Virtual Storage Console、VASA Provider、Storage Replication Adapter for VMware® vSphere

導入およびセットアップ ガイド

（9.6リリース）

2019年8月 | 215-13886_2019-08_ja-jp
ng-gpso-jp-documents@netapp.com

NetApp®

目次

VSC、VASA Provider、SRA仮想アプライアンスの概要

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスは、ネットアップ ストレージ システムを使用するVMware環境で、仮想マシンのエンドツーエンドのライフサイクル管理機能を提供します。管理者がストレージをvCenter Serverで直接管理できるため、VMware環境のストレージとデータの管理が簡単になります。

VMwareはvSphere 6.5でvSphere Clientという名前の新しいHTML5ベースのクライアントを導入しました。VSC、VASA Provider、SRA仮想アプライアンス9.6では、vSphere Clientのみがサポートされます。VSC、VASA Provider、SRA仮想アプライアンスはvSphere Clientと統合されており、シングル サインオン（SSO）サービスを利用できます。vCenter Serverインスタンスが複数ある環境では、管理するvCenter Serverインスタンスごとに固有のVSCインスタンスを登録する必要があります。

仮想アプライアンスの各コンポーネントは、ストレージをより効率的に管理するための機能を提供します。

Virtual Storage Console（VSC）

VSCでは次の作業を実行できます。

- VSCに対し、SRAとVASA Providerの両方で利用できるストレージ コントローラを追加し、クレデンシャルを割り当て、ストレージ コントローラのアクセス許可を設定する
- データストアをプロビジョニングする
- vCenter Server環境のデータストアおよび仮想マシンのパフォーマンスを監視する
- ロールベース アクセス制御（RBAC）を使用してvCenter Serverオブジェクトへの管理者アクセスを次の2つのレベルで制御する
  - vSphereオブジェクト（仮想マシンやデータストアなど）
    これらのオブジェクトの管理にはvCenter Server RBACを使用します。
  - ONTAPストレージ
    ストレージ システムの管理にはONTAP RBACを使用します。
- ネットアップ ストレージに接続されているESXiホストのホスト設定を表示および更新する

NFS Plug-in for VMware VAAIを使用すると、VSCのプロビジョニング処理にメリットがあります。NFS Plug-in for VMware vStorage APIs for Array Integration（VAAI）はソフトウェア ライブラリであり、ESXiホストにインストールされているVMwareの仮想ディスク ライブラリと連携します。VMware VAAIパッケージを使用すると、特定のタスクを物理ホストからストレージ アレイにオフロードできます。シンプロビジョニングやハードウェア アクセラレーションなどのタスクをアレイ レベルで実行して、ESXiホスト上のワークロードを削減できます。コピー オフロード機能やスペース リザベーション機能によって、VSCの処理のパフォーマンスが向上します。

NetApp NFS Plug-in for VAAIはVSCに付属していません。ネットアップ サポート サイトから、このプラグインのインストール パッケージをダウンロードして、インストール手順を確認できます。

VASA Provider

VASA Provider for ONTAPは、VMware vSphere APIs for Storage Awareness（VASA）を使用して、VMware vSphereで使用されているストレージに関する情報をvCenter Serverに送信します。VSC、VASA Provider、SRA仮想アプライアンス9.6では、VASA ProviderはVSCに統合されています。

VASA Providerでは次の作業を実行できます。

- 仮想ボリューム（VVol）データストアをプロビジョニングする
- 環境に応じたストレージのサービス レベル目標（SLO）を定義するストレージ機能プロファイルを作成して使用する
- データストアがストレージ機能プロファイルに準拠しているかどうかを検証する
- ボリュームやアグリゲートがしきい値に近づいたときに警告するアラートを設定する
- VVolデータストアに作成された仮想マシン ディスク（VMDK）と仮想マシンのパフォーマンスを監視する

VASA Providerは、vCenter Serverとの通信にはVASA API、ONTAPとの通信にはネットアップAPI（ZAPI）を使用します。VASA Providerダッシュボードを表示するためには、OnCommand API Servicesをインストールしてvcenter Serverに登録しておく必要があります。

注：VASA Providerには、専用のOnCommand APIサービス インスタンスが必要です。OnCommand APIサービスの1つのインスタンスを複数のVASA Providerインスタンスで共有することはできません。

Storage Replication Adapter（SRA）

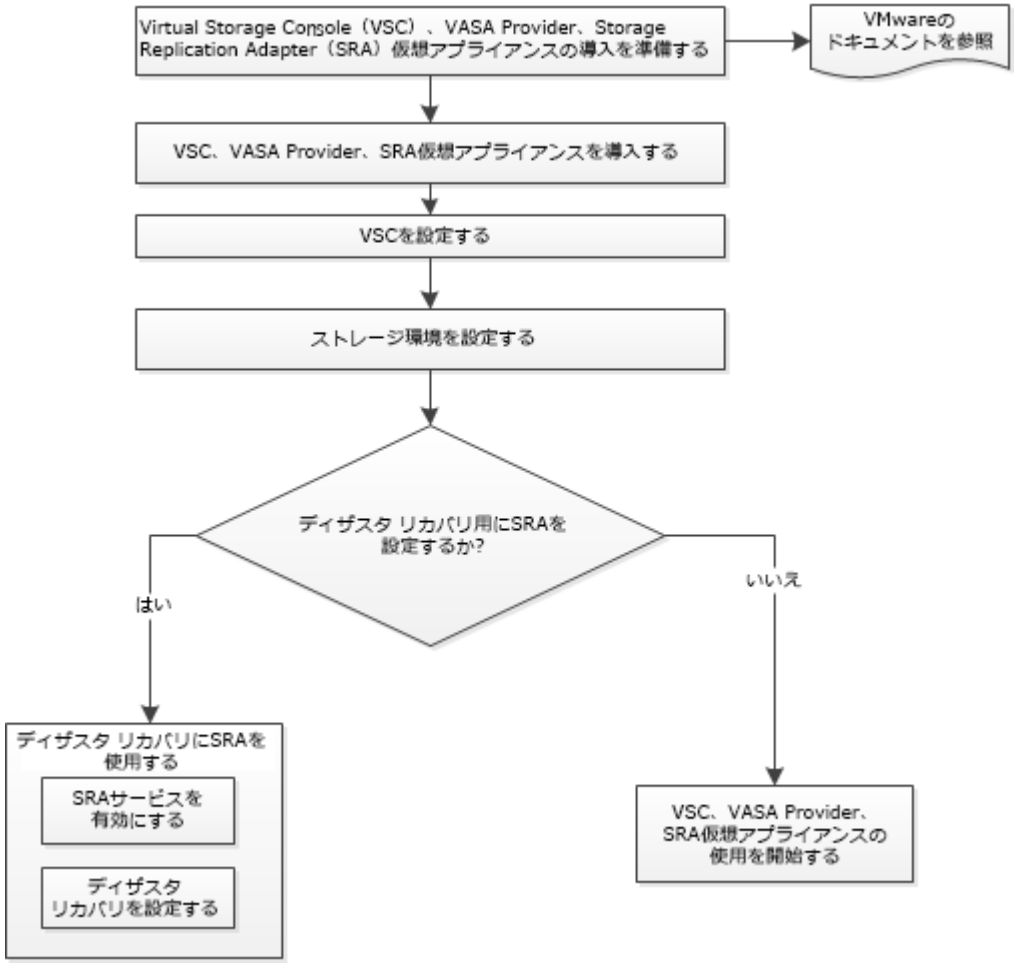
SRAを有効にしてVMware Site Recovery Manager（SRM）と一緒に使用している場合、障害時にvCenter Serverデータストアと仮想マシンをリカバリできます。SRAを使用して、障害時のディザスタ リカバリ用に、環境内の保護対象サイトとリカバリ サイトを設定できます。

関連情報

ネットアップのマニュアル：*OnCommand API Services*
ネットアップのマニュアル：*NetApp NFS Plug-in for VMware VAAI*
ネットアップ サポート

VSC、VASA Provider、SRA仮想アプライアンスの新規ユーザ向けの導入ワークフロー

VMwareを初めて導入し、ネットアップのVSC製品を使用したことがない場合は、VSC、VASA Provider、SRA仮想アプライアンスを導入して設定する前に、vCenter Serverを設定してESXiホストをセットアップする必要があります。



VSC、VASA Provider、SRAの既存ユーザ向けの導入ワークフロー

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンス7.xから最新バージョンへのインプレース アップグレードがサポートされています。

各アプリケーション（VSC、VASA Provider、SRA）の以前のリリースでは、異なるアップグレード プロセスが使用されます。VSC、VASA Provider、またはSRAがインストールされている環境では、次の処理を実行する必要があります。

1. VSC、VASA Provider、SRA仮想アプライアンスの最新バージョンを導入します。
2. 既存の設定データを移行します。

設定データには、ストレージ システムのクレデンシャルとkaminoprefs.xmlファイルおよびvscPreferences.xmlファイル内のプリファレンスが含まれます。

VSCプリファレンス ファイルの設定（28ページ）

多くの場合、設定データを移行する必要はありません。ただし、過去にプリファレンス ファイルをカスタマイズした場合は、それらのファイルを確認し、新しく導入した仮想アプライアンスに対しても同様の変更を実施します。次のいずれかを実行できます。

- ネットアップのユーティリティを使用して、ストレージ システムのクレデンシャルをVSC 6.XおよびSRA 4.Xから新しい導入環境に移行します。
- 新しく導入した仮想アプライアンスに、クレデンシャルを指定してストレージ システムを追加します。

VASA Provider 6.Xからアップグレードする場合は、アップグレード前にVASA Providerの登録を解除する必要があります。詳細については、使用中のリリースのドキュメントを参照してください。

SRA 4.0以前からのアップグレードも実施する場合は、次の手順を実行します。

- SRA 4.0を使用している場合は、SRAサーバ（VMとしてインストールされた.ovaファイル）を最新バージョンにインプレース アップグレードできます。
  VSC、VASA Provider、SRA仮想アプライアンス9.6へのアップグレード（20ページ）
- SRA 2.1または3.0を使用している場合は、最初に既存のサイトの設定をメモしておく必要があります。
  詳細な手順については、『*Installation and Setup Guide for Storage Replication Adapter 4.0 for ONTAP*』の「Upgrade Overview」を参照してください。これらのSRAリリースもVASA Providerを使用するため、VASA Providerの登録を解除してから最新バージョンのVSC、VASA Provider、SRA仮想アプライアンスを導入する必要があります。アップグレードが完了したら、以前のリリースのサーバ（.ova）を削除できます。

SRAをアップグレードする場合は、SRAソフトウェア（.msiファイルによってインストールされた、Site Recovery Managerサーバ上のアダプタ）をSite Recovery Managerサーバから削除する必要があります。このソフトウェアはWindowsシステムのコントロール パネルを使用してアンインストールでき、その後.msiファイルを使用して最新のSRAソフトウェアをSRAサーバにインストールできます。

VASA Providerを導入している場合は、既存の環境からのアップグレード後に、[設定の編集]オプションを使用して仮想アプライアンスのメモリ サイズを12GBに設定する必要があります。仮想メモリの予約サイズも変更する必要があります。メモリ サイズを変更する場合には、仮想マシンの電源をオフにしてください。

最新バージョンの仮想アプライアンスを導入する場合は、「VSC、VASA Provider、SRA仮想アプライアンスの導入要件」を参照してください。インプレース アップグレードの実行方法については、「VSC、VASA Provider、SRA仮想アプライアンス9.6へのアップグレード」を参照してください。

関連概念

VSC、VASA Provider、SRA仮想アプライアンスの導入要件（10ページ）

関連タスク

VSC、VASA Provider、SRA仮想アプライアンス9.6へのアップグレード（20ページ）

関連情報

NetApp ToolChest：NetApp Import Utility for SnapCenter and Virtual Storage Console

*SnapCenter*のインストールとセットアップ

VSC、VASA Provider、SRA仮想アプライアンスの導入要件

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスを導入する前に、導入要件を確認し、実行するタスクを決めておく必要があります。実行するタスクに基づいて、VSC、VASA Provider、SRA仮想アプライアンスの導入モデルを選択できます。

VSCのポート要件

ストレージ システムとVMware vCenter Serverの間の通信など、Virtual Storage Console（VSC）のコンポーネント間の通信には、指定のポートがデフォルトで使用されます。ファイアウォールを有効にしている場合は、例外を許可するようにファイアウォールを設定する必要があります。

Windows以外のファイアウォールについては、VSCで使用する特定のポートへのアクセスを手動で許可する必要があります。それらのポートへのアクセスを許可しないと、「`Unable to communicate with the server`」のようなエラー メッセージが表示されます。

VSCで使用されるデフォルトの双方向ポートは次のとおりです。

デフォルトのポート番号	説明
9083	有効にすると、VASA ProviderとStorage Replication Adapter（SRA）の両方がこのポートを使用してvCenter Serverと通信します。このポートはTCP/IP設定を取得する場合にも必要です。
443	クレデンシャルの設定方法によっては、VMware vCenter Serverとストレージ システムがこのポートで保護された通信をリスンします。
8143	VSCは、このポートでセキュアな通信をリスンします。

VSC、VASA Provider、SRA仮想アプライアンスのスペースとサイジングの要件

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスを導入する前に、導入パッケージのスペース要件とホスト システムのいくつかの基本的な要件について理解しておく必要があります。

インストール パッケージのスペース要件

- シンプロビジョニングの場合：2.1GB
- シックプロビジョニングの場合：54.0GB

ホスト システムのサイジング要件

- ESXi 6.5U2以降
- 推奨メモリ：12GB RAM
- 推奨CPU数：2

VSC、VASA Provider、SRA仮想アプライアンスでサポートされるストレージ システム、ライセンス、アプリケーション

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスの導入を開始する前に、ストレージ システムの基本要件、アプリケーション要件、およびライセンス要件について理解しておく必要があります。

サポートされるONTAP、vCenter Server、ESXiホスト、プラグイン アプリケーション、およびSite Recovery Manager（SRM）のバージョンの最新情報については、Interoperability Matrix Tool（IMT）を参照してください。

- *Interoperability Matrix Tool*：*VSC 9.6*
- *Interoperability Matrix Tool*：*VASA Provider 9.6*
- *Interoperability Matrix Tool*：*SRA 9.6*

