SnapCenter Plug-in for VMware vSphereのドキュメント

SnapCenter Plug-in for VMware vSphere

NetApp
September 29, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/sc-plugin-vmware-vsphere-61/index.html on September 29, 2025. Always check docs.netapp.com for the latest.

目次

SnapCenter Plug-in for VMware vSphereのドキュメント 1
リリース ノート 2
SnapCenter Plug-in for VMware vSphereのリリース ノート 2
SnapCenter Plug-in for VMware vSphereの新機能 2
アップグレード パス 2
概念 4
製品概要 4
各種SnapCenter GUIの概要 5
ライセンス 6
ロールベース アクセス制御（RBAC） 7
SnapCenter Plug-in for VMware vSphereユーザ用のRBACのタイプ 7
vCenter Server RBAC 7
ONTAP RBAC 8
RBAC権限の検証ワークフロー 8
SnapCenter Plug-in for VMware vSphereのONTAP RBAC機能 9
SnapCenter Plug-in for VMware vSphereに組み込みの事前定義のロール 10
SnapCenter Plug-in for VMware vSphere用にONTAP RBACを設定する方法 11
始めましょう 13
導入プロセスの概要 13
既存ユーザ向けの導入ワークフロー 13
SCVを導入するための要件 14
導入の計画と要件 14
必要なONTAP権限 19
必要な最小vCenter権限 21
オープン仮想アプライアンス（OVA）のダウンロード 22
SnapCenter Plug-in for VMware vSphereの導入 22
導入後の必要な処理と問題 26
導入後に必要な処理 26
導入で発生する可能性がある問題 26
認証エラーの管理 27
SnapCenter ServerへのSnapCenter Plug-in for VMware vSphereの登録 27
SnapCenter VMware vSphere Clientへのログイン 28
クイック スタート 29
概要 29
SnapCenter Plug-in for VMware vSphereの導入 29
ストレージの追加 31
バックアップ ポリシーの作成 31
リソース グループの作成 31
監視とレポート 32

ステータス情報の表示 32
ジョブの監視 33
ジョブ ログのダウンロード 34
レポートへのアクセス 35
VMware vSphere Clientからのレポートの種類 35
SnapCenter Plug-in for VMware vSphere GUIからのサポート バンドルの生成 37
メンテナンス コンソールからのサポート バンドルの生成 38
監査ログ 39
データ保護のイベント 40
メンテナンス コンソールのイベント 41
管理コンソールのイベント 41
syslogサーバの設定 42
監査ログ設定の変更 42
ストレージの管理 43
ストレージの追加 43
ストレージ システムの管理 45
Storage VMの変更 45
Storage VMの削除 46
設定されたストレージ タイムアウトの変更 46
データの保護 48
データ保護のワークフロー 48
VMとデータストアのバックアップの表示 49
VMとデータストアのバックアップ ポリシーの作成 50
リソース グループの作成 55
互換性チェックのエラーの管理 62
プリスクリプトとポストスクリプト 63
サポートされるスクリプト タイプ 63
スクリプト パスの場所 63
スクリプトを指定する場所 63
スクリプトが実行されるタイミング 63
スクリプトに渡される環境変数 64
スクリプトのタイムアウト 64
Perlスクリプトの例1 65
Perlスクリプトの例2 65
シェル スクリプトの例 65
リソース グループへの単一のVMまたはデータストアの追加 66
リソース グループへの複数のVMとデータストアの追加 66
名前が変更されたストレージのバックアップのリストア 67
オンデマンドでのリソース グループのバックアップ 68
SnapCenter Plug-in for VMware vSphereのMySQLデータベースのバックアップ 69
リソース グループの管理 70

リソース グループに対する処理の一時停止と再開 70
リソース グループの変更 70
リソース グループの削除 71
ポリシーの管理 71
ポリシーの適用解除 71
ポリシーの変更 72
ポリシーの削除 72
バックアップの管理 73
バックアップの名前の変更 73
バックアップの削除 73
データストアのマウントとアンマウント 75
バックアップのマウント 75
バックアップのアンマウント 76
バックアップのリストア 77
リストアの概要 77
リストア処理の実行方法 77
バックアップの検索 79
バックアップからのVMのリストア 80
削除されたVMのバックアップからのリストア 82
バックアップからのVMDKのリストア 84
MySQLデータベースの最新のバックアップのリストア 85
MySQLデータベースの特定のバックアップのリストア 86
VMDKの接続および接続解除 87
VMまたはvVol VMへのVMDKの接続 87
仮想ディスクの接続解除 89
ゲスト ファイルとフォルダの復元 91
ワークフロー、前提条件、制限事項 91
ゲスト リストアのワークフロー 91
ゲスト ファイルとフォルダをリストアするための前提条件 91
ゲスト ファイル リストアに関する制限事項 92
VMDKからのゲスト ファイルとフォルダのリストア 93
リストア処理用のプロキシVMのセットアップ 96
VMゲスト ファイルのリストア用のクレデンシャルの設定 97
ゲスト ファイル リストア セッションの時間の延長 98
実際に起こり得るゲスト ファイルのリストア シナリオ 99
ゲスト ファイル リストア セッションが空白 99
ゲスト ファイル リストアのディスク接続処理が失敗する 99
ゲストEメールにファイル名として「??????」が表示される 99
ゲスト ファイル リストア セッションを中断してもバックアップが切断されない 99
SnapCenter Plug-in for VMware vSphereアプライアンスの管理 101
VMware vSphere Clientサービスの再起動 101

Linux vCenterでVMware vSphere Client Serviceを再起動します。 101
メンテナンス コンソールへのアクセス 101
メンテナンス コンソールからのSnapCenter Plug-in for VMware vSphereのパスワードの変更 103
証明書の作成とインポート 104
vCenterからのSnapCenter Plug-in for VMware vSphereの登録解除 104
SnapCenter Plug-in for VMware vSphereの無効化および有効化 105
SnapCenter Plug-in for VMware vSphereの削除 106
構成の管理 107
バックアップのタイムゾーンの変更 107
ログオン クレデンシャルの変更 108
vCenterログオン クレデンシャルの変更 109
ネットワーク設定の変更 110
設定のデフォルト値の変更 111
scbr.override構成ファイルの作成 111
上書き可能なプロパティ 111
SnapCenter Plug-in for VMware vSphere用のSSHの有効化 116
REST API 118
概要 118
Swagger API Webページを使用したREST APIへのアクセス 119
Storage VMを追加および変更するためのREST APIのワークフロー 119
リソース グループを作成および変更するためのREST APIのワークフロー 120
オンデマンドでバックアップするためのREST APIのワークフロー 121
VMをリストアするためのREST APIのワークフロー 122
削除されたVMをリストアするためのREST APIのワークフロー 123
VMDKをリストアするためのREST APIのワークフロー 124
VMDKを接続および接続解除するためのREST APIのワークフロー 125
VMDKを接続するには、次のワークフローを実行します。 126
VMDKの接続を解除するには、次のワークフローを実行します。 126
データストアをマウントおよびアンマウントするためのREST APIのワークフロー 127
データストアをマウントするには、次のワークフローを実行します。 127
データストアをアンマウントするには、次のワークフローを実行します。 128
ジョブのダウンロードおよびレポートの生成を行うためのREST API 128
ジョブの詳細情報を取得するには、[Jobs]セクションの次のREST APIを使用します。 128
[Jobs]セクションの次のREST APIを使用して、ジョブのログをダウンロードします。 129
レポートを生成するには、[Reports]セクションの次のREST APIを使用します。 129
組み込みスケジュールを変更するREST APIワークフロー 129
スタック ジョブを失敗としてマークするためのREST API 130
監査ログを生成するためのREST API 130
Upgrade 132
以前のリリースのSnapCenter Plug-in for VMware vSphereからのアップグレード 132
アップグレード パス 132

同じリリースのSnapCenter Plug-in for VMware vSphereの新しいパッチへのアップグレード 134
キャッシュのクリア手順 134
同じリリースの新しいパッチにアップグレードすると表示されなくなる情報 134
キャッシュをクリアする前にアップグレードした場合の対処方法 135
法律上の表示 136
著作権 136
商標 136
特許 136
プライバシー ポリシー 136
オープンソース 136

SnapCenter Plug-in for VMware vSphereのドキュメント

リリース ノート

SnapCenter Plug-in for VMware vSphereのリリース ノート

SnapCenter Plug-in for VMware vSphereで利用できる新機能と拡張機能について説明します。

既知の問題、制限事項、修正された問題の詳細については、以下を参照してください。 "SnapCenter Plug-in for VMware vSphereリリース ノート" 。リリース ノートにアクセスするには、NetAppアカウントでサインインするか、アカウントを作成する必要があります。

> サポートされているバージョンの最新情報については、 NetApp相互運用性マトリックスツールを参照してください。("IMT にログインします。" ）。

SnapCenter Plug-in for VMware vSphereの新機能

- ASA r2 システム上の VM および VMFS データストアのサポート*

VMware vSphere 6.1 リリース用のSnapCenterプラグインは、 ASA r2 システム上の仮想マシン (VM) および VMFS データストアのプロビジョニングをサポートします。 ASA r2 システムは、SAN のみを利用するお客様のニーズに合わせた簡素化されたエクスペリエンスを実現する、統合されたハードウェアおよびソフトウェア ソリューションを提供します。 SnapCenter Plug-in for VMware vSphereでASA r2 システム上の VM、データストア、および仮想マシン ディスク フォーマット (VMDK) に対してサポートされている機能は次のとおりです。

- プライマリ保護のための整合性グループのプロビジョニング
- 一貫性グループベースのバックアップ
- クローンワークフロー
- ワークフローを復元する
- リソース グループを作成または変更するときのセカンダリ保護のプロビジョニング。

> セカンダリ保護は、 ONTAP 9.16.1以降のバージョンでのみサポートされます。

セカンダリ改ざん防止スナップショット **(TPS)** のサポート

SnapCenter Plug-in for VMware vSphereでは、セカンダリ TPS のサポートが導入され、セカンダリ スナップショット コピーがランサムウェア攻撃者や不正な管理者による削除や変更から保護され、攻撃後でも使用できるようになります。

アップグレード パス

アップグレードできるSnapCenter Plug-in for VMware vSphere (SCV) のバージョンは、現在実行しているバージョンによって異なります。

SnapCenter Plug-in for VMware vSphere (SCV) 4.8 以上へのアップグレードは、VMware vCenter Server 7 Update 1 以降のバージョンでのみサポートされます。バージョン 7 アップデート 1 より前の VMware vCenter Server の場合は、引き続き SCV 4.7 を使用する必要があります。

SCV バージョンを使用している場合…	**SCV** を直接アップグレードできます…
SCV 6.0	SCV 6.1
SCV 5.0	SCV 6.0 および SCV 6.1
SCV 4.9	SCV 5.0 および SCV 6.0
SCV 4.8	SCV 4.9 および SCV 5.0
SCV 4.7	SCV 4.8 および SCV 4.9

SnapCenterと統合された仮想化データベースおよびファイル システムの場合、アップグレード パスは次のとおりです。

使用している場合	**VMware** プラグインが…	直接アップグレードできます…
SnapCenter 6.1	SCV 6.0	SCV 6.1
SnapCenter 6.0	SCV 5.0	SCV 6.0
SnapCenter 5.0	SCV 4.9	SCV 5.0
SnapCenter 4.9	SCV 4.8	SCV 4.9
SnapCenter 4.8	SCV 4.7	SCV 4.8

サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool" （IMT）。

概念

製品概要

SnapCenter Plug-in for VMware vSphereは、Linuxベースの仮想アプライアンスとして導入されます。

SnapCenter Plug-in for VMware vSphereは、環境に次の機能を追加します。

- VM整合性およびクラッシュ整合性を備えたデータ保護処理のサポート

  vCenterでVMware vSphere Client GUIを使用して、VMware仮想マシン（従来のVMとvVol VM）、VMDK、およびデータストアのすべてのバックアップ処理とリストア処理を実行できます。vVol VM（vVolデータストア内のVM）の場合は、クラッシュ整合性バックアップのみがサポートされます。また、VMやVMDKをリストアしたり、ゲストOS上に存在するファイルとフォルダをリストアしたりすることもできます。

  VM、VMDK、およびデータストアをバックアップする場合、プラグインではRDMはサポートされません。VMのバックアップ ジョブではRDMが無視されます。RDMをバックアップする必要がある場合は、SnapCenterアプリケーションベースのプラグインを使用する必要があります。

  SnapCenter Plug-in for VMware vSphereには、SnapCenter Plug-in for VMware vSphereのメタデータを格納するMySQLデータベースが含まれています。VM整合性およびクラッシュ整合性を備えたデータ保護を実現するために、SnapCenter Serverをインストールする必要はありません。

- アプリケーション整合性（application-over-VMDK / RDM）を備えたデータ保護処理のサポート

  SnapCenter GUIと適切なSnapCenterアプリケーション プラグインを使用して、VM上のプライマリおよびセカンダリ ストレージにあるデータベースとファイルシステムに対してすべてのバックアップ処理とリストア処理を実行できます。

  SnapCenterは、SnapCenter Plug-in for VMware vSphereをネイティブに活用して、VMDK、rawデバイスマッピング（RDM）、およびNFSデータストア上のすべてのデータ保護処理を実行します。仮想アプライアンスの導入後、vCenterとのやり取りはすべてプラグインによって処理されます。SnapCenter Plug-in for VMware vSphereは、SnapCenterアプリケーションベースのプラグインをすべてサポートしています。

  SnapCenter は、データベースと VM の単一スナップショットをサポートしていません。VM とデータベースのバックアップは個別にスケジュール設定して実行する必要があり、データベースと VM が同じボリュームにホストされている場合でも個別のスナップショットが作成されます。データベース アプリケーションのバックアップ スケジュールは、SnapCenter GUIを使用して設定します。また、VMとデータストアのバックアップ スケジュールは、VMware vSphere Client GUIを使用して設定します。

- VMの整合性のあるスナップショットにはVMwareツールが必要です

  VMware ツールがインストールされておらず、実行されていない場合、ファイル システムは停止されず、クラッシュ整合性のあるスナップショットが作成されます。

- SAN (VMFS) 環境での復元操作には VMware Storage vMotion が必要です。

  VMwareファイルシステム（VMFS）のリストア ワークフローでは、VMware Storage vMotion機能を使用します。Storage vMotionは、vSphere Standardライセンスに含まれていますが、vSphere EssentialsまたはEssentials Plusライセンスでは使用できません。

NFS環境の大部分のリストア処理では、ONTAPのネイティブ機能（Single File SnapRestoreなど）が使用されるため、VMware Storage vMotionは必要ありません。

- VMware vVol VMを設定するには、ONTAP Tools for VMware vSphereが必要

  ONTAPおよびVMware Web ClientでvVol用のストレージをプロビジョニングおよび設定するには、ONTAP Toolsを使用します。

  詳細については、 ONTAP tools for VMware vSphereのドキュメントを参照してください。さらに、以下を参照してください "NetApp Interoperability Matrix Tool"ONTAPツールでサポートされているバージョンに関する最新情報。

- SnapCenter Plug-in for VMware vSphereは、Linux VMに仮想アプライアンスとして導入される

  仮想アプライアンスはLinux VMとしてインストールする必要がありますが、SnapCenter Plug-in for VMware vSphereではWindowsベースのvCenterとLinuxベースのvCenterの両方がサポートされます。SnapCenterはこのプラグインをネイティブで使用し、ユーザの介入は必要ありません。vCenterと通信し、WindowsおよびLinuxの仮想アプリケーションに対してデータ保護処理を実行するSnapCenterアプリケーションベースのプラグインをサポートします。

これらの主要機能に加えて、 SnapCenter Plug-in for VMware vSphereは、iSCSI、ファイバー チャネル、FCoE、NFS 3.0/4.1、VMFS 5.0/6.0、NVMe over FC、NVMe over TCP もサポートします。

サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool" （IMT）。

NFSプロトコルとESXiホストの詳細については、VMwareが提供するvSphere Storageのドキュメントを参照してください。

SnapCenterのデータ保護の詳細については、以下のSnapCenterプラグインのデータ保護情報を参照してください。 "SnapCenterドキュメント" 。

サポートされているアップグレードおよび移行パスの詳細については、以下を参照してください。"SnapCenter Plug-in for VMware vSphereのリリース ノート" 。

各種SnapCenter GUIの概要

SnapCenter環境では、適切なGUIを使用してデータ保護処理と管理処理を実行する必要があります。

SnapCenter Plug-in for VMware vSphereは、他のSnapCenterプラグインとは異なるスタンドアロン プラグインです。VM、VMDK、データストアのすべてのバックアップ処理とリストア処理には、vCenterのVMware vSphere Client GUIを使用する必要があります。また、Web Client GUIダッシュボードを使用して、保護されているVMと保護されていないVMのリストを監視することもできます。バックアップ、リストア、ジョブ監視など、他のすべてのSnapCenterプラグイン（アプリケーションベースのプラグイン）処理には、SnapCenter GUIを使用します。

VMとデータストアを保護するには、VMware vSphere Clientインターフェイスを使用します。Web クライアント GUI は、ストレージ システム上のNetAppスナップショット テクノロジーと統合されます。これにより、VMやデータストアを数秒でバックアップし、ESXiホストをオフラインにすることなくVMをリストアすることが可能です。

また、SnapCenter Plug-in for VMware vSphereで管理操作を実行するための管理GUIも用意されています。

次の表に、SnapCenter GUIで実行される処理を示します。

この **GUI** を使用します…	これらの操作を実行するには…	これらのバックアップにアクセスするには…
SnapCenter vSphere Client GUI	VM およびデータストアのバックアップ VMDK の接続と切断 データストアのマウントとマウント解除 VM および VMDK の復元 ゲストファイルとフォルダの復元	VMware vSphere Client GUIを使用したVMとデータストアのバックアップ
SnapCenter GUI	Microsoft SQL Server、Microsoft Exchange、Oracleのデータベース保護を含む、VM上のデータベースとアプリケーションのバックアップおよびリストア。データベースクローン	SnapCenter GUIを使用して実行されたバックアップ
SnapCenter Plug-in for VMware vSphereの管理GUI	ネットワーク構成の変更、サポートバンドルの生成、NTPサーバ設定の変更、プラグインの無効化/有効化	N/A
vCenter GUI	vCenter Active Directory ユーザーに SCV ロールを追加する ユーザーまたはグループにリソース アクセスを追加する	N/A

VM整合性バックアップおよびリストア処理には、VMware vSphere Client GUIを使用する必要があります。データストアのマウントや名前変更など、一部の処理はVMware Toolsを使用して実行できますが、これらの処理はSnapCenterリポジトリに登録されず、認識されません。

SnapCenter は、データベースと VM の単一スナップショットをサポートしていません。VM とデータベースのバックアップは個別にスケジュール設定して実行する必要があり、データベースと VM が同じボリュームにホストされている場合でも個別のスナップショットが作成されます。アプリケーションベースのバックアップは、SnapCenter GUIを使用してスケジュール設定する必要があります。また、VM整合性バックアップは、VMware vSphere Client GUIを使用してスケジュール設定する必要があります。

ライセンス

次のストレージ システムを使用している場合、SnapCenter Plug-in for VMware vSphere は無償で提供されます。

- オンプレミスのONTAPクラスタ（FAS、 AFF、 ASAシステム）
- Cloud Volumes ONTAP
- ONTAP Select

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 システムでSnapCenter Standard ライセンスが有効になっていない場合、フェイルオーバー操作を実行した後にSnapCenterを使用できません。ただし、マウント処理と接続処理を実行するには、セカンダリ ストレージにFlexCloneライセンスが必要です。リストア処理を実行するには、SnapRestore

ライセンスが必要です。

ロールベース アクセス制御（RBAC）

SnapCenter Plug-in for VMware vSphereでは、仮想リソースを管理するためのRBACが強化されています。このプラグインでは、vCenter Server RBACとONTAP RBACの両方がサポートされています。

SnapCenterとONTAP RBACは、SnapCenter Serverのアプリケーション整合性（application-over-VMDK）ジョブにのみ適用されます。SnapCenter Plug-in for VMware vSphereを使用してSnapCenterのアプリケーション整合性ジョブをサポートする場合は、SnapCenterAdminロールを割り当てる必要があります。また、SnapCenterAdminロールの権限は変更できません。

SnapCenter Plug-in for VMware vSphereには、事前定義されたvCenterロールが付属しています。SnapCenterの操作を実行するには、vCenter GUIを使用してvCenter Active Directoryユーザにこれらのロールを追加する必要があります。

ロールの作成と変更、ユーザへのリソース アクセスの追加はいつでも実行できます。ただし、SnapCenter Plug-in for VMware vSphereを初めて設定する場合は、少なくともActive Directoryのユーザまたはグループをロールに追加してから、それらのユーザまたはグループにリソース アクセスを追加する必要があります。

SnapCenter Plug-in for VMware vSphereユーザ用のRBACのタイプ

SnapCenter Plug-in for VMware vSphereを使用している場合、vCenter Serverでさらに細かくRBACを実装できます。このプラグインでは、vCenter Server RBACとONTAP RBACの両方がサポートされています。

vCenter Server RBAC

このセキュリティ メカニズムは、SnapCenter Plug-in for VMware vSphereで実行されるすべてのジョブに適用されます。これらのジョブには、VM整合性、VMクラッシュ整合性、およびSnapCenter Serverアプリケーション整合性（application-over-VMDK）ジョブが含まれます。このレベルのRBACは、vSphereユーザが仮想マシン（VM）やデータストアなどのvSphereオブジェクトに対してSnapCenter Plug-in for VMware vSphereタスクを実行する権限を制限します。

SnapCenter Plug-in for VMware vSphere環境では、vCenterでのSnapCenter処理用に次のロールが作成されます。

```
SCV Administrator
SCV Backup
SCV Guest File Restore
SCV Restore
SCV View
```

vSphere管理者は、次の手順でvCenter Server RBACを設定します。

- vCenter Serverアクセス許可をルート オブジェクト（ルート フォルダ）に対して設定します。その後、アクセス許可が不要な子エンティティのアクセスを禁止することでセキュリティを強化できます。

- Active DirectoryユーザにSCVロールを割り当てます。

  最低限、すべてのユーザがvCenterオブジェクトを表示できる必要があります。この権限がないと、ユーザはVMware vSphere Client GUIにアクセスできません。

ONTAP RBAC

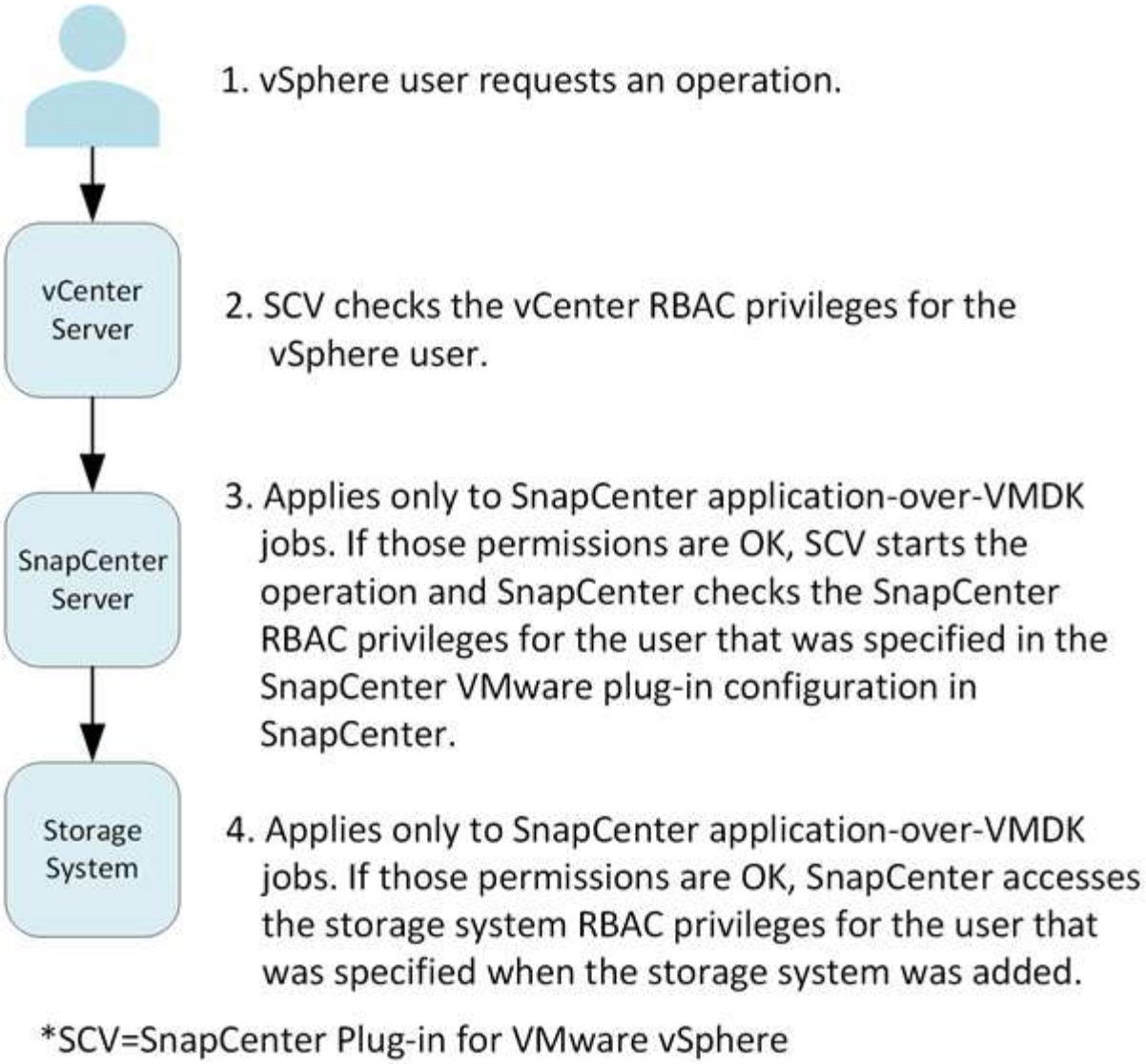
このセキュリティ メカニズムは、SnapCenter Serverのアプリケーション整合性（application-over-VMDK）ジョブにのみ適用されます。このレベルでは、特定のストレージ システムに対して、特定のストレージ処理（データストアのストレージをバックアップするなど）を実行するSnapCenterの権限が制限されます。

ONTAPおよびSnapCenter RBACを設定するには、次のワークフローを使用します。

1. ストレージ管理者が、必要な権限を持つロールをStorage VM上で作成します。
2. 次に、ストレージ管理者がそのロールをストレージ ユーザに割り当てます。
3. SnapCenter管理者が、そのストレージ ユーザ名を使用して、Storage VMをSnapCenter Serverに追加します。
4. 次に、SnapCenter管理者が、SnapCenterユーザにロールを割り当てます。

RBAC権限の検証ワークフロー

次の図に、RBAC権限（vCenterとONTAPの両方）の検証ワークフローの概要を示します。



SnapCenter Plug-in for VMware vSphereのONTAP RBAC機能

> ONTAP RBACは、SnapCenter Serverのアプリケーション整合性（application-over-VMDK）ジョブにのみ適用されます。

ONTAPのRBACを使用すると、特定のストレージ システムへのアクセスとそれらのストレージ システムで実行できる操作を制御できます。SnapCenter Plug-in for VMware vSphereは、vCenter Server RBAC、SnapCenter RBAC（アプリケーションベースの処理をサポートするために必要な場合）、およびONTAP RBACと連携して、特定のユーザが特定のストレージ システムのオブジェクトに対して実行できるSnapCenterタスクを決定します。

SnapCenterは、ユーザが設定したクレデンシャル（ユーザ名とパスワード）を使用して各ストレージ システムを認証し、そのストレージ システムで実行できる操作を決定します。SnapCenter Plug-in for VMware vSphereは、ストレージ システムごとに1セットのクレデンシャルを使用します。このクレデンシャルに基づいてそのストレージ システムで実行できるすべてのタスクが決まります。つまり、このクレデンシャル

はSnapCenterのクレデンシャルであり、個々のSnapCenterユーザのクレデンシャルではありません。

ONTAP RBACは、ストレージ システムへのアクセスとストレージ関連のSnapCenterタスク（VMのバックアップなど）の実行にのみ適用されます。あるストレージ システムに対する適切なONTAP RBAC権限がユーザにないと、そのストレージ システムでホストされているvSphereオブジェクトに対してタスクを実行することはできません。

各ストレージ システムには、一連のONTAP権限が関連付けられます。

ONTAP RBACとvCenter Server RBACの両方を使用すると、次のような利点があります。

- セキュリティ

  どのユーザがどのタスクを実行できるかを、vCenter Serverオブジェクト レベルおよびストレージ システム レベルで制御できます。

- 監査情報

  多くの場合、SnapCenterはストレージ システムについての監査証跡を提供し、ストレージに対して変更を行ったvCenterユーザまでさかのぼってイベントを追跡できます。

- 使いやすさ

  コントローラのクレデンシャルを一元管理できます。

SnapCenter Plug-in for VMware vSphereに組み込みの事前定義のロール

vCenter Server RBACとの連携を簡単にするため、SnapCenter Plug-in for VMware vSphereには、ユーザにSnapCenterタスクの実行を許可する一連の事前定義されたロールが用意されています。また、タスクの実行は許可せず、SnapCenter情報の表示のみを許可する読み取り専用ロールもあります。

事前定義されたロールには、タスクを正しく完了するために必要なSnapCenter固有の権限とvCenter Server標準の権限の両方が含まれています。また、サポートされるすべてのバージョンのvCenter Serverで必要な権限が付与されています。

管理者は、これらのロールを適切なユーザに割り当てることができます。

これらのロールは、管理者がvCenter Web Client Serviceの再起動やインストールの変更を行うたびにSnapCenter Plug-in for VMware vSphereによってデフォルト値（初期の権限セット）に戻されます。SnapCenter Plug-in for VMware vSphereをアップグレードした場合、事前定義されたロールは、新しいバージョンのプラグインに合わせて自動的にアップグレードされます。

次の表に示すように、メニュー **>** 管理 **>** ロール を選択すると、vCenter GUI で事前定義されたロールを確認できます。

ロール	説明
SCV Administrator	すべてのSnapCenter Plug-in for VMware vSphereタスクを実行するために必要なvCenter Server標準の権限とSnapCenter固有の権限がすべて含まれています。SCV 6.1 リリース以降、二次保護を作成するための新しい権限がこのロールに追加されました。
SCV Backup	vSphereオブジェクト（仮想マシンおよびデータストア）のバックアップに必要なvCenter Server標準の権限とSnapCenter固有の権限がすべて含まれています。さらに、設定にアクセスする権限も含まれています。バックアップのリストアはできません。SCV 6.1 リリース以降、二次保護を作成するための新しい権限がこのロールに追加されました。
SCV Guest File Restore	ゲストのファイルとフォルダのリストアに必要なvCenter Server標準の権限とSnapCenter固有の権限がすべて含まれています。VMやVMDKをリストアすることはできません。
SCV Restore	SnapCenter Plug-in for VMware vSphereを使用してバックアップされたvSphereオブジェクトのリストア、およびゲストのファイルとフォルダのリストアに必要なvCenter Server標準の権限とSnapCenter固有の権限がすべて含まれています。さらに、設定にアクセスする権限も含まれています。vSphereオブジェクトはバックアップできません。
SCV View	すべてのSnapCenter Plug-in for VMware vSphereのバックアップ、リソース グループ、およびポリシーへの読み取り専用アクセスが含まれています。

SnapCenter Plug-in for VMware vSphere用にONTAP RBACを設定する方法

ONTAP RBACは、SnapCenter Serverのアプリケーション整合性（application-over-VMDK）ジョブにのみ適用されます。

> 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させるには、SCVサービスを再起動する必要があります。ログインアカウントの作成または変更については、以下を参照してください。 "管理者認証とRBAC設定用のワークシート" 。

SnapCenter Plug-in for VMware vSphereでONTAP RBACを使用する場合は、ストレージ システムでONTAP RBACを設定する必要があります。ONTAPから次のタスクを実行する必要があります。

- ロールを作成します。

  "管理者認証とRBAC"

- ONTAPで、ロールに対してユーザ名とパスワード（ストレージ システム クレデンシャル）を作成する

  このストレージ システムのクレデンシャルは、SnapCenter Plug-in for VMware vSphere用にストレージ システムを設定するために必要です。これを行うには、プラグインでクレデンシャルを入力します。これらのクレデンシャルを使用してストレージ システムにログインするたびに、クレデンシャルの作成時にONTAPで設定したSnapCenter機能が表示されます。

管理者ログインまたはrootログインを使用すればSnapCenterのすべてのタスクにアクセスできますが、ONTAPのRBAC機能を使用して、権限を制限したカスタム アカウントをいくつか作成することを推奨します。

詳細については、 "必要な最小ONTAP権限" 。

始めましょう

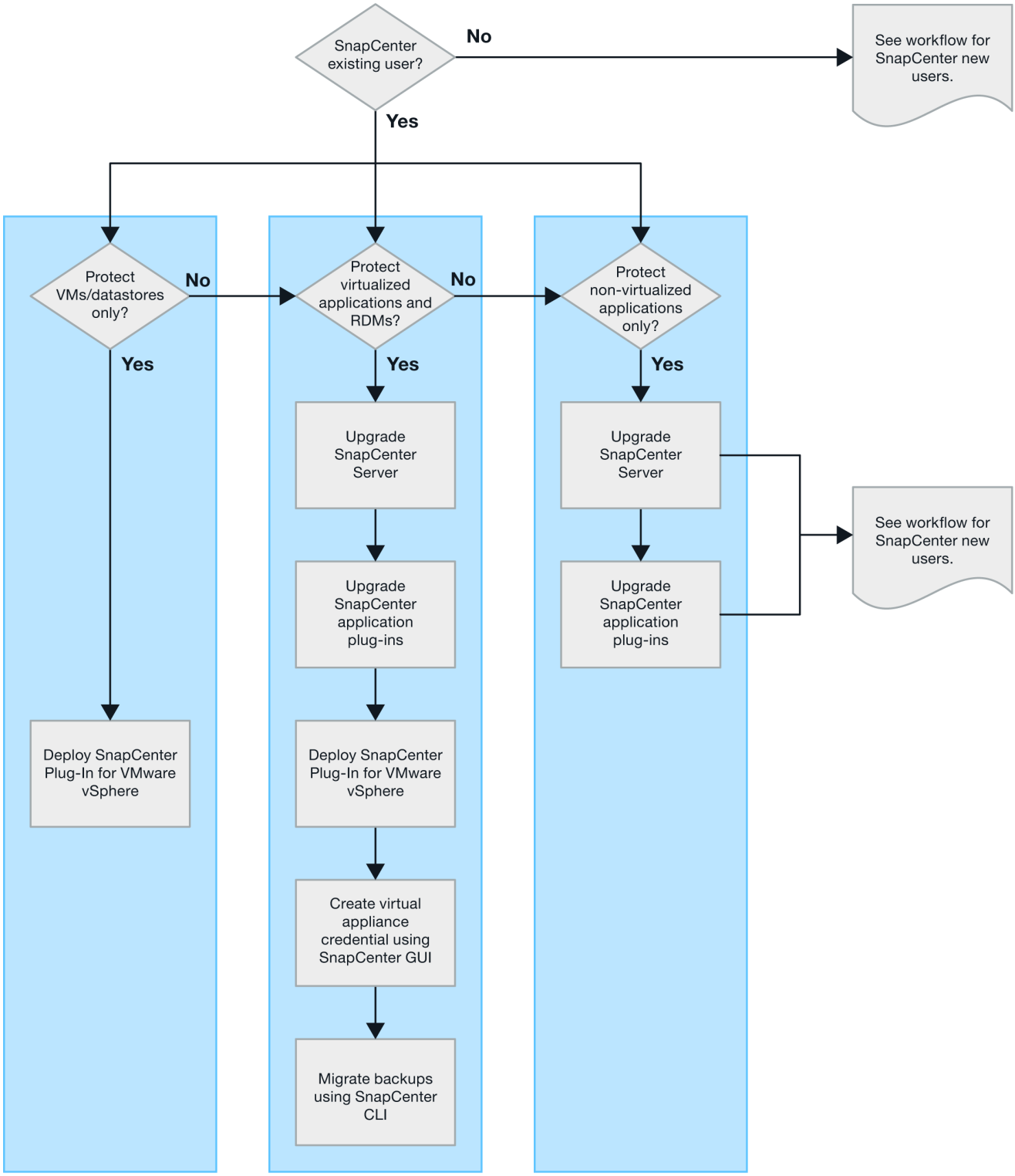
導入プロセスの概要

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、新規の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バックアップをすでに所有しているSnapCenterユーザの場合は、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を導入するための要件

