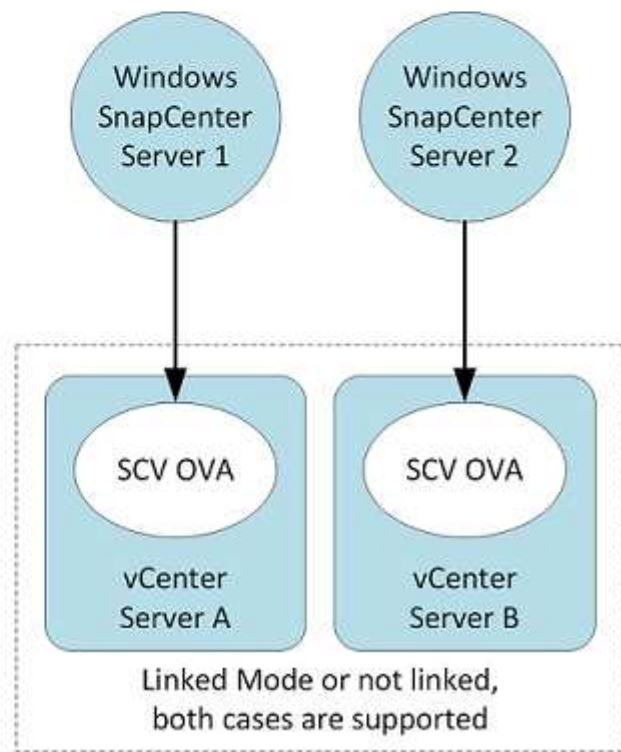
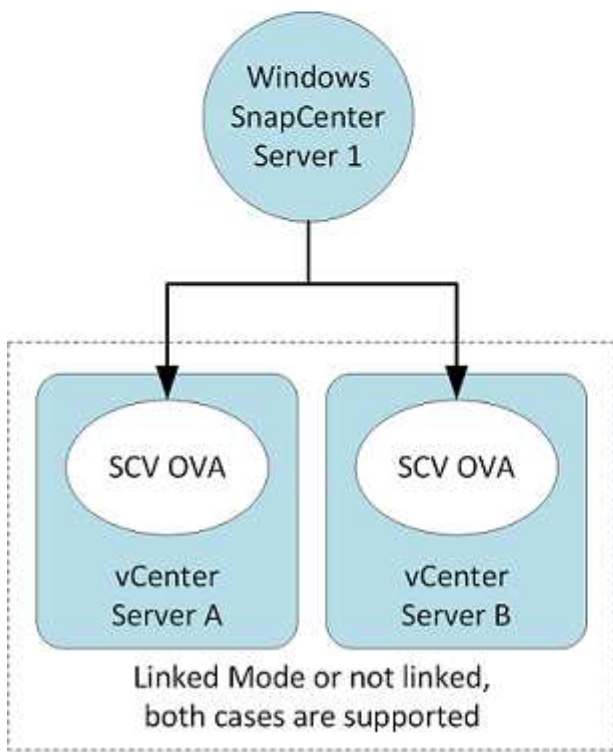
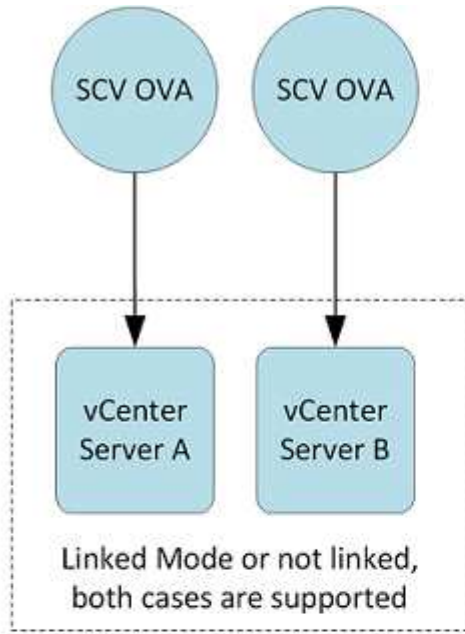
接続とポートの要件