仮想ボリューム（VVol）データストアに対して仮想マシンのSnapshot処理とクローン処理を実行するには、FlexCloneライセンスを有効にする必要があります。

Storage Replication Adapter（SRA）には次のライセンスが必要です。

- SnapMirrorライセンス
  SRAのフェイルオーバー処理を実行するためには、SnapMirrorライセンスを有効にする必要があります。
- FlexCloneライセンス
  SRAのテスト フェイルオーバー処理を実行するためには、FlexCloneライセンスを有効にする必要があります。

データストアのIOPSを表示するには、Storage I/O Controlを有効にするか、Storage I/O Controlの設定でストレージI/O統計の収集を無効にするチェック ボックスをオフにする必要があります。Storage I/O Controlは、VMwareのEnterprise Plusライセンスがある場合にのみ有効にできます。

- *VMwareの技術情報アーティクル1022091*：「*Troubleshooting Storage I/O Control*」
- *VMware vSphereのドキュメント*：「ストレージ *I/O* コントロールの要件」

VSC、VASA Provider、SRA仮想アプライアンスの導入に関する考慮事項と要件

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスを導入する前に、導入計画を作成し、環境でVSC、VASA Provider、SRAをどのように設定するかを決めておくことを推奨します。

次の表に、VSC、VASA Provider、SRA仮想アプライアンスを導入する前に検討が必要な事項について、その概要を記載します。

考慮事項	説明
VSC、VASA Provider、SRA仮想アプライアンスを初めて導入する場合	VSC、VASA Provider、SRA仮想アプライアンスの導入時に、VSCの機能が自動的にインストールされます。 *VSC、VASA Provider、SRAの導入またはアップグレード*（14ページ） *VSC、VASA Provider、SRA仮想アプライアンスの新規ユーザ向けの導入ワークフロー*（7ページ）
VSCの既存の導入環境からアップグレードする場合	VSCの既存の導入環境からVSC、VASA Provider、SRA仮想アプライアンスにアップグレードする場合の手順は、VSCのバージョンと、VASA ProviderとSRAが導入済みかどうかによって異なります。詳細については、導入ワークフローとアップグレードに関するセクションを参照してください。 *VSC、VASA Provider、SRAの既存ユーザ向けの導入ワークフロー*（7ページ） アップグレード前に実施しておくべき作業： • 使用しているストレージ システムとそのクレデンシャルに関する情報を記録しておく必要があります。 アップグレード後に、すべてのストレージ システムが自動的に検出され、正しいクレデンシャルが付与されていることを確認する必要があります。 • 標準のVSCロールに変更を加えた場合、変更を保存するにはそのロールをコピーする必要があります。 標準のロールは、VSCサービスが再起動するたびに現在のデフォルトで上書きされます。
VSCのSSL証明書の再生成	SSL証明書はVSC、VASA Provider、SRA仮想アプライアンスの導入時に自動で生成されます。サイト専用の証明書を作成するには、SSL証明書の再生成が必要な場合があります。 *Virtual Storage ConsoleのSSL証明書の再生成*（27ページ）
ESXiサーバの値の設定	ESXiサーバの値のほとんどはデフォルトで設定されますが、値を検証しておくことを推奨します。デフォルト値は、内部テストに基づいています。環境によっては、パフォーマンスを改善するために値を変更する必要がある場合もあります。 • *ESXiサーバのマルチパスとタイムアウトの設定*（22ページ） • *VSC for VMware vSphereで設定されるESXiホストの値*（23ページ）
ゲスト オペレーティング システムのタイムアウト値	ゲスト オペレーティング システム（ゲストOS）のタイムアウト スクリプトは、フェイルオーバーが適切に動作するように、サポートされているLinux、Solaris、Windowsの各ゲストOSのSCSI I/Oタイムアウト値を設定します。

次の表に、VSC、VASA Provider、SRA仮想アプライアンスを設定する際に必要な事項について、その概要を記載します。

考慮事項	説明
Role-Based Access Control（RBAC;ロール ベース アクセス制御）の要件	VSCは、vCenter Server RBACとONTAP RBACの両方をサポートしています。 管理者としてVSCを実行する場合は、すべてのタスクに必要なすべてのアクセス許可と権限が割り当てられている必要があります。 vSphereオブジェクトへのアクセスを制限する必要がある場合、vCenter Serverの要件に一致する標準のVSCロールをユーザに割り当てます。 NetApp ToolChestで入手できるネットアップ ツールを使用して、推奨されるONTAPロールを作成できます。 適切な権限とアクセス許可を持たないユーザがタスクを実行しようとした場合、そのタスクのオプションはグレー表示されます。 • *VSC、VASA Provider、SRA*仮想アプライアンスに組み込みの標準ロール（43ページ） • *VSC for VMware vSphere*使用時に推奨される*ONTAP*ロール（46ページ）
ONTAPのバージョン	ストレージ システムでONTAP 9.1、9.3、9.4、9.5、または9.6が実行されている必要があります。
ストレージ機能プロファイル	ストレージ機能プロファイルを使用する場合やアラームを設定する場合は、VASA Provider for ONTAPを有効にする必要があります。VASA Providerを有効にすると、仮想ボリューム（VVol）データストアを設定できるようになり、ストレージ機能プロファイルやアラームの作成と管理も可能になります。 ボリュームやアグリゲートの容量が残り少なくなったときや、データストアが関連付けられているストレージ機能プロファイルに準拠しなくなったときに、アラームによって警告されます。

VSC、VASA Provider、SRAの導入またはアップグレード

Virtual Storage Console（VSC）、VASA Provider、およびStorage Replication Adapter（SRA）仮想アプライアンスをダウンロードしてVMware vSphereに導入し、その後、VSC、VASA Provider、SRAを使用して実行するタスクに基づいて必要なアプリケーションを設定する必要があります。

関連タスク

仮想データストアを設定するための*VASA Provider*の有効化 （17ページ）

VSC、VASA Provider、SRA仮想アプライアンスのダウンロード

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスの.ovaファイルをネットアップ サポート サイトからダウンロードできます。

タスク概要

.ovaファイルにはVSC、VASA Provider、SRAが含まれています。導入が完了すると、3つの製品がすべてインストールされます。導入モデルを決定し、その要件に基づいてVASA ProviderとSRAを有効にするかどうかを選択すると、すぐにVSCが起動します。

VSC、VASA Provider、SRA仮想アプライアンスは、ネットアップ サポート サイトから要件に応じて次のソフトウェア ダウンロード ページのいずれかを使用してダウンロードできます。

- **Virtual Storage Console**
- **NetApp VASA Provider**
- **Storage Replication Adapter**

VSC、VASA Provider、SRA仮想アプライアンスの導入時にSRAを有効にする場合は、Site Recovery Manager（SRM）サーバにSRAプラグインをインストールしておく必要があります。SRAアダプタ プラグインのインストール ファイルは**Storage Replication Adapter for ONTAP**のメニューの[Software Downloads]セクションからダウンロードできます。

手順

1. ネットアップ サポート サイトにログインし、**[Downloads]**タブをクリックします。
2. **[Downloads]**ページで、**[Software]**を選択します。
3. 製品のリストから、要件に応じて**[Virtual Storage Console]**、**[NetApp VASA Provider]**、または**[Storage Replication Adapter]**を選択します。
4. ダウンロードするソフトウェアの該当するバージョンを選択し、**[View & Download]**をクリックします。
5. 製品説明ページに表示される指示に従ってダウンロード ページまで進みます。
6. .ovaファイルをvSphere Clientシステムにダウンロードし、OVFテンプレートを導入します。

VSC、VASA Provider、SRA仮想アプライアンスの導入

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスを環境に導入して、アプライアンスを使用できるように必要なパラメータを指定する必要があります。

開始する前に

- 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。

  注： VSC、VASA Provider、SRA仮想アプライアンスを導入できるのは、Windows環境のvCenter ServerまたはVMware vCenter Server Virtual Appliance（vCSA）環境です。

  Interoperability Matrix Tool：VSC 9.6

- 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。
- 仮想マシンに応じた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。
- .ovaファイルをダウンロードしておく必要があります。
- vCenter Serverインスタンスの管理者のログイン クレデンシャルが必要です。
- 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、VSC、VASA Provider、SRA仮想アプライアンス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。

  *vSphere*にキャッシュされたダウンロード済みプラグイン パッケージのクリーンアップ（51ページ）

- ICMPを有効にしておく必要があります。

  ICMPが無効になっていると、VSC、VASA Provider、SRA仮想アプライアンスの初期設定が失敗し、導入後にVSCがVSCサービスとVASA Providerサービスを開始できなくなります。導入後に、VSCサービスとVASA Providerサービスを手動で有効にする必要があります。

タスク概要

VSC、VASA Provider、SRA仮想アプライアンスを新規に導入する場合は、VASA Providerはデフォルトで有効になります。ただし、以前のバージョンの仮想アプライアンスからアップグレードする場合は、アップグレード前のVASA Providerの状態が維持されるため、VASA Providerを手動で有効にしなければならないことがあります。

仮想データストアを設定するための*VASA Provider*の有効化（17ページ）

手順

1. vSphere Clientにログインします。
2. **[ホーム]** > **[ホストおよびクラスタ]**を選択します。
3. 目的のデータセンターを右クリックし、**[OVAテンプレートのデプロイ]**をクリックします。
4. VSC、VASA Provider、SRA用の導入ファイルを指定する方法を選択し、**[次へ]**をクリックします。

場所	操作
URL	VSC、VASA Provider、SRA仮想アプライアンスの.ovaファイルのURLを入力します。
フォルダ	VSC、VASA Provider、SRA仮想アプライアンスの.ovaファイルを保存先から選択します。

5. 次の情報を入力して、導入ウィザードをカスタマイズします。
   - 導入環境の名前
   - 権限を適用するデータセンター
   - VSC、VASA Provider、SRA仮想アプライアンスを導入するホスト
   - 仮想ディスクの形式、VMストレージ ポリシー、ストレージの場所、およびネットワーク
   - 管理者のユーザ名とパスワード

     注：

     - VSC、VASA Provider、SRA仮想アプライアンスを導入する際に、vCenter Serverの管理者クレデンシャルを設定できます。
       vCenter Serverのパスワードが変更になった場合、URL：`https://<IP>:8143/Register.html`から管理者のパスワードを更新できます。IPアドレスは、VSC、VASA Provider、SRA仮想アプライアンスの導入時に指定したIPアドレスです。
     - 管理者パスワードにはスペースは使用できません。
     - メンテナンス コンソールにアクセスするには、ユーザ名「maint」を使用する必要があります。
       デフォルトのパスワードは「admin123」です。
     - DHCPを使用していない場合は、有効なDNSホスト名（非修飾）と仮想アプライアンスの静的IPアドレス、およびその他のネットワーク パラメータを指定します。これらすべてのパラメータは適切なインストールと運用のため必要です。

   - VSC、VASA Provider、SRA仮想アプライアンスの登録先のvCenter ServerインスタンスのIPアドレス（IPv4またはIPv6）。
     生成されるVSCとVASAの証明書のタイプは、導入時に指定したIPアドレス（IPv4またはIPv6）によって異なります。VSC、VASA Provider、SRA仮想アプライアンスの導入時に静的IPの詳細を入力せず、IPv4アドレスとIPv6アドレスの両方がDHCPネットワークから提供される場合は、次の点に注意してください。
     - vCenter Serverへの登録に使用するVSC、VASA Provider、SRA仮想アプライアンスのIPアドレスは、OVA導入ウィザードで入力したvCenter ServerのIPアドレスのタイプ（IPv4またはIPv6）によって異なります。
     - vCenter Serverの登録時に使用したものと同じタイプのIPアドレスを使用して、VSCとVASAの両方の証明書が生成されます。
     - VSC、VASA Provider、SRA仮想アプライアンスのメンテナンス コンソールの[Application Configuration]メニューを使用して、パスワードを変更できます。
       VSC、VASA Provider、SRA仮想アプライアンスのメンテナンス コンソールのオプションへのアクセス（31ページ）

     重要：IPv6はvCenter Server 6.7以降でのみサポートされます。

6. 設定データを確認し、**[次へ]**をクリックして導入を完了します。

   導入が完了するまでの間、[タスク]タブで導入の進捗状況を確認できます。

7. 仮想アプライアンス仮想マシンの電源をオンにして、仮想アプライアンスを実行している仮想マシンのコンソールを開きます。

8. アプライアンス コンソールにプロンプトが表示されたら、vCenter Serverに戻ります。

9. アプライアンス仮想マシンの**[概要]**タブで、**[VMware Tools のインストール/アップグレード]**を選択し、**[マウント]**をクリックします。

   VMware Toolsが自動的にインストールされます。インストールが完了したら、アプライアンス コンソールに表示される手順に従ってToolsのISOを切断します。

10. VSC、VASA Provider、SRA仮想アプライアンスがvCenter Serverに登録されていない場合は、`https://appliance_ip:8143/Register.html`を使用してVSCインスタンスを登録します。

11. vSphere Clientからログアウトして再度ログインすると、導入したVSC、VASA Provider、SRA仮想アプライアンスが表示されます。

    a. 既存のvSphere Clientからログアウトし、ブラウザを閉じます。

    b. vSphere Clientにログインします。

       vSphere Clientでプラグインが更新されるまでに数分かかる場合があります。

       トラブルシューティング：ログインしてもプラグインが表示されない場合は、vSphere Clientのキャッシュをクリーンアップする必要があります。

       *vSphere*にキャッシュされたダウンロード済みプラグイン パッケージのクリーンアップ（51ページ）

次のタスク

注：VASA Provider for ONTAPダッシュボードを表示するには、OnCommand API Servicesをダウンロードしてインストールする必要があります。

*VSC、VASA Provider、SRA*仮想アプライアンスへの*OnCommand API Services*の登録（18ページ）

仮想データストアを設定するためのVASA Providerの有効化

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスでは、VASA Provider機能がデフォルトで有効になっています。各VVolデータストアに必要なストレージ機能プロファイルを使用してVVolデータストアを設定できます。

開始する前に

- vCenter Serverインスタンスをセットアップし、ESXiを設定しておく必要があります。
- VSC、VASA Provider、SRA仮想アプライアンスを導入しておく必要があります。

タスク概要

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンス9.6にアップグレードする前にVASA Provider機能が無効になっていた場合は、アップグレード後もVASA Provider機能は無効なままになります。