導入の計画と要件

SnapCenter Plug-in for VMware vSphere (SCV) の導入を開始する前に、次の要件を理解

しておく必要があります。

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 Plug-in for VMware vSphere は、 Windows システム上のデータを保護するために使用されるか、Linux システム上のデータを保護するために使用されるかに関係なく、Linux VM として展開されます。
- vCenter ServerにSnapCenter Plug-in for VMware vSphere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 Plug-in for VMware vSphereが展開されているタイム ゾーンで実行され、vCenter は、それが配置されているタイム ゾーンでデータを報告します。そのため、SnapCenter Plug-in for VMware vSphereとvCenterが異なるタイムゾーンにある場合は、SnapCenter Plug-in for VMware vSphere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。

- 名前に特殊文字が含まれるフォルダにSnapCenter Plug-in for VMware vSphereを展開しないでください。

  フォルダー名には、次の特殊文字を含めることはできません: $!@#%^&()_+{}';.,*?"<>|

- vCenter Serverごとに、SnapCenter Plug-in for VMware vSphereの固有の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 Plug-in for VMware vSphere 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 Plug-in for VMware vSphereの各インスタンスは、個別のLinux VMとして導入する必要があります。

    たとえば、vCenter Server の 6 つの異なるインスタンスからバックアップを実行するとします。その場合、6 台のホストにSnapCenter Plug-in for VMware vSphereを展開し、各 vCenter Server をSnapCenter Plug-in for VMware vSphere の一意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、まず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するために使用します。

  詳細については、 ONTAP tools for VMware vSphereのドキュメントを参照してください。さらに、以下を参照してください "NetApp Interoperability Matrix Tool"ONTAPツールでサポートされているバージョンに関する最新情報。

- SnapCenter Plug-in for VMware vSphereでは、Storage vMotionをサポートする際の仮想マシンの制限により、共有のPCIデバイスまたはPCIeデバイス（NVIDIA Grid GPUなど）のサポートは限定的です。詳細については、ベンダーが提供するVMwareの導入ガイドを参照してください。
  - サポートされる処理：

    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データストア上にあり、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の接続および接続解除

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

- サポートされない処理：

VM整合性を伴うバックアップの作成

1つ以上のVMDKがVMFSデータストア上にある場合の、VM全体のリストア

- SnapCenter Plug-in for VMware vSphereの制限事項の詳細については、以下を参照してください。"SnapCenter Plug-in for VMware vSphereのリリース 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	SnapMirrorまたはSnapVault（関係のタイプを問わず、セカンダリのデータ保護用）
その他の製品	vSphere Standard、Enterprise、または Enterprise Plus Storage vMotion を使用してリストア操作を実行するには、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 は含まれません。
プライマリ デスティネーション	SnapCenter Standard: VMware 上でアプリケーションベースの保護を実行するために必要SnapRestore: VMware VM およびデータストアのリストア操作のみを実行するために必要FlexClone: VMware VM およびデータストアのマウントおよび接続操作のみに使用
セカンダリ デスティネーション	SnapCenter Standard: VMware FlexClone上のアプリケーションベースの保護のフェイルオーバー操作に使用: VMware VM およびデータストアのマウントおよび接続操作にのみ使用

ソフトウェア サポート

項目	サポート対象のバージョン
vCenter vSphere	7.0U1以上
ESXiサーバ	7.0U1以上
IPアドレス	IPv4、IPv6
VMware TLS	1.2、1.3
SnapCenter ServerでのTLS	1.2、1.3 SnapCenterサーバは、これを使用して、VMDK データ保護操作を介したアプリケーションのためにSnapCenter Plug-in for VMware vSphereと通信します。

項目	サポート対象のバージョン
VMwareアプリケーションvStorage API for Array Integration（VAAI）	SnapCenter Plug-in for VMware vSphereは、これ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させます。
ONTAP tools for VMware	SnapCenter Plug-in for VMware vSphereは、これを使用して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、 "NetApp Interoperability Matrix Tool" 。

サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool" 。

NVMe over TCPおよび**NVMe over FC**プロトコルの要件

NVMe over TCP および NVMe over FC プロトコル サポートの最小ソフトウェア要件は次のとおりです。

- vCenter vSphere 7.0U3
- ESXi 7.0U3
- ONTAP 9.10.1

スペース、サイズ、スケーリングの要件

項目	要件
推奨CPU数	8
推奨RAM	24 GB
SnapCenter Plug-in for VMware vSphere、ログ、MySQLデータベース用の最小ハード ドライブ スペース	100 GB
アプライアンス内の vmcontrol サービスの最大ヒープ サイズ	8 GB

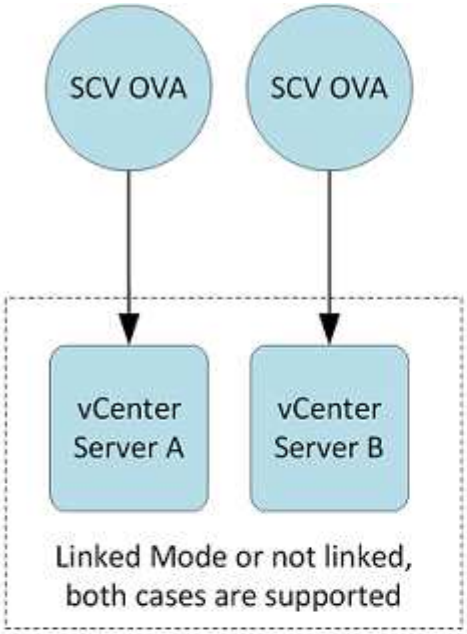
接続とポートの要件

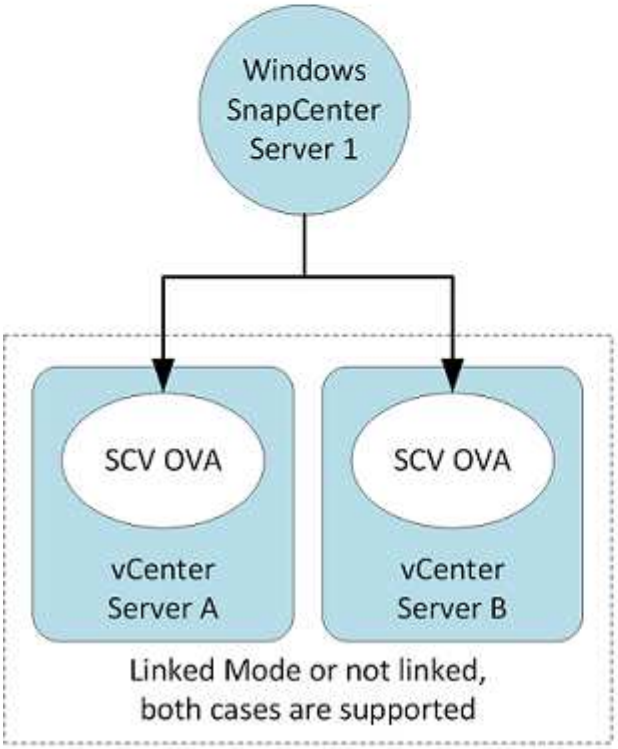
ポートのタイプ	事前設定されたポート
VMware ESXi Serverのポート	443 (HTTPS)、双方向 ゲスト ファイル復元機能はこのポートを使用します。
SnapCenter Plug-in for VMware vSphereのポート	8144 (HTTPS)、双方向 このポートは、VMware vSphere クライアントとSnapCenterサーバーからの通信に使用されます。 8080 双方向 このポートは仮想アプライアンスの管理に使用されます。 注: SnapCenterに SCV ホストを追加するためのカスタム ポートがサポートされています。
VMware vSphere 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。

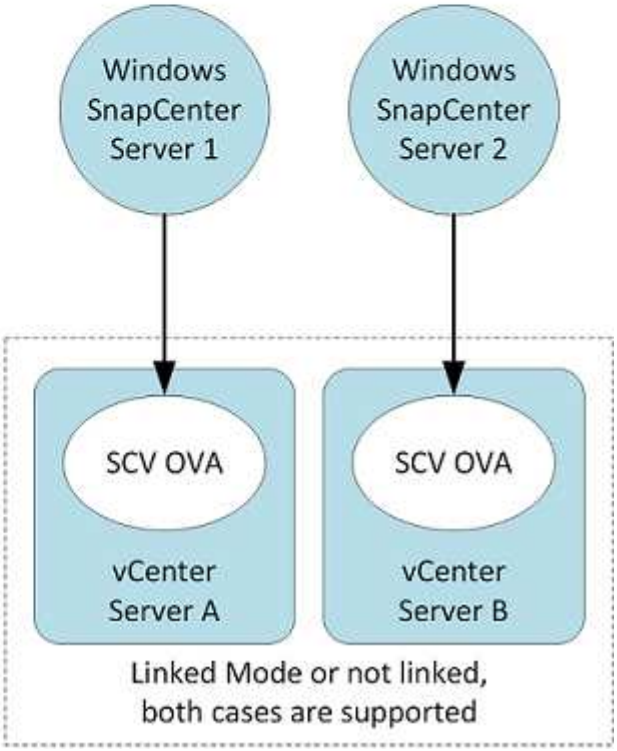
ポートのタイプ	事前設定されたポート
ストレージ クラスタまたはStorage VMのポート	443 (HTTPS)、双方向 80 (HTTP)、双方向 このポートは、仮想アプライアンスとストレージ VM またはストレージ VM を含むクラスター間の通信に使用されます。

サポートされる構成

各プラグイン インスタンスは、リンク モードの 1 つの vCenter Server のみをサポートします。ただし、次の図に示すように、複数のプラグイン インスタンスが同じSnapCenter Server をサポートできます。







必要な**RBAC**権限

vCenter 管理者アカウントには、次の表に記載されている必要な 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を導入および登録する	拡張機能: 拡張機能を登録する
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 • 拡張機能の更新 • 拡張機能の登録解除
SnapCenterに登録されているvCenterのクレデンシャル ユーザ アカウントが、SnapCenter Plug-in for VMware vSphereへのユーザ アクセスを検証できるようにする	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 管理者、SCV バックアップ、SCV ゲスト、ファイル復元、SCV 復元、SCV ビューの権限は、vCenter ルートに割り当てる必要があります。

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、インストール済みプラグインの表が含まれています。この表はAutoSupport Viewerに表示されます。

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させるには、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プラグインには、次の最小権限が必要です。

全アクセス コマンド: 最小限のONTAP権限。
event generate-autosupport-log
ジョブ履歴 ジョブを表示 ジョブを表示 ジョブを停止

lun lun 作成 lun 削除 lun igroup 追加 lun igroup 作成 lun igroup 削除 lun igroup 名前変更 lun igroup 表示 lun マッピング レポート ノード追加 lun マッピング lun マッピング作成 lun マッピング削除 lun マッピング レポート ノード削除 lun マッピング表示 lun 修正 lun ボリューム移動 lun オフライン lun オンライン lun 永続予約クリア lun サイズ変更 lun シリアル lun 表示
snapmirror list-destinations snapmirror policy add-rule snapmirror policy modify-rule snapmirror policy remove-rule snapmirror policy show snapmirror restore snapmirror show snapmirror show-history snapmirror update snapmirror update-ls-set
version
ボリューム クローン、ボリュームの作成、クローンの表示、ボリュームの分割、開始、ボリューム クローンの分割の状態、ボリュームのクローンの分割の停止、ボリュームの作成、ボリュームの削除、ボリュームの破棄、ファイル クローン、ボリュームの作成、ファイル、ディスク使用量の表示、ボリュームのオフライン、ボリュームのオンライン、ボリュームの管理機能、ボリュームの変更、ボリュームの qtree の作成、ボリュームの qtree の削除、ボリュームの qtree の変更、ボリュームの表示、ボリュームの制限、ボリュームの表示、スナップショットの作成、ボリュームのスナップショットの削除、ボリュームのスナップショットの変更、ボリュームのスナップショットのスナップロックの有効期限の変更、ボリュームのスナップショットの名前の変更、ボリュームのスナップショットの復元、ファイルの復元、ボリュームのスナップショットの表示、ボリュームのスナップショットの表示、デルタの表示、ボリュームのマウント解除
vserver cifs vserver cifs share create vserver cifs share delete vserver cifs shadowcopy show vserver cifs share show vserver cifs show vserver export-policy vserver export-policy create vserver export-policy delete vserver export-policy rule create vserver export-policy rule show vserver export-policy show vserver iscsi vserver iscsi connection show vserver nvme subsystem controller vserver nvme subsystem controller show vserver nvme subsystem create vserver nvme subsystem delete vserver nvme subsystem host vserver nvme subsystem host show vserver nvme subsystem host add vserver nvme subsystem host remove vserver nvme subsystem map vserver nvme subsystem map show vserver nvme subsystem map add vserver nvme subsystem map remove vserver nvme subsystem modify vserver nvme subsystem show vserver nvme namespace create vserver nvme namespace delete vserver nvme namespace modify vserver nvme namespace show network interface network interface failover-groups

読み取り専用コマンド**:** 最小限の**ONTAPPrivileges**
クラスタIDの表示、ネットワークインターフェースの表示、vserver、vserver peer、vserverの表示

全アクセスコマンド**:** 最小限の**ONTAP**権限
一貫性グループストレージユニット表示

データ vServer に関連付けるロールを作成するときは、*cluster identity show* クラスター レベル コマンドを無視できます。

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もかまいません。

ONTAPに関するその他の情報

- SnapMirrorアクティブ同期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。
- 改ざん不能のSnapshot（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。
- NVMe over TCP および NVMe over FC プロトコルの場合は、 ONTAP 9.10.1 以降が必要です。

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。場合によっては、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ります。KB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"詳細についてはこちらをご覧ください。

必要な最小vCenter権限

SnapCenter Plug-in for VMware vSphereの導入を開始する前に、最小限必要なvCenter権限があることを確認してください。

vCenter管理者ロールに必要な権限

Datastore.AllocateSpace、Datastore.Browse、Datastore.Delete、Datastore.FileManagement、Datastore.Move、Datastore.Rename、Extension.Register、Extension.Unregister、Extension.Update、Host.Config.AdvancedConfig、Host.Config.Resources、Host.Config.Settings、Host.Config.Storage、Host.Local.CreateVM、Host.Local.DeleteVM、Host.Local.ReconfigVM、Network.Assign、Resource.ApplyRecommendation、Resource.AssignVMToPool、Resource.ColdMigrate、Resource.HotMigrate、Resource.QueryVMotion、System.Anonymous、System.Read、System.View、Task.Create、Task.Update、VirtualMachine.Config.AddExistingDisk、VirtualMachine.Config.AddNewDisk、VirtualMachine.Config.AdvancedConfig、VirtualMachine.Config.ReloadFromPath、VirtualMachine.Config.RemoveDisk、VirtualMachine.Config.Resource、VirtualMachine.GuestOperations.Execute、VirtualMachine.GuestOperations.Modify VirtualMachine.GuestOperations.Query、VirtualMachine.Interact.PowerOff、VirtualMachine.Interact.PowerOn、VirtualMachine.Inventory.Create、VirtualMachine.Inventory.CreateFromExisting、VirtualMachine.Inventory.Delete、VirtualMachine.Inventory.Move、VirtualMachine.Inventory.Register、VirtualMachine.Inventory.Unregister、VirtualMachine.State.CreateSnapshot、VirtualMachine.State.RemoveSnapshot、VirtualMachine.State.RevertToSnapshot

SnapCenter Plug-in for VMware vCenterに固有の必要な権限

Privileges	ラベル
netappSCV.Guest.RestoreFile	ゲスト ファイルのリストア
netappSCV.Recovery.MountUnMount	マウント / アンマウント
netappSCV.Backup.DeleteBackupJob	リソース グループ / バックアップの削除
netappSCV.Configure.ConfigureStorageSystems.Delete	ストレージ システムの削除
netappSCV.View	View
netappSCV.Recovery.RecoverVM	VMの回復
netappSCV.Configure.ConfigureStorageSystems.AddUpdate	ストレージ システムの追加 / 変更
netappSCV.Backup.BackupNow	今すぐバックアップ
netappSCV.Guest.Configure	ゲストの設定
netappSCV.Configure.ConfigureSnapCenterServer	SnapCenterサーバーを構成する
netappSCV.Backup.BackupScheduled	リソース グループを作成

オープン仮想アプライアンス（OVA）のダウンロード

オープン仮想アプライアンス（OVA）をインストールする前に、vCenterに証明書を追加します。.tarファイルには、OVA証明書、Entrustルート証明書、中間証明書が含まれていて、証明書は証明書フォルダで参照できます。OVA環境は、VMware vCenter 7u1以降でサポートされます。

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" ）。
   - 製品リストから * SnapCenter Plug-in for VMware vSphere* を選択し、 最新リリースのダウンロードボタンを選択します。
   - SnapCenter Plug-in for VMware vSphereをダウンロードする `.tar`ファイルを任意の場所に転送します。
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ルート証明書および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 **>** 証明書管理 に移動します。
5. *信頼されたルート証明書*の横にある*追加*を選択します
   - *certs* フォルダに移動します。
   - Entrustルート証明書および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るようになります。

> ダウンロードした OVA が改ざんされていない場合は、[発行者] 列に [信頼できる証明書] が表示されます。

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しておく必要があるすべての操作を示します。

> OVA環境は、VMware vCenter 7u1以降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環境の構成と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 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の.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が含まれた証明書が必要です。詳細については、以下の記事を参照してください。 "ストレージ証明書管理"セクション。
- 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、ブラウザを閉じておく必要があります。また、SnapCenter Plug-in for VMware vSphereの導入時にブラウザ キャッシュの問題が発生するのを回避するために、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 Plug-in for VMware vSphere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 Plug-in for VMware vSphere、および各vCenterを同じ時刻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ツールのサポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool" 。ONTAP toolsを使用して、ONTAPおよびVMware Web Client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 Plug-in for VMware vSphereを導入します。バックアップ スケジュールは、SnapCenter Plug-in for VMware vSphere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 Plug-in for VMware vSphereとvCenterが異なるタイムゾーンにある場合は、SnapCenter Plug-in for VMware vSphere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、"オープン仮想アプライアンス（OVA）のダウンロード"証明書を vCenter にインポートします。
2. ブラウザからVMware vSphere vCenterにアクセスします。

   IPv6 アドレスの HTML Web クライアントの場合は、Chrome または Firefox のいずれか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. ナビゲータ ペインで、データセンター、クラスター、ホストなど、仮想マシンの有効な親オブジェクトである任意のインベントリ オブジェクトを右クリックし、[OVF テンプレートのデプロイ] を選択して VMware デプロイ 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。*OVFテンプレートの選択*ページで、 `.ova` .tar で抽出されたフォルダー内のファイル。
6. *次へ*を選択します。
7. *名前とフォルダーの選択*ページで、VM または vApp の一意の名前を入力し、展開場所を選択して、*次

へ*を選択します。

このステップでは、 `.tar`ファイルを vCenter にアップロードします。 VMのデフォルト名は選択したVMの名前と同じです。 `.ova`ファイル。デフォルト名を変更する場合は、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 オブジェクトとなります。

8. *リソースの選択*ページで、デプロイされた VM テンプレートを実行するリソースを選択し、*次へ*を選択します。
9. *レビューの詳細*ページで、 `.tar`テンプレートの詳細を選択し、[次へ] を選択します。
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、デプロイされた OVF テンプレートのファイルを保存する場所と方法を定義します。

    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 ファイルはこの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. ソース ネットワークを選択し、デスティネーション ネットワークにマップします。

       [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** 割り当て設定 セクションで、必要な IP アドレス プロトコルを選択し、次へ を選択します。

       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。参照 "KB記事: 追加のネットワークアダプタを作成する方法"。

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. 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 資格情報を入力します。

       *vCenterユーザー名*フィールドに、次の形式でユーザー名を入力します。 `domain\username` 。

    b. **SCV** 資格情報の作成 セクションで、ローカル資格情報を入力します。

       ユーザー名 フィールドにローカル ユーザー名を入力します。ドメインの詳細は含めないでください。

> 指定したユーザ名とパスワードをメモしておいてください。あとでSnapCenter Plug-in for VMware vSphereの設定を変更する場合、これらのクレデンシャルが必要になります。

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セットアップ*セクションで、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、IPv4 検索ドメインなどのネットワーク情報を入力します。

   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、IPv6 検索ドメインなどのネットワーク情報を入力します。

   必要に応じて、IPv4 または IPv6 アドレス フィールド、あるいはその両方を選択します。 IPv4 アドレスと IPv6 アドレスの両方を使用している場合は、そのうちの 1 つに対してのみプライマリ DNS を指定する必要があります。

> ネットワーク構成として DHCP を使用して続行する場合は、これらの手順をスキップして、[ネットワーク プロパティのセットアップ] セクションのエントリを空白のままにすることができます。

a. *セットアップ日時*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*を選択します。

    すべてのホストをIPアドレスで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）。導入前に入力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のを待つ間、[Recent Tasks]ウィンドウで導入の進捗状況を確認できます。

    SnapCenter Plug-in for VMware vSphereの導入が正常に完了した場合、プラグインはLinux VMとして導入され、vCenterに登録されます。また、VMware vSphere Clientもインストールされます。

15. SnapCenter Plug-in for VMware vSphereがデプロイされている VM に移動し、[概要] タブを選択して、[電源オン] ボックスを選択し、仮想アプライアンスを起動します。

16. SnapCenter Plug-in for VMware vSphere の電源がオンになっている間に、デプロイされたSnapCenter Plug-in for VMware vSphere を右クリックし、ゲスト **OS** を選択して、**VMware** ツールのインストール を選択します。

    VMware toolsは、SnapCenter Plug-in for VMware vSphere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 Plug-in for VMware vSphereが起動すると導入が成功したことが画面上に通知され、VMware Toolsがインストールされ、SnapCenter Plug-in for VMware vSphereへのログインを求められます。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、静的アドレスからDHCPへの切り替えはサポートされていません。

    画面にはSnapCenter Plug-in for VMware vSphereの導入先のIPアドレスが表示されます。IPアドレスをメモしておきます。SnapCenter Plug-in for VMware vSphereの設定を変更する場合、プラグインの管理GUI

にログインする必要があります。

17. 導入時の画面に表示された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 Plug-in for VMware vSphere管理GUIにログインし、SnapCenter Plug-in for VMware vSphereがvCenterに接続され、有効になっていることをダッシュボードで確認します。

    フォーマットを使用する `\https://<appliance-IP-address>:8080`管理 GUI にアクセスします。

    導入時に設定した管理者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 Plug-in for VMware vSphereが有効になっていない場合は、"VMware vSphere Clientサービスの再起動" 。

    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。

終了後の操作

必要な手続きを完了してください"展開後の運用"。

導入後の必要な処理と問題

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、データ保護処理を実行する前に、Storage VMをSnapCenterに追加する必要があります。Storage VMを追加する際は、管理LIFを指定してください。クラスタを追加し、クラスタ管理LIFを指定することもできます。ストレージの追加については、以下を参照してください。"ストレージの追加" 。

導入で発生する可能性がある問題

- 仮想アプライアンスを展開した後、次のシナリオではダッシュボードの バックアップ ジョブ タブが読み込まれない場合があります。
  - IPv4 アドレスを実行しており、 SnapCenter VMware vSphere ホストに 2 つの IP アドレスがあります。その結果、ジョブ要求がSnapCenter Serverで認識されないIPアドレスに送信されることがあります。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 Plug-in for VMware vSphereがデプロイされている場所に移動します。
    `/opt/netapp/scvservice/standalone_aegis/etc`
    ii. network- interface.propertiesファイルを開きます。
    iii. の中で `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つある場合。
- SnapCenter Plug-in for VMware vSphereの導入後も、vCenterで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す。

これらの問題を修正するには、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 を選択して、* SnapCenter Plug-in for VMware vSphere* を選択します。

認証エラーの管理

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. 次の形式を使用して、SnapCenter Plug-in for VMware vSphere管理 GUI にログオンします。`https://<appliance-IP-address>:8080` 。管理者のユーザ名、パスワード、およびMFAトークンの情報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 ServerへのSnapCenter Plug-in for VMware vSphereの登録

SnapCenterでapplication-over-VMDKワークフロー（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）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 Server 4.2以降が実行され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。

タスク概要

- 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 Plug-in for VMware vSphere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を登録する必要があります。

手順

1. SnapCenter GUI の左側のナビゲーション ペインで、ホスト を選択します。
2. 上部の 管理対象ホスト 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て、それがSnapCenterサーバーから解決されることを確認します。

3. ウィザードを開始するには、[追加] を選択します。
4. [ホストの追加] ダイアログ ボックスで、次の表に示すように、 SnapCenterサーバーに追加するホストを指定します。

フィールド	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。
クレデンシャル	導入時に指定したSnapCenter Plug-in for VMware vSphereのユーザ名とパスワードを入力します。

5. *送信*を選択します。

   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] を選択し、[資格情報] タブを選択して [追加] を選択し、仮想アプライアンスの資格情報を追加します。
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]フィールドでは、[Linux]を選択する必要があります。

終了後の操作

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 Serverでの登録を更新する必要があります。

SnapCenter VMware vSphere Clientへのログイン

SnapCenter Plug-in for VMware vSphereを導入すると、vCenterにVMware vSphere Clientがインストールされ、他のvSphere Clientとともにvcenterの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. ブラウザからVMware vSphere vCenterにアクセスします。
2. **VMware vCenter Single Sign-On** ページにログインします。

   *ログイン*ボタンを選択します。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] を選択し、* SnapCenter Plug-in for VMware vSphere* を選択します。

クイック スタート

概要

このクイック スタート ドキュメントには、SnapCenter Plug-in for VMware vSphere仮想アプライアンスを導入し、SnapCenter Plug-in for VMware vSphereを有効にする手順がまとめられています。これらの手順の対象者は、SnapCenterをまだインストールしておらず、VMとデータストアの保護を必要とするユーザです。

始める前に、"導入の計画と要件" 。

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。その"オープン仮想アプライアンス（OVA）のダウンロード"このページでは、OVA ファイルをダウンロードする手順を説明します。

1. VMware vCenter 7.0.3以降のバージョンの場合は、"オープン仮想アプライアンス（OVA）のダウンロード"証明書を vCenter にインポートします。
2. ブラウザからVMware vSphere vCenterにアクセスします。

   IPv6 アドレスの HTML Web クライアントの場合は、Chrome または Firefox のいずれか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. ナビゲーション ペインで、データセンター、フォルダー、クラスター、ホストなど、仮想マシンの有効な親オブジェクトである任意のインベントリ オブジェクトを右クリックし、**OVF** テンプレートのデプロイを選択して、VMware デプロイ ウィザードを起動します。
5. *OVFテンプレートの選択*ページで、 `.ova`ファイル（次の表に記載）を選択し、[次へ] を選択します。

このウィザード ページでは...	操作
名前とフォルダを選択してください	VMまたはvAppに一意の名前を指定し、導入先の場所を選択します。
リソースを選択	導入したVMテンプレートを実行するリソースを選択します。
Review details	確認する `.ova`テンプレートの詳細。
License agreements	*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選択します。
ストレージを選択	導入したOVFテンプレートのファイルを格納する場所と方法を定義します。
ネットワークを選択	ソース ネットワークを選択してデスティネーション ネットワークにマップします。

このウィザード ページでは...	操作
Customize template	既存の **vCenter** に登録 で、vCenter の資格情報を入力します。 * SnapCenter Plug-in for VMware vSphere の資格情報の作成* で、 SnapCenter Plug-in for VMware vSphere の資格情報を入力します。 指定したユーザ名とパスワードをメモしておいてください。あとでSnapCenter Plug-in for VMware vSphereの設定を変更する場合、これらのクレデンシャルが必要になります。 *ネットワークプロパティのセットアップ*セクションで、ネットワーク情報を入力します。 *セットアップ日時*セクションで、vCenter が配置されているタイムゾーンを選択します。
Ready to complete	ページを確認し、[完了] を選択します。

すべてのホストをIPアドレスで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）。導入前に入力内容は検証されません。

6. SnapCenter Plug-in for VMware vSphereがデプロイされた VM に移動し、[概要] タブを選択して、[電源オン*] ボックスを選択し、 SnapCenter Plug-in for VMware vSphere を起動します。

7. SnapCenter Plug-in for VMware vSphere の電源がオンになっている間に、デプロイされたSnapCenter Plug-in for VMware vSphere を右クリックし、ゲスト **OS** を選択して、**VMware** ツールのインストール を選択します。

   導入が完了するまでに数分かかることがあります。SnapCenter Plug-in for VMware vSphereが起動すると導入が成功したことが画面上に通知され、VMware Toolsがインストールされ、SnapCenter Plug-in for VMware vSphereへのログインを求められます。

   画面にはSnapCenter Plug-in for VMware vSphereの導入先のIPアドレスが表示されます。IPアドレスをメモしておきます。SnapCenter Plug-in for VMware vSphereの設定を変更する場合、プラグインの管理GUIにログインする必要があります。

8. 導入時の画面に表示された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 Plug-in for VMware vSphere管理GUIにログインし、SnapCenter Plug-in for VMware vSphereがvCenterに接続され、有効になっていることをダッシュボードで確認します。

   フォーマットを使用する `\https://<appliance-IP-address>:8080`管理 GUI にアクセスします。

   導入時に設定した管理者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。

9. vCenter HTML5クライアントにログインし、ツールバーの*メニュー*を選択し、* SnapCenter Plug-in for VMware vSphere*を選択します。

ストレージの追加

ストレージを追加するには、このセクションの手順を実行します。

1. SCV プラグインの左側のナビゲータ ペインで、ストレージ システム を選択し、追加 オプションを選択します。
2. [ストレージ システムの追加] ダイアログ ボックスで、基本的な SVM またはクラスタ情報を入力し、[追加] を選択します。

バックアップ ポリシーの作成

バックアップ ポリシーを作成するには、次の手順に従います

1. SCV プラグインの左側のナビゲータ ペインで、ポリシー を選択し、新しいポリシー を選択します。
2. 新しいバックアップ ポリシー ページで、ポリシー構成情報を入力し、追加 を選択します。

リソース グループの作成

リソース グループを作成するには、次の手順を実行します。

1. SCV プラグインの左側のナビゲータ ペインで、リソース グループ を選択し、作成 を選択します。
2. リソース グループの作成ウィザードの各ページに必要な情報を入力し、リソース グループに含める VM とデータストアを選択し、リソース グループに適用するバックアップ ポリシーを選択します。リモート セカンダリ保護の詳細を追加し、バックアップスケジュールを指定します。

バックアップは、リソース グループに設定されたバックアップ ポリシーに従って実行されます。

リソースグループ*ページからオンデマンドでバックアップを実行するには、 *今すぐ実行。

監視とレポート

ステータス情報の表示

vSphere Clientのダッシュボードでステータス情報を確認できます。ステータス情報は1時間に1回更新されます。

手順

1. vCenterクライアントの[Shortcuts]ページで、SnapCenter Plug-in for VMware vSphere（SCV）を選択します。
2. SCV の左側のナビゲーション ペインで、ダッシュボード > ステータス を選択します。
3. 次の表に示すように、概要ステータス情報を表示するか、詳細を表示するリンクを選択してください。

このダッシュボードタイルは...	次の情報を表示します...
最近の職務活動	最新の 3 〜 5 件のバックアップ、復元、マウントジョブ。 • ジョブ ID を選択すると、そのジョブの詳細が表示されます。 • すべてのジョブの詳細を確認するには、[すべて表示] を選択して [ジョブ モニター] タブに移動します。
ジョブ	選択した時間枠内で実行された各ジョブ タイプ (バックアップ、復元、マウント) の数。グラフのセクションにカーソルを合わせると、そのカテゴリの詳細情報が表示されます。

このダッシュボードタイルは...	次の情報を表示します...
最新の保護サマリ	選択した時間枠内のプライマリおよびセカンダリ VM またはデータストアのデータ保護ステータスの概要。 • ドロップダウン メニューを選択して、**VM** または データストア を選択します。 • セカンダリ ストレージの場合は、* SnapVault* または * SnapMirror* を選択します。 • グラフのセクションにカーソルを合わせると、そのカテゴリ内のVMまたはデータストアの数が表示されます。[Successful]カテゴリには、リソースごとに最新のバックアップが表示されます。 • 構成ファイルを編集することで、期間を変更できます。デフォルトの期間は7日です。詳細については、 "設定のカスタマイズ" 。 • 内部カウンタは、プライマリまたはセカンダリのバックアップごとに更新されます。ダッシュボード タイルは6時間ごとに更新されます。更新時間は変更できません。注: ミラー ボールト保護ポリシーを使用する場合、保護サマリーのカウンターはSnapMirrorチャートではなくSnapVaultサマリー チャートに表示されます。
構成	SnapCenter Plug-in for VMware vSphereによって管理される各オブジェクトのタイプごとの合計数。
ストレージ	生成されたスナップショット、 SnapVaultショット、およびSnapMirrorスナップショットの合計数と、プライマリ スナップショットとセカンダリ スナップショットに使用されるストレージの量。線グラフには、過去90日間について、プライマリとセカンダリそれぞれの1日のストレージ使用量が表示されます。ストレージ情報は、24 時間ごとに午前 1 時 8 分に更新されます。ストレージ節約は、論理容量 (スナップショット節約と消費されたストレージ) とプライマリ ストレージの物理容量の比率です。棒グラフはストレージ削減率を示しています。 グラフの線にカーソルを合わせると、1日ごとの詳細な結果が表示されます。

ジョブの監視

VMware vSphere Clientを使用してデータ保護処理を実行したあとは、ダッシュボード

の[Job Monitor]タブでジョブ ステータスを監視し、ジョブの詳細を確認できます。

手順

1. vCenterクライアントの[Shortcuts]ページで、SnapCenter Plug-in for VMware vSphere（SCV）を選択します。
2. SCV の左側のナビゲーション ペインで、ダッシュボード を選択します。
3. 2 つ以上の vCenter がリンク モードで構成されている場合は、SCV プラグイン インスタンスを選択し、[ジョブ モニター] タブを選択します。[Job Monitor]タブに、各ジョブ、およびそのステータス、開始時刻、終了時刻が表示されます。ジョブ名が長い場合は、右にスクロールしないと開始時刻と終了時刻が表示されない場合があります。表示は30秒ごとに更新されます。
   - オンデマンドで表示を更新するには、ツールバーの更新アイコンを選択します。
   - 表示するジョブの期間、タイプ、タグ、ステータスを選択するには、フィルタ アイコンを選択します。フィルタでは大文字と小文字が区別されます。
   - ジョブの実行中に表示を更新するには、[Job Details]ウィンドウで更新アイコンを選択します。

ダッシュボードにジョブ情報が表示されない場合は、 "KB 記事: SnapCenter vSphere クライアント ダッシュボードにジョブが表示されない" 。

ジョブ ログのダウンロード

ジョブ ログは、SnapCenter VMware vSphere Clientのダッシュボードにある[Job Monitor]タブからダウンロードできます。

VMware vSphere Clientの使用時に予期しない動作が発生した場合、ログ ファイルで原因を特定して問題を解決することができます。

> ジョブ ログの保持期間のデフォルト値は30日です。また、ジョブの保持期間のデフォルト値は90日です。設定された保持期間よりも古いジョブ ログおよびジョブは、6時間ごとにパージされます。設定を使用することができます `jobs/cleanup`ジョブとジョブ ログの保持期間を変更するための REST API。パージ スケジュールは変更できません。

手順

1. vCenterクライアントの[Shortcuts]ページで、SnapCenter Plug-in for VMware vSphere（SCV）を選択します。
2. SCV の左側のナビゲーション ペインで、ダッシュボード > ジョブ モニター を選択します。
3. [Job Monitor]タイトル バーで、ダウンロード アイコンを選択します。

   アイコンが表示されない場合は、右にスクロールしてください。

   ジョブをダブルクリックしてジョブの詳細ウィンドウにアクセスし、*ジョブ ログのダウンロード*を選択することもできます。

結果

ジョブ ログは、SnapCenter Plug-in for VMware vSphereが導入されているLinux VMホストに保存されます。デフォルトのジョブログの場所は `/var/log/netapp`。

ジョブログをダウンロードしようとしたが、エラー メッセージに指定されたログ ファイルが削除されている場合は、次のエラーが発生する可能性があります。 `HTTP ERROR 500 Problem accessing /export-scv-logs` 。このエラーを修正するには、エラー メッセージで指定されたファイルのファイル アクセス ステータスと権限を確認し、アクセスの問題を修正します。

レポートへのアクセス

ダッシュボードから1つ以上のジョブのレポートを要求できます。

[Reports]タブには、ダッシュボードの[Jobs]ページで選択したジョブに関する情報が表示されます。ジョブを選択していない場合、[Reports]タブは空白になります。

手順

1. vCenterクライアントの[Shortcuts]ページで、SnapCenter Plug-in for VMware vSphere（SCV）を選択します。
2. SCV の左側のナビゲーション ペインで、ダッシュボード > レポート タブを選択します。
3. [Backup Reports]では、次の操作を実行できます。
   a. レポートの変更

