vCenter 用のストレージプラグイン

E-Series Systems

NetApp
August 13, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/e-series/vcenter-plugin/san-spvc-ic-overview.html on August 13, 2024. Always check docs.netapp.com for the latest.

目次

vCenter 用のストレージプラグイン . . . 1
vCenter 向けストレージプラグインの概要 . . . 1
はじめに . . . 3
証明書を管理します . . . 19
アレイを管理します . . . 26
設定をインポートします . . . 32
アレイグループを管理します . . . 39
OSソフトウェアをアップグレードします . . . 41
ストレージのプロビジョニング . . . 47
ホストを設定 . . . 73
プールとボリュームグループを設定 . . . 82
vCenter 向けストレージプラグインを削除します . . . 112
よくある質問です . . . 113

vCenter 用のストレージプラグイン

vCenter 向けストレージプラグインの概要

SANtricity Storage Plugin for vCenter では、 VMware vSphere Client セッションから E シリーズストレージアレイを統合管理できます。

使用可能なタスク

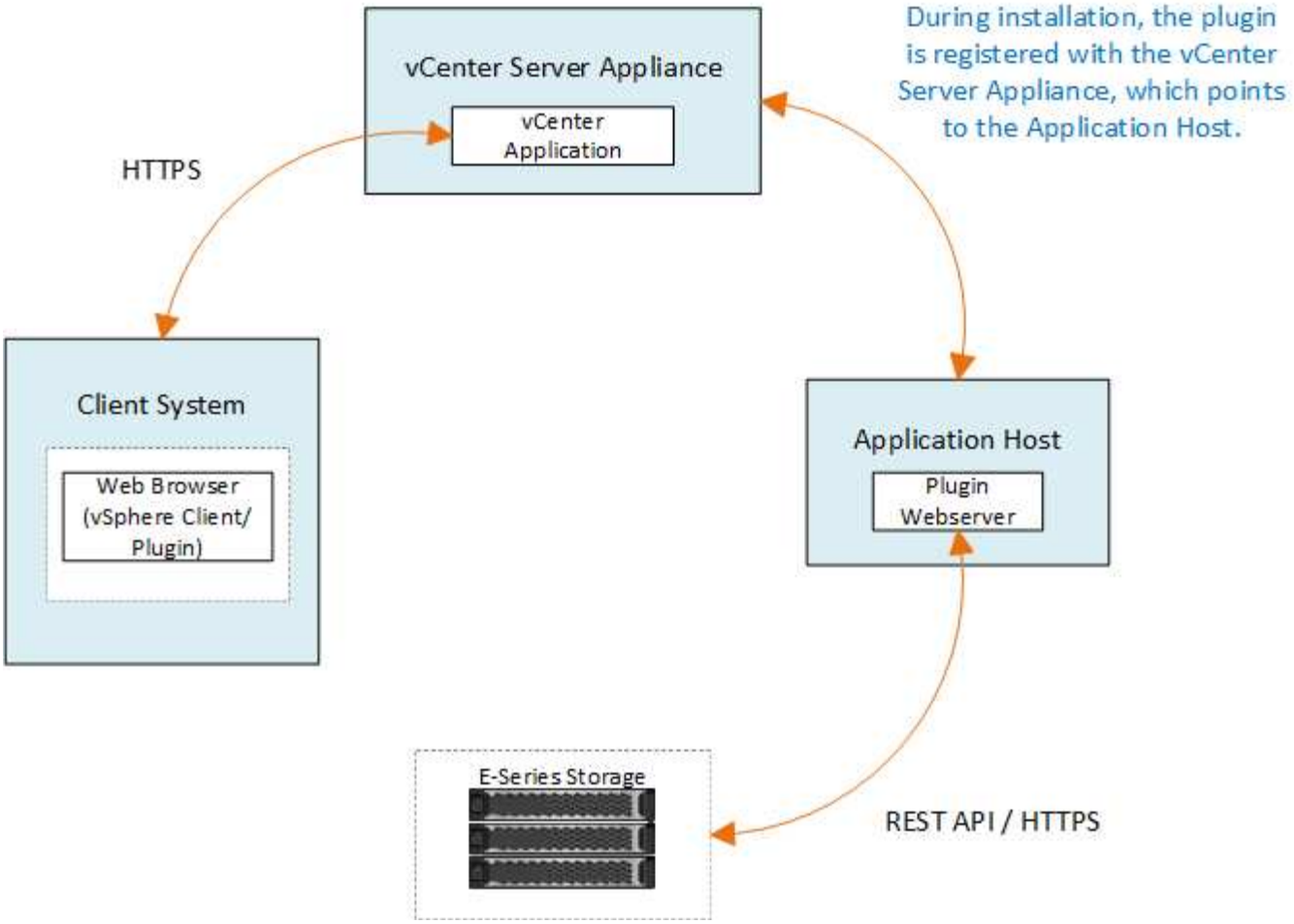
このプラグインを使用して、次のタスクを実行できます。

- ネットワーク内で検出されたストレージアレイを表示および管理します。
- 複数のストレージアレイのグループに対してバッチ処理を実行する。
- ソフトウェア OS でアップグレードを実行
- ストレージアレイから別のストレージアレイへ設定をインポートする。
- ボリューム、 SSD キャッシュ、ホスト、ホストクラスタ、プールの構成 ボリュームグループを指定します。
- アレイでのその他の管理タスクを実行するには、 System Manager インターフェイスを起動してください。

> プラグインは、System Managerインターフェイスに直接代わるものではなく、ストレージアレイの各コントローラに組み込まれています。System Managerには管理機能が追加されています。必要に応じて、プラグインのメインビューでストレージアレイを選択し、* Launch *をクリックすると、System Managerを開くことができます。

このプラグインを使用するには、 VMware 環境に導入された VMware vCenter Server Appliance と、プラグイン Web サーバをインストールして実行するアプリケーションホストが必要です。

vCenter 環境での通信の詳細については、次の図を参照してください。



インターフェイスの概要

プラグインにログインすると、メインページが* Manage-All *に開きます。このページでは、ネットワークで検出されたすべてのストレージアレイを表示および管理できます。

ナビゲーションサイドバー

ナビゲーションサイドバーには、次の情報が表示されます。

- 管理--ネットワーク内のストレージアレイの検出、アレイのSystem Managerの起動、1つのアレイから複数のアレイへの設定のインポート、アレイグループの管理、SANtricity OSのアップグレード、ストレージのプロビジョニングを行います。
- 証明書管理--ブラウザとクライアント間の認証に使用する証明書を管理します
- オペレーション--あるアレイから別のアレイへの設定のインポートなど’バッチ操作の進行状況を表示します

> ストレージアレイのステータスが最適でない場合は、一部の処理は使用できません。

- サポート--テクニカルサポートのオプション、リソース、連絡先を表示します。

サポートされているブラウザ

vCenter向けストレージプラグインには、いくつかの種類のブラウザからアクセスできます。サポートされるブラウザとバージョンを次に示します。

- Google Chrome 89以降
- Mozilla Firefox 80以降
- Microsoft Edge 90以降

ユーザロールと権限

vCenter向けストレージプラグインのタスクにアクセスするには、読み取り/書き込み権限が必要です。デフォルトでは、定義されているすべてのVMware vCenterユーザIDに、プラグインでタスクを実行する権限がありません。

設定の概要

設定には、次の手順が含まれます。

1. "プラグインをインストールして登録します"。
2. "プラグインアクセス権限を設定します"。
3. "プラグインインターフェイスにログインします"。
4. "ストレージアレイを検出"。
5. "ストレージのプロビジョニング"。

詳細については、こちらをご覧ください

vSphere Client でのデータストアの管理の詳細については、を参照してください "VMware vSphere のドキュメント"。

はじめに

インストールとアップグレードの要件を確認

SANtricity Storage Plugin for vCenterをインストールまたはアップグレードする前に、インストール要件とアップグレード時の考慮事項を確認してください。

インストールの要件

Windowsホストシステムにvcenter向けストレージプラグインをインストールして設定できます。プラグインのインストールには次の要件が含まれています

要件	説明
サポートされるバージョン	• VMware vCenter Server Applianceのサポートされるバージョン：6.7U3J、7.0U1、7.0U2、7.0U3、および8.0。 • NetApp SANtricity OS バージョン： 11.60.2 以降 • サポートされるアプリケーションホストのバージョン：Windows 2016、Windows 2019、Windows 2022 互換性の詳細については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。
複数のインスタンス	WindowsホストにインストールできるvCenter向けStorage Pluginのインスタンスは1つだけで、1つのvCSAに登録できます。
キャパシティプランニング	vCenter向けストレージプラグインを実行してログを作成するために必要な十分なスペースがあります。使用可能なディスクスペースについて、システムが次の要件を満たしていることを確認してください。 • 必要なインストールスペース：275MB • ストレージ容量：275 MB + 200 MB（ロギング） • システムメモリ—1.5 GB
使用許諾	vCenter向けストレージプラグインは、ライセンスキーを必要としない、無償のスタンドアロン製品です。ただし、該当する著作権とサービス利用規約が適用されます。

アップグレード時の考慮事項

以前のバージョンからアップグレードする場合は、アップグレード前にプラグインをvCSAから登録解除する必要があります。

- アップグレード中は、プラグインの以前の構成設定のほとんどが保持されます。これには、ユーザパスワード、検出されたすべてのストレージシステム、サーバ証明書、信頼された証明書、サーバのランタイム設定などが含まれます。
- アップグレードプロセスでは*。vcenter.properties*ファイルは保持されないため、アップグレード前にプラグインの登録を解除する必要があります。アップグレードが完了したら、プラグインをvCSAに再度登録できます。
- リポジトリにロードされていたすべてのSANtricity OSファイルは、アップグレード中に削除されます。

vCenter向けストレージプラグインをインストールまたはアップグレードします

Storage Plugin for vCenterをインストールし、プラグインの登録を確認する手順は、次のとおりです。これらの手順を使用してプラグインをアップグレードすることもできます。

インストールの前提条件を確認する

の要件をシステムが満たしていることを確認します "インストールとアップグレードの要件を確認"。

> アップグレードプロセスでは、*。vcenter.properties*ファイルは保持されません。アップグレードする場合は、アップグレード前にプラグインの登録を解除する必要があります。アップグレードが完了したら、プラグインをvCSAに再度登録できます。

プラグインソフトウェアをインストールします

プラグインソフトウェアをインストールするには：

1. アプリケーションサーバとして使用するホストにインストーラファイルをコピーし、インストーラをダウンロードしたフォルダにアクセスします。
2. インストールファイルをダブルクリックします。

   'santricity _savcenterplugin -windows_x64 --nn.nn.nnnn.exe`

   上記のファイル名の「 nn.nn.nn.nnnn 」はバージョン番号です。

3. インストールが開始されたら、画面の指示に従っていくつかの機能を有効にし、いくつかの設定パラメータを入力します。選択した内容は、必要に応じてあとで構成ファイルで変更できます。

   > アップグレードの実行中、構成パラメータの入力は求められません。

   > インストール時に、証明書の検証を求めるプロンプトが表示されます。プラグインとストレージアレイの間で証明書の検証を実施する場合は、このチェックボックスを選択したままにします。この適用では、ストレージアレイ証明書がプラグインに対して信頼されているかどうかがチェックされます。証明書が信頼されていない場合は、プラグインに追加できません。証明書の検証を無視する場合は、チェックボックスを選択解除して、すべてのストレージアレイを自己署名証明書を使用してプラグインに追加できるようにします。証明書の詳細については、プラグインインターフェイスから入手できるオンラインヘルプを参照してください。

4. Webserver Startedというメッセージが表示されたら、* OK をクリックしてインストールを完了し、 Done *をクリックします。
5. *services.msc * コマンドを実行して、アプリケーションサーバーが正常にインストールされたことを確認します。
6. アプリケーションサーバ（ VCP ）サービス * NetApp SANtricity Storage Plugin for vCenter * がインストールされ、サービスが開始されていることを確認します。

必要に応じて、インストール後に証明書の検証と Web サービスポートの設定を変更できます。インストールディレクトリから、 wsconfig.xml ファイルを開きます。ストレージ・アレイの証明書検証を削除するには 'env' キー 'trust.all.arrays' を 'true' に変更しますWeb Services ポートを変更するには 'slport' の値を 0 〜 65535 の範囲の任意のポート値に変更します使用するポート番号が別のプロセスにバインドされていないことを確認します。完了したら、変更を保存してプラグイン Web サーバを再起動します。プラグインを vCSA に登録したあとにプラグイン Web サーバのポート値が変更された場合は、変更されたポートの vCSA がプラグインに通信するように、プラグインの登録を解除して再登録する必要があります。

プラグインを **vCenter Server Appliance** に登録します

プラグインソフトウェアをインストールしたら、 vCSA にプラグインを登録します。

プラグインを登録できる vCSA は 1 つだけです。別のvCSAに登録するには、現在のvCSAからプラグインの登録を解除し、アプリケーションホストからアンインストールする必要があります。その後、プラグインを再インストールして他のvCSAに登録できます。

1. コマンドラインでプロンプトを開き、次のディレクトリに移動します。

   `< インストールディレクトリ >\vcenter-register-bin'

2. vCenter の登録 .bat * ファイルを実行します。 vcenter-register.bat アクション registerPlugin^-vcenterHostname <vCenter FQDN>^-UserName <Administrator username>^`
3. スクリプトが正常に完了したことを確認します。

ログは '%install_dir%/working/logs/vc-registration.log' に保存されます

プラグインの登録を確認します

プラグインをインストールして登録スクリプトを実行したら、プラグインが vCenter Server Appliance に正常に登録されていることを確認します。

1. vSphere Client から vCenter Server Appliance を開きます。
2. メニューバーで、 [管理者][クライアントプラグイン] を選択します。
3. vCenter向けストレージプラグインが「* enabled *」と表示されていることを確認してください。

   [無効] と表示され、アプリケーションサーバーと通信できないことを示すエラーメッセージが表示された場合は、アプリケーションサーバーに定義されているポート番号が使用中のファイアウォールを通過できることを確認します。デフォルトのアプリケーションサーバーの Transmission Control Protocol （ TCP ）ポート番号は 8445 です。

プラグインアクセス権限を設定します

vCenter 向けストレージプラグインのアクセス権限を設定できます。この権限には、ユーザ、ロール、および権限が含まれます。

必要な **vSphere** 権限を確認します

vSphere Client 内でプラグインにアクセスするには、適切な vSphere 権限を持つロールが割り当てられている必要があります。vSphere の「データストアの設定」権限を持つユーザーは、プラグインへの読み取り / 書き込みアクセス権を持ち、「データストアの参照」権限を持つユーザーは読み取り専用アクセス権を持ちます。ユーザーがこれらの権限を持たない場合、プラグインに「不十分な権限」というメッセージが表示されます。

プラグインのアクセスタイプ	**vSphere** 権限が必要です
読み取り / 書き込み（設定）	データストア。設定
読み取り専用（表示）	データストア参照

ストレージ管理者のロールを設定する

プラグインユーザに読み取り / 書き込み権限を付与するには、ロールを作成、クローニング、または編集します。vSphere Client でのロールの設定の詳細については、 VMware ドキュメントセンターの次のトピックを参照してください。

- "カスタムロールを作成します"

アクセスロールのアクション

1. vSphere Client のホームページで、アクセス制御領域から * Administrator * を選択します。
2. アクセス制御領域で * 役割 * をクリックします。
3. 次のいずれかを実行します。
    - * 新しい役割の作成 *: [役割の作成 *] アクションアイコンをクリックします。
    - * 役割のクローン * ：既存の役割を選択し、 * 役割のクローン * アクションアイコンをクリックします。
    - * 既存のロールの編集 *: 既存のロールを選択し、 * ロールの編集 * アクションアイコンをクリックします。

> 管理者ロールは編集できません。

上記の選択に応じて、適切なウィザードが表示されます。

新しいロールを作成します

1. 権限リストで、このロールに割り当てるアクセス権限を選択します。

   プラグインへの読み取り専用アクセスを許可するには、 [MENU] ： [Browse Datastore] を選択します。読み取り / 書き込みアクセスを許可するには、メニューから [データストアの設定] を選択します。

2. 必要に応じて、リストに他の権限を割り当て、 [* 次へ *] をクリックします。
3. ロールに名前を付け、概要を指定します。
4. [完了] をクリックします。

ロールのクローンを作成します

1. ロールに名前を付け、概要を指定します。
2. [OK] をクリックしてウィザードを終了します。
3. リストから複製されたロールを選択し、 * 役割の編集 * をクリックします。
4. 権限リストで、このロールに割り当てるアクセス権限を選択します。

   プラグインへの読み取り専用アクセスを許可するには、 [MENU] ： [Browse Datastore] を選択します。読み取り / 書き込みアクセスを許可するには、メニューから [データストアの設定] を選択します。

5. 「 * 次へ * 」をクリックします。
6. 必要に応じて、名前と概要を更新します。
7. [完了] をクリックします。

既存のロールを編集します

1. 権限リストで、このロールに割り当てるアクセス権限を選択します。

   プラグインへの読み取り専用アクセスを許可するには、 [MENU] ： [Browse Datastore] を選択します。読み取り / 書き込みアクセスを許可するには、メニューから [データストアの設定] を選択します。

2. 「 * 次へ * 」をクリックします。
3. 必要に応じて、名前または概要を更新します。
4. [完了] をクリックします。

vCenter Server Appliance のアクセス許可を設定します

ロールの権限を設定したら、 vCenter Server Appliance に権限を追加する必要があります。この権限は、指定されたユーザまたはグループにプラグインへのアクセスを許可します。

1. メニューのドロップダウン・リストから、 **Hosts and Clusters** を選択します。
2. アクセス制御領域から * vCenter Server Appliance * を選択します。
3. [* アクセス許可 *] タブをクリックします。
4. [権限の追加] アクションアイコンをクリックします。
5. 適切なドメインとユーザ / グループを選択します。
6. 読み取り / 書き込みプラグイン権限を許可する、作成されたロールを選択します。
7. 必要に応じて、 [子に伝播（ * Propagate to children ）] オプションを有効にします。
8. [OK] をクリックします。

> 既存の権限を選択し、作成したロールを使用するように変更できます。* ただし、権限で正規表現を行わないようにするためには、読み取り / 書き込みプラグイン権限と同じ権限が役割に付与されている必要があります。 *

プラグインにアクセスするには、そのプラグインの読み取り / 書き込み権限を持つユーザアカウントで vSphere Client にログインする必要があります。

権限の管理の詳細については、 VMware ドキュメントセンターの次のトピックを参照してください。

- "vCenter コンポーネントのアクセス許可の管理"
- "ロールと権限のベストプラクティス"

ログインして、 **Storage Plugin for vCenter** に移動します

vCenter 向けストレージプラグインにログインして、ユーザインターフェイスを操作できます。

1. プラグインにログインする前に、次のいずれかのブラウザを使用していることを確認してください。
   - Google Chrome 89以降
   - Mozilla Firefox 80以降
   - Microsoft Edge 90以降
2. プラグインの読み取り / 書き込み権限を持つユーザアカウントで vSphere Client にログインします。
3. vSphere Client のホームページで、 * SANtricity Storage Plugin for vCenter * をクリックします。

   vSphere Client ウィンドウにプラグインが開きます。プラグインのメインページが開き、 * Manage-All * が表示されます。

4. 左側のナビゲーションサイドバーからストレージ管理タスクにアクセスします。
   - * 管理 * –ネットワーク内のストレージ・アレイの検出 ' アレイの System Manager の起動 ' アレイから複数のアレイへの設定のインポート ' アレイ・グループの管理 'OS ソフトウェアのアップグレード ' ストレージのプロビジョニングを行います
   - * 証明書管理 * –ブラウザとクライアント間で認証するための証明書を管理します。
   - * 操作 * - あるアレイから別のアレイへの設定のインポートなど、バッチ操作の進行状況を表示します。
   - * サポート * –テクニカルサポートのオプション、リソース、連絡先を表示します。

ストレージアレイのステータスが最適でない場合は、一部の処理は使用できません。

プラグインでストレージアレイを検出します

ストレージリソースを表示および管理するには、 Storage Plugin for vCenter インターフェイスを使用して、ネットワーク内のアレイの IP アドレスを検出する必要があります。

作業を開始する前に

- アレイコントローラのネットワーク IP アドレス（またはアドレスの範囲）を確認しておく必要があります。
- ストレージアレイが正しくセットアップおよび設定され、ストレージアレイのログインクレデンシャル（ユーザ名とパスワード）が必要です。

手順 **1** ：検出するネットワークアドレスを入力します

手順

1. [管理] ページで、 [* 追加 / 検出 *] を選択します。

   [Enter Network Address Range] ダイアログボックスが表示されます。

2. 次のいずれかを実行します。

   - 1 つのアレイを検出するには、 * 単一のストレージアレイの検出 * オプションボタンを選択し、ストレージアレイのいずれかのコントローラの IP アドレスを入力します。
   - 複数のストレージアレイを検出するには、「ネットワーク範囲内のすべてのストレージアレイを検出」ラジオボタンを選択し、開始ネットワークアドレスと終了ネットワークアドレスを入力してローカルサブネットワーク全体を検索します。

3. [検出の開始] をクリックします。

   検出プロセスが開始されると、ストレージアレイが検出されるときにダイアログボックスに表示されます。検出プロセスが完了するまでに数分かかることがあります。

   管理可能なアレイが検出されない場合は、ストレージアレイがネットワークに適切に接続されていて、割り当てられたアドレスが範囲内にあることを確認してください。[新規検出パラメータ *] をクリックして、 [追加 / 検出] ページに戻ります。

4. 管理ドメインに追加するストレージアレイの横にあるチェックボックスをオンにします。

   管理ドメインに追加する各アレイについて、クレデンシャルのチェックが実行されます。信頼されていない証明書に関する問題の解決が必要になる場合があります。

5. 「 * 次へ * 」をクリックして、ウィザードの次の手順に進みます。

   ストレージアレイに有効な証明書がある場合は、に進みます 手順 3 ：パスワードを入力する。

   有効な証明書がないストレージアレイがある場合は、自己署名証明書の解決ダイアログボックスが表示されます。に進みます 手順 2 ：検出時に信頼されていない証明書を解決する。

   CA 署名証明書をインポートする場合は、検出ウィザードをキャンセルし、左パネルから * 証明書の管理 * をクリックします。詳細については、オンラインヘルプを参照してください。

手順 **2** ：検出時に信頼されていない証明書を解決する

証明書の問題を解決してから検出プロセスを開始する必要があります。

1. [自己署名証明書の解決] ダイアログボックスが開いた場合は、信頼されていない証明書について表示される情報を確認します。詳細については、表の右端にある省略記号をクリックし、ポップアップメニューから「 * 表示 * 」を選択することもできます。
2. 次のいずれかを実行します。

   - 検出されたストレージアレイへの接続を信頼する場合は、 * Next * （次へ）をクリックし、 * Yes * （はい）をクリックして確認し、ウィザードの次のダイアログに進みます。自己署名証明書は信頼済みとしてマークされ、ストレージアレイがプラグインに追加されます。
   - ストレージアレイへの接続を信頼しない場合は、「 * キャンセル」を選択し、各ストレージアレイの

セキュリティ証明書戦略を検証してから追加してください。

3. 「 * 次へ * 」をクリックして、ウィザードの次の手順に進みます。

手順 **3** ：パスワードを入力する

検出の最後の手順として、管理ドメインに追加するストレージアレイのパスワードを入力する必要があります。

1. 検出された各アレイの admin パスワードをフィールドに入力します。
2. [完了] をクリックします。

   指定したストレージアレイへの接続がシステムで確立されるまでに数分かかることがあります。処理が完了すると、ストレージアレイが管理ドメインに追加され、選択したグループ（指定されている場合）に関連付けられます。

プラグインでストレージをプロビジョニングします

ストレージをプロビジョニングするには、ボリュームを作成してホストにボリュームを割り当ててから、データストアにボリュームを割り当てます。

手順**1**：ボリュームを作成する

ボリュームは、ストレージアレイ上のストレージスペースを管理および編成するデータコンテナです。ストレージアレイで使用可能なストレージ容量からボリュームを作成すると、システムのリソースを整理するのに役立ちます。「ボリューム」という概念は、コンピュータ上のフォルダやディレクトリを使用してファイルにすばやくアクセスできるようにする方法に似ています。

ボリュームは、ホストから認識できる唯一のデータレイヤです。SAN 環境では、ボリュームは論理ユニット番号（ LUN ）にマッピングされます。これらの LUN は、ストレージアレイでサポートされている 1 つ以上のホストアクセスプロトコルを使用してアクセス可能なユーザデータを保持します。

手順

1. 管理ページで、ストレージアレイを選択します。
2. メニューを選択します。 Provisioning [ボリュームの管理] 。
3. メニューから「 Create [Volumes] 」を選択します。