手順

1. VMware vSphereのWebユーザ インターフェイスにログインします。
2. vSphere Clientで、**[メニュー]** > **[Virtual Storage Console]**をクリックします。
3. **[設定]**をクリックします。
4. **[管理設定]**タブで**[機能の管理]**をクリックします。
5. **[機能の管理]**ダイアログ ボックスで、有効にするVASA Provider拡張機能を選択します。
6. VSC、VASA Provider、SRA仮想アプライアンスのIPアドレスと管理者パスワードを入力し、**[適用]**をクリックします。

VSC、VASA Provider、SRA仮想アプライアンスへのOnCommand API Servicesの登録

VVolダッシュボードに仮想ボリューム（VVol）データストアと仮想マシンの詳細を表示するには、VASA ProviderにOnCommand API Servicesを登録する必要があります。OnCommand API ServicesはVVol VMおよびデータストアのレポートのデータを取得する際にも必要です。

開始する前に

ネットアップ サポート サイトからOnCommand API Services 2.1以降をダウンロードしておく必要があります。

注：VVolダッシュボードには、ONTAP 9.3以降を使用してVVolデータストアと仮想マシンが設定されている場合にのみパフォーマンス指標が表示されます。

手順

1. Virtual Storage Console（VSC）の**[ホーム]**ページで、**[設定]**をクリックします。
2. **[管理設定]**タブで**[拡張機能の管理]**をクリックします。
3. **[OnCommand API Servicesの登録]**スライダを使用してOnCommand API Servicesを有効にします。
4. OnCommand API ServicesのIPアドレス、サービス ポート、およびクレデンシャルを入力します。

   [VASA Provider の拡張機能の管理]ダイアログ ボックスでは、次の変更も実行できます。

   - クレデンシャルに変更があったときにOnCommand API Servicesの登録を更新する。
   - VASA Providerダッシュボードが不要になったときにOnCommand API Servicesを登録解除する。
     VASA ProviderへのOnCommand API Servicesの登録を解除するには、[OnCommand API Services の登録]チェック ボックスをオフにする必要があります。
5. **[適用]**をクリックします。

   VVolダッシュボードには、OnCommand API Servicesの登録が完了した時点で初めて指標が表示されます。

関連情報

ネットアップ サポート

Storage Replication Adapterの有効化

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスでは、ディザスタ リカバリを設定するためにVSCでSRA機能を使用できるようにすることができます。

開始する前に

- vCenter Serverインスタンスをセットアップし、ESXiを設定しておく必要があります。
- Site Recovery Manager（SRM）ディザスタ リカバリ ソリューションを設定する場合のみ、SRAプラグインの`.msi`ファイルをダウンロードしておく必要があります。
- VSC、VASA Provider、SRA仮想アプライアンスを導入しておく必要があります。

タスク概要

必要に応じてVASA ProviderとSRAの機能を有効化できるため、必要なワークフローだけを実行できます。

手順

1. VMware vSphereのWebユーザ インターフェイスにログインします。
2. vSphere Clientで、**[メニュー]** > **[Virtual Storage Console]**をクリックします。
3. **[設定]**をクリックします。
4. **[管理設定]**タブで**[機能の管理]**をクリックします。
5. **[機能の管理]**ダイアログ ボックスで、有効にするSRA拡張機能を選択します。
6. VSC、VASA Provider、SRA仮想アプライアンスのIPアドレスと管理者パスワードを入力し、**[適用]**をクリックします。
7. Windows SRMサーバで、ダウンロードしたSRAプラグインの`.msi`インストーラをダブルクリックして、画面に表示される手順に従います。
8. SRMサーバへのSRAプラグインのインストールを完了するには、導入済みの仮想アプライアンスのIPアドレスとパスワードを入力します。

   選択した拡張機能が設定可能になったかどうかを確認するには、vSphere Web Clientからログアウトして、再度ログインする必要があります。

関連概念

ディザスタ リカバリ用の*Storage Replication Adapter*の設定（49ページ）

NFS VAAIプラグインのインストール

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスのGUIを使用して、NetApp NFS Plug-in for VMware vStorage APIs for Array Integration（VAAI）をインストールできます。

開始する前に

- ネットアップ サポート サイトからNFS Plug-in for VAAIのインストール パッケージ（`.vib`）をダウンロードしておく必要があります。

ネットアップ サポート

- ESXiホスト6.5以降とONTAP 9.1以降をインストールしておく必要があります。
- ESXiホストの電源をオンにし、NFSデータストアをマウントしておく必要があります。
- `DataMover.HardwareAcceleratedMove`、`DataMover.HardwareAcceleratedInit`、および`VMFS3.HardwareAcceleratedLocking`のホスト設定の値を「1」に設定しておく必要があります。
  これらの値はVSCホストの設定で設定します。
- `vserver nfs modify -vserver vserver_name -vstorage enabled`コマンドを使用し、Storage Virtual Machine（SVM）のvstorageオプションを有効にしておく必要があります。

手順

1. VSCで使用される事前定義の名前に合わせて、ネットアップ サポート サイトからダウンロードした`.vib`ファイルの名前を`NetAppNasPlugin.vib`に変更します。
2. VSCの[ホーム]ページで、**[設定]**をクリックします。
3. **[NFS VAAIツール]**タブをクリックします。
4. **[既存のバージョン]**セクションで**[変更]**をクリックします。
5. 名前を変更した`.vib`ファイルを検索して選択し、**[アップロード]**をクリックしてファイルを仮想アプライアンスにアップロードします。
6. **[ESXiホストにインストール]**セクションで、NFS VAAIプラグインをインストールするESXiホストを選択し、**[インストール]**をクリックします。

   画面に表示される手順に従ってインストールを完了する必要があります。vSphere Web Clientの[タスク]セクションで、インストールの進捗状況を監視できます。
7. インストールが終了したら、ESXiホストをリブートします。

   ESXiホストをリブートすると、NFS VAAI Plug-inがVSCによって自動的に検出されます。プラグインを有効にするための追加の手順は必要ありません。

VSC、VASA Provider、SRA仮想アプライアンス9.6へのアップグレード

ここに記載されている手順に従って、既存の環境のVirtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスからバージョン9.6へのインプレース アップグレードを実行できます。

開始する前に

- VSC、VASA Provider、SRA仮想アプライアンス9.6の`.iso`ファイルをダウンロードしておく必要があります。
- VSC、VASA Provider、SRA仮想アプライアンスがアップグレード後に最適に機能するためには、12GB以上のRAMを確保する必要があります。
- vSphere Clientのブラウザ キャッシュを消去する必要があります。
  *vSphere*にキャッシュされたダウンロード済みプラグイン パッケージのクリーンアップ（51ページ）

タスク概要

VASA Providerのステータスは、アップグレード後も既存の導入環境と同じになります。アップグレード後の要件に基づいて、VASA Providerを手動で有効または無効にする必要があります。VASA Providerを有効にすると従来のデータストアのプロビジョニング用のストレージ機能プロファイルとストレージ アラームが有効になるため、VVolを使用しない場合もVASA Providerを有効にすることを推奨します。

注：仮想アプライアンス9.6へのインプレース アップグレードは、バージョン7.xの既存のVSC、VASA Provider、SRA仮想アプライアンスからのみ実行できます。

手順

1. ダウンロードした.isoファイルを仮想アプライアンスにマウントします。
   a. **[設定の編集]** > **[CD/DVD ドライブ]**をクリックします。
   b. ドロップダウンリストから**[データストア ISO ファイル]**を選択します。
   c. ダウンロードした.isoファイルを選択して、**[パワーオン時に接続]**チェック ボックスをオンにします。
2. 導入した仮想アプライアンスの**[サマリ]**タブにアクセスします。
3.  をクリックして、メンテナンス コンソールを起動します。
4. メイン メニューのプロンプトで、「**2**」と入力して**System Configuration**オプションを選択し、続けて「**8**」と入力して**Upgrade**オプションを選択します。

   アップグレードが終了すると、仮想アプライアンスが再起動します。VSC、VASA Provider、SRA仮想アプライアンスは、アップグレード前と同じIPアドレスでvCenter Serverに登録されます。
5. IPv6アドレスを使用してvCenter ServerにVSC、VASA Provider、SRA仮想アプライアンスを登録するには、次の手順を実行します。
   a. VSC、VASA Provider、SRA仮想アプライアンスの登録を解除します。
   b. **[登録]**ページを使用して、VSC、VASA Provider、SRA仮想アプライアンスのIPv6アドレスをvCenter Serverに登録します。
   c. 登録後、VSCとVASA Providerの証明書を再生成します。

   重要：IPv6はvCenter Server 6.7以降でのみサポートされます。
6. vSphere Clientからログアウトして再度ログインすると、導入したVSC、VASA Provider、SRA仮想アプライアンスが表示されます。
   a. 既存のvSphere Web ClientまたはvSphere Clientからログアウトし、ウィンドウを閉じます。
   b. vSphere Clientにログインします。

      vSphere Clientでプラグインが更新されるまでに数分かかる場合があります。

関連タスク

仮想データストアを設定するための *VASA Provider*の有効化 （17ページ）

Virtual Storage Console for VMware vSphere環境の設定

Virtual Storage Console（VSC）はさまざまな環境に対応しています。それらの環境の機能を使用するために、追加の設定が必要になることがあります。

ESXiホスト、ゲスト オペレーティング システム、VSCを設定するには、次の作業の一部が必要になることがあります。

- ESXiホストの設定（UNMAPの設定など）の確認
- ゲストOSのタイムアウト値の追加
- VSCのSSL証明書の再生成
- ストレージ機能プロファイルとしきい値アラームの作成
- 異なるサブネット間でのデータストアのマウントを有効化するためのプリファレンス ファイルの変更

ESXiサーバのマルチパスとタイムアウトの設定

Virtual Storage Console for VMware vSphereにより、ESXiホストのマルチパスの設定とHBAタイムアウトの設定が確認され、ネットアップ ストレージ システムに合わせた最適な設定が行われます。

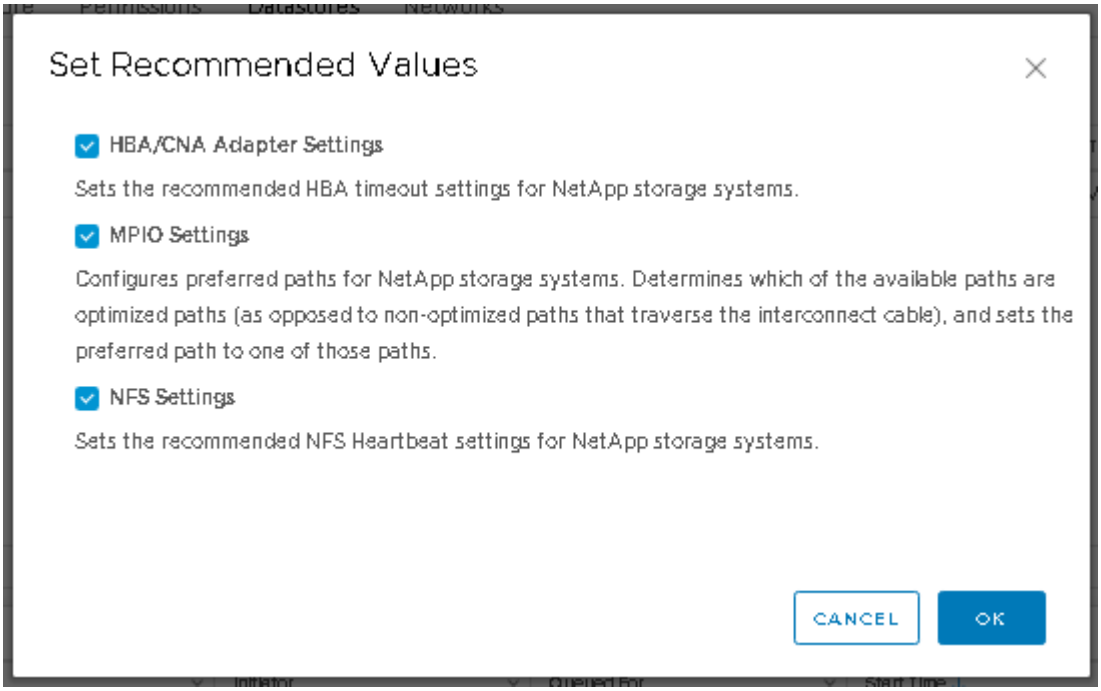
タスク概要

この処理には、構成やシステムの負荷によっては時間がかかることがあります。タスクの進捗状況は[最近のタスク]パネルに表示されます。タスクが完了すると、ホストのステータスを示す[アラート]アイコンが[正常]アイコンまたは[リブートを保留中]アイコンに変わります。

手順

1. VMware vSphere Web Clientの**[ホーム]**ページで、**[vCenter]** > **[ホスト]**をクリックします。
2. ホストを右クリックし、**[アクション]** > **[NetApp VSC]** > **[推奨値に設定]**を選択します。
3. **[ネットアップの推奨設定]**ダイアログ ボックスで、システムに最適な値を選択します。

   デフォルトで標準の推奨値が設定されます。



4. **[OK]**をクリックします。

VSC for VMware vSphereで設定されるESXiホストの値

Virtual Storage Console for VMware vSphereでは、最適なパフォーマンスが得られ、フェイルオーバーが正常に実行されるように、ESXiホストのタイムアウトなどの値が設定されます。Virtual Storage Console（VSC）で設定される値は、ネットアップ独自のテスト結果に基づいています。