      フィルタ アイコンを選択して、期間、ジョブ ステータスのタイプ、リソース グループ、およびレポートに含めるポリシーを変更します。

   b. 詳細なレポートの生成

      任意のジョブをダブルクリックして、そのジョブの詳細なレポートを生成します。

4. オプション: [レポート] タブで [ダウンロード] を選択し、形式 (HTML または CSV) を選択します。

   ダウンロード アイコンを選択してプラグイン ログをダウンロードすることもできます。

VMware vSphere Clientからのレポートの種類

SnapCenterのVMware vSphere Clientには、カスタマイズ可能なレポートが用意されており、データ保護ジョブやプラグイン リソースのステータスに関する詳細を確認できます。プライマリ保護のレポートのみを生成できます。

> バックアップ スケジュールは、SnapCenter Plug-in for VMware vSphere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 Plug-in for VMware vSphereとvCenterが異なるタイムゾーンにある場合、VMware vSphere Clientのダッシュボードのデータはレポートのデータと異なる可能性があります。

移行されたバックアップに関する情報は、移行後にバックアップが実行されたあと、ダッシュボードに表示されます。

レポートの種類	説明
Backup Report	バックアップ ジョブに関する概要データが表示されます。グラフ上のセクション/ステータスを選択すると、レポート タブにそのステータスのジョブのリストが表示されます。レポートには、ジョブごとにジョブ ID、対応するリソース グループ、バックアップ ポリシー、開始時刻と期間、ステータス、ジョブの詳細 (ジョブが完了した場合はジョブ名 (スナップショット名) を含む)、および警告やエラー メッセージがリストされます。レポート テーブルは、HTML形式またはCSV形式でダウンロードできます。レポート内のジョブだけでなく、すべてのジョブの[Job Monitor]ジョブ ログもダウンロードできます。削除されたバックアップはレポートに含まれません。
Mount Report	マウント ジョブに関する概要データが表示されます。グラフ上のセクション/ステータスを選択すると、レポート タブにそのステータスのジョブのリストが表示されます。ジョブごとに、ジョブID、ジョブ ステータス、ジョブ名、およびジョブの開始時刻と終了時刻が表示されます。ジョブ名にはスナップショット名が含まれます。例えば： `Mount Backup <snapshot-copy-name>`レポート テーブルを HTML または CSV 形式でダウンロードできます。レポート内のジョブだけでなく、すべてのジョブの[Job Monitor]ジョブ ログもダウンロードできます。
Restore Report	リストア ジョブに関する概要ステータス情報が表示されます。グラフ上のセクション/ステータスを選択すると、レポート タブにそのステータスのジョブのリストが表示されます。ジョブごとに、ジョブID、ジョブ ステータス、ジョブ名、およびジョブの開始時刻と終了時刻が表示されます。ジョブ名にはスナップショット名が含まれます。例えば： `Restore Backup <snapshot-copy-name>`レポート テーブルを HTML または CSV 形式でダウンロードできます。レポート内のジョブだけでなく、すべてのジョブの[Job Monitor]ジョブ ログもダウンロードできます。

レポートの種類	説明
VMまたはデータストアの最新の保護ステータスレポート	SnapCenter Plug-in for VMware vSphereで管理されているVMとデータストアについて、設定された日数における保護ステータスに関する概要情報が表示されます。デフォルトの期間は7日です。プロパティファイルの値を変更するには、"設定のデフォルト値の変更" 。プライマリ保護チャートのセクション/ステータスを選択すると、レポート タブにそのステータスの VM またはデータストアのリストが表示されます。保護された VM およびデータストアの VM またはデータストア保護ステータス レポートには、構成された日数の間にバックアップされた VM またはデータストアの名前、最新のスナップショット名、および最新のバックアップ実行の開始時刻と終了時刻が表示されます。保護されていないVMまたはデータストアの「VM or Datastores Protection Status Report」には、設定された日数の間に一度も適切にバックアップされなかったVMまたはデータストアの名前が表示されます。レポート テーブルは、HTML形式またはCSV形式でダウンロードできます。レポート内のジョブだけでなく、すべてのジョブの[Job Monitor]ジョブ ログもダウンロードできます。このレポートは、プラグインのキャッシュが更新されるのに合わせて1時間ごとに更新されます。そのため、最近バックアップされたVMまたはデータストアが表示されないことがあります。

SnapCenter Plug-in for VMware vSphere GUIからのサポートバンドルの生成

開始する前に

SnapCenter Plug-in for VMware vSphere管理GUIにログオンするには、IPアドレスとログイン クレデンシャルが必要です。また、メンテナンス コンソールから生成されたMFAトークンもメモしておく必要があります。

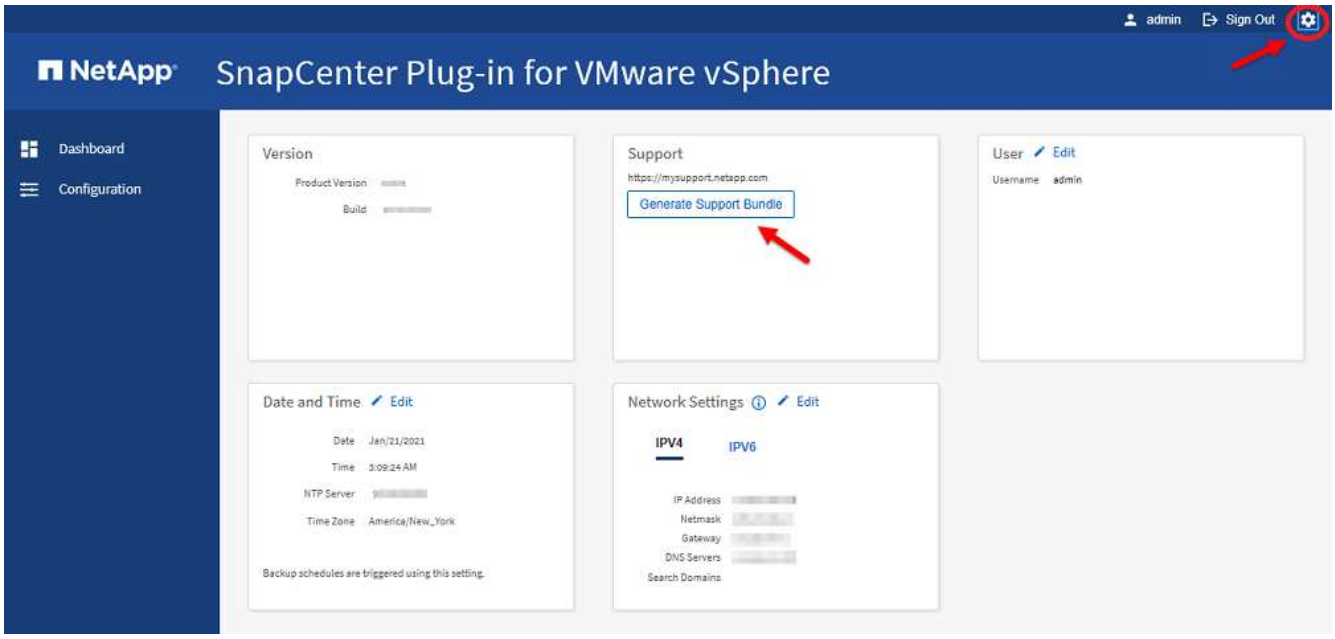
- このIPアドレスは、SnapCenter Plug-in for VMware vSphereの導入時に表示されたものです。
- SnapCenter Plug-in for VMware vSphereの導入時に指定したログイン クレデンシャル、またはあとで変更したログイン クレデンシャルを使用します。
- メンテナンス コンソールのシステム構成オプションを使用して、6桁のMFAトークンを生成します。

手順

1. SnapCenter Plug-in for VMware vSphereのGUIにログインします。

   フォーマットを使用する `https://<OVA-IP-address>:8080`。

2. 上部のツールバーにある設定アイコンを選択します。



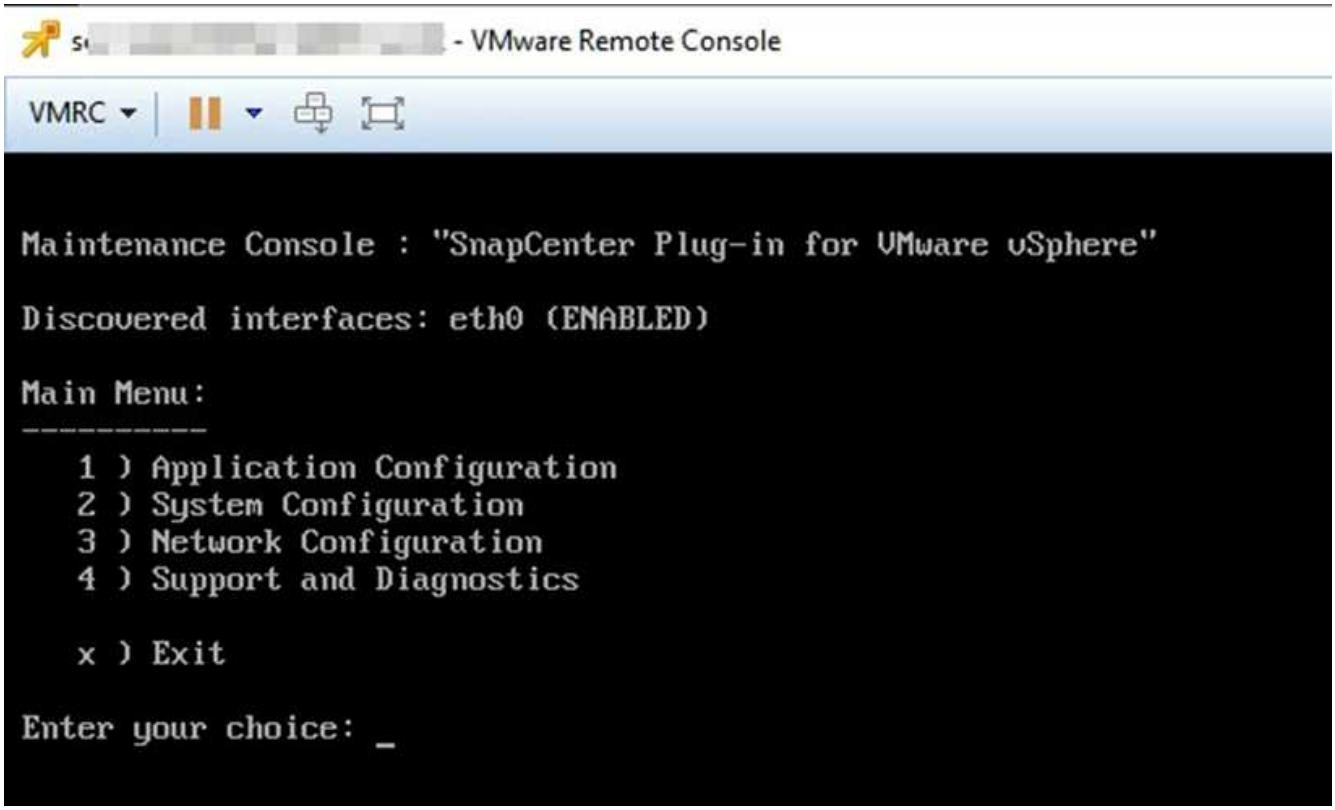
3. *設定*ページの*サポート*セクションで、*サポートバンドルの生成*を選択します。
4. サポート バンドルが生成されたら、提供されているリンクを選択してバンドルをNetAppにダウンロードします。

メンテナンス コンソールからのサポート バンドルの生成

手順

1. VMware vSphere Clientで、SnapCenter Plug-in for VMware vSphereが配置されているVMを選択します。
2. 仮想アプライアンスの 概要 タブで、リモート コンソールの起動または **Web** コンソールの起動 を選択してメンテナンス コンソール ウィンドウを開き、ログオンします。

   メンテナンスコンソールへのアクセスとログインについては、以下を参照してください。"メンテナンスコンソールにアクセスする" 。



3. メインメニューからオプション*4) サポートと診断*を入力します。
4. [サポートと診断] メニューから、オプション **1)** サポート バンドルの生成 を入力します。

サポート バンドルにアクセスするには、[サポートと診断] メニューでオプション **2) [**診断シェルにアクセス**]** を入力します。コンソールで、 `/support/support/<bundle_name>.tar.gz` 。

監査ログ

監査ログは時系列でイベントを集めたもので、アプライアンス内のファイルに書き込まれます。監査ログファイルは、`/var/log/netapp/audit`場所、ファイル名は以下の命名規則のいずれかに従います。

- audit.log: 使用中のアクティブな監査ログ ファイル。
- audit-%d{yyyy-MM-dd-HH-mm-ss}.log.gz: ロールオーバーされた監査ログファイル。ファイル名の日時（例：audit-2022-12-15-16-28-01.log.gz）は、ファイルが作成された日時を示します。

SCV プラグインのユーザー インターフェイスでは、ダッシュボード > 設定 > 監査ログ タブから監査ログの詳細を表示およびエクスポートできます。監査ログで操作監査を表示できます。監査ログはサポート バンドルでダウンロードされます。

Eメールが設定されている場合、監査ログの整合性検証エラーが発生したときに、SCVからEメール通知が送信されます。監査ログの整合性検証エラーは、いずれかのファイルが改ざんまたは削除された場合に発生することがあります。

監査ファイルのデフォルト設定は次のとおりです。

- 使用中の監査ログ ファイルの最大サイズは10MB
- 最大10個の監査ログ ファイルが保持される

ロール オーバーされた監査ログは定期的に整合性が検証されます。SCVには、ログを表示したり整合性を検証したりするためのREST APIが用意されています。組み込みのスケジュールがトリガーされ、次の整合性ステータスのいずれかが割り当てられます。

ステータス	説明
TAMPERED	監査ログ ファイルの内容が変更されています
NORMAL	監査ログ ファイルは変更されていません
ROLLOVER DELETE	- 監査ログファイルは保存期間に基づいて削除されます - デフォルトでは10ファイルのみが保存されます
UNEXPECTED DELETE	監査ログ ファイルが削除されました
ACTIVE	- 監査ログファイルが使用中です - audit.log にのみ適用されます

イベントは、主に次の3つのカテゴリに分類されます。

- データ保護のイベント
- メンテナンス コンソールのイベント
- 管理コンソールのイベント

データ保護のイベント

SCVのリソースは次のとおりです。

- Storage System
- Resource Group
- Policy
- バックアップ
- Subscription
- Account

次の表に、各リソースで実行できる処理を示します。

リソース	操作
Storage System	作成、変更、削除
Subscription	作成、変更、削除
Account	作成、変更、削除
Resource Group	作成、変更、削除、中断、再開
Policy	作成、変更、削除

バックアップ	作成、名前変更、削除、マウント、アンマウント、リストア済みVMDK、リストア済みVM、VMDKの接続、VMDKの接続解除、ゲスト ファイルのリストア

メンテナンス コンソールのイベント

メンテナンス コンソールでの管理処理が監査されます。メンテナンス コンソールで使用できるオプションは次のとおりです。

1. サービスの開始 / 停止
2. ユーザ名とパスワードの変更
3. MySQLのパスワードの変更
4. MySQLバックアップの設定
5. MySQLバックアップのリストア
6. 「maint」ユーザーのパスワードを変更する
7. タイムゾーンを変更する
8. NTPサーバーの変更
9. SSHアクセスの無効化
10. jailディスク サイズの拡張
11. Upgrade
12. VMware Tools をインストールします (これを open-vm ツールに置き換える作業を進めています)
13. IPアドレス設定を変更する
14. ドメイン名検索設定を変更する
15. 静的ルートを変更する
16. 診断シェルにアクセスする
17. リモート診断アクセスを有効にする

管理コンソールのイベント

管理コンソールUIでは、次の処理が監査されます。

- 設定
  - adminクレデンシャルの変更
  - タイムゾーンの変更
  - NTPサーバーの変更
  - IPv4/IPv6アドレス設定を変更する
- 構成
  - vCenterクレデンシャルの変更
  - プラグインの有効化 / 無効化

syslogサーバの設定

監査ログはアプライアンス内に保存され、定期的に整合性が検証されます。イベント転送を使用すると、ソース コンピュータまたは転送元コンピュータからイベントを取得し、一元化されたコンピュータ（syslogサーバ）に保存できます。データは、ソースとデスティネーション間での転送時に暗号化されます。

開始する前に

管理者権限が必要です。

タスク概要

このタスクは、syslogサーバの設定に役立ちます。

手順

1. SnapCenter Plug-in for VMware vSphereにログインします。
2. 左側のナビゲーション ペインで、設定 > 監査ログ > 設定 を選択します。
3. *監査ログ設定*パネルで、*監査ログをSyslogサーバーに送信する*を選択します。
4. 次の情報を入力します。
    - syslogサーバのIP
    - syslogサーバのポート
    - RFCタイプ
    - syslogサーバ証明書
5. Syslog サーバーの設定を保存するには、[保存] を選択します。

監査ログ設定の変更

ログ設定のデフォルトの設定を変更できます。

開始する前に

管理者権限が必要です。

タスク概要

このタスクは、デフォルトの監査ログ設定を変更するのに役立ちます。

手順

1. SnapCenter Plug-in for VMware vSphereにログインします。
2. 左側のナビゲーション ペインで、設定 > 監査ログ > 設定 を選択します。
3. 監査ログ設定 ペインで、監査ログ ファイルの最大数と監査ログ ファイルのサイズ制限を入力します。
4. ログを Syslog サーバーに送信する場合は、監査ログを **Syslog** サーバーに送信する オプションを選択します。サーバの詳細を入力します。
5. 設定を保存します。

ストレージの管理

ストレージの追加

VMをバックアップまたはリストアする前に、ストレージ クラスタまたはStorage VMを追加する必要があります。ストレージを追加すると、SnapCenter Plug-in for VMware vSphereでvCenterでのバックアップとリストアの処理を認識および管理できるようになります。

- 使用するGUI

  VMware vSphere Clientを使用してストレージを追加します。

- 大規模なLUN

  SnapCenter Plug-in for VMware vSphere 4.5以降では、ASAアグリゲートで最大128TBの大規模なLUNのデータストアがサポートされます。大規模なLUNの場合、レイテンシを回避するために、SnapCenterではシック プロビジョニングされたLUNのみがサポートされます。

- VMware仮想ボリューム（vVol）

  vVolデータ保護を機能させるには、SnapCenter Plug-in for VMware vSphereおよびONTAP tools for VMware vSphereにストレージ クラスタを追加する必要があります。

  詳細については、 ONTAP tools for VMware vSphereのドキュメントを参照してください。さらに、以下を参照してください "NetApp Interoperability Matrix Tool"ONTAPツールでサポートされているバージョンに関する最新情報。

開始する前に

ESXiサーバ、SnapCenter Plug-in for VMware vSphere、および各vCenterが、同じ時刻に同期されている必要があります。ストレージを追加しようとしても、vCenterの時刻設定が同期されていない場合、Java証明書のエラーが発生して処理が失敗することがあります。

タスク概要

SnapCenter Plug-in for VMware vSphereは、直接接続されたStorage VMおよびストレージ クラスタ内のStorage VMに対して、バックアップとリストアの処理を実行します。

> SnapCenter Plug-in for VMware vSphereを使用してVMDKでのアプリケーションベースのバックアップをサポートする場合は、SnapCenter GUIを使用してストレージ認証の詳細情報を入力し、ストレージ システムを登録する必要があります。

- リンク モードのvCenterについては、vCenterごとにストレージ システムを個別に追加する必要があります。
- SVMを追加する場合は、Storage VMの名前が管理LIFに解決される必要があります。

  SnapCenterのストレージ VM 名のエントリを *etc\hosts* ファイルに追加した場合は、これらも仮想アプライアンスから解決可能であることを確認する必要があります。そうでない場合は、アプライアンス内の *etc/hosts* ファイルに同様のエントリを追加する必要があります。

管理LIFに解決できない名前でStorage VMを追加した場合、プラグインがそのStorage VM上のデータストアまたはボリュームを検出できないため、スケジュールしたバックアップ ジョブは失敗します。この場合は、Storage VMをSnapCenterに追加して管理LIFを指定するか、Storage VMを含むクラスタを追加してクラスタ管理LIFを指定してください。

- ストレージ認証の詳細情報は、SnapCenter Plug-in for VMware vSphereの複数のインスタンス間や、Windows SnapCenter ServerとvCenter上のSnapCenterプラグインの間では共有されません。

手順

1. vCenterクライアントの[Shortcuts]ページで、SnapCenter Plug-in for VMware vSphere（SCV）を選択します。
2. SCV の左側のナビゲーション ペインで、ダッシュボード > ストレージ システム を選択します。
3. [ストレージ システム] ページで、[追加] オプションを選択します。
4. ストレージ システムの追加 ウィザードで、次の表に示すように、基本的なストレージ VM またはクラスター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 クラスタまたはStorage VMの完全修飾ドメイン名または管理LIFのIPアドレスを入力します。SnapCenter Plug-in for VMware vSphereでは、異なるクラスタにある同じ名前の複数のStorage VMをサポートしません。
Authentication Method	クレデンシャルまたは証明書のいずれかを選択します。2種類の証明書がサポートされています: - "自己署名証明書" - "CA署名証明書" 。
ユーザー名	このフィールドは、認証方法として[Credentials]を選択した場合に表示されます。Storage VMまたはクラスタへのログオンに使用するONTAPユーザ名を入力します。
パスワード	このフィールドは、認証方法として[Credentials]を選択した場合に表示されます。Storage VMまたはクラスタのログイン パスワードを入力します。
Certificate	このフィールドは、認証方法として[Certificate]を選択した場合に表示されます。証明書ファイルを参照して選択します。
Private Key	このフィールドは、認証方法として[Certificate]を選択した場合に表示されます。秘密鍵ファイルを参照して選択します。
プロトコル	ストレージ プロトコルを選択します。
ポート	ストレージ システムが受け入れるポート。- HTTPS接続の場合は443、HTTP接続の場合は80
Timeout	SnapCenter Plug-in for VMware vSphereの処理がタイムアウトするまでの秒数を入力します。デフォルトは60秒です。

フィールド	操作
Preferred IP address	Storage VMに管理IPアドレスが複数ある場合は、このボックスをオンにし、SnapCenter Plug-in for VMware vSphereで使用するIPアドレスを入力します。注意: IP アドレスを入力するときは、角括弧 ([]) を使用しないでください。
Event Management System(EMS) & AutoSupport Setting	保護が適用されたとき、リストア処理が完了したとき、または処理が失敗したときにEMSメッセージをストレージ システムのsyslogに送信、またはAutoSupportメッセージをストレージ システムに送信するには、該当するチェックボックスをオンにします。AutoSupport通知を有効にするには、失敗した操作に関する**AutoSupport**通知をストレージ システムに送信する チェックボックスと *SnapCenter Server イベントを syslog に記録する* チェックボックスをオンにします。
SnapCenter Server のイベントを syslog に記録	このボックスをオンにすると、SnapCenter Plug-in for VMware vSphereのイベントが記録されます。
失敗した操作に関するAutoSupport通知をストレージ システムに送信する	データ保護ジョブが失敗したときにAutoSupport通知を受信する場合は、このボックスをオンにします。Storage VMでAutoSupportを有効にするとともに、AutoSupportのEメール設定を指定する必要もあります。

5. *追加*を選択します。

   ストレージ クラスタを追加した場合は、そのクラスタ内のすべてのStorage VMが自動的に追加されます。自動的に追加されたStorage VM（「暗黙的な」Storage VMと呼ばれることがあります）は、クラスタの概要ページにユーザ名ではなくハイフン（-）付きで表示されます。ユーザ名は、明示的なストレージ エンティティにのみ表示されます。

ストレージ システムの管理

VMware vSphere Clientを使用してVMやデータストアをバックアップまたはリストアする前に、ストレージを追加する必要があります。

Storage VMの変更

SnapCenter Plug-in for VMware vSphereに登録され、VMのデータ保護処理に使用されるクラスタおよびStorage VMの設定は、VMware vSphere Clientを使用して変更できます。

クラスタの一部として自動的に追加されたStorage VM（暗黙的なStorage VMと呼ばれることがあります）を変更すると、そのStorage VMは明示的なStorage VMに変更され、クラスタ内の他のStorage VMを変更することなく個別に削除できます。証明書を使用した認証方式を使用している場合、[Storage Systems]ページのユーザ名は「N/A」と表示されます。ユーザ名はクラスタ リスト内の明示的なStorage VMに対してのみ表示され、ExplicitSVMフラグがtrueに設定されています。Storage VMはすべて、常に、関連付けられているクラスタの下に表示されます。

SnapCenter GUIを使用してアプリケーションベースのデータ保護処理用にStorage VMを追加した場合は、同じGUIを使用してこれらのStorage VMを変更する必要があります。

手順

1. SCV プラグインの左側のナビゲータ 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 ページで、変更するストレージ VM を選択し、編集 を選択します。
3. ストレージ システムの編集 ウィンドウで新しい値を入力し、更新 を選択して変更を適用します。

Storage VMの削除

VMware vSphere Clientを使用して、vCenterのインベントリからStorage VMを削除できます。

SnapCenter GUIを使用してアプリケーションベースのデータ保護処理用にStorage VMを追加した場合は、同じGUIを使用してこれらのStorage VMを変更する必要があります。

開始する前に

Storage VMを削除する前に、Storage VM内のすべてのデータストアをアンマウントする必要があります。

タスク概要

削除するStorage VMに存在するバックアップがリソース グループに含まれていると、そのリソース グループのそれ以降のバックアップは失敗します。

手順

1. SCV プラグインの左側のナビゲータ 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 ページで、削除するストレージ VM を選択し、削除 を選択します。
3. ストレージ システムの削除 確認ボックスで、ストレージ システムの削除 のボックスをオンにし、はい を選択して確認します。 注意: ESXi ホスト 7.0U1 以降のリリースのみがサポートされています。

   "VMware vSphere Clientサービスの再起動" 。

設定されたストレージ タイムアウトの変更

これまでバックアップが正常に実行されていたとしても、SnapCenter Plug-in for VMware vSphereがStorage VMを待機する時間が、設定されているタイムアウト時間を超えてしまうと、バックアップが失敗することがあります。この状況が発生した場合は、設定されているタイムアウト時間を長くすることで対処できます。

エラーが発生する可能性があります `Unable to discover resources on SCV: Unable to get storage details for datastore <xxx>…`

手順

1. SCV プラグインの左側のナビゲータ 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] ページで、変更するストレージ システムを選択し、[編集] を選択します。
3. [Timeout]フィールドで、秒数を増やします。

大規模な環境では180秒を推奨します。

データの保護

データ保護のワークフロー

SnapCenter vSphere Clientを使用して、VM、VMDK、およびデータストアのデータ保護処理を実行します。すべてのバックアップ処理はリソース グループに対して実行されます。リソース グループには1つ以上のVMとデータストアを任意の組み合わせで含めることができます。バックアップは、オンデマンドで実行するか、または定義した保護スケジュールに従って実行できます。

データストアをバックアップすると、そのデータストア内のすべてのVMがバックアップされます。

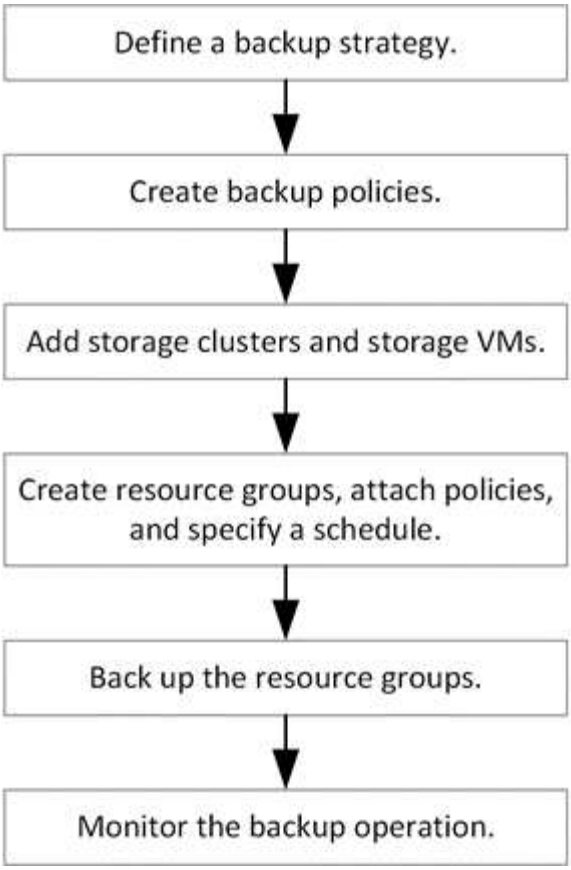
同じリソース グループに対してバックアップ処理とリストア処理を同時に実行することはできません。

SnapCenter Plug-in for VMware vSphere がサポートする内容とサポートしない内容に関する情報を確認する必要があります。"導入の計画と要件"

MetroCluster構成：

- フェイルオーバー後に、SnapCenter Plug-in for VMware vSphereで保護関係を検出できないことがあります。参照 "KB 記事: MetroClusterフェイルオーバー後にSnapMirrorまたはSnapVault関係を検出できない"詳細についてはこちらをご覧ください。
- バックアップがエラーで失敗した場合 `Unable to discover resources on SCV: <xxx>…`スイッチオーバー/スイッチバック後の NFS および VMFS VM の場合は、メンテナンス コンソールからSnapCenter VMware サービスを再起動します。

次のワークフロー図は、バックアップ処理の実行順序を示しています。



VMとデータストアのバックアップの表示

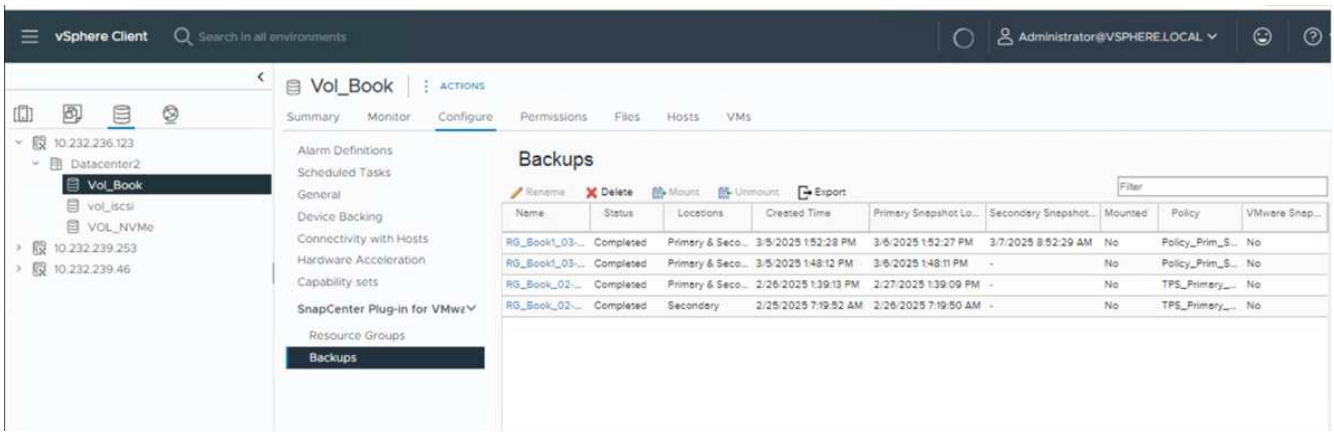
VM またはデータストアのバックアップまたは復元の準備をするときに、そのリソースで使用可能なすべてのバックアップを確認し、それらのバックアップの詳細を表示することが必要になる場合があります。

タスク概要

10K ファイル フォルダーなどの大きなファイル フォルダーを参照する場合、初めての場合は 1 分以上かかることがあります。以降の参照セッションの所要時間は短くなります。

手順

1. vCenter Serverにログインします。
2. インベントリ ページに移動し、データストアまたは VM を選択します。
3. 右側のペインで、構成 > * SnapCenter Plug-in for VMware vSphere* > バックアップ を選択します。



ポリシー作成段階で「セカンダリ スナップショット ロックを有効にする」オプションが選択されていない場合は、「プライマリ スナップショット ロックを有効にする」オプションに設定された値がデフォルトで使用されます。バックアップ リストの「セカンダリ スナップショット ロックの有効期限」フィールドのハイフンは、プライマリ ロック期間とセカンダリ ロック期間が同じであることを示します。

4. 表示するバックアップを選択します。

VMとデータストアのバックアップ ポリシーの作成

SnapCenter Plug-in for VMware vSphereを使用してVMとデータストアをバックアップするには、事前にバックアップ ポリシーを作成する必要があります。

開始する前に

- 前提条件を確認しておく必要があります。
- セカンダリ ストレージの関係を設定しておく必要があります。
  - スナップショットをミラーまたはボールト セカンダリ ストレージに複製する場合は、関係を構成し、SnapCenter管理者がソース ボリュームと宛先ボリュームの両方に対してストレージ VM を割り当てておく必要があります。
  - NFS または VMFS データストア上の Version-FlexibleMirror 関係のスナップショットをセカンダリ ストレージに正常に転送するには、 SnapMirrorポリシー タイプが非同期ミラーであり、「all_source_snapshots」オプションがオンになっていることを確認します。
  - セカンダリ ストレージ (ミラー ボールト) 上のスナップショットの数が最大制限に達すると、バックアップ操作でバックアップを登録して保持を適用するアクティビティが次のエラーで失敗します。

    ```
    This snapshot is currently used as a reference snapshot by one or more
    SnapMirror relationships. Deleting the snapshot can cause future SnapMirror
    operations to fail.
    ```

    この問題を修正するには、スナップショットの最大制限に達しないように、セカンダリ ストレージのSnapMirror保持ポリシーを構成します。

管理者がユーザーにリソースを割り当てる方法については、以下を参照してください。 "ロールベースのアクセス制御の使用に関するSnapCenterの情報" 。

- VMと整合性のあるバックアップが必要な場合は、VMware Toolsをインストールして実行しておく必要があります。VMware Toolsは、VMを休止するために必要となります。VM整合性バックアップは、vVol VMではサポートされていません。

- SnapMirrorアクティブ同期を使用すると、サイト全体の障害が発生した場合でもビジネス サービスの運用を継続でき、アプリケーションがセカンダリ コピーを使用して透過的にフェイルオーバーできるようになります。

  SnapMirrorアクティブ同期は、VMFSデータストアに対してのみサポートされます。

  SnapMirrorアクティブ同期環境のVMFSデータストアを保護するには、SnapCenter管理者が次の作業を行う必要があります。

  - 技術レポートの説明に従ってクラスターとメディエーターを構成します。 "SnapMirrorアクティブ同期用のONTAP Mediatorとクラスタの設定" 。
  - VMFS データストアに関連付けられたボリュームをコンシステンシー グループに追加し、2 つのONTAPストレージ システム間に *AutomatedFailOver* または *AutomatedFailOverDuplex* 保護ポリシーを使用してデータ保護関係を作成します。 *AutomatedFailOverDuplex* ポリシーは、 ONTAP 9.15.1 リリース以降でサポートされます。

ファンアウト構成では、3次サイトでは整合性グループはサポートされません。

タスク概要

ウィザードの各ページのフィールドのほとんどはわかりやすいもので、説明を必要としません。以下の手順では、説明が必要な一部のフィールドを取り上げます。

手順

1. SCV プラグインの左側のナビゲータ ペインで、ポリシー を選択します。
2. ポリシー ページで、作成 を選択してウィザードを開始します。
3. 新しいバックアップ ポリシー ページで、ポリシー名と説明を入力します。

   - リンク モード

     リンク モードでは、vCenterごとに個別の仮想アプライアンスがあります。そのため、複数のvCenterで重複する名前を使用できます。ただし、ポリシーはリソース グループと同じvCenterで作成する必要があります。

   - サポートされない文字

     VM、データストア、クラスター、ポリシー、バックアップ、またはリソース グループの名前には、次の特殊文字を使用しないでください: % & * $ # @ ! \ / : * ? " < > - | ; ' 、およびスペース。

   アンダースコア（_）は使用できます。

4. 頻度を指定します。

   ポリシーではバックアップの頻度のみを指定します。バックアップの具体的なスケジュールは、リソース グループで定義します。したがって、複数のリソース グループで同じポリシーとバックアップ頻度を使用している場合でも、別々のバックアップ スケジュールを設定できます。

5. スナップショットのロックを有効にするには、「ロック期間」チェックボックスを選択します。プライマリおよびセカンダリ スナップショットのロック期間を日数/月数/年数として選択できます。

ONTAP SnapMirrorポリシーで設定された保持値に関係なく、指定されたセカンダリ スナップショットのロック期間が経過するまではセカンダリ スナップショット コピーは削除されません。

6. 保持設定を指定します。

SnapVaultレプリケーションを有効にする場合は、バックアップの保持数を2以上に設定する必要があります。バックアップの保持数を1に設定すると、保持処理が失敗する場合があります。これは、新しいスナップショットがターゲットに複製されるまで、最初のスナップショットがSnapVault関係の参照スナップショットとなるためです。

最大保持値は 1018 バックアップです。保持数を、使用しているONTAPバージョンがサポートする値よりも大きい値に設定すると、バックアップが失敗します。これは、スパニング データストアにも当てはまります。