ポートのタイプ	事前設定されたポート
VMware ESXi Serverのポート	443 (HTTPS)、双方向のゲストファイルリストア機能では、このポートが使用されます。
SnapCenter Plug-in for VMware vSphereのポート	8144 (HTTPS)。双方向のポートは、VMware vSphereクライアントとSnapCenter サーバからの通信に使用されます。8080 Bidirectional このポートは仮想アプライアンスの管理に使用されます。 注：SnapCenterにSCVホストを追加するためのカスタムポートがサポートされています。
VMware vSphere vCenter Serverのポート	VVol VMを保護する場合は、ポート443を使用する必要があります。
ストレージクラスタまたはStorage VMポート	443 (HTTPS)、双方向 80 (HTTP)、仮想アプライアンスと Storage VM または Storage VM を含むクラスタ間の通信に使用されるポート。

サポートされる構成

各プラグイン インスタンスでサポートされるvCenter Serverは1つだけです。リンク モードのvCenterがサポ

ートされます。次の図に示すように、複数のプラグインインスタンスで同じSnapCenterサーバをサポートできます。



RBACケンケンノヒツヨウ

vCenter管理者アカウントには、次の表に示す必要なvCenter権限が必要です。

この操作を実行するには ...	次の vCenter 権限が必要です ...
vCenterでSnapCenter Plug-in for VMware vSphereを導入して登録する	拡張子：拡張子を登録します

この操作を実行するには ...	次の vCenter 権限が必要です ...
SnapCenter Plug-in for VMware vSphereをアップグレードまたは削除する	エクステンション <ul style="list-style-type: none"> • 拡張機能の更新 • 拡張機能の登録解除
SnapCenterに登録されたvCenterクレデンシャルユーザアカウントに、SnapCenter Plug-in for VMware vSphereへのユーザアクセスの検証を許可する	sessions.validate.session
ユーザにSnapCenter Plug-in for VMware vSphereへのアクセスを許可する	SCV Administrator Backup SCV Guest File Restore SCV Restore SCV View 権限が vCenter ルートで割り当てられている必要があります。

AutoSupport

SnapCenter Plug-in for VMware vSphereは、プラグインのURLなど、使用状況を追跡するための最小限の情報を提供します。AutoSupportには、AutoSupportビューアに表示されるインストール済みプラグインの表が含まれています。

必要なONTAP権限

必要な最小 ONTAP 権限は、データ保護に使用する SnapCenter プラグインによって異なります。



SnapCenter Plug-in for VMware (SCV) 5.0以降では、SCVへのカスタマイズされたロールベースアクセスを持つすべてのONTAPユーザに対して、HTTPおよびONTAPIタイプのアプリケーションをユーザのログイン方法として追加する必要があります。これらのアプリケーションにアクセスできないと、バックアップは失敗します。ONTAPユーザのログイン方法の変更を認識するには、SCVサービスを再起動する必要があります。

必要な最小ONTAP権限

すべてのSnapCenterプラグインに必要な最小権限は次のとおりです。

フルアクセスコマンド： ONTAP 8.3 以降に必要な最小権限
cluster identity show の実行
event generate-autosupport-log
job history show job show job stop
lun lun create lun delete lun igroup add lun igroup create lun igroup delete lun igroup rename lun igroup rename lun igroup show lun mapping add-reporting-nodes lun mapping create lun mapping remove-reporting-nodes lun mapping show lun modify lun move-in-volume LUN offline LUN online lun persistent-reservation clear lun resize lun serial lun show をクリックします
snapmirror list-destinations snapmirror policy add-rule snapmirror policy modify -rule snapmirror policy show snapmirror restore snapmirror show -history snapmirror update snapmirror update-ls-set
バージョン

