



導入とアップグレード VSC, VASA Provider, and SRA 9.7

NetApp
March 21, 2024

目次

導入とアップグレード	1
VSC、VASA Provider、SRA仮想アプライアンスの概要	1
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	2
VSC、VASA Provider、SRA仮想アプライアンスを導入するための要件	4
VSC、VASA Provider、SRAを導入またはアップグレードする	9

導入とアップグレード

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環境の仮想マシンに対してエンドツーエンドのライフサイクル管理を提供します。管理者が vCenter Server 内でストレージを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。複数の vCenter Server インスタンスがある環境では、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。

VSC、VASA Provider、SRA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。

- SRAとVASA Providerの両方で使用できるストレージコントローラをVSCに追加し、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
- vCenter Server 環境でデータストアと仮想マシンのパフォーマンスを監視します
- Role-Based Access Control (RBAC ; ロールベースアクセス制御) を使用して、次の 2 つのレベルで vCenter Server オブジェクトへの管理者アクセスを制御します。
 - 仮想マシンやデータストアなどの vSphere オブジェクト

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。

- 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します

NFS Plug-in for VMware vStorage APIs for Array Integration (VAAI) を使用することは、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 VAAI は、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を統合するソフトウェアライブラリです。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ー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。ただし、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、からプラグインの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はVSCと統合されており、VASA Providerを使用して次のタスクを実行できます。

- VMware 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
- 環境に応じた異なる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します
- 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確認する
- 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ようにアラームを設定します
- 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

ONTAP 9.6以前を使用している場合、VASA ProviderはVASA APIを使用してvCenter Serverと通信し、ZAPIと呼ばれるAPIを使用してONTAP と通信します。ONTAP 9.6以前のvVolダッシュボードを表示するためには、vCenter Serverをインストールして登録しておく必要があります。ONTAP 9.7を使用している場合、vVolダッシュボードを表示するためにVASA Providerに登録する必要はありません。



ONTAP 9.6 以前では、VASA Provider に専用の 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 の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 *

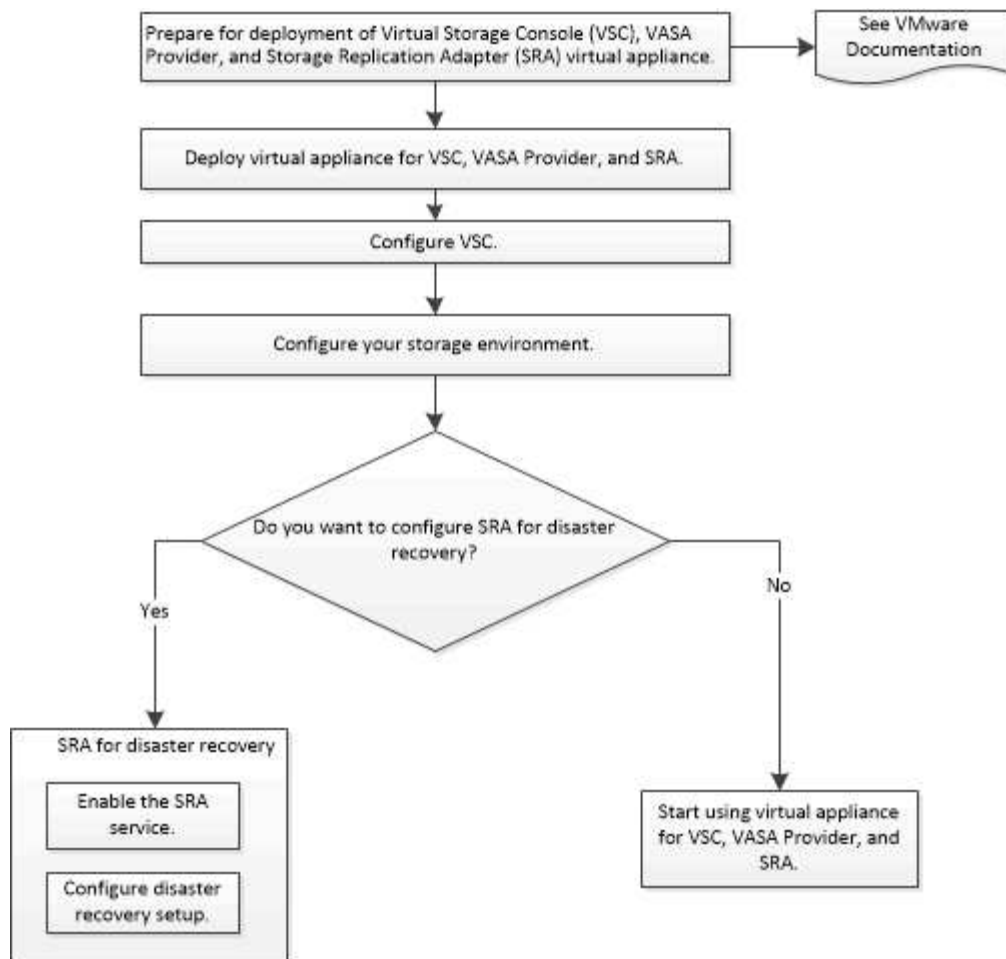
["ネットアップのマニュアル：OnCommand API Services"](#)

["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ー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

VSC、VASA Provider、SRA仮想アプライアンス9.7では、最新バージョンへの直接アップグレードがサポートされます。

VSC、VASA Provider、SRAなど、個々のアプリケーションの以前のリリースでは、使用しているアップグレードプロセスが異なります。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. 最新リリースのVSC、VASA Provider、SRA仮想アプライアンスを導入する
2. 既存の設定データを移行します。

構成データにはストレージ・システムのクレデンシャルのほかに 'kaminoprefs.xml' ファイルおよび vscPreferences.xml ファイルで使用されるプリファレンスも含まれます

"VSC プリファレンスファイルを設定する"

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、以前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て、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行うことを推奨します。次のいずれかを実行できます。

- 使用 ["SnapCenter およびVirtual Storage Console用のインポートユーティリティ"](#) をクリックして、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、ご使用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 4.0P1 を使用している場合は、まず SRA 9.6 にアップグレードする必要があります。その後、SRA 9.6 から最新リリースへのインプレースアップグレードを実行できます。

["VSC、VASA Provider、SRA仮想アプライアンス9.7.1にアップグレードする"](#)

- 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。

ONTAP 用 Storage Replication Adapter 4.0 のインストールおよびセットアップガイドの詳細な手順については、「アップグレードの概要」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。Windows システムのコントロールパネルを使用してソフトウェアをアンインストールし、最新の SRA ソフトウェアを .msi ファイルを使用して 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、既存のセットアップからアップグレードしたあと、「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。仮想メモリの予約も変更する必要があります。メモリサイズを変更するには、仮想マシンの電源をオフにする必要があります。

9.7より前のリリースから9.7P2以降への直接アップグレードは、VSC、VASA Provider、SRA仮想アプライアンスではサポートされていません。最初に既存の環境をVSC、VASA Provider、SRA仮想アプライアンス9.7にアップグレードしてから、新しいリリースにアップグレードする必要があります。

最新リリース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。

- 関連情報 *

["NetApp ToolChest : NetApp Import Utility for SnapCenter and Virtual Storage Console"](#)

["VSC、VASA Provider、SRA仮想アプライアンスを導入するための要件"](#)

["VSC、VASA Provider、SRA仮想アプライアンス9.7.1にアップグレードする"](#)

VSC、VASA Provider、SRA仮想アプライアンスを導入するための要件

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。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

(VSC) は、ストレージシステムとVMware vCenter Serverなど、コンポーネント間の通信に指定のポートをデフォルトで使用します。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。これらのポートへのアクセスを許可しないと、次のようなエラーメッセージが表示されます。

_ サーバと通信できません

VSC で使用されるデフォルトの双方向 TCP 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 年	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 設定を取得するためにも必要です。
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セキュアな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。
7.	エコー要求が ONTAP に送信されて到達可能性が検証されます。この要求はストレージシステムの追加時にのみ必要であり、あとで無効にすることができます。

VSC、VASA Provider、SRA仮想アプライアンスを導入する前に、Internet Control Message Protocol (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。

VSC、VASA Provider、SRA仮想アプライアンスのスペースとサイズの要件

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基本的な要件を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は 2.1GB
 - シックプロビジョニングの場合は 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、およびアプリケーション

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、(IMT) を参照してください。

- ["Interoperability Matrix Tool : VSC 9.7.1"](#)
- ["Interoperability Matrix Tool : VASA Provider 9.7.1"](#)
- ["Interoperability Matrix Tool : SRA 9.7.1"](#)

VMware Virtual Volumes (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ためには、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：「Storage I/O Control Requirements」"](#)

VSC、VASA Provider、SRA仮想アプライアンスを導入する際の考慮事項と要件

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、VSC、VASA Provider、およびSRAを環境に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、その概要を示します。

考慮事項	説明
VSC、VASA Provider、SRA仮想アプライアンスの初回導入	<p>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を導入またはアップグレードする"</p> <p>"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"</p>
VSC の既存の導入環境からアップグレードする	<p>VSCの既存の導入環境からVSC、VASA Provider、SRA仮想アプライアンスへのアップグレード手順は、VSCのバージョン、およびVSC、VASA Provider、SRAの導入状況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"</p> <p>アップグレード前に実施しておくべき作業：</p> <ul style="list-style-type: none">• 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。 <p>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。</p> <ul style="list-style-type: none">• 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。 <p>標準のロールは、VSC サービスを再起動するたびに現在のデフォルトで上書きされます。</p>
VSC の SSL 証明書の再生成	<p>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的に生成されます。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になることがあります。"のSSL証明書を再生成します"</p>

考慮事項	説明
ESXi サーバの値を設定しています	<p>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。これらの値は、内部テストに基づいています。環境によっては、パフォーマンスを向上させるために値を変更しなければならない場合があります。</p> <ul style="list-style-type: none"> • "ESXi サーバのマルチパスとタイムアウトを設定" • "Virtual Storage Console for VMware vSphereを使用して設定されるESXiホストの値"
ゲストオペレーティングシステムのタイムアウト値	<p>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 の各ゲストオペレーティングシステムの SCSI I/O タイムアウト値を設定します。</p>