7. レプリケーション フィールドで、次の表に示すように、セカンダリ ストレージへのレプリケーションの種類を指定します。

フィールド	操作
Update SnapMirror after backup	プライマリ バックアップ ボリュームとのSnapMirror関係がある別のボリュームにバックアップ セットのミラー コピーを作成する場合は、このオプションを選択します。ボリュームにミラー ボールト関係が設定されている場合、バックアップをミラー ボールトの宛先にコピーするには、[バックアップ後にSnapVault を更新] オプションのみを選択する必要があります。 このオプションは、SnapCenter Plug-in for VMware vSphere 4.5以降のFlexGroupボリュームのデータストアでサポートされます。 SnapMirrorアクティブ シンク展開でVMFS データストアを保護するには、「始める前に」セクションに記載されている前提条件を完了し、バックアップ後に**SnapMirror** を更新を有効にする必要があります。

フィールド	操作
Update SnapVault after backup	プライマリ バックアップ ボリュームとのSnapVault関係がある別のボリュームでディスクツーディスク バックアップ レプリケーションを実行する場合は、このオプションを選択します。 ボリュームにmirror-vault関係が設定されている場合、mirror-vaultデスティネーションにバックアップをコピーするには、このオプションのみを選択する必要があります。 このオプションは、SnapCenter Plug-in for VMware vSphere 4.5以降のFlexGroupボリュームのデータストアでサポートされます。
Snapshot label	このポリシーで作成されたSnapVaultおよびSnapMirrorスナップショットに追加するオプションのカスタム ラベルを入力します。スナップショット ラベルは、このポリシーで作成されたスナップショットをセカンダリ ストレージ システム上の他のスナップショットと区別するのに役立ちます。 スナップショット ラベルには最大31 文字まで使用できます。

8. オプション: 詳細 フィールドで、必要なフィールドを選択します。[Advanced]フィールドの詳細を次の表に示します。

フィールド	操作
VM consistency	バックアップ ジョブが実行される際に毎回VMを休止してVMwareスナップショットを作成する場合、オンにします。 このオプションは、vVolではサポートされていません。vVol VMの場合、クラッシュ整合性のあるバックアップのみが実行されます。 VM整合性バックアップを実行するには、VMでVMware Toolsが実行されている必要があります。VMware Toolsが実行されていない場合は、代わりにクラッシュ整合性バックアップが実行されます。 [VM consistency]ボックスをオンにすると、バックアップ処理に必要な時間とストレージ スペースが増えることがあります。オンにした場合、まずVMが休止され、VMwareによってVM整合性スナップショットが実行されます。次に、SnapCenterによってバックアップ処理が実行され、その後VMの処理が再開されます。VM ゲスト メモリは VM 整合性スナップショットには含まれません。
独立型ディスクのデータストアを含める	一時的なデータが格納された独立型ディスクのデータストアをバックアップに含める場合は、このボックスをオンにします。
Scripts	バックアップ操作の前または後にSnapCenter Plug-in for VMware vSphere で実行するプレスクリプトまたはポストスクリプトの完全修飾パスを入力します。たとえば、SNMPトラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。スクリプト パスは、スクリプトの実行時に検証されます。 プリスクリプトとポストスクリプトは、仮想アプライアンスVM上に配置する必要があります。複数のスクリプトを入力するには、各スクリプト パスの後に **Enter** を押して、各スクリプトを別々の行にリストします。セミコロン「;」は使用できません。

9. *追加*を選択します。

[Policies]ページで、ポリシーが作成されたことを確認し、ポリシーを選択してその設定を確認できます。

リソース グループの作成

リソース グループは、保護するVM、データストア、vSphereタグ、vSphere VMフォルダのコンテナです。

リソース グループには、次のリソースを含めることができます。

- 従来のVMとデータストア

  従来のVM、従来のSANデータストア、従来のNASデータストアの任意の組み合わせ。従来のVMをvVol VMと組み合わせることはできません。

- FlexGroupデータストア

  単一のFlexGroupデータストア。スパニングFlexGroupデータストアはサポートされていません。FlexGroupデータストアを従来のVMまたはデータストアと組み合わせることはできません。

- FlexVolデータストア

  1つ以上のFlexVolデータストア。スパニング データストアがサポートされています。

- vVol VM

  1つ以上のvVol VM。vVol VMを従来のVMまたはデータストアと組み合わせることはできません。

- vSphereタグ

  指定したvSphereタグが設定されたすべてのVMとデータストア（vVolデータストアを除く）。

- フォルダ内のvVol VM

  指定した1つのvVolフォルダ内のすべてのvVol。フォルダ内にvVol VMと従来のVMが混在している場合、SnapCenter Plug-in for VMware vSphereではvVol VMがバックアップされ、従来のVMはスキップされます。

- ASA r2 上の VM とデータストア

  ASA r2 VM およびデータストアを他の VM およびデータストアと組み合わせることはできません。

すべてのリソース グループ：

> VMware vSphereクラスタ サービス（vCLS）を使用している場合は、SnapCenter Plug-in for VMware vSphereのリソース グループに、vCLSで管理されているVMを含めないでください。

詳細については、 "vCenter を 7.0.x にアップデートした後、SCV が vCLS VM をバックアップできない"

SnapCenter Plug-in for VMware vSphere 4.5以降では、最大128 TBの大規模なLUNおよびファイルのデータストアと、最大300TBのボリュームがサポートされます。大規模なLUNを保護する場合は、レイテンシを回避するために、シック プロビジョニングされたLUNのみを使用します。

アクセスできない状態のVMは追加しないでください。アクセスできないVMを含むリソース グループを作成することは可能ですが、そのリソース グループのバックアップは失敗します。

開始する前に

vVol VMを含むリソース グループを作成する前に、ONTAP tools for VMwareを導入する必要があります。

詳細については、 ONTAP tools for VMware vSphereのドキュメントを参照してください。さらに、以下を参照してください "NetApp Interoperability Matrix Tool"ONTAPツールでサポートされているバージョンに関する最新情報。

タスク概要

リソース グループに対して、リソースの追加または削除をいつでも実行できます。

- 単一リソースのバックアップ

  単一のリソース（単一のVMなど）をバックアップするには、その単一のリソースを含むリソース グループを作成する必要があります。

- 複数リソースのバックアップ

  複数のリソースをバックアップするには、複数のリソースを含むリソース グループを作成する必要があります。

- MetroCluster環境のFlexGroupボリュームを含むリソース グループ

  ONTAP 9.8またはONTAP 9.9を実行している場合は、スイッチオーバーまたはスイッチバックのあとに、SnapCenter Plug-in for VMware vSphereサービスを再起動し、SnapMirror関係を再同期してから、MetroCluster環境でリソース グループをバックアップする必要があります。

  ONTAP 9.8では、スイッチバック後にバックアップがハングします。ONTAP 9.9では、この問題が修正されています。

- スナップショットの最適化

  スナップショットを最適化するには、同じボリュームに関連付けられている VM とデータストアを 1 つのリソース グループにグループ化する必要があります。

- バックアップ ポリシー

  リソース グループはバックアップ ポリシーがなくても作成できますが、データ保護処理は少なくとも1つのポリシーがリソース グループに適用されている場合にのみ実行できます。リソース グループの作成プロセスで、既存のポリシーを使用するか新しいポリシーを作成するかを選択できます。

  スナップショット ロック期間を含むバックアップ ポリシーを選択する場合は、 ONTAP 9.12.1 以降のバージョンを選択する必要があります。

- 互換性チェック

  リソース グループの作成時に、SnapCenterによって互換性チェックが実行されます。

  [互換性チェックのエラーの管理]

- リソース グループの二次保護を作成する

  セカンダリ保護は、リソース グループに追加されたリソースのレプリケーション関係の作成を担当します。プライマリから指定されたポリシーを使用して、優先クラスタと SVM にコンシステンシー グループベースのSnapMirror関係を作成する必要があります。セカンダリ保護は、 ASA r2 システム ベースのデータストアと仮想マシンでのみサポートされます。クラスタ ピアリングと SVM ピアリングを事前に構成する必要があります。セカンダリ保護では、非同期SnapMirrorポリシーのみが許可されます。セカンダリ保護を作成するときは、整合性グループのサフィックスを指定する必要があります。

セカンダリ保護は、リソース グループに追加されたリソースのレプリケーション関係の作成を担当します。

手順

1. SCV プラグインの左側のナビゲータ ペインで、リソース グループ を選択し、作成 を選択してウィザードを開始します。

リソース グループを作成するには、この方法が最も簡単です。ただし、次のいずれかを実行して、1つのリソースを含むリソース グループを作成することもできます。

- 1 つの VM のリソース グループを作成するには、ショートカット ページで [ホストとクラスター] を選択し、VM を右クリックして [SnapCenter Plug-in for VMware vSphere] > [リソース グループの作成] を選択します。
- 1 つのデータストアのリソース グループを作成するには、ショートカット ページで [ホストとクラスター] を選択し、データストアを右クリックして [SnapCenter Plug-in for VMware vSphere] > [リソース グループの作成] を選択します。

  a. ウィザードの*一般情報と通知*ページで、次の操作を行います。

フィールド	操作
vCenter Server	vCenterサーバを選択します。
Name	リソース グループの名前を入力します。VM、データストア、ポリシー、バックアップ、またはリソース グループの名前には、次の特殊文字を使用しないでください: % & * $ # @ ! \ / : * ? " < > - [縦棒] ; ' 、およびスペース。アンダースコア（_）は使用できます。特殊文字を含むVMまたはデータストアの名前は切り捨てられるため、特定のバックアップを検索することが難しくなります。リンク モードでは、vCenterごとに個別のSnapCenter Plug-in for VMware vSphereリポジトリがあります。そのため、複数のvCenterで重複する名前を使用できます。
説明	リソース グループの説明を入力します。

フィールド	操作
通知	このリソース グループの操作に関する通知をいつ受信するかを選択します: エラーまたは警告: エラーと警告のみ通知を送信します エラー: エラーのみ通知を送信します 常に: すべてのメッセージ タイプについて通知を送信します なし: 通知を送信しません
Email send from	通知の送信元とするEメール アドレスを入力します。
Email send to	通知の受信者のEメール アドレスを入力します。受信者が複数いる場合は、Eメール アドレスをカンマで区切ります。
Email subject	通知Eメールに使用する件名を入力します。
最新のスナップショット名	最新のスナップショットにサフィックス「_recent」を追加する場合は、このボックスをオンにします。 「_recent」サフィックスは日付とタイムスタンプを置き換えます。 あ `_recent`リソース グループに添付されているポリシーごとにバックアップが作成されます。したがって、複数のポリシーを持つリソースグループには複数の `_recent`バックアップ。手動で名前を変更しないでください `_recent`バックアップ。 ASA r2 ストレージ システムはスナップショットの名前変更をサポートしていないため、SCV の名前変更バックアップおよび _recent スナップショット命名機能はサポートされていません。

フィールド	操作
カスタムスナップショット形式	スナップショット名にカスタム形式を使用する場合は、このボックスをオンにして、名前の形式を入力します。 • デフォルトでは、この機能は無効になっています。 • デフォルトのスナップショット名は次の形式を使用します `<ResourceGroup>_<Date-TimeStamp>`ただし、変数 `$ResourceGroup`、`$Policy`、`$HostName`、`$ScheduleType`、および `$CustomText` を使用してカスタム形式を指定できます。カスタム名フィールドのドロップダウン リストを使用して、使用する変数とその使用順序を選択します。 `$CustomText`を選択した場合、名前の形式は `<CustomName>_<Date-TimeStamp>`。表示された追加ボックスにカスタム テキストを入力します。 [注意]: 「_recent」サフィックスも選択する場合は、カスタム スナップショット名がデータストア内で一意であることを確認する必要があります。そのため、名前に $ResourceGroup および $Policy 変数を追加する必要があります。 • 特殊文字 名前内の特殊文字については、「名前」フィールドと同じガイドラインに従ってください。

b. リソース ページで、次の操作を行います。

フィールド	操作
Scope	保護するリソースの種類を選択します: * データストア (指定された 1 つ以上のデータストア内のすべての従来の VM)。vVolデータストアは選択できません。 * 仮想マシン (個別の従来の VM または vVol VM。フィールドでは、VM または vVol VM を含むデータストアに移動する必要があります)。FlexGroupデータストア内の個々のVMは選択できません。 * タグ タグベースのデータストア保護は、NFS および VMFS データストア、仮想マシン、および vVol 仮想マシンに対してのみサポートされます。 * VM フォルダ (指定されたフォルダ内のすべての vVol VM。ポップアップ フィールドで、フォルダが配置されているデータセンターに移動する必要があります)
Datacenter	追加する VM、データストア、またはフォルダに移動します。リソース グループ内の VM およびデータストアの名前は一意である必要があります。

フィールド	操作
Available entities	保護するリソースを選択し、**>** を選択して、選択内容を [選択したエンティティ] リストに移動します。

*次へ*を選択すると、システムはまず、選択したリソースが配置されているストレージをSnapCenterが管理し、互換性があるかどうかを確認します。

メッセージが `Selected <resource-name> is not SnapCenter compatible`が表示される場合、選択したリソースはSnapCenterと互換性がありません。

1つ以上のデータストアをバックアップからグローバルに除外するには、データストア名を指定する必要があります。 `global.ds.exclusion.pattern`の財産 `scbr.override`設定ファイル。。 "上書き可能なプロパティ" 。

a. スパニング ディスク ページで、複数のデータストアにまたがる複数の VMDK を持つ VM のオプションを選択します。

   - Always exclude all spanning datastores（データストアの場合のデフォルト）
   - Always include all spanning datastores（VMの場合のデフォルト）
   - Manually select the spanning datastores to be included

     FlexGroupデータストアとvVolデータストアでは、スパニングVMはサポートされていません。

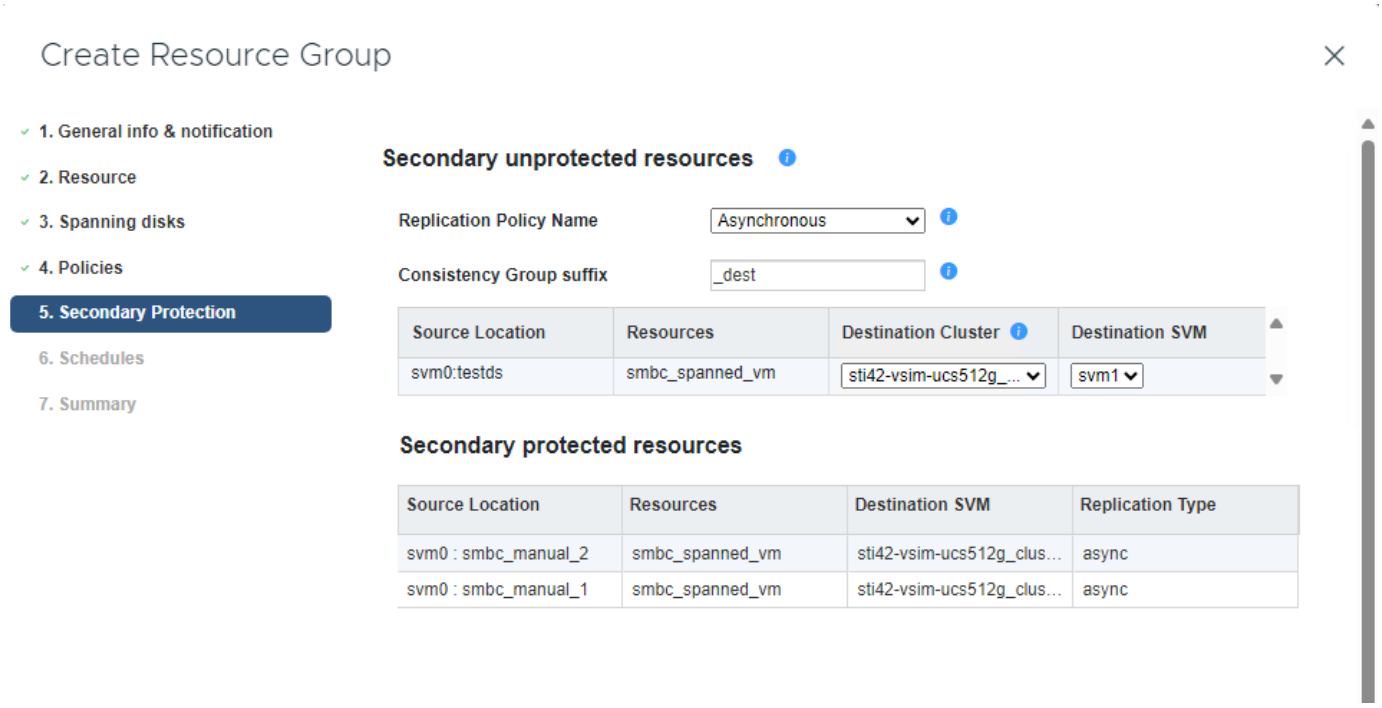
b. ポリシー ページで、次の表に示すように、1 つ以上のバックアップ ポリシーを選択または作成します。

使用するには...	操作
既存のポリシー	リストから1つ以上のポリシーを選択します。セカンダリ保護は、 SnapMirrorとSnapVault の両方の更新を選択した既存および新しいポリシーに適用できます。
新しいポリシー	i. *作成*を選択します。 ii. [New Backup Policy]ウィザードを完了して、[Create Resource Group]ウィザードに戻ります。

リンク モードでは、リンクされたすべてのvCenterにあるポリシーがリストに含まれます。リソース グループと同じvCenterにあるポリシーを選択する必要があります。

c. 二次保護 ページには、選択したリソースのリストとその保護ステータスが表示されます。保護されていないリソースを保護するには、ドロップダウンからレプリケーション ポリシー タイプ、整合性グループのサフィックス、宛先クラスタ、および宛先 SVM を選択します。リソース グループを作成すると、二次保護用の別のジョブが作成され、ジョブ モニター ウィンドウで確認できます。

フィールド	説明
レプリケーションポリシー名	SnapMirrorポリシーの名前。 *非同期*および*ミラーとボールト*セカンダリ ポリシーのみがサポートされます。
一貫性グループのサフィックス	プライマリ整合性グループに追加して宛先整合性グループ名を形成するために使用される宛先設定。たとえば、プライマリ コンシステンシー グループの名前が sccg_2024-11-28_120918 で、サフィックスとして _dest を入力すると、セカンダリ コンシステンシー グループは sccg_2024-11-28_120918_dest として作成されます。サフィックスは、保護されていない整合性グループにのみ適用されます。
デスティネーション クラスタ	保護されていないすべてのストレージ ユニットの場合、SCV はドロップダウンにピア クラスターの名前を表示します。 SCV に追加されたストレージが SVM スコープ内にある場合、 ONTAP の制限により、名前の代わりにクラスタ ID が表示されます。
デスティネーション SVM	保護されていないすべてのストレージ ユニットの場合、SCV はピア SVM の名前を表示します。整合性グループの一部であるストレージ ユニットの 1 つを選択すると、クラスタと SVM が自動的に選択されます。同じ一貫性グループ内の他のすべてのストレージ ユニットにも同じことが適用されます。
二次保護資源	リソース ページに追加されたリソースのすべての保護されたストレージ ユニットについて、クラスタ、SVM、レプリケーション タイプなどのセカンダリ関係の詳細が表示されます。



1. スケジュール ページで、選択したポリシーごとにバックアップ スケジュールを構成します。

開始時刻のフィールドに、ゼロ以外の日時を入力します。日付は次の形式でなければなりません `day/month/year`。

[Every]フィールドで日数を選択すると、その月の1日目にバックアップが実行され、それ以降は指定した間隔で実行されます。たとえば、*2 日ごと*オプションを選択した場合、開始日が偶数か奇数かに関係なく、月を通して 1 日目、3 日目、5 日目、7 日目などにバックアップが実行されます。

すべてのフィールドに情報を入力する必要があります。SnapCenter Plug-in for VMware vSphereでは、SnapCenter Plug-in for VMware vSphereが導入されているタイム ゾーンでスケジュールが作成されます。タイム ゾーンは、SnapCenter Plug-in for VMware vSphereのGUIを使用して変更できます。

"バックアップのタイムゾーンの変更" 。

2. 概要を確認して、[完了] を選択します。 SCV 6.1 以降では、 ASA r2 システムのリソースの二次保護が概要ページに表示されます。

   *[完了]*を選択する前に、ウィザードの任意のページに戻って情報を変更できます。

   *[完了]*を選択すると、新しいリソース グループがリソース グループ リストに追加されます。

   バックアップ内のいずれかのVMで休止処理が失敗すると、選択したポリシーでVM整合性が選択されていても、バックアップはVMと不整合とマークされます。この場合、一部のVMは正常に休止されている可能性があります。

互換性チェックのエラーの管理

リソース グループを作成しようとすると、SnapCenterによって互換性チェックが実行されます。常に参照 "NetApp Interoperability Matrix Tool（IMT）"SnapCenterサポートの最新情報については、こちらをご覧ください。互換性の問題が発生する理由は次のとおりです。

- 共有PCIデバイスがVMに接続されている
- SnapCenterで優先IPアドレスが設定されていない
- Storage VM（SVM）管理IPアドレスがSnapCenterに追加されていない
- Storage VMが停止している

互換性エラーを修正するには、次の手順を実行します。

1. Storage VMが実行されていることを確認します。
2. VMが配置されているストレージ システムがSnapCenter Plug-in for VMware vSphereインベントリに追加されていることを確認します。
3. Storage VMがSnapCenterに追加されていることを確認します。VMware vSphere ClientのGUIで、[Add storage system]オプションを使用します。
4. NetAppのデータストアとNetApp以外のデータストアの両方にVMDKがあるスパニングVMがある場合は、VMDKをNetAppのデータストアに移動します。

プリスクリプトとポストスクリプト

カスタムのプリスクリプトとポストスクリプトをデータ保護処理の一部として使用することができます。これらのスクリプトによって、データ保護ジョブの前後の処理を自動化できます。たとえば、データ保護ジョブのエラーや警告を自動的に通知するスクリプトを組み込むことができます。プリスクリプトとポストスクリプトを設定する前に、スクリプトを作成するための要件を理解しておく必要があります。

サポートされるスクリプト タイプ

Perlスクリプトとシェル スクリプトがサポートされています。シェルスクリプトは `!/bin/bash`。(`!/bin/sh` はサポートされていません。

スクリプト パスの場所

プリスクリプトとポストスクリプトは、SnapCenter Plug-in for VMware vSphereによって実行されます。そのため、スクリプトは実行ファイル権限を持つSnapCenter Plug-in for VMware vSphere OVAに配置されている必要があります。

例えば: * PERLスクリプトのパスは次のようになります `/support/support/script.pl`* シェルスクリプトのパスは次のようになります `/support/support/script.sh`

スクリプト パスは、スクリプトの実行時に検証されます。

スクリプトを指定する場所

スクリプトはバックアップ ポリシーに指定します。バックアップ ジョブが開始されると、ポリシーによってスクリプトがバックアップされるリソースに自動的に関連付けられます。

複数のスクリプトを指定するには、各スクリプト パスの後に **Enter** キーを押して、各スクリプトを別々の行にリストします。セミコロン（;）は使用できません。プリスクリプトとポストスクリプトをそれぞれ複数指定できます。1つのスクリプトをプリスクリプトとポストスクリプトの両方として作成し、そのスクリプトから他のスクリプトを呼び出すことができます。

スクリプトが実行されるタイミング

スクリプトは、BACKUP_PHASE に設定された値に従って実行されます。

- BACKUP_PHASE=PRE_BACKUP

  プレスクリプトは、操作の PRE_BACKUP フェーズで実行されます。

  > プリスクリプトが失敗しても、バックアップは正常に完了しますが、警告メッセージが送信されます。

- BACKUP_PHASE=POST_BACKUP または BACKUP_PHASE=FAILED_BACKUP

  ポストスクリプトは、バックアップが正常に完了した後の操作の POST_BACKUP フェーズで実行されるか、バックアップが正常に完了しなかった場合は FAILED_BACKUP フェーズで実行されます。

ポストスクリプトが失敗しても、バックアップは正常に完了しますが、警告メッセージが送信されます。

スクリプトの値が設定されていることを確認するには、次の点を確認してください。 * PERL スクリプトの場合: `/support/support/log_env.log` * シェルスクリプトの場合: `/support/support/log_file.log`

スクリプトに渡される環境変数

スクリプトで使用できる環境変数を次の表に示します。

環境変数	説明
`BACKUP_NAME`	バックアップの名前。ポストスクリプトでのみ渡される変数です。
`BACKUP_DATE`	バックアップの日付（形式： `yyyymmdd`変数はポストスクリプトでのみ渡されます。
`BACKUP_TIME`	バックアップの時刻（形式： `hhmmss`変数はポストスクリプトでのみ渡されます。
`BACKUP_PHASE`	スクリプトを実行するバックアップのフェーズ。有効な値は次のとおりです。 `PRE_BACKUP`, `POST_BACKUP`, and `FAILED_BACKUP` 。プリスクリプトとポストスクリプトで渡される変数です。
`STORAGE_SNAPSHOTS`	バックアップ内のストレージSnapshotの数。ポストスクリプトでのみ渡される変数です。
`STORAGE_SNAPSHOT.#`	定義されたストレージ スナップショットの 1 つ。形式は次のとおりです。 `<filer>:/vol/<volume>:<ONTAP-snapshot-name>`変数はポストスクリプトでのみ渡されます。
`VIRTUAL_MACHINES`	バックアップ内のVMの数。プリスクリプトとポストスクリプトで渡される変数です。
`VIRTUAL_MACHINE.#`	定義された仮想マシンの 1 つ。形式は次のとおりです。 `<VM name>[vertical bar]<VM UUID>[vertical bar]<power-state>[vertical bar]<VM snapshot>[vertical bar]<ip-addresses>` `<power-state>` has the values `POWERED_ON`, `POWERED_OFF`, or `SUSPENDED` `<VM snapshot>`価値観を持っている `true`または `false`プレスクリプトとポストスクリプトに渡される変数。

スクリプトのタイムアウト

バックアップ スクリプトのタイムアウトは15分です。この値は変更できません。

Perlスクリプトの例1

次のPerlスクリプトの例では、バックアップの実行時に環境変数が出力されます。

```
#!/usr/bin/perl
use warnings;
use strict;
my $argnum;
my $logfile = '/support/support/log_env.log';
open (FH, '>>', $logfile) or die $!;
foreach (sort keys %ENV) {
print FH "$_ = $ENV{$_}\n";
}
print FH "=========\n";
close (FH);
```

Perlスクリプトの例2

次の例では、バックアップに関する情報が出力されます。

```
#!/usr/bin/perl
use warnings;
use strict;

my $argnum;
my $logfile = '/support/support/log_env.log';
open (FH, '>>', $logfile) or die $!;

print FH "BACKUP_PHASE is $ENV{'BACKUP_PHASE'}\n";
print FH "Backup name $ENV{'BACKUP_NAME'}\n";
print FH "Virtual Machine $ENV{'VIRTUAL_MACHINES'}\n";
print FH "VIRTUAL_MACHINE # is $ENV{'VIRTUAL_MACHINE.1'}\n";
print FH "BACKUP_DATE is $ENV{'BACKUP_DATE'}\n";
print FH "BACKUP_TIME is $ENV{'BACKUP_TIME'}\n";
print FH "STORAGE_SNAPSHOTS is $ENV{'STORAGE_SNAPSHOTS'}\n";
print FH "STORAGE_SNAPSHOT # is $ENV{'STORAGE_SNAPSHOT.1'}\n";

print FH "PWD is $ENV{'PWD'}\n";
print FH "INVOCATION_ID is $ENV{'INVOCATION_ID'}\n";

print FH "=========\n";
close (FH);
```

シェル スクリプトの例

```
================================================
#!/bin/bash
echo Stage $BACKUP_NAME >> /support/support/log_file.log
env >> /support/support/log_file.log
================================================
```

リソース グループへの単一のVMまたはデータストアの追加

SnapCenter Plug-in for VMware vSphereで管理されている既存のリソース グループに、単一のVMまたはデータストアを簡単に追加することができます。

タスク概要

SANおよびNASデータストアは追加できますが、VSANまたはVVOLデータストアは追加できません。

手順

1. vSphere クライアント GUI で、ツールバーの メニュー を選択し、追加する VM またはデータストアに移動します。
2. 左側のナビゲータ ペインで、VM またはデータストアを右クリックし、セカンダリ ドロップダウン リストから * SnapCenter Plug-in for VMware vSphere* > * リソース グループに追加 * を選択します。

   システムはまず、選択した VM が配置されているストレージ システムをSnapCenterが管理し、互換性があることを確認し、次に [リソース グループに追加] ページを表示します。メッセージが `SnapCenter Compatibility Error`が表示される場合、選択した VM はSnapCenterと互換性がないため、まず適切なストレージ VM をSnapCenterに追加する必要があります。

3. リソース グループに追加 ページで、リソース グループを選択し、**OK** を選択します。

   [OK] を選択すると、システムはまず、選択した VM またはデータストアが配置されているストレージをSnapCenterが管理し、互換性があるかどうかを確認します。

   メッセージが `Selected <resource-name> is not SnapCenter compatible`が表示される場合、選択した VM またはデータストアはSnapCenterと互換性がありません。参照"互換性チェックのエラーの管理"詳細についてはこちらをご覧ください。

リソース グループへの複数のVMとデータストアの追加

SnapCenter VMware vSphere Clientの[Edit Resource Group]ウィザードを使用して、既存のリソース グループに複数のリソースを追加できます。

リソース グループには、次のいずれかを含めることができます。

- 従来のVM、SANデータストア、NASデータストアの任意の組み合わせ（vVolデータストアはサポートされていません）
- 1つのFlexGroupデータストア（スパニングVMはサポートされていません）
- 1つ以上のFlexVolデータストア（スパニングVMがサポートされています）
- 1台以上のvVol VM
- 指定したvSphereタグが設定されたすべてのvVol VM
- 指定したフォルダ内のすべてのvVol VM

> SnapCenterでバックアップされるのは、選択したプライマリvVolデータストア内のvVolのみであるため、複数のvVolデータストアにまたがるvVol VMはサポートされていません。

手順

1. SCVプラグインの左側のナビゲータペインで*リソースグループ*を選択し、リソースグループを選択して、✏ リソース グループの編集 をクリックしてウィザードを開始します。
2. リソース ページで、次の操作を行います。

   a. [Datastores]フィールドで、追加するVMまたはデータストアに移動します。

   b. [使用可能なエンティティ] リストで、リソース グループに追加する 1 つ以上の VM またはデータストアを選択し、[>] を選択して、選択内容を [選択したエンティティ] リストに移動します。利用可能なすべてのエンティティを移動するには、[] を選択します。

      デフォルトでは、[Available entities]リストにはデータセンター オブジェクトが表示されます。データストアを選択して、データストア内の VM を表示し、リソース グループに追加できます。

   [次へ] を選択すると、システムはまず、選択した VM またはデータストアが配置されているストレージをSnapCenterが管理し、互換性があるかどうかを確認します。メッセージが `Some entities are not SnapCenter compatible`が表示される場合、選択した VM またはデータストアはSnapCenterと互換性がありません。参照"互換性チェックのエラーの管理"詳細についてはこちらをご覧ください。

3. 追加するVMまたはデータストアごとに手順2を繰り返します。
4. 概要 ページに到達するまで [次へ] を選択し、概要を確認して [完了] を選択します。

名前が変更されたストレージのバックアップのリストア

ストレージの名前を変更すると、名前の変更前に作成されたバックアップを使用するワークフローが失敗します。REST APIからのみアクセスできるバックアップ名変更機能が導入され、ストレージ名の変更前に作成されたバックアップを使用できるようになりました。REST APIのワークフローと使用方法を以下に示します。

ⓘ ASA r2 ストレージ システムは、_recent スナップショット命名機能をサポートしていません。

手順

1. 新しいストレージ接続を追加または更新し、新しいクラスタ名またはSVM名がSCVに反映されるようにします。
2. KB 記事の説明に従って、サービスを再起動してキャッシュを更新します。 "「SCV backups fail after SVM rename」"
3. 新しいバックアップを作成します。
4. バックアップの詳細を使用して、古いストレージ名と新しいストレージ名を見つけます。
5. vSphere クライアントの バックアップ 画面で、バックアップを選択して詳細を表示します。
6. 次の URL から Swagger にアクセスします。 `https://<SCV-IP>:8144/api/swagger-ui/index.html`

   次のAPIを使用してストレージの名前を変更します。

   パッチ /4.1/ストレージシステム

   例: { "existingSVM": { "name": "string" }, "newSVM": { "name": "string" } }

応答：

{ "statusMessage": "OK", "statusCode": 200, "responseMessage": ["ストレージシステムの名前が正常に変更されました。"] }

このAPIを実行すると、古いバックアップからのリストア処理を含む、すべてのワークフローを実行できるようになります。

オンデマンドでのリソース グループのバックアップ

バックアップ処理は、リソース グループに定義されているすべてのリソースに対して実行されます。リソース グループにポリシーが適用され、かつスケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが行われます。

> ASA r2 バックアップは、整合性グループのスナップショットを作成し、指定されたリソースにプライマリ整合性グループがまだ存在しない場合はプライマリ整合性グループをプロビジョニングします。

開始する前に

ポリシーを適用したリソース グループを作成しておく必要があります。

> SnapCenter Plug-in for VMware vSphereのMySQLデータベースのバックアップ ジョブがすでに実行中の場合は、オンデマンド バックアップ ジョブを開始しないでください。メンテナンス コンソールを使用して、MySQLデータベースのバックアップ スケジュールを確認します。

タスク概要

以前のリリースのVirtual Storage Console（VSC）では、VMまたはデータストアのバックアップ ジョブが設定されていなくても、オンデマンド バックアップを実行できました。一方、SnapCenter Plug-in for VMware vSphereの場合、バックアップを実行するには、VMとデータストアがリソース グループに含まれている必要があります。

手順

1. SCVプラグインの左側のナビゲータペインで*リソースグループ*を選択し、リソースグループを選択して、*今すぐ実行*してバックアップを開始します。
2. リソース グループに複数のポリシーが設定されている場合は、[今すぐバックアップ] ダイアログ ボックスで、このバックアップ操作に使用するポリシーを選択します。
3. バックアップを開始するには、[**OK**] を選択します。
4. オプション: ウィンドウの下部にある 最近のタスク を選択するか、ダッシュボードの ジョブ モニター を選択して、操作の進行状況を監視し、詳細を確認します。 。結果

バックアップ内のいずれかのVMで休止処理が失敗すると、バックアップは警告付きで完了し、選択したポリシーでVM整合性が選択されていても、VMの不整合とマークされます。この場合、一部のVMは正常に休止されている可能性があります。ジョブ モニタには、障害が発生したVMの詳細に休止が失敗と表示されます。

SnapCenter Plug-in for VMware vSphereのMySQLデータベースのバックアップ

SnapCenter Plug-in for VMware vSphereには、プラグインで実行されるすべてのジョブのメタデータを格納するMySQLデータベース（NSMデータベースとも呼ばれます）が含まれています。このリポジトリを定期的にバックアップする必要があります。

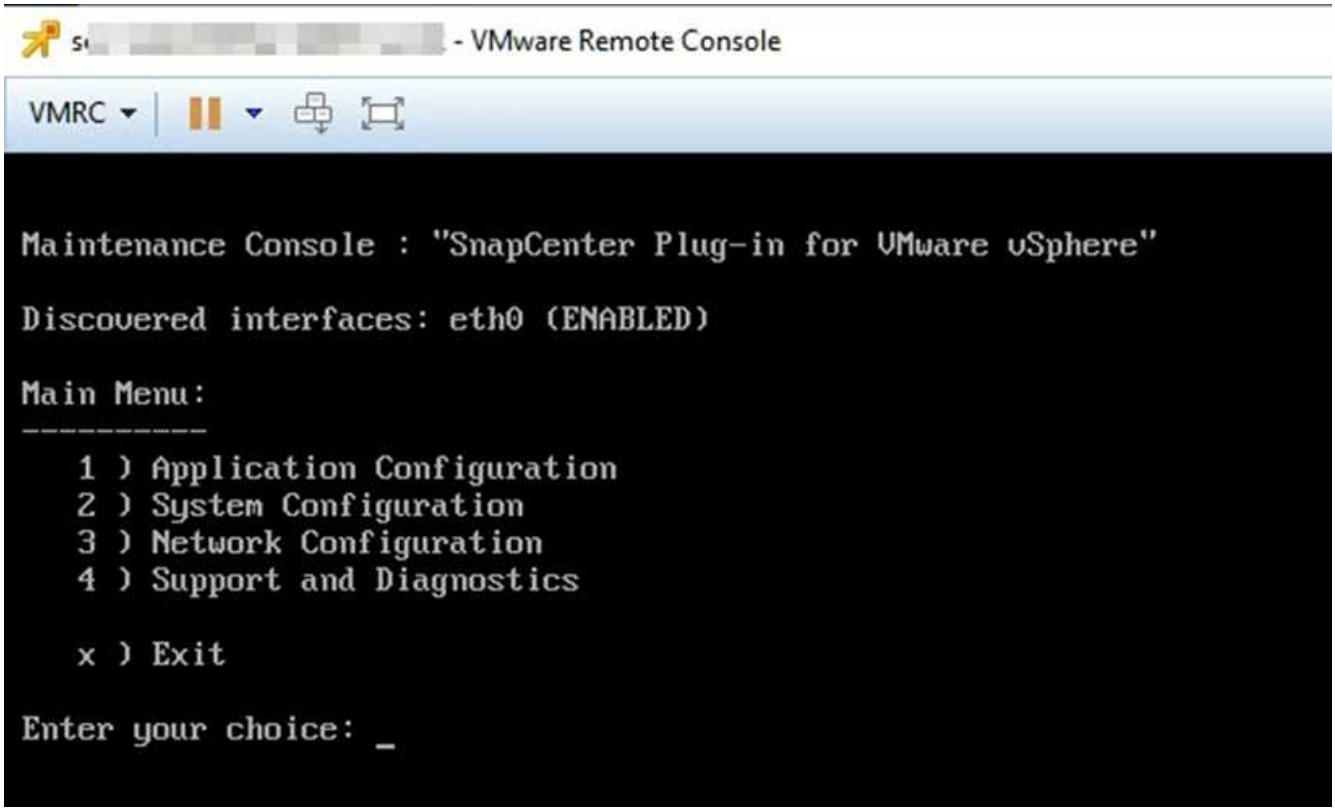
移行またはアップグレードを実行する前にも、リポジトリをバックアップします。

開始する前に

オンデマンド バックアップ ジョブがすでに実行中の場合は、MySQLデータベースのバックアップ ジョブを開始しないでください。

手順

1. VMware vSphere Clientで、SnapCenter Plug-in for VMware vSphereが配置されているVMを選択します。
2. 仮想アプライアンスの 概要 タブで、リモート コンソールの起動 または **Web** コンソールの起動 を選択して、メンテナンス コンソール ウィンドウを開きます。