volume clone create volume clone show volume clone split start volume clone split stop volume create volume delete volume destroy volume file clone create volume file show -disk-usage volume offline volume online volume modify volume qtree create volume qtree delete volume qtree modify volume qtree show volume restrict volume show volume snapshot create volume snapshot delete volume snapshot modify volume snapshot rename volume snapshot restore volume snapshot restore -file volume snapshot show volume unmount

vserver cifs share create vserver cifs share create vserver cifs share delete vserver cifs shadowcopy show vserver cifs share show vserver cifs share show vserver cifs show vserver export-policy vserver export-policy vserver export-policy vserver export-policy create vserver export-policy rule create vserver export-policy rule create vserver export-policy rule show vserver export-policy rule show vserver iscsi vserver iscsi vserver iscsi connection show vserver show network interface network interface failover-groups network interface show を実行します

読み取り専用コマンド： **ONTAP 8.3** 以降に必要な最小権限

SVM SVMピア



サポートされていないvServerコマンドに関する警告メッセージは無視してかまいません。

ONTAPに関するその他の情報

- ONTAP 8.2.xを実行している場合：

SnapCenter Plug-in for VMware vSphereの処理を実行するための適切な権限を割り当てるには、Storage VMとしてログインする必要があります vsadmin。

- ONTAP 8.3以降を実行している場合：

またはとして、上記の表に記載されている最小限の権限を持つロールでログインする必要があります vsadmin。

- ユーザロールを作成および管理するには、クラスタ管理者である必要があります。ユーザをクラスタStorage VMまたはStorage VMに関連付けることができます。
- SnapMirrorビジネス継続性（SM-BC）機能を使用するには、ONTAP 9.12.1以降のバージョンが必要です。
- 改ざん防止スナップショット（TPS）機能を使用するには、次の手順を実行します。
 - SANにはONTAP 9.13.1以降のバージョンが必要です。
 - NFSにはONTAP 9.12.1以降のバージョンが必要です。



ONTAPバージョン9.11.1以降の場合、ONTAPクラスタとの通信にはREST APIを使用します。ONTAPユーザは、httpアプリケーションを有効にしておく必要があります。ただし、ONTAP REST APIで問題が見つかった場合は、設定キー「force_zapi」を使用して従来のZAPIワークフローに切り替えることができます。設定APIを使用してこのキーを追加または更新し、trueに設定する必要がある場合があります。技術情報の記事、を参照してください ["RestAPIを使用してSCVの設定パラメータを編集する方法"](#)。

VMware vCenter 7.0.3以降のバージョンでは、Entrust証明書によって署名されたOVAは信頼されなくなりました。この問題を解決するには、次の手順を実行する必要があります。

手順

1. SnapCenter Plug-in for VMwareをダウンロードするには、次の手順を実行します。
 - NetAppサポートサイトにログインします（"<https://mysupport.netapp.com/products/index.html>"）。
 - 製品のリストから、「SnapCenter Plug-in for VMware vSphere *」を選択し、「最新リリースをダウンロード」ボタンをクリックします。
 - SnapCenter Plug-in for VMware vSphereのファイルを任意の場所にダウンロードし .tar ます。
2. tarファイルの内容を展開します。tarファイルには、ovaフォルダとcertsフォルダが含まれています。certsフォルダには、Entrustルート証明書と中間証明書が含まれています。
3. vSphere ClientでvCenter Serverにログインします。
4. [管理]>[証明書]>[証明書の管理]に移動します。
5. の横にある[追加]*をクリックします
 - _certs_folderに移動します。
 - Entrustルート証明書と中間証明書を選択します。
 - 各証明書を一度に1つずつインストールします。
6. 証明書は*信頼されたルート証明書*の下のパネルに追加されます。証明書をインストールしたら、OVAを検証して導入できます。



ダウンロードしたOVAが改ざんされていない場合は、「* Publisher」列に「Trusted certificate *」と表示されます。

SnapCenter Plug-in for VMware vSphereの導入

SnapCenterの機能を使用して仮想マシン上のVM、データストア、アプリケーションと整合性のあるデータベースを保護するには、SnapCenter Plug-in for VMware vSphereを導入する必要があります。