VSCで設定されるESXiホストの値を次に示します。

ESXiの高度な設定

VMFS3.HardwareAcceleratedLocking

この値を1に設定します。

VMFS3.EnableBlockDelete

この値を0に設定します。

NFS設定

Net.TcpipHeapSize

この値を32に設定します。

他のすべてのNFS構成では、この値を30に設定します。

Net.TcpipHeapMax

vSphere 6.0以降を使用している場合は、この値を1536に設定します。

vSphere 5.5を使用している場合には、この値を512に設定します。

vSphere 5.0または5.1を使用している場合は、この値を128に設定します。

vSphere 5.0以前を使用している場合は、この値を120に設定します。

NFS.MaxVolumes

vSphere 5.0以降を使用している場合は、この値を256に設定します。

他のすべてのNFS構成では、この値を64に設定します。

NFS41.MaxVolumes

vSphere 6.0以降を使用している場合は、この値を256に設定します。

NFS.MaxQueueDepth

vSphere 6.0以降のESXiホストを使用している場合は、キューのボトルネックを回避するためにこの値を128以上に設定します。

vSphereのバージョンが6.0より前の場合は、この値を64に設定します。

NFS.HeartbeatMaxFailures

すべてのNFS構成でこの値を10に設定します。

NFS.HeartbeatFrequency

すべてのNFS構成でこの値を12に設定します。

NFS.HeartbeatTimeout

すべてのNFS構成でこの値を5に設定します。

FC / FCoEの設定

パス選択ポリシー

ALUAに対応するFCパスを使用する場合は、この値を「RR」（ラウンドロビン）に設定します。

他のすべての構成では、この値を「FIXED」に設定します。

この値を「RR」に設定すると、最適化されたすべてのアクティブなパスで負荷を分散できます。「FIXED」は、ALUAに対応していない従来の構成用の値で、プロキシI/Oを防止できます。つまり、Data ONTAP 7-Modeを実行する環境で高可用性（HA）ペアの他方のノードにI/Oが送られないようにすることができます。

Disk.QFullSampleSize

すべての構成でこの値を32に設定します。この値を設定すると、I/Oエラーの防止に役立ちます。

Disk.QFullThreshold

すべての構成でこの値を8に設定します。この値を設定すると、I/Oエラーの防止に役立ちます。

Emulex FC HBAタイムアウト

デフォルト値を使用します。

QLogic FC HBAタイムアウト

デフォルト値を使用します。

iSCSI設定

パス選択ポリシー

すべてのiSCSIパスで、この値を「RR」に設定します。

この値を「RR」に設定すると、最適化されたすべてのアクティブなパスで負荷を分散できます。

Disk.QFullSampleSize

すべての構成でこの値を32に設定します。この値を設定すると、I/Oエラーの防止に役立ちます。

Disk.QFullThreshold

すべての構成でこの値を8に設定します。この値を設定すると、I/Oエラーの防止に役立ちます。

ゲスト オペレーティング システム スクリプトの設定

ゲスト オペレーティング システム（OS）スクリプトのISOイメージは、Virtual Storage Console for VMware vSphere Virtual Storage Consoleサーバにマウントされます。仮想マシンのストレージ タイムアウトの設定にゲストOSスクリプトを使用するには、vSphere Clientからスクリプトをマウントする必要があります。

表 1 : ゲスト オペレーティング システムのISOの場所

オペレーティング システム タイプ	60秒のタイムアウト設定	190秒のタイムアウト設定
Linux	`https://<appliance_ip>:8143/vsc/public/writable/linux_gos_timeout-install.iso`	`https://<appliance_ip>:8143/vsc/public/writable/linux_gos_timeout_190-install.iso`
Windows	`https://<appliance_ip>:8143/vsc/public/writable/windows_gos_timeout.iso`	`https://<appliance_ip>:8143/vsc/public/writable/windows_gos_timeout_190.iso`
Solaris	`https://<appliance_ip>:8143/vsc/public/writable/solaris_gos_timeout-install.iso`	`https://<appliance_ip>:8143/vsc/public/writable/solaris_gos_timeout_190-install.iso`

仮想マシンを管理するvCenter Serverに登録されているVSCインスタンスのコピーからスクリプトをインストールする必要があります。環境に複数のvCenter Serverが含まれている場合は、ストレージのタイムアウト値を設定する仮想マシンを含むサーバを選択する必要があります。

仮想マシンにログインし、スクリプトを実行してストレージのタイムアウト値を設定します。

Windowsゲスト オペレーティング システムのタイムアウト値の設定

Windowsゲスト オペレーティング システムのSCSI I/Oタイムアウト設定は、ゲスト オペレーティング システム（OS）のタイムアウト スクリプトで設定されます。タイムアウト値として60秒または190秒のどちらかを指定できます。この設定を有効にするには、WindowsゲストOSをリブートする必要があります。

開始する前に

Windowsスクリプトを含むISOイメージをマウントしておく必要があります。

手順

1. Windows仮想マシンのコンソールにアクセスし、管理者権限を持つアカウントでログインします。

2. スクリプトが自動的に開始されない場合は、CDドライブを開き、`windows_gos_timeout.reg`スクリプトを実行します。

   [レジストリ エディター]ダイアログ ボックスが表示されます。

3. **[はい]**をクリックして処理を続行します。

   「`D:\windows_gos_timeout.reg` に含まれるキーと値が、レジストリに正常に追加されました」というメッセージが表示されます。

4. WindowsゲストOSをリブートします。

5. ISOイメージをアンマウントします。

Solarisゲスト オペレーティング システムのタイムアウト値の設定

Solaris 10のSCSI I/Oタイムアウト設定は、ゲスト オペレーティング システム（OS）のタイムアウト スクリプトで設定されます。タイムアウト値として60秒または190秒のどちらかを指定できます。

開始する前に

Solarisスクリプトを含むISOイメージをマウントしておく必要があります。

手順

1. Solaris仮想マシンのコンソールにアクセスし、root権限を持つアカウントでログインします。

2. `solaris_gos_timeout-install.sh`スクリプトを実行します。

   Solaris 10の場合、次のようなメッセージが表示されます。

   ```
   Setting I/O Timeout for /dev/s-a - SUCCESS!
   ```

3. ISOイメージをアンマウントします。

Linuxゲスト オペレーティング システムのタイムアウト値の設定

Red Hat Enterprise Linuxバージョン4、5、6、7およびSUSE Linux Enterprise Serverバージョン9、10、11のSCSI I/Oタイムアウト設定は、ゲスト オペレーティング システム（OS）のタイムアウト スクリプトで設定されます。タイムアウト値として60秒または190秒のどちらかを指定できます。Linuxを新しいバージョンにアップグレードしたときは、必ずこのスクリプトを実行する必要があります。

開始する前に

Linuxスクリプトを含むISOイメージをマウントしておく必要があります。

手順

1. Linux仮想マシンのコンソールにアクセスし、root権限を持つアカウントでログインします。

2. `linux_gos_timeout-install.sh`スクリプトを実行します。

   Red Hat Enterprise Linux 4またはSUSE Linux Enterprise Server 9の場合は、次のようなメッセージが表示されます。

   ```
   Restarting udev... this may take a few seconds.
   ```

```
Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
```

Red Hat Enterprise Linux 5、Red Hat Enterprise Linux 6、およびRed Hat Enterprise Linux 7の場合は、次のようなメッセージが表示されます。

```
patching file /etc/udev/rules.d/50-udev.rules
```

```
Hunk #1 succeeded at 333 (offset 13 lines).
```

```
Restarting udev... this may take a few seconds.
```

```
Starting udev: [ OK ]
```

```
Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
```

SUSE Linux Enterprise Server 10またはSUSE Linux Enterprise Server 11の場合は、次のようなメッセージが表示されます。

```
patching file /etc/udev/rules.d/50-udev-default.rules
```

```
Hunk #1 succeeded at 114 (offset 1 line).
```

```
Restarting udev ...this may take a few seconds.
```

```
Updating all available device nodes in /dev:   done
```

3. ISOイメージをアンマウントします。

Virtual Storage ConsoleのSSL証明書の再生成

Virtual Storage Console（VSC）をインストールするとSSL証明書が生成されます。このSSL証明書用に生成される識別名（DN）は、クライアント マシンが認識する共通名（CN）とは異なる場合があります。キーストアと秘密鍵のパスワードを変更して証明書を再生成し、サイト固有の証明書を作成することができます。

タスク概要

メンテナンス コンソールを使用してリモート診断を有効にして、サイト固有の証明書を生成することができます。

ネットアップ ナレッジベースの回答*1075654*：「*Virtual Storage Console 7.x: Implementing CA signed certificates*」

手順

1. メンテナンス コンソールにログインします。
2. 「**1**」と入力して`Application Configuration`メニューにアクセスします。
3. `Application Configuration`メニューで、「**3**」と入力してVSCサービスを停止します。
4. 「**7**」と入力してSSL証明書を再生成します。

複数のvCenter Server環境でVSCを登録するための要件

1つのVMware vSphere Web Clientで複数のvCenter Serverインスタンスを管理している環境でVirtual Storage Console for VMware vSphereを使用する場合は、vCenter ServerごとにVSCインスタンスを1つ登録して、VSCとvCenter Serverを1:1のペアにする必要があります。そうすることで、vCenter 6.0以降を実行するすべてのサーバを、単一のvSphere Web Clientからリンク モードと非リンク モードの両方で管理することができます。

注：VSCをvCenter Serverと一緒に使用する場合は、管理するvCenter ServerインスタンスごとにVSCインスタンスを1つ設定または登録する必要があります。登録するすべてのVSCインスタンスのバージョンを同じにする必要があります。

リンク モードは、vCenter Serverの導入時に自動的に設定されます。リンク モードでは、Microsoft Active Directory Application Mode（ADAM）を使用して、複数のvCenter Serverシステムにわたってデータが格納され、同期されます。

vSphere Web Clientを使用して複数のvCenter ServerにわたってVSCタスクを実行するには、次の条件を満たす必要があります。

- VMwareインベントリ内で管理するvCenter Serverごとに1つVSCサーバを登録して一意の1:1ペアにする必要があります。
  たとえば、VSCサーバAをvCenter Server Aに登録し、VSCサーバBをvCenter Server Bに登録し、VSCサーバCをvCenter Server Cに登録できます。
  VSCサーバAをvCenter Server AとvCenter Server Bの両方に登録することは**できません**。
  また、VSCサーバが登録されていないvCenter ServerがVMwareインベントリに1つでも含まれている場合は、インベントリ内の他の1つ以上のvCenter ServerにVSCが登録されていても、VSCのインスタンスが一切表示されません。
- Single Sign-On（SSO;シングル サインオン）に登録された各vCenter Serverに、VSC固有のView権限が必要です。
  適切なRBACアクセス許可も必要です。

vCenter Serverの指定を必要とするタスクを実行する場合は、**[vCenter Server]**ドロップダウン ボックスに指定可能なvCenter Serverがアルファベット順に表示されます。デフォルトのvCenter Serverが、常にドロップダウン リストの先頭のサーバとなります。

ストレージの場所が認識されている場合（たとえば、特定のvCenter Serverで管理されているホスト上にデータストアがある状態でプロビジョニング ウィザードを使用した場合）は、vCenter Serverの一覧が読み取り専用オプションとして表示されます。これは、vSphere Web Clientで右クリック オプションを使用して項目を選択した場合にのみ該当します。

VSCで管理していないオブジェクトを選択しようとすると警告が表示されます。

VSCの概要ページで、特定のvCenter Serverに基づいてストレージ システムをフィルタリングできます。概要ページは、vCenter Serverに登録されているすべてのVSCインスタンスで表示されます。特定のVSCインスタンスとvCenter Serverに関連付けられているストレージ システムを管理できますが、複数のVSCインスタンスを実行する場合は、ストレージ システムごとに登録情報を分けておく必要があります。

VSCプリファレンス ファイルの設定

プリファレンス ファイルには、Virtual Storage Console for VMware vSphereの処理を制御する設定が格納されています。ほとんどの場合、これらのファイル内の設定を変更する必要はあ

りません。Virtual Storage Console（VSC）で使用されるプリファレンス ファイルを把握しておくと役立ちます。

VSCには複数のプリファレンス ファイルがあります。これらのファイルには、VSCによるさまざまな処理の実行方法を決定するエントリ キーと値が含まれています。VSCで使用される一部のプリファレンス ファイルを次に示します。

`/opt/netapp/vscserver/etc/kamino/kaminoprefs.xml`

`/opt/netapp/vscserver/etc/vsc/vscPreferences.xml`

状況によっては、プリファレンス ファイルを変更しなければならない場合があります。たとえば、iSCSIまたはNFSを使用していて、ESXiホストとストレージ システムとでサブネットが異なる場合は、プリファレンス ファイルを変更する必要があります。プリファレンス ファイル内の設定を変更しないと、VSCでデータストアをマウントできないためにデータストアのプロビジョニングが失敗します。

IPv4またはIPv6の設定

プリファレンス ファイル`kaminoprefs.xml`に新しいオプションが追加されました。このオプションを使用して、VSCに追加されるすべてのストレージ システムに対してIPv4またはIPv6のサポートを有効にすることができます。

- `kaminoprefs.xml`プリファレンス ファイルに、データストアのプロビジョニングで優先的に使用するデータLIFプロトコルを設定するための`default.override.option.provision.mount.datastore.address.family`パラメータが追加されました。
  このプリファレンスは、VSCに追加されるすべてのストレージ システムに適用されます。
- 新しいオプションの値は、`IPv4`、`IPv6`、および`NONE`です。
- デフォルトでは、この値は`NONE`に設定されています。

値	説明
NONE	• プロビジョニングの際、クラスタ管理LIFまたはSVM管理LIFと同じIPv6またはIPv4アドレス タイプのデータLIFを使用してストレージが追加されます。 • 同じIPv6またはIPv4アドレス タイプのデータLIFがSVMに存在しない場合は、他のタイプのデータLIF（利用可能な場合）を使用してプロビジョニングが実行されます。
IPv4	• 選択したSVM内のIPv4データLIFを使用してプロビジョニングが実行されます。 • SVMにIPv4データLIFがない場合は、IPv6データLIF（そのSVM内にある場合）を使用してプロビジョニングが実行されます。

値	説明
IPv6	• 選択したSVM内のIPv6データLIFを使用してプロビジョニングが実行されます。 • SVMにIPv6データLIFがない場合は、IPv4データLIF（そのSVM内にある場合）を使用してプロビジョニングが実行されます。

異なるサブネット間でのデータストアのマウントの有効化

iSCSIまたはNFSを使用していて、ESXiホストとストレージ システムとでサブネットが異なる場合は、Virtual Storage Console for VMware vSphereのプリファレンス ファイルを変更する必要があります。プリファレンス ファイルを変更しないと、Virtual Storage Console（VSC）でデータストアをマウントできないためにデータストアのプロビジョニングが失敗します。

タスク概要

データストアのプロビジョニングに失敗した場合、以下のエラー メッセージが記録されます。

```
Unable to continue. No ip addresses found when cross-referencing kernel ip addresses and addresses on the controller.
```

```
Unable to find a matching network to NFS mount volume to these hosts.
```