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、その概要を示します。

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	<p>VSC は、vCenter Server RBAC と ONTAP RBAC の両方をサポートしています。VSCをvCenter Serverに登録するために使用するアカウント（`https://<apply_ip>:8143/Register_html`）を使用）は、vCenter Server管理者（vCenter Serverの管理者ロールまたは管理者ロールに割り当てられている）である必要があります。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アクセス許可と権限がすべて付与されている必要があります。</p> <p>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 ロールを作成してユーザに割り当てることができます。</p> <p>ONTAP System Managerで、VSC、VASA Provider、SRA仮想アプライアンスに付属のJSONファイルを使用して、推奨されるONTAP ロールを作成できます。</p> <p>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。</p> <ul style="list-style-type: none"> • "VSC、VASA Provider、SRA仮想アプライアンスに組み込みの標準ロール" • "VSC for VMware vSphere使用時に推奨されるONTAP ロール"
ONTAP バージョン	ストレージシステムでONTAP 9.1、9.3、9.5、9.6、または9.7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	<p>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、VMware Virtual Volumes（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。</p> <p>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。</p>

VSC、VASA Provider、SRAを導入またはアップグレードする

VSC、VASA Provider、SRA仮想アプライアンスをダウンロードしてVMware vSphere環

境に導入し、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。

- 関連情報 *

[仮想データストアを設定するための VASA Provider の有効化](#)

VSC、VASA Provider、SRA仮想アプライアンスのダウンロード方法

Virtual Storage Console、VASA Provider、Storage Replication Adapter仮想アプライアンスの「.ova」ファイルは、[こちら](#)からダウンロードできます。

「.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、[こちら](#)からダウンロードできます ["ネットアップサポートサイト"](#) ソフトウェアのダウンロードページを使用します。

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プラグインのインストールファイルは、「ソフトウェアのダウンロード」セクションの「ONTAP *用Storage Replication Adapter」メニューからダウンロードできます。

VSC、VASA Provider、SRA仮想アプライアンスを導入する

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、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。

作業を開始する前に

- サポートされているリリースの vCenter Server が実行されている必要があります。



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

["Interoperability Matrix Tool : VSC 9.7"](#)

- vCenter Server 環境を設定およびセットアップしておく必要があります。
- 仮想マシン用の 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。
- 「.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問題 がブラウザキャッシュに表示されないようにするには、ブラウザ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ます](#)

- Internet Control Message Protocol（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。

このタスクについて

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がデフォルトで有効になります。ただし、以前のリリース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場合があります。

"仮想データストアを設定するための VASA Provider の有効化"

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]メニューを選択します。
3. 必要なデータセンターを右クリックし、* OVA テンプレートの導入 * をクリックします。
4. 該当する方法を選択してVSC、VASA Provider、SRAの導入ファイルを指定し、* Next *をクリックします。

場所	アクション
URL	VSC、VASA Provider、SRA仮想アプライアンスの「.ova」ファイルのURLを指定します。
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. 詳細を入力して、導入ウィザードをカスタマイズします。

を参照してください ["導入のカスタマイズに関する考慮事項"](#) を参照してください。

6. 構成データを確認し、[次へ*]をクリックして導入を終了します。

展開が完了するまで待つ間に、[タスク]タブから展開の進行状況を表示できます。

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. 導入の完了後に、VSC、VASA Provider、SRAの各サービスが実行されていることを確認
9. VSC、VASA Provider、SRA仮想アプライアンスがいずれのvCenter Serverにも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。
10. 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。

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。



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ます

完了後

[NOTE]

====

ONTAP 9.6以前を使用している場合、vVolダッシュボードを表示するには、をダウンロードしてインストールする必要があります。ただし、ONTAP 9.7の場合は、VASA Providerに登録する必要はありません。

====

xref:{relative_path}task-register-oncommand-api-services-with-the-virtual-appliance-for-vsc-vasa-provider-and-sra.adoc[VSC、VASA Provider、SRA仮想アプライアンスに登録する]

:leveloffset: +1

[[ID09c4e4120e0ba9b4a24e6581c4a86bc6]]

= 導入のカスタマイズに関する考慮事項

:allow-uri-read:

:icons: font

:relative_path: ./deploy/

:imagesdir: {root_path}{relative_path}../media/

[role="lead"]

VSC、VASA Provider、

SRA仮想アプライアンスの導入をカスタマイズするときは、いくつかの制限事項について考慮する必要があります。

== アプライアンスの管理者ユーザのパスワード

管理者パスワードにはスペースは使用できません。

== アプライアンスのメンテナンスコンソールのクレデンシャル

メンテナンスコンソールにアクセスするには、「maint」ユーザ名を使用する必要があります。導入時に「maint

」ユーザのパスワードを設定できます。パスワードは、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*アプリケーションの設定*メニューを使用して変更できます。

== vCenter Server 管理者のクレデンシャル

vCenter Serverの管理者クレデンシャルは、VSC、VASA Provider、SRA仮想アプライアンスを導入するときに設定できます。

vCenter Serverのパスワードが変更された場合は、次のURLを使用して管理者のパスワードを更新できます。`_https_://<IP>:8143/Register.html'。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。

== vCenter Server の IP アドレス

* VSC、VASA Provider、SRA仮想アプライアンスの登録先となるvCenter ServerインスタンスのIPアドレス（IPv4またはIPv6）を指定する必要があります。

+

生成される VSC 証明書と VASA 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の詳細とDHCPを入力していない場合は、IPv4アドレスとIPv6アドレスの両方がネットワークから提供されます。

* 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、導入ウィザードで入力したvCenter Server 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一タイプの 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。

[NOTE]

=====

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

=====

== アプライアンスのネットワーク・プロパティ

DHCPを使用していない場合は、有効なDNSホスト名（非修飾）と、VSC、VASA Provider、

SRA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。これらのパラメータはすべて、適切なインストールと運用のために必要です。

```
:leveloffset: -1
```

```
[[ID0e01f0e384b876e3880a40022cc2c7ce]]
```

= 仮想データストアを設定するための VASA Provider の有効化

```
:allow-uri-read:
```

```
:experimental:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

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。VMware 仮想ボリューム (vVol)

データストアは、それぞれの 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設定できます。

. 作業を開始する前に

* 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。

. このタスクについて

Virtual Storage Console (VSC)、VASA Provider、Storage Replication Adapter (SRA) 仮想アプライアンス9.7.1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。本リリースでは、VVOL データストアに対する vVol のレプリケーション機能を有効にすることができます。

. 手順

. VMware vSphere の Web ユーザインターフェイスにログインします。

. vSphere Clientで、メニューをクリックします。メニュー[Virtual Storage Console]。

. [* 設定 *] をクリックします。

. [管理設定 *] タブの [機能の管理 *] をクリックします。

. 管理機能*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。

. VVOL データストアのレプリケーション機能を使用する場合は、「* vVol

レプリケーションを有効にする *」切り替えボタンを使用します。

. 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、* Apply *をクリックします。

.完了後

ONTAP 9.6以前のクラスタを使用している場合は、SAN vVol VMおよびSAN vVolデータストアのレポートで使用されるvVolデータストアと仮想マシンの詳細を取得するために VASA Providerに登録する必要があります。ただし、ONTAP 9.7以降を使用している場合は、VASA Providerに登録する必要はありません。

```
:leveloffset: +1
```

```
[[ID6f4f8ab7d6183d6a7e3400a6dc96e642]]  
= VSC、VASA Provider、SRA仮想アプライアンスに登録する  
:allow-uri-read:  
:icons: font  
:relative_path: ./deploy/  
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

ONTAP 9.6以前を使用している場合、VMware仮想ボリューム（vVol）データストアと仮想マシンの詳細をvVolダッシュボードに表示するためには、VASA Providerに登録して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必要があります。

.作業を開始する前に

から2.1以降をダウンロードしておく必要があります。

```
[NOTE]
```

```
====
```

vVolダッシュボードには、ONTAP 9.3以降を使用してSAN 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

- . Virtual Storage Console (VSC) * Home *ページで、* Settings *をクリックします。
- . [管理設定*] タブの [拡張機能の管理*] をクリックします。
- . [API OnCommand サービスの登録*] スライダを使用して有効にします。
- . 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拡張機能の管理

*ダイアログボックスを使用して、次の変更を行うこともできます。

+

- ** クレデンシャルに変更があったときに登録を更新する。
- ** vVolダッシュボードが不要になったときに登録を解除する。

+

VASA Providerの登録を解除するには、「OnCommand APIサービスの登録

*」チェックボックスをオフにする必要があります。

・ [適用 (Apply)] をクリックします。

+

vVolダッシュボードには、の登録が完了した時点で初めて、ONTAP 9.6以前のSAN

vVolデータストアの指標が表示されます。

* 関連情報 *

[https://mysupport.netapp.com/site/\["ネットアップサポート"^\]](https://mysupport.netapp.com/site/[)

:leveloffset: -1

[[ID5fb74e40f0a7fcb3a0d9cf2c59cb06b6]]

= NFS VAAI プラグインをインストールします

:allow-uri-read:

:icons: font

:relative_path: ./deploy/

:imagesdir: {root_path}{relative_path}../media/

[role="lead"]

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、NFS Plug-in for VMware vStorage APIs for Array Integration (VAAI) をインストールできます。

・作業を開始する前に

* NFS Plug-in for VAAI

(`.vib')のインストールパッケージをからダウンロードしておく必要があります。

+

[https://mysupport.netapp.com/site/\["ネットアップサポート"^\]](https://mysupport.netapp.com/site/[)

* 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、* Recommended Settings *ダイアログボックスが更新されると、ESXiホストで自動的に設定されます。

* vservice nfs modify -vservice vservice_name -vStorage enabled` コマンドを使用して、でvstorageオプションを有効にしておく必要があります。

.手順

- . からダウンロードした「.vib`」ファイルの名前を、VSCで使われる事前定義された名前に変更してください。
- . VSCのホームページで「* Settings」をクリックします。
- . NFS VAAI ツール * タブをクリックします。
- . [既存のバージョン * (Existing version *)] セクションで [* 変更 * (Change *)] をクリックする
- . 名前を変更した「.vib`」ファイルを参照して選択し、「*アップロード」をクリックして仮想アプライアンスにファイルをアップロードします。
- . ESXiホストにインストールする*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。インストールの進行状況は、 vSphere Web Client のタスクセクションで監視できます。