開始する前に

このセクションでは、導入を開始する前に実行する必要があるすべてのアクションを示します。



OVA環境は、VMware vCenter 7u1以上でサポートされます。

- 導入要件を確認しておく必要があります。
- サポートされているバージョンのvCenter Serverが実行されている必要があります。
- vCenter Server環境の設定とセットアップが完了している必要があります。
- SnapCenter VMwareプラグインVM用のESXiホストのセットアップが完了している必要があります。
- SnapCenter Plug-in for VMware vsphere.tarファイルをダウンロードしておく必要があります。
- vCenter Serverインスタンスのログイン認証の詳細を確認しておく必要があります。

- 有効な公開鍵ファイルと秘密鍵ファイルを持つ証明書が必要です。詳細については、セクションの記事を参照してください "[ストレージ証明書の管理](#)"。
- vSphere Clientのすべてのブラウザセッションからログアウトして閉じておく必要があります。また、SnapCenter VMwareプラグインの導入時にブラウザキャッシュの問題が発生しないように、ブラウザキャッシュを削除しておく必要があります。
- vCenterでTransport Layer Security (TLS) を有効にしておく必要があります。VMwareのドキュメントを参照してください。
- SnapCenter VMwareプラグインが導入されているvCenter以外のvCenterでバックアップを実行する場合は、ESXiサーバ、SnapCenter VMwareプラグイン、および各vCenterを同時に同期する必要があります。
- VVOLデータストアのVMを保護するには、まずONTAP tools for VMware vSphereを導入する必要があります。ONTAP Tools for VMware vSphereバージョン9.10以降がサポートされます。ONTAP toolsは、ONTAPおよびVMware Web Client上でストレージをプロビジョニングおよび設定します。

vCenterと同じタイムゾーンでSnapCenter VMwareプラグインを導入します。バックアップスケジュールは、SnapCenter VMwareプラグインが導入されているタイムゾーンで実行されます。vCenterは、vCenterが配置されているタイムゾーンでデータをレポートします。そのため、SnapCenter VMwareプラグインとvCenterが異なるタイムゾーンにある場合は、SnapCenter VMwareプラグインのダッシュボードのデータがレポートのデータと異なることがあります。

手順

1. VMware vCenter 7.0.3以降のバージョンの場合は、の手順に従って、"[Open Virtual Appliance \(OVA ; オープン仮想アプライアンス\) のダウンロード](#)" 証明書をvCenterにインポートします。
2. ブラウザで、VMware vSphere vCenterに移動します。



IPv6 HTML Webクライアントの場合は、ChromeまたはFirefoxを使用する必要があります。

3. VMware vCenter Single Sign-On * ページにログインします。
4. Navigator ペインで、データセンター、クラスタ、ホストなどの仮想マシンの有効な親オブジェクトであるインベントリオブジェクトを右クリックし、* Deploy OVF Template * を選択して VMware Deploy ウィザードを起動します。
5. .ovaファイルを含む.tarファイルをローカルシステムに展開します。[Select an OVF template*]ページで、.tar抽出フォルダ内のファイルの場所を指定します .ova。
6. 「* 次へ *」をクリックします。
7. [名前とフォルダの選択 *] ページで、VM または vApp の一意の名前を入力し、導入場所を選択して、[次へ *] をクリックします。

この手順では、ファイルをvCenterにインポートする場所を指定し .tar ます。VMのデフォルト名は、選択したファイルの名前と同じ .ova です。デフォルトの名前を変更した場合は、各vCenter Server VMフォルダ内で一意の名前を選択します。

VMのデフォルトの導入場所は、ウィザードを開始したインベントリオブジェクトです。

8. [リソースの選択 *] ページで、導入した VM テンプレートを実行するリソースを選択し、[次へ *] をクリックします。
9. [詳細の確認] ページで、テンプレートの詳細を確認し .tar、*[次へ]* をクリックします。