   Select Host （ホストの選択）ダイアログボックスが表示されます。

4. ボリュームを割り当てるホストまたはホストクラスタをドロップダウンリストから選択するか、ホストまたはホストクラスタをあとで割り当てるように選択します。
5. 選択したホストまたはホストクラスタのボリューム作成手順を続行するには、 * Next * をクリックします。

   ワークロードの選択ダイアログボックスが表示されます。ワークロードには、ワークロードがサポートするアプリケーションのタイプに基づいて最適化された、特性が似たボリュームが含まれます。ワークロードを定義することも、既存のワークロードを選択することもできます。

6. 次のいずれかを実行します。

- 既存のワークロード用のボリュームの作成 * オプションを選択し、ドロップダウンリストからワークロードを選択します。
- [新しいワークロードの作成] オプションを選択して、サポートされているアプリケーションまたは「その他」のアプリケーションの新しいワークロードを定義し、次の手順に従います。
  i. ドロップダウンリストから、新しいワークロードを作成するアプリケーションの名前を選択します。このストレージアレイで使用するアプリケーションがリストにない場合は、「 Other 」エントリのいずれかを選択します。
  ii. 作成するワークロードの名前を入力します。

7. 「 * 次へ * 」をクリックします。ワークロードがサポート対象のアプリケーションタイプに関連付けられている場合は、要求された情報を入力します。それ以外の場合は、次の手順に進みます。

   Add/Edit Volumes （ボリュームの追加 / 編集）ダイアログボックスが表示されます。このダイアログでは、対応するプールまたはボリュームグループからボリュームを作成します。対象となる各プールおよびボリュームグループについて、使用可能なドライブの数と合計空き容量が表示されます。アプリケーション固有のワークロードがある場合、候補となる各プールまたはボリュームグループに、推奨されるボリューム構成に基づいて提示される容量が表示され、残りの空き容量が GiB 単位で表示されます。それ以外のワークロードの場合、プールまたはボリュームグループにボリュームを追加してレポート容量を指定した時点で容量が提示されます。

8. ボリュームの追加を開始する前に、次の表に示すガイドラインを確認してください。

フィールド	説明
空き容量	ボリュームはプールまたはボリュームグループから作成されるため、選択するプールまたはボリュームグループに十分な空き容量が必要です。
Data Assurance （ DA ）	DA 対応ボリュームを作成する場合は、使用するホスト接続で DA がサポートされている必要があります。 • DA対応ボリュームを作成する場合は、DAに対応したプールまたはボリュームグループを選択します（プールとボリュームグループの候補テーブルで「DA」の横にある「* Yes」を探します）。 • DA 機能はプールおよびボリュームグループのレベルで提供されます。DA 保護は、データがコントローラ経由でドライブに転送される際に発生する可能性があるエラーをチェックして修正します。新しいボリュームに DA 対応のプールまたはボリュームグループを選択すると、エラーがある場合には検出されて修正されます。 • ストレージアレイのコントローラで DA をサポートしていないホスト接続が使用されている場合、関連付けられているホストからは DA 対応ボリュームのデータにアクセスできません。

フィールド	説明
ドライブセキュリティ	セキュリティ有効ボリュームを作成するには、ストレージアレイのセキュリティキーを作成する必要があります。 • セキュリティ有効ボリュームを作成する場合は、セキュリティ対応のプールまたはボリュームグループを選択します（プールとボリュームグループの候補テーブルで、「セキュリティ対応」の横にある「はい」*を探します）。 • ドライブセキュリティ機能は、プールおよびボリュームグループのレベルで提供されます。セキュリティ対応ドライブを使用すると、ストレージアレイから物理的に取り外されたドライブ上のデータへの不正アクセスを防止できます。セキュリティ有効ドライブでは、一意の暗号化キーを使用して、書き込み時にデータが暗号化され、読み取り時に復号化されます。 • プールまたはボリュームグループにはセキュリティ対応とセキュリティ対応でないドライブの両方を含めることができますが、暗号化機能を使用するためにはすべてのドライブがセキュリティ対応である必要があります。
リソースのプロビジョニング	リソースプロビジョニングボリュームを作成するには、すべてのドライブが Deallocated or Unwritten Logical Block Error （ DULBE ）オプションを適用した NVMe ドライブである必要があります。

9. 前の手順で「その他」とアプリケーション固有のワークロードのどちらを選択したかに基づいて、次のいずれかの操作を実行します。

   - * その他 * - 1 つ以上のボリュームの作成に使用する各プールまたはボリュームグループで、 * 新しいボリュームの追加 * をクリックします。
   - * アプリケーション固有のワークロード * - 選択したワークロードについてシステムで推奨されるボリュームと特性を受け入れるには、 [次へ *] をクリックします。選択したワークロードに対してシステムで推奨されるボリュームと特性を変更、追加、または削除するには、 [ボリュームの編集] をクリックします。

     次のフィールドが表示されます。

フィールド	説明
ボリューム名	ボリュームには、作成時にデフォルトの名前が割り当てられます。デフォルトの名前をそのまま使用することも、ボリュームに格納されたデータのタイプを表した名前を指定することもできます。
レポート容量	新しいボリュームの容量と単位（ MiB 、 GiB 、または TiB ）を定義します。シックボリュームの場合、最小容量は 1MiB であり、最大容量はプールまたはボリュームグループ内のドライブの数と容量で決まります。プールの容量は 4GiB 単位で割り当てられます。4GiB の倍数でない容量を割り当てた場合、その容量は使用できません。全容量を使用できるようにするため、 4GiB 単位で容量を指定してください。使用不可容量が存在する場合、その容量を使用するにはボリュームの容量を増やすしかありません。

フィールド	説明
ボリュームタイプ	「アプリケーション固有のワークロード」を選択した場合は、「ボリュームタイプ」フィールドが表示されます。アプリケーション固有のワークロード用に作成されたボリュームのタイプを示します。
ボリュームのブロックサイズ（ EF300 および EF600 のみ）	ボリュームに対して作成できるブロックサイズが表示されます。 • 512 〜 512 バイト • 4K – 4 、 096 バイト
セグメントサイズ（ Segment Size ）	セグメントのサイジングに関する設定が表示されます。これは、ボリュームグループのボリュームについてのみ表示されます。セグメントサイズを変更することでパフォーマンスを最適化することができます。 • 許容される変更後のセグメントサイズ * –許容される変更後のセグメントサイズがシステムによって決定されます。現在のセグメントサイズの変更後のサイズとして適切でないものは、ドロップダウンリストに表示されません。通常、許容される変更後のサイズは、現在のセグメントサイズの倍または半分です。たとえば、ボリュームの現在のセグメントサイズが 32KiB であれば、ボリュームの新しいセグメントサイズとして 16KiB または 64KiB が許容されます。 • SSD キャッシュが有効なボリューム * – SSD キャッシュが有効なボリュームに対しては、セグメントサイズを 4KiB に指定することができます。4KiB のセグメントサイズを選択するのは、 SSD キャッシュが有効なボリュームで小さいブロックの I/O 処理を実行する（ I/O ブロックサイズが 16KiB 以下の場合など）場合のみにしてください。SSD キャッシュが有効なボリュームで大きいブロックのシーケンシャル処理を実行する場合は、セグメントサイズとして 4KiB を選択するとパフォーマンスが低下することがあります。 • セグメントサイズの変更にかかる時間 * –ボリュームのセグメントサイズの変更にかかる時間は、次の要因によって異なります。 ◦ ホストからの I/O 負荷 ◦ ボリュームの修正の優先順位 ◦ ボリュームグループ内のドライブの数 ◦ ドライブチャネルの数 ◦ ストレージアレイコントローラの処理能力 ボリュームのセグメントサイズを変更すると I/O パフォーマンスに影響しますが、データの可用性は維持されます。

フィールド	説明
セキュリティ対応	• 「 Secure Capable 」の横には、プールまたはボリュームグループ内のドライブが暗号化に対応している場合のみ「 SecureCapable 」と表示されます。ドライブセキュリティは、ストレージアレイから物理的に取り外されたドライブ上のデータへの不正アクセスを防止します。このオプションは、ドライブセキュリティ機能が有効になっていて、ストレージアレイのセキュリティキーが設定されている場合にのみ使用できます。プールまたはボリュームグループにはセキュリティ対応とセキュリティ対応でないドライブの両方を含めることができますが、暗号化機能を使用するためにはすべてのドライブがセキュリティ対応である必要があります。
ダ	* 「 DA 」の横には、プールまたはボリュームグループのドライブで Data Assurance （ DA ）がサポートされている場合にのみ「 Yes 」と表示されます。DA を使用すると、ストレージシステム全体のデータの整合性が向上します。DA を使用すると、データがコントローラ経由でドライブに転送される際にストレージアレイがエラーの有無をチェックできます。新しいボリュームに DA を使用すると、すべてのエラーが検出されます。

10. 選択したアプリケーションのボリューム作成手順を続行するには、 * 次へ * をクリックします。
11. 最後の手順で、作成するボリュームの概要を確認し、必要に応じて変更を加えます。変更するには、「 * 戻る」をクリックします。ボリューム構成に問題がなければ、「 * 完了 * 」をクリックします。

手順**2**：ホストアクセスを作成してボリュームを割り当てます

ホストは手動で作成できます。

- * 手動 * –ホストの手動作成中に、ホストポート識別子をリストから選択するか、手動で入力して関連付けます。ホストの作成後、ボリュームへのアクセスを共有する場合は、ボリュームをホストに割り当てたり、ホストクラスタに追加したりできます。

ホストを手動で作成する

作業を開始する前に

次のガイドラインを参照してください。

- 環境でストレージアレイを追加または検出しておく必要があります。
- ホストに関連付けられたホストポート識別子を定義する必要があります。
- ホストに割り当てられたシステム名と同じ名前を指定してください。
- 選択した名前がすでに使用されている場合、この処理は失敗します。
- 名前は 30 文字以内にする必要があります。

手順

1. Manage （管理）ページで、ホスト接続があるストレージアレイを選択します。
2. メニューを選択します。 Provisioning [ホストの設定] 。

   Configure Hosts ページが開きます。

3. メニュー： Create [Host] をクリックします。

Create Host （ホストの作成）ダイアログボックスが表示されます。

4. ホストの設定を必要に応じて選択します。

フィールド	説明
名前	新しいホストの名前を入力します。
ホストオペレーティングシステムのタイプ	新しいホストで実行しているオペレーティングシステムをドロップダウンリストから選択します。
ホストインターフェイスタイプ	（オプション）ストレージアレイで複数のタイプのホストインターフェイスがサポートされている場合、使用するホストインターフェイスタイプを選択します。
ホストポート	次のいずれかを実行します。 • * I/Oインターフェイスの選択*--通常'ホストポートはログインしており'ドロップダウン・リストから使用できるようになっている必要がありますリストからホストポート識別子を選択することができます。 • 手動追加--ホストポート識別子がリストに表示されない場合は'ホストポートがログインしていないことを意味しますHBA ユーティリティまたは iSCSI イニシエータユーティリティを使用して、ホストポート識別子を検索してホストに関連付けることができます。 ホストポート識別子を手動で入力するか、ユーティリティから（一度に 1 つずつ）ホストポートフィールドにコピーして貼り付けることができます。 ホストポート識別子は、一度に 1 つずつ選択してホストに関連付ける必要がありますが、ホストに関連付けられている識別子をいくつでも選択することができます。各識別子はホストポートフィールドに表示されます。必要に応じて、横の * X * を選択して識別子を削除することもできます。
CHAP イニシエータシークレットを設定する	（オプション）iSCSI IQNを使用してホストポートを選択または手動で入力した場合に、Challenge Handshake Authentication Protocol（CHAP）を使用して認証するためにストレージアレイへのアクセスを試みるホストが必要な場合は、* Set CHAP initiator secret *チェックボックスを選択します。選択または手動で入力した iSCSI ホストポートごとに、次の手順を実行します。 • CHAP 認証用に各 iSCSI ホストイニシエータに設定されたものと同じ CHAP シークレットを入力します。相互 CHAP 認証（ホストが自身をストレージアレイに対して検証し、ストレージアレイが自身をホストに対して検証できるようにする双方向認証）を使用する場合は、ストレージアレイの初期セットアップまたは設定変更時に CHAP シークレットも設定する必要があります。 • ホストの認証が不要な場合は、このフィールドを空白のままにします。 現在使用されている iSCSI 認証方式は CHAP だけです。

5. [作成（ Create ）] をクリックします。

6. ホスト情報を更新する必要がある場合は、表からホストを選択し、 * 表示 / 設定の編集 * をクリックします。

   ホストの作成が完了すると、ホストに設定されている各ホストポートのデフォルト名（ユーザラベル）が作成されます。デフォルトのエイリアスは「 <Hostname_Port number>` 」です。たとえば、ホスト IPT に対して最初に作成されたポートのデフォルトのエイリアスは「 ipt_1 」です。

7. 次に、ボリュームをホストまたはホストクラスタに割り当てて、 I/O 処理に使用できるようにする必要があります。メニューを選択します。 Provisioning [ホストの設定] 。

   Configure Hosts ページが開きます。

8. ボリュームを割り当てるホストまたはホストクラスタを選択し、 * ボリュームの割り当て * をクリックします。

   ダイアログボックスに割り当て可能なすべてのボリュームが表示されます。列をソートしたり、フィルタボックスに何かを入力したりすると、特定のボリュームを簡単に見つけることができます。

9. 割り当てる各ボリュームの横にあるチェックボックスを選択するか、テーブルヘッダーにあるチェックボックスを選択してすべてのボリュームを選択します。
10. [**Assign**] をクリックして、操作を完了します。

    システムは次の処理を実行します。

    - 割り当てられたボリュームに次に使用可能な LUN 番号が受信されます。ホストはこの LUN 番号を使用してボリュームにアクセスします。
    - ホストに関連付けられているボリュームの一覧にユーザが指定したボリューム名が表示されます。該当する場合、ホストに関連付けられているボリュームの一覧には、工場出荷時に設定されたアクセスボリュームも表示されます。

手順**3**：**vSphere Client**でデータストアを作成する

vSphere Clientでデータストアを作成するには、 "vSphere Client で VMFS データストアを作成します" VMwareドキュメントセンターのトピック。

ボリューム容量を増やして既存のデータストアの容量を増やします

プールまたはボリュームグループ内の使用可能な空き容量を使用して、ボリュームのレポート容量（ホストに報告される容量）を拡張できます。

作業を開始する前に

次の点を確認してください。

- ボリュームの関連付けられたプールまたはボリュームグループに十分な空き容量が必要です。
- ボリュームが最適状態で、変更中の状態ではありません。
- ボリュームでホットスペアドライブが使用されていない必要があります。（ボリュームグループ内のボリュームにのみ適用されます）。

ボリュームの容量の拡張は、特定のオペレーティングシステムでのみサポートされています。LUN 拡張をサポートしていないホストオペレーティングシステム上でボリューム容量を拡張した場合、拡張した容量は使用できず、元のボリューム容量をリストアすることもできません。

手順

1. vSphere Client でプラグインに移動します。
2. プラグインで、目的のストレージアレイを選択します。
3. [* プロビジョニング *] をクリックし、 [* ボリュームの管理 *] を選択します。
4. 容量を拡張するボリュームを選択し、 * 容量を拡張 * を選択します。

   容量の拡張の確認ダイアログボックスが表示されます。

5. 続行するには、 * はい * を選択します。

   レポート容量の拡張ダイアログボックスが表示されます。

   このダイアログボックスには、ボリュームの現在のレポート容量と、ボリュームの関連付けられたプールまたはボリュームグループ内で使用可能な空き容量が表示されます。

6. レポート容量の拡張に使用できるレポート容量を追加するには、 * ボックスを使用します。メビバイト（ MiB ）、ギビバイト（ GiB ）、またはテビバイト（ TiB ）のいずれかで表示するように容量の値を変更できます。
7. [* 拡大（ * ）] をクリックします
8. 選択したボリュームで現在実行されている容量の拡張処理の進捗状況については、 Recent Tasks ペインを表示します。この処理には時間がかかることがあり、システムのパフォーマンスに影響する可能性があります。
9. ボリューム容量が完了したら、の説明に従ってVMFSサイズを手動で拡張する必要があります。 "vSphere Client で VMFS データストアの容量を増やします" VMwareドキュメントセンターのトピック。

ボリュームを追加して既存のデータストアの容量を拡張してください

1. ボリュームを追加してデータストアの容量を増やすことができます。の手順に従います [手順1：ボリュームを作成する]。
2. 次に、ボリュームを目的のホストに割り当て、データストアの容量を増やします。

   を参照してください "vSphere Client で VMFS データストアの容量を増やします" 詳細については、VMwareドキュメントセンターのトピックを参照してください。

ステータスを表示します

システムステータスは、Storage Plugin for vCenterまたはvSphere Clientで確認できます。

1. vSphere Clientでプラグインを開きます。
2. 次のパネルからステータスを表示します。

- ストレージ・アレイのステータス--[* Manage-All*]パネルに移動します検出された各アレイについて、行にStatus列が表示されます。
- 操作が進行中--サイドパネルの*操作*をクリックすると、設定のインポートなど、長時間実行されているすべてのタスクが表示されます。Provisioningドロップダウンから、実行時間の長い処理を表示することもできます。[実行中の処理]ダイアログに表示された各処理について、完了率と処理が完了するまでの推定時間が表示されます。場合によっては、処理を停止したり、処理の優先度を変更したりできます。必要に応じて、[アクション（Actions）]列のリンクを使用して、オペレーションの優先度を停止または変更します。

特に、処理を停止する場合は、ダイアログボックスに表示されているすべての警告テキストをお読みください。

プラグインに対して表示される処理を次の表に示します。その他の処理は、System Managerインターフェイスに表示される場合もあります。

操作	処理のステータス	対処方法
ボリュームの作成（64TiBを超えるシックプールボリュームのみ）	実行中です	なし
ボリュームの削除（64TiBを超えるシックプールボリュームのみ）	実行中です	なし
プールまたはボリュームグループに容量を追加してください	実行中です	なし
ボリュームのRAIDレベルを変更します	実行中です	なし
プールの容量を削減します	実行中です	なし
プールボリュームのInstant Availability Format（IAF）処理の残り時間を確認します	実行中です	なし
ボリュームグループのデータ冗長性をチェックします	実行中です	なし
ボリュームを初期化	実行中です	なし
ボリュームの容量を拡張します	実行中です	なし
ボリュームのセグメントサイズを変更します	実行中です	なし

証明書を管理します

証明書の概要

vCenter向けストレージプラグインの証明書管理では、証明書署名要求（CSR）の作成、証明書のインポート、および既存の証明書の管理を行うことができます。

証明書とは何ですか？

証明書は、Webサイトやサーバなどのオンラインエンティティを識別するデジタルファイルで、インターネット上のセキュアな通信を実現します。これらのコマンドは、指定されたサーバとクライアント間でのみ、Web通信が非公開かつ変更されずに、暗号化された形式で送信されることを保証します。ストレージプラグインfor vCenterを使用すると、ホスト管理システムのブラウザおよび検出されたストレージアレイのコントローラの証明書を管理できます。

証明書には信頼できる認証局が署名した証明書と自己署名の証明書があります。「署名」とは、第三者が所有者のIDを検証し、そのデバイスが信頼できると判断したことを意味します。

ストレージアレイの各コントローラには、自動生成された自己署名証明書が付属しています。自己署名証明書を引き続き使用することも、CA署名証明書を取得してコントローラとホストシステム間のよりセキュアな接続を確立することもできます。

> CA署名証明書はセキュリティ保護を強化しますが（中間者攻撃を阻止するなど）、大規模なネットワークの場合はコストがかかる可能性があります。一方、自己署名証明書の方が安全性は低くなりますが、無料です。したがって、自己署名証明書は本番環境ではなく内部テスト環境で最もよく使用されます。

署名済み証明書

署名済み証明書は、信頼できる第三者機関である認証局（CA）によって検証されます。署名済み証明書には、エンティティ（通常、サーバまたはWebサイト）の所有者に関する詳細、証明書の問題 および有効期限、エンティティの有効なドメイン、およびアルファベットと数字で構成されるデジタル署名が含まれています。

ブラウザを開いてWebアドレスを入力すると、証明書チェックプロセスがバックグラウンドで実行され、有効なCA署名証明書を含むWebサイトに接続しているかどうかが確認されます。通常、署名済み証明書で保護されたサイトのアドレスには、鍵のアイコンとhttpsの指定が含まれています。CA署名証明書が含まれていないWebサイトに接続しようとすると、サイトがセキュアでないことを示す警告がブラウザに表示されます。

CAは、アプリケーションプロセス中に自分の身元を確認するための手順を実行します。登録済みの会社にEメールを送信し、会社の住所を確認して、HTTPまたはDNSの検証を実行する場合があります。アプリケーションプロセスが完了すると、ホスト管理システムにロードするデジタルファイルがCAから送信されます。通常、これらのファイルには次のような信頼チェーンが含まれます。

- ルート--階層の最上位にあるのはルート証明書です。この証明書には、他の証明書への署名に使用する秘密鍵が含まれています。ルートは特定のCA組織を識別します。すべてのネットワークデバイスで同じCAを使用する場合は、ルート証明書が1つだけ必要です。
- *Intermediate *--ルートからの分岐は中間証明書です。CAは、保護されたルート証明書とサーバ証明書の間の証明書として機能する、1つ以上の中間証明書を発行します。
- サーバー--チェーンの下部にあるサーバー証明書は、Webサイトやその他のデバイスなど、特定のエンティティを識別するサーバー証明書です。ストレージアレイの各コントローラには個別のサーバ証明書が必要です。

自己署名証明書

ストレージアレイの各コントローラには、自己署名証明書が事前にインストールされています。自己署名証明書はCA署名証明書と似ていますが、第三者ではなくエンティティの所有者によって検証される点が異なります。CA署名証明書と同様に、自己署名証明書には独自の秘密鍵が含まれており、サーバとクライアントの間のHTTPS接続を介してデータが暗号化および送信されることも保証されます。

自己署名証明書は、ブラウザでは「信頼」されません。自己署名証明書のみを含むWebサイトに接続しようとするたびに、ブラウザに警告メッセージが表示されます。Webサイトに進むには、警告メッセージ内のリンクをクリックする必要があります。これにより、基本的には自己署名証明書が受け入れられます。

管理証明書

プラグインを開くと、ブラウザはデジタル証明書を確認して、管理ホストが信頼できるソースであるかどうかを確認しようとします。ブラウザでCA署名証明書が見つからない場合は、警告メッセージが表示されます。そこからWebサイトにアクセスして、そのセッションの自己署名証明書を受け入れることができます。CAから署名入りのデジタル証明書を取得して、警告メッセージが表示されないようにすることもできます。

信頼された証明書

プラグインセッション中に、CA署名証明書のないコントローラにアクセスしようとすると、追加のセキュリティメッセージが表示されることがあります。この場合、自己署名証明書を永続的に信頼するか、コントローラのCA署名証明書をインポートして、プラグインがこれらのコントローラから受信するクライアント要求を認証できるようにすることができます。

CA署名証明書を使用する

Storage Plug-in for vCenterをホストしている管理システムへのセキュアなアクセスを確立するために、CA署名証明書を取得してインポートできます。

CA署名証明書の使用は、3つのステップで構成される手順 です。

- 手順1：CSRファイルを作成します。
- 手順2：CSRファイルを送信する。
- [手順3：管理証明書をインポートする]。

手順**1**：**CSR**ファイルを作成します

最初に証明書署名要求（CSR）ファイルを生成する必要があります。このファイルは、組織とプラグインが実行されているホストシステムを識別します。または、OpenSSLなどのツールを使用してCSRファイルを生成し、に進みます 手順2：CSRファイルを送信する。

手順

1. [証明書管理]を選択します。
2. [管理（**Management**）**]**タブで、**[** CSR全体*（* Complete CSR *）]を選択します。
3. 次の情報を入力し、[次へ*]をクリックします。
   - 組織--会社または組織の正式名称。Inc.やCorp.などの接尾辞も含めて入力してください
   - 組織単位（オプション）--証明書を処理している組織の部門。
   - 市区町村--ホストシステムまたは事業の所在地である市区町村。
   - 都道府県**(**オプション**)**--ホストシステムまたは事業の所在地である都道府県。
   - 国の**ISO**コード--自国を表す2桁のISO（国際標準化機構）コード（USなど）。
4. プラグインが実行されているホストシステムに関する次の情報を入力します。

- 共通名--プラグインが実行されているホストシステムのIPアドレスまたはDNS名。このアドレスが正しいことを確認してください。ブラウザでプラグインにアクセスするには、入力したアドレスと正確に一致している必要があります。http：//またはhttps：//を含めないでください。DNS名の先頭にワイルドカードを使用することはできません。
- 代替**IP**アドレス--共通名がIPアドレスの場合は'オプションでホストシステムの追加のIPアドレスまたはエイリアスを入力できます複数指定する場合は、カンマで区切って入力します。
- 代替**DNS**名--共通名がDNS名の場合は'ホストシステムの追加のDNS名を入力します複数指定する場合は、カンマで区切って入力します。代替DNS名がない場合は、最初のフィールドに入力したDNS名をここにコピーします。DNS名の先頭にワイルドカードを使用することはできません。