- . 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 プラグインが VSC で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。

```
[[ID978b212e35fcd0b8d0a84585d1861532]]
= Storage Replication Adapter を有効にする
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Virtual Storage Console (VSC) 、VASA Provider、Storage Replication Adapter (SRA) 仮想アプライアンスには、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オプションがあります。

.作業を開始する前に

- * 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。
- * Site Recovery Manager (SRM) ディザスタリカバリ解決策を設定する場合のみ、SRA プラグインの .msi ファイル、または SRM アプライアンスの .tar.gz ファイルをダウンロードしておく必要があります。

+

https://docs.vmware.com/en/Site-Recovery-Manager/8.2/com.vmware.srm.install_config.doc/GUID-B3A49FFF-E3B9-45E3-AD35-093D896596A0.html["Site Recovery Manager Installation and Configuration Site Recovery Manager 8.2"] を参照してください^^
に詳細を示します。

. このタスクについて

VASA Provider と SRA

の機能を柔軟に有効化できるため、必要なワークフローだけを実行できます。

. 手順

- . VMware vSphere の Web ユーザインターフェイスにログインします。
- . vSphere Clientで、メニューをクリックします。メニュー[Virtual Storage Console]。
- . [* 設定 *] をクリックします。
- . [管理設定 *] タブの [機能の管理 *] をクリックします。
- . Manage Capabilities * 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。
- . 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、* Apply *をクリックします。
- . SRA を導入するには、次のいずれかの方法を使用します。

+

[cols="1a,1a"]

|===

| オプション | 説明

a|

Windows SRMの場合

a|

- .. 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ます。
- .. 画面に表示される指示に従います。
- .. 導入した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。

a|

SRMアプライアンスの場合

a|

- .. SRMアプライアンスのページにアクセスし、SRMアプライアンスの* Storage Replication

Adapters *ページに移動します。

.. [新しいアダプタ] をクリックします。

.. SRAプラグインの.tar.gzインストーラをSRMにアップロードします。

.. アダプタを再スキャンして、SRM * Storage Replication Adapters

*ページで詳細が更新されていることを確認します。

|===

+

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 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。

* 関連情報 *

xref:{relative_path}concept-configure-storage-replication-adapter-for-disaster-recovery.adoc[ディザスタリカバリ用の Storage Replication Adapter を設定する]

:leveloffset: +1

[[IDabe4b546c8684c4c13c36394b5305278]]

= SRM アプライアンスで SRA を設定する

:allow-uri-read:

:icons: font

:relative_path: ./deploy/

:imagesdir: {root_path}{relative_path}../media/

[role="lead"]

SRM アプライアンスを導入したら、 SRM アプライアンスに SRA を設定する必要があります。SRA を正しく設定すると、ディザスタリカバリ管理のために SRM アプライアンスが SRA と通信できるようになります。SRMアプライアンスと SRAの間の通信を有効にするためには、VSC、VASA Provider、SRA仮想アプライアンスのクレデンシャル（IPアドレスと管理者パスワード）をSRMアプライアンスに保存する必要があります。

.作業を開始する前に

tar .gzファイルをSRMアプライアンスにアップロードする必要があります。

.このタスクについて

SRM アプライアンスで SRA を設定すると、 SRA クレデンシャルが SRM アプライアンスに保存されます。

.手順

- . putty を使用して、管理者アカウントで SRM アプライアンスにログインします。
 - . root ユーザに切り替えます。 root ユーザには「 root 」コマンドを使用します
 - . ログの場所で、次のコマンドを入力して、SRAの「Docker PS-1」で使用されるDocker IDを取得します
 - . コンテナIDにログインするには、コマンド「docker exec-it-u SRM <container id>sh`」を入力します
 - . 次のコマンドを使用して、SRMにVSC、VASA Provider、SRA仮想アプライアンスの IPアドレスとパスワードを設定します。「perl command.pl -i <va-IP> administrator <va-password>」
- +
- ストレージクレデンシャルが保存されたことを示す成功メッセージが表示されます。SRAは、指定された IP アドレス、ポート、およびクレデンシャルを使用して SRAサーバと通信できます。

```
[[ID11f7e3b6b93c299cb4757688523eb809]]
= Storage Replication Adapter (SRA) クレデンシャルを更新する
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

SRM が SRA と通信するためには、 SRA クレデンシャルを変更した場合に SRMサーバ上のクレデンシャルを更新する必要があります。

.作業を開始する前に

「 SRM アプライアンスでの SRA の設定」に記載されている手順を実行しておく必要があります。

```
xref:{relative_path}task-configure-sra-on-srm-appliance.adoc[SRM
アプライアンスで SRA を設定する]
```

.手順

- . 次のコマンドを使用して「/SRM/SRA/conf」ディレクトリの内容を削除します
- +
- ```
.. cd /SRM / SRA /conf
.. RM-RF *
```
- +
- . perl コマンドを実行して、 SRA に新しいクレデンシャルを設定します。
- +

```
.. cd /SRM / SRA /
.. Perl command.pl -i <va-IP>管理者<va-password>
```

```
:leveloffset: -1
```

```
[[IDad214f7890e0befda469a5406dc6f10e]]
= Windows SRM から SRM アプライアンスへの移行
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]  
ディザスタリカバリーに Windows ベースの Site Recovery Manager (SRM) を使用している場合、同じセットアップで SRM アプライアンスを使用するには、Windows のディザスタリカバリーセットアップをアプライアンスベースの SRM に移行する必要があります。

ディザスタリカバリーの移行に必要な手順は次のとおりです。

. VSC、VASA Provider、SRA仮想アプライアンスの9.7.1リリースへのアップグレード  
+  
xref:{relative\_path}task-upgrade-to-the-9-7-1-virtual-appliance-for-vsc-vasa-provider-and-sra.html["VSC、VASA Provider、SRA仮想アプライアンス 9.7.1にアップグレードする"^]

. Windows ベースの Storage Replication Adapter をアプライアンスベースの SRA に移行します。

. Windows SRM のデータを SRM アプライアンスに移行します。

[https://docs.vmware.com/en/Site-Recovery-Manager/8.2/com.vmware.srm.install\\_config.doc/GUID-F39A84D3-2E3D-4018-97DD-5D7F7E041B43.html](https://docs.vmware.com/en/Site-Recovery-Manager/8.2/com.vmware.srm.install_config.doc/GUID-F39A84D3-2E3D-4018-97DD-5D7F7E041B43.html)["ここをクリックしてください"^] を参照してください。

```
[[ID249de6acfd87d74b3704b517f21a4045]]
= VSC、VASA Provider、SRA仮想アプライアンス9.7.1にアップグレードする
:allow-uri-read:
:experimental:
```

```
:icons: font
:relative_path: ../deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

ここに記載されている手順に従って、VSC、VASA Provider、SRA仮想アプライアンス 9.7.1への直接アップグレードを既存の9.7から実行できます。

#### .作業を開始する前に

- \* VSC、VASA Provider、SRA仮想アプライアンス9.7.1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クリーンアップする必要があります。

+

xref:{relative\_path}task-clean-the-vsphere-cached-downloaded-plugin-packages.adoc[vSphere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ます]

#### .このタスクについて

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。アップグレード後に要件に基づいて VASA Provider を手動で有効または無効にする必要があります。ただし、従来のデータストアのプロビジョニングやストレージアラームのストレージ機能プロファイルが有効になるため、 VASA Provider は VMware 仮想ボリューム（ vVol ）を使用していない場合でも有効にすることを推奨します。

[NOTE]

====

9.7より前のリリースから9.7P2以降への直接アップグレードは、VSC、VASA Provider、SRA仮想アプライアンスではサポートされていません。最初に既存の環境をVSC、VASA Provider、SRA仮想アプライアンス9.7にアップグレードしてから、新しいリリースにアップグレードする必要があります。VSC、VASA Provider、SRA仮想アプライアンス 9.7.1にアップグレードし、VVOLレプリケーションを使用する場合は、Site Recovery Manager（SRM）がインストールされた仮想アプライアンスでvCenter Serverをもう1つセットアップする必要があります。

====

#### .手順

- . 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。

+

- .. メニュー：設定の編集[DVD/CD-ROMドライブ]をクリックします。

- .. ドロップダウンリストから \* Datastore ISO \* file を選択します。



.. ダウンロードした「.iso」ファイルを参照して選択し、「パワーオン時に  
\*接続」チェックボックスを選択します。

. 導入した仮想アプライアンスの\* Summary \*タブにアクセスします。

. \* をクリックしますimage:../media/launch-maintenance-console.gif[""]\*  
メンテナンスコンソールを起動します。

. 「ドメインメニュー」プロンプトで、「システム構成」に「 2  
」オプションを入力し、「アップグレード」に「 8 」オプションを入力します。

+

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アドレスを使用してvCenter  
Serverに登録されます。

. VSC、VASA Provider、SRA仮想アプライアンスをIPv6アドレスでvCenter  
Serverに登録するには、次の手順を実行する必要があります。

+

.. VSC、VASA Provider、SRA仮想アプライアンスの登録を解除する

.. 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。

.. 登録後、 VSC と VASA Provider の証明書を再生成します。

+

[NOTE]

====

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

====

. vSphere Clientからログアウトして再度ログインすると、VSC、VASA Provider、  
SRA仮想アプライアンスが導入されていることが表示されます。

+

.. 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。

.. 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。

\* 関連情報 \*

xref:{relative\_path}task-enable-vasa-provider-for-configuring-virtual-  
datastores.adoc[仮想データストアを設定するための VASA Provider の有効化]

```
[[ID7840c6952c35d400031646120095cc37]]
= Storage Replication Adapter をアップグレードする
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

VSC、VASA Provider、  
SRA仮想アプライアンスをアップグレードするか最新バージョンの仮想アプライアンスを導入したら  
、Storage Replication Adapter (SRA) をアップグレードする必要があります。

## .手順

アダプタに応じて、次のいずれかの手順で最新のアダプタにアップグレードする必要があります。

```
+
[cols="1a,1a"]
|===
| * は ...* のため | 実行する手順
```

```
a|
* Windows *
a|
.. SRM Windows Server にログインします。
.. 既存の SRA *.msi インストーラを SRM サーバからアンインストールします。
.. システム・パスを C:\Program Files\VMware\VMware vCenter Site Recovery
Manager\external\perl\c\bin' に変更します
.. ネットアップサポートサイトからダウンロードした *.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。
.. 導入したVSC、VASA Provider、SRA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。
```