10. [ライセンス契約 *] ページで、[すべてのライセンス契約に同意します]のチェックボックスをオンにします。 *
11. [*ストレージの選択 *] ページで、導入した OVF テンプレートのファイルの保存場所と保存方法を定義します。

- a. VMDKのディスクフォーマットを選択します。
- b. VMストレージポリシーを選択します。

このオプションは、デスティネーションリソースでストレージポリシーが有効になっている場合にのみ使用できます。

- c. 導入したOVAテンプレートを格納するデータストアを選択します。

構成ファイルと仮想ディスクファイルはデータストアに格納されます。

仮想マシンまたはvApp、および関連するすべての仮想ディスクファイルを格納できるサイズのデータストアを選択します。

12. [ネットワークの選択 *] ページで、次の操作を行います。

- a. 送信元ネットワークを選択し、宛先ネットワークにマッピングします。

[Source Network]列には、OVAテンプレートで定義されているすべてのネットワークが表示されます。

- b. [IP Allocation Settings] セクションで、必要な IP プロトコルを選択し、[*Next] をクリックします。

SnapCenter Plug-in for VMware vSphereは、1つのネットワークインターフェイスをサポートします。複数のネットワークアダプタが必要な場合は、手動で設定する必要があります。を参照してください"[技術情報アーティクル：「How to create additional network adapters」](#)。

13. [テンプレートのカスタマイズ] ページで、次の操作を行います。

- a. [* Register to Existing vCenter* (既存の vCenter に登録)] セクションで、仮想アプライアンスの vCenter 名と vCenter クレデンシャルを入力します。

[vCenter username (vCenterユーザー名)]フィールドに、の形式でユーザー名を入力し`domain\username` ます。

- b. Create SCV credentials * セクションにローカルクレデンシャルを入力します。

[Username] フィールドに、ローカルユーザ名を入力します。ドメインの詳細は入力しないでください。



指定したユーザ名とパスワードをメモしておきます。あとでSnapCenter VMwareプラグインの設定を変更する場合は、これらのクレデンシャルを使用する必要があります。

- c. maintユーザのクレデンシャルを入力します。

- d. [ネットワークプロパティの設定 *] に、ホスト名を入力します。

- i. [*IPv4 ネットワークプロパティの設定 *] セクションで、IPv4 アドレス、IPv4 ネットマスク、IPv4 ゲートウェイ、IPv4 プライマリ DNS、IPv4 セカンダリ DNS などのネットワーク情報を入

力します。 および IPv4 検索ドメインを使用できます。

- ii. [*IPv6 ネットワークプロパティの設定*] セクションで、IPv6 アドレス、IPv6 ネットマスク、IPv6 ゲートウェイ、IPv6 プライマリ DNS、IPv6 セカンダリ DNS などのネットワーク情報を入力します。 および IPv6 検索ドメインを使用できます。

必要に応じて、[IPv4]フィールド、[IPv6]フィールド、またはその両方を選択します。IPv4とIPv6の両方を使用している場合は、そのうちの1つにのみプライマリDNSを指定する必要があります。



ネットワーク設定として DHCP を使用する場合は、これらの手順を省略し、**[Setup Network Properties]** セクションのエントリを空白のままにしておくことができます。

- a. * Setup Date and Time * で、vCenter が配置されているタイムゾーンを選択します。

14. [完了準備完了] ページでページを確認し、[完了] をクリックします。

すべてのホストにIPアドレスを設定する必要があります (FQDNホスト名はサポートされません)。導入処理では、導入前に入力した内容は検証されません。

OVFのインポートタスクと導入タスクが完了するまでの間、[Recent Tasks]ウィンドウで導入の進捗状況を確認できます。

SnapCenter VMware プラグインの導入が完了すると、Linux VMとして導入されてvCenterに登録され、VMware vSphere Clientがインストールされます。

15. SnapCenter VMware プラグインが導入された VM に移動し、* 概要 * タブをクリックしてから * 電源オン * ボックスをクリックして仮想アプライアンスを起動します。
16. SnapCenter VMware プラグインの電源をオンにした状態で、展開された SnapCenter VMware プラグインを右クリックし、* ゲスト OS * を選択して、* VMware Tools のインストール * をクリックします。