3. メインメニューからオプション*1) アプリケーション構成*を入力します。
4. アプリケーション構成メニューから、オプション*6) MySQLのバックアップと復元*を入力します。
5. MySQL バックアップおよび復元構成メニューから、オプション **1) MySQL** バックアップの構成 を入力します。
6. プロンプトで、リポジトリのバックアップの場所、保持するバックアップの数、およびバックアップの開始時刻を入力します。

これらを入力すると、すべての入力内容が保存されます。バックアップの保持数に達すると、新しいバックアップの実行時に古いバックアップが削除されます。

> リポジトリのバックアップの名前は「backup-<date>」になります。リポジトリのリストア機能で「backup」プレフィックスが検索されるため、これを変更しないでください。

リソース グループの管理

バックアップ リソース グループを作成、変更、削除し、リソース グループに対してバックアップ処理を実行することができます。

> Virtual Storage Console（VSC）では、リソース グループはバックアップ ジョブと呼ばれます。

リソース グループに対する処理の一時停止と再開

スケジュールされた処理を一時的に無効にして、リソース グループで開始されないように設定できます。無効にした処理は、必要に応じてあとから有効にすることができます。

手順

1. SCV プラグインの左側のナビゲータ ペインで、リソース グループ を選択し、リソース グループを選択して、一時停止 (または 再開) を選択します。
2. 確認ボックスで「**OK**」を選択して確定します。

終了後の操作

リソースグループページでは、中断されたリソースのジョブステータスは `Under_Maintenance`。[Job Status]列が表示されない場合は、表を右にスクロールしてください。

バックアップ操作が再開されると、ジョブステータスは次のように変わります。 `Production` 。

リソース グループの変更

vCenterでのリソース グループ内のリソースの削除または追加、ポリシーの適用解除または適用、スケジュールの変更、その他のリソース グループ オプションの変更を行うことができます。

タスク概要

リソース グループの名前を変更する場合は、VM、データストア、ポリシー、バックアップ、またはリソース グループの名前に次の特殊文字を使用しないでください。

% & * $ # @ ! \ / : * ? " < > - | ; ' 、およびスペース。アンダースコア（_）は使用できます。

手順

1. SCV プラグインの左側のナビゲータ ペインで、リソース グループ を選択し、リソース グループを選択して、編集 を選択します。
2. リソース グループの編集 ウィザードの左側のリストで、変更するカテゴリを選択し、変更を入力します。

複数のカテゴリに変更を加えることができます。このオプションでは、二次的に保護されたリソースを編集することもできます。

3. 概要ページが表示されるまで [次へ] を選択し、[完了] を選択します。

リソース グループの削除

リソース グループ内のリソースを保護する必要がなくなった場合は、vCenterでリソース グループを削除できます。vCenterからSnapCenter Plug-in for VMware vSphereを削除する前に、すべてのリソース グループが削除されていることを確認する必要があります。

タスク概要

リソース グループの削除処理は、すべて強制削除として実行されます。削除操作では、vCenter リソース グループからすべてのポリシーがデタッチされ、 SnapCenter Plug-in for VMware vSphereからリソース グループが削除され、リソース グループのすべてのバックアップとスナップショットが削除されます。

> SnapVault関係では、最後のスナップショットを削除できないため、リソース グループを削除できません。 SnapVault関係の一部であるリソース グループを削除する前に、System Manager またはONTAP CLI を使用してSnapVault関係を削除し、最後のスナップショットを削除する必要があります。

手順

1. SCV プラグインの左側のナビゲータ ペインで、リソース グループ を選択し、リソース グループを選択して、削除 を選択します。
2. リソース グループの削除 確認ボックスで、**OK** を選択して確認します。

ポリシーの管理

SnapCenter Plug-in for VMware vSphereのバックアップ ポリシーを作成、変更、表示、適用解除、および削除できます。データ保護処理を実行するにはポリシーが必要です。

ポリシーの適用解除

リソースのデータ保護を管理するポリシーが不要になった場合は、SnapCenter Plug-in for VMware vSphereのリソース グループからポリシーの適用を解除できます。ポリシーを削除する場合や実行頻度を変更する場合は、事前にポリシーの適用を解除する必要があります。

タスク概要

SnapCenter Plug-in for VMware vSphereのリソース グループからポリシーの適用を解除する際のガイドラインは、SnapCenterのリソース グループのガイドラインとは異なります。VMware vSphere Clientリソース グループの場合、すべてのポリシーの適用を解除できるため、リソース グループにポリシーが適用されていない状態になります。ただし、そのリソース グループに対してデータ保護処理を実行するには、少なくとも1つのポリシーを適用する必要があります。

手順

1. SCV プラグインの左側のナビゲータ ペインで、リソース グループ を選択し、リソース グループを選択して、編集 を選択します。
2. リソース グループの編集 ウィザードの ポリシー ページで、デタッチするポリシーの横にあるチェック

マークをオフにします。

ポリシーのチェック マークをオンにすると、ポリシーがリソース グループに追加されます。

3. ウィザードの残りの部分でリソース グループに追加の変更を加え、[完了] を選択します。

ポリシーの変更

SnapCenter Plug-in for VMware vSphereのリソース グループのポリシーを変更できます。ポリシーがリソース グループにアタッチされている間に、頻度、レプリケーション オプション、スナップショットの保持設定、またはスクリプト情報を変更できます。

タスク概要

SnapCenter Plug-in for VMware vSphereのバックアップ ポリシーの変更は、SnapCenterアプリケーションベースのプラグインのバックアップ ポリシーの変更とは異なります。プラグインのポリシーを変更する際に、リソース グループからポリシーの適用を解除する必要はありません。

レプリケーションまたは保持の設定を変更する前に、その影響を考慮する必要があります。

- レプリケーションまたは保持の設定を引き上げる場合

  新しい設定に達するまでバックアップが蓄積され続けます。

- レプリケーションまたは保持の設定を引き下げる場合

  新しい設定を超過したバックアップは、次のバックアップの実行時に削除されます。

> SnapCenter Plug-in for VMware vSphereのポリシー スケジュールを変更するには、プラグインのリソース グループでスケジュールを変更する必要があります。

手順

1. SCV プラグインの左側のナビゲータ ペインで、ポリシー を選択し、ポリシーを選択して 編集 を選択します。
2. ポリシーのフィールドを変更します。
3. 完了したら、[更新] を選択します。

変更は、スケジュールされたバックアップが次回実行されるときに有効になります。

ポリシーの削除

SnapCenter Plug-in for VMware vSphereの設定済みのバックアップ ポリシーが不要になった場合は、そのポリシーを削除できます。

開始する前に

ポリシーを削除するには、SnapCenterの仮想アプライアンス内のすべてのリソース グループからポリシーの適用を解除しておく必要があります。

手順

1. SCV プラグインの左側のナビゲータ ペインで、ポリシー を選択し、ポリシーを選択して 削除 を選択し

ます。

2. 確認ダイアログボックスで*OK*を選択します。

バックアップの管理

SnapCenter Plug-in for VMware vSphereで実行されたバックアップの名前変更および削除を行うことができます。複数のバックアップを同時に削除することもできます。

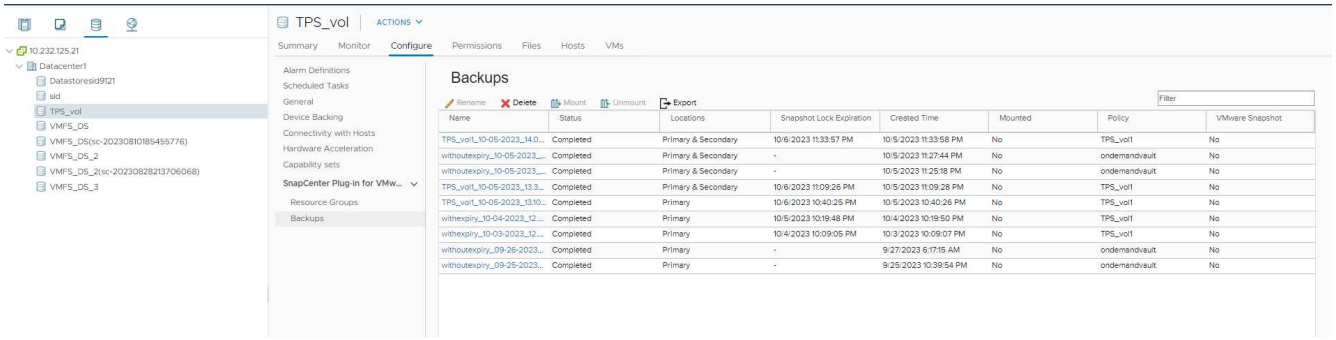
バックアップの名前の変更

SnapCenter Plug-in for VMware vSphereのバックアップの検索性を高めるために、バックアップの名前を変更できます。

> ASA r2 ストレージ システムは、バックアップの名前変更をサポートしていません。

手順

1. メニュー を選択し、ホストとクラスター メニュー オプションを選択して、VM を選択し、構成 タブを選択して、* SnapCenter Plug-in for VMware vSphere* セクションで バックアップ を選択します。



2. [構成] タブでバックアップを選択し、[名前の変更] を選択します。
3. バックアップの名前変更 ダイアログボックスで新しい名前を入力し、**OK** を選択します。

   VM、データストア、ポリシー、バックアップ、またはリソース グループの名前には、次の特殊文字を使用しないでください: & * $ # @ ! \ / : * ? " < > - | ; ' 、およびスペース。アンダースコア（_）は使用できます。

バックアップの削除

SnapCenter Plug-in for VMware vSphereのバックアップが他のデータ保護処理で不要になった場合、そのバックアップを削除できます。1つのバックアップを削除することも、複数のバックアップを同時に削除することもできます。

開始する前に

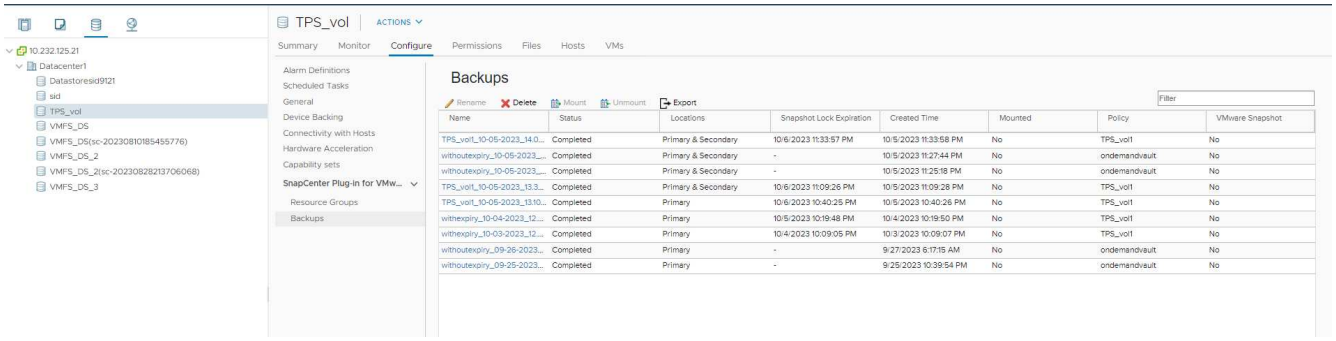
マウントされているバックアップは削除できません。バックアップを削除するには、事前にアンマウントする必要があります。

タスク概要

セカンダリ ストレージ上のスナップショットは、 SnapCenter Plug-in for VMware vSphereではなく、

ONTAP保持設定によって管理されます。したがって、 SnapCenter Plug-in for VMware vSphereを使用してバックアップを削除すると、プライマリ ストレージ上のスナップショットは削除されますが、セカンダリ ストレージ上のスナップショットは削除されません。セカンダリ ストレージにスナップショットがまだ存在する場合、 SnapCenter Plug-in for VMware vSphereは、復元要求をサポートするためにバックアップに関連付けられたメタデータを保持します。 ONTAP保持プロセスによってセカンダリ スナップショットが削除されると、 SnapCenter Plug-in for VMware vSphere は、定期的に実行されるパージ ジョブを使用してメタデータを削除します。

1. メニュー を選択し、ホストとクラスター メニュー オプションを選択して、VM を選択し、構成 タブを選択して、* SnapCenter Plug-in for VMware vSphere* セクションで バックアップ を選択します。



2. 1 つまたは複数のバックアップを選択し、[削除] を選択します。

   削除するバックアップは最大40個まで選択できます。

3. 削除操作を確認するには、[**OK**] を選択します。
4. 左側の vSphere メニュー バーにある更新アイコンを選択して、バックアップ リストを更新します。

データストアのマウントとアンマウント

バックアップのマウント

バックアップ内のファイルにアクセスする必要がある場合は、バックアップから従来のデータストアをマウントできます。バックアップは、バックアップが作成されたESXiホストにも、同じタイプのVMおよびホスト構成を使用する代替ESXiホストにもマウントできます。同じデータストアを1つのホストに複数回マウントできます。

vVolデータストアはマウントできません。

開始する前に

- 代替ESXiホストがストレージに接続できることを確認する

  代替ESXiホストにマウントする場合は、その代替ESXiホストがストレージに接続できること、および次の要件を満たしていることを確認する必要があります。

  - UIDとGIDが元のホストと同じである
  - SnapCenter Plug-in for VMware vSphere仮想アプライアンスのバージョンが元のホストと同じである
- iSCSIプロトコルを使用する場合は、ストレージ システムのイニシエータがESXiホストにマッピングされていることを確認します。NVMeプロトコルを使用する場合は、コントローラを追加して必要なサブシステムをESXiホストにマッピングします。
- 古いLUN / ネームスペースをクリーンアップする

  ESXiホストで検出できる一意のLUN / ネームスペースはデータストアごとに1つだけであるため、複数のLUN / ネームスペースが検出された場合は処理が失敗します。これは、前のマウント処理が完了する前にマウント処理を開始した場合、LUN / ネームスペースを手動でクローニングした場合、またはアンマウント処理中にストレージからクローンが削除されなかった場合に発生する可能性があります。複数のクローンが検出されないようにするには、ストレージ上の古いLUN / ネームスペースをすべてクリーンアップする必要があります。

タスク概要

データストアが配置されているFabricPoolのストレージ階層が使用できない場合、マウント処理が失敗することがあります。

手順

1. VMware vSphere クライアントのショートカット ページで、ストレージ を選択します。
2. データストアを右クリックし、* SnapCenter Plug-in for VMware vSphere* > * バックアップのマウント * を選択します。
3. *データストアのマウント*ページで、バックアップとバックアップの場所 (プライマリまたはセカンダリ) を選択し、*完了*を選択します。
4. オプション: データストアがマウントされていることを確認するには、次の手順を実行します。
   a. ツールバーの*メニュー*を選択し、ドロップダウンリストから*ストレージ*を選択します。
   b. 左側のナビゲーション ペインで、マウントしたデータストアがリストの最上位に表示されます。

ボリュームのクローンを作成するときに新しいスナップショットが作成されないようにするには、SnapVaultボリュームのONTAPスケジュールをオフにします。以前存在していたスナップショットは削除されません。

バックアップのアンマウント

データストア内のファイルにアクセスする必要がなくなった場合は、バックアップをアンマウントできます。

VMware vSphereクライアントGUIにバックアップがマウント済みとして表示されているが、バックアップのアンマウント画面に表示されない場合は、REST APIを使用する必要があります。 `/backup/{backup-Id}/cleanup`範囲外のデータストアをクリーンアップしてから、マウント解除手順を再度試してください。

負荷共有ミラー関係にあるルートボリュームを持つストレージVM（SVM）にNFSデータストアのバックアップコピーをマウントしようとすると、次のエラーが発生する可能性があります。 `You may have reached the maximum number of NFS volumes configured in the vCenter. Check the vSphere Client for any error messages.`この問題を回避するには、**ESX** > 管理 > 設定 > 詳細システム設定 に移動して NFS.MaxVolumes 値を変更し、最大ボリューム設定を変更します。最大値は256です。

手順

1. VMware vSphere クライアントのショートカット ページで、ストレージ を選択します。
2. 左側のナビゲータ ペインでデータストアを右クリックし、ドロップダウン リストで * SnapCenter Plug-in for VMware vSphere* を選択し、セカンダリ ドロップダウン リストで * アンマウント* を選択します。

   アンマウントするデータストアを間違えないようにしてください。間違えると、本番環境に影響が生じるおそれがあります。

3. クローン データストアのアンマウント ダイアログ ボックスで、データストアを選択し、クローン データストアのアンマウント チェックボックスをオンにして、アンマウント を選択します。

バックアップのリストア

リストアの概要

プライマリ バックアップまたはセカンダリ バックアップからVM、VMDK、ファイル、フォルダをリストアできます。

- VMのリストア先

  従来のVMをリストアできる先は、元のホスト、同じvCenter Server内の別のホスト、同じvCenterまたはリンクモードの任意のvCenterで管理される別のESXiホストです。

  vVol VMは元のホストにリストアできます。

- VMDKのリストア先

  従来のVMのVMDKは、元のデータストアまたは別のデータストアにリストアできます。

  vVol VMのVMDKは元のデータストアにリストアできます。

ゲスト ファイル リストア セッションで、個々のファイルやフォルダをリストアすることもできます。このセッションでは、仮想ディスクのバックアップ コピーを接続し、選択したファイルやフォルダをリストアします。

以下のものはリストアできません。

- データストア

  SnapCenter Plug-in for VMware vSphereを使用してデータストアをリストアすることはできません。リストアできるのは、データストア内の個々のVMのみです。

- 削除されたVMのバックアップ

  削除されたStorage VMのバックアップはリストアできません。たとえば、管理LIFを使用してStorage VMを追加したあとにバックアップを作成するとします。その後、そのStorage VMを削除してそのStorage VMを含むクラスタを追加すると、バックアップのリストア処理が失敗します。

リストア処理の実行方法

VMFS環境の場合、SnapCenter Plug-in for VMware vSphereは、クローニングとマウントの処理およびStorage vMotionを使用してリストア処理を実行します。NFS環境では、ネイティブのONTAP Single File SnapRestore（SFSR）を使用し、ほとんどのリストア処理をより効率的に実行します。vVol VM の場合、プラグインは復元操作にONTAP単一ファイル スナップショット復元 (ONTAP SFSR) とSnapMirror復元を使用します。次の表に、リストア処理の実行方法を示します。

復元操作	から	使用方法
VMとVMDK	プライマリ バックアップ	NFS環境: ONTAP Single File SnapRestore VMFS環境: Storage VMotionによるクローン作成とマウント
VMとVMDK	セカンダリ バックアップ	NFS環境: ONTAP Single File SnapRestore VMFS環境: Storage VMotionによるクローン作成とマウント
削除したVMとVMDK	プライマリ バックアップ	NFS環境: ONTAP Single File SnapRestore VMFS環境: Storage VMotionによるクローン作成とマウント
削除したVMとVMDK	セカンダリ バックアップ	NFS 環境: Storage VMotion を使用したクローン作成とマウント VMFS 環境: Storage VMotion を使用したクローン作成とマウント
VMとVMDK	VM整合性のあるプライマリ バックアップ	NFS環境: ONTAP Single File SnapRestore VMFS環境: Storage VMotionによるクローン作成とマウント
VMとVMDK	VM整合性のあるセカンダリ バックアップ	NFS環境: ONTAP SnapMirror Restore VMFS環境: Storage VMotionによるクローン作成とマウント
vVol VM	クラッシュ整合性のあるプライマリ バックアップ	すべてのプロトコルに対してONTAP Single File SnapRestore
vVol VM	クラッシュ整合性のあるセカンダリ バックアップ	すべてのプロトコルに対してONTAP SnapMirrorリストア
FlexGroup VM	プライマリ バックアップ	NFS 環境: * ONTAPバージョン 9.10.1 以降を使用している場合は、 ONTAP Single File SnapRestore を使用します。 * ONTAPの以前のバージョンでは、Storage VMotion を使用してクローンを作成し、マウントします。 VMFS環境: FlexGroupsではサポートされません

復元操作	から	使用方法
FlexGroup VM	セカンダリ バックアップ	NFS環境： • ONTAPバージョン 9.10.1 以降を使用している場合は、ONTAP SnapMirror復元 • それより前のONTAPバージョンの場合、クローニングとマウントおよびStorage vMotion VMFS環境: FlexGroupsではサポートされません

vVolコンテナのリバランシング後にvVol VMをリストアすることはできません。

ゲスト ファイルのリストア処理は、NFS環境とVMFS環境の両方で、（Storage vMotionを使わない）クローニングおよびマウント処理を使用して実行されます。

復元操作中に、次のエラーが発生する場合があります。 `Host unresolved volumes is null`または `Exception while calling pre-restore on SCV….Error mounting cloned LUN as datastore…`これは、SnapCenter Plug-in for VMware vSphereがクローンの再署名を試行したときに発生します。VMwareの制限により、SnapCenter Plug-in for VMware vSphereでESXiホストの詳細設定の自動再署名の値を制御できません。 NVMe over TCP および NVMe over FC ストレージの場合、新しいサブシステムが追加されても、SCV はコントローラーを動的に追加できません。マウント処理の前に、必要なマッピングを作成しておいてください。

参照 "KB記事: SCVクローンまたは復元が「ホストの未解決ボリュームがnullです」というエラーで失敗する" エラーの詳細については、こちらをご覧ください。

バックアップの検索

[Restore]ウィザードを使用して、VMまたはデータストアの特定のバックアップを検索できます。バックアップが見つかったら、リストアできます。

手順

1. VMware vSphere クライアント GUI で、ツールバーの メニュー を選択し、次のいずれかを実行します。

バックアップを表示するには...	操作
VM	ホストとクラスター メニュー オプションを選択し、VM を選択して、構成 タブを選択し、* SnapCenter Plug-in for VMware vSphereセクション* で バックアップ を選択します。
データストア	ストレージ メニュー オプションを選択し、データストアを選択して、構成 タブを選択し、* SnapCenter Plug-in for VMware vSphere* セクションで バックアップ を選択します。

2. 左側のナビゲータ ペインで、VMまたはデータストアを含むデータセンターを展開します。
3. オプション: VM またはデータストアを右クリックし、ドロップダウン リストで * SnapCenter Plug-in for VMware vSphere* を選択し、セカンダリ ドロップダウン リストで * 復元 * を選択します。
4. *復元*ウィザードで検索名を入力し、*検索*を選択します。

   フィルター アイコンを選択し、日付と時刻の範囲、VMware スナップショットを含むバックアップが必要かどうか、マウントされたバックアップが必要かどうか、および場所を選択することで、バックアップ リストをフィルターできます。「OK」を選択します。

バックアップからのVMのリストア

VMをリストアするときに、選択したバックアップ コピーで既存の内容を上書きするか、VMのコピーを作成できます。

VMは次の場所にリストアできます。

- 元の場所へのリストア
  - 元のESXiホストにマウントされている元のデータストア（元のVMは上書きされます）
- 別の場所へのリストア
  - 元のESXiホストにマウントされている別のデータストア
  - 同じvCenterで管理されている別のESXiホストにマウントされている元のデータストア
  - 同じvCenterで管理されている別のESXiホストにマウントされている別のデータストア
  - リンク モードの別のvCenterで管理されている別のESXiホストにマウントされている別のデータストア

vVol VMを別のホストにリストアすることはできません。

次の復元ワークフローはサポートされていません: ストレージ VM を追加し、その VM のバックアップを実行し、ストレージ VM を削除して同じストレージ VM を含むクラスターを追加し、元のバックアップの復元を試みます。

NFS環境でのリストア処理のパフォーマンスを向上させるには、VMwareアプリケーションのvStorage API for Array Integration（VAAI）を有効にします。

開始する前に

- バックアップが存在している必要があります。

  VMをリストアするには、SnapCenter Plug-in for VMware vSphereを使用してVMのバックアップを作成しておく必要があります。

  SnapCenter Plug-in for VMware vSphere以外のソフトウェアによって実行された VM のスナップショットがある場合、復元操作は正常に完了しません。

- デスティネーション データストアの準備が完了している必要があります。

- リストア処理のデスティネーション データストアには、すべてのVMファイル（vmdk、vmx、vmsdなど）のコピーを格納できるだけの十分なスペースが必要です。
- デスティネーション データストアに、以前のリストア処理の失敗で発生した古いVMファイルが含まれていてはなりません。古いファイルの名前の形式は次のようになります `restore_xxx_xxxxxx_<filename>`。

- 転送中のVMはリストアできません。

  リストアするVMがvMotionまたはStorage vMotionの状態であってはいけません。

- HA構成エラー

  バックアップを別の場所にリストアする前に、[vCenter ESXi Host Summary]画面にHA構成エラーが表示されていないことを確認してください。

- 別の場所へのリストア
  - 別の場所にリストアする場合は、リストア処理のデスティネーションであるvCenterでSnapCenter Plug-in for VMware vSphereが実行されている必要があります。デスティネーション データストアに十分なスペースが必要です。
  - [Restore To alternate Location]フィールドのデスティネーションvCenterをDNSで解決できる必要があります。

タスク概要

- VMの登録が解除され、再登録される

  VM の復元操作では、元の VM を登録解除し、バックアップ スナップショットから VM を復元し、復元された VM を同じ名前と構成で同じ ESXi サーバーに登録します。リストア後に、VMをリソース グループに手動で追加する必要があります。

- データストアのリストア

  データストアはリストアできませんが、データストア内のVMはリストアできます。

- vVol VMのリストア
  - 複数のVMにまたがるvVolデータストアはサポートされていません。複数のVMにまたがるvVolデータストア内の接続されたVMDKはバックアップされないため、リストア後のVMには一部のVMDKしか含まれません。
  - vVolを別のホストにリストアすることはできません。
  - vVolの自動リバランシングはサポートされていません。
- VMのVMware整合性スナップショットに失敗した場合

  VMのVMware整合性スナップショットの作成に失敗した場合でも、VMはバックアップされます。バックアップ コピーに格納されたエンティティは、リストア ウィザードで表示し、リストア処理に使用できます。

- VMが配置されているFabricPoolのストレージ階層が使用できない場合、リストア処理が失敗することがあります。

手順

1. VMware vSphere クライアント GUI で、ツールバーの メニュー を選択し、ドロップダウン リストから **VM** とテンプレート を選択します。

> 削除されたVMを復元する場合は、 SnapCenter Plug-in for VMware vSphereに追加されたストレージVMの資格情報が必要です。 `vsadmin`または、 `vsadmin` 。

2. 左側のナビゲータ ペインで VM を右クリックし、ドロップダウン リストで * SnapCenter Plug-in for VMware vSphere* を選択し、セカンダリ ドロップダウン リストで * 復元 * を選択してウィザードを起動します。
3. *復元*ウィザードの*バックアップの選択*ページで、復元するバックアップ スナップショットを選択します。

   特定のバックアップ名または部分的なバックアップ名を検索することも、フィルタ アイコンを選択して日付と時刻の範囲を選択し、VMware スナップショットを含むバックアップが必要かどうか、マウントされたバックアップが必要かどうか、および場所を選択して、バックアップ リストをフィルタすることもできます。 [OK] を選択してウィザードに戻ります。

4. *範囲の選択*ページで、*復元範囲*フィールドで*仮想マシン全体*を選択し、復元場所を選択して、バックアップをマウントする宛先情報を入力します。

   *VM名*フィールドに同じVM名が存在する場合、新しいVM名の形式は次のようになります。 `<vm_name>_<timestamp>` 。

   部分的なバックアップを復元する場合、復元操作では*範囲の選択*ページがスキップされます。

5. *場所の選択*ページで、復元されたデータストアの場所を選択します。

   SnapCenter Plug-in for VMware vSphere 4.5以降では、FlexGroupボリューム用のセカンダリ ストレージを選択できます。

6. 概要ページを確認し、[完了] を選択します。
7. オプション: 画面下部の*最近のタスク*を選択して、操作の進行状況を監視します。

   最新の情報を表示するには画面を更新します。

終了後の操作

- IPアドレスの変更

  別の場所にリストアした場合は、静的IPアドレスが設定されている場合にIPアドレスが競合しないように、新しく作成したVMのIPアドレスを変更する必要があります。

- リソース グループへのリストアしたVMの追加

  VMは、リストアされても、以前のリソース グループに自動的に追加されることはありません。そのため、リストアしたVMを適切なリソース グループに手動で追加する必要があります。

削除された**VM**のバックアップからのリストア

削除したVMは、データストアのプライマリ バックアップまたはセカンダリ バックアッ

プから選択したESXiホストにリストアできます。

VMは次の場所にリストアできます。

- 元の場所へのリストア
  - 元のESXiホストにマウントされている元のデータストア（VMのコピーが作成されます）
- 別の場所へのリストア
  - 元のESXiホストにマウントされている別のデータストア
  - 同じvCenterで管理されている別のESXiホストにマウントされている元のデータストア
  - 同じvCenterで管理されている別のESXiホストにマウントされている別のデータストア
  - リンク モードの別のvCenterで管理されている別のESXiホストにマウントされている別のデータストア

別の場所にリストアする場合は、リストア処理のデスティネーションであるリンクされたvCenterでSnapCenter Plug-in for VMware vSphereが実行されている必要があります。デスティネーション データストアに十分なスペースが必要です。

vVol VMを別の場所にリストアすることはできません。

削除されたVMをリストアする場合、そのVMに元々割り当てられていたタグやフォルダはリストアされません。

開始する前に

- VMware vSphereクライアントのストレージシステムページで、ストレージシステムのユーザーアカウントには、"ONTAPに必要な最小限のONTAP権限" 。
- vCenterのユーザーアカウントには、"SnapCenter Plug-in for VMware vSphereに必要な最小限の vCenter権限" 。
- バックアップが存在している必要があります。

  VMにVMDKをリストアするには、SnapCenter Plug-in for VMware vSphereを使用してVMのバックアップを作成しておく必要があります。

NFS環境でのリストア処理のパフォーマンスを向上させるには、VMwareアプリケーションのvStorage API for Array Integration（VAAI）を有効にします。

タスク概要

データストアはリストアできませんが、データストア内のVMはリストアできます。

VMが配置されているFabricPoolのストレージ階層が使用できない場合、リストア処理が失敗することがあります。

手順

1. vCenter Server で、インベントリ > データストア に移動し、データストアを選択します。
2. SnapCenter Plug-in for VMware vSphereセクションで、[構成] > [バックアップ] を選択します。

3. バックアップをダブルクリックすると、バックアップに含まれるすべてのVMのリストが表示されます。
4. バックアップ リストから削除された VM を選択し、[復元] を選択します。
5. *復元*ウィザードの*バックアップの選択*ページで、復元するバックアップ コピーを選択します。

   特定のバックアップ名または部分的なバックアップ名を検索することも、フィルタ アイコンを選択して日付と時刻の範囲を選択し、VMware スナップショットを含むバックアップが必要かどうか、マウントされたバックアップが必要かどうか、および場所を選択して、バックアップ リストをフィルタすることもできます。 [OK] を選択してウィザードに戻ります。

6. *範囲の選択*ページで、*復元範囲*フィールドで*仮想マシン全体*を選択し、復元場所を選択して、バックアップをマウントする宛先ESXiホスト情報を入力します。

   リストア先は、SnapCenterに追加されている任意のESXiホストにすることができます。このオプションは、指定された日時のスナップショットから、VM が存在していた選択したバックアップの内容を復元します。このオプションを選択すると、**VM** を再起動 チェックボックスがオンになり、VM の電源がオンになります。

   NFSデータストア内のVMをESXiクラスタ内の別のESXiホストにリストアすると、リストア後、そのVMが代替ホストに登録されます。

7. *場所の選択*ページで、復元するバックアップの場所（プライマリまたはセカンダリ）を選択します。
8. 概要ページを確認し、[完了] を選択します。

バックアップからの**VMDK**のリストア

従来のVMまたはvVol VMのプライマリ バックアップまたはセカンダリ バックアップから、既存のVMDKのほか、削除や切断したVMDKをリストアできます。

VM上の1つ以上の仮想マシン ディスク（VMDK）を同じデータストアにリストアできます。

> NFS環境でのリストア処理のパフォーマンスを向上させるには、VMwareアプリケーションのvStorage API for Array Integration（VAAI）を有効にします。

開始する前に

- バックアップが存在している必要があります。

  SnapCenter Plug-in for VMware vSphereを使用してVMのバックアップを作成しておく必要があります。

- 転送中のVMはリストアできません。

  リストアするVMがvMotionまたはStorage vMotionの状態であってはいけません。

タスク概要

- VMDKがVMから削除されているか切断されている場合、リストア処理によってVMDKがVMに接続されます。
- VMが配置されているFabricPoolのストレージ階層が使用できない場合、リストア処理が失敗することがあります。

- 接続処理とリストア処理では、デフォルトのSCSIコントローラを使用してVMDKが接続されます。ただし、NVMeディスクを使用してVMに接続されたVMDKがバックアップされる際、接続処理とリストア処理では、利用可能な場合はNVMeコントローラが使用されます。

手順

1. VMware vSphere クライアント GUI で、ツールバーの メニュー を選択し、ドロップダウン リストから **VM** とテンプレート を選択します。
2. 左側のナビゲータ ペインで VM を右クリックし、ドロップダウン リストで * SnapCenter Plug-in for VMware vSphere* を選択し、セカンダリ ドロップダウン リストで * 復元 * を選択します。
3. *復元*ウィザードの「バックアップの選択」ページで、復元するバックアップ コピーを選択します。

   特定のバックアップ名または部分的なバックアップ名を検索したり、フィルタ アイコンを選択して日付と時刻の範囲を選択し、VMware スナップショットを含むバックアップが必要かどうか、マウントされたバックアップが必要かどうか、およびプライマリまたはセカンダリの場所を選択して、バックアップ リストをフィルタすることができます。 [OK] を選択してウィザードに戻ります。

4. *範囲の選択*ページで、復元先を選択します。

復元するには...	復元先を指定してください...
元のデータストア	ドロップダウンリストから*特定のディスク*を選択し、*次へ*を選択します。データストア選択表で、VMDKを選択または選択解除できます。
別の場所にある別のデータストア	宛先データストアを選択し、リストから別のデータストアを選択します。

5. *場所の選択*ページで、復元するスナップショット (プライマリまたはセカンダリ) を選択します。
6. 概要ページを確認し、[完了] を選択します。
7. オプション: 画面下部の*最近のタスク*を選択して、操作の進行状況を監視します。
8. 最新の情報を表示するには画面を更新します。

MySQLデータベースの最新のバックアップのリストア

メンテナンス コンソールを使用して、SnapCenter Plug-in for VMware vSphere のMySQLデータベース（NSMデータベースとも呼ばれる）の最新のバックアップをリストアできます。

手順

1. メンテナンス コンソールのウィンドウを開きます。

   "メンテナンスコンソールにアクセスする" 。

2. メインメニューからオプション*1) アプリケーション構成*を入力します。
3. アプリケーション構成メニューから、オプション*6) MySQL のバックアップと復元*を入力します。
4. MySQL バックアップおよび復元構成メニューから、オプション **4) MySQL** バックアップの復元 を入力します。

5. 「最新のバックアップを使用して復元します」というプロンプトで **y** と入力し、**Enter** を押します。

   バックアップMySQLデータベースが元の場所にリストアされます。

MySQLデータベースの特定のバックアップのリストア

メンテナンス コンソールを使用して、SnapCenter Plug-in for VMware vSphere仮想アプライアンスのMySQLデータベース（NSMデータベースとも呼ばれる）の特定のバックアップをリストアすることができます。