```
a|
アプライアンスベースのアダプタ
a|
.. SRMアプライアンス管理ページにログインします。
.. Storage Replication Adapter * をクリックし、 * Delete * をクリックして既存の
SRA を削除します。
.. [メニュー]、[新しいアダプタ]、[参照]の順にクリックします。
```

.. ネットアップサポートサイトからダウンロードした最新の SRA tar  
ファイルをクリックして選択し、 \* Install \* をクリックします。

.. SRM アプライアンスで SRA を設定する

+

xref:{relative\_path}task-configure-sra-on-srm-appliance.adoc[SRM  
アプライアンスで SRA を設定する]

|===

:leveloffset: -1

[[ID3dfb22f08313e727c4ecb63109bdb7ba]]

= Virtual Storage Console for VMware vSphere環境を設定します

:allow-uri-read:

:icons: font

:relative\_path: ./deploy/

:imagesdir: {root\_path}{relative\_path}../media/

[role="lead"]

(VSC) はさまざまな環境をサポートしています。これらの環境の機能によっては、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。

- \* UNMAP 設定を含む ESXi ホストの設定の確認
- \* ゲストオペレーティングシステムのタイムアウト値の追加
- \* VSC の SSL 証明書を再生成します
- \* 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にするためのプリファレンスファイルの変更

:leveloffset: +1

```
[[IDd9bb9c1fdfef4133cb5e6964e5a96193]]
= ESXi サーバのマルチパスとタイムアウトを設定
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Virtual Storage Console for VMware vSphereは、ESXiホストのマルチパス設定とHBAタイムアウト設定をチェックし、ストレージシステムに最も適した設定を行います。

### . このタスクについて

構成やシステムの負荷によっては、この処理に長時間かかることがあります。タスクの進行状況が\*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アラートアイコンが Normal アイコンまたは Pending Reboot アイコンに変わります。

### . 手順

. VMware vSphere Web Client \* Home \* ページで、メニュー：vCenter [Hosts] をクリックします。

. ホストを右クリックして、メニューを選択します。アクションNetApp VSC >推奨値の設定

. NetApp Recommended Settings

\*ダイアログボックスで、ご使用のシステムに最も適した値を選択します。

+

標準の推奨値がデフォルトで設定されます。

+

image:.../media/vsc-recommended-hosts-settings.gif[VSC で推奨されるホスト設定]

. [OK] をクリックします。

```
:leveloffset: +1
```

```
[[IDd15cbf8736c77a6a281a3ea193a696ec]]
```

= Virtual Storage Console for VMware vSphereを使用して設定されるESXiホストの値

```
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

フェイルオーバーが最適な状態で確実に実行されるように、Virtual Storage Console for

VMware vSphereを使用して  
ESXiホストにタイムアウト値やその他の値を設定することができます。Virtual Storage  
Console (VSC) で設定される値は、内部テストに基づいています。

ESXi ホストでは、次の値を設定できます。

#### == 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.TcpipHeHeapSize *
```

+

vSphere 6.0 以降を使用している場合は、この値を 32 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。

```
* * NFS.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。

```
* * 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 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「固定」に設定する必要があります。

+

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ロード・バランシングを行うことができます。値「fixed」は、ALUA に対応していない古い構成に使用され、プロキシ I/O の防止に役立ちます

\* \* 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 パスに対してこの値を「 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ロード・バランシングを行うことができます。

\* \* 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。

```
[[ID0452ab6e69cd154869d6362bd1441729]]
```

= ゲストオペレーティングシステムスクリプトを設定する

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

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サーバにマウントされます。ゲスト OS

スクリプトを使用して仮想マシンのストレージタイムアウトを設定するには、 vSphere Client

からスクリプトをマウントする必要があります。

```
[cols="1a,1a,1a"]
```

```
|===
```

```
| 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
```

```
a|
```

Linux の場合

```
a|
```

```
`_https_://<apply_ip>:8143/VSC/public/writed/linux_gos_timeout-install.iso
```

```
a|
```

```
`_https_://<apply_ip>: 8143/VSC/public/writable /linux_gos_timeout_190
-install.iso
```

```
a|
```

Windows の場合

```
a|
```

```
`_https_://<apply_ip>: 8143/VSC/public/writed/windows_gos_timeout.iso
```

```
a|
```

```
`_https_://<apply_ip>:8143/VSC/public/writable
/windows_gos_timeout_190.isoの形式で指定します
```

```
a|
```

Solaris の場合

```
a|
```

```
`_https_://<apply_ip>:8143/VSC/public/writable /solaris_Gos_timeout-
install.iso
```

```
a|
```

```
`_https_://<apply_ip>: 8143/VSC/public/writable /solaris_Gos_timeout_190
-install.iso
```

```
|===
```

仮想マシンを管理している 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。

```
:leveloffset: +1
```



```
[[ID3f119ec5527d75e33783848b11d580ff]]
= Windows ゲストオペレーティングシステムのタイムアウト値を設定します
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]  
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。タイムアウトは 60 秒または 190  
秒のどちらかを指定できます。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。

#### .作業を開始する前に

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

. 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。

. 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ダイアログが表示されます。

. 続行するには、[ はい ] をクリックします。

+

「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

. Windows ゲスト OS をリブートします。

. ISO イメージをアンマウントします。

```
[[ID7d9b21859b4c63d7e1cfe923263643c6]]
= Solaris ゲストオペレーティングシステムのタイムアウト値を設定します
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

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。タイムアウトは 60 秒または 190 秒のどちらかを指定できます。

.作業を開始する前に

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

. 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。

. 「 'olaris \_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。

+

```
[listing]
```

```

```

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

```

```

. ISO イメージをアンマウントします。

```
[[ID4dd16bf234e41bf4b475d012cff8cb19]]
```

= Linux ゲストオペレーティングシステムのタイムアウト値を設定します

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

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。タイムアウトは 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。

.作業を開始する前に

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

. 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。

. 「 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。

+

[listing]

----

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

----

+

[listing]

----

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。

+

[listing]

----

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

----

+

[listing]

----

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

----

+

[listing]

----

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

----

+

[listing]

----

Starting udev: [ OK ]

----

+

[listing]

----

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。

```
+
[listing]

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

+
[listing]

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

+
[listing]

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

+
[listing]

Updating all available device nodes in /dev: done

. ISO イメージをアンマウントします。
```

```
:leveloffset: -1
```

```
:leveloffset: -1
```

```
[[IDbc6bc1e5de2105940bb77bf4f65faf15]]
= Virtual Storage Console の SSL 証明書を再生成する
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

(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 証明書に対して生成される Distinguished Name ( DN ; 識別名) は、クライアントマシンで認識される Common Name ( CN ; 共通名) 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。

. このタスクについて  
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。

[https://kb.netapp.com/app/answers/answer\\_view/a\\_id/1075654](https://kb.netapp.com/app/answers/answer_view/a_id/1075654)["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

- . メンテナンスコンソールにログインします。
- . 「アプリケーション構成」メニューにアクセスするには、「1」を入力します。
- . [Application Configuration]メニューで「3」と入力して、VSCサービスを停止します。
- . SSL 証明書を再生成するには「7」と入力します

```
[[IDff239b60a95d82cb105a65bddd82ecce]]
= 複数の vCenter Server 環境で VSC を登録するための要件
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

単一のVMware vSphere HTML5クライアントで複数の vCenter Server インスタンスを管理している環境で VSC と vCenter Server を 1 : 1 のペアにするため、各 vCenter Server に VSC のインスタンスを 1 つ登録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 HTML5 クライアント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。

[NOTE]

====

VSC を vCenter Server で使用する場合は、管理する vCenter Server インスタンスごとに VSC インスタンスを 1 つ設定または登録しておく必要があります。登録する各 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 HTML5 クライアントを使用して複数の vCenter Server で VSC

タスクを実行するためには、次の条件を満たす必要があります。

- \* VMware インベントリ内の管理対象の各 vCenter Server に 1 つずつ 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

+

VMware インベントリに VSC サーバが登録されていない vCenter Server が含まれていて、VSC に登録されている vCenter Server が 1 つ以上ある場合は、その後、VSC が登録された vCenter Server に対する VSC のインスタンスを表示して VSC 処理を実行できます。

- \* シングルサインオン（SSO）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 の指定が必要なタスクを実行すると、「\* vCenter Server \*」ドロップダウンボックスに、使用可能な vCenter Server が英数字順に表示されます。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、\* Provisioning \*ウィザードを使用し、データストアが特定のvCenter Serverで管理されているホスト上にある場合）、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。

。

```
[[ID69d2737241b4b79ab0e5733af94ddd52]]
= VSC プリファレンスファイルを設定する
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

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含まれています。ほとんどの場合、これらのファイルの設定を変更する必要はありません。どのプリファレンスファイル（vsc）が使用されるかを理解しておく役立ちます。

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 が含まれています

「 /opt/NetApp/vscserver /etc/vsc/vscPreferences.xml 」を参照してください

状況によっては、プリファレンスファイルの変更が必要になることがあります。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、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。

```
:leveloffset: +1
```

```
[[IDd41c0b6c953e0e32664a74bed26c6eae]]
= IPv4またはIPv6を設定します
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

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。このオプションを設定すると、vscに追加されるすべてのストレージシステムでIPv4またはIPv6のサポートを有効にすることができます。

\* 「 default.override.option.provision.mount.datastore.address.family`

」パラメータが「 kaminoprefs.xml

」プリファレンスファイルに追加され、データストアプロビジョニング用の優先データ LIF プロトコルが設定されました。

+

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、値は「 NONE 」に設定されています。

```
[cols="1a,1a"]
```

```
|===
```

```
| 価値 | 説明
```

```
 a|
```

なし

```
 a|
```

\* プロビジョニングの際、クラスタのタイプまたは管理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。

\* データLIFのIPv6またはIPv4

アドレスタイプがで使用されていない場合は、他のタイプのデータLIFがある場合はそのデータLIFを使用してプロビジョニングが行われます。

```
 a|
```

IPv4

```
 a|
```

\* 選択したの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。

\* にIPv4データLIFがない場合、で使用可能なIPv6データLIFがあれば、そのデータLIFを使用してプロビジョニングが行われます。

```
 a|
```