5. ホスト情報が正しいことを確認します。証明書が含まれていないと、CAから返された証明書をインポートしようとしたときに失敗します。
6. [完了] をクリックします。

手順**2**：**CSR**ファイルを送信する

Certificate Signing Request（CSR；証明書署名要求）ファイルを作成したら、生成されたCSRファイルをCAに送信して、プラグインをホストするシステムの署名付き管理証明書を受信します。

Eシリーズシステムには、署名済み証明書用のPEM形式（Base64 ASCIIエンコード）が必要です。これには、.pem、.crt、.cer、.keyのいずれかのファイルタイプが含まれます。

手順

1. ダウンロードしたCSRファイルの場所を確認します。

   ダウンロードフォルダの場所は、ブラウザによって異なります。

2. CSRファイルをCA（VerisignやDigiCertなど）に送信し、PEM形式の署名付き証明書を要求します。

   CSRファイルをCAに送信したあとは、別のCSRファイルを再生成しないでください。

CSRを生成すると、システムによって秘密鍵と公開鍵のペアが作成されます。公開鍵はCSRの一部であり、秘密鍵はシステムのキーストアに保持されます。署名済み証明書を受け取ってインポートすると、秘密鍵と公開鍵の両方が元のペアになります。キーが一致しないと署名済み証明書は機能せず、CAに新しい証明書を要求する必要があります。

手順**3**：管理証明書をインポートする

認証局（CA）から署名付き証明書を受け取ったら、プラグインがインストールされているホストシステムに証明書をインポートします。

作業を開始する前に

- CAから署名済み証明書を取得しておく必要があります。これらのファイルには、ルート証明書、1つ以上の中間証明書、およびサーバ証明書が含まれます。
- CAからチェーン証明書ファイル（たとえば、.p7bファイル）が提供された場合は、チェーンファイルを個々のファイル（ルート証明書、1つ以上の中間証明書、サーバ証明書）に展開する必要があります。Windows certmgrユーティリティーを使用してファイルを展開できます(右クリックしてメニューから[すべてのタスク][エクスポート]を選択します)。base-64エンコーディングが推奨されます。エクスポートが完了すると、チェーン内の証明書ファイルごとに1つのCERファイルが表示されます。

- 証明書ファイルは、プラグインが実行されているホストシステムにコピーする必要があります。

手順

1. [証明書管理]を選択します。
2. [管理（ Management）]タブで、[インポート（ Import）]を選択します。

   証明書ファイルをインポートするためのダイアログボックスが表示されます。

3. [**Browse**]をクリックして、最初にルート証明書ファイルと中間証明書ファイルを選択し、次にサーバ証明書を選択します。外部ツールからCSRを生成した場合は、CSRと一緒に作成された秘密鍵ファイルもインポートする必要があります。

   ファイル名がダイアログボックスに表示されます。

4. [* インポート *] をクリックします。

結果

ファイルがアップロードされて検証されます。証明書の情報は、証明書の管理ページに表示されます。

管理証明書をリセットします

vCenter向けストレージプラグインをホストしている管理システムでは、管理証明書を工場出荷時の自己署名証明書の状態に戻すことができます。

このタスクについて

このタスクでは、vCenter向けストレージプラグインを実行しているホストシステムから現在の管理証明書を削除します。証明書をリセットすると、ホストシステムでは自己署名証明書が再び使用されるようになります。

手順

1. [証明書管理]を選択します。
2. [管理（ Management）]タブで、[リセット（ Reset）]を選択します。

   管理証明書のリセットの確認ダイアログボックスが開きます。

3. フィールドにresetと入力し、* Reset *をクリックします。

   ブラウザをリフレッシュすると、デスティネーションサイトへのアクセスがブロックされ、サイトでHTTP Strict Transport Securityが使用されていると報告されることがあります。この状況は、自己署名証明書に切り替えると発生します。デスティネーションへのアクセスをブロックしている状態をクリアするには、ブラウザから参照データをクリアする必要があります。

結果

システムでサーバの自己署名証明書が再び使用されるようになります。そのため、セッションの自己署名証明書を手動で承認するように求められます。

アレイの証明書をインポートします

必要に応じて、ストレージアレイの証明書をインポートして、Storage Plug-in for vCenterをホストしているシステムで認証することができます。証明書には、認証局（CA）が署名した証明書と自己署名の証明書があります。

作業を開始する前に

信頼された証明書をインポートする場合は、System Managerを使用してストレージアレイのコントローラの証明書をインポートする必要があります。

手順

1. [証明書管理]を選択します。
2. [**Trusted**]タブを選択します。

   このページには、ストレージアレイについて報告されたすべての証明書が表示されます。

3. 次のいずれかのメニューを選択します。Import [Certificates] CA certificate or menu：Import [Self-Signed storage array certificates]。自己署名証明書をインポートします。
4. 表示を制限するには、[*次の証明書を表示…]フィルタリングフィールドを使用するか、いずれかの列見出しをクリックして証明書の行をソートします。
5. ダイアログボックスで証明書を選択し、*インポート*をクリックします。

   証明書がアップロードされて検証されます。

証明書を表示します

証明書を使用している組織、証明書を発行した機関、有効期間、フィンガープリント（一意の識別子）など、証明書の概要情報を表示できます。

手順

1. [証明書管理]を選択します。
2. 次のいずれかのタブを選択します。
   - **Management**--プラグインをホストしているシステムの証明書を表示します管理証明書には、自己署名の証明書と認証局（CA）によって承認された証明書があります。プラグインへのセキュアなアクセスを許可します。
   - *Trusted --プラグインがストレージアレイやLDAPサーバーなどの他のリモートサーバーにアクセスできる証明書を表示します認証局（CA）から発行された証明書と自己署名の証明書が含まれます。
3. 証明書の詳細を表示するには、その行を選択し、行の最後にある省略記号を選択して、*表示*または*エクスポート*をクリックします。

証明書をエクスポートします

証明書をエクスポートして詳細を確認することができます。

作業を開始する前に

エクスポートしたファイルを開くには、証明書ビューアアプリケーションが必要です。

手順

1. [証明書管理]を選択します。
2. 次のいずれかのタブを選択します。
   - **Management**--プラグインをホストしているシステムの証明書を表示します管理証明書には、自己署名の証明書と認証局（CA）によって承認された証明書があります。プラグインへのセキュアなアクセスを許可します。
   - *Trusted --プラグインがストレージアレイやLDAPサーバーなどの他のリモートサーバーにアクセスできる証明書を表示します認証局（CA）から発行された証明書と自己署名の証明書が含まれます。
3. 証明書をページから選択し、行の最後にある省略記号をクリックします。
4. [* Export*]をクリックし、証明書ファイルを保存します。
5. 証明書ビューアアプリケーションでファイルを開きます。

信頼された証明書を削除する

期限切れになった証明書など、不要になった証明書を削除することができます。

作業を開始する前に

古い証明書を削除する前に、新しい証明書をインポートしてください。

> ルート証明書または中間証明書を削除すると、同じ証明書ファイルが共有されている可能性があるため、複数のストレージアレイに影響する可能性があります。

手順

1. [証明書管理]を選択します。
2. [**Trusted**]タブを選択します。
3. テーブルで1つ以上の証明書を選択し、*削除*をクリックします。

   > 削除機能は、事前にインストールされている証明書では使用できません。

   [信頼された証明書の削除の確認]ダイアログボックスが開きます。

4. 削除を確認し、* Delete *をクリックします。

   証明書がテーブルから削除されます。

信頼されていない証明書を

証明書ページでは、信頼されていない証明書を解決するために、ストレージアレイから自己署名証明書をインポートするか、信頼できる第三者機関から発行された認証局（CA）証明書をインポートします。

作業を開始する前に

CA署名証明書をインポートする場合は、次の点を確認してください。

- ストレージアレイの各コントローラの証明書署名要求（.CSRファイル）を生成してCAに送信しておく必要があります。
- 信頼された証明書ファイルをCAから受け取っておきます。
- 証明書ファイルがローカルシステム上にある必要があります。

このタスクについて

信頼されていない証明書の問題は、ストレージアレイからプラグインへのセキュアな接続を確立しようとしたときに、接続がセキュアであることが確認できなかった場合に発生します。信頼された追加のCA証明書のインストールが必要になる可能性があるのは、次のいずれかに該当する場合です。

- ストレージアレイを新たに追加した。
- 一方または両方の証明書の期限が切れているか失効している。
- 一方または両方の証明書のルート証明書または中間証明書がない。

手順

1. [証明書管理]を選択します。
2. [**Trusted**]タブを選択します。

   このページには、ストレージアレイについて報告されたすべての証明書が表示されます。

3. 次のいずれかのメニューを選択します。Import [Certificates] CA certificate or menu：Import [Self-Signed storage array certificates]。自己署名証明書をインポートします。
4. 表示を制限するには、[*次の証明書を表示…]フィルタリングフィールドを使用するか、いずれかの列見出しをクリックして証明書の行をソートします。
5. ダイアログボックスで証明書を選択し、*インポート*をクリックします。

   証明書がアップロードされて検証されます。

アレイを管理します

アレイ管理の概要

アド/検出機能を使用して、vCenter向けStorageプラグインで管理対象のストレージアレイを検索および追加します。[管理]ページでは、これらの検出されたアレイの名前の変更、削除、および新しいパスワードの入力もできます。

アレイの検出に関する考慮事項

プラグインでストレージリソースを表示して管理するには、組織のネットワークで管理対象のストレージアレイを検出する必要があります。単一のアレイまたは複数のアレイを検出して追加できます。

複数のストレージアレイ

複数のアレイを検出する場合は、ネットワークIPアドレスの範囲を入力すると、その範囲の各IPアドレスへの

接続が個別に試行されます。接続に成功したストレージアレイがプラグインに表示され、管理ドメインに追加できます。

単一のストレージアレイです

単一のアレイを検出する場合は、ストレージアレイのいずれかのコントローラのIPアドレスを1つ入力してから、そのアレイを管理ドメインに追加します。

> プラグインは、コントローラに割り当てられた範囲内の単一のIPアドレスまたはIPアドレスのみを検出して表示します。これらのコントローラに割り当てられている代替コントローラまたはIPアドレスが、この1つのIPアドレスまたはIPアドレス範囲外の場合、プラグインはそれらを検出または表示しません。ただし、ストレージアレイを追加すると、関連付けられているすべてのIPアドレスが検出され、管理ビューに表示されます。

ユーザクレデンシャル

追加する各ストレージアレイの管理者パスワードを指定する必要があります。

証明書

検出プロセスでは、検出されたストレージアレイに信頼できるソースからの証明書があるかどうかが確認されます。システムは、ブラウザでとの接続を確立するすべての接続に対して、2種類の証明書ベースの認証を使用します。

- 信頼された証明書--一方または両方のコントローラ証明書の有効期限が切れた場合、失効した場合、またはチェーン内に証明書がない場合は、認証局が提供する信頼された証明書を追加でインストールする必要があります。
- 自己署名証明書--アレイは自己署名証明書を使用することもできます署名済み証明書をインポートせずにアレイを検出しようとすると、プラグインに自己署名証明書を受け入れるための追加の手順が表示されます。自己署名証明書が信頼済みとしてマークされ、ストレージアレイがプラグインに追加されます。ストレージアレイへの接続を信頼しない場合は、ストレージアレイをプラグインに追加する前に* Cancel *を選択し、ストレージアレイのセキュリティ証明書戦略を検証します。

ストレージアレイのステータス

vCenter向けストレージプラグインを開くと、各ストレージアレイとの通信が確立され、各ストレージアレイのステータスが表示されます。

Manage-All *ページでは、ストレージアレイのステータスおよびストレージアレイ接続のステータスを表示できます。

ステータス	を示します
最適	ストレージアレイが最適な状態です。証明書の問題はなく、パスワードが有効です。
パスワードが無効です	無効なストレージアレイパスワードが指定されました。
信頼できない証明書です	HTTPS証明書が自己署名証明書でインポートされていないか、CA署名証明書でルート証明書と中間CA証明書がインポートされていないため、ストレージアレイとの1つ以上の接続が信頼されていません。

ステータス	を示します
要注意	ストレージアレイにユーザによる修正操作が必要な問題があります。
ロックダウン	ストレージアレイがロックダウン状態です。
不明です	ストレージアレイに一度も接続していません。この状況は、プラグインが起動中でまだストレージアレイに接続していない場合や、ストレージアレイがオフラインでプラグインの起動後に一度も接続されていない場合に発生することがあります。
オフラインです	プラグインは以前にストレージアレイに接続しましたが、現在はすべての接続が失われています。

プラグインインターフェイスと**System Manager**の比較

ストレージアレイの基本的な操作にはStorage Plugin for vCenterを使用できますが、プラグインで使用できないタスクを実行するためにSystem Managerの起動が必要になる場合があります。

System Managerは、ストレージアレイのコントローラに組み込まれたアプリケーションであり、イーサネット管理ポートを介してネットワークに接続されます。System Managerにはアレイベースのすべての機能が含まれています。

次の表は、プラグインインターフェイスとSystem Managerインターフェイスのどちらを使用できるかをストレージアレイの特定のタスクで判断する際に役立ちます。

機能	プラグインインターフェイス	**System Manager**インターフェイス
複数のストレージアレイのグループに対するバッチ処理	はい。	いいえ処理は1つのアレイに対して実行されます。
SANtricity OSファームウェアのアップグレード	はい。バッチ処理内の1つ以上のアレイ。	はい。シングルアレイのみ。
1つのアレイから複数のアレイに設定をインポートします	はい。	いいえ
ホストとホストクラスタの管理（ボリュームの作成、割り当て、更新、削除）	はい。	はい。
プールとボリュームグループの管理（作成、更新、セキュリティの有効化、削除）	はい。	はい。
ボリュームの管理（作成、サイズ変更、更新、削除）	はい。	はい。
SSDキャッシュの管理（作成、更新、削除）	はい。	はい。
ミラーリングとSnapshotの管理	いいえ	はい。

機能	プラグインインターフェイス	**System Manager**インターフェイス
ハードウェア管理（コントローラステータスの表示、ポート接続の設定、コントローラのオフライン化、ホットスペアの有効化、ドライブの消去、 など）	いいえ	はい。
アラートの管理（Eメール、SNMP、syslog）	いいえ	はい。
セキュリティキーの管理	いいえ	はい。
コントローラの証明書管理	いいえ	はい。
コントローラのアクセス管理（LDAP、SAMLなど）	いいえ	はい。
AutoSupport 管理	いいえ	はい。

ストレージアレイを検出

vCenter向けストレージプラグインでストレージリソースを表示および管理するには、ネットワーク内のアレイのIPアドレスを検出する必要があります。

作業を開始する前に

- アレイコントローラのネットワーク IP アドレス（またはアドレスの範囲）を確認しておく必要があります。
- ストレージアレイが正しくセットアップおよび設定されている必要があります。
- ストレージアレイのパスワードは、System Managerのアクセス管理タイルを使用して設定する必要があります。

このタスクについて

アレイの検出は複数の手順からなる手順 です。

- 手順 1 ：検出するネットワークアドレスを入力します
- 手順 2 ：検出時に信頼されていない証明書を解決する
- 手順 3 ：パスワードを入力する

手順 **1** ：検出するネットワークアドレスを入力します

ストレージアレイを検出する最初の手順として、ローカルサブネットワーク全体を検索するための単一のIPアドレスまたはIPアドレス範囲を入力します。追加/検出機能を使用すると、検出プロセスをガイドするウィザードが開きます。

手順

1. [* Manage （管理）**]**ページで、**[** Add/Discover*（追加/検出*）]を選択します。

   [Enter Network Address Range] ダイアログボックスが表示されます。

2. 次のいずれかを実行します。
    - 1 つのアレイを検出するには、 * 単一のストレージアレイの検出 * オプションボタンを選択し、ストレージアレイのいずれかのコントローラの IP アドレスを入力します。
    - 複数のストレージアレイを検出するには、「ネットワーク範囲内のすべてのストレージアレイを検出」ラジオボタンを選択し、開始ネットワークアドレスと終了ネットワークアドレスを入力してローカルサブネットワーク全体を検索します。
3. [検出の開始] をクリックします。

    検出プロセスが開始されると、ストレージアレイが検出されるときにダイアログボックスに表示されます。検出プロセスが完了するまでに数分かかることがあります。

    > 管理可能なアレイが検出されない場合は、ストレージアレイがネットワークに適切に接続されていて、割り当てられたアドレスが範囲内にあることを確認してください。[新規検出パラメータ *] をクリックして、 [追加 / 検出] ページに戻ります。

4. 管理ドメインに追加するストレージアレイの横にあるチェックボックスをオンにします。

    管理ドメインに追加する各アレイについて、クレデンシャルのチェックが実行されます。信頼されていない証明書に関する問題の解決が必要になる場合があります。

5. 「 * 次へ * 」をクリックして、ウィザードの次の手順に進みます。
6. ストレージアレイに有効な証明書がある場合は、に進みます 手順 3 ：パスワードを入力する。有効な証明書がないストレージアレイがある場合は、自己署名証明書の解決ダイアログボックスが表示されます。に進みます 手順 2 ：検出時に信頼されていない証明書を解決する。CA署名証明書をインポートする場合は、検出ダイアログをキャンセルしてに進みます "アレイの証明書をインポートします"。

手順 **2** ：検出時に信頼されていない証明書を解決する

必要に応じて、証明書の問題を解決してから検出プロセスを開始する必要があります。

検出時に「信頼されていない証明書」のステータスが表示されるストレージアレイがある場合は、自己署名証明書の解決ダイアログボックスが表示されます。このダイアログで信頼されていない証明書を解決するか、CA証明書をインポートできます（を参照） "アレイの証明書をインポートします"）。

手順

1. [自己署名証明書の解決] ダイアログボックスが開いた場合は、信頼されていない証明書について表示される情報を確認します。詳細については、表の右端にある省略記号をクリックし、ポップアップメニューから「 * 表示 * 」を選択することもできます。
2. 次のいずれかを実行します。
    - 検出されたストレージアレイへの接続を信頼する場合は、* Next （次へ）をクリックし、 Yes *（はい）をクリックして確認し、ウィザードの次のカードに進みます。自己署名証明書は信頼済みとしてマークされ、ストレージアレイがプラグインに追加されます。
    - ストレージアレイへの接続を信頼しない場合は、キャンセル*を選択し、各ストレージアレイのセキュリティ証明書戦略を検証してからプラグインに追加してください。

手順 **3** ：パスワードを入力する

検出の最後の手順として、管理ドメインに追加するストレージアレイのパスワードを入力する必要がありま

す。

手順

1. 必要に応じて、アレイのグループを設定済みの場合、ドロップダウンを使用して検出されたアレイのグループを選択できます。
2. 検出された各アレイの admin パスワードをフィールドに入力します。
3. [完了] をクリックします。

> 指定したストレージアレイへの接続がシステムで確立されるまでに数分かかることがあります。

結果

ストレージアレイが管理ドメインに追加され、指定した場合は選択したグループに関連付けられます。

> 管理操作を実行する場合は、起動オプションを使用して、1つ以上のストレージアレイのブラウザベースのSystem Managerを開くことができます。

ストレージアレイの名前を変更します

Storage Plugin for vCenterの［管理］ページに表示されるストレージアレイの名前を変更できます。

手順

1. Manage *ページで、ストレージ・アレイ名の左にあるチェックボックスを選択します。
2. 行の右端にある省略記号を選択し、ポップアップ・メニューから*ストレージ・アレイ名の変更*を選択します。
3. 新しい名前を入力し、*保存*をクリックします。

ストレージアレイのパスワードを変更する

vCenter向けストレージプラグインでストレージアレイの表示とアクセスに使用するパスワードを更新できます。

作業を開始する前に

System Managerで設定されているストレージアレイの現在のパスワードを確認しておく必要があります。

このタスクについて

このタスクでは、プラグインでストレージアレイにアクセスできるようにストレージアレイの現在のパスワードを入力します。これは、System Managerでアレイのパスワードが変更された場合に必要になることがあります。

手順

1. [* Manage *（管理）]ページで、1つ以上のストレージ・アレイを選択します。
2. [メニュー]：[一般的でないタスク][ストレージアレイのパスワードの入力]を選択します。
3. 各ストレージアレイのパスワードを入力し、*保存*をクリックします。

ストレージアレイを削除します

ストレージプラグインfor vCenterでストレージアレイを管理する必要がなくなった場合は、削除することができます。

このタスクについて

削除すると、そのストレージアレイにはアクセスできなくなります。ただし、ブラウザでIPアドレスまたはホスト名を直接指定すれば、削除したストレージアレイへの接続を確立できます。

ストレージアレイを削除しても、ストレージアレイ自体やそのデータには影響はありません。ストレージアレイを誤って削除した場合は、再度追加することができます。

手順

1. [* Manage *（管理）]ページで、削除する1つ以上のストレージ・アレイを選択します。
2. メニューを選択します。一般的でないタスク[ストレージアレイの削除]。

   ストレージアレイがプラグインインターフェイスのすべてのビューから削除されます。

System Manager を起動します

単一のアレイを管理するには、起動オプションを使用して、新しいブラウザウィンドウでSANtricity System Managerを開きます。

System Managerは、ストレージアレイのコントローラに組み込まれたアプリケーションであり、イーサネット管理ポートを介してネットワークに接続されます。System Managerにはアレイベースのすべての機能が含まれています。System Managerにアクセスするには、Webブラウザを使用してネットワーク管理クライアントにアウトオブバンド接続する必要があります。

手順

1. [* Manage *（管理）]ページで、管理する1つ以上のストレージ・アレイを選択します。
2. [* 起動 *] をクリックします。

   ブラウザに新しいタブが開き、System Managerのログインページが表示されます。

3. ユーザー名とパスワードを入力し、*ログイン*をクリックします。

設定をインポートします

設定のインポートの概要

設定のインポート機能は、vCenter向けストレージプラグインの1つのストレージアレイ（ソース）の設定を複数のアレイ（ターゲット）にレプリケートするためのバッチ処理です。

インポートできる設定

アレイ間でインポートできる構成は次のとおりです。

- アラート--電子メール、syslogサーバ、またはSNMPサーバを使用して管理者に重要なイベントを送信するアラート方法。
- * AutoSupport *--ストレージ・アレイの状態を監視し’テクニカル・サポートに自動ディスパッチを送信する機能
- ディレクトリサービス-- LDAP (Lightweight Directory Access Protocol)サーバとディレクトリサービス(MicrosoftのActive Directoryなど)を介して管理されるユーザー認証の方法。
- システム設定--以下に関連する設定。
  - ボリュームのメディアスキャン設定
  - SSD設定
  - 自動ロードバランシング（ホスト接続レポートは含まれません）
- ストレージ構成--以下に関連する構成。
  - ボリューム（リポジトリボリュームでないシックボリュームのみ）
  - ボリュームグループとプール
  - ホットスペアドライブの割り当て

設定ワークフロー

設定をインポートするワークフローは次のとおりです。

1. ソースとして使用するストレージアレイで、System Managerを使用して設定を行います。
2. ターゲットとして使用するストレージアレイで、System Managerを使用して設定をバックアップします。
3. プラグイン・インターフェイスから* Manage *ページに移動し、設定をインポートします。
4. [操作]ページで、[設定のインポート]操作の結果を確認します。

ストレージ構成のレプリケートに関する要件

ストレージアレイ間でストレージ構成をインポートする前に、要件およびガイドラインを確認してください。

シェルフ

- コントローラが配置されているシェルフがソースとターゲットのアレイで同一である。
- シェルフIDがソースとターゲットのアレイで同じである。
- 拡張シェルフの同一のスロットに同じドライブタイプが搭載されている必要があります（ドライブが構成で使用されている場合、未使用ドライブの場所は問題になりません）。

コントローラ

- コントローラタイプはソースアレイとターゲットアレイで同一である必要がありますが、RBODエンクロージャのタイプは同一である必要があります。
- ホストのDA機能を含むHICが、ソースとターゲットのアレイで同じである必要があります。
- デュプレックス構成からシンプレックス構成へのインポートはサポートされていませんが、シンプレックス構成からデュプレックス構成へのインポートは可能です。

- FDE設定はインポートプロセスに含まれない。

ステータス

- ターゲットアレイのステータスが最適Iである必要があります。
- ソースアレイのステータスが「最適」である必要はありません。

ストレージ

- ターゲットのボリューム容量がソースよりも大きいかぎり、ソースとターゲットのアレイでドライブ容量が異なることがあります。（ターゲットアレイには容量の大きい新しいドライブが搭載されている場合、それらのドライブはレプリケーション処理によってボリュームに完全には構成されない可能性があります）。
- ソースアレイのディスクプールのボリュームが64TB以上の場合、ターゲットでインポートプロセスを実行できない。