手順

1. メンテナンス コンソールのウィンドウを開きます。

   "メンテナンスコンソールにアクセスする" 。

2. メインメニューからオプション*1) アプリケーション構成*を入力します。
3. アプリケーション構成メニューから、オプション*6) MySQL のバックアップと復元*を入力します。
4. MySQL バックアップおよび復元構成メニューから、オプション **2) MySQL** バックアップの一覧 を入力し、復元するバックアップをメモします。
5. MySQL バックアップおよび復元構成メニューから、オプション **4) MySQL** バックアップの復元 を入力します。
6. 「最新のバックアップを使用して復元します」というプロンプトで、**n** と入力します。
7. 「復元元のバックアップ」というプロンプトでバックアップ名を入力し、**Enter** を押します。

   選択したバックアップMySQLデータベースが元の場所にリストアされます。

VMDKの接続および接続解除

VMまたはvVol VMへのVMDKの接続

バックアップから1つ以上のVMDKを、親VM、同じESXiホスト上の代替VM、またはリンク モードで同じvCenterか別のvCenterによって管理されている代替ESXiホスト上の代替VMに接続できます。従来のデータストア内のVMと、vVolデータストア内のVMがサポートされます。

これにより、ドライブ全体をリストアしなくても、ドライブ内のファイルを簡単にリストアできます。必要なファイルのリストアや利用が終わったら、VMDKの接続を解除できます。

タスク概要

次の接続オプションがあります。

- プライマリ バックアップまたはセカンダリ バックアップの仮想ディスクを接続できます。
- 仮想ディスクは、親VM（仮想ディスクが元々関連付けられていたVM）または同じESXiホスト上の代替VMに接続できます。

仮想ディスクの接続には次の制限事項があります。

- 仮想マシン テンプレートは接続および接続解除できません。
- VMware側の制限により、1つのiSCSIコントローラに15本を超えるVMDKが接続されている場合、SnapCenter Plug-in for VMware vSphereの仮想マシンは15より上のVMDKユニット番号を検出できません。

  この場合は、SCSIコントローラを手動で追加してから、接続処理を再試行してください。

- ゲスト ファイルのリストア処理の一環として接続またはマウントされた仮想ディスクは、手動では接続できません。
- 接続処理とリストア処理では、デフォルトのSCSIコントローラを使用してVMDKが接続されます。ただし、NVMeディスクを使用してVMに接続されたVMDKがバックアップされる際、接続処理とリストア処理では、利用可能な場合はNVMeコントローラが使用されます。

開始する前に

NVMeコントローラをディスクに追加するには、次の手順を実行します。

1. vCenterクライアントにログインします。
2. VMFSデータストアからVMを選択します。
3. VMを右クリックして*設定の編集*に進みます
4. 設定編集ウィンドウで、新しいデバイスの追加 > *NVMeコントローラー*を選択します。

手順

1. VMware vSphere クライアント GUI で、ツールバーの メニュー を選択し、ドロップダウン リストから ホストとクラスタ を選択します。

2. 左側のナビゲーション ペインで、VM を右クリックし、* SnapCenter Plug-in for VMware vSphere* > 仮想ディスクの接続 を選択します。
3. 仮想ディスクの接続 ウィンドウの バックアップ セクションで、バックアップを選択します。

   フィルター アイコンを選択し、日付と時刻の範囲、VMware スナップショットを含むバックアップが必要かどうか、マウントされたバックアップが必要かどうか、および場所を選択することで、バックアップ リストをフィルターできます。「OK」を選択します。

4. *ディスクの選択*セクションで、接続する 1 つ以上のディスクと、接続元の場所 (プライマリまたはセカンダリ) を選択します。

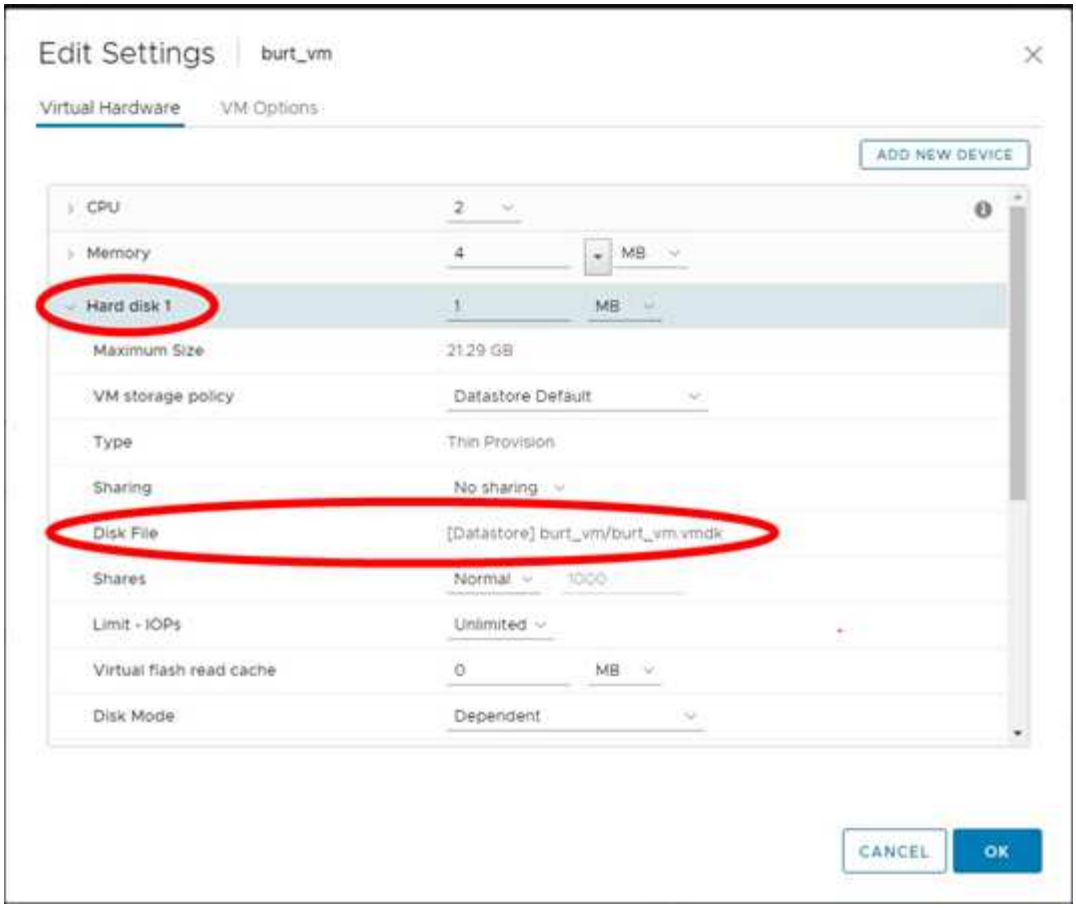
   フィルタを変更すると、プライマリ ロケーションとセカンダリ ロケーションを表示できます。

5. デフォルトでは、選択した仮想ディスクは親VMに接続されます。選択した仮想ディスクを同じ ESXi ホスト内の代替 VM に接続するには、[代替 **VM** に接続するにはここをクリック] を選択し、代替 VM を指定します。
6. *添付*を選択します。
7. オプション: 最近のタスク セクションで操作の進行状況を監視します。

   最新の情報を表示するには画面を更新します。

8. 次の手順を実行して仮想ディスクが接続されたことを確認します。

   a. ツールバーの*メニュー*を選択し、ドロップダウンリストから*VMとテンプレート*を選択します。
   b. 左側のナビゲータ ペインで VM を右クリックし、ドロップダウン リストから [設定の編集] を選択します。
   c. 設定の編集 ウィンドウで、各ハードディスクのリストを展開して、ディスク ファイルのリストを表示します。



[Edit Settings]ページに、VM上のディスクが一覧表示されます。ハードディスクごとに詳細を展開して、接続されている仮想ディスクのリストを確認できます。

結果

接続されたディスクにホスト オペレーティング システムからアクセスし、ディスクから必要な情報を取得できます。

仮想ディスクの接続解除

仮想ディスクを接続して個々のファイルをリストアしたあとに、親VMから仮想ディスクの接続を解除することができます。

手順

1. VMware vSphere クライアント GUI で、ツールバーの メニュー を選択し、ドロップダウン リストから **VM** とテンプレート を選択します。
2. 左側のナビゲーション ペインでVMを選択します。
3. 左側のナビゲーション ペインで、VM を右クリックし、ドロップダウン リストで * [SnapCenter Plug-in for VMware vSphere]* を選択し、セカンダリ ドロップダウン リストで * [仮想ディスクの切断]* を選択します。
4. *仮想ディスクの切断*画面で、切断するディスクを 1 つ以上選択し、*選択したディスクの切断*チェックボックスをオンにして、*切断*を選択します。

選択する仮想ディスクを間違えないようにしてください。間違ったディスクを選択すると、本番環境に影響する可能性があります。

5. オプション: 最近のタスク セクションで操作の進行状況を監視します。

   最新の情報を表示するには画面を更新します。

6. 次の手順を実行して、仮想ディスクの接続が解除されたことを確認します。
   a. ツールバーの*メニュー*を選択し、ドロップダウンリストから*VMとテンプレート*を選択します。
   b. 左側のナビゲータ ペインで VM を右クリックし、ドロップダウン リストから [設定の編集] を選択します。
   c. 設定の編集 ウィンドウで、各ハードディスクのリストを展開して、ディスク ファイルのリストを表示します。

      設定の編集 ページには、VM 上のディスクが一覧表示されます。ハードディスクごとに詳細を展開して、接続されている仮想ディスクのリストを確認できます。

ゲスト ファイルとフォルダの復元

ワークフロー、前提条件、制限事項

WindowsゲストOSの仮想マシン ディスク（VMDK）からファイルやフォルダをリストアできます。

ゲスト リストアのワークフロー

ゲストOSリストア処理には、次の手順が含まれます。

1. 接続

   仮想ディスクをゲストVMまたはプロキシVMに接続し、ゲスト ファイル リストア セッションを開始します。

2. 待機

   接続処理が完了し、参照およびリストアを実行できるようになるまで待ちます。接続

   処理が完了すると、ゲスト ファイル リストア セッションが自動的に作成され、Eメール通知が

   送信されます。

3. ファイルまたはフォルダの選択

   ゲスト ファイル リストア セッションでVMDKを参照し、リストアするファイルまたはフォルダを1つ以上選択します。

4. リストア

   選択したファイルまたはフォルダを指定した場所にリストアします。

ゲスト ファイルとフォルダをリストアするための前提条件

WindowsゲストOSのVMDKから1つ以上のファイルまたはフォルダをリストアする前に、すべての要件を確認しておく必要があります。

- VMware Toolsがインストールされ、実行されている必要があります。

  SnapCenterは、VMware Toolsからの情報を使用して、VMwareゲストOSへの接続を確立します。

- WindowsゲストOSでWindows Server 2008 R2以降が実行されている必要があります。

  サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool（IMT）"。

- ターゲットVMのクレデンシャルで、組み込みのドメイン管理者アカウントまたは組み込みのローカル管理者アカウントを指定する必要があります。ユーザ名は「Administrator」である必要があります。リストア処理を開始する前に、仮想ディスクを接続するVMの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、接続処理と後続のリストア処理の両方で必要です。ワークグループ ユーザは、組み込みのローカル管理者アカウントを使用できます。

> 組み込みの管理者アカウントではなく、VM内の管理者権限を持つアカウントを使用する必要がある場合は、ゲストVMのUACを無効にする必要があります。

- 復元元のバックアップ スナップショットと VMDK を知っておく必要があります。

  SnapCenter Plug-in for VMware vSphereでは、リストアするファイルやフォルダの検索はサポートされていません。したがって、開始する前に、スナップショットおよび対応する VMDK に関するファイルまたはフォルダーの場所を知っておく必要があります。

- 接続する仮想ディスクはSnapCenterバックアップに含まれている必要があります。

  リストアするファイルまたはフォルダが格納されている仮想ディスクが、SnapCenter Plug-in for VMware vSphere仮想アプライアンスを使用して実行されたVMバックアップに含まれている必要があります。

- プロキシVMを使用するには、プロキシVMを設定する必要があります。

  仮想ディスクをプロキシVMに接続する場合は、接続およびリストア処理を開始する前にプロキシVMを設定しておく必要があります。

- 英語のアルファベット以外を使った名前のファイルの場合は、単一のファイルとしてではなく、ディレクトリにリストアする必要があります。

  日本語の漢字など、アルファベット以外の名前のファイルをリストアするには、ファイルが配置されているディレクトリをリストアします。

- LinuxゲストOSからのリストアはサポートされていません。

  LinuxゲストOSを実行しているVMからファイルやフォルダをリストアすることはできません。ただし、VMDKを接続し、ファイルとフォルダを手動でリストアすることもできます。サポートされているゲストOSの最新情報については、 "NetApp Interoperability Matrix Tool（IMT）" 。

ゲスト ファイル リストアに関する制限事項

ゲストOSからファイルまたはフォルダをリストアする前に、この機能でサポートされない処理について理解しておく必要があります。

- ゲストOS内でダイナミック ディスク タイプをリストアすることはできません。
- 暗号化されたファイルまたはフォルダをリストアした場合、暗号化属性は保持されません。ファイルまたはフォルダを暗号化されたフォルダにリストアすることはできません。
- [Guest File Browse]ページには、隠しファイルとフォルダが表示されますが、フィルタすることはできません。
- LinuxゲストOSからはリストアできません。

  LinuxゲストOSを実行しているVMからファイルやフォルダをリストアすることはできません。ただし、VMDKを接続し、ファイルとフォルダを手動でリストアすることもできます。サポートされているゲストOSの最新情報については、 "NetApp Interoperability Matrix Tool（IMT）" 。

- NTFSファイルシステムからFATファイルシステムにリストアすることはできません。

  NTFS形式からFAT形式にリストアしようとした場合、FATファイルシステムはWindowsセキュリティ属性をサポートしていないため、NTFSセキュリティ記述子はコピーされません。

- クローニングされたVMDKまたは初期化されていないVMDKからゲスト ファイルをリストアすることはできません。
- ファイルのディレクトリ構造はリストアできません。

  ネストされたディレクトリ内のファイルをリストア対象として選択した場合、そのファイルは同じディレクトリ構造ではリストアされません。ディレクトリ ツリーはリストアされず、ファイルのみがリストアされます。ディレクトリ ツリーをリストアする場合は、構造の最上部にディレクトリ自体をコピーします。

- vVol VMから別のホストにゲスト ファイルをリストアすることはできません。
- 暗号化されたゲスト ファイルはリストアできません。

VMDKからのゲスト ファイルとフォルダのリストア

WindowsゲストOSのVMDKから1つ以上のファイルまたはフォルダをリストアできます。

タスク概要

デフォルトでは、仮想ディスクは接続してから24時間使用可能であり、その後、自動的に接続解除されます。ウィザードで、復元操作が完了したらセッションを自動的に削除するように選択することも、いつでも手動でゲスト ファイル復元セッションを削除したり、[ゲスト構成] ページで時間を延長したりすることもできます。

ゲスト ファイルまたはフォルダのリストア パフォーマンスは、リストアするファイル/ /フォルダのサイズと、リストアするファイル / フォルダの数という2つの要因によって決まります。リストア対象のデータ セットのサイズが同じ場合、サイズの小さいファイルを多数リストアするのにかかる時間は、サイズの大きいファイルを少数リストアするのにかかる時間と比較して、想定よりも長くなることがあります。

> 1つのVMで一度に実行できる接続処理またはリストア処理は1つだけです。同じVMに対して並行して接続処理またはリストア処理を実行することはできません。

> ゲスト リストア機能を使用すると、システム ファイルおよび隠しファイルの表示とリストア、および暗号化されたファイルの表示を行うことができます。既存のシステム ファイルを上書きしたり、暗号化されたファイルを暗号化されたフォルダに復元したりしないでください。リストア処理中、ゲスト ファイルの隠し属性、システム属性、および暗号化属性は、リストアされたファイルに保持されません。予約済みパーティションを表示または参照すると、エラーが発生する可能性があります。

手順

1. vSphere クライアントのショートカット ウィンドウから、ホストとクラスタ を選択し、VM を選択します。
2. VM を右クリックし、* SnapCenter Plug-in for VMware vSphere* > ゲスト ファイル リストア を選択します。
3. *復元範囲*ページで、次の操作を実行して、接続する仮想ディスクを含むバックアップを指定します。

a. バックアップ名 テーブルで、接続する仮想ディスクを含むバックアップを選択します。

b. **VMDK** テーブルで、復元するファイルまたはフォルダーが含まれている仮想ディスクを選択します。

c. 場所 テーブルで、接続する仮想ディスクの場所 (プライマリまたはセカンダリ) を選択します。

4. *ゲストの詳細*ページで、次の操作を行います。

   a. 仮想ディスクの接続先を選択します。

このオプションを選択してください...	もし...
Use Guest VM	ウィザードを開始する前に右クリックした VM に仮想ディスクを接続し、右クリックした VM の資格情報を選択します。 VMのクレデンシャルを作成しておく必要があります。
Use Guest File Restore proxy VM	仮想ディスクをプロキシ VM に接続し、プロキシ VM を選択します。 接続とリストアの処理を開始する前に、プロキシVMを設定しておく必要があります。

   b. *電子メール通知を送信*オプションを選択します。

   アタッチ操作が終了し、仮想ディスクが使用可能になったときに通知を受け取りたい場合は、このオプションが必要です。通知Eメールには、仮想ディスク名、VM名、およびVMDKに新しく割り当てられたドライブ レターが記載されています。

   ゲスト ファイルのリストアは非同期処理であり、ゲスト セッションの確立には時間がかかる可能性があるため、このオプションを有効にします。

このオプションでは、vCenterでVMware vSphere Clientをセットアップするときに設定したEメール設定が使用されます。

5. 概要を確認して、[完了] を選択します。

   *[完了]*を選択する前に、ウィザードの任意のページに戻って情報を変更できます。

6. 接続処理が完了するまで待ちます。

   処理の進捗状況はダッシュボードのジョブ モニタで確認できます。または、Eメール通知が届くまで待つこともできます。

7. 接続されている仮想ディスクから復元するファイルを見つけるには、vSphere クライアントのショートカット ウィンドウから * SnapCenter Plug-in for VMware vSphere* を選択します。

8. 左側のナビゲータ ペインで、ゲスト ファイルの復元 > ゲスト構成 を選択します。

ゲスト セッション モニター テーブルで、* を選択すると、セッションに関する追加情報を表示できます。 *右側の列にあります。

9. 通知メールに記載されている仮想ディスクのゲスト ファイル リストア セッションを選択します。

   システムで予約済みのパーティションを含め、すべてのパーティションにドライブ レターが割り当てられます。VMDKに複数のパーティションがある場合は、[Guest File Browse]ページの上部にあるドライブ フィールドのドロップダウン リストでドライブを選択して、特定のドライブを選択できます。

10. *ファイルの参照*アイコンを選択すると、仮想ディスク上のファイルとフォルダのリストが表示されます。

    フォルダーをダブル選択して参照し、個々のファイルを選択する場合、取得操作は実行時に実行されるため、ファイルの一覧を取得するときに時間がかかることがあります。

    参照を簡単にするために、検索文字列にフィルタを使用できます。フィルタは、スペースを含まないPerl式で、大文字と小文字が区別されます。デフォルトの検索文字列は .*。次の表に、Perl検索式の例を示します。

この表現は…	検索対象…
。	改行文字以外の任意の文字。
.*	任意の文字列。これがデフォルトです。
a	文字a。
ab	文字列ab。
a [縦棒] b	文字aまたはb。
a*	文字aの0個以上のインスタンス。
a+	文字aの1個以上のインスタンス。
a?	文字aの0個または1個のインスタンス。
斧}	文字aのx個のインスタンス。
斧、}	文字aのx個以上のインスタンス。
a{x,y}	文字aのx個以上y個以下のインスタンス。
\	特殊文字をエスケープします。

    [Guest File Browse]ページには、すべての隠しファイルとフォルダに加えて、他のすべてのファイルとフォルダが表示されます。

11. 復元するファイルまたはフォルダーを 1 つ以上選択し、[復元場所の選択] を選択します。

    リストアするファイルとフォルダが[Selected File(s)]の表に一覧表示されます。

12. *復元場所の選択*ページで、以下を指定します。

オプション	説明
Restore to path	選択したファイルをリストアするゲストへのUNC共有パスを入力します。IPv4アドレスの例: `\\10.60.136.65\c$` IPv6アドレスの例: `\\fd20-8b1e-b255-832e-61.ipv6-literal.net\C\restore`
元のファイルが存在する場合	復元先のファイルに復元対象のファイルまたはフォルダーが既に存在する場合に実行するアクションを選択します: 常に上書きする、または常にスキップする。 フォルダがすでに存在する場合は、フォルダの内容が既存のフォルダにマージされます。
復元が成功したらゲストセッションを切断します	このオプションは、リストア処理の完了時にゲスト ファイル リストア セッションを削除する場合に選択します。

13. *復元*を選択します。

    リストア処理の進捗状況はダッシュボードのジョブ モニタで確認できます。または、Eメール通知が届くまで待つこともできます。Eメール通知が送信されるまでの時間は、リストア処理が完了するまでの時間によって異なります。

    通知Eメールには、リストア処理の出力が添付されています。リストア処理が失敗した場合は、添付ファイルを開いて追加情報を確認してください。

リストア処理用のプロキシVMのセットアップ

ゲスト ファイル リストア処理でプロキシVMを使用して仮想ディスクを接続する場合は、リストア処理を開始する前にプロキシVMを設定する必要があります。プロキシVMはいつでもセットアップできますが、プラグインの導入が完了したらすぐにセットアップする方が便利な場合があります。

手順

1. vSphere クライアントのショートカット ウィンドウで、プラグインの下にある * SnapCenter Plug-in for VMware vSphere* を選択します。
2. 左側のナビゲーションで、[ゲスト ファイルの復元] を選択します。
3. *実行資格情報*セクションで、次のいずれかを実行します。

これをするには...	操作
既存のクレデンシャルを使用する	設定済みの任意のクレデンシャルを選択します。

これをするには...	操作
新しいクレデンシャルを追加する	a. *追加*を選択します。 b. *[実行資格情報] ダイアログ ボックスで、資格情報を入力します。 c. **VM** の選択*を選択し、*プロキシ **VM** ダイアログ ボックスで VM を選択します。 **[**保存**]** を選択して、**[**実行資格情報**]** ダイアログボックスに戻ります。 d. クレデンシャルを入力します。[Username] に「Administrator」と入力する必要があります。

SnapCenter Plug-in for VMware vSphereは、選択したクレデンシャルを使用して、選択したプロキシVMにログインします。

Run Asクレデンシャルは、Windowsに用意されているデフォルトのドメイン管理者または組み込みのローカル管理者である必要があります。ワークグループ ユーザは、組み込みのローカル管理者アカウントを使用できます。

4. *プロキシ資格情報*セクションで*追加*を選択して、プロキシとして使用する VM を追加します。
5. プロキシ **VM** ダイアログ ボックスで情報を入力し、保存 を選択します。

ESXiホストからプロキシVMを削除する前に、SnapCenter Plug-in for VMware vSphere UIからプロキシVMを削除しておく必要があります。

VMゲスト ファイルのリストア用のクレデンシャルの設定

ゲスト ファイルまたはフォルダのリストア処理用に仮想ディスクを接続する場合は、リストア前に接続先のVMでクレデンシャルを設定しておく必要があります。

タスク概要

次の表に、ゲスト リストア処理のクレデンシャル要件を示します。

	ユーザーアクセス制御が有効	ユーザーアクセス制御が無効
ドメイン ユーザ	ユーザ名が「administrator」のドメイン ユーザは問題なく機能します。「NetApp\administrator」が一例です。しかし、ローカル管理者グループに属するユーザ名が「xyz」のドメイン ユーザは機能しません。たとえば、「NetApp\xyz」は使用できません。	ユーザ名が「administrator」のドメイン ユーザとローカル管理者グループに属するユーザ名が「xyz」のドメイン ユーザのどちらも問題なく機能します。たとえば、「NetApp\administrator」や「NetApp\xyz」です。

	ユーザーアクセス制御が有効	ユーザーアクセス制御が無効
ワークグループ ユーザ	ユーザ名が「administrator」のローカル ユーザであれば問題なく機能します。しかし、ローカル管理者グループに属するユーザ名が「xyz」のローカル ユーザは機能しません。	ユーザ名が「administrator」のローカル ユーザとローカル管理者グループに属するユーザ名が「xyz」のローカル ユーザのどちらも問題なく機能します。しかし、ユーザ名が「xyz」で、ローカル管理者グループに属していないローカル ユーザは機能しません。

上記の例で、「NetApp」はダミーのドメイン名、「xyz」はダミーのローカル ユーザ名です

手順

1. vSphere クライアントのショートカット ウィンドウで、プラグインの下にある * SnapCenter Plug-in for VMware vSphere* を選択します。
2. 左側のナビゲーションで、[ゲスト ファイルの復元] を選択します。
3. *実行資格情報*セクションで、次のいずれかを実行します。

これをするには...	操作
既存のクレデンシャルを使用する	設定済みの任意のクレデンシャルを選択します。
新しいクレデンシャルを追加する	a. *追加*を選択します。 b. **[**実行資格情報**]** ダイアログ ボックスで、資格情報を入力します。[Username]に「Administrator」と入力する必要があります。 c. **VM** の選択*を選択し、*プロキシ **VM** ダイアログ ボックスで VM を選択します。 **[**保存**]** を選択して、**[**実行資格情報**]** ダイアログボックスに戻ります。クレデンシャルの認証に使用するVMを選択します。

SnapCenter Plug-in for VMware vSphereは、選択したクレデンシャルを使用して、選択したVMにログオンします。

4. *保存*を選択します。

ゲスト ファイル リストア セッションの時間の延長

デフォルトでは、ゲスト ファイル リストアVMDKは接続してから24時間使用可能であり、その後、自動的に接続解除されます。*ゲスト設定*ページで時間を延長できます。

タスク概要

接続したVMDKからあとで追加のファイルやフォルダをリストアする場合は、ゲスト ファイル リストア セッションを延長できます。ただし、ゲスト ファイル リストア セッションでは多くのリソースが使用されるため、セッション時間の延長は頻繁に行わないようにします。

手順

1. VMware vSphere クライアントで、ゲスト ファイルの復元 を選択します。
2. ゲスト ファイルの復元セッションを選択し、ゲスト セッション モニターのタイトル バーにある [選択したゲスト セッションの延長] アイコンを選択します。

   セッションが24時間延長されます。

実際に起こり得るゲスト ファイルのリストア シナリオ

ゲスト ファイルをリストアしようとすると、次のいずれかの状況が発生することがあります。

ゲスト ファイル リストア セッションが空白

この問題は、ゲスト ファイル リストア セッションを作成したときに、そのセッションがアクティブの状態でゲスト オペレーティング システムがリブートされた場合に発生します。これが発生した場合、ゲストOSのVMDKはオフラインのままになることがあります。そのため、ゲスト ファイル リストア セッションを参照しようとすると、リストは空白になっています。

この問題を修正するには、ゲストOSでVMDKを手動でオンラインに戻します。VMDKがオンラインになると、ゲスト ファイル リストア セッションに正しい内容が表示されます。

ゲスト ファイル リストアのディスク接続処理が失敗する

この問題は、ゲスト ファイルの復元操作を開始したときに、VMware ツールが実行されていてゲスト OS の資格情報が正しいにもかかわらず、ディスクの接続操作が失敗した場合に発生します。これが発生すると、次のエラーが返されます。

```
Error while validating guest credentials, failed to access guest system using
specified credentials: Verify VMWare tools is running properly on system and
account used is Administrator account, Error is SystemError vix error codes =
(3016, 0).
```

この問題を修正するには、ゲストOSでVMware Tools Windowsサービスを再起動してから、ゲスト ファイル リストア処理を再試行します。

ゲスト**E**メールにファイル名として「**??????**」が表示される

この問題は、ゲスト ファイル リストア機能を使用して名前に英語以外の文字が含まれているファイルまたはフォルダをリストアした場合に発生し、Eメール通知に「??????」と表示されます。Eメールの添付ファイルには、リストアされたファイルとフォルダの名前が正しくリストされています。

ゲスト ファイル リストア セッションを中断してもバックアップが切断されない

この問題は、VM整合性バックアップからゲスト ファイル リストア処理を実行した場合に発生します。ゲスト ファイル リストア セッションがアクティブな間に、同じVMに対して別のVM整合性バックアップが実行されます。ゲスト ファイル リストア セッションが手動または24時間後に自動的に切断されても、セッションのバックアップは切断されません。

この問題を修正するには、アクティブ ゲスト ファイル リストア セッションから接続されていたVMDKを手動

で切断します。

SnapCenter Plug-in for VMware vSphereアプライアンスの管理

VMware vSphere Clientサービスの再起動

SnapCenter VMware vSphere Clientの動作が正しくない場合は、ブラウザ キャッシュをクリアしてみてください。問題が解決しない場合は、Web Client Serviceを再起動します。

Linux vCenterでVMware vSphere Client Serviceを再起動します。

開始する前に

vCenter 7.0U1以降を実行している必要があります。

手順

1. SSHを使用してvCenter Server Applianceにrootとしてログインします。
2. 次のコマンドを使用して、アプライアンス シェルまたはBashシェルにアクセスします。

   ```
   shell
   ```

3. 次のHTML5コマンドを使用して、Web Client Serviceを停止します。

   ```
   service-control --stop vsphere-ui
   ```

4. 次のシェル コマンドを使用して、vCenterで古いHTML5 scvmパッケージをすべて削除します。

   ```
   etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/

   rm -rf com.netapp.scv.client-<version_number>
   ```

   VASAやvCenter 7.x以降のパッケージは削除しないでください。

5. 次のHTML5コマンドを使用して、Web Client Serviceを起動します。

   ```
   service-control --start vsphere-ui
   ```

メンテナンス コンソールへのアクセス

SnapCenter Plug-in for VMware vSphereのメンテナンス コンソールを使用して、アプリケーション、システム、ネットワークの構成を管理できます。管理者パスワードやメンテナンス パスワードを変更したり、サポート バンドルを生成したり、リモート診断を開始したりできます。

開始する前に

SnapCenter Plug-in for VMware vSphereのサービスを停止して再起動する前に、すべてのスケジュールを一

時停止しておく必要があります。

タスク概要

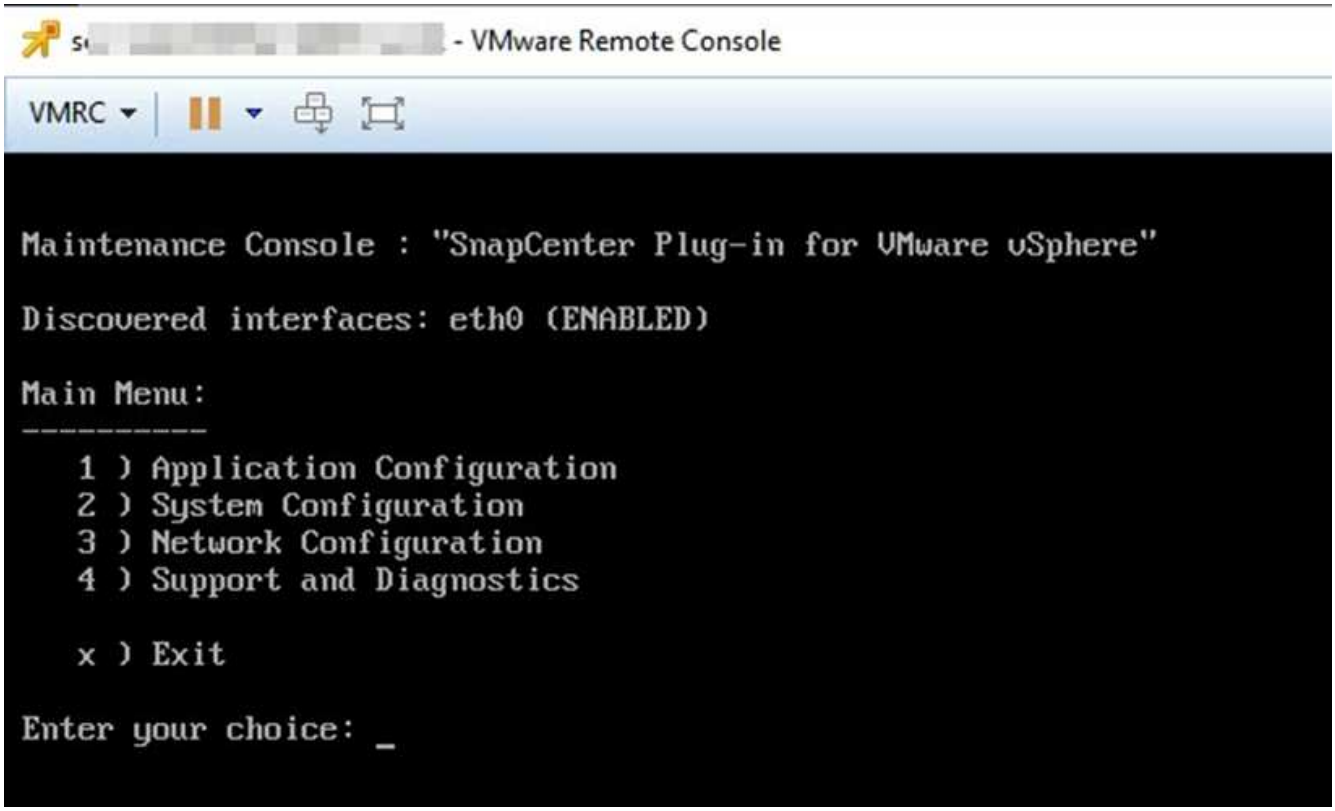
- SnapCenter Plug-in for VMware vSphere 4.6P1では、初めてSnapCenter Plug-in for VMware vSphereをインストールする際にパスワードを指定する必要があります。リリース4.6以前からリリース4.6P1以降にアップグレードする場合は、これまでのデフォルト パスワードを使用できます。
- リモート診断を有効にする場合、「diag」ユーザのパスワードを設定する必要があります。

  コマンドを実行するためのルート ユーザー権限を取得するには、sudo <コマンド> を使用します。

手順

1. VMware vSphere Clientで、SnapCenter Plug-in for VMware vSphereが配置されているVMを選択します。
2. 仮想アプライアンスの 概要 タブで リモート コンソールの起動 を選択して、メンテナンス コンソール ウィンドウを開きます。

   デフォルトのメンテナンスコンソールのユーザー名を使用してログインします `maint`インストール時に設定したユーザー名とパスワードを入力します。



3. 次の操作を実行できます。

   - オプション1: アプリケーション構成

     SnapCenter Plug-in for VMware vSphereの概要を表示するSnapCenter Plug-in for VMware vSphereサービスを開始または停止するSnapCenter Plug-in for VMware vSphere のログイン ユーザー名またはパスワードを変更する MySQL のパスワードを変更する MySQL をバックアップおよび復元し、MySQL のバックアップを設定および一覧表示する

- オプション2: システム構成

  仮想マシンを再起動する 仮想マシンをシャットダウンする 'maint' ユーザーのパスワードを変更する タイムゾーンを変更する NTP サーバーを変更する SSH アクセスを有効にする jail ディスク サイズを増やす (/jail) アップグレードする VMware Tools をインストールする MFA トークンを生成する

  > MFAは常に有効になっており、無効にすることはできません。

- オプション3: ネットワーク構成

  IPアドレス設定の表示または変更 ドメイン名検索設定の表示または変更 静的ルートの表示または変更 変更のコミット ホストへのping

- オプション4: サポートと診断

  サポート バンドルを生成する 診断シェルにアクセスする リモート診断アクセスを有効にする コア ダンプ バンドルを生成する

メンテナンス コンソールからのSnapCenter Plug-in for VMware vSphereのパスワードの変更

SnapCenter Plug-in for VMware vSphereの管理GUIの管理パスワードがわからない場合は、メンテナンス コンソールで新しいパスワードを設定できます。

開始する前に

SnapCenter Plug-in for VMware vSphereのサービスを停止して再起動する前に、すべてのスケジュールを一時停止しておく必要があります。