IPv6

```
 a|
```

\* 選択したの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。

\* にIPv6データLIFがない場合、で使用可能なIPv4のデータLIFがあれば、プロビジョニングはIPv4のデータLIFを介して行われます。

```
|===
```



```
:leveloffset: -1
```

```
[[ID1437ae3eac4505c1ef4f65163317718c]]
```

= 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にする

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

NFSまたはiSCSI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、(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。

. このタスクについて

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。

' 続行できません。コントローラ上のカーネルIPアドレスとアドレスの相互参照時にIPアドレスが見つかりませんでした

これらのホストにNFSマウント・ボリュームと一致するネットワークが見つかりません、

. 手順

. vCenter Server インスタンスにログインします。

. 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。

+

xref:{relative\_path}task-access-virtual-appliance-maintenance-console-options.html["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にアクセスする"]

. \*Support and Diagnostics\*オプションにアクセスするには'4`を入力します

. 「2」を入力して、「\* Access Diagnostic Shell \*」オプションにアクセスします。

. 「 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。

. kaminoprefs.xml ファイルを更新します

+

```
[cols="1a,1a"]
```

```
|===
```

| を使用する場合 | 手順

```
a|
iSCSI
a|
エントリキー「efault.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。
```

```
a|
NFS
a|
エントリキー「efault.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のサンプル値が含まれています。
```

```
+
[NOTE]
```

```
=====
値「all」はすべてのネットワークを意味するわけではありません。「
all」の値を指定すると、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
が、データストアのマウントに使用されます。ホストネットワークを指定すると、指定したサブネ
ット間でのみマウントを有効にできます。
```

```
=====
. 'kaminoprefs.xml ファイルを保存して閉じます
```

```
[[ID970266415cc664a8eb6b5a9a706ad536]]
= 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にアクセスする
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
アプリケーション、システム、およびネットワークの構成は、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することができます。サポートバンドルの生成、異なるログレベル
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行うこともできます。
```

## .作業を開始する前に

VSC、VASA Provider、SRA仮想アプライアンスの導入後に  
VMwareツールをインストールする必要があります。

## .このタスクについて

- \* ユーザ名に「maint」を使用し、導入時に設定したパスワードを使用して、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。
- \* リモート診断をイネーブルにするときは、「 ``ip` 」ユーザのパスワードを設定する必要があります。

## .手順

- . 導入した仮想アプライアンスの\* Summary \*タブにアクセスします。
- . をクリックします image:../media/launch-maintenance-console.gif[""]  
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。

+

\*\* \*アプリケーション構成\*

+

次のオプションを使用できます。

+

- \*\*\* サーバステータスの概要を表示します
- \*\*\* Virtual Storage Console サービスを開始します
- \*\*\* Virtual Storage Console サービスを停止します
- \*\*\* VASA Provider および SRA サービスを開始する
- \*\*\* VASA Provider および SRA サービスを停止する
- \*\*\* 「管理者」ユーザのパスワードを変更します
- \*\*\* 証明書を再生成します
- \*\*\* キーストアと証明書をハードリセットします
- \*\*\* データベースをハードリセットしました
- \*\*\* Virtual Storage Console サービスのログレベルを変更します
- \*\*\* VASA Provider サービスと SRA サービスのログレベルを変更します
- \*\*\* TLS 設定を表示する
- \*\*\* TLS プロトコルを有効にします
- \*\*\* TLS プロトコルを無効にします

\*\* \*システム構成\*

+

次のオプションを使用できます。

+

\*\*\* 仮想マシンをリブートします

\*\*\* 仮想マシンをシャットダウンします  
\*\*\* 「 maint 」 ユーザのパスワードを変更します  
\*\*\* タイムゾーンを変更します  
\*\*\* NTPサーバを変更します

+

NTP サーバの IPv6 アドレスを指定できます。

\*\*\* SSHアクセスを有効/無効にします  
\*\*\* jail ディスクサイズ ( /jail ) の拡張  
\*\*\* アップグレード  
\*\*\* VMware Tools をインストールします

\*\* \*ネットワーク構成\*

+

次のオプションを使用できます。

+

\*\*\* IP アドレス設定を表示します  
\*\*\* IP アドレスの設定を変更します

+

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を表示します  
\*\*\* ドメイン名検索設定を変更します  
\*\*\* 静的ルートを表示します  
\*\*\* 静的ルートを変更します

+

このオプションを使用すると、IPv6 ルートを追加できます。

\*\*\* 変更をコミットします  
\*\*\* ホストに ping を実行します

+

このオプションを使用すると、IPv6 ホストに ping を送信できます。

\*\*\* デフォルト設定に戻します

\*\* \*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  
\*\*\* 診断シェルにアクセスします  
\*\*\* リモート診断アクセスを有効にします

\* 関連情報 \*

xref:{relative\_path}concept-virtual-storage-console-and-vasa-provider-log-files.adoc[VSC および VASA Provider のログファイル]

```
[[ID8fc76b9559c39735c0619bb09515297b]]
= 管理者パスワードを変更します
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]  
メンテナンスコンソールを使用して、導入後にVSC、VASA Provider、SRA仮想アプライアンスの管理者パスワードを変更することができます。

.手順

- . 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。
- . maintenance ユーザとしてログインします。
- . メンテナンスコンソールで「1」と入力して、「アプリケーション構成」を選択します。
- . 「6」を入力して、「管理者」ユーザーパスワードの変更\*を選択します。
- . 8~63 文字のパスワードを入力します。
- . 確認ダイアログボックスに「 y 」と入力します。

```
[[ID48631b2d52995230ef65c2265e180d47]]
= VSC、VASA Provider、SRA仮想アプライアンスの高可用性を設定する
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]  
Virtual Storage Console (VSC) 、VASA Provider、Storage Replication Adapter

(SRA) 仮想アプライアンスでは、(HA) 構成がサポートされます。これにより、障害時にVSC、V ASA Provider、SRAの機能を中断なく提供できます。

VSC、VASA Provider、SRA仮想アプライアンスでは、VMware vSphere (HA) 機能と vSphereフォールトトレランス (FT) 機能を利用して以下の機能を実現します。(HA) 解決策を使用すると、次のような理由でシステム停止からの迅速なリカバリが可能です。

- \* ホスト障害です
- \* ネットワーク障害
- \* 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) がクラッシュする

仮想アプライアンスで追加の設定を行う必要はありません。要件に応じて、vCenter Server ホストと ESXi ホストで 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解決策 およびvSphere FT解決策 に加え、仮想アプライアンスでもVSC、VASA Provider、SRA のサービスを常時実行できるようになります。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。

[NOTE]

=====

vCenter HAは、VSC、VASA Provider、SRA仮想アプライアンスではサポートされません。

=====

```
:leveloffset: +1
```

```
[[IDf54163fbfae2f13602f5e0e7d0354996]]
```

```
= VMware vSphere HA の場合
```

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Virtual Storage Console (VSC)、VASA Provider、Storage Replication Adapter (SRA) 仮想アプライアンスが導入されているvSphere環境 (HA) を設定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提供します。

仮想マシンを監視してオペレーティングシステムの障害やハードウェアの障害を検出し、リソースプール内の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 を設定する手順は、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 のバージョンを選択してください。

<https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.avail.doc/GUID-5432CA24-14F1-44E3-87FB-61D937831CF6.html>["VMware vSphere のドキュメント：「vSphere HA クラスタの作成と使用」"]

```
[[ID3a827601cf6714f0e6952a6174d3e819]]
= VMware vSphere フォールトトレランス
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

VMware vSphereのフォールトトレランス（FT）機能を使用すると（HA）のレベルが高くなり、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機能を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 が有効になっている場合は、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ターゲットホストが選択されます。vSphere FT

では、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、それぞれの仮想マシンの実行状態をセカンダリ仮想マシンにミラーリングします。

ハードウェアに障害が発生してプライマリ仮想マシンに障害が発生すると、セカンダリ仮想マシンはプライマリ仮想マシンが停止した場所をすぐに検出します。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の実行が継続されます。

vCenter Server インスタンスで vSphere FT を設定するには、システムが CPU 要件、仮想マシンの制限要件、およびライセンス要件を満たしている必要があります。

HA を設定する手順は、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 のバージョンを選択してください。

<https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.avail.doc/GUID-57929CF0-DA9B-407A-BF2E-E7B72708D825.html>["VMware vSphere のドキュメント: 「Fault Tolerance の要件、制限、およびライセンス」"]

```
:leveloffset: -1
```

```
[[IDaba32e78debee949ca5110b564bfa40f]]
= VSC、VASA Provider、SRA仮想アプライアンスでサポートされるMetroCluster 構成
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
Virtual Storage Console (VSC)、VASA Provider、Storage Replication Adapter (SRA) 仮想アプライアンスでは、ONTAP のMetroCluster IP構成と FC構成を使用する環境がサポートされます。このサポートはほぼ自動的に行われます。ただし、MetroCluster 環境で VSC および VASA Provider を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ている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がテイクオーバーします。これらの名前には「-

mc」サフィックスが付加されています。データストアのプロビジョニングなどの処理の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の名称が「-

mc」サフィックスのついたものになります。スイッチバックが発生してプライマリサイトののに制御が戻ると、このサフィックスは削除されます。

[NOTE]

====

MetroCluster 構成を直接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。VASA  
Providerに直接を追加することはできません。

[NOTE]

====

VASA Providerでは、スイッチオーバー後にセカンダリサイトのの名称に「-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。

:leveloffset: -1

```
[[ID77d930cfad626c845f6d1823ea34b0c7]]
```

```
= Virtual Storage Console for VMware vSphereストレージシステム環境を設定します
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Virtual Storage Console for VMware

vSphereを使用すると、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を単一のメカニズムで実行できます。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。を使用して、ONTAP RBACロールを定義できます。

[NOTE]

====

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、および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入力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。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、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するときに、ストレージシステムを追加する vCenter Server ボックスが表示されます。このボックスで、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できます。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、次のいずれかの方法で実行されます。いずれの場合も、新たに検出されるすべてのストレージシステムのクレデンシャルを指定する必要があります。

- \* VSC サービスが開始されると、VSC の自動バックグラウンド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またはホスト/データセンターですべて再検出
- \* ボタンをクリックすると、\*アクション\*メニュー（メニュー：アクション[ NetApp VSC >ホストおよびストレージデータの更新]）からこのボタンを選択できます。概要セクションの [ はじめに ] タブで \* 発見 \* をクリックすることもできます。

## VSC

の機能を使用してタスクを実行するときは、いずれも特定の権限が必要です。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。