手順

1. vCenter Serverインスタンスにログインします。
2. 統合アプライアンス仮想マシンを使用してメンテナンス コンソールを起動します。

   *VSC、VASA Provider、SRA*仮想アプライアンスのメンテナンス コンソールのオプションへのアクセス（31ページ）
3. 「**4**」と入力して、**[Support and Diagnostics]**オプションにアクセスします。
4. 「**2**」と入力して、**[Access Diagnostic Shell]**オプションにアクセスします。
5. 「**`vi /opt/netapp/vscserver/etc/kamino/kaminoprefs.xml`**」と入力して`kaminoprefs.xml`ファイルを更新します。
6. `kaminoprefs.xml`ファイルを更新します。

インターフェイス	操作
iSCSI	エントリ キー`default.allow.iscsi.mount.networks`の値を「ALL」からESXiホストのネットワークの値に変更します。
NFS	エントリ キー`default.allow.nfs.mount.networks`の値を「ALL」からESXiホストのネットワークの値に変更します。

プリファレンス ファイルには、これらのエントリ キー用のサンプル値が含まれています。

注 :「ALL」はすべてのネットワークという意味ではありません。「ALL」はホストとストレージ システムの間にある一致するすべてのネットワークを、データストアのマウントに使用できることを意味します。ホスト ネットワークを指定した場合、マウントを有効にできるのは指定したサブネット間のみになります。

7. `kaminoprefs.xml`ファイルを保存して、閉じます。

VSC、VASA Provider、SRA仮想アプライアンスのメンテナンス コンソールのオプションへのアクセス

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスのメンテナンス コンソールを使用して、アプリケーション、システム、およびネットワークの構成を管理できます。管理者パスワードとメンテナンス パスワードを変更できるほか、 サポート バンドルの生成、別のログ レベルの設定、TLS設定の表示と管理、およびリモート診断の開始を実行できます。

開始する前に

VSC、VASA Provider、SRA仮想アプライアンスの導入後にVMware Toolsをインストールしておく必要があります。

タスク概要

- ユーザ名「maint」とパスワード「admin123」を使用して、VSC、VASA Provider、SRA仮想アプライアンスのメンテナンス コンソールにログインする必要があります。
- 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。

手順

1. 導入した仮想アプライアンスの**[サマリ]**タブにアクセスします。
2.  をクリックして、メンテナンス コンソールを起動します。

   次のメンテナンス コンソール オプションにアクセスできます。

   アプリケーション設定

   次のオプションを使用できます。

   - サーバ ステータスのサマリの表示
   - Virtual Storage Consoleサービスの開始
   - Virtual Storage Consoleサービスの停止
   - VASA ProviderおよびSRAサービスの開始
   - VASA ProviderおよびSRAサービスの停止
   - 「管理者」ユーザのパスワードの変更
   - 証明書の再生成
   - キーストアおよび証明書のハード リセット
   - データベースのハード リセット
   - Virtual Storage Consoleサービスのログ レベルの変更
   - VASA ProviderおよびSRAサービスのログ レベルの変更
   - TLS設定の表示
   - TLSプロトコルの有効化

- TLSプロトコルの無効化

システム設定

次のオプションを使用できます。

- 仮想マシンのリブート
- 仮想マシンのシャットダウン
- 「maint」ユーザのパスワードの変更
- タイム ゾーンの変更
- NTPサーバの変更
  NTPサーバのIPv6アドレスを指定できます。
- SSHアクセスの有効化 / 無効化
- jailディスク サイズ（/jail）の拡張
- アップグレード
- VMware Toolsのインストール

ネットワーク設定

次のオプションを使用できます。

- IPアドレス設定の表示
- IPアドレス設定の変更
  このオプションを使用すると、導入後にIPアドレスをIPv6に変更できます。
- ドメイン名検索設定の表示
- ドメイン名検索設定の変更
- 静的ルートの表示
- 静的ルートの変更
  このオプションを使用すると、IPv6ルートを追加できます。
- 変更内容のコミット
- ホストへのpingの実行
  このオプションを使用すると、IPv6ホストに対してpingを実行できます。
- デフォルト設定のリストア

サポートと診断

次のオプションを使用できます。

- サポート バンドルの生成
- 診断シェルへのアクセス
- リモート診断アクセスの有効化

関連概念

Virtual Storage ConsoleとVASA Providerのログ ファイル（53ページ）

Web CLIへのアクセスと管理者パスワードの変更

VSC、VASA Provider、SRA仮想アプライアンスのWeb CLIにアクセスして、導入後に管理者パスワードを変更できます。

手順

1. `https://<IP>:9083`を使用してWebコマンドライン インターフェイス（CLI）にアクセスします。

   IPアドレスは、VSC、VASA Provider、SRA仮想アプライアンスの導入時に指定したIPアドレスです。

2. 導入時に指定した管理者のユーザ名とパスワードを使用して、Web CLIにログインします。

3. 8～63文字のパスワードを作成します。

VSC、VASA Provider、SRA仮想アプライアンスの高可用性の設定

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスでは、VSC、VASA Provider、SRAの機能を中断させないためのハイアベイラビリティ（HA）構成がサポートされます。

VSC、VASA Provider、SRA仮想アプライアンスはVMware vSphereのハイアベイラビリティ（HA）機能とフォールト トレランス（FT）機能を活用することで高可用性を実現します。ハイアベイラビリティ（HA）ソリューションは、次の原因でシステムが停止した場合に迅速なリカバリを提供します。

- ホストの障害
- ネットワークの障害
- 仮想マシンの障害（ゲストOSの障害）
- アプリケーション（VSC、VASA Provider、SRA）のクラッシュ

高可用性を確保するために仮想アプライアンスで必要な設定は特にありません。vCenter ServerおよびESXホストでのみ、要件に応じてVMware vSphere HAまたはvSphere FTを設定する必要があります。HAとFTのどちらにも、クラスタ ホストと共有ストレージが必要です。FTには追加の要件と制限事項があります。

VMware vSphere HAソリューションとvSphere FTソリューションに加え、仮想アプライアンスもVSC、VASA Provider、SRAのサービスの常時実行をサポートします。仮想アプライアンスのwatchdogプロセスが3つのサービスをすべて定期的に監視し、何らかの障害を検出するとサービスを自動的に再起動します。これにより、アプリケーションの障害を防止できます。

VMware vSphere HA

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスが導入されたvSphere環境をハイアベイラビリティ（HA）構成にすることができ

ます。VMware HAは、仮想環境でハードウェアやオペレーティング システムの障害が発生した場合にフェイルオーバー保護を実現します。

仮想マシンを監視してオペレーティングシステムやハードウェアの障害を検出し、 リソース プールにある他の物理サーバ上の仮想マシンを再起動します。サーバの障害が検出された場合、手動での対応は不要です。

VMware HAの設定手順は、vCenter Serverのバージョンによって異なります。VMware HAの設定手順を確認するには、次の参照先で必要なvCenter Serverバージョンを選択してください。

*VMware vSphere*のドキュメント：「*vSphere HA* クラスタの作成と使用」

VMware vSphereフォールト トレランス

VMware vSphereフォールト トレランス（FT）機能を使用すると、高度なハイアベイラビリティ（HA）を実現し、データや接続が失われないよう仮想マシンを保護することができます。VSC、VASA Provider、SRA仮想アプライアンスのvSphere FT機能は、vCenter Serverから有効または無効にする必要があります。

環境内の仮想アプライアンスに必要な数のvCPU（少なくとも2個、大規模環境の場合は4個）とFTがvSphereライセンスでサポートされていることを確認してください。

vSphere FTを使用すると、サーバの障害時にも仮想マシンを継続的に稼働できます。仮想マシンでvSphere FTが有効な場合は、Distributed Resource Scheduler（DRS）で選択された別のホスト（セカンダリ仮想マシン）にプライマリ仮想マシンのコピーが自動的に作成されます。DRSが有効になっていない場合は、使用可能なホストの中から選択されます。vSphere FTでは、プライマリ仮想マシンの稼働状態をセカンダリ仮想マシンにミラーリングすることで、プライマリ仮想マシンとセカンダリ仮想マシンをロックステップ モードで運用します。

ハードウェア障害によってプライマリ仮想マシンが動作しなくなると、プライマリ仮想マシンが停止したポイントがセカンダリ仮想マシンですぐに検出され、 ネットワーク接続、トランザクション、データが失われることなく、セカンダリ仮想マシンで実行が継続されます。

ご使用のシステムが、vCenter Serverインスタンス向けにvSphere FTを設定するためのCPU要件、仮想マシンの制限要件、ライセンス要件を満たしている必要があります。

HAの設定手順は、vCenter Serverのバージョンによって異なります。HAの設定手順を確認するには、次の参照先で必要なvCenter Serverバージョンを選択してください。

*VMware vSphere*のドキュメント：「*Fault Tolerance* の要件、制限、およびライセンス」

VSC、VASA Provider、SRA仮想アプライアンスでサポートされるMetroCluster構成

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスでは、ONTAPのMetroCluster構成を使用する環境がサポートされます。ほとんどのサポートは自動的に行われますが、MetroCluster環境をVSCで使用している場合とVASA Providerで使用している場合はいくつかの違いがあります。

MetroCluster構成とVSC

プライマリ サイトとセカンダリ サイトでVSCがストレージ システム コントローラを検出することを確認する必要があります。通常、VSCは自動的にストレージ コントローラを検出します。クラスタ管理LIFを使用している場合は、VSCが両方のサイトでクラスタを検出したことを確認することを推奨します。検出されていない場合は、手動でストレージ コントローラをVSCに追加できます。VSCがストレージ コントローラへの接続に使用するユーザ名とパスワードのペアを変更することもできます。

スイッチオーバーが発生した場合、セカンダリ サイトのSVMがテイクオーバーします。このようなSVMには、名前に「-mc」というサフィックスがつけられています。プロビジョニングなど、何らかの処理を実行中にスイッチオーバー操作が発生すると、データストアが存在するSVMの名前が「-mc」サフィックスのついたものに変わります。スイッチバックが発生してプライマリ サイトのSVMに制御が戻ると、このサフィックスは削除されます。

注: MetroCluster構成の直接接続SVMをVSCに追加した場合は、スイッチオーバー後にSVM名の変更（「-mc」サフィックスの追加）が反映されません。他のスイッチオーバー操作は、いずれも引き続き通常どおりに実行されます。

スイッチオーバーまたはスイッチバック後、VSCで自動的にクラスタが検出されて認識されるまでに数分かかる場合があります。データストアのプロビジョニングなどのVSC処理を実行中にスイッチオーバーまたはスイッチバックが発生した場合、処理に遅れが生じることがあります。

MetroCluster構成とVASA Provider

VASA Providerでは、MetroCluster構成を使用する環境が自動的にサポートされます。VASA Provider環境では、スイッチオーバーは透過的に行われます。直接接続SVMをVASA Providerに追加することはできません。

注： VASA Providerでは、スイッチオーバーの実行後にセカンダリ サイトのSVMの名前に「-mc」というサフィックスが付加されません。

MetroCluster構成とSRA

SRAではMetroCluster構成がサポートされません。

ストレージ システム環境の設定

Virtual Storage Console for VMware vSphereでは、1つのメカニズムでストレージ システムの検出とストレージ クレデンシャルの設定が実行されます。クレデンシャルに基づいて、Virtual Storage Console（VSC）ユーザがストレージ システムを使用してタスクを実行するために必要なONTAPアクセス許可が付与されます。

VSCでストレージ リソースを表示して管理するには、まずストレージ システムを検出しなければなりません。検出プロセスでは、ストレージ システムのONTAPクレデンシャルが必要になります。これはユーザ名とパスワードのペアに関連付けられた権限（ロール）で、ストレージ システムごとに割り当てられます。これらのユーザ名とパスワードのペアは、ONTAP RBACを使用するため、ONTAPで設定する必要があります。これらのクレデンシャルをVSCで変更することはできません。ONTAP RBACロールはRBAC User Creator for ONTAPなどのツールを使用して定義できます。これらのクレデンシャルをVSCで変更することはできません。

注 : 管理者としてログインすると、そのストレージ システムに対するすべての権限が自動的に付与されます。

VSCにストレージ システムを追加するときは、ストレージ システムのIPアドレスと、そのシステムに関連付けられているユーザ名とパスワードのペアを指定する必要があります。VSCがストレージ システムの検出プロセスで使用するデフォルト クレデンシャルを設定することも、ストレージ システムが検出されたときにクレデンシャルを手動で入力することもできます。 VSCに追加されるストレージ システムの詳細は、導入環境で有効にする拡張機能に自動的にプッシュされます。そのため、VASA ProviderとStorage Replication Adapter（SRA）にストレージを手動で追加する必要はありません。VSCとSRAは、クラスタ レベルおよびStorage Virtual Machine（SVM）レベルでクレデンシャルの追加をサポートします。VASA Providerは、ストレージ システムを追加するためのクラスタ レベルのクレデンシャルのみをサポートします。

環境に複数のvCenter Serverインスタンスが含まれている場合に[ストレージ システム]ページからVSCにストレージ システムを追加しようとすると、**[ストレージ システムの追加]**ダイアログ ボックスに、ストレージ システムを追加するvCenter Serverインスタンスを指定するための**[vCenter Server]**ボックスが表示されます。データセンター名を右クリックしてストレージ システムを追加する場合は、そのデータセンターにサーバがすでに関連付けられているため、vCenter Serverインスタンスを指定するオプションは表示されません。

検出は次の場合に実行されます。いずれの場合も、新しいストレージ システムが検出されるたびにクレデンシャルを指定する必要があります。

- VSCサービスを開始したとき（バックグラウンドでVSCによる自動検出プロセスが開始されます）
- [ストレージ システム]ページの**[すべて再検出]**ボタンをクリックしたとき、 ホストまたはデータセンターで、[アクション]メニュー（**[アクション]** > **[Netapp VSC]** > **[ホスト データとストレージ データの更新]**）から[すべて再検出]ボタンを選択したとき、または[概要]の[クイック ガイド]タブにある**[検出]**をクリックしたとき

注 : IPv6アドレスはサポートされません。

VSCの機能を使用してタスクを実行するときは、いずれも特定のアクセス許可が必要になります。ユーザが実行できる操作は、ONTAPロールに関連付けられたクレデンシャルに基づいて制限できます。ストレージ システムのユーザ名とパスワードのペアを同じにすれば、複数のユーザで同じストレージ システムのクレデンシャルを共有し、同じ処理を実行することができます。