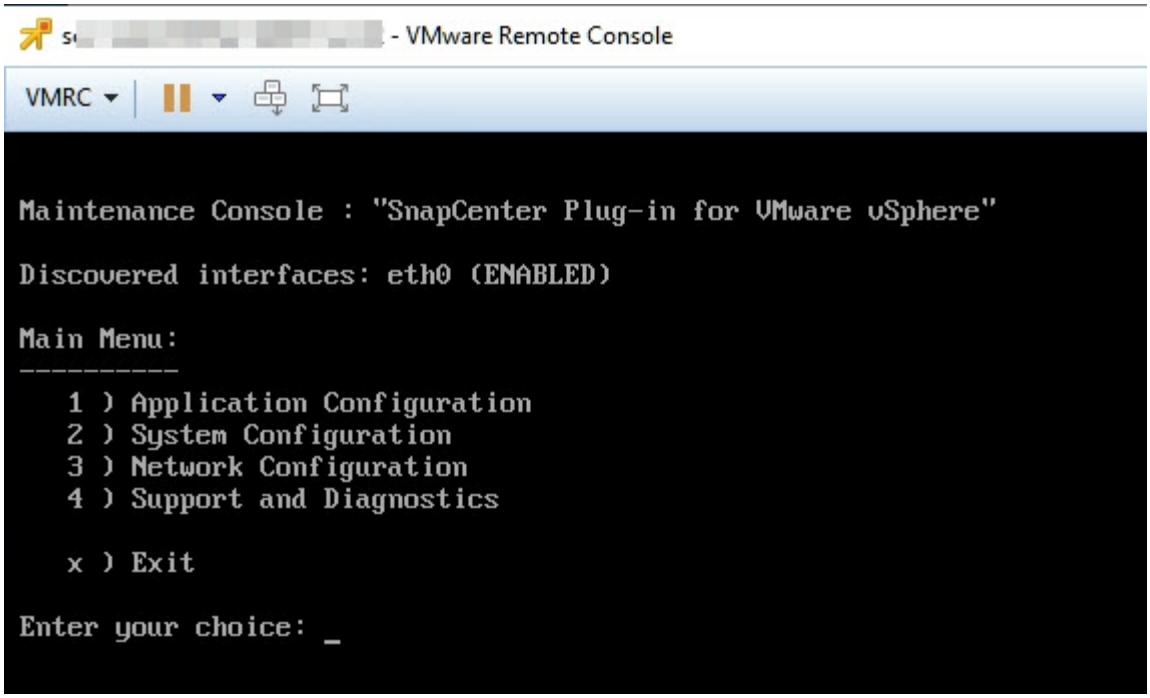
タスク概要

メンテナンスコンソールへのアクセスとログインについては、以下を参照してください。"メンテナンスコンソールにアクセスする" 。

手順

1. VMware vSphere Clientで、SnapCenter Plug-in for VMware vSphereが配置されているVMを選択します。
2. 仮想アプライアンスの 概要 タブで リモート コンソールの起動 を選択してメンテナンス コンソール ウィンドウを開き、ログオンします。

   メンテナンスコンソールへのアクセスとログインについては、以下を参照してください。"メンテナンスコンソールにアクセスする" 。



3. アプリケーション構成に「**1**」と入力します。
4. ユーザー名またはパスワードを変更するには、「**4**」と入力します。
5. 新しいパスワードを入力します。

   SnapCenter VMware仮想アプライアンス サービスが停止し、再起動されます。

証明書の作成とインポート

SnapCenter Plug-in for VMware vSphereでは、クライアント ブラウザとのセキュアな通信にSSL暗号化を採用しています。この方法ではネットワーク全体でデータを暗号化できますが、新しい自己署名証明書を作成するか、独自の認証局（CA）インフラまたはサードパーティのCAを使用すると、証明書が現在の環境に固有であることが保証されます。

参照 "KB 記事: SnapCenter Plug-in for VMware vSphereに SSL 証明書を作成および/またはインポートする方法"詳細についてはこちらをご覧ください。

vCenterからのSnapCenter Plug-in for VMware vSphereの登録解除

リンク モードのvCenterでSnapCenter Plug-in for VMware vSphereサービスを停止すると、リンクされている他のvCenterでSnapCenter Plug-in for VMware vSphereサービスが実行されている場合でも、リンクされているすべてのvCenterでリソース グループを使用できなくなります。

SnapCenter Plug-in for VMware vSphereの拡張機能の登録を手動で解除する必要があります。

手順

1. SnapCenter Plug-in for VMware vSphereサービスが停止中のリンクされているvCenterで、管理オブジェクト参照（MOB）マネージャに移動します。
2. プロパティ オプションで、値列の **content** を選択し、次の画面で値列の **ExtensionManager** を選択して、登録されている拡張機能の一覧を表示します。
3. 拡張機能の登録を解除する `com.netapp.scv.client`そして `com.netapp.aegis`。

SnapCenter Plug-in for VMware vSphereの無効化および有効化

SnapCenterのデータ保護機能が不要になった場合は、SnapCenter Plug-in for VMware vSphereの設定を変更する必要があります。たとえば、テスト環境にプラグインを導入した場合、SnapCenterの機能をテスト環境で無効にし、本番環境で有効にしなければならないことがあります。

開始する前に

- 管理者権限が必要です。
- 実行中のSnapCenterジョブがないことを確認します。

タスク概要

SnapCenter Plug-in for VMware vSphereを無効にすると、すべてのリソース グループが一時停止され、プラグインは拡張機能としてのvCenterへの登録を解除されます。

SnapCenter Plug-in for VMware vSphereを有効にすると、プラグインは拡張機能としてvCenterに登録され、すべてのリソース グループが本番モードになり、すべてのスケジュールが有効になります。

手順

1. オプション: 新しい仮想アプライアンスに復元する場合に備えて、SnapCenter Plug-in for VMware vSphereをバックアップします。

   "SnapCenter Plug-in for VMware vSphereのMySQLデータベースのバックアップ" 。

2. 次の形式を使用して、SnapCenter Plug-in for VMware vSphere管理 GUI にログインします。`https://<OVA-IP-address>:8080` 。導入時に設定した管理者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 Plug-in for VMware vSphereを導入すると、このプラグインのIPアドレスが表示されます。

3. 左側のナビゲーション ペインで [構成] を選択し、[プラグインの詳細] セクションで [サービス] オプションの選択を解除して、プラグインを無効にします。
4. 選択内容を確認します。
   - SnapCenter Plug-in for VMware vSphereを使用してVM整合性のあるバックアップのみを実行した場合

     プラグインが無効になり、これ以上の操作は必要ありません。

   - SnapCenter Plug-in for VMware vSphereを使用してアプリケーションと整合性のあるバックアップを実行した場合

プラグインが無効になり、さらにクリーンアップが必要です。

i. VMware vSphereにログインします。

ii. VMの電源をオフにします。

iii. 左側のナビゲータ画面で、 SnapCenter Plug-in for VMware vSphere のインスタンス（ `.ova`仮想アプライアンスの展開時に使用されたファイル）を削除し、「ディスクから削除」を選択します。

iv. SnapCenterにログインし、vSphereホストを削除します。

SnapCenter Plug-in for VMware vSphereの削除

SnapCenterのデータ保護機能を使用する必要がなくなった場合は、SnapCenter Plug-in for VMware vSphereを無効にしてvCenterへの登録を解除し、vCenterからSnapCenter Plug-in for VMware vSphereを削除し、残りのファイルを手動で削除する必要があります。

開始する前に

- 管理者権限が必要です。
- 実行中のSnapCenterジョブがないことを確認します。

手順

1. 次の形式を使用して、SnapCenter Plug-in for VMware vSphere管理 GUI にログインします。 `https://<OVA-IP-address>:8080` 。

   SnapCenter Plug-in for VMware vSphereを導入すると、このプラグインのIPアドレスが表示されます。

2. 左側のナビゲーション ペインで [構成] を選択し、[プラグインの詳細] セクションで [サービス] オプションの選択を解除して、プラグインを無効にします。
3. VMware vSphereにログインします。
4. 左側のナビゲータ画面で、 SnapCenter Plug-in for VMware vSphere のインスタンス（ `.tar`仮想アプライアンスの展開時に使用されたファイル）を削除し、「ディスクから削除」を選択します。
5. アプリケーションと整合性のあるバックアップのために、SnapCenter Plug-in for VMware vSphereを使用して他のSnapCenterプラグインをサポートしていた場合は、SnapCenterにログインしてvSphereホストを削除します。

終了後の操作

仮想アプライアンスは引き続き環境内にありますが、SnapCenter Plug-in for VMware vSphereは削除されています。

SnapCenter Plug-in for VMware vSphereのホストVMを削除したあと、vCenterのローカル キャッシュが更新されるまで、プラグインがvCenterに表示されたままになることがあります。ただし、プラグインは削除されているため、そのホストに対してSnapCenter VMware vSphereの処理は実行できません。vCenterのローカルキャッシュを更新する場合は、最初にSnapCenter Plug-in for VMware vSphereの[Configuration]ページでアプライアンスが無効な状態になっていることを確認してから、vCenter Web Client Serviceを再起動します。

構成の管理

バックアップのタイムゾーンの変更

開始する前に

SnapCenter Plug-in for VMware vSphereの管理GUIのIPアドレスとログイン クレデンシャルを確認しておく必要があります。また、メンテナンス コンソールから生成されたMFAトークンもメモしておく必要があります。

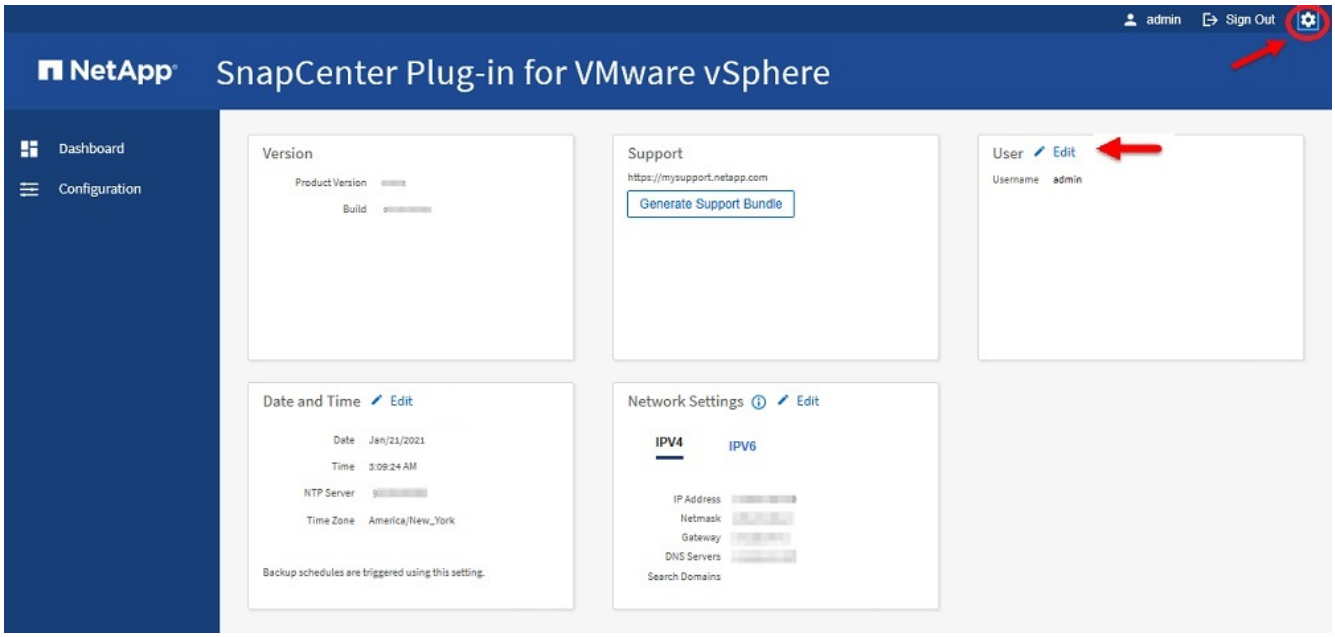
- このIPアドレスは、SnapCenter Plug-in for VMware vSphereの導入時に表示されたものです。
- SnapCenter Plug-in for VMware vSphereの導入時に指定したログイン クレデンシャル、またはあとで変更したログイン クレデンシャルを使用します。
- メンテナンス コンソールのシステム構成オプションを使用して、6桁のMFAトークンを生成します。

手順

1. SnapCenter Plug-in for VMware vSphere管理GUIにログインします。

   フォーマットを使用する `https://<appliance-IP-address>:8080`

2. 上部のツールバーにある設定アイコンを選択します。



3. *設定*ページの*日付と時刻*セクションで、*編集*を選択します。
4. 新しいタイムゾーンを選択し、[保存] を選択します。

   新しいタイムゾーンは、SnapCenter Plug-in for VMware vSphereで実行されるすべてのバックアップに使用されます。

ログオン クレデンシャルの変更

SnapCenter Plug-in for VMware vSphereの管理GUIのログオン クレデンシャルを変更できます。

開始する前に

SnapCenter Plug-in for VMware vSphereの管理GUIのIPアドレスとログオン クレデンシャルを確認しておく必要があります。また、メンテナンス コンソールから生成されたMFAトークンもメモしておく必要があります。

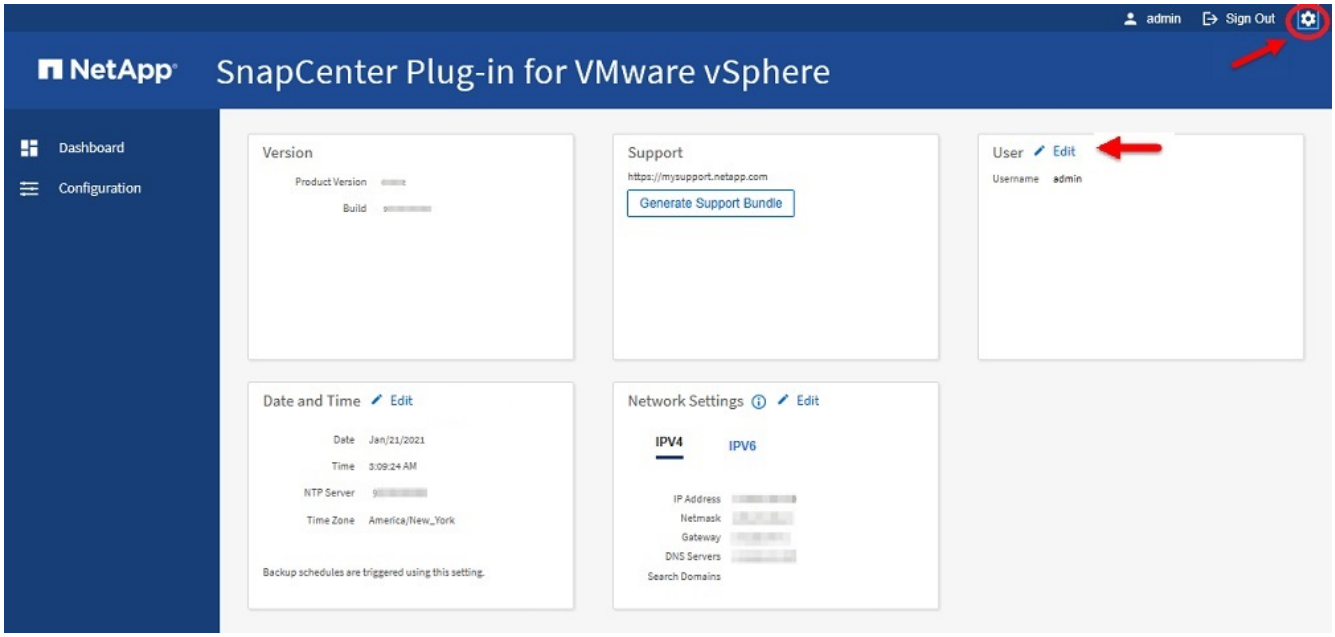
- このIPアドレスは、SnapCenter Plug-in for VMware vSphereの導入時に表示されたものです。
- SnapCenter Plug-in for VMware vSphereの導入時に指定したログイン クレデンシャル、またはあとで変更したログイン クレデンシャルを使用します。
- メンテナンス コンソールのシステム構成オプションを使用して、6桁のMFAトークンを生成します。

手順

1. SnapCenter Plug-in for VMware vSphere管理GUIにログインします。

   フォーマットを使用する `https://<appliance-IP-address>:8080`

2. 上部のツールバーにある設定アイコンを選択します。



3. *設定*ページの*ユーザー*セクションで、*編集*を選択します。
4. 新しいパスワードを入力し、「保存」を選択します。

   すべてのサービスが復旧するまでに数分かかることがあります。

vCenterログオン クレデンシャルの変更

SnapCenter Plug-in for VMware vSphereで設定されているvCenterログオン クレデンシャルは変更できます。これらの設定を使用して、プラグインからvCenterにアクセスします。vCenterのパスワードを変更した場合、vVolバックアップがシームレスに機能するためには、ONTAP Tools for VMware vSphereの登録を解除し、新しいパスワードで再登録する必要があります。

開始する前に

SnapCenter Plug-in for VMware vSphereの管理GUIのIPアドレスとログオン クレデンシャルを確認しておく必要があります。また、メンテナンス コンソールから生成されたMFAトークンもメモしておく必要があります。

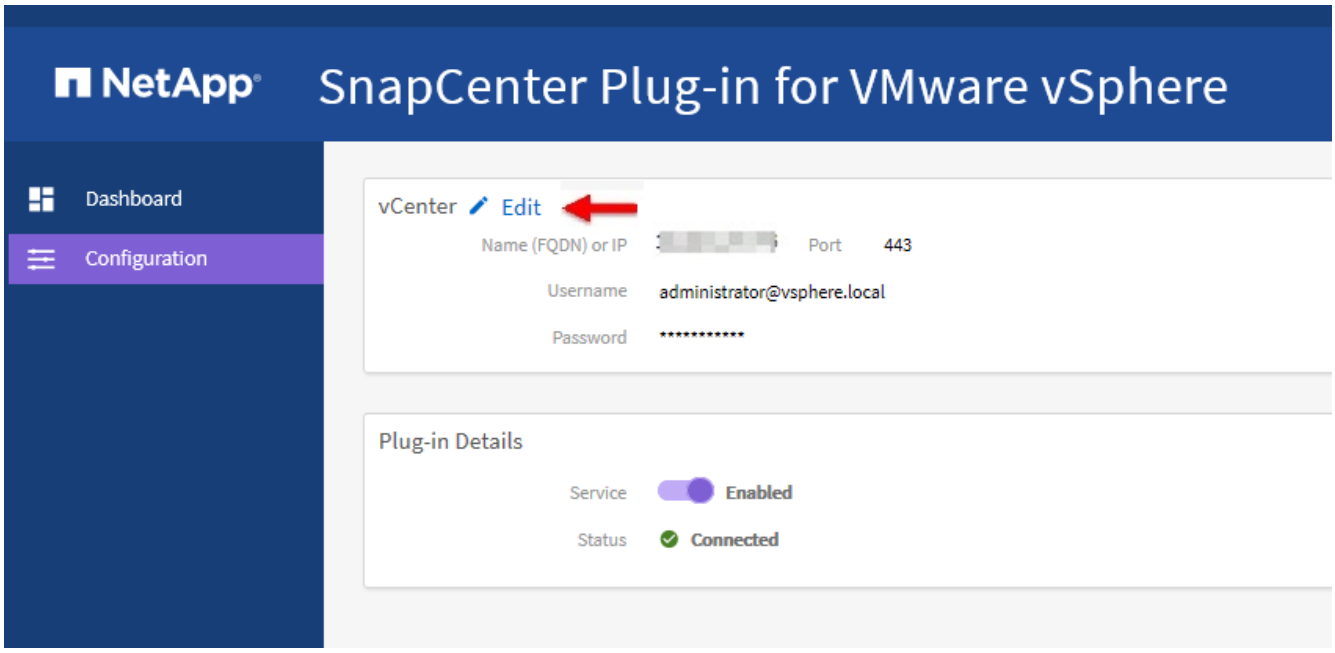
- このIPアドレスは、SnapCenter Plug-in for VMware vSphereの導入時に表示されたものです。
- SnapCenter Plug-in for VMware vSphereの導入時に指定したログイン クレデンシャル、またはあとで変更したログイン クレデンシャルを使用します。
- メンテナンス コンソールのシステム構成オプションを使用して、6桁のMFAトークンを生成します。

手順

1. SnapCenter Plug-in for VMware vSphere管理GUIにログインします。

   フォーマットを使用する `https://<appliance-IP-address>:8080`

2. 左側のナビゲーション ペインで、[構成] を選択します。



3. 構成 ページの **vCenter** セクションで、編集 を選択します。
4. 新しいパスワードを入力し、「保存」を選択します。

   ポート番号は変更しないでください。

ネットワーク設定の変更

SnapCenter Plug-in for VMware vSphereで設定されているネットワーク設定は変更できます。これらの設定を使用して、プラグインからvCenterにアクセスします。

開始する前に

SnapCenter Plug-in for VMware vSphereの管理GUIのIPアドレスとログオン クレデンシャルを確認しておく必要があります。また、メンテナンス コンソールから生成されたMFAトークンもメモしておく必要があります。

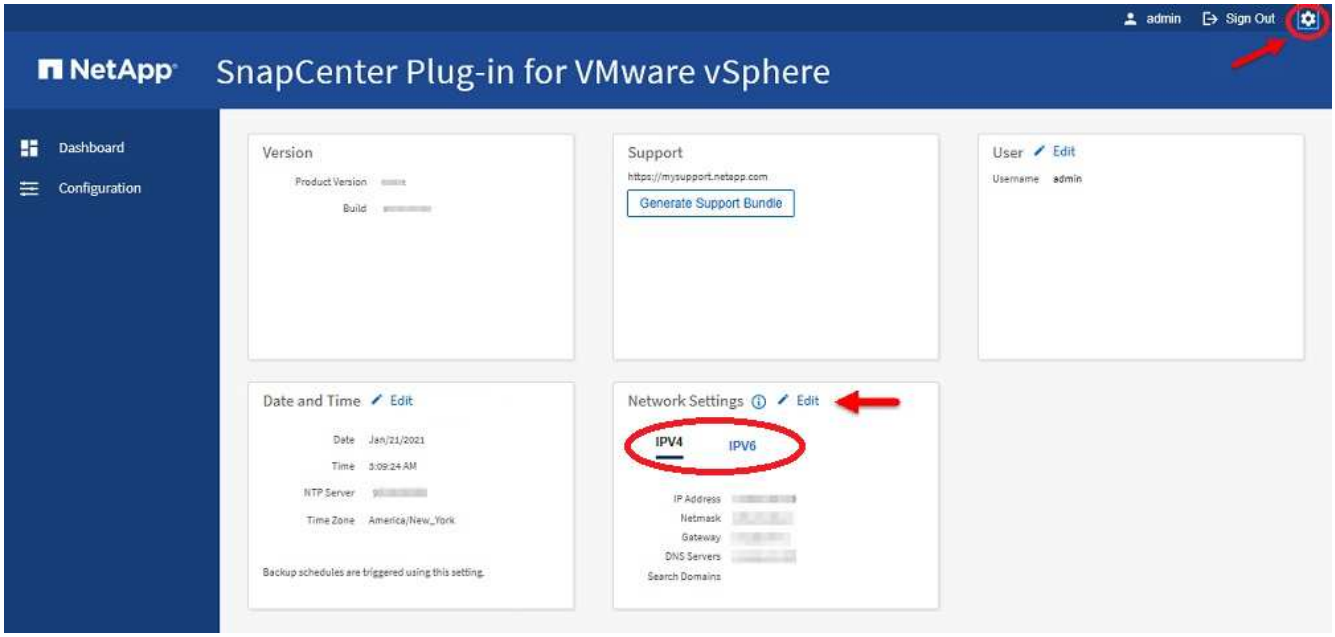
- このIPアドレスは、SnapCenter Plug-in for VMware vSphereの導入時に表示されたものです。
- SnapCenter Plug-in for VMware vSphereの導入時に指定したログイン クレデンシャル、またはあとで変更したログイン クレデンシャルを使用します。
- メンテナンス コンソールのシステム構成オプションを使用して、6桁のMFAトークンを生成します。

手順

1. SnapCenter Plug-in for VMware vSphere管理GUIにログインします。

   フォーマットを使用する `https://<appliance-IP-address>:8080`

2. 上部のツールバーにある設定アイコンを選択します。



3. *設定*ページの*ネットワーク設定*セクションで、*IPv4*または*IPv6*アドレスを選択し、*編集*を選択します。

   新しい情報を入力し、「保存」を選択します。

4. ネットワーク設定を削除する場合は、次の手順を実行します。
   - IPv4: **IP**アドレス*フィールドに入力します `**0.0.0.0**`次に、**[***保存]を選択します。
   - IPv6: **IP**アドレス*フィールドに入力します `**: :0**`次に、**[***保存]を選択します。

IPv4 アドレスと IPv6 アドレスの両方を使用している場合は、両方のネットワーク設定を削除することはできません。残っているネットワークでは、[DNS Servers]フィールドと[Search Domains]フィールドを指定する必要があります。

設定のデフォルト値の変更

運用効率を向上させるには、 `scbr.override`デフォルト値を変更するには、構成ファイルを使用します。これらの値は、バックアップの実行時に作成または削除するVMwareスナップショットの数や、バックアップ スクリプトの実行を中止するまでの時間などの設定を制御します。

その `scbr.override`構成ファイルは、 SnapCenterアプリケーション ベースのデータ保護操作をサポートする環境で、 SnapCenter Plug-in for VMware vSphereによって使用されます。このファイルが存在しない場合は、テンプレート ファイルから作成する必要があります。

scbr.override構成ファイルの作成

その `scbr.override`構成ファイルは、 SnapCenterアプリケーション ベースのデータ保護操作をサポートする環境で、 SnapCenter Plug-in for VMware vSphereによって使用されます。

1. へ移動 `/opt/netapp/scvservice/standalone_aegis/etc/scbr/scbr.override-template`。
2. コピー `scbr.override-template`ファイルを新しいファイルに `scbr.override`の中で `\opt\netapp\scvservice\standalone_aegis\etc\scbr`ディレクトリ。

上書き可能なプロパティ

にリストされているプロパティを使用できます `scbr.override`デフォルト値を変更するには、構成ファイルを使用します。

- デフォルトのテンプレートでは、ハッシュ記号により設定プロパティがコメント化されています。プロパティを使用して構成値を変更するには、 `#`文字。
- 変更を有効にするには、SnapCenter Plug-in for VMware vSphereホスト上のサービスを再起動する必要があります。

以下のプロパティを使用できます。 `scbr.override`デフォルト値を変更するには、構成ファイルを使用します。

- ダッシュボード保護された**VM**カウント間隔**=7**

  ダッシュボードにVMの保護ステータスが表示される日数です。

  デフォルト値は「7」です。

- **disable.weakCiphers=true**

  SnapCenter Plug-in for VMware vSphereとSnapCenter間の通信チャネルの次の weakCipher と、以下にリ

ストされている追加の weakCipher を無効にします。 `include.weakCiphers`：TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384

- グローバル**.ds.**除外パターン

  バックアップ処理から除外する従来のデータストアまたはvVolデータストアを1つ以上指定します。データストアは、有効なJava正規表現を使用して指定できます。

  例1: 式 `global.ds.exclusion.pattern=.*21`共通のパターンを持つデータストアを除外します。例: `datastore21`そして `dstest21`除外されます。

  例2: 式 `global.ds.exclusion.pattern=ds-.*|^vol123`を含むすべてのデータストアを除外します `ds-（例えば scvds-test）または vol123。

- **guestFileRestore.guest.operation.interval=5**

  SnapCenter Plug-in for VMware vSphereがゲスト（オンライン ディスクとリストア ファイル）でのゲスト処理の完了を監視する時間（秒）です。合計待ち時間は、`guestFileRestore.online.disk.timeout`そして `guestFileRestore.restore.files.timeout。

  デフォルト値は「5」です。

- ゲストファイルリストア**.**監視間隔**=30**

  SnapCenter Plug-in for VMware vSphereが期限切れゲスト ファイル リストア セッションを監視する時間（分）です。設定されたセッション時間を超えて実行されているセッションはすべて切断されます。

  デフォルト値は「30」です。

- **guestFileRestore.online.disk.timeout=100**

  SnapCenter Plug-in for VMware vSphereがゲストVMでのオンライン ディスク処理が完了するまで待機する時間（秒）です。プラグインがオンライン ディスク処理の完了をポーリングするまでに、さらに30秒の待機時間があります。

  デフォルト値は「100」です。

- **guestFileRestore.restore.files.timeout=3600**

  SnapCenter Plug-in for VMware vSphereがゲストVMでのファイルのリストア処理が完了するまで待機する時間（秒）です。この時間を超過するとプロセスは終了され、ジョブは失敗としてマークされます。

  デフォルト値は「3600」（1時間）です。

- **guestFileRestore.robocopy.directory.flags=/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /e /NJH /NDL /NP**

  ゲスト ファイルのリストア処理中に、ディレクトリをコピーする際に使用される追加のRobocopyフラグです。

  削除しないでください `/NJH`または追加 `/NJS`復元出力の解析が壊れるからです。

無制限の再試行を許可しない（`/R`フラグ) を使用すると、失敗したコピーの再試行が無限に発生する可能性があります。

デフォルト値は `"/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /e /NJH /NDL /NP"`。

- **guestFileRestore.robocopy.file.flags=/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /NJH /NDL /NP**

  ゲスト ファイルのリストア処理中に、個々のファイルをコピーする際に使用される追加のRobocopyフラグです。

  削除しないでください `/NJH`または追加 `/NJS`復元出力の解析が壊れるからです。

  無制限の再試行を許可しない（`/R`フラグ) を使用すると、失敗したコピーの再試行が無限に発生する可能性があります。

  デフォルト値は `"/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /NJH /NDL /NP"`。

- ゲストファイルリストア.セッションタイム**=1440**

  SnapCenter Plug-in for VMware vSphereがゲスト ファイル リストア セッションをアクティブにしておく時間（分）です。

  デフォルト値は「1440」（24時間）です。

- **guestFileRestore.use.custom.online.disk.script=true**

  ゲスト ファイル リストア セッションの作成時に、ディスクのオンライン化とドライブ レターの取得のためにカスタム スクリプトを使用するかどうかを指定します。スクリプトは次の場所に置く必要があります `[Install Path] \etc\guestFileRestore_onlineDisk.ps1`。デフォルトのスクリプトがインストール時に配置されています。価値観 `[Disk_Serial_Number]`、 `[Online_Disk_Output]` 、 そして `[Drive_Output]`アタッチプロセス中にスクリプト内で置き換えられます。

  デフォルト値は「false」です。

- **include.esx.initiator.id.from.cluster=true**

  VMDKワークフローを介したアプリケーションで、クラスタ内のすべてのESXiホストのiSCSIイニシエータとFCPイニシエータのIDをSnapCenter Plug-in for VMware vSphereに含めるように指定します。

  デフォルト値は「false」です。

- **include.weakCiphers**

  いつ `disable.weakCiphers`設定されている `true`は、無効にする弱い暗号と、 `disable.weakCiphers`デフォルトでは無効になっています。

- 最大同時**DS**ストレージクエリ数**=15**

  SnapCenter Plug-in for VMware vSphereがデータストアのストレージ容量を検出するためにSnapCenter Serverに対して実行できる同時呼び出しの最大数です。これらの呼び出しは、SnapCenter Plug-in for VMware vSphereのVMホストでLinuxサービスを再起動すると、プラグインによって実行されます。

- **nfs.**データストアのマウント再試行回数**=3**

SnapCenter Plug-in for VMware vSphereがvCenterでボリュームをNFSデータストアとしてマウントする際の最大試行回数です。

デフォルト値は「3」です。

- **nfs.datastore.mount.retry.delay=60000**

  SnapCenter Plug-in for VMware vSphereがvCenterでボリュームをNFSデータストアとしてマウントする際の試行間隔（ミリ秒）です。

  デフォルト値は「60000」（60秒）です。

- **script.virtual.machine.count.variable.name=VIRTUAL_MACHINES**

  仮想マシンの数を含む環境変数の名前です。この変数は、バックアップ ジョブ時にユーザ定義スクリプトを実行する場合に必ず定義する必要があります。

  たとえば、VIRTUAL_MACHINES=2と指定した場合、2台の仮想マシンがバックアップされます。

- **script.virtual.machine.info.variable.name=VIRTUAL_MACHINE.%s**

  バックアップのn台目の仮想マシンに関する情報を含む環境変数の名前です。この変数は、バックアップ時にユーザ定義スクリプトを実行する場合に必ず定義する必要があります。

  たとえば、環境変数VIRTUAL_MACHINE.2は、バックアップの2台目の仮想マシンに関する情報を提供します。

- **script.virtual.machine.info.format= %s|%s|%s|%s|%s**

  仮想マシンに関する情報を提供します。環境変数で設定されるこの情報の形式は次のとおりです。 `VM name|VM UUID| VM power state (on|off)|VM snapshot taken (true|false)|IP address(es)`

  指定できる情報の例を次に示します。

  ```
  VIRTUAL_MACHINE.2=VM 1|564d6769-f07d-6e3b-
  68b1f3c29ba03a9a|POWERED_ON||true|10.0.4.2
  ```

- ストレージ接続タイムアウト**=600000**

  SnapCenter Serverがストレージ システムからの応答を待つ時間（ミリ秒）です。

  デフォルト値は「600000」（10分）です。

- **vmware.esx.ip.kernel.ip.map**

  デフォルト値はありません。この値は、ESXiホストのIPアドレスをVMkernel IPアドレスにマップするために使用します。デフォルトでは、SnapCenter Plug-in for VMware vSphereはESXiホストの管理VMkernelアダプタIPアドレスを使用します。SnapCenter Plug-in for VMware vSphereで別のVMkernelアダプタIPアドレスを使用する場合は、上書きする値を指定する必要があります。

  次の例では、管理 VMkernel アダプタの IP アドレスは 10.225.10.56 ですが、 SnapCenter Plug-in for VMware vSphereは指定されたアドレス 10.225.11.57 および 10.225.11.58 を使用します。管理VMkernelアダプタIPアドレスが10.225.10.60の場合、プラグインではアドレス10.225.11.61が使用されます。

```
vmware.esx.ip.kernel.ip.map=10.225.10.56:10.225.11.57,10.225.11.58;
10.225.10.60:10.225.11.61
```

- **vmware.max.concurrent.snapshots=30**

  SnapCenter Plug-in for VMware vSphereがサーバで実行できる同時VMwareスナップショットの最大数です。

  この数は、ポリシーで[VM consistent]が選択されている場合にのみ、データストア単位でチェックされます。クラッシュ整合性バックアップを実行する場合、この設定は適用されません。

  デフォルト値は「30」です。

- **vmware.max.concurrent.snapshots.delete=30**

  SnapCenter Plug-in for VMware vSphereがサーバで実行できる同時VMware Snapshot削除処理の、データストアあたりの最大数です。

  この数はデータストア単位でチェックされます。

  デフォルト値は「30」です。

- **vmware.query.unresolved.retry.count=10**

  SnapCenter Plug-in for VMware vSphereが、「…time limit for holding off I/O…」エラーが原因で未解決のボリュームに関するクエリの送信を再試行する最大回数です。

  デフォルト値は「10」です。

- **vmware.quiesce.retry.count=0**

  SnapCenter Plug-in for VMware vSphereが、バックアップ中の「…time limit for holding off I/O…」エラーが原因でVMwareスナップショットに関するクエリの送信を再試行する最大回数です。

  デフォルト値は「0」です。

- **vmware.quiesce.retry.interval=5**

  SnapCenter Plug-in for VMware vSphereが、バックアップ中の「…time limit for holding off I/O…」エラーが原因でVMwareスナップショットに関するクエリを送信する間隔（秒）です。

  デフォルト値は「5」です。

- **vmware.query.unresolved.retry.delay= 60000**

  SnapCenter Plug-in for VMware vSphereが、「…time limit for holding off I/O…」エラーが原因で未解決のボリュームに関するクエリを送信する間隔（ミリ秒）です。このエラーは、VMFSデータストアのクローンを作成する際に発生します。

  デフォルト値は「60000」（60秒）です。

- **vmware.reconfig.vm.**再試行回数**=10**

  SnapCenter Plug-in for VMware vSphereが、「…time limit for holding off I/O…」エラーが原因でVMの再

設定に関するクエリの送信を再試行する最大回数です。

デフォルト値は「10」です。

- **vmware.reconfig.vm.retry.delay=30000**

  SnapCenter Plug-in for VMware vSphereが、「…time limit for holding off I/O…」エラーが原因でVMの再設定に関するクエリを送信する間隔（ミリ秒）です。

  デフォルト値は「30000」（30秒）です。

- **vmware.rescan.hba.**再試行回数**=3**

  SnapCenter Plug-in for VMware vSphereが、「…time limit for holding off I/O…」エラーが原因でホスト バス アダプタの再スキャンに関するクエリを送信する間隔（ミリ秒）です。