アラート設定をインポートします

ストレージアレイから別のストレージアレイにアラート設定をインポートできます。このバッチ処理により、ネットワーク内に複数のアレイを設定する必要がある場合に時間を節約できます。

作業を開始する前に

次の点を確認してください。

- アラートは、ソースとして使用するストレージアレイのSystem Manager（メニュー：Settings [Alerts]）で設定します。
- ターゲットストレージアレイの既存の構成は、System Managerでバックアップされます（メニュー：[設定][システム]>[ストレージアレイ構成の保存]）。
- でストレージ構成のレプリケートに関する要件を確認しておく必要があります "設定のインポートの概要"。

このタスクについて

インポート処理では、Eメール、SNMP、またはsyslogのいずれかのアラートを選択できます。

- *Email alerts *--メールサーバのアドレスとアラート受信者の電子メールアドレス。
- **Syslog**アラート-- syslogサーバのアドレスとUDPポート。
- *snmp alerts *-- SNMPサーバのコミュニティ名とIPアドレス。

手順

1. [管理]ページで、[メニュー]、[アクション]、[設定のインポート]の順にクリックします。

   設定のインポートウィザードが開きます。

2. Select Settings（設定の選択）ダイアログで、* Email alerts 、 SNMP alerts 、または Syslog alerts のいずれかを選択し、 Next（次へ）*をクリックします。

   ソースアレイを選択するためのダイアログボックスが開きます。

3. [ソースの選択]ダイアログで、インポートする設定のアレイを選択し、[次へ]をクリックします。
4. ターゲットの選択ダイアログで'新しい設定を受信する1つまたは複数のアレイを選択します

> ファームウェアが8.50未満のストレージアレイは選択できません。また、プラグインがそのアレイと通信できない場合（オフラインの場合や、証明書、パスワード、ネットワークに問題がある場合など）、このダイアログにアレイは表示されません。

5. [完了] をクリックします。

   Operationsページには、インポート処理の結果が表示されます。処理が失敗した場合は、その行をクリックすると詳細を確認できます。

結果

Eメール、SNMP、またはsyslogを使用して管理者にアラートを送信するようにターゲットストレージアレイが設定されます。

AutoSupport 設定をインポートします

ストレージアレイから別のストレージアレイにAutoSupport 構成をインポートできます。このバッチ処理により、ネットワーク内に複数のアレイを設定する必要がある場合に時間を節約できます。

作業を開始する前に

次の点を確認してください。

- AutoSupport は、ソースとして使用するストレージアレイのSystem Manager（メニュー：サポート[サポートセンター]）で設定します。
- ターゲットストレージアレイの既存の構成は、System Managerでバックアップされます（メニュー：[設定][システム]>[ストレージアレイ構成の保存]）。
- でストレージ構成のレプリケートに関する要件を確認しておく必要があります "設定のインポートの概要"。

このタスクについて

インポートされる設定には、個別の機能（Basic AutoSupport 、AutoSupport OnDemand、Remote Diagnostics）、メンテナンス期間、配信方法、 およびディスパッチスケジュール。

手順

1. [管理]ページで、[メニュー]、[アクション]、[設定のインポート]の順にクリックします。

   設定のインポートウィザードが開きます。

2. 設定の選択ダイアログで、* AutoSupport *を選択し、*次へ*をクリックします。

   ソースアレイを選択するためのダイアログボックスが開きます。

3. [ソースの選択]ダイアログで、インポートする設定のアレイを選択し、[次へ]をクリックします。
4. ターゲットの選択ダイアログで'新しい設定を受信する1つまたは複数のアレイを選択します

ファームウェアが8.50未満のストレージアレイは選択できません。また、プラグインがそのアレイと通信できない場合（オフラインの場合や、証明書、パスワード、ネットワークに問題がある場合など）、このダイアログにアレイは表示されません。

5. [完了] をクリックします。

   Operationsページには、インポート処理の結果が表示されます。処理が失敗した場合は、その行をクリックすると詳細を確認できます。

結果

ターゲットストレージアレイのAutoSupport 設定がソースアレイと同じに設定されます。

ディレクトリサービス設定をインポートします

ストレージアレイから別のストレージアレイにディレクトリサービス設定をインポートできます。このバッチ処理により、ネットワーク内に複数のアレイを設定する必要がある場合に時間を節約できます。

作業を開始する前に

次の点を確認してください。

- ディレクトリサービスは、ソースとして使用するストレージアレイのSystem Manager（メニュー：設定[Access Management]）で設定します。
- ターゲットストレージアレイの既存の構成は、System Managerでバックアップされます（メニュー：[設定][システム]>[ストレージアレイ構成の保存]）。
- でストレージ構成のレプリケートに関する要件を確認しておく必要があります "設定のインポートの概要"。

このタスクについて

インポートされる設定には、LDAP（Lightweight Directory Access Protocol）サーバのドメイン名とURL、およびLDAPサーバのユーザグループとストレージアレイの事前定義されたロールとのマッピングが含まれます。

手順

1. [管理]ページで、[メニュー]、[アクション]、[設定のインポート]の順にクリックします。

   設定のインポートウィザードが開きます。

2. 設定の選択ダイアログで、*ディレクトリサービス*を選択し、*次へ*をクリックします。

   ソースアレイを選択するためのダイアログボックスが開きます。

3. [ソースの選択]ダイアログで、インポートする設定のアレイを選択し、[次へ]をクリックします。
4. ターゲットの選択ダイアログで'新しい設定を受信する1つまたは複数のアレイを選択します

ファームウェアが8.50未満のストレージアレイは選択できません。また、プラグインがそのアレイと通信できない場合（オフラインの場合や、証明書、パスワード、ネットワークに問題がある場合など）、このダイアログにアレイは表示されません。

5. [完了] をクリックします。

   Operationsページには、インポート処理の結果が表示されます。処理が失敗した場合は、その行をクリックすると詳細を確認できます。

結果

ターゲットストレージアレイのディレクトリサービスがソースアレイと同じに設定されます。

システム設定をインポートします

ストレージアレイから別のストレージアレイにシステム設定をインポートできます。このバッチ処理により、ネットワーク内に複数のアレイを設定する必要がある場合に時間を節約できます。

作業を開始する前に

次の点を確認してください。

- ソースとして使用するストレージアレイのシステム設定をSystem Managerで設定しておきます。
- ターゲットストレージアレイの既存の構成は、System Managerでバックアップされます（メニュー：[設定][システム]>[ストレージアレイ構成の保存]）。
- でストレージ構成のレプリケートに関する要件を確認しておく必要があります "設定のインポートの概要"。

このタスクについて

インポートされる設定には、ボリュームのメディアスキャン設定、コントローラのSSD設定、および自動ロードバランシングが含まれます（ホスト接続レポートは含まれません）。

手順

1. [管理]ページで、[メニュー]、[アクション]、[設定のインポート]の順にクリックします。

   設定のインポートウィザードが開きます。

2. 設定の選択ダイアログで、*システム*を選択し、*次へ*をクリックします。

   ソースアレイを選択するためのダイアログボックスが開きます。

3. [ソースの選択]ダイアログで、インポートする設定のアレイを選択し、[次へ]をクリックします。
4. ターゲットの選択ダイアログで'新しい設定を受信する1つまたは複数のアレイを選択します

ファームウェアが8.50未満のストレージアレイは選択できません。また、プラグインがそのアレイと通信できない場合（オフラインの場合や、証明書、パスワード、ネットワークに問題がある場合など）、このダイアログにアレイは表示されません。

5. [完了] をクリックします。

   Operationsページには、インポート処理の結果が表示されます。処理が失敗した場合は、その行をクリックすると詳細を確認できます。

結果

ターゲットストレージアレイのシステム設定がソースアレイと同じに設定されます。

ストレージ構成の設定をインポートします

ストレージアレイから別のストレージアレイにストレージ構成をインポートできます。このバッチ処理により、ネットワーク内に複数のアレイを設定する必要がある場合に時間を節約できます。

作業を開始する前に

次の点を確認してください。

- ソースとして使用するストレージアレイのストレージをSystem Managerで設定しておきます。
- ターゲットストレージアレイの既存の構成は、System Managerでバックアップされます（メニュー：[設定][システム]>[ストレージアレイ構成の保存]）。
- でストレージ構成のレプリケートに関する要件を確認しておく必要があります "設定のインポートの概要"。
- ソースアレイとターゲットアレイが次の要件を満たしている必要があります。
  - コントローラが配置されているシェルフが同じである必要があります。
  - シェルフIDが同じである必要があります。
  - 拡張シェルフの同一のスロットに同じドライブタイプが搭載されている。
  - RBODエンクロージャタイプが同一である。
  - HICが、ホストのData Assurance機能を含めて同一である。
  - ターゲットアレイのステータスが最適Iである必要があります。
  - ターゲットアレイのボリューム容量がソースアレイよりも大きい。
- 次の制限事項を理解しておきます。
  - デュプレックス構成からシンプレックス構成へのインポートはサポートされていませんが、シンプレックス構成からデュプレックス構成へのインポートは可能です。
  - ソースアレイのディスクプールのボリュームが64TB以上の場合、ターゲットでインポートプロセスを実行できない。

このタスクについて

インポートされる設定には、設定済みのボリューム（リポジトリボリュームでないシックボリュームのみ）、ボリュームグループ、プール、およびホットスペアドライブの割り当てが含まれます。

手順

1. [管理]ページで、[メニュー]、[アクション]、[設定のインポート]の順にクリックします。

設定のインポートウィザードが開きます。

2. 設定の選択ダイアログで、*ストレージ構成*を選択し、*次へ*をクリックします。

   ソースアレイを選択するためのダイアログボックスが開きます。

3. [ソースの選択]ダイアログで、インポートする設定のアレイを選択し、[次へ]をクリックします。
4. ターゲットの選択ダイアログで'新しい設定を受信する1つまたは複数のアレイを選択します

   ファームウェアが8.50未満のストレージアレイは選択できません。また、プラグインがそのアレイと通信できない場合（オフラインの場合や、証明書、パスワード、ネットワークに問題がある場合など）、このダイアログにアレイは表示されません。

5. [完了] をクリックします。

   Operationsページには、インポート処理の結果が表示されます。処理が失敗した場合は、その行をクリックすると詳細を確認できます。

結果

ターゲットストレージアレイのストレージ構成がソースアレイと同じに設定されます。

アレイグループを管理します

アレイグループの概要

ストレージプラグインfor vCenterでは、一連のストレージアレイをグループ化して物理インフラや仮想インフラを管理することができます。ストレージアレイをグループ化すると、ジョブの監視やレポートが簡単になります。

ストレージアレイグループのタイプ：

- すべてのグループ--すべてのグループがデフォルトのグループで、組織内で検出されたすべてのストレージアレイが含まれます。Allグループには、メインビューからアクセスできます。
- ユーザーが作成したグループ--ユーザーが作成したグループには'手動で選択してそのグループに追加するストレージアレイが含まれますユーザが作成したグループには、メインビューからアクセスできます。

ストレージアレイグループを作成します

ストレージグループを作成し、そのグループにストレージアレイを追加します。ストレージグループでは、ボリュームを構成するストレージをどのドライブから提供するかを定義します。

- 手順 *
  1. 管理ページで、メニューからグループの管理[ストレージアレイグループの作成]を選択します。
  2. [名前]フィールドに、新しいグループの名前を入力します。
  3. 新しいグループに追加するストレージアレイを選択します。

4. [作成（ Create ）] をクリックします。

ストレージアレイをグループに追加します

ユーザが作成したグループにストレージアレイを追加することができます。

- 手順 *
  1. メインビューで、* Manage *を選択し、ストレージ・アレイを追加するグループを選択します。
  2. 選択メニュー：グループの管理[グループへのストレージアレイの追加]。
  3. グループに追加するストレージアレイを選択します。
  4. [追加（ Add ）] をクリックします。

ストレージアレイグループの名前を変更します

現在の名前が適切でない場合は、ストレージアレイグループの名前を変更できます。

このタスクについて

これらのガイドラインに注意してください。

- 名前には、アルファベット、数字、アンダースコア（_）、ハイフン（-）、シャープ（#）を使用できます。他の文字を選択すると、エラーメッセージが表示されます。別の名前を選択するように求められます。
- 名前は30文字以内にしてください。名前の先頭と末尾のスペースはすべて削除されます。
- わかりやすい一意の名前を使用してください。
- わかりにくい名前は使用しないでください。

手順

1. メインビューで* Manage *を選択し、名前を変更するストレージ・アレイ・グループを選択します。
2. メニューを選択します。Manage Groups [Rename storage array group]（グループの名前変更）。
3. ［グループ名］フィールドに、グループの新しい名前を入力します。
4. [名前の変更 *] をクリックします。

グループからストレージアレイを削除します

管理対象のストレージアレイを特定のストレージグループで管理する必要がなくなった場合は、それらのストレージアレイをグループから削除することができます。

このタスクについて

グループからストレージアレイを削除しても、ストレージアレイ自体やそのデータには影響はありません。ストレージアレイをSystem Managerで管理している場合は、引き続きブラウザを使用して管理できます。ストレージアレイをグループから誤って削除した場合は、再度追加することができます。

手順

1. 管理ページで、メニュー：グループの管理[グループからストレージアレイを削除]を選択します。

2. 削除するストレージアレイが含まれているグループをドロップダウンから選択し、グループから削除する各ストレージアレイの横にあるチェックボックスをクリックします。
3. [削除（ Remove ）] をクリックします。

ストレージアレイグループを削除します

不要になった1つ以上のストレージアレイグループを削除することができます。

このタスクについて

この処理で削除されるのは、ストレージアレイグループだけです。削除したグループに関連付けられているストレージアレイには、Manage Allビューまたはそれに関連付けられているその他のグループからアクセスできます。

手順

1. 管理ページで、メニューからグループの管理[ストレージアレイグループの削除]を選択します。
2. 削除するストレージアレイグループを1つ以上選択します。
3. [削除（ Delete ）] をクリックします。

OSソフトウェアをアップグレードします

アップグレードの概要

vCenter向けストレージプラグインでは、同じタイプの複数のストレージアレイのSANtricity ソフトウェアとNVSRAMのアップグレードを管理できます。

アップグレードワークフロー

以下に、ソフトウェアのアップグレードを実行するための大まかなワークフローを示します。

1. 最新のSANtricity OSファイルをサポートサイトからダウンロードします（リンクはサポートページから入手できます）。管理ホストシステム（ブラウザでプラグインにアクセスするホスト）にファイルを保存し、ファイルを解凍します。
2. プラグインでは、SANtricity OSソフトウェアファイルとNVSRAMファイルをリポジトリ（ファイルが格納されているサーバの領域）にロードできます。
3. リポジトリにファイルをロードしたら、アップグレードに使用するファイルを選択できます。SANtricity OSソフトウェアのアップグレードページで、OSソフトウェアファイルとNVSRAMファイルを選択します。ソフトウェアファイルを選択すると、互換性があるストレージアレイのリストがこのページに表示されます。次に、新しいソフトウェアでアップグレードするストレージアレイを選択します。（互換性のないアレイは選択できません）。
4. ソフトウェアの転送とアクティブ化をすぐに開始することも、ファイルをステージングしてあとでアクティブ化することもできます。アップグレードプロセス中に、プラグインは次のタスクを実行します。
    - ストレージアレイの健全性チェックが実行され、アップグレードの完了の妨げとなる状況がないかどうかが確認されます。健全性チェックでいずれかのアレイに問題が見つかった場合は、そのアレイをスキップして他のアレイのアップグレードを続行するか、プロセス全体を停止して該当するアレイのトラブルシューティングを行うことができます。

- 各コントローラにアップグレードファイルが転送されます。
- コントローラが一度に1台ずつリブートされ、新しいOSソフトウェアがアクティブ化されます。アクティブ化の際に、既存のOSファイルが新しいファイルに置き換えられます。

ソフトウェアをあとでアクティブ化するように指定することもできます。

アップグレード時の考慮事項

複数のストレージアレイをアップグレードする場合は、計画段階で主な考慮事項を確認してください。

現在のバージョン

検出された各ストレージアレイについて、vCenter向けストレージプラグインの管理ページからSANtricity OSの現在のソフトウェアバージョンを表示できます。バージョンはSANtricity OSソフトウェア列に表示されます。各行のOSのバージョンをクリックするとポップアップダイアログボックスが表示され、コントローラのファームウェアとNVSRAMの情報を確認できます。

アップグレードが必要なその他のコンポーネント

アップグレードプロセスの一環として、ホストがコントローラと正しく連携するように、ホストのマルチパス/フェイルオーバードライバやHBAドライバのアップグレードも必要になることがあります。互換性の情報については、を参照してください "Interoperability Matrix Tool で確認してください"。

デュアルコントローラ

ストレージアレイにコントローラが 2 台あり、マルチパスドライバがインストールされている場合は、アップグレードの実行中もストレージアレイで I/O の処理を継続できます。アップグレードの実行中は、次の処理が実行されます。

1. コントローラ A のすべての LUN がコントローラ B にフェイルオーバーされます
2. コントローラ A でアップグレードが実行されます
3. コントローラ A に LUN が戻され、コントローラ B の LUN もすべて移されます。
4. コントローラ B でアップグレードが実行されます

アップグレードの完了後、所有権のある正しいコントローラにボリュームが配置されるように、コントローラ間で手動でのボリュームの再配置が必要になることがあります。

アップグレード前の健常性チェックを実行

健全性チェックはアップグレードプロセスの一環として実行されますが、開始前に別途実行することもできます。健全性チェックでは、ストレージアレイのコンポーネントについて、アップグレードを実行できる状態であるかがチェックされます。

- 手順 *

1. メインビューで * Manage * を選択し、メニューから Upgrade Center [Pre-Upgrade Health Check] を選択します。

   [Pre-Upgrade Health Check] ダイアログ・ボックスが開き ' 検出されたすべてのストレージ・システムが一覧表示されます

2. 必要に応じて、ストレージシステムのリストをフィルタまたはソートして、状態が現在「最適」でないすべてのシステムを確認します。
3. 健全性チェックを実行するストレージシステムのチェックボックスを選択します。
4. [スタート] ボタンをクリックします。

   健全性チェックの実行中、ダイアログボックスに進捗状況が表示されます。

5. 健全性チェックが完了したら、各行の右側にある省略記号（ … ）をクリックして、詳細情報を表示したり他のタスクを実行したりできます。

> 健全性チェックでいずれかのアレイに問題が見つかった場合は、そのアレイをスキップして他のアレイのアップグレードを続行するか、プロセス全体を停止して該当するアレイのトラブルシューティングを行うことができます。

SANtricity OSをアップグレードします

ストレージアレイのソフトウェアとNVSRAMをアップグレードして、最新の機能とバグ修正をすべて適用します。コントローラNVSRAMは、コントローラのデフォルトの設定を指定するコントローラファイルです。

作業を開始する前に

次の点を確認してください。

- 最新のSANtricity OSファイルは、プラグインが実行されているホストシステムで使用できます。
- ソフトウェアのアップグレードをすぐにアクティブ化するかあとでアクティブ化するかを決めます。あとでアクティブ化する理由は次のとおりです。
  - * 時間帯 * — ソフトウェアのアクティブ化には時間がかかることがあるため、 I/O 負荷の低い時間帯に実行できます。アクティブ化の際にはコントローラがフェイルオーバーするため、アップグレードが完了するまではパフォーマンスが通常よりも低下する可能性があります。
  - * パッケージのタイプ *-- 他のストレージアレイのファイルをアップグレードする前に ' 新しい OS ソフトウェアを 1 つのストレージアレイでテストすることをお勧めします

> * データ損失のリスク、ストレージアレイの損傷のリスク * — アップグレードの実行中にストレージアレイを変更しないでください。ストレージアレイの電源は切らないでください。

手順

1. ストレージアレイにコントローラが 1 台しかない場合やマルチパスドライバが使用されていない場合は、アプリケーションエラーを回避するためにストレージアレイへの I/O アクティビティを停止します。ストレージアレイにコントローラが 2 台あり、マルチパスドライバがインストールされている場合は、 I/O アクティビティを停止する必要はありません。
2. メイン・ビューから* Manage *を選択し、アップグレードするストレージ・アレイを1つ以上選択します。
3. メニューから[Upgrade]> SANtricity OS]>[Software]を選択します。

   SANtricity OS ソフトウェアのアップグレードページが表示されます。

4. サポートサイトからローカルマシンに最新のSANtricity OSソフトウェアパッケージをダウンロードします。
   a. [新しいファイルをソフトウェアリポジトリに追加]をクリックします
   b. 最新のSANtricity OSダウンロードを検索するためのリンクをクリックします。
   c. [Download Latest Release] リンクをクリックします。
   d. 以降の手順に従って、OSファイルとNVSRAMファイルをローカルマシンにダウンロードします。

> バージョン 8.42 以降のデジタル署名されたファームウェアが必要です。署名のないファームウェアをダウンロードしようとすると、エラーが表示されてダウンロードが中止されます。

5. コントローラのアップグレードに使用する OS ソフトウェアファイルと NVSRAM ファイルを選択します。
   a. ドロップダウンから、ローカルマシンにダウンロードしたOSファイルを選択します。

      使用可能なファイルが複数ある場合は、日付が新しい順にファイルがソートされます。

> ソフトウェアリポジトリには、プラグインに関連付けられているすべてのソフトウェアファイルが一覧表示されます。使用するファイルが表示されない場合は、リンク * ソフトウェアリポジトリに新しいファイルを追加 * をクリックして、追加する OS ファイルが保存されている場所を参照します。

   a. Select an NVSRAM file * ドロップダウンから、使用するコントローラファイルを選択します。

      ファイルが複数ある場合は、日付が新しい順にファイルがソートされます。

6. [Compatible Storage Array] テーブルで ' 選択した OS ソフトウェア・ファイルと互換性のあるストレージ・アレイを確認し ' アップグレードするアレイを選択します
   - [管理] ビューで選択したストレージ・アレイおよび選択したファームウェア・ファイルと互換性のあるストレージ・アレイは ' デフォルトで [互換性のあるストレージ・アレイ] テーブルで選択されています
   - 選択したファームウェアファイルで更新できないストレージアレイは、ステータス * incompatible * と表示される互換性があるストレージアレイテーブルで選択できません。
7. （オプション）ソフトウェアファイルをアクティブ化せずにストレージアレイに転送するには、 * OS ソフトウェアをストレージアレイに転送し、ステージング済みとしてマークし、あとでアクティブ化 * チェックボックスをオンにします。
8. [スタート] ボタンをクリックします。
9. すぐにアクティブ化するかあとでアクティブ化するかに応じて、次のいずれかを実行します。
   - 「transfer」と入力して、アップグレードするアレイ上のOSソフトウェアの推奨バージョンを転送することを確認し、「Transfer」をクリックします。転送されたソフトウェアをアクティブにするには、メニューから[アップグレードセンター][ステージング済みSANtricity OSソフトウェアのアクティブ化]を選択します。
   - アップグレード対象として選択したアレイ上のOSソフトウェアのバージョンを転送してアクティブ化することを確認するには’upgrade]と入力し'[**Upgrade**]をクリックします

アップグレード対象として選択した各ストレージアレイにソフトウェアファイルが転送され、ストレージアレイがリブートされてファイルがアクティブ化されます。

アップグレード処理では次の処理が実行されます。

- アップグレードプロセスの一環として、アップグレード前の健常性チェックが実行されます。アップグレード前の健常性チェックでは、ストレージアレイのすべてのコンポーネントについて、アップグレードを実行できる状態であるかがチェックされます。
- いずれかの健全性チェックでストレージアレイに問題が見つかった場合、アップグレードが停止します。省略記号(…)をクリックします 「ログを保存」を選択してエラーを確認します。ヘルスチェックエラーを無視するように選択し、 * Continue * をクリックしてアップグレードを続行することもできます。
- アップグレード前の健常性チェックのあとに、アップグレード処理をキャンセルすることができます。

10. （オプション）アップグレードが完了したら、省略記号（…）をクリックすると、特定のストレージアレイのアップグレード対象の一覧が表示されます。 次に、[ログの保存]を選択します。

    ブラウザのDownloadsフォルダに’upgrade_log-<date>という名前でファイルが保存されますJSON形式

ステージング済み**OS**ソフトウェアをアクティブ化します

ソフトウェアファイルはただちにアクティブ化することも、都合のいいタイミングでアクティブ化することもできます。この手順では、ソフトウェアファイルをあとでアクティブ化するように選択した場合を想定しています。

このタスクについて

ファームウェアファイルは、アクティブ化せずに転送できます。あとでアクティブ化する理由は次のとおりです。

- * 時間帯 * — ソフトウェアのアクティブ化には時間がかかることがあるため、 I/O 負荷の低い時間帯に実行できます。アクティブ化の際にはコントローラがリブートしてフェイルオーバーするため、アップグレードが完了するまではパフォーマンスが通常よりも低下する可能性があります。
- * パッケージのタイプ * — 他のストレージアレイ上のファイルをアップグレードする前に ' 新しいソフトウェアとファームウェアを 1 つのストレージアレイでテストすることをお勧めします