ストレージ システムのデフォルト クレデンシャルの設定

Virtual Storage Console for VMware vSphereを使用して、vCenter Serverでストレージ システムのデフォルト クレデンシャルを設定できます。

開始する前に

デフォルト クレデンシャルの作成に使用するvCenter Serverを選択しておく必要があります。

タスク概要

ストレージ システムのデフォルト クレデンシャルを設定すると、Virtual Storage Console（VSC）ではそれらのクレデンシャルを使用して、VSCが検出したストレージ システムにログインします。デフォルト クレデンシャルでログインできない場合は、ストレージ システムに手動でログインする必要があります。VSCとSRAは、クラスタ レベルまたはSVMレベルでストレージ システムのクレデンシャルの追加をサポートします。ただし、VASA Providerはクラスタ レベルのクレデンシャルとのみ連携します。

手順

1. VSCの**[ホーム]**ページで、**[設定]** > **[管理設定]** > **[ストレージ システムのデフォルト クレデンシャルの設定]**をクリックします。
2. **[ストレージ システムのデフォルト クレデンシャル]**ダイアログ ボックスで、ストレージ システムのユーザ名とパスワードを入力します。

   ストレージ コントローラのクレデンシャルは、ユーザ名とパスワードのペアに基づいてONTAPで割り当てられます。ストレージ コントローラのクレデンシャルは、管理者アカウントまたはロールベース アクセス制御（RBAC）を使用するカスタム アカウントです。

   ストレージ コントローラのユーザ名とパスワードのペアに関連付けられているロールをVSCで変更することはできません。ストレージ コントローラのクレデンシャルを変更するには、RBAC User Creator for ONTAPなどのツールを使用する必要があります。
3. **[OK]**をクリックして、デフォルト クレデンシャルを保存します。

次のタスク

ストレージ システムのステータスが「認証エラー」になったためにストレージ システムのクレデンシャルを更新した場合は、[ストレージ システム]ページの**[すべて再検出]**オプションをクリックする必要があります。これにより、新しいクレデンシャルを使用してストレージ システムへの接続が試行されます。

VSCへのストレージ システムの追加

ストレージ システムは、手動でVirtual Storage Console（VSC）に追加できます。ストレージ システムの数が多い場合は、**[すべて再検出]**オプションを使用してストレージ システムを検出するより、手動で新しいストレージ システムを追加した方が速い場合があります。

タスク概要

Virtual Storage Console（VSC）を開始するか、**[すべて再検出]**オプションを選択すると、使用可能なストレージ システムがVSCで自動的に検出されます。VSCに手動でストレージ システムを追加することもできます。

手順

1. VSCの[ホーム]ページを使用して、VSCにストレージ システムを追加します。
   - **[ストレージ システム]** > **[追加]**をクリックします。
   - **[概要]** > **[開始]**をクリックし、[ストレージ システムの追加]にある**[追加]**ボタンをクリックします。
2. **[ストレージ システムの追加]**ダイアログ ボックスで、ストレージ システムの管理IPアドレスとクレデンシャルを入力します。

   クラスタまたはSVMのIPv6アドレスを使用してストレージ システムを追加することもできます。このダイアログ ボックスでは、TLSのデフォルト値とポート番号を変更することもできます。

   VSCの[ストレージ システム]ページからストレージを追加する場合は、ストレージを配置するvCenter Serverインスタンスも指定する必要があります。[ストレージ システムの追加]ダイアログ ボックスには、使用可能なvCenter Serverインスタンスがドロップダウンリストに表示されます。vCenter Serverインスタンスにすでに関連付けられているデータセンターにストレージを追加する場合、このオプションは表示されません。
3. 必要な情報をすべて追加したら、**[OK]**をクリックします。

ストレージ システムとホストの検出

vSphere ClientでのVirtual Storage Console（VSC）の初回実行時に、ESXiホスト、そのLUNとNFSエクスポート、およびLUNとエクスポートを所有するネットアップ ストレージ システムがVSCによって検出されます。

開始する前に

- すべてのESXiホストの電源をオンにして接続しておく必要があります。
- 検出するStorage Virtual Machine（SVM）を実行しておく必要があります。また、使用中のストレージ プロトコル（NFS、iSCSI、またはFC）用のデータLIFを各クラスタ ノードに少なくとも1つ設定しておく必要があります。

タスク概要

新しいストレージ システムの検出や既存のストレージ システムの情報の更新はいつでも実行でき、容量や設定に関する最新の情報を確認することができます。VSCでストレージ システムへのログインに使用されるクレデンシャルを変更することもできます。

ストレージ システムの検出時に、VSCはvCenter Serverインスタンスで管理しているESXiホストから情報を収集します。

手順

1. vSphere Clientの**[ホーム]**ページで、**[ホストおよびクラスタ]**を選択します。
2. 必要なデータセンターを右クリックし、**[NetApp VSC]** > **[ホスト データとストレージ データの更新]**を選択します。

   処理に時間がかかる場合があることを示す[確認]ダイアログ ボックスが表示されます。
3. **[OK]**をクリックします。
4. 検出されたストレージ コントローラのうち、ステータスが「認証エラー」であるものを選択し、**[アクション]** > **[変更]**をクリックします。

5. **[ストレージ システムの変更]**ダイアログ ボックスで必要な情報を入力します。
6. ステータスが「認証エラー」のすべてのストレージ コントローラについて、手順4と5を繰り返します。

次のタスク

検出プロセスが完了したら、次の手順を実行します。

- [アダプタ設定]、[MPIO 設定]、または[NFS 設定]の列に[アラート]アイコンが表示されているESXiホストについて、VSCを使用して設定を行います。
- ストレージ システムのクレデンシャルを入力します。

ストレージ システムの表示の更新

Virtual Storage Console for VMware vSphereの更新機能を使用して、ストレージ システムに関する情報を更新し、Virtual Storage Console（VSC）でストレージ システムを検出することができます。

タスク概要

「更新」オプションは、認証エラーの発生後にストレージ システムのデフォルト クレデンシャルを変更した場合に役立ちます。ストレージ システムのステータスが「認証エラー」になったためにストレージ システムのクレデンシャルを変更した場合は、必ず更新処理を実行してください。更新処理では、VSCが新しいクレデンシャルを使用してストレージ システムへの接続を試みます。

システムの設定によっては、この処理が完了するまでに時間がかかることがあります。

手順

1. VMware vSphere Clientの**[ホーム]**ページで、**[ストレージ システム]**をクリックします。
2. 更新を開始します。

現在の場所	操作
Virtual Storage Console	**[すべて再検出]**アイコン
データセンター	データセンターを右クリックし、**[NetApp VSC]** > **[ホスト データとストレージ データの更新]**をクリックします。

3. **[ホスト データとストレージ データの更新]**ダイアログ ボックスで**[OK]**をクリックします。

   データセンター内のホストとストレージ システムの数によっては、検出に数分かかる場合があります。この検出処理はバックグラウンドで実行されます。
4. **[成功]**ダイアログ ボックスで**[OK]**をクリックします。

VSC for VMware vSphereでのvCenter Server RBAC機能の使用

vCenter ServerのRBACを使用すると、vSphereオブジェクトへのアクセスを制御できます。Virtual Storage Console for VMware vSphereでは、vCenter Server RBACとONTAP RBACにより、特定のストレージ システムのオブジェクトに対して特定のユーザが実行できるVSCタスクが決まります。

タスクを完了するには、適切なvCenter Server RBACアクセス許可が必要です。VSCでのタスクの実行時、まずユーザのvCenter Serverアクセス許可が確認され、次にユーザのONTAP権限が確認されます。

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、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。

vCenter Serverアクセス許可の要素

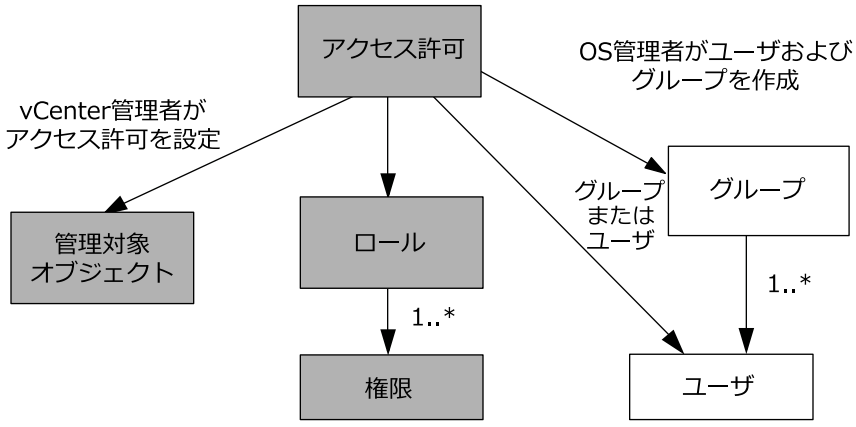
vCenter Serverで認識されるのはアクセス許可で、権限ではありません。vCenter Serverアクセス許可は3つの要素で構成されます。

vCenter Serverの要素は次のとおりです。

- 1つまたは複数の権限（ロール）
  ユーザが実行できるタスクを定義します。
- vSphereオブジェクト
  タスクの対象オブジェクトです。
- ユーザまたはグループ
  タスクを実行できるユーザまたはグループを定義します。

次の図に示すように、3つの要素がすべて揃っていないとアクセスは許可されません。

注 : グレーのボックスはvCenter Server側の要素、白のボックスはvCenter Serverを実行しているオペレーティング システム側の要素を表しています。



権限

Virtual Storage Console for VMware vSphereに関連付けられる権限は2種類あります。

- vCenter Server標準の権限
  vCenter Serverに付属している権限です。
- VSC固有の権限
  特定のVSCタスク用に定義された、 VSC固有の権限です。

VSCのタスクを実行するには、VSC固有の権限とvCenter Server標準の権限の両方が必要です。これらの権限からユーザの「ロール」が構成されます。アクセス許可には複数の権限を含めることができます。

注：vCenter Server RBACの使用を簡単にするため、VSCには、VSCタスクの実行に必要なVSC固有の権限と標準の権限をすべて含む標準ロールがいくつか用意されています。

アクセス許可に含まれる権限が変更された場合、そのアクセス許可が関連付けられたユーザは、更新されたアクセス許可を有効にするためにログアウトしてログインし直す必要があります。

表 2：VSCの権限

権限	ロール	タスク
NetApp Virtual Storage Console > **View**	• VSC Administrator • VSC Provision • VSC Read-Only	VSCおよびVASA Provider固有のタスクにはすべてView権限が必要です。
NetApp Virtual Storage Console > **Policy Based Management** > **Management** または **privilege.nvpfVSC.VASAGroup.com.netapp.nvpf.label** > **Management**	VSC Administrator	ストレージ機能プロファイルおよびしきい値設定に関連するVSCおよびVASA Providerのタスク。

vSphereオブジェクト

アクセス許可はvSphereオブジェクトに関連付けられます。vCenter Server、ESXiホスト、仮想マシン、データストア、データセンター、フォルダなど、 任意のvSphereオブジェクトにアクセス許可を割り当てることができます。vSphereオブジェクトに割り当てられたアクセス許可に基づいて、そのオブジェクトに対してどのユーザがどのタスクをvCenter Serverで実行できるかが決まります。VSC固有のタスクについては、アクセス許可の割り当てと検証はルートフォルダ レベル（vCenter Server）でのみ行われ、それ以外のエンティティでは行われません。ただしVAAIプラグインの処理は例外で、関連するESXiに対してアクセス許可が検証されます。

ユーザとグループ

ユーザとグループは、Active Directory（またはローカルのvCenter Serverマシン）を使用して設定できます。その後、設定したユーザまたはグループにvCenter Serverアクセス許可を付与することで、特定のVSCタスクの実行を許可することができます。

注：これらのvCenter Serverアクセス許可は、VSC管理者以外のVSC vCenterユーザに適用されます。VSC管理者には、デフォルトでフル アクセスが許可されるため、アクセス許可を割り当てる必要はありません。

ユーザとグループにはロールは割り当てられません。vCenter Serverアクセス許可を割り当てることで、間接的にロールが適用されます。

vCenter Serverのアクセス許可の割り当てと変更に関する要点

vCenter Serverのアクセス許可を使用する際にはいくつかの注意点があります。Virtual Storage Console for VMware vSphereのタスクを実行できるかどうかは、アクセス許可を割り当てた場所、およびアクセス許可の変更後にユーザが実行した操作によって決まります。

vCenter Serverのアクセス許可は、vSphereのオブジェクトおよびタスクへのアクセスを制限したい場合にのみ設定します。アクセス許可を設定しない場合は、管理者としてログインできます。管理者としてログインした場合、自動的にすべてのvSphereオブジェクトへのアクセスが可能になります。

アクセス許可の割り当て

アクセス許可を割り当てる場所によって、ユーザが実行できるVSCタスクが決まります。

タスクによっては、最後まで実行するためにはルート オブジェクトなどの上位レベルにアクセス許可を割り当てる必要があります。具体的には、特定のvSphereオブジェクトには適用されない権限（タスクの追跡など）がタスクに必要な場合や、必要な権限がvSphere以外のオブジェクト（ストレージ システムなど）に適用される場合です。

これらの場合には、子エンティティに継承されるようにアクセス許可を設定します。子エンティティには、その他のアクセス許可も割り当てることができます。子エンティティに割り当てたアクセス許可は、親エンティティから継承されたアクセス許可を上書きします。したがって、子エンティティにアクセス許可を割り当てることで、ルート オブジェクトに割り当てられ、子エンティティに継承されたアクセス許可の対象を制限することができます。

ヒント：会社のセキュリティ ポリシーでアクセス許可を厳しく制限することが求められる場合を除き、ルート オブジェクト（ルート フォルダとも呼ばれる）にアクセス許可を割り当てることをお勧めします。

アクセス許可と非vSphereオブジェクト

作成した権限は、vSphere以外のオブジェクトに適用されます。たとえば、ストレージ システムはvSphereオブジェクトではありません。ある権限がストレージ システムに適用される場合、アクセス許可を割り当てることができるvSphereオブジェクトがないため、その権限を含むアクセス許可をVSCルート オブジェクトに割り当てる必要があります。