  デフォルト値は「3」です。

- **vmware.rescan.hba.retry.delay=30000**

  SnapCenter Plug-in for VMware vSphereが、ホスト バス アダプタの再スキャン要求を再試行する最大回数です。

  デフォルト値は「30000」です。

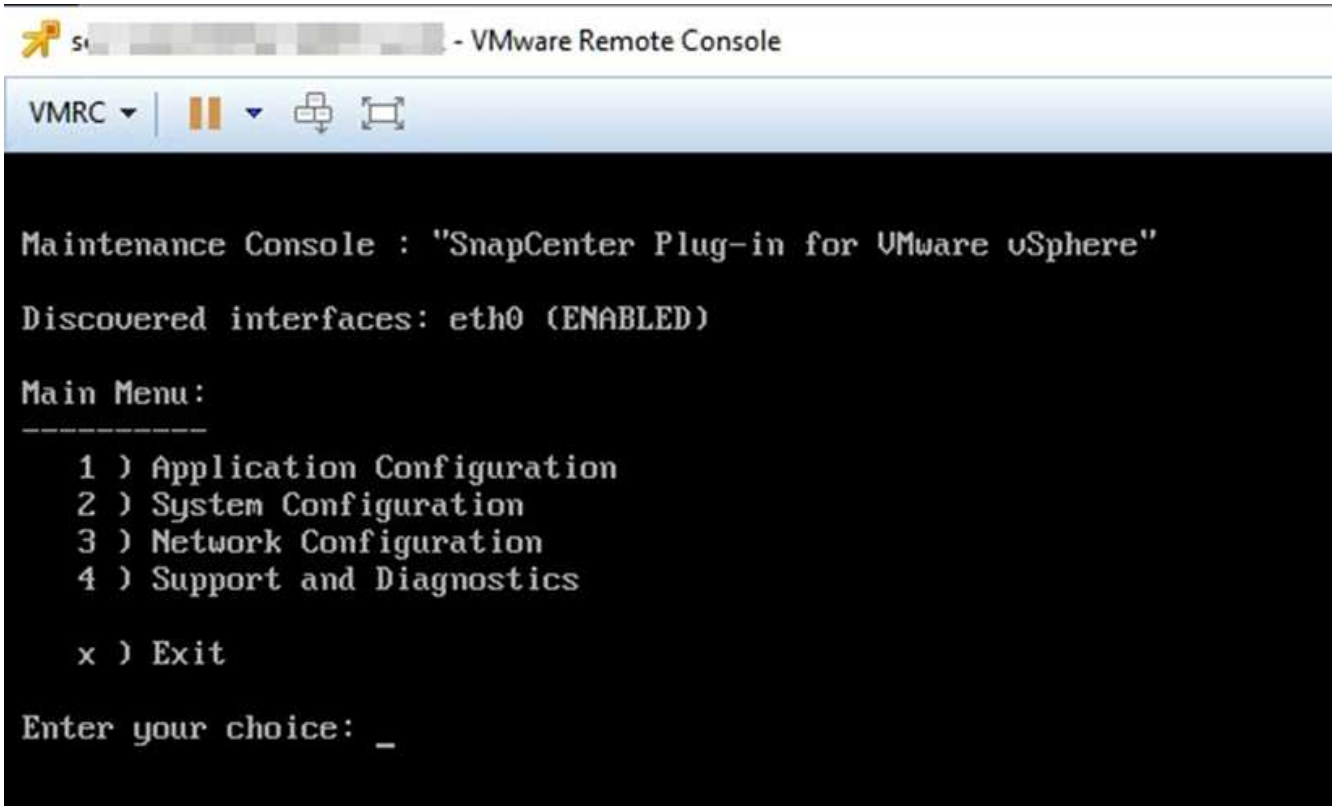
SnapCenter Plug-in for VMware vSphere用のSSHの有効化

SnapCenter Plug-in for VMware vSphereの導入時、SSHはデフォルトで無効になっています。

手順

1. VMware vSphere Clientで、SnapCenter Plug-in for VMware vSphereが配置されているVMを選択します。
2. 仮想アプライアンスの 概要 タブで リモート コンソールの起動 を選択してメンテナンス コンソール ウィンドウを開き、ログオンします。

   メンテナンスコンソールへのアクセスとログインについては、以下を参照してください。"メンテナンスコンソールにアクセスする" 。



3. メインメニューから、メニューオプション*2) システム構成*を選択します。
4. システム構成メニューから、メニュー オプション **6) SSH** アクセスを有効にする を選択し、確認プロンプトで「**y**」と入力します。
5. 「SSH アクセスを有効にしています…」というメッセージが表示されるまで待ち、**Enter** キーを押して続行し、プロンプトで **X** と入力してメンテナンス モードを終了します。

REST API

概要

SnapCenter Plug-in for VMware vSphere REST APIを使用して、一般的なデータ保護処理を実行できます。このプラグインのSwagger Webページは、Windows SnapCenterのSwagger Webページとは異なります。

- VMware vSphere用のREST APIを使用した、VMおよびデータストアに対する次の処理のREST APIワークフローについて説明します。
  - Storage VMおよびクラスタの追加、変更、削除
  - リソース グループの作成、変更、削除
  - VMのスケジュールされたバックアップおよびオンデマンド バックアップ
  - 既存のVMおよび削除されたVMのリストア
  - VMDKのリストア
  - VMDKの接続および接続解除
  - データストアのマウントとアンマウント
  - ジョブのダウンロードおよびレポートの生成
  - 組み込みのスケジュールの変更
  - ASA r2の二次保護を構成する
- VMware vSphere用のREST APIでサポートされない処理
  - ゲスト ファイルのリストア
  - SnapCenter Plug-in for VMware vSphereのインストールおよび設定
  - ユーザへのRBACロールまたはアクセスの割り当て
- `uri`パラメータ

  その `uri`パラメータは常に「null」値を返します。

- ログイン タイムアウト

  デフォルトのタイムアウトは120分（2時間）です。vCenterの設定で別のタイムアウト値を設定できます。

- トークン管理

  セキュリティ上の理由から、REST APIは必須トークンを使用します。必須トークンは各要求で渡され、すべてのAPI呼び出しでクライアント検証に使用されます。VMware vSphere用のREST APIでは、VMware認証APIを使用してトークンを取得します。VMwareではトークンを管理できます。

  トークンを取得するには、 `/4.1/auth/login` REST API を使用して vCenter の資格情報を提供します。

- APIのバージョン指定

各REST API名には、そのREST APIが最初にリリースされたSnapCenterのバージョン番号が含まれています。例えば、REST API `/4.1/datastores/{moref}/backups` SnapCenter 4.1 で初めてリリースされました。

今後のリリースのREST APIは通常、後方互換性があり、必要に応じて新機能に対応するように変更されます。

Swagger API Webページを使用したREST APIへのアクセス

REST APIはSwagger Webページから利用できます。SnapCenter ServerまたはSnapCenter Plug-in for VMware vSphereのREST APIを表示する場合、およびAPIを手動で呼び出す場合は、Swagger Webページにアクセスします。VMとデータストアに対して処理を実行するには、SnapCenter Plug-in for VMware vSphere REST APIを使用します。

このプラグインのSwagger Webページは、SnapCenter ServerのSwagger Webページとは異なります。

開始する前に

SnapCenter Plug-in for VMware vSphere REST APIの場合は、SnapCenter Plug-in for VMware vSphereのIPアドレスまたはホスト名を確認する必要があります。

> このプラグインでは、サードパーティ製アプリケーションとの統合を目的としたREST APIのみがサポートされており、PowerShellコマンドレットやCLIはサポートされていません。

手順

1. ブラウザで、次のURLを入力してプラグインのSwagger Webページにアクセスします。

   ```
   https://<SCV_IP>:8144/api/swagger-ui/index.html
   ```

   > REST API URL では次の文字を使用しないでください: +、.、%、&

   例

   SnapCenter Plug-in for VMware vSphereのREST APIにアクセスします。

   ```
   https://<SCV_IP>:8144/api/swagger-ui/index.html
   ```

   ```
   https://OVAhost:8144/api/swagger-ui/index.html
   ```

   ログインし、vCenter認証メカニズムを使用して、トークンを生成します。

2. API リソース タイプを選択すると、そのリソース タイプ内の API が表示されます。

Storage VMを追加および変更するためのREST APIのワークフロー

SnapCenter Plug-in for VMware vSphere REST APIを使用してStorage VMの追加処理お

よび変更処理を実行するには、所定の順序でREST API呼び出しを実行する必要があります。

各REST APIごとに、 `https://<server>:<port>` REST API の先頭に追加して、完全なエンドポイントを形成します。

Storage VMを追加するには、次のワークフローを実行します。

手順	**REST API**	コメント
1	`/4.1/storage-system`	`Add Storage System`指定されたストレージ VM をSnapCenter Plug-in for VMware vSphere に追加します。

Storage VMを変更するには、次のワークフローを実行します。

手順	**REST API**	コメント
1	`/4.1/storage-system`	`getSvmAll`利用可能なすべてのストレージ VM のリストを取得します。変更するストレージ VM の 名前 をメモします。
2	`/4.1/storage-system`	`Modify Storage System`指定されたストレージ VM を変更します。他のすべての必須属性に加えて、ステップ 1 の **name** を渡します。

リソース グループを作成および変更するための**REST API**のワークフロー

SnapCenter Plug-in for VMware vSphere REST APIを使用してリソース グループの作成処理および変更処理を実行するには、所定の順序でREST API呼び出しを実行する必要があります。

各REST APIごとに、 `https://<server>:<port>` REST API の先頭に追加して、完全なエンドポイントを形成します。

リソース グループを作成するには、次のワークフローを実行します。

手順	**REST API**	コメント
1	`/4.1/policies`	`Get Policies`VMware vSphere クライアント ポリシーのリストを取得します。リソース グループとポリシーの **frequency** を作成するときに使用する **policyId** をメモします。ポリシーがリストされていない場合は、 `Create Policy`新しいポリシーを作成するための REST API。

手順	**REST API**	コメント
2	`/4.1/resource-groups`	`Create a Resource Group`指定されたポリシーを持つリソース グループを作成します。ステップ 1 の **policyId** を渡し、その他すべての必須属性に加えて、ポリシーの **freqency** の詳細を入力します。この REST API を使用して二次保護を有効にすることができます。

リソース グループを変更するには、次のワークフローを実行します。

手順	**REST API**	コメント
1	`/4.1/resource-groups`	`Get List of Resource Groups`VMware vSphere クライアント リソース グループのリストを取得します。変更する **resourceGroupId** をメモします。
2	`/4.1/policies`	割り当てられたポリシーを変更する場合は、 `Get Policies` VMware vSphere クライアント ポリシーのリストを取得します。リソース グループとポリシーの 頻度を変更するときに使用する **policyId** をメモします。
3	`/4.1/resource-groups/{resouceGroupId}`	`Update a Resource Group`指定されたリソース グループを変更します。ステップ 1 の **resourceGroupId** を渡します。オプションで、ステップ 2 の **policyId** を渡し、その他すべての必須属性に加えて **frequency** の詳細を入力します。

オンデマンドでバックアップするための**REST API**のワークフロー

SnapCenter Plug-in for VMware vSphere REST APIを使用してバックアップ処理をオンデマンドで実行するには、所定の順序でREST API呼び出しを実行する必要があります。

各REST APIごとに、 `https://<server>:<port>` REST API の先頭に追加して、完全なエンドポイントを形成します。

手順	REST API	コメント
1	`/4.1/resource-groups`	`Get List of Resource Groups`VMware vSphere クライアント リソース グループのリストを取得します。バックアップするリソース グループの **resourceGroupId** と **policyId** をメモします。
2	`/4.1/resource-groups/backupnow`	`Run a backup on a Resource Group`オンデマンドでリソース グループをバックアップします。ステップ 1 の **resourceGroupId** と **policyId** を渡します。

VMをリストアするためのREST APIのワークフロー

SnapCenter Plug-in for VMware vSphere REST APIを使用してVMバックアップのリストア処理を実行するには、所定の順序でREST API呼び出しを実行する必要があります。

各REST APIごとに、 `https://<server>:<port>` REST API の先頭に追加して、完全なエンドポイントを形成します。

手順	REST API	コメント
1	へ移動 `http://<vCenter-IP>/mob`	VMware管理オブジェクトのURLからVMのmorefを見つけます。復元する VM の **moref** をメモします。
2	`/4.1/vm/{moref}/backups`	`Get VM Backups`指定された VM のバックアップのリストを取得します。ステップ 1 の **moref** を渡します。復元するバックアップの **backupId** をメモします。
3	`/4.1/vm/backups/{backupId}/snapshotlocations`	`Get snapshot locations`指定されたバックアップのスナップショットの場所を取得します。ステップ 2 の **backupId** を渡します。**snapshotLocationsList** 情報をメモします。
4	`/4.1/vm/{moref}/backups/availableesxhosts`	`Get available ESX Hosts`バックアップが保存されているホストの情報を取得します。**availableEsxHostsList** 情報をメモします。

手順	REST API	コメント
5	`/4.1/vm/{moref}/backups/{backupId}/restore`	`Restore a VM from a backup`指定されたバックアップを復元します。手順 3 と 4 の情報を **restoreLocations** 属性に渡します。 VMバックアップが部分バックアップの場合は、`restartVM`パラメータを「false」に設定します。 テンプレートであるVMはリストアできません。

削除された**VM**をリストアするための**REST API**のワークフロー

SnapCenter Plug-in for VMware vSphere REST APIを使用してVMバックアップのリストア処理を実行するには、所定の順序でREST API呼び出しを実行する必要があります。

各REST APIごとに、 `https://<server>:<port>` REST API の先頭に追加して、完全なエンドポイントを形成します。

手順	REST API	コメント
1	へ移動 `http://<vCenter-IP>/mob`	VMware管理オブジェクトのURLからVMのUUIDを見つけます。復元する VM の **uuid** をメモします。
2	`/4.1/vm/{uuid}/backups`	`Get VM Backups`指定された VM のバックアップのリストを取得します。ステップ 1 の **uuid** を渡します。復元するバックアップの **backupId** をメモします。
3	`/4.1/vm/backups/{backupId}/snapshotlocations`	`Get snapshot locations`指定されたバックアップのスナップショットの場所を取得します。ステップ 2 の **backupId** を渡します。**snapshotLocationsList** 情報をメモします。
4	`/4.1/vm/{moref}/backups/availableesxhosts`	`Get available ESX Hosts`バックアップが保存されているホストの情報を取得します。**availableEsxHostsList** 情報をメモします。

手順	REST API	コメント
5	`/4.1/vm/{uuid}/backups/{backupId}/restore`	`Restore VM from a backup using uuid or restore a deleted VM`指定されたバックアップを復元します。ステップ 1 の **uuid** を渡します。ステップ 2 の **backupId** を渡します。手順 3 と 4 の情報を **restoreLocations** 属性に渡します。 VMバックアップが部分バックアップの場合は、 `restartVM`パラメータを「false」に設定します。注意: テンプレートである VM を復元することはできません。

VMDKをリストアするための**REST API**のワークフロー

SnapCenter Plug-in for VMware vSphere REST APIを使用してVMDKのリストア処理を実行するには、所定の順序でREST API呼び出しを実行する必要があります。

各REST APIごとに、 `https://<server>:<port>` REST API の先頭に追加して、完全なエンドポイントを形成します。

手順	REST API	コメント
1	へ移動 `http://<vCenter-IP>/mob`	VMware管理オブジェクトのURLからVMのmorefを見つけます。VMDK が配置されている VM の **moref** に注意してください。
2	`/4.1/vm/{moref}/backups`	`Get VM Backups`指定された VM のバックアップのリストを取得します。ステップ 1 の **moref** を渡します。復元するバックアップの **backupId** をメモします。
3	`/4.1/vm/backups/{backupId}/snapshotlocations`	`Get snapshot locations`指定されたバックアップのスナップショットの場所を取得します。ステップ 2 の **backupId** を渡します。 **snapshotLocationsList** 情報をメモします。
4	`/4.1/vm/{moref}/backups/vmdklocations`	`Get Vmdk Locations`指定された VM の VMDK のリストを取得します。 **vmdkLocationsList** 情報をメモします。

手順	REST API	コメント
5	`/4.1/vm/{ moref}/backups/{backupId}/availabledatastores`	`Get Available Datastores`復元操作に使用できるデータストアのリストを取得します。ステップ 1 の **moref** を渡します。ステップ 2 の **backupId** を渡します。**DatastoreNameList** 情報をメモします。
6	`/4.1/vm/{moref}/backups/availableesxhosts`	`Get available ESX Hosts`バックアップが保存されているホストの情報を取得します。ステップ 1 の **moref** を渡します。**availableEsxHostsList** 情報をメモします。
7	`/4.1/vm/{moref}/backups/{backupId}/restorevmdks`	`Restore a VMDK from a backup`指定されたバックアップから指定された VMDK を復元します。**esxHost** 属性に、手順 6 の **availableEsxHostsList** の情報を渡します。手順 3 から 5 の情報を **vmdkRestoreLocations** 属性に渡します。 • restoreFromLocation属性に、手順3でメモしたsnapshotLocationsListの情報を渡します。 • vmdkToRestore属性に、手順4でメモしたvmdkLocationsListの情報を渡します。 • restoreToDatastore属性に、手順5でメモしたDatastoreNameListの情報を渡します。

VMDKを接続および接続解除するためのREST APIのワークフロー

SnapCenter Plug-in for VMware vSphere REST APIを使用してVMDKの接続処理および接続解除処理を実行するには、所定の順序でREST API呼び出しを実行する必要があります。

各REST APIごとに、 `https://<server>:<port>` REST API の先頭に追加して、完全なエンドポイントを形成します。

VMDKを接続するには、次のワークフローを実行します。

手順	REST API	コメント
1	へ移動 `http://<vCenter-IP>/mob`	VMware管理オブジェクトのURLからVMのmorefを見つけます。VMDK を接続する VM の **moref** をメモします。
2	`/4.1/vm/{moref}/backups`	`Get VM Backups`指定された VM のバックアップのリストを取得します。ステップ 1 の **moref** を渡します。復元するバックアップの **backupId** をメモします。
3	`/4.1/vm/{moref}/backups/{backupId}/vmdklocations`	`Get VMDK Locations`指定された VM の VMDK のリストを取得します。ステップ 2 の **backupId** とステップ 1 の **moref** を渡します。**vmdkLocationsList** 情報をメモします。
4	`/4.1/vm/{moref}/attachvmdks`	`Attach VMDKs`指定された VMDK を元の VM に接続します。ステップ 2 の **backupId** とステップ 1 の **moref** を渡します。手順 3 の **vmdkLocationsList** を **vmdkLocations** 属性に渡します。 VMDKを別のVMに接続するには、alternateVmMoref属性にターゲットVMのmorefを渡します。

VMDKの接続を解除するには、次のワークフローを実行します。

手順	REST API	コメント
1	へ移動 `http://<vCenter-IP>/mob`	VMware管理オブジェクトのURLからVMのmorefを見つけます。VMDK をデタッチする VM の **moref** をメモします。
2	`/4.1/vm/{moref}/backups`	`Get VM Backups`指定された VM のバックアップのリストを取得します。ステップ 1 の **moref** を渡します。復元するバックアップの **backupId** をメモします。

手順	REST API	コメント
3	`/4.1/vm/{moref}/backups/{backupId}/vmdklocations`	`Get VMDK Locations`指定された VM の VMDK のリストを取得します。ステップ 2 の **backupId** とステップ 1 の **moref** を渡します。**vmdkLocationsList** 情報をメモします。
4	`/4.1/vm/{moref}/detachvmdks`	`Detach VMDKs`指定された VMDK をデタッチします。ステップ 1 の **moref** を渡します。手順 3 の VMDK **vmdkLocationsList** の詳細を **vmdksToDetach** 属性に渡します。

データストアをマウントおよびアンマウントするための**REST API**のワークフロー

SnapCenter Plug-in for VMware vSphere REST APIを使用してデータストアのバックアップのマウント処理およびアンマウント処理を実行するには、所定の順序でREST API呼び出しを実行する必要があります。

各REST APIごとに、 `https://<server>:<port>` REST API の先頭に追加して、完全なエンドポイントを形成します。

データストアをマウントするには、次のワークフローを実行します。

手順	REST API	コメント
1	へ移動 `http://<vCenter-IP>/mob`	VMware管理オブジェクトのURLからデータストアのmorefを見つけます。マウントするデータストアの **moref** をメモします。
2	`/4.1/datastores/{moref}/backups`	`Get the list of backups for a datastore`指定されたデータストアのバックアップのリストを取得します。ステップ 1 の **moref** を渡します。マウントする **backupId** をメモします。
3	`/4.1/datastores/backups/{backupId}/snapshotlocators`	`Get the list of Snapshot Locations`指定されたバックアップの場所に関する詳細を取得します。ステップ 2 の **backupId** を渡します。**datastore** と **snapshotLocationsList** リストの場所をメモします。

手順	REST API	コメント
4	`/4.1/datastores/{moref}/availableEsxHosts`	`Get the list of Available Esxi Hosts` マウント操作に使用できる ESXi ホストのリストを取得します。ステップ 1 の **moref** を渡します。 **availableEsxHostsList** 情報をメモします。
5	`/4.1/datastores/backups/{backupId}/mount`	`Mount datastores for a backup`指定されたデータストアのバックアップをマウントします。ステップ 2 の **backupId** を渡します。 **datastore** 属性と **location** 属性には、次の情報を渡します。 `snapshotLocationsList`ステップ3で。 **esxHostName** 属性に、手順 4 の **availableEsxHostsList** の情報を渡します。

データストアをアンマウントするには、次のワークフローを実行します。

手順	REST API	コメント
1	`/4.1/datastores/backups/{backupId}/mounted`	`Get the list of mounted datastores` 。アンマウントするデータストア **moref** をメモします。
2	`/4.1/datastores/unmount`	`UnMount datastores for a backup` 指定されたデータストアのバックアップをアンマウントします。ステップ 1 からデータストアの **moref** を渡します。

ジョブのダウンロードおよびレポートの生成を行うための**REST API**

SnapCenter Plug-in for VMware vSphere REST APIを使用してVMware vSphere Clientジョブのレポートの生成およびログのダウンロードを行うには、VMware vSphere用のREST API呼び出しを使用する必要があります。

各REST APIごとに、 `https://<server>:<port>` REST API の先頭に追加して、完全なエンドポイントを形成します。

ジョブの詳細情報を取得するには、**[Jobs]**セクションの次の**REST API**を使用します。

REST API	コメント
`/4.1/jobs`	`Get all jobs`複数のジョブのジョブ詳細を取得します。ジョブタイプを指定することでリクエストの範囲を絞り込むことができます。 `backup`、`mountBackup`、 または `restore`。
`/4.1/jobs/{id}`	`Get job details`指定されたジョブの詳細情報を取得します。

[Jobs]セクションの次の**REST API**を使用して、ジョブのログをダウンロードします。

REST API	コメント
`/4.1/jobs/{id}/logs`	`getJobLogsById`指定されたジョブのログをダウンロードします。

レポートを生成するには、**[Reports]**セクションの次の**REST API**を使用します。

REST API	コメント
`4.1/reports/protectedVM`	`Get Protected VM List`過去 7 日間に保護された VM のリストを取得します。
`/4.1/reports/unProtectedVM`	`Get Unprotected VM List`過去 7 日間に保護されていない VM のリストを取得します。

組み込みスケジュールを変更する**REST API**ワークフロー

SnapCenter Plug-in for VMware vSphere REST APIを使用してVMware vSphere Clientジョブの組み込みスケジュールを変更するには、所定の順序でREST API呼び出しを実行する必要があります。

組み込みスケジュールとは、MySQLデータベースのダンプ スケジュールなど、製品の一部として提供されるスケジュールです。次のスケジュールを変更できます。

```
Schedule-DatabaseDump
Schedule-PurgeBackups
Schedule-AsupDataCollection
Schedule-ComputeStorageSaving
Schedule-PurgeJobs
```

各REST APIごとに、 `https://<server>:<port>` REST API の先頭に追加して、完全なエンドポイントを形成します。

手順	REST API	コメント
1	`/4.1/schedules`	`Get all built-in`スケジュールは、製品に元々提供されていたジョブ スケジュールのリストを取得します。変更するスケジュール名と、関連付けられているcron式をメモします。
2	`/4.1/schedules`	`Modify any built-in schedule`名前付きスケジュールを変更します。手順1でメモしたスケジュール名を渡し、そのスケジュールの新しいcron式を作成します。

スタック ジョブを失敗としてマークするための**REST API**

SnapCenter Plug-in for VMware vSphere REST APIを使用してVMware vSphere ClientジョブのジョブIDを調べるには、VMware vSphere用のREST API呼び出しを使用する必要があります。これらのREST APIは、SnapCenter Plug-in for VMware vSphere 4.4で追加されました。

各 REST API の先頭に https://<server>:<port>` を追加して、完全なエンドポイントを形成します。

実行中状態でスタックしているジョブを失敗状態に変更するには、[Jobs]セクションの次のREST APIを使用します。

REST API	コメント
`/4.1/jobs/{id}/failJobs`	実行状態のままになっているジョブのIDを渡すと、`failJobs`これらのジョブを失敗としてマークします。実行中状態でスタックしているジョブを特定するには、ジョブ監視GUIを使用してすべてのジョブの状態とジョブIDを確認します。

監査ログを生成するための**REST API**

監査ログの詳細は、Swagger REST APIおよびSCVプラグインのユーザ インターフェイスから収集できます。

次に、Swagger REST APIを示します。

1. GET 4.1/audit/logs: すべてのログの監査データを取得する
2. GET 4.1/audit/logs/{filename}: 特定のログファイルの監査データを取得します
3. POST 4.1/audit/verify: 監査ログの検証をトリガーします。
4. GET 4.1/audit/config: 監査および syslog サーバーの設定を取得します。
5. PUT 4.1/audit/config: 監査およびSyslogサーバーの設定を更新します

SnapCenter Plug-in for VMware vSphere REST APIを使用してVMware vSphere Clientジョブの監査ログを生成するには、VMware vSphere用のREST API呼び出しを使用する必要があります。

各REST APIごとに、 `https://<server>:<port>/api` REST API の先頭に追加して、完全なエンドポイントを形成します。

ジョブの詳細情報を取得するには、[Jobs]セクションの次のREST APIを使用します。

REST API	コメント
`4.1/audit/logs`	整合性データを含む監査ログ ファイルを返します
`4.1/audit/logs/{filename}`	整合性データを含む特定の監査ログ ファイルを取得します
`4.1/audit/verify`	監査の検証をトリガーします
`4.1/audit/syslogcert`	syslogサーバ証明書を更新します

Upgrade

以前のリリースのSnapCenter Plug-in for VMware vSphereからのアップグレード

> SCV 6.1へのアップグレードは、VMware vCenter Server 7 Update 1以降のバージョンでのみサポートされます。バージョン7 Update 1より前のVMware vCenter Serverでは、引き続きSCV 4.7を使用する必要があります。サポートされていないバージョンのVMware vCenter Serverでは、アップグレードが中断されます。

SnapCenter Plug-in for VMware vSphere仮想アプライアンスを使用している場合は、新しいリリースにアップグレードできます。アップグレード プロセスでは、既存のプラグインが登録解除され、vSphere 7.0U1以降のバージョンとのみ互換性のあるプラグインが導入されます。

アップグレード パス

SnapCenter Plug-in for VMware vSphere (SCV) バージョンを使用している場合…	SnapCenter Plug-in for VMware vSphere を直接アップグレードできます…
SCV 6.0	SCV 6.1へのアップグレード
SCV 5.0	SCV 6.0およびSCV 6.1へのアップグレード
SCV 4.9	SCV 5.0およびSCV 6.0へのアップグレード
SCV 4.8	SCV 4.9およびSCV 5.0へのアップグレード
SCV 4.7	SCV 4.8およびSCV 4.9へのアップグレード
SCV 4.6	SCV 4.7およびSCV 4.8へのアップグレード

> アップグレードを開始する前に、SnapCenter Plug-in for VMware vSphere OVAをバックアップしてください。

> ネットワーク設定を静的からDHCPに切り替えることはできません。

サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool" （IMT）。

手順

1. SnapCenter Plug-in for VMware vSphereを無効にしてアップグレードを準備します。
   a. SnapCenter Plug-in for VMware vSphere管理GUIにログインします。このIPアドレスは、SnapCenter Plug-in for VMware vSphereの導入時に表示されたものです。
   b. 左側のナビゲーション ペインで [構成] を選択し、[プラグインの詳細] セクションで [サービス] オプションを選択してプラグインを無効にします。
2. アップグレードをダウンロードする `.iso`ファイル。
   a. NetAppサポートサイトにログイン(https://mysupport.netapp.com/products/index.html）。
   b. 製品リストから * SnapCenter Plug-in for VMware vSphere* を選択し、最新リリースのダウンロード

ボタンを選択します。

c. SnapCenter Plug-in for VMware vSphereをダウンロードする `.iso`ファイルを任意の場所に転送します。

3. アップグレードをインストールします。

a. ブラウザからVMware vSphere vCenterにアクセスします。

b. vCenter GUI で、**vSphere** クライアント **(HTML)** を選択します。

c. **VMware vCenter Single Sign-On** ページにログインします。

d. ナビゲーター ペインで、アップグレードする VM を選択し、[概要] タブを選択します。

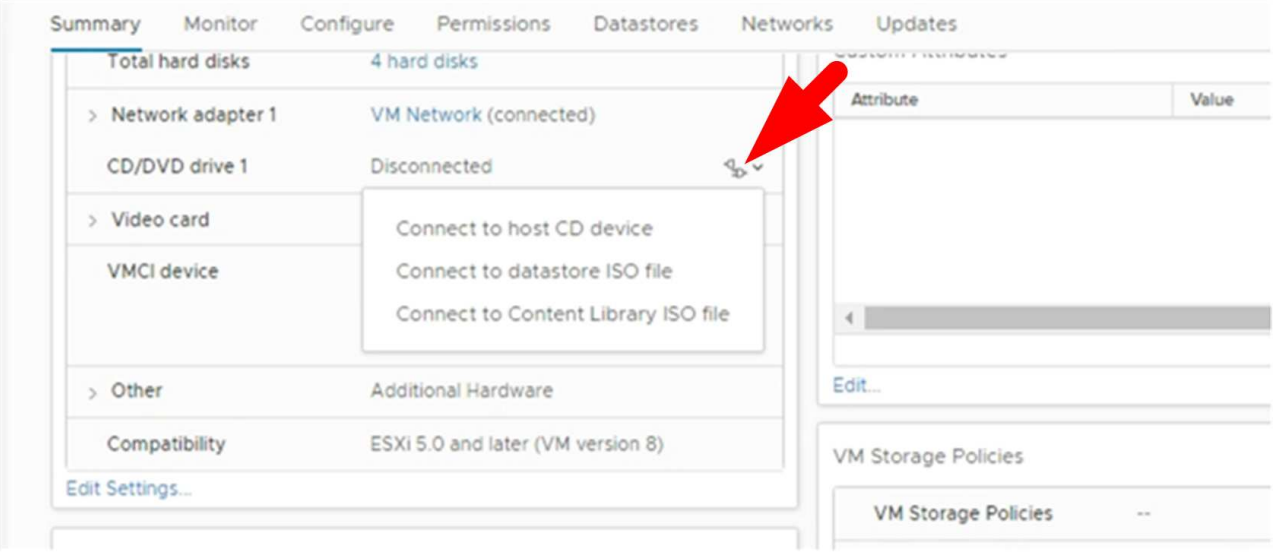
e. 関連オブジェクト ペインで、リスト内の任意のデータストアを選択し、概要 タブを選択します。

f. 選択したデータストアの ファイル タブで、リスト内の任意のフォルダーを選択し、 ファイルのアップロード を選択します。

g. アップロードポップアップ画面で、ダウンロードした場所に移動します。 `.iso`ファイルを選択し、`.iso`ファイルイメージを選択し、[開く] を選択します。ファイルがデータストアにアップロードされます。

h. アップグレードする VM に戻り、[概要] タブを選択します。 **VM** ハードウェア ペインの CD/DVD フィールドの値は「切断」になっている必要があります。

i. CD/DVD フィールドの接続アイコンを選択し、*データストア上の CD/DVD イメージに接続*を選択します。



j. ウィザードで、次の手順を実行します。

i. データストア列で、アップロードしたデータストアを選択します。 `.iso`ファイル。

ii. コンテンツ列で、 `.iso`アップロードしたファイルの場合は、[ファイル タイプ] フィールドで [ISO イメージ] が選択されていることを確認し、[OK] を選択します。フィールドに「Connected」ステータスが表示されるまで待ちます。

k. 仮想アプライアンスの 概要 タブにアクセスしてメンテナンス コンソールにログオンし、緑色の実行矢印を選択してメンテナンス コンソールを起動します。

l. システム構成の場合は **2** を入力し、アップグレードの場合は **8** を入力します。

m. 続行してアップグレードを開始するには、「**y**」と入力します。

同じリリースの**SnapCenter Plug-in for VMware vSphere**の新しいパッチへのアップグレード

同じリリースの新しいパッチにアップグレードする場合は、アップグレードまたは登録を行う前に、vCenter Web ServerでSnapCenter Plug-in for VMware vSphereのキャッシュをクリアし、サーバを再起動する必要があります。

次の場合、プラグインのキャッシュをクリアしないと、最近のジョブがダッシュボードとジョブ モニタに表示されません。

- vCenterを使用してSnapCenter Plug-in for VMware vSphereを導入し、その後、同じリリースのパッチにアップグレードしました。
- SnapCenter VMware仮想アプライアンスをvCenter 1に導入しました。その後、このSnapCenter Plug-in for VMware vSphereを新しいvCenter2に登録しました。SnapCenter Plug-in for VMware vSphereの新しいインスタンスをパッチを適用して作成し、vCenter1に登録します。ただし、vCenter1にはパッチが適用されていない最初のSnapCenter Plug-in for VMware vSphereからキャッシュされたプラグインが残っているため、キャッシュをクリアする必要があります。

キャッシュのクリア手順

1. 見つける `vsphere-client-serenity`フォルダに移動し、 `com.netapp.scv.client-<release-number>`フォルダを削除してください。

   フォルダ名はリリースごとに変わります。

   場所についてはVMwareのドキュメントを参照してください。 `vsphere-client-serenity`オペレーティングシステムのフォルダー。

2. vCenter Serverを再起動します。

   その後、SnapCenter Plug-in for VMware vSphereをアップグレードできます。

同じリリースの新しいパッチにアップグレードすると表示されなくなる情報

SnapCenter Plug-in for VMware vSphereを同じリリースの新しいパッチにアップグレードしたあと、最近のジョブやその他の情報がダッシュボードとジョブ モニタに表示されないことがあります。

同じリリースの新しいパッチにアップグレードする場合は、アップグレードまたは登録を行う前に、vCenter Web ServerでSnapCenter Plug-in for VMware vSphereのキャッシュをクリアし、サーバを再起動する必要があります。

次の場合、プラグインのキャッシュをクリアしないと、最近のジョブがダッシュボードとジョブ モニタに表示されません。

- vCenterを使用してSnapCenter Plug-in for VMware vSphereを導入し、その後、同じリリースのパッチにアップグレードしました。

- SnapCenter VMware仮想アプライアンスをvCenter 1に導入しました。その後、このSnapCenter Plug-in for VMware vSphereを新しいvCenter2に登録しました。SnapCenter Plug-in for VMware vSphereの新しいインスタンスをパッチを適用して作成し、vCenter1に登録します。ただし、vCenter1にはパッチが適用されていない最初のSnapCenter Plug-in for VMware vSphereからキャッシュされたプラグインが残っているため、キャッシュをクリアする必要があります。

キャッシュは、サーバ オペレーティング システムのタイプに応じて、次の場所に配置されます。

- vCenter Server Linux Appliance

  ```
  /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/
  ```

- Windows OS

  ```
  %PROGRAMFILES%/VMware/vSphere client/vc-packages/vsphere-client-serenity/
  ```

キャッシュをクリアする前にアップグレードした場合の対処方法

1. SnapCenter Plug-in for VMware vSphere管理GUIにログインします。

   このIPアドレスは、SnapCenter Plug-in for VMware vSphereの導入時に表示されたものです。

2. 左側のナビゲーション ペインで [構成] を選択し、[プラグインの詳細] セクションで [サービス] オプションを選択してプラグインを無効にします。

   SnapCenter Plug-in for VMware vSphereサービスが無効になり、vCenterで拡張機能の登録が解除されます。

3. 見つける `vsphere-client-serenity`フォルダに移動し、 `com.netapp.scv.client-<release-number>`フォルダを削除してください。

   フォルダ名はリリースごとに変わります。

4. vCenter Serverを再起動します。
5. VMware vSphere Clientにログインします。
6. 左側のナビゲーション ペインで [構成] を選択し、[プラグインの詳細] セクションで [サービス] オプションを選択してプラグインを有効にします。

   SnapCenter Plug-in for VMware vSphereサービスが有効になり、vCenterに拡張機能が登録されます。

法律上の表示

法的通知から、著作権情報、商標、特許などを確認できます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp、NetAppのロゴ、NetAppの商標一覧のページに掲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。

"https://www.netapp.com/company/legal/trademarks/"

特許

現在NetAppが所有する特許の一覧は以下のページから閲覧できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

プライバシー ポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

オープンソース

通知ファイルには、 NetAppソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が提供されます。

"SnapCenter Plug-in for VMware vSphereに関するお知らせ"

著作権に関する情報

Copyright © 2025 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権を有し、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権については、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。