```
:leveloffset: +1
```

```
[[ID817016e8358a97a62a59137eae992872]]
```

= 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

```
:allow-uri-read:
```

```
:experimental:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

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。

.作業を開始する前に

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。

.このタスクについて

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、(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

. VSC \* Home \* ページで、メニュー：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。

. 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のどちらかです。

+

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。VSC、VASA Provider、SRA

仮想アプライアンスで使用する新しいONTAP ユーザロールを変更または作成するには、System Managerを使用します。

+

『Virtual Storage Console、VASA Provider、and Storage Replication Adapter for VMware®vSphere Deployment and Setup Guide for 9.7 Release]

の「Configuring user roles and privileges」の項を参照してください。

. 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。

## .完了後

ストレージ・システムのステータスが「認証エラー」と報告され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 ] ページで [ 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。

```
[[IDe9300542b9c6d26c08ed7821d4003358]]
```

= ストレージシステムを VSC に追加

```
:allow-uri-read:
```

```
:experimental:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Virtual Storage Console ( VSC ) には手動でストレージシステムを追加できます。

## .このタスクについて

(VSC) を起動するたび、または\* rediscover all

\* オプションを選択するたびに、使用可能なストレージシステムが自動的に検出されます。

#### . 手順

. 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。

+

\*\* [メニュー]、[ストレージシステム]、[追加]の順にクリックします。

\*\* [メニュー]、[はじめに]の順にクリックし、[ストレージシステムの追加]の下の[\*追加]ボタンをクリックします。

. Add Storage System \* (ストレージ・システムの追加) ダイアログ・ボックスで、そのストレージ・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 \* Storage System \*

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。Add Storage System

\* (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インスタンスのドロップダウンリストが表示されます。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。

. 必要な情報をすべて追加したら、「 \* OK 」をクリックします。

```
[[ID0b11d6e75f908f9d8df8e62860119aa1]]
```

= ストレージシステムとホストを検出

```
:allow-uri-read:
```

```
:experimental:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

vSphere Clientで (VSC) を初めて実行すると、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。

#### . 作業を開始する前に

\* 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。

\*

検出するすべてののが実行されている必要があります。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が各クラスターノードに少なくとも1つ設定されている必要があります。

#### . このタスクについて

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、vCenter Server インスタンスで管理している ESXi ホストから情報が収集されます。

#### . 手順

- . vSphere Client \* Home \* ページで、\* Hosts and Clusters \* を選択します。
- . 必要なデータセンターを右クリックし、メニューを選択します。NetApp VSC [ホストおよびストレージデータの更新]。

+

この処理に時間がかかることを通知する確認ダイアログボックスが表示されます。

- . [OK] をクリックします。

.

ステータスが「認証エラー」の検出されたストレージコントローラを選択し、メニューからアクション [Modify] をクリックします。

- . [ストレージ・システムの変更] ダイアログ・ボックスに必要な情報を入力します
- . 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。

#### . 完了後

検出プロセスが完了したら、次の手順を実行します。

- \* VSCを使用して、\* Adapter Settings \* 列、\* MPIO Settings \* 列、または\* NFS Settings \* 列にAlertアイコンが表示されるホスト用のESXiホスト設定を構成します。
- \* ストレージシステムのクレデンシャルを入力します。

```
[[ID87c3d8a7842f28eb2fa36e7208ea1ecc]]
= ストレージシステムの表示を更新します
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

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。

#### . このタスクについて

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は、「`re Fresh`」オプションを使用すると便利です。ストレージ・システムが「Authentication Failure Status」を報告したあとでストレージ・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。更新処理を実行すると、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。

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

- . VMware vSphere Client \* Home \* ページで、\* Storage Systems \* をクリックします。
- . 更新を開始します。

+

```
[cols="1a,1a"]
```

```
|===
```

```
| 場所 | をクリックします
```

```
a|
```

Virtual Storage Console の略

```
a|
```

[ すべて再検出 ( Rediscover All ) ] アイコン

```
a|
```

データセンター

```
a|
```

データセンターを右クリックし、メニューをクリックします。NetApp VSC

[ ホストおよびストレージデータの更新 ]。

```
|===
```

- . [ ホストおよび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、検出に数分かかることがあります。この検出処理はバックグラウンドで実行されます。

- . [ \*成功\* ( \* Success \* ) ] ダイアログボックスで、\* OK \* をクリックする。

```
:leveloffset: -1
```

```
[[ID2a146ff2ee6ca4198bb4d4aa9668375a]]
= VSC for VMware vSphereでのvCenter Server RBAC機能の使用
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
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）に対して設定することができます。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。

```
:leveloffset: +1
```

```
[[ID4a70ef6216f9c61eddcbe9fda523f02fc]]
= vCenter Server アクセス許可の要素
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
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 には次のコンポーネントがあります。

- \* 1 つ以上の権限（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

+

タスクの対象となるオブジェクトです。

- \* 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。

[NOTE]

====

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。

====

image:.../media/permission-updated-graphic.png [アクセス権のグラフィックを更新しました]

== 権限

Virtual Storage Console for VMware vSphereには次の  
2種類の権限が関連付けられています。

- \* 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。これらの権限は、ユーザーのロールを構成し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。これらの権

限は、 vCenter Server にログインしているユーザを対象としています。

[NOTE]

====

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。

[cols="1a,1a,1a"]

|===

| 権限 | ロール | タスク

a|

メニュー：NetApp Virtual Storage Console [表示]

a|

- \* VSC 管理者
- \* VSC によるプロビジョニング
- \* VSC 読み取り専用

a|

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。

a|

メニュー：NetApp Virtual Storage Console [ポリシーベースの管理>管理

]またはメニュー：privilege.nvpfVSC.VASAGroup.com.netapp.nvpf.label[Management]

a|

VSC 管理者

a|

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、 とフォルダ。任意の vSphere オブジェクトに権限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 に対して権限が検証されます。

## == 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。

[NOTE]

=====

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。

```
[[ID13bf9367aafdf350b22462fb6f533430]]
= vCenter Server のアクセス許可の割り当てと変更に関する要点
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

vCenter Server

のアクセス許可を使用する際にはいくつかの点に注意する必要があります。Virtual Storage Console for VMware

vSphereのタスクを実行するかどうかは、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。

## == 権限を割り当てます

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。それ以外の場合は

、管理者としてログインできます。このログインでは、すべての vSphere オブジェクトに自動的にアクセスできます。

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、完了を確認するために、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、必要な権限環境が vSphere 以外のオブジェクト（ストレージシステムなど）に必要な場合です。

このような場合は、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できます。子エンティティには、他の権限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。

**TIP:**

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推奨します。

## == アクセス許可と非 vSphere オブジェクト

作成したアクセス許可は、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。環境ストレージシステムに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、権限がある場合は、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。

[[IDa8327e65ef7eb4b8cf88e4ca77debf38]]

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

```
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

(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 でも必要な権限が付与さ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ユーザに割り当てることができます。

```
[NOTE]
```

```
====
```

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。

```
====
```

VSCの標準ロールは、vSphere Client \* Home \*ページで\* Roles \*をクリックして表示できます。

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。

```
[cols="1a,1a"]
```

```
|====
```

```
| ロール | 説明
```

```
a|
```

VSC 管理者

```
a|
```

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。

```
a|
```

VSC 読み取り専用

```
a|
```

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。

a|  
VSC によるプロビジョニング

a|  
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を作成する
- \* データストアを削除
- \* ストレージ機能プロファイルに関する情報を表示する

|===

:leveloffset: +1

```
[[ID0202e62bbd6526b218f1aa2a2c5cbb60]]
= VSC の標準ロールの使用に関するガイドライン
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]

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従う必要があります。

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たびに、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。これによ  
り、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できます。

ただし、標準のロールを使用して環境に合わせたロールを作成することもできます。これを行うに  
は、VSC

の標準ロールをコピーし、コピーしたロールを編集します。新しいロールを作成しても、VSC  
Windows サービスを再起動またはアップグレードしてもこのロールを維持できます。

VSC の標準ロールの用途としては、次のようなものがあります。

\* 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ることで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します。

+

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、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。

```
:leveloffset: -1
```

```
[[IDe5978efb345f255d33ef6c8c121a4f28]]
```

= VSC タスクに必要な権限

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Virtual Storage Console for VMware

vSphereのタスクを実行するために必要な権限の組み合わせは、(VSC) と vCenter  
Server 標準の権限のそれぞれに異なります。

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  
を参照してください。

[https://kb.netapp.com/Advice\\_and\\_Troubleshooting/Data\\_Storage\\_Software/Virtual\\_Storage\\_Console\\_for\\_VMware\\_vSphere/How\\_to\\_configure\\_RBAC\\_for\\_Virtual\\_Storage\\_Console](https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Virtual_Storage_Console_for_VMware_vSphere/How_to_configure_RBAC_for_Virtual_Storage_Console)["Virtual Storage Console 用の RBAC の設定方法"]

```
:leveloffset: +1
```

```
[[ID47f9e610739ad1ac021259fa67b98de4]]
```

= VSC for VMware vSphereで必要な製品レベルの権限

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

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。この権限なしでログインすると、NetApp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。

```
[cols="1a,1a,1a"]
```

```
|===
```

```
| 権限 | 説明 | 割り当てレベル
```

```
a|
```

表示

```
a|
```

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、タスクで使用する適切なVSC固有の権限とvCenter Serverの標準権限が必要です。

```
a|
```

割り当てレベルによって、表示できるUIの部分が決まります。

ルートオブジェクト（フォルダ）にView権限が割り当てられている場合、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。



|===

```
[ID9f25bdc3d6600e2606d77508039813ec]]
```

= VSC、VASA Provider、SRA仮想アプライアンスに対するONTAP のロールベースアクセス制御

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

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、および仮想マシンのプロビジョニングなど、ストレージに関連するVSC タスク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、

vCenterUserBにデータストアのプロビジョニングを許可し、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を検証されます。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にアクセスできません。

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）が確認されます。その VSC タスクに必要なストレージ処理を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を確認すること。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。