VMware Toolsは、SnapCenter VMwareプラグインが導入されているVMにインストールされます。VMware Toolsのインストールの詳細については、VMwareのドキュメントを参照してください。

導入が完了するまでに数分かかることがあります。SnapCenter VMwareプラグインの電源がオンになると導入が成功したことが通知され、VMware toolsがインストールされ、SnapCenter VMwareプラグインへのログインを求める画面が表示されます。初回リブート時に、ネットワーク設定をDHCPから静的アドレスに切り替えることができます。ただし、スタティックからDHCPへの切り替えはサポートされていません。

SnapCenter VMwareプラグインが導入されているIPアドレスが画面に表示されます。IPアドレスをメモします。SnapCenter VMwareプラグインの設定を変更する場合は、SnapCenter VMwareプラグインの管理GUIにログインする必要があります。

17. 導入画面に表示されたIPアドレスと導入ウィザードで指定したクレデンシャルを使用してSnapCenter VMwareプラグインの管理GUIにログインし、SnapCenter VMwareプラグインがvCenterに接続されて有効になっていることをダッシュボードで確認します。

管理GUIにアクセスするには、の形式を使用し `https://<appliance-IP-address>:8080` ます。

導入時に設定したadminユーザ名とパスワード、およびメンテナンスコンソールを使用して生成されたMFAトークンを使用してログインします。

SnapCenter VMwareプラグインが有効になっていない場合は、を参照してください ["VMware vSphere](#)

Client Serviceを再起動します。"。

ホスト名が「UnifiedVSC/SCV」の場合は、アプライアンスを再起動します。アプライアンスを再起動してもホスト名が指定したホスト名に変更されない場合は、アプライアンスを再インストールする必要があります。

終了後

必要な完了する必要があります ["導入後の処理"](#)。

導入後に必要な処理と問題

SnapCenter Plug-in for VMware vSphereを導入したら、インストールを完了する必要があります。

導入後に必要な処理

SnapCenterを初めて使用する場合は、Storage VMをSnapCenterに追加してからデータ保護処理を実行する必要があります。Storage VMを追加するときは、管理LIFを指定してください。クラスタを追加してクラスタ管理LIFを指定することもできます。ストレージの追加の詳細については、[を参照してください "ストレージの追加"](#)。

トウニユウニカンスルモンタイ

- 仮想アプライアンスの導入後、ダッシュボードの * Backup Jobs * タブに次のような状況でロードされないことがあります。
 - IPv4を実行しており、SnapCenter VMware vSphereホストのIPアドレスが2つある。その結果、ジョブ要求はSnapCenterサーバで認識されないIPアドレスに送信されます。この問題を回避するには、使用するIPアドレスを次のように追加します。
 - i. SnapCenter VMwareプラグインが導入されている場所に移動します。
`/opt/netapp/scvservice/standalone_aegis/etc`
 - ii. ネットワーク- interface.propertiesファイルを開きます。
 - iii. ``network.interface=10.10.10.10`` フィールドに、使用するIPアドレスを追加します。
 - NICが2つあります。
- SnapCenter VMwareプラグインの導入後も、vCenter for SnapCenter Plug-in for VMware vSphereのMOBエントリに古いバージョン番号が表示されることがあります。これは、vCenterで他のジョブが実行されている場合に発生することがあります。時間の経過とともに、vCenterによってエントリが更新されません。

これらの問題のいずれかを修正するには、次の手順を実行します。

1. ブラウザキャッシュをクリアし、GUIが正常に動作しているかどうかを確認します。

問題が解決しない場合は、VMware vSphere Client Serviceを再起動します

2. vCenter にログインし、ツールバーの * メニュー * をクリックして、 * SnapCenter Plug-in for VMware vSphere * を選択します。