起動後にアクティブ化プロセスを停止することはできません。

手順

1. メインビューで、* Manage *（管理）を選択します。必要に応じて、ステータス*列をクリックして、ページ上部の「OS Upgrade（waiting activation）」というステータスのすべてのストレージアレイをソートします。
2. ソフトウェアをアクティブ化するストレージアレイを1つ以上選択し、メニューから[Upgrade Center][Activate Staged SANtricity Software]を選択します。

   アップグレード処理では次の処理が実行されます。

   - アップグレード前の健常性チェックは、アクティブ化プロセスの一環として実行されます。アップグレード前の健常性チェックでは、ストレージアレイのすべてのコンポーネントについて、アクティブ

化を実行できる状態であるかがチェックされます。

- いずれかの健全性チェックでストレージアレイに問題が見つかった場合、アクティブ化は停止します。省略記号(…)をクリックします 「ログを保存」を選択してエラーを確認します。ヘルスチェックエラーを無視して、 [* Continue （続行）] をクリックしてアクティブ化を続行することもできます。
- アップグレード前の健常性チェックのあとに、アクティブ化処理をキャンセルすることができます。

  アップグレード前の健常性チェックが正常に完了すると、アクティブ化が実行されます。アクティブ化にかかる時間は、ストレージアレイの構成とアクティブ化しているコンポーネントによって異なります。

3. （オプション）アクティブ化が完了したら、省略記号（…）をクリックすると、特定のストレージアレイに対してアクティブ化された項目のリストが表示されます。 次に、[ログの保存]を選択します。

   ブラウザのDownloadsフォルダに’activate_log-<date>という名前でファイルが保存されますJSON形式

ステージング済み**OS**ソフトウェアをクリアします

保留中のバージョンがあとで誤ってアクティブ化されないように、ステージング済みのOSソフトウェアを削除することができます。ステージング済みOSソフトウェアを削除しても、ストレージアレイで実行されている現在のバージョンには影響しません。

手順

1. メインビューで* Manage *を選択し、メニューからUpgrade Center [ステージ済みSANtricity ソフトウェアのクリア]を選択します。

   ステージング済みSANtricity ソフトウェアのクリアダイアログボックスが開き、検出されたすべてのストレージシステムの中に保留中のソフトウェアまたはNVSRAMが表示されます。

2. 必要に応じて、ストレージシステムのリストをフィルタまたはソートして、ソフトウェアがステージング済みのすべてのシステムを確認します。
3. 保留中のソフトウェアをクリアするストレージシステムのチェックボックスを選択します。
4. [クリア]をクリックします。

   処理のステータスがダイアログボックスに表示されます。

ソフトウェアリポジトリを管理します

ソフトウェアリポジトリを表示および管理することができます。このリポジトリには、vCenter向けストレージプラグインに関連付けられているすべてのソフトウェアファイルが表示されます。

作業を開始する前に

リポジトリを使用してSANtricity OSファイルを追加する場合は、ローカルシステム上にOSファイルがあることを確認します。

このタスクについて

Manage SANtricity OS Software Repositoryオプションを使用すると、プラグインが実行されているホストシ

ステムに1つ以上のOSファイルをインポートできます。ソフトウェアリポジトリにある1つ以上のOSファイルを削除することもできます。

手順

1. メインビューから* Manage *を選択し、メニューからUpgrade Center [Manage SANtricity Software Repository]を選択します。

   Manage SANtricity OS Software Repository（OSソフトウェアリポジトリの管理）ダイアログが表示されます。

2. 次のいずれかを実行します。
   - インポート：
     i. [* インポート *] をクリックします。
     ii. [*参照]をクリックし、追加するOSファイルが保存されている場所に移動します。OSファイルのファイル名は「N2800-830000-000.dlp」のようになります。
     iii. 追加するOSファイルを1つ以上選択し、*インポート*をクリックします。
   - 削除：
     i. ソフトウェアリポジトリから削除するOSファイルを1つ以上選択します。
     ii. [削除（ Delete ）] をクリックします。

結果

インポートを選択した場合は、ファイルがアップロードされて検証されます。削除を選択した場合は、ファイルがソフトウェアリポジトリから削除されます。

ストレージのプロビジョニング

プロビジョニングの概要

vCenter向けストレージプラグインでは、ボリュームと呼ばれるデータコンテナを作成して、ホストがアレイ上のストレージにアクセスできるようにすることができます。

ボリュームのタイプと特性

ボリュームは、ストレージアレイ上のストレージスペースを管理および編成するデータコンテナです。

ストレージアレイで使用可能なストレージ容量からボリュームを作成すると、システムのリソースを整理するのに役立ちます。「ボリューム」という概念は、コンピュータ上のフォルダやディレクトリを使用してファイルにすばやくアクセスできるようにする方法に似ています。

ボリュームは、ホストから認識できる唯一のデータレイヤです。SAN 環境では、ボリュームは論理ユニット番号（ LUN ）にマッピングされます。これらのLUNは、FC、iSCSI、SASなど、ストレージアレイでサポートされている1つ以上のホストアクセスプロトコルを使用してアクセス可能なユーザデータを保持します。

プールまたはボリュームグループ内の各ボリュームには、格納されるデータのタイプに基づいて独自の特性があります。たとえば、次のような特性があります。

- セグメントサイズ-セグメントは、あるドライブに格納されるデータの量（KiB）です。この量に達する

と、ストライプ（RAIDグループ）内の次のドライブへと進みます。セグメントサイズは、ボリュームグループの容量と同じかそれよりも小さくなります。プールのセグメントサイズは固定で、変更することはできません。

- 容量-プールまたはボリュームグループの空き容量からボリュームを作成します。ボリュームを作成するには、プールまたはボリュームグループがすでに存在している必要があります。また、ボリュームを作成するための十分な空き容量がプールまたはボリュームグループに必要です。
- コントローラ所有権--すべてのストレージアレイは'1台または2台のコントローラを持つことができますシングルコントローラアレイでは、ボリュームのワークロードは単一のコントローラによって管理されます。デュアルコントローラアレイでは、ボリュームを「所有」する優先コントローラ（AまたはB）がボリュームに割り当てられます。デュアルコントローラ構成では、自動ロードバランシング機能を使用してボリューム所有権が自動的に調整され、コントローラ間でワークロードが移動する際の負荷の不均衡が解消されます。自動ロードバランシングはI/Oワークロードを自動的に分散する機能を提供し、ホストからの受信I/Oトラフィックは動的に管理されて両方のコントローラに分散されます。
- ボリューム割り当て--ボリュームの作成時または後で、ホストにボリュームへのアクセス権を与えることができます。すべてのホストアクセスは、論理ユニット番号（LUN）を使用して管理されます。ホストは、ボリュームに割り当てられているLUNを検出します。ボリュームを複数のホストに割り当てる場合は、クラスタリングソフトウェアを使用して、すべてのホストからボリュームを使用できるようにしてください。

  ホストタイプでは、ホストがアクセスできるボリュームの数に制限がある場合があります。特定のホストで使用するボリュームを作成するときは、この制限に注意してください。

- リソースプロビジョニング-- EF600またはEF300ストレージアレイでは、バックグラウンド初期化プロセスなしですぐにボリュームを使用するように指定できます。リソースプロビジョニングボリュームは、SSDグループまたはプール内のシックボリュームです。ボリュームの作成時にはドライブ容量が割り当てられますが（ボリュームに割り当てられます）、ドライブブロックは割り当て解除されます（マッピング解除されます）。
- わかりやすい名前--ボリュームに任意の名前を付けることができますが、わかりやすい名前にすることをお勧めします。

ボリュームの作成時には、各ボリュームに容量が割り当てられ、名前、セグメントサイズ（ボリュームグループの場合のみ）、コントローラ所有権、およびボリュームとホストの割り当てが指定されます。ボリュームデータは、必要に応じてコントローラ間で自動的に負荷分散されます。

ボリュームの容量

ストレージアレイ内のドライブは、データに対して物理ストレージ容量を提供します。データの格納を開始する前に、プールまたはボリュームグループと呼ばれる論理コンポーネントに割り当て容量を設定する必要があります。これらのストレージオブジェクトを使用して、ストレージアレイのデータを設定、格納、メンテナンス、および保持できます。

ボリュームの作成および拡張に必要な容量

プールまたはボリュームグループ内の未割り当て容量または空き容量からボリュームを作成できます。

- 未割り当て容量からボリュームを作成する場合は、プールまたはボリュームグループとボリュームを同時に作成できます。
- 空き容量からボリュームを作成する場合は、既存のプールまたはボリュームグループに追加のボリュームを作成します。ボリュームの容量を拡張したら、それに一致するようにファイルシステムのサイズを手動で拡張する必要があります。方法は、使用しているファイルシステムによって異なります。詳細については、ホストオペレーティングシステムのドキュメントを参照してください。

プラグインインターフェイスには、シンボリュームを作成するオプションはありません。

ボリュームのレポート容量

ボリュームのレポート容量は、割り当てられている物理ストレージ容量と同じです。物理ストレージ容量全体が存在している必要があります。物理的に割り当てられるスペースは、ホストに報告されるスペースと同じです。

通常は、ボリュームのレポート容量を、ボリュームが拡張すると予想される最大容量に設定します。ボリュームは、予測可能な高パフォーマンスをアプリケーションに提供します。これは主に、すべてのユーザ容量が作成時に予約されて割り当てられているためです。

容量制限

ボリュームの最小容量は1MiBであり、最大容量はプールまたはボリュームグループ内のドライブの数と容量で決まります。

ボリュームのレポート容量を拡張するときは、次のガイドラインに注意してください。

- 小数点以下3桁まで指定できます（例：65.375GiB）。
- ボリュームグループで使用可能な最大値以下の容量を指定してください。ボリュームを作成する場合は、セグメントサイズの動的（DSS）変更のための追加容量が事前に割り当てられます。DSS変更は、ボリュームのセグメントサイズを変更できるソフトウェアの機能です。
- 一部のホストオペレーティングシステムでは、2TiBを超えるボリュームがサポートされます（最大レポート容量はホストオペレーティングシステムで決定されます）。実際には、一部のホストオペレーティングシステムでサポートされるのは最大128TiBのボリュームです。詳細については、ホストオペレーティングシステムのドキュメントを参照してください。

アプリケーション固有のワークロード

ボリュームを作成する際には、ワークロードを選択して特定のアプリケーション用にストレージアレイの構成をカスタマイズします。

ワークロードは、アプリケーションをサポートするストレージオブジェクトです。アプリケーションごとに1つ以上のワークロードまたはインスタンスを定義できます。一部のアプリケーションでは、特性が似たボリュームで構成されるようにワークロードが設定されます。これらのボリューム特性は、ワークロードがサポートするアプリケーションのタイプに基づいて最適化されます。たとえば、Microsoft SQL Serverアプリケーションをサポートするワークロードを作成し、そのワークロード用のボリュームを作成すると、Microsoft SQL Serverをサポートするようにボリューム特性が最適化されます。

ボリュームの作成中に、ワークロードの使用に関する回答 の質問が表示されます。たとえば、Microsoft Exchange用のボリュームを作成する場合は、必要なメールボックスの数、メールボックスに必要とされる平均容量、およびデータベースのコピーをいくつ作成するかについて設定します。この情報に基づいて最適なボリューム構成が作成されるため、必要に応じて編集することができます。必要に応じて、ボリューム作成のこの手順をスキップできます。

ワークロードのタイプ

アプリケーション固有とその他の2種類のワークロードを作成できます。

- アプリケーション固有--アプリケーション固有のワークロードを使用してボリュームを作成する場合、アプリケーションワークロードのI/Oとアプリケーションインスタンスからの他のトラフィックの競合を最小

限に抑えるために最適化されたボリューム構成が推奨される場合があります。I/Oタイプ、セグメントサイズ、コントローラ所有権、読み取り/書き込みキャッシュなどのボリューム特性が自動的に推奨され、次のアプリケーションタイプ用に作成されるワークロードに合わせて最適化されます。

  - Microsoft SQL Server の場合
  - Microsoft Exchange Server の略
  - ビデオ監視アプリケーション
  - VMware ESXi（ボリュームをVirtual Machine File Systemで使用する場合）

    ボリュームの追加/編集ダイアログボックスを使用して、推奨されるボリューム構成を確認し、システムで推奨されるボリュームや特性を編集、追加、削除できます。

- その他（または特定のボリューム作成サポートのないアプリケーション）- 特定のアプリケーションに関連付けられていないワークロードを作成する場合や、ストレージアレイで使用する予定のアプリケーションに対する最適化が組み込まれていない場合は、その他のワークロードではボリューム構成を手動で指定する必要があります。ボリュームの追加/編集ダイアログボックスを使用して、ボリューム構成を手動で指定する必要があります。

アプリケーションとワークロードの表示

アプリケーションとワークロードを表示するには、System Managerを起動します。このインターフェイスから、アプリケーション固有のワークロードに関連する情報をいくつかの方法で表示できます。

- ボリュームタイルのアプリケーションとワークロードタブを選択すると、ストレージアレイのボリュームをワークロード別にグループ化し、ワークロードが関連付けられているアプリケーションタイプを表示できます。
- パフォーマンスタイルのアプリケーションとワークロードタブを選択して、論理オブジェクトのパフォーマンス指標（レイテンシ、IOPS、MB）を表示できます。オブジェクトはアプリケーションおよび関連付けられているワークロード別にグループ化されます。このパフォーマンスデータを定期的に収集することで、ベースラインとなる数値を設定して傾向を分析することができ、I/Oパフォーマンスに関する問題の調査に役立ちます。

ストレージを作成します

vCenter向けストレージプラグインでは、最初に特定のアプリケーションタイプのワークロードを作成することでストレージを作成します。次に、特性が共通する複数のボリュームを作成し、ワークロードにストレージ容量を追加します。

手順**1**：ワークロードを作成する

ワークロードは、アプリケーションをサポートするストレージオブジェクトです。アプリケーションごとに1つ以上のワークロードまたはインスタンスを定義できます。

このタスクについて

一部のアプリケーションでは、特性が似たボリュームで構成されるようにワークロードが設定されます。これらのボリューム特性は、ワークロードがサポートするアプリケーションのタイプに基づいて最適化されます。たとえば、Microsoft SQL Serverアプリケーションをサポートするワークロードを作成し、そのワークロード用のボリュームを作成すると、Microsoft SQL Serverをサポートするようにボリューム特性が最適化されます。

次のアプリケーションタイプにかぎり、最適化されたボリューム構成が推奨されます。

- Microsoft SQL Server の場合
- Microsoft Exchange Server の略
- ビデオ監視
- VMware ESXi（ボリュームをVirtual Machine File Systemで使用する場合）

手順

1. 管理ページで、ストレージアレイを選択します。
2. メニューを選択します。 Provisioning [ボリュームの管理] 。
3. メニューを選択します。Create [Workload]。

   [アプリケーションワークロードの作成]ダイアログボックスが表示されます。

4. ドロップダウンリストを使用してワークロードを作成するアプリケーションのタイプを選択し、ワークロード名を入力します。
5. [作成（ Create ）] をクリックします。

手順**2**：ボリュームを作成する

ボリュームを作成してアプリケーション固有のワークロードにストレージ容量を追加し、作成したボリュームが特定のホストまたはホストクラスタに認識されるように設定します。

このタスクについて

ほとんどのアプリケーションタイプでは、デフォルトでユーザ定義のボリューム構成が使用されますが、その他のタイプではボリューム作成時にスマート構成が適用されます。たとえば、Microsoft Exchangeアプリケーション用のボリュームを作成する場合は、必要なメールボックスの数、メールボックスに必要とされる平均容量、およびデータベースのコピーをいくつ作成するかについて設定します。この情報に基づいて最適なボリューム構成が作成されるため、必要に応じて編集することができます。

ボリュームは、メニューから作成できます。プロビジョニング[ボリュームの管理]>[作成]>[ボリューム]またはメニューからプロビジョニング[プールとボリュームグループの設定]>[作成]>[ボリューム]。どちらの選択でも手順 は同じです。

ボリュームを作成するプロセスは複数の手順で構成される手順 です。

手順**2a**：ボリュームのホストを選択します

最初の手順では、ボリュームに特定のホストまたはホストクラスタを選択するか、あとからホストを割り当てることができます。

作業を開始する前に

次の点を確認してください。

- 有効なホストまたはホストクラスタが定義されている（メニュー：Provisioning [Configure Hosts]）。
- ホストに対してホストポート識別子が定義されている。
- DA対応ボリュームを作成する場合、ホスト接続でData Assurance（DA）がサポートされている必要があります。ストレージアレイのコントローラで DA をサポートしていないホスト接続が使用されている場

合、関連付けられているホストからは DA 対応ボリュームのデータにアクセスできません。

このタスクについて

ボリュームを割り当てる際は、次のガイドラインに注意してください。

- ホストのオペレーティングシステムによって、ホストがアクセスできるボリュームの数に制限がある場合があります。特定のホストで使用するボリュームを作成するときは、この制限に注意してください。
- 割り当てることができる割り当ては、ストレージアレイのボリュームごとに1つです。
- 割り当てられたボリュームは、ストレージアレイのコントローラ間で共有されます。
- あるホストまたはホストクラスタからボリュームへのアクセスに、同じ論理ユニット番号（LUN）を複数回使用することはできません。一意のLUNを使用する必要があります。
- ボリューム作成プロセスの速度を上げる場合は、ホスト割り当ての手順を省略して、新しく作成したボリュームをオフラインにすることができます。

> ホストクラスタにボリュームを割り当てる場合、そのホストクラスタ内のいずれかのホストに対してすでに確立されている割り当てと競合していると、割り当ては失敗します。

手順

1. 管理ページで、ストレージアレイを選択します。
2. メニューを選択します。 Provisioning [ボリュームの管理] 。
3. メニューから「 Create [Volumes] 」を選択します。

   Select Host （ホストの選択）ダイアログボックスが表示されます。

4. ボリュームを割り当てるホストまたはホストクラスタをドロップダウンリストから選択するか、ホストまたはホストクラスタをあとで割り当てるように選択します。
5. 選択したホストまたはホストクラスタのボリューム作成手順を続行するには、* Next.*をクリックします

   ワークロードの選択ダイアログボックスが表示されます。

手順**2b**：ボリュームのワークロードを選択します

2番目の手順では、ワークロードを選択して、VMwareなどの特定のアプリケーション用にストレージアレイの構成をカスタマイズします。

このタスクについて

このタスクでは、ワークロード用のボリュームを作成する方法について説明します。一般に、ワークロードには、ワークロードがサポートするアプリケーションのタイプに基づいて最適化された、同様の特性を持つボリュームが含まれます。この手順でワークロードを定義するか、既存のワークロードを選択できます。

次のガイドラインに注意してください。

- アプリケーション固有のワークロードを使用する場合、アプリケーションワークロードのI/Oとアプリケーションインスタンスからの他のトラフィックの競合が最小限になるように最適化されたボリューム構成が提示されます。ボリュームの追加/編集ダイアログボックス（次の手順で使用可能）を使用して、推奨されるボリューム構成を確認し、システム推奨のボリュームや特性を編集、追加、削除できます。
- 他の種類のアプリケーションを使用する場合は、ボリュームの追加/編集ダイアログボックス（次の手順で

使用可能）を使用して、ボリューム構成を手動で指定します。

手順

1. 次のいずれかを実行します。
    - 既存のワークロード用のボリュームの作成 * オプションを選択し、ドロップダウンリストからワークロードを選択します。
    - サポート対象のアプリケーションまたは「その他」のアプリケーションに対して新しいワークロードを定義するには、「*新しいワークロードを作成する」オプションを選択し、次の手順を実行します。
        - ドロップダウンリストから、新しいワークロードを作成するアプリケーションの名前を選択します。このストレージアレイで使用するアプリケーションが表示されていない場合は、「Other」エントリのいずれかを選択します。
        - 作成するワークロードの名前を入力します。
2. 「 * 次へ * 」をクリックします。
3. ワークロードがサポート対象のアプリケーションタイプに関連付けられている場合は、要求された情報を入力します。それ以外の場合は、次の手順に進みます。

手順**2c**：ボリュームを追加または編集する

3つ目の手順では、ボリューム構成を定義します。

作業を開始する前に

- プールまたはボリュームグループに十分な空き容量が必要です。
- 1つのボリュームグループに含めることができるボリュームの最大数は256です。
- プールで使用できる最大ボリューム数は、ストレージシステムのモデルによって異なります。
    - 2、048ボリューム（EF600およびE5700シリーズ）
    - 1、024ボリューム（EF300）
    - 512ボリューム（E2800シリーズ）
- Data Assurance（DA）対応ボリュームを作成する場合は、使用するホスト接続でDAがサポートされている必要があります。
    - DA対応ボリュームを作成する場合は、DAに対応したプールまたはボリュームグループを選択します（プールとボリュームグループの候補テーブルで「DA」の横にある「* Yes」を探します）。
    - DA 機能はプールおよびボリュームグループのレベルで提供されます。DA 保護は、データがコントローラ経由でドライブに転送される際に発生する可能性があるエラーをチェックして修正します。新しいボリュームに DA 対応のプールまたはボリュームグループを選択すると、エラーがある場合には検出されて修正されます。
    - ストレージアレイのコントローラで DA をサポートしていないホスト接続が使用されている場合、関連付けられているホストからは DA 対応ボリュームのデータにアクセスできません。
- セキュリティ有効ボリュームを作成するには、ストレージアレイのセキュリティキーを作成する必要があります。
    - セキュリティ有効ボリュームを作成する場合は、セキュリティ対応のプールまたはボリュームグループを選択します（プールとボリュームグループの候補テーブルで「セキュリティ対応」の横にある「はい」を探します）。
    - ドライブセキュリティ機能は、プールおよびボリュームグループのレベルで提供されます。セキュリ

ティ対応ドライブを使用すると、ストレージアレイから物理的に取り外されたドライブ上のデータへの不正アクセスを防止できます。セキュリティ有効ドライブでは、一意の暗号化キーを使用して、書き込み時にデータが暗号化され、読み取り時に復号化されます。

  - プールまたはボリュームグループにはセキュリティ対応とセキュリティ対応でないドライブの両方を含めることができますが、暗号化機能を使用するためにはすべてのドライブがセキュリティ対応である必要があります。

- リソースプロビジョニングボリュームを作成するには、すべてのドライブが Deallocated or Unwritten Logical Block Error （ DULBE ）オプションを適用した NVMe ドライブである必要があります。

このタスクについて

対応するプールまたはボリュームグループからボリュームを作成します。これらのプールは、ボリュームの追加と編集ダイアログボックスに表示されます。対象となる各プールおよびボリュームグループについて、使用可能なドライブの数と合計空き容量が表示されます。

アプリケーション固有のワークロードがある場合、候補となる各プールまたはボリュームグループに、推奨されるボリューム構成に基づいて提示される容量が表示され、残りの空き容量が GiB 単位で表示されます。それ以外のワークロードの場合、プールまたはボリュームグループにボリュームを追加してレポート容量を指定した時点で容量が提示されます。

手順

1. 前の手順でほかにワークロードを選択したかアプリケーション固有のワークロードを選択したかに基づいて、次のいずれかの操作を実行します。

   - その他：1つ以上のボリュームの作成に使用する各プールまたはボリュームグループで’新しいボリュームの追加をクリックします

フィールドの詳細

フィールド	説明
ボリューム名	ボリュームには、作成時にデフォルトの名前が割り当てられます。デフォルトの名前をそのまま使用することも、ボリュームに格納されたデータのタイプを表した名前を指定することもできます。
レポート容量	新しいボリュームの容量と単位（ MiB 、 GiB 、または TiB ）を定義します。シックボリュームの場合、最小容量は1MiBであり、最大容量はプールまたはボリュームグループに含まれるドライブの数と容量で決まります。コピーサービス（Snapshotイメージ、Snapshotボリューム、ボリュームコピー、およびリモートミラー）用のストレージ容量も必要であることに注意してください。そのため、 標準ボリュームにすべての容量を割り当てないでください。プールの容量は4GiB単位で割り当てられます。4GiBの倍数でない容量を割り当てた場合、その容量は使用できません。全容量を使用できるようにするため、4GiB単位で容量を指定してください。使用不可容量が存在する場合、その容量を使用するにはボリュームの容量を増やすしかありません。
ボリュームのブロックサイズ（EF300およびEF600のみ）	ボリュームに対して作成できるブロックサイズが表示されます。 • 512 〜 512 バイト • 4K – 4 、 096 バイト