- \* 使いやすさ

+

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。

```
[[IDbff6881f930eb65cee0a916b01136444]]
= VSC for VMware vSphere使用時に推奨されるONTAP ロール
:allow-uri-read:
:icons: font
```

```
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

推奨されるONTAP ロールを設定して、Virtual Storage Console for VMware vSphereおよびRole-Based Access Control (RBAC; ロールベースアクセス制御) を使用できます。これらのロールには、(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。

\* 9.7以降

+

```
xref:{relative_path}task-configure-user-role-and-
privileges.html["ユーザロールと権限を設定"]
```

\* RBAC User Creator for ONTAP ツール (ONTAP 9.6 以前を使用している場合)

+

```
https://community.netapp.com/t5/Virtualization-Articles-and-
Resources/RBAC-User-Creator-tool-for-VSC-VASA-Provider-and-Storage-
Replication-Adapter-7-0/ta-p/133203["VSC 、 VASA Provider 、 Storage
Replication Adapter 7.0 for VMware vSphere 用の RBAC User Creator ツール"^]
```

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。

セキュリティ対策として、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。

． 検出

+

ストレージシステムを追加できます。

． ストレージを作成します

+

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。

． ストレージを変更します

+

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。

． ストレージを破棄します

+

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、「検出」ロールも設定する必要があります。

```
[[ID5fb7bc22bb776978428598f348cdf14d]]
= VSC for VMware vSphere用のONTAP RBACの設定方法
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

Virtual Storage Console for VMware vSphere（`VSC`）でロールベースアクセス制御を使用する場合は、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 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。詳細を直接追加してストレージ・システムを追加する場合は、

`vsadmin` ユーザーには特定のタスクを実行するために必要なすべての役割と機能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 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。

- \* クラスタ管理者または管理者ロールを作成する

+

[NOTE]

====

これらのロールは、次のいずれかを使用して作成できます。

- \*\* ONTAP System Manager 9.7 以降が必要です

xref:{relative\_path}task-configure-user-role-and-privileges.html["ユーザロールと権限を設定"^]

- \*\* RBAC User Creator for ONTAP ツール ( ONTAP 9.6 以前を使用している場合)

link:https://community.netapp.com/t5/Virtualization-Articles-and-Resources/RBAC-User-Creator-tool-for-VSC-VASA-Provider-and-Storage-Replication-Adapter-7-0/ta-p/133203/t5/Virtualization-Articles-and-Resources/How-to-use-the-RBAC-User-Creator-for-Data-ONTAP/ta-p/86601["VSC、 VASA Provider、 Storage Replication Adapter 7.0 for VMware vSphere 用の RBAC User Creator ツール"^]

====

- \* ONTAP

を使用して、ロールが割り当てられ、適切なアプリケーションが設定されたユーザを作成します

+

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になります。 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します

== 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。

\* 検出

+

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

\* ストレージを作成します

+

ボリュームおよび論理ユニット番号 ( LUN ) を作成できます

\* ストレージを変更します

+

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

\* ストレージを破棄します

+

ボリュームおよび LUN を破棄できます

== VASA Provider ロール

クラスタレベルで作成できるのは Policy Based Management  
のみです。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 権限をクラスタレベルまたはレベルでSANまたは  
NASロールに分類します。これにより、ユーザは SRM 処理を実行できるようになります。

[NOTE]

=====

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、ナレッジベースの記事を参照してください。

=====

\*

[https://kb.netapp.com/Advice\\_and\\_Troubleshooting/Data\\_Storage\\_Software/Virtual\\_Storage\\_Console\\_for\\_VMware\\_vSphere/VSC%2C\\_VASA%2C\\_and\\_SRA\\_7.0\\_ONTAP\\_RBAC\\_Configuration\\_Version\\_1](https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Virtual_Storage_Console_for_VMware_vSphere/VSC%2C_VASA%2C_and_SRA_7.0_ONTAP_RBAC_Configuration_Version_1)["VSC 、 VASA 、 SRA 7.0 の ONTAP RBAC 設定"]

\*

[https://kb.netapp.com/Advice\\_and\\_Troubleshooting/Data\\_Storage\\_Software/Virtual\\_Storage\\_Console\\_for\\_VMware\\_vSphere/Roll\\_up\\_of\\_all\\_commands\\_for\\_VSC\\_an](https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Virtual_Storage_Console_for_VMware_vSphere/Roll_up_of_all_commands_for_VSC_an)

```
d_SRA_for_SVM_level["SVM レベルで VSC と SRA
に対するすべてのコマンドを集計します"^]
```

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。

```
[[IDf76805a9f3d31f2c7aee238a4eefbedf]]
= ユーザロールと権限を設定
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

VSC、VASA Provider、SRA仮想アプライアンスに付属のJSONファイルとONTAP System Managerを使用して、ストレージシステムの管理に使用する新しいユーザロールを設定できます。

#### .作業を開始する前に

- \* VSC、VASA Provider、SRA仮想アプライアンスから、「+  
[https://{virtual\\_appliance\\_IP}:9083/vsc/config/VSC\\_ONTAP\\_User\\_Privileges.zip+`](https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip+`)」を使用してONTAP Privilegesファイルをダウンロードしておく必要があります。
- \* ONTAP 9.7 System Managerを設定しておく必要があります。
- \* ストレージシステムの管理者権限でログインしている必要があります。

#### .手順

##### . ダウンロードした「+

[https://{virtual\\_appliance\\_IP}:9083/vsc/config/VSC\\_ONTAP\\_User\\_Privileges.zip+`](https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip+`)」ファイルを解凍します。

- . ONTAP システムマネージャにアクセスします。
- . メニューをクリックします。cluster [設定]、[ユーザとロール]の順に選択します。
- . [ ユーザーの追加 ] をクリックします。
- . [ユーザーの追加\*]ダイアログボックスで、[仮想化製品\*]を選択します。
- . [\* Browse] をクリックして、ONTAP 権限 JSON ファイルを選択し、アップロードします。

+

プロダクトフィールドには、自動的に値が入力されます。

- . 必要な機能を\*Product Capability \*(製品機能\*)ドロップダウンメニューから選択します。

+

```
[* 役割 * (* role *)]
```

フィールドは、選択したプロダクト機能に基づいて自動的に入力されます。

- ．必要なユーザ名とパスワードを入力します。
- ．ユーザに必要な権限（ Discovery 、 Create Storage 、 Modify Storage 、 Destroy Storage ）を選択し、 \* Add \* をクリックします。

## ．結果

新しいロールとユーザが追加され、設定したロールの詳細な権限が表示されます。

```
:leveloffset: -1
```

```
:leveloffset: -1
```

```
[[IDc436f1457375105909eb1fe9d3f379b1]]
= ディザスタリカバリ用の Storage Replication Adapter を設定する
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

ディザスタリカバリ用にvCenter Serverを設定する場合は、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に、vCenter Server用のSRAを有効にする必要があります。

## \* 関連情報 \*

```
xref:{relative_path}task-enable-storage-replication-adapter.adoc[Storage
Replication Adapter を有効にする]
```

```
:leveloffset: +1
```

```
[[ID9ff8cae5228e46dec36b3ffa0142d40c]]
= SAN 環境向けの Storage Replication Adapter の設定
:allow-uri-read:
:icons: font
```



```
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

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。

.作業を開始する前に

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 の場合

+

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。

+

[https://www.vmware.com/support/pubs/srm\\_pubs.html](https://www.vmware.com/support/pubs/srm_pubs.html)["VMware Site Recovery Manager のドキュメント"^]

\* SRA

+

アダプタは SRM にインストールされます。

.手順

. 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。

. プライマリ・ストレージ・システムで、「\* ostype \*」オプションが `_vmware_` に設定されているigroupにLUNが含まれていることを確認します。

. リカバリサイトのESXiホストがFCまたは iSCSI経由で適切に接続されていることを確認します。

+

これを行うには、ESXiホストの上にローカルLUNが接続されていることを確認するか、上の `fcps show initiators` コマンドまたは `iscsi show initiators` コマンドを使用します。

```
[[ID461ab72aae10e4bf29c49ca8a7616f71]]
```

= NAS 環境向けの Storage Replication Adapter の設定

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

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。

.作業を開始する前に

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 の場合

+

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。

+

[https://www.vmware.com/support/pubs/srm\\_pubs.html](https://www.vmware.com/support/pubs/srm_pubs.html)["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

. 保護対象サイトのデータストアに、 vCenter Server に登録された仮想マシンがあることを確認します。

. 保護対象サイトのESXiホストに、から 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。

. SRMにアレイを追加するために、\* Array Manager \*ウィザードを使用して、 NFSエクスポートが存在するIPアドレス、ホスト名、FQDNなどの有効なアドレスが\* NFS Addresses \*フィールドに指定されていることを確認します。

. リカバリサイトの各ESXiホストでpingコマンドを使用して、ホストがから NFSエクスポートへの接続に使用されるIPアドレスにアクセスできるVMkernelポートを持っていることを確認します。

<https://mysupport.netapp.com/site/>["ネットアップサポート"^]

```
[[ID4aeb4aa6f920e63d695219764501e23c]]
```

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

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]

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

12000 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。

<https://docs.vmware.com/en/Site-Recovery-Manager/6.5/com.vmware.srm.admin.doc/GUID-E4060824-E3C2-4869-BC39-76E88E2FF9A0.html> ["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

[NOTE]

====

指定したタイムアウト間隔が最大値です。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内に終了します。

====

[https://kb.netapp.com/app/answers/answer\\_view/a\\_id/1001111](https://kb.netapp.com/app/answers/answer_view/a_id/1001111) ["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。

<https://docs.vmware.com/en/Site-Recovery-Manager/6.5/com.vmware.srm.admin.doc/GUID-711FD223-50DB-414C-A2A7-3BEB8FAFDBD9.html> ["VMware Site Recovery Manager のドキュメント：「ストレージ設定の変更"^]

```
:leveloffset: -1
```

```
[[ID0a373b3de28889d978279dbfd063de03]]
```

= VSC、VASA Provider、SRA仮想アプライアンスの問題のトラブルシューティング

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

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、原因 の問題を特定し、解決することができます。