認証エラーを管理します。

Adminクレデンシャルを使用しないと、SnapCenter Plug-in for VMware vSphereの導入後または移行後に認証エラーが表示されることがあります。認証エラーが発生した場合は、サービスを再起動する必要があります。

手順

1. の形式を使用して、SnapCenter VMwareプラグインの管理GUIにログインし `https://<appliance-IP-address>:8080` ます。adminユーザ名、パスワード、およびMFAトークンの詳細を使用してログインします。MFAトークンはメンテナンスコンソールから生成できます。
2. サービスを再起動します。

SnapCenter Plug-in for VMware vSphereをSnapCenter Serverに登録

SnapCenter（仮想化されたデータベースとファイルシステムのアプリケーションベースの保護ワークフロー）でVMDKを介したアプリケーションワークフローを実行する場合は、SnapCenter Plug-in for VMware vSphereをSnapCenter Serverに登録する必要があります。

開始する前に

- SnapCenterサーバ4.2以降を実行している必要があります。
- SnapCenter Plug-in for VMware vSphereを導入して有効にしておく必要があります。

タスクの内容

- SnapCenter Plug-in for VMware vSphereをSnapCenter Serverに登録するには、SnapCenter GUIを使用して「vSphere」タイプのホストを追加します。

ポート8144は、SnapCenter VMwareプラグイン内の通信用に事前に定義されています。

SnapCenter Plug-in for VMware vSphereの複数のインスタンスを同じSnapCenter Serverに登録することで、VMでのアプリケーションベースのデータ保護処理をサポートできます。同じSnapCenter Plug-in for VMware vSphereを複数のSnapCenter Serverに登録することはできません。

- vCenterがリンクモードの場合は、vCenterごとにSnapCenter Plug-in for VMware vSphereに登録する必要があります。

手順

1. SnapCenter GUI の左ナビゲーションペインで、 **Hosts** 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、仮想アプライアンスのホスト名を見つけ、 SnapCenter サーバから解決されることを確認します。
3. 「* 追加」 をクリックしてウィザードを開始します。
4. [Add Hosts] ダイアログ・ボックスで ' 次の表に示すように SnapCenter サーバに追加するホストを指定します

このフィールドでは...	操作
ホストタイプ	ホストのタイプとして「* vsphere *」を選択します。
ホスト名	仮想アプライアンスのIPアドレスを確認します。

このフィールドでは...	操作
クレデンシャル	導入時に指定したSnapCenter VMwareプラグインのユーザ名とパスワードを入力します。

5. [Submit (送信)] をクリックします。

追加されたVMホストは、[Managed Hosts]タブに表示されます。

6. 左側のナビゲーションペインで、[設定]*をクリックし、[クレデンシャル]タブをクリックし、[追加]*を選択して仮想アプライアンスのクレデンシャルを追加します。

7. SnapCenter Plug-in for VMware vSphereの導入時に指定したクレデンシャル情報を入力します。



[Authentication]フィールドで[Linux]を選択する必要があります。

終了後

SnapCenter Plug-in for VMware vSphereのクレデンシャルが変更された場合は、SnapCenterの[Managed Hosts]ページを使用してSnapCenterサーバでの登録を更新する必要があります。

SnapCenter VMware vSphere Clientにログインします。

SnapCenter Plug-in for VMware vSphereを導入すると、vCenterにVMware vSphereクライアントがインストールされ、他のvSphereクライアントとともにvCenter画面に表示されます。

開始する前に

vCenterでTransport Layer Security (TLS) が有効になっている必要があります。VMwareのドキュメントを参照してください。

手順

1. ブラウザで、VMware vSphere vCenterに移動します。
2. VMware vCenter Single Sign-On * ページにログインします。



[* ログイン *] ボタンをクリックします。VMwareに既知の問題があるため、ログインする際はEnterキーを使用してしないでください。詳細については、ESXi Embedded Host Clientの問題に関するVMwareのドキュメントを参照してください。

3. VMware vSphereクライアント*ページで、ツールバーのメニューをクリックし、* SnapCenter Plug-in for VMware vSphere *を選択します。

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。