フィールド	説明
セグメントサイズ（Segment Size）	セグメントのサイジングに関する設定が表示されます。これは、ボリュームグループのボリュームについてのみ表示されます。セグメントサイズを変更することでパフォーマンスを最適化することができます。許容されるセグメントサイズの推移-許容されるセグメントサイズの推移がシステムによって決定されます。現在のセグメントサイズの変更後のサイズとして適切でないものは、ドロップダウンリストに表示されません。通常、許容される変更後のサイズは、現在のセグメントサイズの倍または半分です。たとえば、ボリュームの現在のセグメントサイズが 32KiB であれば、ボリュームの新しいセグメントサイズとして 16KiB または 64KiB が許容されます。* SSDキャッシュが有効なボリューム*- SSDキャッシュが有効なボリュームでは、セグメントサイズを4KiBに指定することができます。4KiB のセグメントサイズを選択するのは、 SSD キャッシュが有効なボリュームで小さいブロックの I/O 処理を実行する（ I/O ブロックサイズが 16KiB 以下の場合など）場合のみにしてください。SSD キャッシュが有効なボリュームで大きいブロックのシーケンシャル処理を実行する場合は、セグメントサイズとして 4KiB を選択するとパフォーマンスが低下することがあります。セグメントサイズの変更にかかる時間-ボリュームのセグメントサイズの変更にかかる時間は、次の要因によって異なります。 • ホストからの I/O 負荷 • ボリュームの修正の優先順位 • ボリュームグループ内のドライブの数 • ドライブチャネルの数 • ストレージアレイコントローラの処理能力 ボリュームのセグメントサイズを変更すると I/O パフォーマンスに影響しますが、データの可用性は維持されます。
セキュリティ対応	*「Secure Capable」の横には、プールまたはボリューム・グループ内のドライブがセキュア対応である場合のみ「Secure Capable」と表示されます。ドライブセキュリティは、ストレージアレイから物理的に取り外されたドライブ上のデータへの不正アクセスを防止します。このオプションは、ドライブセキュリティ機能が有効になっていて、ストレージアレイのセキュリティキーが設定されている場合にのみ使用できます。プールまたはボリュームグループにはセキュリティ対応とセキュリティ対応でないドライブの両方を含めることができますが、暗号化機能を使用するためにはすべてのドライブがセキュリティ対応である必要があります。
ダ	*はい*は、プールまたはボリュームグループ内のドライブがData Assurance（DA）をサポートしている場合にのみ「DA」の横に表示されます。DA を使用すると、ストレージシステム全体のデータの整合性が向上します。DA を使用すると、データがコントローラ経由でドライブに転送される際にストレージアレイがエラーの有無をチェックできます。新しいボリュームに DA を使用すると、すべてのエラーが検出されます。

フィールド	説明
リソースのプロビジョニング（EF300およびEF600のみ）	• Yes *は、ドライブがこのオプションをサポートしている場合にのみ、[Resource Provisioned（リソースのプロビジョニング）]の横に表示されます。リソースプロビジョニングは、EF300およびEF600ストレージアレイで使用できる機能です。これにより、バックグラウンドの初期化プロセスを実行せずに、ボリュームをただちに使用できます。

◦ アプリケーション固有のワークロード--選択したワークロードのシステム推奨のボリュームと特性を受け入れるには、[次へ]をクリックします。選択したワークロードのシステム推奨のボリュームと特性を変更、追加、または削除するには、[ボリュームの編集]をクリックします。

フィールドの詳細

フィールド	説明
ボリューム名	ボリュームには、作成時にデフォルトの名前が割り当てられます。デフォルトの名前をそのまま使用することも、ボリュームに格納されたデータのタイプを表した名前を指定することもできます。
レポート容量	新しいボリュームの容量と単位（ MiB 、 GiB 、または TiB ）を定義します。シックボリュームの場合、最小容量は1MiBであり、最大容量はプールまたはボリュームグループに含まれるドライブの数と容量で決まります。コピーサービス（Snapshotイメージ、Snapshotボリューム、ボリュームコピー、およびリモートミラー）用のストレージ容量も必要であることに注意してください。そのため、 標準ボリュームにすべての容量を割り当てないでください。プールの容量は 4GiB 単位で割り当てられます。4GiB の倍数でない容量を割り当てた場合、その容量は使用できません。全容量を使用できるようにするため、 4GiB 単位で容量を指定してください。使用不可容量が存在する場合、その容量を使用するにはボリュームの容量を増やすしかありません。
ボリュームタイプ	アプリケーション固有のワークロード用に作成されたボリュームのタイプを示します。
ボリュームのブロックサイズ（EF300およびEF600のみ）	ボリュームに対して作成できるブロックサイズが表示されます。 • 512 — 512バイト • 4k — 4,096バイト

フィールド	説明
セグメントサイズ（ Segment Size ）	セグメントのサイジングに関する設定が表示されます。これは、ボリュームグループのボリュームについてのみ表示されます。セグメントサイズを変更することでパフォーマンスを最適化することができます。許容されるセグメントサイズの推移-許容されるセグメントサイズの推移がシステムによって決定されます。現在のセグメントサイズの変更後のサイズとして適切でないものは、ドロップダウンリストに表示されません。通常、許容される変更後のサイズは、現在のセグメントサイズの倍または半分です。たとえば、ボリュームの現在のセグメントサイズが 32KiB であれば、ボリュームの新しいセグメントサイズとして 16KiB または 64KiB が許容されます。* SSDキャッシュが有効なボリューム*- SSDキャッシュが有効なボリュームでは、セグメントサイズを4KiBに指定することができます。4KiB のセグメントサイズを選択するのは、 SSD キャッシュが有効なボリュームで小さいブロックの I/O 処理を実行する（ I/O ブロックサイズが 16KiB 以下の場合など）場合のみにしてください。SSD キャッシュが有効なボリュームで大きいブロックのシーケンシャル処理を実行する場合は、セグメントサイズとして 4KiB を選択するとパフォーマンスが低下することがあります。セグメントサイズの変更にかかる時間-ボリュームのセグメントサイズの変更にかかる時間は、次の要因によって異なります。 • ホストからの I/O 負荷 • ボリュームの修正の優先順位 • ボリュームグループ内のドライブの数 • ドライブチャネルの数 • ストレージアレイコントローラの処理能力 ボリュームのセグメントサイズを変更すると I/O パフォーマンスに影響しますが、データの可用性は維持されます。
セキュリティ対応	*「Secure Capable」の横には、プールまたはボリューム・グループ内のドライブがセキュア対応である場合のみ「Secure Capable」と表示されます。ドライブセキュリティを使用すると、ストレージアレイから物理的に取り外されたドライブ上のデータへの不正アクセスを防止できます。このオプションは、ドライブセキュリティ機能が有効になっていて、ストレージアレイのセキュリティキーが設定されている場合にのみ使用できます。プールまたはボリュームグループにはセキュリティ対応とセキュリティ対応でないドライブの両方を含めることができますが、暗号化機能を使用するためにはすべてのドライブがセキュリティ対応である必要があります。
ダ	*はい*は、プールまたはボリュームグループ内のドライブがData Assurance（DA）をサポートしている場合にのみ「DA」の横に表示されます。DA を使用すると、ストレージシステム全体のデータの整合性が向上します。DA を使用すると、データがコントローラ経由でドライブに転送される際にストレージアレイがエラーの有無をチェックできます。新しいボリュームに DA を使用すると、すべてのエラーが検出されます。

フィールド	説明
リソースのプロビジョニング（EF300およびEF600のみ）	• Yes *は、ドライブがこのオプションをサポートしている場合にのみ、[Resource Provisioned（リソースのプロビジョニング）]の横に表示されます。リソースプロビジョニングは、EF300およびEF600ストレージアレイで使用できる機能です。これにより、バックグラウンドの初期化プロセスを実行せずに、ボリュームをただちに使用できます。

2. 選択したアプリケーションのボリューム作成手順を続行するには、 * 次へ * をクリックします。

手順**2d**：ボリュームの構成を確認します

最後の手順では、作成するボリュームの概要を確認し、必要に応じて変更を加えます。

手順

1. 作成するボリュームを確認します。変更するには、「 * 戻る」をクリックします。
2. ボリューム構成に問題がなければ、「 * 完了 * 」をクリックします。

完了後

- vSphere Clientで、ボリューム用のデータストアを作成します。
- アプリケーションがボリュームを使用できるように、アプリケーションホストのオペレーティングシステムに対して必要な変更を行います。
- オペレーティングシステム固有のユーティリティ（サードパーティベンダーから入手可能）を実行してから、SMcliコマンドを実行します。 `-identifyDevices` ボリューム名をホストストレージアレイ名に関連付けるには、次の手順を実行します。

  SMcliはSANtricity OSに含まれており、SANtricityシステムマネージャからダウンロードできます。SANtricityシステムマネージャからSMcliをダウンロードする方法の詳細については、 "SANtricity System Managerオンラインヘルプのコマンドラインインターフェイス（CLI）のダウンロードのトピック"。

ボリュームの容量を拡張します

ボリュームのサイズを変更して、レポート容量を拡張できます。

作業を開始する前に

次の点を確認してください。

- ボリュームの関連付けられたプールまたはボリュームグループに十分な空き容量が必要です。
- ボリュームが最適状態で、変更中の状態ではありません。
- ボリュームでホットスペアドライブが使用されていない必要があります。（ボリュームグループ内のボリュームにのみ適用されます）。

このタスクについて

このタスクでは、プールまたはボリュームグループ内の使用可能な空き容量を使用してボリュームのレポート

容量（ホストに報告される容量）を拡張する方法について説明します。このプールまたはボリュームグループ内の他のボリュームについて、今後必要になる容量を考慮してください。

> ボリュームの容量の拡張は、特定のオペレーティングシステムでのみサポートされています。サポートされていないホストオペレーティングシステム上でボリューム容量を拡張すると、拡張した容量は使用できなくなり、元のボリューム容量をリストアすることもできなくなります。

手順

1. [* Manage *（管理）]ページで、サイズを変更するボリュームを含むストレージ・アレイを選択します。
2. メニューを選択します。 Provisioning [ボリュームの管理] 。
3. 容量を拡張するボリュームを選択し、 * 容量を拡張 * を選択します。

   容量の拡張の確認ダイアログボックスが表示されます。

4. 続行するには、 * はい * を選択します。

   レポート容量の拡張ダイアログボックスが表示されます。このダイアログボックスには、ボリュームの現在のレポート容量と、ボリュームの関連付けられたプールまたはボリュームグループ内で使用可能な空き容量が表示されます。

5. レポート容量の拡張に使用できるレポート容量を追加するには、 * ボックスを使用します。メビバイト（ MiB ）、ギビバイト（ GiB ）、またはテビバイト（ TiB ）のいずれかで表示するように容量の値を変更できます。
6. [* 拡大（ * ）] をクリックします

   選択に基づいて、ボリュームの容量が拡張されます。この処理には時間がかかることがあり、システムのパフォーマンスに影響する可能性があります。

完了後

ボリュームの容量を拡張したら、それに応じてファイルシステムのサイズを手動で拡張する必要があります。方法は、使用しているファイルシステムによって異なります。詳細については、ホストオペレーティングシステムのドキュメントを参照してください。

ボリュームの設定を変更します

ボリュームの名前、ホストの割り当て、セグメントサイズ、変更の優先順位、キャッシュなど、ボリュームの設定を変更できます。 など。

作業を開始する前に

変更するボリュームのステータスが「最適」であることを確認してください。

手順

1. 管理ページで、変更するボリュームが含まれているストレージアレイを選択します。
2. メニューを選択します。 Provisioning [ボリュームの管理] 。
3. 変更するボリュームを選択し、*表示/設定の編集*を選択します。

Volume Settings（ボリューム設定）ダイアログボックスが表示されます。選択したボリュームの設定がこのダイアログボックスに表示されます。

4. ボリュームの名前とホストの割り当てを変更するには、* Basic *タブを選択します。

フィールドの詳細

設定	説明
名前	ボリュームの名前が表示されます。現在の名前が適切でない場合はボリュームの名前を変更します。
容量	選択したボリュームのレポート容量と割り当て容量が表示されます。
プール/ボリュームグループ	プールまたはボリュームグループの名前とRAIDレベルが表示されます。プールまたはボリュームグループがセキュリティ対応か、およびセキュリティ有効かを示します。
ホスト	ボリュームの割り当てが表示されます。I/O処理でボリュームにアクセスできるように、ボリュームをホストまたはホストクラスタに割り当てます。これにより、ストレージアレイ内の特定のボリューム、または複数のボリュームへのアクセスがホストまたはホストクラスタに許可されます。 • 割り当て先--選択したボリュームにアクセスできるホストまたはホストクラスタを指定します • * lun *：ホストがボリュームへのアクセスに使用するアドレス・スペースに割り当てられる番号ボリュームは、LUNの形式でホストに容量として提示されます。各ホストには独自のLUNアドレススペースがあります。したがって、同じLUNを複数のホストで使用して、異なるボリュームにアクセスできます。 NVMeインターフェイスの場合、この列にはネームスペースIDが表示されます。ネームスペースは、ブロックアクセス用にフォーマットされたNVMストレージです。SCSIの論理ユニットに相当し、ストレージアレイではボリュームに関連します。ネームスペースIDは、NVMeコントローラのネームスペースの一意の識別子です。1~255の値を設定できます。SCSIの論理ユニット番号（LUN）に相当します。
識別子	選択したボリュームの識別子が表示されます。 • World-Wide Identifier（WWID）。ボリュームの一意の16進数の識別子。 • Extended Unique Identifier（EUI）。ボリュームのEUI-64識別子。 • サブシステム識別子（SSID）。ボリュームのストレージアレイサブシステムの識別子。

5. プールまたはボリュームグループ内のボリュームの追加設定を変更するには、*詳細*タブを選択します。

フィールドの詳細

設定	説明
アプリケーションとワークロードの情報	ボリュームの作成時に、アプリケーション固有のワークロードまたはその他のワークロードを作成できます。該当する場合は、選択したボリュームのワークロード名、アプリケーションタイプ、およびボリュームタイプが表示されます。ワークロード名は必要に応じて変更できます。
QoS設定	• Data Assuranceを永続的に無効にする*-この設定は、ボリュームがData Assurance（DA）対応の場合にのみ表示されます。DAは、データがコントローラ経由でドライブに転送される際に発生する可能性があるエラーをチェックして修正します。選択したボリュームのDAを完全に無効にする場合は、このオプションを使用します。DAは無効にすると再度有効にすることはできません。読み取り前冗長性チェックを有効にする--この設定は'ボリュームがシックボリュームの場合にのみ表示されます読み取り前冗長性チェックは、読み取りの実行時にボリュームのデータの整合性を確認する機能です。この機能を有効にしたボリュームでは、コントローラファームウェアによってデータに整合性がないと判断されると読み取りエラーを返します。
コントローラ所有権	ボリュームを所有するプライマリコントローラを定義します。コントローラ所有権は非常に重要であり、慎重に計画する必要があります。コントローラ間で総I/O数をできるだけ均等に分散する必要があります。

設定	説明
セグメントサイジング	セグメントのサイジングに関する設定が表示されます。これは、ボリュームグループのボリュームについてのみ表示されます。セグメントサイズを変更することでパフォーマンスを最適化することができます。許容されるセグメントサイズの推移-許容されるセグメントサイズの推移がシステムによって決定されます。現在のセグメントサイズの変更後のサイズとして適切でないものは、ドロップダウンリストに表示されません。通常、許容される変更後のサイズは、現在のセグメントサイズの倍または半分です。たとえば、ボリュームの現在のセグメントサイズが 32KiB であれば、ボリュームの新しいセグメントサイズとして 16KiB または 64KiB が許容されます。* SSDキャッシュが有効なボリューム*- SSDキャッシュが有効なボリュームでは、セグメントサイズを4KiBに指定することができます。4KiBのセグメントサイズを選択するのは、 SSD キャッシュが有効なボリュームで小さいブロックの I/O 処理を実行する（ I/O ブロックサイズが 16KiB 以下の場合など）場合のみにしてください。SSD キャッシュが有効なボリュームで大きいブロックのシーケンシャル処理を実行する場合は、セグメントサイズとして 4KiB を選択するとパフォーマンスが低下することがあります。*セグメントサイズの変更にかかる時間。*ボリュームのセグメントサイズの変更にかかる時間は、次の要因によって異なります。 • ホストからの I/O 負荷 • ボリュームの修正の優先順位 • ボリュームグループ内のドライブの数 • ドライブチャネルの数 • ストレージアレイコントローラの処理能力 ボリュームのセグメントサイズを変更すると I/O パフォーマンスに影響しますが、データの可用性は維持されます。
修正の優先順位	変更優先度の設定が表示されます。これは、ボリュームグループ内のボリュームについてのみ表示されます。変更優先度は、ボリュームの変更処理にどの程度の処理時間を割り当てるかをシステムパフォーマンスに対する相対的な優先度として定義したものです。修正の優先順位を上げると、システムパフォーマンスが低下する場合があります。優先度レベルを選択するには、スライダバーを動かします。修正の優先順位率--優先順位が最も低いとシステムのパフォーマンスは向上しますが、修正操作にかかる時間は長くなります。優先度を最も高くすると修正処理にかかる時間は短縮されますが、システムパフォーマンスが低下する可能性があります。
キャッシュ	キャッシュ設定が表示されます。この設定を変更すると、ボリュームの全体的なI/Oパフォーマンスを向上させることができます。

設定	説明
SSD キャッシュ	（この機能はEF600またはEF300ストレージシステムでは使用できません）。 SSDキャッシュの設定が表示されます。互換性のあるボリュームでこの設定を有効にすると、読み取り専用のパフォーマンスが向上します。互換性があるのは、同じドライブセキュリティ機能とData Assurance機能を共有しているボリュームです。SSDキャッシュ機能は、1つまたは複数のソリッドステートディスク（SSD）を使用して読み取りキャッシュを実装します。SSDの読み取り時間が速くなるため、アプリケーションパフォーマンスが向上します。読み取りキャッシュはストレージアレイ内にあるため、ストレージアレイを使用するすべてのアプリケーションでキャッシュが共有されます。キャッシュするボリュームを選択すると、あとは動的に自動でキャッシングが実行されます。

6. [保存（ Save ）] をクリックします。

結果

選択内容に基づいてボリューム設定が変更されます。

ワークロードにボリュームを追加する

既存または新規のワークロードに未割り当てのボリュームを追加できます。

このタスクについて

ボリュームをコマンドラインインターフェイス（CLI）を使用して作成した場合や別のストレージアレイから移行（インポート/エクスポート）した場合、それらのボリュームはワークロードに関連付けられません。

手順

1. 管理ページで、追加するボリュームが含まれているストレージアレイを選択します。
2. メニューを選択します。 Provisioning [ボリュームの管理] 。
3. [アプリケーションとワークロード]タブを選択します。

   [アプリケーションとワークロード]ビューが表示されます。

4. 「ワークロードに追加」を選択します。

   ワークロードの選択ダイアログボックスが表示されます。

5. 次のいずれかを実行します。
   - 既存のワークロードにボリュームを追加する-既存のワークロードにボリュームを追加する場合は、このオプションを選択します。ドロップダウンリストを使用してワークロードを選択します。そのワークロードに関連付けられているアプリケーションタイプが、追加するボリュームに割り当てられます。
   - 新しいワークロードにボリュームを追加--アプリケーションタイプの新しいワークロードを定義して新しいワークロードにボリュームを追加するには、このオプションを選択します。
6. 「次へ」を選択して、ワークロードへの追加手順を続行します。

Select Volumes（ボリュームの選択）ダイアログボックスが表示されます。

7. ワークロードに追加するボリュームを選択します。
8. 選択したワークロードに追加するボリュームを確認します。
9. ワークロードの設定が完了したら、[完了]をクリックします。

ワークロードの設定を変更する

ワークロードの名前を変更し、関連付けられているアプリケーションタイプを確認できます。

手順

1. 管理ページで、変更するワークロードを含むストレージアレイを選択します。
2. メニューを選択します。 Provisioning [ボリュームの管理] 。
3. [アプリケーションとワークロード]タブを選択します。

   [アプリケーションとワークロード]ビューが表示されます。

4. 変更するワークロードを選択し、*表示/設定の編集*を選択します。

   [アプリケーションとワークロードの設定]ダイアログボックスが表示されます。

5. （オプション）ユーザが指定したワークロードの名前を変更します。
6. [保存（ Save ）] をクリックします。

ボリュームを初期化

ボリュームは、最初に作成されるときに自動的に初期化されます。ただし、一定の障害状況からリカバリするために、ボリュームを手動で初期化するようRecovery Guruから指示される場合があります。

このオプションを使用する場合は、必ずテクニカルサポートの指示に従ってください。初期化するボリュームは1つ以上選択できます。

作業を開始する前に

- すべてのI/O処理を停止しておきます。
- 初期化するボリューム上のデバイスまたはファイルシステムをすべてアンマウントしておく必要があります。
- ボリュームは最適状態であり、ボリュームで変更処理が実行されていません。*注意：*開始後に処理をキャンセルすることはできません。ボリュームのすべてのデータが消去されます。Recovery Guruの指示があった場合を除き、この処理は実行しないでください。この手順 を開始する前に、テクニカルサポートにお問い合わせください。

このタスクについて

ボリュームを初期化しても、ボリュームのWWN、ホストの割り当て、割り当て済み容量、およびリザーブ容量の設定は保持されます。Data Assurance（DA）設定とセキュリティ設定も同じままです。

次のタイプのボリュームは初期化できません。

- Snapshotボリュームのベースボリューム
- ミラー関係のプライマリボリューム
- ミラー関係のセカンダリボリューム
- ボリュームコピーのソースボリューム
- ボリュームコピーのターゲットボリューム
- すでに初期化が進行中のボリューム

この手順 は、プールまたはボリュームグループから作成された標準ボリュームにのみ適用されます。

手順

1. 管理ページで、初期化するボリュームを含むストレージアレイを選択します。
2. メニューを選択します。 Provisioning [ボリュームの管理] 。
3. 任意のボリュームを選択し、メニューを選択します。More [Initialize volumes]。

   Initialize Volumes（ボリュームの初期化）ダイアログボックスが表示されます。このダイアログボックスには、ストレージアレイ上のすべてのボリュームが表示されます。

4. 初期化するボリュームを1つ以上選択し、処理を確定します。

結果

システムは次の処理を実行します。

- 初期化されたボリュームからすべてのデータが消去されます。
- ブロックインデックスがクリアされます。これにより、書き込み前のブロックはゼロで埋められているかのように読み取られます（ボリュームは完全に空のように表示されます）。

この処理には時間がかかることがあり、システムのパフォーマンスに影響する可能性があります。

ボリュームを再配置する

ボリュームの再配置は、ボリュームを優先コントローラ所有者に戻すために実行します。通常、ホストとストレージアレイの間のデータパスに問題が発生した場合、マルチパスドライバがボリュームを優先コントローラ所有者から移動します。

作業を開始する前に

- 再配置するボリュームが使用中でない必要があります。使用中の場合はI/Oエラーが発生します。
- 再配置するボリュームを使用しているすべてのホストにマルチパスドライバがインストールされている必要があります。インストールされていない場合はI/Oエラーが発生します。ホストにマルチパスドライバがインストールされていないボリュームを再配置する場合は、再配置処理実行中のボリュームに対するI/Oアクティビティをすべて停止して、アプリケーションエラーを回避する必要があります。

このタスクについて

ほとんどのホストマルチパスドライバは、優先コントローラ所有者へのパスで各ボリュームへのアクセスを試みます。ただし、この優先パスが使用できなくなると、ホストのマルチパスドライバは代替パスにフェイルオ

ーバーします。このフェイルオーバー原因 によって、ボリューム所有権が代替コントローラに変更される可能性があります。フェイルオーバーの原因となった状況を解決すると、一部のホストではボリュームの所有権が優先コントローラ所有者に自動的に戻りますが、場合によっては手動でのボリュームの再配置が必要になります。

手順

1. 管理ページで、再配置するボリュームを含むストレージアレイを選択します。
2. メニューを選択します。 Provisioning [ボリュームの管理] 。
3. メニューを選択します。 More [redistribute volumes （ボリュームの再配置）]

   ボリュームの再配置ダイアログボックスが表示されますストレージアレイ上のボリュームのうち、優先コントローラ所有者が現在の所有者と一致しないボリュームがすべてこのダイアログボックスに表示されます。

4. 再配置するボリュームを1つ以上選択し、処理を確定します。

結果

選択したボリュームが優先コントローラ所有者に移動されるか、ボリュームの再配置の不要なダイアログボックスが表示されることがあります。

ボリュームのコントローラ所有権を変更する

ボリュームの優先コントローラ所有権を変更して、ホストアプリケーションのI/Oが新しいパス経由で転送されるようにすることができます。

作業を開始する前に

マルチパスドライバを使用しない場合は、現在ボリュームを使用しているホストアプリケーションをすべてシャットダウンする必要があります。これにより、I/Oパスが変更された場合にアプリケーションエラーを回避できます。

このタスクについて

プールまたはボリュームグループに含まれる1つ以上のボリュームのコントローラ所有権を変更することができます。

手順

1. 管理ページで、コントローラ所有権を変更するボリュームを含むストレージアレイを選択します。
2. メニューを選択します。 Provisioning [ボリュームの管理] 。
3. 任意のボリュームを選択し、メニューを選択します。[More（その他）][Change ownership（所有権の変更）]。