```
:leveloffset: +1
```

```
[[ID08f6e53fc8e040f94994a7ff140b7e02]]
```

=

vSphere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ます

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ./deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

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のプラグインパッケージをクリーンアップして、vCenter Serverのプラグインの問題を解決する必要があります。

#### . 手順

- . 既存の vSphere Web Client または vSphere Client からログアウトします。
- . ブラウザキャッシュを削除します。
- . 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。

+

```
[cols="1a,1a"]
```

```
|===
```

```
| 使用するポート | 実行する手順
```

```

a|
Windows vCenter Server の場合
a|
次の場所にあるcom.netapp.vasa.vvol.webclient-x.x.x.xxxx
、 com.netapp.nvpf.webclient-x.x.x.xxxx、 およびcom.netapp.vsch5-
x.x.x.xxxx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

a|
vCSA
a|
.. SSH で vCSA アプライアンスに接続します。
.. cd /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity
を使用して、 vCenter Web Client UI 拡張ディレクトリにディレクトリを変更します
.. 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`

.. 「 cd /etc/vmware/vsphere-clientui/vc-packages/vsphere-client-serenity
」を使用して、ディレクトリを vCenter クライアント (HTML5) UI
拡張ディレクトリに変更します
.. 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`

|===
. 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 -- vsphere-stop vsphere-client vsphere-ui`
** 「service-control」 -- vSphereクライアントのvsphere-uiを起動します
```

```
[[ID8e7d29b416e0c55a9e1bb9cca08b6ab6]]
= アンインストールしても、標準のVSCロールは削除されません
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
Virtual Storage Console for VMware vSphere (VSC) をアンインストールしても、標準のVSCロールは維持されます。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固有の権限のローカライズ名が削除され、代わりに「XXX missing privilege」というプレフィックスが付けられます。たとえば、VSCのインストール後にvSphere \* Edit Role \*ダイアログボックスを開くと、VSC固有の権限が「XXX missing privilege」と表示されます。`<privilege name>`.label not found XXX`

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。

```
[[IDd78aa40fe2b180127ff6ec4c9c736038]]
= Virtual Storage Console と VASA Provider のログファイル
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
エラーが発生した場合は、「 /opt/NetApp/vscserver/log 」ディレクトリと「 /opt/NetApp/smsserver/log' 」ディレクトリでログファイルを確認できます。
```

問題の特定には、次の 3 つのログファイルが役立ちます。

- \* 「cxf.log」。VASA Providerとの間で送受信される API トラフィックに関する情報が記録されます
- \* 「kaminoPrefs.xml」。VSC の設定に関する情報が含まれます
- \* vvolvp.log : VASA Provider に関するすべてのログ情報が含まれます

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。次のログレベルを使用できます。

- \* 情報
- \* デバッグ
- \* エラー
- \* トレース

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 サーバー: 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 ページは '\_https\_://<IP\_address\_or\_hostname>:9083/stats' にあります

```
[[IDdabe5439c0865e24104f676858d6d32d]]
= 大規模な環境では、VSC サービスと VASA Provider サービスが再起動します
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

== 問題

大規模な環境で 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する

[https://kb.netapp.com/Advice\\_and\\_Troubleshooting/Data\\_Storage\\_Software/Virtual\\_Storage\\_Console\\_for\\_VMware\\_vSphere/tune\\_memory\\_settings\\_of\\_VM\\_VSC%2C\\_VASA\\_Provider%2C\\_and\\_SRA\\_for\\_scale\\_and\\_performance\[\]](https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Virtual_Storage_Console_for_VMware_vSphere/tune_memory_settings_of_VM_VSC%2C_VASA_Provider%2C_and_SRA_for_scale_and_performance[])

```
[[ID24b324dbe26bf9d1fe9921f438064014]]
= SSH を使用するように VASA Provider を設定する
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
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、セキュアなアクセスにSSHを使用するようにVASA Providerを設定できます。
```

### . このタスクについて

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です。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

- . 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。
- . maintenance ユーザとしてログインします。
- . 「 3 」を入力して、「 \* システム構成 \* 」を選択します。
- . 「 6 」と入力して、「 SSH アクセスを有効にする」を選択します。
- . 確認ダイアログボックスに「 y 」と入力します。

```
[[IDd3818a3d2a826ec3c4fb737ad9fa18dc]]
= リモートdiagアクセスにSSHを使用するようにVSC、VASA Provider、SRA仮想アプライアンスを設定する
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
```



```
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```

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。

.作業を開始する前に

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。

.このタスクについて

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をアクティブ化した場合、ログインは1回だけ許可されます。
- \* 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

- . vCenter Server で、 VASA Provider へのコンソールを開きます。
- . maintユーザとしてログインします。
- . 「4」と入力して、「\* Support and Diagnostics (サポートおよび診断)」\*を選択します。
- . 「3」と入力して、「\*リモート診断アクセスを有効にする\*」を選択します。
- . [\*Confirmation\*]ダイアログボックスに「y」と入力して、リモート診断アクセスを有効にします。
- . リモート診断アクセス用のパスワードを入力します。

```
[[ID31cacc9da9fdcaa7be2b90a5eb2d4a09]]
```

= SRAのインストールがスクリプトエラーで失敗する

```
:allow-uri-read:
```

```
:icons: font
```

```
:relative_path: ../deploy/
```

```
:imagesdir: {root_path}{relative_path}../media/
```

## == 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、Windows 2008 R2仮想アプライアンス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することがあります。

## == 対処方法

Windows 2008 R2にSRAをインストールする場合は、メンテナンスコンソールで次の手順に従って、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。

- ・ 「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。
- ・ メインメニューから\* 1 \*を選択し、\*アプリケーション設定\*メニューを表示します。
- ・ [アプリケーションの構成\*]メニューで\*13\*と入力し、[アプリケーションの構成\*]メニューから\*Enable TLS Protocol\*を選択します。
- ・ TLSプロトコルリストで\*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。

```
[[ID5540edf914621c0d1f08d82a7eafe398]]
= 大規模な環境でSRAのパフォーマンスを最適化できない
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

## == 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（250 PG、250 RP、5000 VMなどの上限を指定してVMwareを実行している場合）、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する場合があります。

## == 対処方法

タイムアウト間隔を変更する必要があります。

xref:{relative\_path}reference-configure-storage-replication-adapter-for-highly-scaled-environment.html["大規模な環境向けのStorage Replication Adapterの設定"]

[NOTE]

====

大規模な環境では、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。

[https://kb.netapp.com/Advice\\_and\\_Troubleshooting/Data\\_Storage\\_Software/Virtual\\_Storage\\_Console\\_for\\_VMware\\_vSphere/tune\\_memory\\_settings\\_of\\_VM\\_VSC%2C\\_VASA\\_Provider%2C\\_and\\_SRA\\_for\\_scale\\_and\\_performance\[\]](https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Virtual_Storage_Console_for_VMware_vSphere/tune_memory_settings_of_VM_VSC%2C_VASA_Provider%2C_and_SRA_for_scale_and_performance[])

====

```
[[IDecdda279fb16f2e8cec1d9fd127c6279]]
= SRAプラグインをインストールできません
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

## == 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、「The credentials you entered are not valid.有効なホスト名とパスワードを入力してください。」

## == 原因

このエラーは、次のいずれかの原因で発生することがあります。

- \* 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、技術情報アーティクルを参照してください。

+

[https://kb.netapp.com/app/answers/answer\\_view/a\\_id/1005074](https://kb.netapp.com/app/answers/answer_view/a_id/1005074)["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-upgrade .msi) hangs at the server IP and password screen"^]

```
[[IDb412e97f54b7f9fc8426bcf5cdd373b7]]
= NetApp Storage Replication Adapter for ONTAP は、Site Recovery
Managerアプライアンスに表示されません
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

## == 問題

Storage Replication Adapter (SRA) をアップロードおよび設定したあと、Site Recovery Manager (SRM) アプライアンスインターフェイスにSRAが表示されません。

## == 原因

次のコマンドで誤ったSRAクレデンシャル（ユーザ名またはパスワード）を使用してSRAを設定して

も、エラーが表示されません。

```
`perl command.pl -i <sra_server-ip><vp_username><vp_passwd>`
```

## == 対処方法

次のコマンドを使用して、SRAの設定の詳細を更新します。「perl command.pl -U <sra\_server-ip><vp\_username><vp\_passwd>`」

```
[[IDc472b07a3c643d5c35786549dd0239f4]]
= VSC 、 VASA Provider 、 SRA 仮想アプライアンスの新規導入時にエラーが発生する
:allow-uri-read:
:icons: font
:relative_path: ./deploy/
:imagesdir: {root_path}{relative_path}../media/
```

## == 問題

無効なvCenter ServerIPv4アドレスが使用されている場合、VSC、VASA Provider、SRA仮想アプライアンスの新規導入時にエラーログ「vmware tools OVF vCenter configuration not found」が表示されます。

## == 原因

VSC、VASA Provider、SRA仮想アプライアンスでは、IPv4およびIPv6アドレスがサポートされます。ユーザがネットワークで使用できないvCenter Serverに対してIPv4アドレスを指定し、IPv6アドレスが指定されていない場合、これらのログメッセージがメンテナンスコンソールに表示されます。

## == 対処方法

エラーを削除するには、次の手順を実行する必要があります。

- ・ メンテナンスコンソールにログインします。
- ・ 診断シェルにアクセスします。
- ・ 「sudo su」コマンドを使用して、ユーザを「diag」から「root」に変更します。

- ・ viエディタvi /etc/network/interfaceを使用して  
「インタフェース・ファイルを編集します
- ・ 「inet6」のエントリを削除します。
- ・ ファイルを保存して、VSC、VASA Provider、SRA仮想アプライアンスをリブートします。

仮想アプライアンスのリブート後、エラーメッセージは表示されません。

```
:leveloffset: -1
```

```
:leveloffset: -1
```

```
:leveloffset: -1
```

<<<

\*著作権に関する情報\*

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

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

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

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

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

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年

2月) および FAR 5252.227-19 (2007年12月) の Rights in Technical Data -Noncommercial Items (技術データ - 非商用品目に関する諸権利) 条項の (b) (3) 項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス (FAR 2.101の定義に基づく) に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ

ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015 (b) 項 (2014年2月) で定められた権利のみが認められます。

\*商標に関する情報\*

NetApp、NetAppのロゴ、link:<http://www.netapp.com/TM>[<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。