たとえば、「Add/Modify/Skip storage systems」といったVSC権限を含む任意のアクセス許可は、ルート オブジェクト レベルに割り当てる必要があります。

アクセス許可の変更

一度に変更できるアクセス許可は1つです。

アクセス許可に含まれる権限が変更された場合、そのアクセス許可が関連付けられたユーザは、更新されたアクセス許可を有効にするためにログアウトしてログインし直す必要があります。

VSC、VASA Provider、SRA仮想アプライアンスに組み込みの標準ロール

Virtual Storage Console（VSC）には、vCenter Serverの権限とRBACを簡単に使用できるように、主要なVSCタスクを実行できる標準のVSCロールが用意されています。また、タスクの実行を制限し、VSC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。

標準のVSCロールには、ユーザがVSCタスクを実行するために必要なVSC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、サポートされるどのバージョンのvCenter Serverでも必要な権限が含まれるように設定されています。

管理者は、必要に応じて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。

注：VSCを最新バージョンにアップグレードした場合は、新しいバージョンのVSCで使用できるように自動的にアップグレードされます。

標準のVSCロールを表示するには、vSphere Clientの[ホーム]ページの**[ロール]**をクリックします。

VSCの組み込みのロールで実行できるタスクを次に示します。

ロール	説明
VSC Administrator	すべてのVSCタスクを実行するために必要なvCenter Server標準の権限とVSC固有の権限がすべて含まれています。
VSC Read-Only	VSCに対する読み取り専用アクセスが許可されます。 アクセスが制御されたVSCの処理は実行できません。
VSC Provision	ストレージのプロビジョニングに必要なvCenter Server標準の権限とVSC固有の権限がすべて含まれています。 次のタスクを実行できます。 • 新しいデータストアの作成 • データストアの破棄 • ストレージ機能プロファイルに関する情報の表示

VSCの標準ロールの使用に関するガイドライン

Virtual Storage Console for VMware vSphereの標準ロールを使用するときは、一定のガイドラインに留意する必要があります。

標準ロールは直接変更しないでください。ロールを直接変更すると、VSCをアップグレードするたびに変更が上書きされます。VSCをアップグレードすると、インストーラによって標準ロールの定義が更新されます。これは、そのバージョンのVSCおよびサポートされるすべてのバージョンのvCenter Serverでロールを最新の状態に維持するためです。

代わりに、標準ロールを使用して環境に応じたカスタム ロールを作成することができます。これを行うには、VSCの標準ロールをコピーし、そのロールを編集します。この方法で作成したロールは、VSC Windowsサービスを再起動またはアップグレードしても維持されます。

VSCの標準ロールの用途としては次のケースが考えられます。

- すべてのVSCタスクに標準のVSCロールを使用する。
  このシナリオでは、標準ロールはVSCタスクの実行に必要なすべての権限をユーザに提供します。

- 複数のロールを組み合わせてユーザが実行できるタスクを拡張する。
  単独では要件に合う標準のVSCロールがない場合は、複数のロールを含む上位グループを作成してロールを拡張することができます。
  ユーザがvCenter Server標準の別の権限を必要とするVSC以外のタスクも実行する必要がある場合は、それらの権限を提供するロールを作成し、グループに追加します。
- より細分化されたロールを作成する。
  標準のVSCロールよりも少ない権限のロールが必要な場合は、VSCロールを使用して新しいロールを作成することができます。
  この場合は、必要なVSCロールのクローンを作成してから、そのクローンを編集してユーザに必要な権限だけを残します。

VSCタスクに必要な権限

各種のVirtual Storage Console for VMware vSphereタスクを実行するには、Virtual Storage Console（VSC）固有の権限とvCenter Server標準の権限のさまざまな組み合わせが必要です。

VSCタスクに必要な権限については、ネットアップの技術情報アーティクル1032542。

ネットアップ ナレッジベースの回答*1032542*：「*How to configure RBAC for Virtual Storage Console*」

VSC for VMware vSphereで必要とされる製品レベルの権限

Virtual Storage Console for VMware vSphereのGUIにアクセスするには、製品レベルのVSC固有のView権限が、適切なvSphereオブジェクト レベルで割り当てられている必要があります。この権限がないユーザがVSCにログインすると、ネットアップアイコンをクリックしたときにエラー メッセージが表示され、VSCにアクセスできません。

次の表に、VSCの製品レベルのView権限について説明します。

権限	説明	割り当てレベル
View	VSCのGUIにアクセスできます。 VSCでタスクを実行することはできません。VSCのタスクを実行するには、タスクで必要とされる適切なVSC固有の権限とvCenter Server標準の権限が必要です。	割り当てレベルによって表示できるUIの領域が決定します。 ルート オブジェクト（フォルダ）にView権限を割り当てた場合、NetAppアイコンをクリックしてVSCにアクセスできます。 他のvSphereオブジェクト レベルにView権限を割り当てることもできますが、その場合は表示および使用できるVSCメニューが制限されます。 View権限を含む任意のアクセス許可は、ルート オブジェクトに割り当てることを推奨します。

VSC、VASA Provider、SRA仮想アプライアンス用のONTAPのRBAC

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。Virtual Storage Console for VMware vSphereで

は、ONTAP RBACとvCenter Server RBACにより、特定のストレージ システムのオブジェクトに対して特定のユーザが実行できるVirtual Storage Console（VSC）タスクが決まります。

VSCでは、各ストレージ システムの認証とそのストレージ システムで実行できるストレージ操作の判別に、VSCで設定したクレデンシャル（ユーザ名とパスワード）が使用されます。ストレージ システムごとに1組のクレデンシャルが使用され、そのクレデンシャルに基づいて、ストレージ システムで実行できるVSCタスクが決まります。つまり、このクレデンシャルはVSCのクレデンシャルであり、個々のVSCユーザに対するものではありません。

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VSCタスク（仮想マシンのプロビジョニングなど）の実行にのみ適用されます。それぞれのストレージ システムに対する適切なONTAP RBAC権限がないと、そのストレージ システムでホストされる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。ONTAP RBACとVSC固有の権限を組み合わせることで、ユーザが実行できるVSCタスクを制御することができます。

- ストレージまたはストレージ システムに格納されているvCenter Serverオブジェクトの監視と設定
- ストレージ システムに格納されているvSphereオブジェクトのプロビジョニング

ONTAP RBACとVSC固有の権限を使用すると、ストレージ主体のセキュリティ レイヤをストレージ管理者が管理できるようになります。これにより、ONTAP RBACまたはvCenter Server RBACのどちらか一方のアクセス制御だけを使用した場合に比べ、よりきめ細かい制御が可能になります。たとえば、vCenter Server RBACを使用して、ネットアップ ストレージでのデータストアのプロビジョニングをvCenterUserBには許可し、vCenterUserAには許可しないように設定したとします。この場合、特定のストレージ システムのクレデンシャルに対してストレージの作成を禁止すれば、vCenterUserBとvCenterUserAのどちらもそのストレージ システムでデータストアのプロビジョニングを実行することはできません。

VSCタスクを開始すると、最初にそのタスクに対する正しいvCenter Serverアクセス許可がユーザにあるかどうかが検証されます。タスクを実行するための十分なvCenter Serverアクセス許可がなければ、最初のvCenter Serverのセキュリティ チェックをパスできないため、そのストレージ システムのONTAP権限は確認されません。そのため、ストレージ システムへのアクセスは許可されません。

十分なvCenter Serverアクセス許可がある場合は、次にストレージ システムのクレデンシャル（ユーザ名とパスワード）に関連付けられたONTAP RBAC権限（ONTAPロール）について、VSCタスクで必要なストレージ操作をそのストレージ システムで実行するための十分な権限があるかどうかが確認されます。適切なONTAP権限があれば、ストレージ システムにアクセスしてVSCタスクを実行できます。ストレージ システムで実行できるVSCタスクはONTAPロールで決まります。

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、VSCはストレージ システムについての監査証跡を提供します。これにより、ストレージに対して変更を行ったvCenter Serverユーザまでさかのぼってイベントを追跡できます。
- ユーザビリティ
  コントローラのクレデンシャルをすべて集約して一元管理できます。

VSC for VMware vSphere使用時に推奨されるONTAPロール

Virtual Storage Console for VMware vSphereでRBACを使用する際には、推奨されるONTAPロールを設定できます。これらのロールには、Virtual Storage Console（VSC）タスクで実行するストレージ処理に必要なONTAP権限が含まれています。

新しいユーザ ロールを作成するには、ONTAPを実行しているストレージ システムに管理者としてログインする必要があります。次のいずれかを使用してONTAPロールを作成できます。

- RBAC User Creator for ONTAPツール
  ネットアップ コミュニティのドキュメント：「*RBAC User Creator for Data ONTAP*」
- ONTAP System Manager（WindowsプラットフォームまたはLinuxプラットフォームにダウンロード可能）

各ONTAPロールには、ロールのクレデンシャルを構成するユーザ名とパスワードのペアが関連付けられています。このクレデンシャルを使用してログインしないと、ロールに関連付けられたストレージ処理にアクセスできません。作成する各ONTAPロールは、1つのユーザ名に関連付けられます。ストレージ システムに対してこれらのロールベースのタスクを実行するには、適切なユーザ名とパスワードのペアを使用してストレージ システムにログインする必要があります。

セキュリティ上の理由から、VSC固有のONTAPロールは階層構造になっています。最初のロールは最も制限のあるロールで、VSCの最も基本的なストレージ処理に関連する権限だけを含みます。次のロールには、そのロール独自の権限と、前のロールに関連付けられているすべての権限が含まれます。以降、上位のロールほど制限が少なく、より多くのストレージ処理をサポートします。

VSCを使用する際に推奨されるONTAP RBACロールのいくつかを次に示します。ロールを作成したら、仮想マシンのプロビジョニングなど、ストレージに関するタスクを実行する必要があるユーザにそのロールを割り当てることができます。

1. Discovery
   ストレージ システムを追加できます。
2. Create Storage
   ストレージを作成できます。また、Discoveryロールに関連付けられているすべての権限が含まれます。
3. Modify Storage
   ストレージを変更できます。また、DiscoveryロールとCreate Storageロールに関連付けられているすべての権限が含まれます。
4. Destroy Storage
   ストレージを破棄できます。また、Discoveryロール、Create Storageロール、Modify Storageロールに関連付けられているすべての権限が含まれます。

VASA Provider for ONTAPを使用する場合は、Policy-Based Management（PBM;ポリシーベース管理）ロールも設定します。ストレージ ポリシーを使用してストレージを管理できます。このロールを使用するには、Discoveryロールも設定する必要があります。

VSC for VMware vSphere用のONTAP RBACの設定

ONTAPのRBACをVirtual Storage Console for VMware vSphere（VSC）で使用する場合は、ストレージ システムでRBACを設定する必要があります。ONTAPのRBAC機能を使用すると、アクセス権限を制限したカスタム ユーザ アカウントを1つ以上作成できます。

VSCとSRAは、クラスタ レベルまたはSVMレベルでストレージ システムにアクセスできます。クラスタ レベルでストレージ システムを追加する場合、必要なすべての機能を使用す

るためには管理者ユーザのクレデンシャルを指定する必要があります。SVMの詳細を直接指定してストレージ システムを追加する場合は、「vsadmin」ユーザには特定のタスクを実行するために必要な一部のロールと権限がないことに注意してください。

VASA Providerは、クラスタ レベルでのみストレージ システムにアクセスできます。特定のストレージ コントローラでVASA Providerが必要な場合は、VSCまたはSRAを使用している場合でも、クラスタ レベルでストレージ システムをVSCに追加する必要があります。

新しいユーザを作成し、クラスタまたはSVMをVSC、VASA Provider、SRAに接続するには、次の作業を行う必要があります。

- ONTAPを使用して、クラスタ管理者またはSVM管理者ロールを作成する。

  注：ロールを作成するには、RBAC User Creator for ONTAPツールを使用します。

  ネットアップ コミュニティのドキュメント：「*RBAC User Creator for Data ONTAP*」

- ONTAPを使用してユーザを作成し、ロールを割り当て、適切なアプリケーションを設定する。
  作成したストレージ システム クレデンシャルは、VSC用にストレージ システムを構成する際に必要です。VSC用のストレージ システムを構成するには、VSCでクレデンシャルを入力する必要があります。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と、クレデンシャルの作成時にONTAPで設定したVSC機能に対する権限が付与されます。
- VSCにストレージ システムを追加し、作成したユーザのクレデンシャルを指定する。

VSCロール

VSCでは、ONTAPの権限を以下に示すVSCロールに分類します。

- Discovery
  接続されているすべてのストレージ コントローラを検出できます。
- Create Storage
  ボリュームおよび論理ユニット番号（LUN）を作成できます。
- Modify Storage
  ストレージ システムのサイズ変更と重複排除を実行できます。
- Destroy Storage
  ボリュームおよびLUNを破棄できます。

VASA Providerロール

クラスタ レベルではPolicy Based Managementのみを作成できます。このロールでは、ストレージ機能プロファイルを使用してポリシーベースでストレージを管理できます。

SRAロール

SRAでは、ONTAPの権限をクラスタ レベルまたはSVMレベルでSANまたはNASロールに分類します。これにより、ユーザはSRM処理を実行できます。

注：ONTAPコマンドを使用してロールと権限を手動で設定する場合は、ネットアップ ナレッジベースの記事を参照してください。

- ネットアップ ナレッジベースの回答*1001058*：「*FAQ: VSC, VASA, and SRA 7.0 ONTAP RBAC Configuration*」
- ネットアップ ナレッジベースの回答*1001056*：「*FAQ: Roll up of all commands for VSC and SRA for SVM level*」

VSCにクラスタを追加する場合は、ONTAP RBACロールの権限の初期検証が実行されます。直接接続のSVMのストレージIPを追加した場合、初期検証は実行されません。タスク ワークフローの段階で権限が確認されて適用されます。

ディザスタ リカバリ用のStorage Replication Adapterの設定

vCenter Serverをディザスタリカバリ用に設定する場合は、Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスを導入したあとにStorage Replication Adapter（SRA）を有効にする必要があります。仮想アプライアンスを導入すると、デフォルトでVSCがインストールされます。仮想アプライアンスの導入後、vCenter ServerのSRAを有効にする必要があります。