   [ボリューム所有権の変更]ダイアログボックスが表示されます。このダイアログボックスには、ストレージアレイ上のすべてのボリュームが表示されます。

4. [* Preferred Owner]*ドロップダウン・リストを使用して、変更する各ボリュームの優先コントローラを変更し、操作を確定します。

結果

- ボリュームのコントローラ所有権が変更されます。ボリュームへのI/Oが、このI/Oパス経由で転送される

ようになります。

- マルチパスドライバが新しいパスを認識するように再設定されるまで、ボリュームで新しいI/Oパスが使用されない場合があります。

この処理にかかる時間は通常5分未満です。

ボリュームのキャッシュ設定を変更します

読み取りキャッシュと書き込みキャッシュの設定を変更して、ボリュームの全体的なI/Oパフォーマンスを調整することができます。

このタスクについて

ボリュームのキャッシュ設定を変更する際は、次のガイドラインに注意してください。

- [キャッシュ設定の変更]ダイアログボックスを開いた後、選択したキャッシュプロパティの横にアイコンが表示されることがあります。このアイコンは、コントローラがキャッシュ処理を一時的に停止したことを示しています。この処理は、新しいバッテリを充電しているとき、コントローラが削除されたとき、またはコントローラによってキャッシュサイズの不一致が検出された場合に発生します。この状況が解消されると、ダイアログボックスで選択したキャッシュプロパティがアクティブになります。選択したキャッシュプロパティがアクティブにならない場合は、テクニカルサポートにお問い合わせください。
- キャッシュ設定は、単一のボリュームまたはストレージアレイ上の複数のボリュームに対して変更できます。キャッシュ設定は、すべてのボリュームについて同時に変更できます。

手順

1. [管理]ページで、キャッシュ設定を変更するボリュームを含むストレージアレイを選択します。
2. メニューを選択します。 Provisioning [ボリュームの管理] 。
3. 任意のボリュームを選択し、メニューを選択します。 More [キャッシュ設定の変更] 。

   [キャッシュ設定の変更]ダイアログボックスが表示されます。このダイアログボックスには、ストレージアレイ上のすべてのボリュームが表示されます。

4. [**Basic**]タブを選択して、リード・キャッシュとライト・キャッシュの設定を変更します。

   フィールドの詳細

キャッシュ設定	説明
読み取りキャッシュ	読み取りキャッシュは、ドライブから読み取られたデータを格納するバッファです。読み取り処理の対象となるデータが以前の処理ですでにキャッシュに格納されていれば、ドライブにアクセスする必要はありません。読み取りキャッシュのデータは、フラッシュされるまで保持されます。
書き込みキャッシュ	書き込みキャッシュは、ドライブにまだ書き込まれていないホストからのデータを格納するバッファです。書き込みキャッシュ内のデータは、ドライブに書き込まれるまで保持されます。書き込みキャッシュにより、I/Oパフォーマンスを向上させることができます。キャッシュは、ボリュームの書き込みキャッシュが無効になったあとに自動的にフラッシュされます。

5. 「詳細設定」タブを選択して、シックボリュームの詳細設定を変更します。アドバンストキャッシュ設定

は、シックボリュームに対してのみ使用できます。

フィールドの詳細

設定	説明
動的キャッシュ読み取りプリフェッチ	Dynamic Cache Read Prefetchを使用すると、コントローラは、ドライブからキャッシュにデータブロックを読み取っているときに、連続する追加のデータブロックをキャッシュにコピーできます。このキャッシングにより、以降のデータ要求にキャッシュから対応できる可能性が高まります。動的キャッシュ読み取りプリフェッチは、シーケンシャルI/Oを使用するマルチメディアアプリケーションで重要ですデータがキャッシュにプリフェッチされる速度と量は、ホスト読み取りの速度と要求サイズに基づいて自動で調整されます。ランダムアクセスの場合、原因 データがキャッシュにプリフェッチされることはありません。この機能は、読み取りキャッシュが無効になっている場合は適用されません。
バッテリなしの書き込みキャッシュ	バッテリなしの書き込みキャッシュを有効にすると、バッテリがない、障害が発生している、完全に放電されている、フル充電されていないなどの状況でも書き込みキャッシュが続行されます。バッテリなしの書き込みキャッシュを選択すると電源の喪失時にデータが失われる可能性があるため、一般には推奨されません。通常、書き込みキャッシュは、バッテリが充電されるか障害が発生したバッテリが交換されるまで、コントローラによって一時的にオフにされます。注意：データ損失の可能性--保護用のユニバーサル電源装置がない場合にこのオプションを選択すると、データが失われる可能性があります。また、コントローラのバッテリがない場合にWrite caching without Batteriesオプションを有効にすると、データが失われる可能性があります。
ミラーリングありの書き込みキャッシュ	ミラーリングありの書き込みキャッシュでは、一方のコントローラのキャッシュメモリに書き込まれたデータがもう一方のコントローラのキャッシュメモリにも書き込まれます。そのため、一方のコントローラで障害が発生した場合、もう一方のコントローラで未処理の書き込み処理をすべて完了できます。書き込みキャッシュのミラーリングは、書き込みキャッシュが有効で、2台のコントローラが配置されている場合にのみ使用できます。ミラーリングありの書き込みキャッシュは、ボリュームの作成時にデフォルトで設定されます。

6. [保存（Save）]をクリックして、キャッシュ設定を変更します。

ボリュームのメディアスキャン設定を変更します

メディアスキャンは、ボリューム内のすべてのデータと冗長性情報をスキャンするバックグラウンド処理です。このオプションは、1つ以上のボリュームのメディアスキャン設定を有効または無効にしたり、スキャン期間を変更したりする場合に使用します。

作業を開始する前に

次の点を理解しておきます

- メディアスキャンは、スキャンする容量とスキャン期間に基づいて一定の速度で継続的に実行されます。優先度の高いバックグラウンドタスク（再構築など）によってバックグラウンドスキャンが一時的に中断されることはありますが、その場合も同じ速度で再開されます。

- ボリュームは、ストレージアレイとそのボリュームでメディアスキャンオプションが有効になっている場合にのみスキャンされます。そのボリュームで冗長性チェックも有効になっている場合、ボリュームに冗長性情報があるかぎり、ボリューム内の冗長性情報とデータの整合性がチェックされます。メディアスキャンでの冗長性チェックは、ボリュームの作成時にデフォルトで有効になります。
- スキャン中に回復不能なメディアエラーが発生した場合、可能であれば、冗長性情報を使用してデータが修復されます。

  たとえば、最適なRAID 5ボリューム、または最適なRAID 6ボリュームまたは1本のドライブのみで障害が発生したRAID 6ボリュームには、冗長性情報が存在します。冗長性情報を使用して回復不能なエラーを修復できない場合は、読み取り不能セクターログにデータブロックが追加されます。イベントログには、修正可能なメディアエラーと修正不可能なメディアエラーの両方が記録されます。

- 冗長性チェックでデータと冗長性情報の間に不整合が検出された場合は、イベントログに報告されます。

このタスクについて

メディアスキャンは、アプリケーションで頻繁に読み取られないディスクブロック上のメディアエラーを検出して修復します。これにより、ドライブ障害が発生しても、障害ドライブのデータが冗長性情報とボリュームグループまたはプール内の他のドライブのデータを使用して再構築されるため、データが失われることはありません。

次の操作を実行できます。

- ストレージアレイ全体のバックグラウンドメディアスキャンを有効または無効にします
- ストレージアレイ全体のスキャン期間を変更します
- 1つ以上のボリュームのメディアスキャンを有効または無効にします
- 1つ以上のボリュームの冗長性チェックを有効または無効にします

手順

1. 管理ページで、メディアスキャン設定を変更するボリュームが含まれているストレージアレイを選択します。
2. メニューを選択します。 Provisioning [ボリュームの管理] 。
3. 任意のボリュームを選択し、メニューを選択します。More [メディアスキャン設定の変更]。

   Change Drive Media Scan Settings（ドライブメディアスキャン設定の変更）ダイアログボックスが表示されます。このダイアログボックスには、ストレージアレイ上のすべてのボリュームが表示されます。

4. メディアスキャンを有効にするには、*スキャン期間中にメディアをスキャンする*チェックボックスをオンにします。メディアスキャンを無効にすると、すべてのメディアスキャン設定が一時停止されます。
5. メディアスキャンを実行する日数を指定します。
6. メディアスキャンを実行する各ボリュームの[メディアスキャン]チェックボックスをオンにします。メディアスキャンの実行を選択した各ボリュームに対して、冗長性チェックオプションが有効になります。冗長性チェックを実行しないボリュームが個々にある場合は、*冗長性チェック*チェックボックスの選択を解除します。
7. [保存（ Save ）] をクリックします。

結果

選択内容に基づいて、バックグラウンドメディアスキャンに対する変更が適用されます。

ボリュームを削除します

1つ以上のボリュームを削除して、プールまたはボリュームグループの空き容量を増やすことができます。

作業を開始する前に

削除するボリュームで、次の点を確認します。

- すべてのデータがバックアップされます。
- すべての入出力（I/O）が停止しています。
- デバイスとファイルシステムがアンマウントされている。

このタスクについて

通常、作成したボリュームのパラメータや容量が正しくない場合、またはストレージ構成のニーズを満たさなくなった場合に、ボリュームを削除します。ボリュームを削除すると、プールまたはボリュームグループの空き容量が増えます。

> ボリュームを削除すると、それらのボリューム上のすべてのデータが失われます。

次のいずれかの条件に該当するボリュームは、*削除できない*ことに注意してください。

- ボリュームが初期化中である。
- ボリュームが再構築中である。
- ボリュームが属するボリュームグループにコピーバック処理を実行中のドライブが含まれている。
- ボリュームのステータスが失敗になった場合を除き、セグメントサイズの変更などの変更処理を実行中です。
- ボリュームにいずれかのタイプの永続的予約が設定されている。
- ボリュームがボリュームコピー処理のソースボリュームまたはターゲットボリュームで、処理のステータスが「保留」、「実行中」、または「失敗」である。

> ボリュームのサイズが指定したサイズ（現在は128TB）を超えると、削除処理がバックグラウンドで実行され、解放されたスペースをすぐに使用できなくなることがあります。

手順

1. [* Manage *（管理）]ページで、削除するボリュームを含むストレージ・アレイを選択します。
2. メニューを選択します。 Provisioning [ボリュームの管理] 。
3. [削除（ Delete ）] をクリックします。

   ボリュームの削除ダイアログボックスが表示されます。

4. 削除するボリュームを1つ以上選択し、処理を確定します。
5. [削除（ Delete ）] をクリックします。

ホストを設定

ホスト作成の概要

vCenter向けストレージプラグインを使用してストレージを管理するには、ネットワーク内の各ホストを検出または定義する必要があります。ホストは、ストレージアレイ上のボリュームにI/Oを送信するサーバです。

ホストの手動作成

ホストの作成は、ストレージアレイが接続されているホストを認識して、ボリュームへのI/Oアクセスを許可するために必要な手順の1つです。ホストは手動で作成できます。

- 手動--ホストを手動で作成するときに'ホスト・ポート識別子をリストから選択するか'手動で入力することによって'それらを関連付けますホストの作成後、ボリュームへのアクセスを共有する場合は、ボリュームをホストに割り当てたり、ホストクラスタに追加したりできます。

ボリュームの割り当て方法

ホストからボリュームにI/Oを送信するには、ボリュームをボリュームに割り当てる必要があります。ボリュームの作成時にホストまたはホストクラスタを選択するか、あとからボリュームをホストまたはホストクラスタに割り当てることができます。ホストクラスタはホストのグループです。ホストクラスタを作成すると、同じボリュームを複数のホストに簡単に割り当てることができます。

ホストへのボリュームの割り当ては柔軟性が高く、ストレージの特定のニーズを満たすことができます。

- ホストクラスタの一部ではなく、スタンドアロンホスト--ボリュームを個々のホストに割り当てることができます。ボリュームにアクセスできるのは1つのホストだけです。
- ホストクラスタ--ボリュームをホストクラスタに割り当てることができますボリュームには、ホストクラスタ内のすべてのホストからアクセスできます。
- ホストクラスタ内のホスト--ホストクラスタの一部である個別のホストにボリュームを割り当てることができますホストはホストクラスタの一部ですが、ボリュームにアクセスできるのは個々のホストだけであり、ホストクラスタ内の他のホストからはアクセスできません。

ボリュームの作成時に、論理ユニット番号（LUN）が自動的に割り当てられます。LUNは、I/O処理中のホストとコントローラの間のアドレスとして機能します。LUNはボリュームが作成されたあとに変更できます。

ホストアクセスを作成

vCenter向けストレージプラグインを使用してストレージを管理するには、ネットワーク内の各ホストを検出または定義する必要があります。

このタスクについて

ホストを作成すると、ストレージアレイへの接続とボリュームへのI/Oアクセスを提供するホストパラメータを定義できます。

ホストを作成する際は、次のガイドラインに注意してください。

- ホストに関連付けられたホストポート識別子を定義する必要があります。

- ホストに割り当てられたシステム名と同じ名前を指定してください。
- 選択した名前がすでに使用されている場合、この処理は失敗します。
- 名前は 30 文字以内にする必要があります。

手順

1. Manage （管理）ページで、ホスト接続があるストレージアレイを選択します。
2. メニューを選択します。 Provisioning [ホストの設定] 。

   Configure Hosts ページが開きます。

3. メニュー： Create [Host] をクリックします。

   Create Host （ホストの作成）ダイアログボックスが表示されます。

4. ホストの設定を必要に応じて選択します。

フィールドの詳細

設定	説明
名前	新しいホストの名前を入力します。
ホストオペレーティングシステムのタイプ	新しいホストで実行しているオペレーティングシステムをドロップダウンリストから選択します。
ホストインターフェイスタイプ	（オプション）ストレージアレイで複数のタイプのホストインターフェイスがサポートされている場合、使用するホストインターフェイスタイプを選択します。
ホストポート	次のいずれかを実行します。 • * I/Oインターフェイスの選択*--通常’ホストポートはログインしており’ドロップダウン・リストから使用できるようになっている必要がありますリストからホストポート識別子を選択することができます。 • 手動追加--ホストポート識別子がリストに表示されない場合は’ホストポートがログインしていないことを意味しますHBA ユーティリティまたは iSCSI イニシエータユーティリティを使用して、ホストポート識別子を検索してホストに関連付けることができます。ホストポート識別子を手動で入力するか、ユーティリティから（一度に 1 つずつ）ホストポートフィールドにコピーして貼り付けることができます。ホストポート識別子は、一度に 1 つずつ選択してホストに関連付ける必要がありますが、ホストに関連付けられている識別子をいくつでも選択することができます。各識別子はホストポートフィールドに表示されます。必要に応じて、横の * X * を選択して識別子を削除することもできます。
CHAP イニシエータシークレットを設定する	（オプション）iSCSI IQNを使用してホストポートを選択または手動で入力し、ストレージアレイにアクセスしてCHAP（Challenge Handshake Authentication Protocol）を使用して認証するホストを必要とする場合は、[Set CHAP initiator secret]チェックボックスをオンにします。選択または手動で入力した iSCSI ホストポートごとに、次の手順を実行します。 • CHAP 認証用に各 iSCSI ホストイニシエータに設定されたものと同じ CHAP シークレットを入力します。相互 CHAP 認証（ホストが自身をストレージアレイに対して検証し、ストレージアレイが自身をホストに対して検証できるようにする双方向認証）を使用する場合は、ストレージアレイの初期セットアップまたは設定変更時に CHAP シークレットも設定する必要があります。 • ホストの認証が不要な場合は、このフィールドを空白のままにします。現在使用されている iSCSI 認証方式は CHAP だけです。

5. [作成（ Create ）] をクリックします。
6. ホスト情報を更新する必要がある場合は、表からホストを選択し、 * 表示 / 設定の編集 * をクリックします。

結果

ホストの作成が完了すると、ホストに設定されている各ホストポートのデフォルト名（ユーザラベル）が作成されます。デフォルトのエイリアスは「 <Hostname_Port number>` 」です。たとえば、ホスト IPT に対して最初に作成されたポートのデフォルトのエイリアスは「 ipt_1 」です。

完了後

I/O処理に使用できるように、ボリュームをホストに割り当てる必要があります。に進みます "ホストにボリュームを割り当てます"。

ホストクラスタを作成する

複数のホストが同じボリュームへのI/Oアクセスを必要とする場合は、ホストクラスタを作成できます。

このタスクについて

ホストクラスタを作成する際は、次のガイドラインに注意してください。

- クラスタの作成に使用できるホストが複数ない場合、この処理は開始されません。
- ホストクラスタ内のホストはオペレーティングシステムが異なっていてもかまいません（異機種混在）。
- ホストクラスタのNVMeホストをNVMe以外のホストと混在させることはできません。
- Data Assurance（DA）対応ボリュームを作成する場合は、使用するホスト接続でDAがサポートされている必要があります。

  ストレージアレイのコントローラで DA をサポートしていないホスト接続が使用されている場合、関連付けられているホストからは DA 対応ボリュームのデータにアクセスできません。

- 選択した名前がすでに使用されている場合、この処理は失敗します。
- 名前は 30 文字以内にする必要があります。

手順

1. Manage （管理）ページで、ホスト接続があるストレージアレイを選択します。
2. メニューを選択します。 Provisioning [ホストの設定] 。

   Configure Hosts ページが開きます。

3. メニューを選択します。Create [Host cluster]（ホストクラスタの作成）。

   Create Host Cluster（ホストクラスタの作成）ダイアログボックスが表示されます。

4. ホストクラスタの設定を必要に応じて選択します。

設定	説明
名前	新しいホストクラスタの名前を入力します。
ボリュームアクセスを共有するホストを選択します	ドロップダウンリストから2つ以上のホストを選択します。このリストには、ホストクラスタにまだ含まれていないホストのみが表示されます。

5. [作成（ Create ）] をクリックします。

   選択したホストが接続されているインターフェイスタイプのData Assurance（DA）機能が異なる場合、ホストクラスタでDAを使用できないことを示すメッセージがダイアログに表示されます。この場合、ホストクラスタにDA対応ボリュームを追加することはできません。続行するには「*はい」を選択し、キャンセルするには「*いいえ」を選択します。

   DA を使用すると、ストレージシステム全体のデータの整合性が向上します。ホストとドライブの間でデータが移動されたときにストレージアレイがエラーの有無をチェックします。新しいボリュームに DA を使用すると、すべてのエラーが検出されます。

結果

新しいホストクラスタが表に表示され、その下の行に割り当てられたホストが表示されます。

完了後

I/O処理に使用できるように、ボリュームをホストクラスタに割り当てる必要があります。に進みます "ホストにボリュームを割り当てます"。

ホストにボリュームを割り当てます

I/O処理に使用できるように、ボリュームをホストまたはホストクラスタに割り当てる必要があります。

作業を開始する前に

ホストにボリュームを割り当てる際は、次のガイドラインに注意してください。

- ボリュームは一度に 1 つのホストまたはホストクラスタにのみ割り当てることができます。
- 割り当てられたボリュームは、ストレージアレイのコントローラ間で共有されます。
- あるホストまたはホストクラスタからボリュームへのアクセスに、同じ論理ユニット番号（LUN）を複数回使用することはできません。一意のLUNを使用する必要があります。
- 新しいボリュームグループでは、すべてのボリュームが作成されて初期化されるまでホストに割り当てると、ボリュームの初期化時間が短縮されます。ボリュームグループに関連付けられているボリュームをマッピングすると、すべてのボリュームの初期化速度が低下することに注意してください。

このタスクについて

ボリューム割り当ては、ストレージアレイ内のそのボリュームへのアクセスをホストまたはホストクラスタに許可します。

このタスクでは、未割り当てのボリュームはすべて表示されますが、ホストがData Assurance（DA）対応かどうかで処理は次のように異なります。

- DA 対応ホストの場合は、 DA 有効、 DA 無効のどちらのボリュームでも選択できます。
- DA 対応でないホストで DA が有効なボリュームを選択した場合、ボリュームをホストに割り当てる前にボリュームの DA を自動的に無効にする必要があるという警告が表示されます。

  次の場合、ボリュームの割り当ては失敗します。

- すべてのボリュームが割り当てられている。

- ボリュームはすでに別のホストまたはホストクラスタに割り当てられています。次の場合、ボリュームを割り当てることはできません。
- 有効なホストまたはホストクラスタが存在しません。
- ホストポート識別子がホストに対して定義されていない。
- すべてのボリューム割り当てが定義されている。

手順

1. Manage （管理）ページで、ホスト接続があるストレージアレイを選択します。
2. メニューを選択します。 Provisioning [ホストの設定] 。

   Configure Hosts ページが開きます。

3. ボリュームを割り当てるホストまたはホストクラスタを選択し、 * ボリュームの割り当て * をクリックします。

   ダイアログボックスに割り当て可能なすべてのボリュームが表示されます。列をソートしたり、フィルタボックスに何かを入力したりすると、特定のボリュームを簡単に見つけることができます。

4. 割り当てる各ボリュームの横にあるチェックボックスを選択するか、テーブルヘッダーにあるチェックボックスを選択してすべてのボリュームを選択します。
5. [**Assign**] をクリックして、操作を完了します。

結果

ホストまたはホストクラスタへのボリュームの割り当てが完了すると、次の処理が実行されます。

- 割り当てられたボリュームに次に使用可能な LUN 番号が受信されます。ホストはこの LUN 番号を使用してボリュームにアクセスします。
- ホストに関連付けられているボリュームの一覧にユーザが指定したボリューム名が表示されます。該当する場合、ホストに関連付けられているボリュームの一覧には、工場出荷時に設定されたアクセスボリュームも表示されます。

ボリュームの割り当てを解除する

ボリュームへのI/Oアクセスが不要になった場合は、ホストまたはホストクラスタへの割り当てを解除できます。

このタスクについて

ボリュームの割り当てを解除する際は、次のガイドラインに注意してください。

- 最後に割り当てたボリュームをホストクラスタから削除する際に、特定のボリュームが割り当てられているホストがホストクラスタにある場合は、最後に割り当てたボリュームを削除する前にホストに割り当てられたボリュームを削除または移動してください。
- ホストクラスタ、ホスト、またはホストポートがオペレーティングシステムに登録されたボリュームに割り当てられている場合は、その登録をクリアしてからこれらのノードを削除する必要があります。

手順

1. Manage （管理）ページで、ホスト接続があるストレージアレイを選択します。

2. メニューを選択します。 Provisioning [ホストの設定] 。

   Configure Hosts ページが開きます。

3. 編集するホストまたはホストクラスタを選択し、*ボリュームの割り当て解除*をクリックします。

   現在割り当てられているすべてのボリュームを示すダイアログボックスが表示されます。

4. 割り当てを解除する各ボリュームの横にあるチェックボックスを選択するか、テーブルヘッダーにあるチェックボックスを選択してすべてのボリュームを選択します。
5. Unassign *をクリックします。

結果

- 割り当てを解除したボリュームは新しい割り当てに使用できます。
- 変更がホストで設定されるまで、ボリュームは引き続きホストオペレーティングシステムで認識されます。

ホストの設定を変更します

ホストまたはホストクラスタの名前、ホストのオペレーティングシステムタイプ、および関連付けられているホストクラスタを変更できます。

手順

1. Manage （管理）ページで、ホスト接続があるストレージアレイを選択します。
2. メニューを選択します。 Provisioning [ホストの設定] 。

   Configure Hosts ページが開きます。

3. 編集するホストを選択し、*表示/設定の編集*をクリックします。

   ダイアログボックスが開き、現在のホスト設定が表示されます。

4. ホストのプロパティを変更するには、[プロパティ*]タブが選択されていることを確認し、必要に応じて設定を変更します。

フィールドの詳細

設定	説明
名前	ユーザが指定したホストの名前を変更できます。ホストの名前は必ず指定する必要があります。
関連付けられているホストクラスタです	次のいずれかのオプションを選択できます。 • なし--ホストはスタンドアロンホストのままです。ホストがホストクラスタに関連付けられている場合は、ホストがクラスタから削除されます。 • **<**ホストクラスタ**>--**選択したクラスタにホストを関連付けます
ホストオペレーティングシステムのタイプ	定義したホストで実行されているオペレーティングシステムのタイプを変更できます。