関連タスク

Storage Replication Adapterの有効化（19ページ）

SAN環境向けのStorage Replication Adapterの設定

Site Recovery Manager（SRM）向けStorage Replication Adapter（SRA）を実行するには、事前にストレージ システムのセットアップが必要です。

開始する前に

保護対象サイトとリカバリ サイトに次のプログラムがインストールされている必要があります。

- SRM
  SRMのインストールについては、VMwareサイトのドキュメントを参照してください。
  VMware Site Recovery Manager Documentation
- SRA
  SRMとSRAサーバにアダプタをインストールします。

手順

1. 保護対象サイトで、プライマリESXiホストがプライマリ ストレージ システムのLUNに接続されていることを確認します。
2. プライマリ ストレージ システムで、LUNが属するigroupの`ostype`オプションが*vmware*に設定されていることを確認します。
3. リカバリ サイトのESXiホストがFCまたはiSCSIを使用してStorage Virtual Machine（SVM）に適切に接続されていることを確認します。

   確認するには、ESXiホストがSVM上のローカルLUNに接続されていることを確認するか、SVMで`fcp show initiators`コマンドまたは`iscsi show initiators`コマンドを使用します。

NAS環境向けのStorage Replication Adapterの設定

VMware vCenter Site Recovery Manager（SRM）向けStorage Replication Adapter（SRA）を実行するには、事前にストレージ システムの設定が必要です。

開始する前に

保護対象サイトとリカバリ サイトに次のプログラムがインストールされている必要があります。

- SRM
  SRMのインストールに関するドキュメントは、VMwareのサイトで入手できます。
  VMware Site Recovery Managerのドキュメント
- SRA
  SRMとSRAサーバにアダプタをインストールします。

手順

1. 保護対象サイトのデータストアに、vCenter Serverに登録されている仮想マシンがあることを確認します。
2. 保護対象サイトのESXiホストに、Storage Virtual Machine（SVM）のNFSエクスポート ボリュームがマウントされていることを確認します。
3. **Array Manager**ウィザードを使用してSRMにアレイを追加する場合は、NFSエクスポートの場所を示す有効なアドレス（IPアドレス、ホスト名、またはFQDN）が**[NFS Addresses]**フィールドに指定されていることを確認します。
4. リカバリ サイトの各ESXiホストで`ping`コマンドを実行して、SVMがNFSエクスポートへの接続に使用するIPアドレスにホストのVMkernelポートからアクセスできることを確認します。

関連情報

ネットアップ サポート

大規模な環境向けのStorage Replication Adapterの設定

大規模な環境で最適なパフォーマンスを実現するには、Storage Replication Adapter（SRA）の推奨設定に従ってストレージのタイムアウト間隔を設定する必要があります。

ストレージ プロバイダの設定

- `StorageProvider.resignatureTimeout`設定の値を900秒から12,000秒に増やす必要があります。
- `StorageProvider.autoResignatureMode`オプションを有効にする必要があります。

ストレージ プロバイダの設定を変更する方法の詳細については、VMwareのドキュメントを参照してください。

VMware vSphereのドキュメント：「ストレージ プロバイダ設定の変更」

ストレージ設定

大規模な環境では、`storage.commandTimeout`タイムアウト間隔の値を12,000秒に設定する必要があります。

注：このタイムアウト間隔は最大値です。最大タイムアウトに達することはありません。ほとんどのコマンドは、設定された最大タイムアウト間隔以内に終了します。

ネットアップ ナレッジベースの回答*1001111*：「*NetApp Storage Replication Adapter 4.0/7.X for ONTAP Sizing Guide*」

詳細については、SANプロバイダの設定の変更に関するVMwareのドキュメントを参照してください。

VMware Site Recovery Managerのドキュメント：「ストレージ設定の変更」

VSC、VASA Provider、SRA仮想アプライアンスに関する問題のトラブルシューティング

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスのインストール中または設定中に予期しない動作が発生した場合は、特定のトラブルシューティング手順に従って、問題の原因を特定し、解決することができます。

vSphereにキャッシュされたダウンロード済みプラグイン パッケージのクリーンアップ

VSC、VASA Provider、SRA仮想アプライアンスの導入またはアップグレード後にプラグインが自動的に更新されない場合は、ブラウザおよびvCenter Serverにキャッシュされているダウンロード済みプラグイン パッケージをクリーンアップして、vCenter Serverプラグインの問題を解決する必要があります。

手順

1. 既存のvSphere Web ClientまたはvSphere Clientからログアウトします。
2. ブラウザ キャッシュを削除します。
3. vSphere Clientにキャッシュされたプラグイン パッケージを削除します。

対象	操作
Windows vCenterサーバ	次の場所にあるcom.netapp.vasa.vvol.webclient-x.x.x.xxxx、com.netapp.nvpf.webclient-x.x.x.xxxx、com.netapp.vsch5-x.x.x.xxxxの各フォルダを削除します。 • vSphere Web Clientのパス：C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity • vSphere Client（HTML5）のパス：C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity

対象	操作
VCSA	a. SSHでVCSAアプライアンスに接続します。 b. `cd /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity`を使用して、vCenter Web Client UI拡張機能のディレクトリに移動します。 c. 次のコマンドを使用して、キャッシュされたプラグイン パッケージを削除します。 • `rm -rf com.netapp.vasa.vvol.webclient-x.x.x.xxxx` • `rm -rf com.netapp.nvpf.webclient-x.x.x.xxxx` • `rm -rf com.netapp.vsch5-x.x.x.xxxx` d. `cd /etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity`を使用して、vSphere Client（HTML5）UI拡張機能のディレクトリに移動します。 e. 次のコマンドを使用して、キャッシュされたプラグイン パッケージを削除します。 • `rm -rf com.netapp.vasa.vvol.webclient-x.x.x.xxxx` • `rm -rf com.netapp.nvpf.webclient-x.x.x.xxxx` • `rm -rf com.netapp.vsch5-x.x.x.xxxx`

4. vSphereにログインし、次のコマンドを使用してvSphere Web Clientサービスとvsphere Clientサービスを再起動します。
   - `service-control --stop vsphere-client vsphere-ui`
   - `service-control --start vsphere-client vsphere-ui`

アンインストールしても標準のVSCロールは削除されない

Virtual Storage Console for VMware vSphere（VSC）をアンインストールしても、標準のVSCロールはそのまま残ります。これは想定される動作であり、VSCのパフォーマンスや新しいバージョンへのアップグレードには影響しません。これらのロールは、必要に応じて手動で削除できます。

アンインストール処理によってVSCロールは削除されませんが、VSC固有の権限の日本語名が削除され、代わりに「XXX missing privilege」というプレフィックスが追加されます。たとえば、VSCのインストール後にvSphereの[ロールの編集]ダイアログ ボックスを開くと、VSC固有の権限が「`XXX missing privilege.<privilege name>.label not found XXX`」のように表示されます。

これは、vCenter Serverに権限を削除するオプションがないためです。

VSCを再インストールするか新しいバージョンにアップグレードすると、標準のVSCロールとVSC固有の権限がすべてリストアされます。

Virtual Storage ConsoleとVASA Providerのログ ファイル

エラーが発生した場合は、`/opt/netapp/vscserver/logs`ディレクトリと`/opt/netapp/vpserver/logs`ディレクトリのログ ファイルを確認できます。

問題の特定には、次の2つのログ ファイルが役立ちます。

- `cxf.log`：VASA Providerとの間のAPIトラフィックに関する情報が記録されます。
- `kamino.log`：VSC設定に関する情報が記録されます。
- `vvolvp.log`：VASA Providerに関するすべてのログ情報が記録されます。

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスのメンテナンス メニューでは、要件に応じたさまざまなログ レベルを設定できます。指定できるログ レベルは次のとおりです。

- Info
- Debug
- Error
- Trace

ログ レベルを設定すると次のファイルが更新されます。

- VSCサーバ：`kamino.log`および`vvolvp.log`
- VASA Providerサーバ：`vvolvp.log`、`error.log`、および`netapp.log`

また、VASA Provider Webコマンドライン インターフェイス（CLI）ページで、実行されたAPI呼び出し、返されたエラー、パフォーマンス関連のいくつかのカウンタを確認できます。Web CLIページには、`https://<IP_address_or_hostname>:9083/stats`でアクセスできます。

大規模な環境でVSCおよびVASA Providerサービスが再起動する

問題

大規模な環境において、VSC、VASA Provider、SRA仮想アプライアンスのパフォーマンスが最適にならず、VSCおよびVASA Providerサービスが頻繁に再起動するなどの問題が発生することがあります。

対処方法

VSC、VASA Provider、SRA仮想アプライアンスのRAMおよびヒープ メモリの要件を変更します。

ネットアップ ナレッジベースの回答*1079321*:「*How to tune memory settings of virtual appliance for VSC, VASA Provider, and SRA for scale and performance*」

SSHを使用するためのVASA Providerの設定

Virtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスを設定することで、VASA Providerでセキュアなアクセスに SSHを使用するように設定できます。

タスク概要

SSHの設定を行うときは、maintenanceユーザとしてログインする必要があります。VASA Providerへのルート アクセスは無効になっているため、他のログイン クレデンシャルを使用すると、SSHを使用してVASA Providerにアクセスできません。

手順

1. vCenter Serverで、VSC、VASA Provider、SRA仮想アプライアンスへのコンソールを開きます。
2. maintenanceユーザとしてログインします。
3. 「**3**」と入力して**[System Configuration]**を選択します。
4. 「**6**」と入力して**[Enable SSH Access]**を選択します。
5. 確認ダイアログ ボックスで「**y**」と入力します。

リモートdiagアクセスにSSHを使用するためのVSC、VASA Provider、SRA仮想アプライアンスの設定

diagユーザのSSHアクセスを有効にするようにVirtual Storage Console（VSC）、VASA Provider、Storage Replication Adapter（SRA）仮想アプライアンスを設定することができます。

開始する前に

vCenter ServerインスタンスのVASA Provider拡張機能を有効にする必要があります。

タスク概要

SSHを使用してdiagユーザにアクセスする際は次の制限があります。

- SSHを使用した場合、同時に複数のdiagユーザとしてログインできません。
- diagユーザへのSSHアクセスは、次のいずれかの状況になると無効になります。
  - タイムアウトした場合。
    ログインセッションの有効期限は翌日の午前0時までです。
  - SSHを使用してdiagユーザとして再度ログインした場合。

手順

1. vCenter Serverで、VASA Providerへのコンソールを開きます。
2. maintユーザとしてログインします。
3. 「**4** 」と入力して**[Support and Diagnostics]**を選択します。

4. 「**3**」と入力して**[Enable remote diagnostics access]**を選択します。
5. **[Confirmation]**ダイアログ ボックスで「**y**」と入力して、リモート診断アクセスを有効にします。
6. リモート診断アクセス用のパスワードを入力します。

SRAのインストールがスクリプト エラーで失敗する

問題

Windows 2008 R2へのStorage Replication Adapter（SRA）のインストールが、無効なクレデンシャルのエラーで失敗します。

原因

このエラーは、VSC、VASA Provider、SRA仮想アプライアンスとWindows 2008 R2で有効になっているTransport Layer Security（TLS）のバージョンが異なることが原因で発生します。

対処方法

Windows 2008 R2にSRAをインストールする場合は、VSC、VASA Provider、SRA仮想アプライアンス用にTLSv1.0を有効にする必要があります。メンテナンス コンソールで次の手順を実行してください。

1. 「maint」ユーザのクレデンシャルを使用してメンテナンス コンソールにログインします。
2. メイン メニューで、**1**を入力して[Application configuration]メニューを選択します。
3. [Application configuration]メニューで**13**を入力して、[Application Configuration]メニューの[Enable TLS Protocol]を選択します。
4. TLSプロトコルのリストで**[TLSv1]**を選択します。
   VSCサービスおよびVASA Providerサービスが再起動し、TLSv1.0が有効になります。

Windows 2008 R2ではTLSv1.2も有効にできます。

大規模な環境でSRAのパフォーマンスを最適化できない

問題

大規模な環境でSRAのパフォーマンスを最適化できず、タイムアウト エラーやONTAPタイムアウトなどの問題が発生します。

対処方法

タイムアウト間隔を変更する必要があります。

大規模な環境向けの*Storage Replication Adapter*の設定（50ページ）

注：大規模な環境の場合は、VSC、VASA Provider、SRA仮想アプライアンスの規模とパフォーマンスに応じてメモリ設定を変更することもできます。

ネットアップ ナレッジベースの回答*1079321*：「*How to tune memory settings of virtual appliance for VSC, VASA Provider, and SRA for scale and performance*」

SRAプラグインをインストールできない

問題

Storage Replication Adapter（SRA）プラグインのインストール中に、サーバのIPアドレスとパスワードの画面でシステムが停止し、次のエラー メッセージが表示されます。「The credentials you entered are not valid. Please enter a valid hostname and password.」

原因

このエラーは、次のいずれかの原因で発生する可能性があります。

- 入力した管理者のクレデンシャルが正しくない。
- WinHTTPプロキシの設定が正しくない。

対処方法

- 管理者のクレデンシャルを確認します。
- WinHTTPプロキシの設定に関する問題の解決方法の詳細については、ネットアップの技術情報アーティクルを参照してください。
  ネットアップ ナレッジベースの回答*1005074*：「*Installing of SRA 4.0P1 client plugin (netapp_sra_4.0P1_ontap_64bit.msi) hangs at the server IP and password screen*」

著作権に関する情報

商標に関する情報

NetApp、NetAppのロゴ、ネットアップの商標一覧のページ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。

http://www.netapp.com/jp/legal/netapptmlist.aspx

マニュアルの更新について

弊社では、マニュアルの品質を向上していくため、皆様からのフィードバックをお寄せいただく専用のEメール アドレスを用意しています。また、GA/FCS版の製品マニュアルの初回リリース時や既存マニュアルへの重要な変更があった場合にご案内させていただくTwitterアカウントもあります。

本マニュアルの改善についてご提案がある場合は、次のアドレスまでコメントをEメールでお送りください。

ng-gpso-jp-documents@netapp.com

その際、担当部署で適切に対応させていただくため、製品名、バージョン、オペレーティング システム、弊社営業担当者または代理店の情報を必ず入れてください。

GA/FCS版の製品マニュアルの初回リリース時や既存マニュアルへの重要な変更があった場合のご案内を希望される場合は、Twitterアカウント@NetAppDocをフォローしてください。