5. ポート設定を変更するには、[ホストポート]タブをクリックし、必要に応じて設定を変更します。

フィールドの詳細

設定	説明
ホストポート	次のいずれかのオプションを選択できます。 • *追加-- Addを使用して'新しいホストポート識別子をホストに関連付けますホストポート識別子名の長さは、ホストインターフェイスのテクノロジによって決まります。Fibre ChannelとInfiniBandのホストポート識別子名は、16文字にする必要があります。iSCSI のホストポート識別子名は最大 223 文字です。ポートは一意である必要があります。すでに設定されているポート番号は使用できません。 • *Delete *-- Deleteを使用して、ホストポート識別子を削除(関連付けを解除)します。Deleteオプションを使用しても、ホストポートは物理的には削除されません。このオプションを選択すると、ホストポートとホストの間の関連付けが削除されます。ホストバスアダプタまたはiSCSI イニシエータを削除しないかぎり、ホストポートは引き続きコントローラで認識されます。 ホストポート識別子を削除すると、そのホストとの関連付けが解除されます。また、ホストはホストに割り当てられているボリュームにこのホストポート識別子経由でアクセスできなくなります。
ラベル	ポートラベル名を変更するには、* Edit *アイコン（鉛筆）をクリックします。ポートラベル名は一意である必要があります。すでに設定されているラベル名は使用できません。
CHAPシークレット	iSCSIホストにのみ表示されます。イニシエータ（iSCSIホスト）のCHAPシークレットを設定または変更できます。システムは、チャレンジハンドシェイク認証プロトコル（CHAP）方式を使用します。CHAPは初回のリンク確立時にターゲットとイニシエータのIDを検証します。認証は、CHAPシークレットと呼ばれる共有セキュリティキーに基づいて行われます。

6. [保存（ Save ）] をクリックします。

ホストまたはホストクラスタを削除

ホストまたはホストクラスタを削除して、ボリュームがそのホストに関連付けられないようにすることができます。

このタスクについて

ホストまたはホストクラスタを削除する際は、次のガイドラインに注意してください。

- ボリュームの割り当てはすべて削除され、関連付けられたボリュームを新しい割り当てに使用できるようになります。

- ホストが属するホストクラスタに固有の割り当てがある場合、ホストクラスタへの影響はありません。ただし、ホストが属するホストクラスタに他の割り当てがない場合は、ホストクラスタとそれに関連付けられている他のすべてのホストまたはホストポート識別子にデフォルトの割り当てが継承されます。
- ホストに関連付けられていたホストポート識別子の定義は削除されます。

手順

1. Manage （管理）ページで、ホスト接続があるストレージアレイを選択します。
2. メニューを選択します。 Provisioning [ホストの設定] 。

   Configure Hosts ページが開きます。

3. 削除するホストまたはホストクラスタを選択し、* Delete *をクリックします。

   確認ダイアログボックスが表示されます。

4. 処理を実行することを確認し、* Delete *をクリックします。

結果

ホストを削除すると、システムは次の処理を実行します。

- ホストを削除し、該当する場合はホストクラスタからも削除します。
- 割り当てられているボリュームへのアクセスを削除します。
- 関連付けられているボリュームの割り当てを解除します。
- ホストに関連付けられているホストポート識別子の関連付けを解除します。ホストクラスタを削除すると、システムは次の処理を実行します。
  - ホストクラスタとそれに関連付けられているホスト（存在する場合）を削除します。
  - 割り当てられているボリュームへのアクセスを削除します。
  - 関連付けられているボリュームの割り当てを解除します。
  - ホストに関連付けられているホストポート識別子の関連付けを解除します。

プールとボリュームグループを設定

プールとボリュームグループの概要

vCenter向けストレージプラグインでストレージをプロビジョニングするには、ストレージアレイで使用するハードディスクドライブ（HDD）またはソリッドステートディスク（SSD）ドライブを格納するプールまたはボリュームグループを作成します。

プロビジョニング

物理ハードウェアは、データを整理して簡単に取得できるように、論理コンポーネントにプロビジョニングされます。次の2種類のグループ化がサポートされています。

- プール
- ボリュームグループ

プールとボリュームグループは、ストレージアレイ内の最上位のストレージ単位であり、ドライブの容量を管理可能な区分に分割します。これらの論理区分内に、データが格納される個々のボリュームまたはLUNがあります。

ストレージシステムを導入したら、まず次の処理を実行して使用可能なドライブ容量をさまざまなホストに提供します。

- 十分な容量のプールまたはボリュームグループを作成しています
- パフォーマンス要件を満たすために必要な数のドライブをプールまたはボリュームグループに追加します
- 特定のビジネス要件を満たすために必要なレベルのRAID保護（ボリュームグループを使用している場合）を選択

同じストレージシステム上にプールまたはボリュームグループを複数作成することはできますが、1本のドライブを複数のプールまたはボリュームグループに所属させることはできません。その後、プールまたはボリュームグループのスペースを使用して、I/O用にホストに表示されるボリュームが作成されます。

プール

プールは、物理ハードディスクドライブを1つの大きなストレージスペースに集約し、RAID保護を強化するために設計されています。プールに割り当てられたドライブをすべて使用して多数の仮想RAIDセットを作成したり、プールを構成する全ドライブにデータを均等に分散することができます。ドライブを減らしたり追加したりした場合は、アクティブドライブ全体にわたってデータの再分散が動的に実行されます。

プール機能はワンランク上のRAIDとして機能します。基盤となるRAIDアーキテクチャが仮想化されるため、リビルド、ドライブ拡張、ドライブ障害への対応といったタスクの処理に最適なパフォーマンスと柔軟性が提供されます。8+2構成（8本のデータディスクと2本のパリティディスク）では、RAIDレベルは自動的に6に設定されます。

ドライブが一致しません

プールにはHDDまたはSSDのいずれかを選択できます。ただし、ボリュームグループと同様に、プール内のすべてのドライブが同じテクノロジを使用する必要があります。どのドライブを含めるかは、コントローラが自動的に選択するため、選択したテクノロジに対応する十分な数のドライブがあることを確認する必要があります。

障害ドライブの管理

プールの最小容量は11ドライブですが、ドライブに障害が発生した場合に備えて、1ドライブ分の容量がスペア容量として確保されます。このスペア容量を「予約済み容量」と呼びます。

プールが作成されると、一定量の容量が緊急用に保持されます。この容量はドライブ数で表されますが、実際の実装はドライブのプール全体に分散されます。保持されるデフォルトの容量は、プール内のドライブの数に基づきます。

プールの作成後、予約済み容量の値は増減できます。また、予約済み容量なし（0ドライブ分）に設定することもできます。保持可能な最大容量（ドライブ数）は10ですが、プール内のドライブの総数に基づいて、使用可能な容量はこれより少なくなる可能性があります。

ボリュームグループ

ボリュームグループは、ストレージシステム内で容量をボリュームに割り当てる方法を定義します。ディスクドライブはRAIDグループにまとめられ、ボリュームは1つのRAIDグループ内の複数のドライブにまたがって

実装されます。したがって、ボリュームグループの設定により、グループに含まれるドライブと、使用されているRAIDレベルが特定されます。

ボリュームグループを作成するときに、グループに含めるドライブはコントローラによって自動的に選択されます。グループのRAIDレベルは手動で選択する必要があります。ボリュームグループの容量は、選択したドライブの合計数にドライブの容量を掛けた値となります。

ドライブが一致しません

ボリュームグループ内のドライブのサイズとパフォーマンスを一致させる必要があります。ボリュームグループ内のドライブの容量が異なる場合、すべてのドライブが最小容量サイズとして認識されます。ボリュームグループ内のドライブの速度が異なる場合、すべてのドライブが最低速度で認識されます。これらの要素は、ストレージシステムのパフォーマンスと全体的な容量に影響します。

異なるドライブテクノロジ（HDDとSSDドライブ）を混在させることはできません。RAID 3、5、6は、最大30ドライブまでに制限されています。RAID 1およびRAID 10はミラーリングを使用するため、ディスク数は偶数にする必要があります。

障害ドライブの管理

ボリュームグループに含まれるRAID 1/10、RAID 3、RAID 5、またはRAID 6のボリュームでドライブに障害が発生した場合に備えて、ボリュームグループではホットスペアドライブをスタンバイとして使用します。ホットスペアドライブにはデータは含まれず、ストレージアレイの冗長性レベルの向上に使用されます。

ストレージアレイのドライブで障害が発生した場合、障害が発生したドライブからホットスペアドライブに自動的に切り替わります。物理的にドライブを交換する必要はありません。ドライブ障害の発生時にホットスペアドライブが使用可能であれば、冗長性データを使用して障害が発生したドライブからホットスペアドライブにデータが再構築されます。

プールまたはボリュームグループを使用するかどうかを決定します

プールを選択します

- 迅速なドライブのリビルドやストレージ管理の簡易化が必要な場合、ランダムワークロードが大量に発生する場合。
- 各ボリュームのデータをプールを構成する一連のドライブにランダムに分散する場合。プールまたはプール内のボリュームのRAIDレベルを設定または変更することはできません。プールではRAIDレベル6を使用します。

ボリュームグループを選択します

- システムの帯域幅を最大限に使用する必要がある場合、ストレージの設定を調整する機能、大量のシーケンシャルワークロードを利用する場合。
- データをRAIDレベルに基づいてドライブに分散する場合。ボリュームグループは作成時にRAIDレベルを指定できます。
- 各ボリュームのデータをボリュームグループを構成する一連のドライブにシーケンシャルに書き込む場合。

> プールとボリュームグループは共存可能なため、ストレージアレイにプールとボリュームグループの両方を含めることができます。

プールの自動作成と手動作成

ストレージ構成に応じて、プールを自動的に作成することも、手動で作成することもできます。プールは、論理的にグループ化された一連のドライブです。

プールを作成して管理する前に、プールの自動作成方法と、プールを手動で作成する必要があるタイミングについて、次のセクションを確認してください。

自動作成

ストレージアレイに未割り当て容量が検出されると、ストレージアレイで未割り当て容量が検出されるとプールの自動作成が開始されます。1つ以上のプールの作成、既存のプールへの未割り当て容量の追加、またはその両方を自動で実行するように求められます。

プールの自動作成は、次のいずれかの条件に該当する場合に実行されます。

- プールがストレージアレイに存在せず、新しいプールの作成に十分なドライブがない。
- 新しいドライブは、少なくとも1つのプールがあるストレージアレイに追加されます。プール内の各ドライブは、同じタイプ（HDDまたはSSD）であり、容量が同等である必要があります。次のタスクを実行するよう求められます。
- タイプが十分な数のドライブがある場合は、単一のプールを作成する。
- 未割り当て容量が異なるドライブタイプで構成されている場合は、複数のプールを作成する。
- ストレージアレイにすでにプールが定義されている場合は、既存のプールにドライブを追加し、同じタイプの新しいドライブをプールに追加する。
- タイプの異なる複数のドライブを追加した場合は、ドライブタイプが同じドライブを既存のプールに追加し、別のドライブタイプのドライブを使用して別のプールを作成する。

手動作成

最適な構成を自動作成で判断できない場合は、プールを手動で作成できます。この状況は、次のいずれかの理由で発生する可能性があります。

- 新しいドライブが複数のプールに追加される可能性があります。
- 1つ以上の新しいプールの候補で、シェルフ損失の保護またはドロワー損失の保護を使用できる。
- 1つ以上の現在のプールの候補で、シェルフ損失の保護またはドロワー損失の保護のステータスを維持できません。ストレージアレイに複数のアプリケーションがあり、同じドライブリソース間で競合しないようにする場合は、プールを手動で作成することもできます。この場合、1つ以上のアプリケーション用に小規模なプールを手動で作成することを検討してください。データを分散するための多数のボリュームを含む大規模なプールにワークロードを割り当てるのではなく、1~2個のボリュームだけを割り当てることができます。特定のアプリケーションのワークロード専用の個別のプールを手動で作成すると、ストレージアレイの処理をより迅速に実行でき、競合が軽減されます。

プールを自動的に作成する

未割り当てのドライブが11本以上検出された場合、または既存のプールに対応する未割り当てのドライブが1本検出された場合、プールを自動的に作成できます。プールは、論理的にグループ化された一連のドライブです。

作業を開始する前に

次のいずれかの条件に該当する場合は、Pool Auto-Configurationダイアログボックスを起動できます。

- ドライブタイプが類似する既存のプールに追加できる未割り当てドライブが1本以上検出された場合。
- 新しいプールの作成に使用できる未割り当てドライブが11本以上検出された場合（ドライブタイプが異なるために既存のプールに追加できない場合）。

このタスクについて

プールの自動作成を使用すると、ストレージアレイ内のすべての未割り当てドライブを1つのプールに簡単に設定したり、既存のプールにドライブを追加したりできます。

次の点に注意してください。

- ストレージアレイにドライブを追加すると、ドライブが自動的に検出され、ドライブタイプと現在の構成に基づいて、1つまたは複数のプールを作成するように求められます。
- プールが以前に定義されている場合は、互換性があるドライブを既存のプールに追加するかどうかを確認するプロンプトが自動的に表示されます。新しいドライブを既存のプールに追加すると、システムによって、追加した新しいドライブを含む新しい容量にデータが自動的に再配分されます。
- EF600またはEF300ストレージアレイを設定する場合は、各コントローラが最初の12個のスロットと直近の12個のスロットに同じ数のドライブにアクセスできることを確認します。この構成により、コントローラは両方のドライブ側PCIeバスをより効果的に使用できます。プールの作成には、ストレージアレイのすべてのドライブを使用する必要があります。

手順

1. [管理]ページで、プールのストレージアレイを選択します。
2. メニューを選択します。Provisioning（プロビジョニング）[Configure Pools and Volume Groups]（プールとボリュームグループの構成）。
3. メニューを選択します。More [Launch pool auto-configuration]。

   新しいプール、ドライブが追加されている既存のプール、またはその両方が表示されます。新しいプールには、連番を付した名前がデフォルトで付けられます。

   システムで次の処理が行われていることに注意してください。

   - ドライブタイプ（HDDまたはSSD）が同じで容量が同等の十分な数のドライブがある場合は、単一のプールが作成されます。
   - 未割り当て容量が異なるドライブタイプで構成されている場合は、複数のプールが作成されます。
   - ストレージアレイにすでにプールが定義されている場合に、そのプールにドライブタイプが同じ新しいドライブを追加すると、既存のプールにドライブが追加されます。
   - ドライブタイプが同じドライブを既存のプールに追加し、別のドライブタイプのドライブを使用して別のプールを作成する。
4. 新しいプールの名前を変更するには、* Edit *アイコン（鉛筆）をクリックします。
5. プールのその他の特性を表示するには、カーソルを合わせるか、詳細アイコン（ページ）をタッチします。

   ドライブタイプ、セキュリティ機能、Data Assurance（DA）機能、シェルフ損失の保護、ドロワー損失の保護に関する情報が表示されます。

EF600およびEF300ストレージアレイについては、リソースのプロビジョニングとボリュームのブロックサイズについても設定が表示されます。

6. [* 同意する *] をクリックします。

プールを手動で作成する

プールの自動構成の要件を満たしていない場合は、プールを手動で作成できます。プールは、論理的にグループ化された一連のドライブです。

作業を開始する前に

- ドライブタイプ（HDDまたはSSD）が同じドライブが少なくとも11本必要です。
- シェルフ損失の保護を有効にするには、プールを構成するドライブが少なくとも6つのドライブシェルフに配置されていて、同じシェルフのドライブが3本以上含まれていないことが必要です。
- ドロワー損失の保護を有効にするには、プールを構成するドライブが少なくとも5つのドロワーに同じ数ずつ配置されている必要があります。
- EF600またはEF300ストレージアレイを設定する場合は、各コントローラが最初の12個のスロットと直近の12個のスロットに同じ数のドライブにアクセスできることを確認します。この構成により、コントローラは両方のドライブ側PCIeバスをより効果的に使用できます。プールの作成には、ストレージアレイのすべてのドライブを使用する必要があります。

このタスクについて

プールの作成時に、ドライブタイプ、セキュリティ機能、Data Assurance（DA）機能、シェルフ損失の保護、ドロワー損失の保護など、その特性を確認します。

EF600およびEF300ストレージアレイについては、リソースのプロビジョニングやボリュームのブロックサイズも設定に含まれます。

手順

1. [管理]ページで、プールのストレージアレイを選択します。
2. メニューを選択します。Provisioning（プロビジョニング）[Configure Pools and Volume Groups]（プールとボリュームグループの構成）。
3. メニュー：[Create Pool（プールの作成）]をクリックします。

   Create Pool（プールの作成）ダイアログボックスが表示されます。

4. プールの名前を入力します。
5. （オプション）ストレージアレイに複数のタイプのドライブがある場合、使用するドライブタイプを選択します。

   作成可能なすべてのプールの候補が表示されます。

6. 次の特性に基づいて使用するプール候補を選択し、*作成*をクリックします。

フィールドの詳細

特性	使用
空き容量	プールの空き容量がGiB単位で表示されます。アプリケーションのストレージニーズに合わせて、容量の候補となるプールを選択します。予約済み（スペア）容量もプール全体に分散され、空き容量に含まれることはありません。
合計ドライブ数	プール候補に含まれるドライブの数が表示されます。できるだけ多くのドライブが予約済み容量として自動的に確保されます（プール内の6本につき1本のドライブが予約済み容量として確保されます）。ドライブ障害が発生すると、予約済み容量を使用して再構築されたデータが格納されます。
ドライブブロックサイズ（EF300およびEF600のみ）	プール内のドライブが書き込めるブロックサイズ（セクターサイズ）が表示されます。値は次のとおりです。 • 512 — 512バイトのセクターサイズ。 • 4K — 4、096バイトのセクターサイズ。
セキュリティ対応	プール候補がセキュリティ対応ドライブだけで構成されているかどうかを示します。セキュリティ対応ドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。 • プールはドライブセキュリティを使用して保護できますが、この機能を使用するには、すべてのドライブがセキュリティ対応である必要があります。 • FDEのみのプールを作成する場合は、SecureCapable列で「* Yes- fde」を検索してください。FIPSのみのプールを作成する場合は、「はい- FIPS *」または「はい- FIPS（混在）」を探します。「Mixed」は140-2と140-3レベルのドライブが混在していることを示します。これらのレベルを組み合わせて使用する場合は、プールが下位レベルのセキュリティ（140〜2）で動作することに注意してください。 • セキュリティ対応かどうかがドライブによって異なるプールや、セキュリティレベルが異なるドライブが混在したプールを作成することもできます。プールにセキュリティ対応でないドライブが含まれている場合、プールをセキュリティ対応にすることはできません。
セキュリティを有効化	セキュリティ対応ドライブでドライブセキュリティ機能を有効にするオプションです。プールがセキュリティ対応で、セキュリティキーを作成している場合、チェックボックスを選択してセキュリティを有効にできます。 一度有効にしたドライブセキュリティは、プールを削除してドライブを消去しないかぎり解除できません。

特性	使用
DA対応	プール候補でData Assurance（DA）を使用できるかどうかを示します。DAは、データがコントローラ経由でドライブに転送される際に発生する可能性があるエラーをチェックして修正します。DAを使用する場合は、DAに対応したプールを選択します。このオプションはDA機能が有効になっている場合にのみ使用できます。プールにはDAに対応したドライブとDAに対応していないドライブを含めることができますが、DAを使用するためにはすべてのドライブがDAに対応している必要があります。
リソースプロビジョニング対応（EF300およびEF600のみ）	プール候補でリソースプロビジョニングを使用できるかどうかを示します。リソースプロビジョニングは、EF300およびEF600ストレージアレイで使用できる機能です。これにより、バックグラウンドの初期化プロセスを実行せずに、ボリュームをただちに使用できます。
シェルフ損失の保護	シェルフ損失の保護が使用可能かどうかを示します。シェルフ損失の保護が有効な場合、1台のドライブシェルフとの通信が完全に失われた場合でもプール内のボリューム上のデータへのアクセスが保証されます。
ドロワー損失の保護	ドロワー損失の保護が使用可能かどうかを示します。この保護は、使用しているドライブシェルフにドロワーが搭載されている場合にのみ提供されます。ドロワー損失の保護が有効な場合、ドライブシェルフの1台のドロワーとの通信が完全に失われた場合でもプール内のボリューム上のデータへのアクセスが保証されます。
サポートされるボリュームのブロックサイズ（EF300およびEF600のみ）	プール内のボリュームに対して作成できるブロックサイズが表示されます。 • 512n — 512バイトネイティブ。 • 512e — 512バイトエミュレーション。 • 4k — 4,096バイト

ボリュームグループを作成します

ホストからアクセス可能な1つ以上のボリュームのボリュームグループを作成できます。ボリュームグループは、RAIDレベルや容量などの特性が同じボリュームのコンテナです。

作業を開始する前に

次のガイドラインを確認してください。

- 未割り当てのドライブが少なくとも1本必要です。
- 1つのボリュームグループに含めることができるドライブ容量には制限があります。これらの制限はホストタイプによって異なります。
- シェルフ/ドロワー損失の保護を有効にするには、RAID 1を使用している場合を除き、少なくとも3台のシェルフまたはドロワーに配置されたドライブを使用するボリュームグループを作成する必要があります。

最小のシェルフ/ドロワーは2台です。

- EF600またはEF300ストレージアレイを設定する場合は、各コントローラが最初の12個のスロットと直近の12個のスロットに同じ数のドライブにアクセスできることを確認します。この構成により、コントローラは両方のドライブ側PCIeバスをより効果的に使用できます。現在、ボリュームグループの作成時に、Advanced機能でドライブを選択することができます。

ボリュームグループの容量は、選択するRAIDレベルによって次のように異なります。

- RAID 1を使用する場合は、ドライブを一度に2本ずつ追加してミラーペアを構成する必要があります。ミラーリングとストライピング（RAID 10またはRAID 1+0）は、ドライブを4本以上選択した場合に実装されます。
- RAID 5を使用する場合は、少なくとも3本のドライブを追加してボリュームグループを作成する必要があります。
- RAID 6を使用する場合は、少なくとも5本のドライブを追加してボリュームグループを作成する必要があります。

このタスクについて

ボリュームグループ作成時に、ドライブ数、セキュリティ機能、Data Assurance（DA）機能、シェルフ損失の保護、ドロワー損失の保護など、グループの特性を確認します。

EF600およびEF300ストレージアレイの場合は、リソースのプロビジョニング、ドライブブロックサイズ、ボリュームブロックサイズも設定に含まれます。

> 大容量ドライブとボリュームをコントローラ間で分散させる機能を利用して、1つのボリュームグループに複数のボリュームを作成すると、ストレージ容量を有効に活用してデータを保護するのに役立ちます。

手順

1. Manage（管理）ページで、ボリュームグループのストレージアレイを選択します。
2. メニューを選択します。Provisioning（プロビジョニング）[Configure Pools and Volume Groups]（プールとボリュームグループの構成）。
3. メニュー：Create [Volume group]（ボリュームグループの作成）をクリックします。

   Create Volume Group（ボリュームグループの作成）ダイアログボックスが表示されます。

4. ボリュームグループの名前を入力します。
5. データストレージと保護の要件に最も適したRAIDレベルを選択します。ボリュームグループ候補の表に、選択したRAIDレベルをサポートする候補だけが表示されます。
6. （オプション）ストレージアレイに複数のタイプのドライブがある場合、使用するドライブタイプを選択します。

   ボリュームグループ候補の表に、選択したドライブタイプとRAIDレベルをサポートする候補だけが表示されます。

7. （オプション）ボリュームグループで使用するドライブを自動で定義するか手動で定義するかを選択できます。デフォルトでは、自動方式が選択されています。

ドライブの冗長性と最適なドライブ構成を理解している専門家でない場合は、手動で操作しないでください。

ドライブを手動で選択するには、ドライブを手動で選択する*（アドバンスト）リンクをクリックします。クリックすると、ドライブが自動的に選択されます（アドバンスト）*。

手動方式では、ボリュームグループを構成するドライブを選択できます。未割り当ての特定のドライブを選択して必要な容量を確保することができます。ストレージアレイにメディアタイプやインターフェイスタイプが異なるドライブが含まれている場合、新しいボリュームグループの作成用に選択できるのは1つのドライブタイプの未設定の容量のみです。

8. 表示されたドライブ特性に基づいて、ボリュームグループで使用するドライブを選択し、*作成*をクリックします。

表示されるドライブ特性は、自動方式と手動方式のどちらを選択したかによって異なります。詳細については、SANtricity System Managerのドキュメントを参照してください。 "ボリュームグループを作成します"。

プールまたはボリュームグループに容量を追加します

ドライブを追加することで、既存のプールまたはボリュームグループの空き容量を拡張することができます。

作業を開始する前に

- ドライブのステータスが最適Iである必要があります。
- ドライブタイプ（HDDまたはSSD）が同じである必要があります。
- プールまたはボリュームグループのステータスが最適である必要があります。
- プールまたはボリュームグループに含まれているドライブがいずれもセキュリティ対応ドライブの場合、セキュリティ対応ドライブの暗号化機能を引き続き使用するには、セキュリティ対応のドライブだけを追加します。

セキュリティ対応ドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。

このタスクについて

このタスクでは、プールまたはボリュームグループに含める空き容量を追加できます。この空き容量は追加ボリュームの作成に使用できます。この処理の実行中もボリューム内のデータには引き続きアクセスできます。

プールに一度に追加できるドライブは最大60本です。ボリュームグループに一度に追加できるドライブは最大2本です。最大数を超えるドライブを追加する必要がある場合は、手順 を繰り返します。（プールにはストレージアレイの上限を超えるドライブを含めることはできません）。

ドライブの追加に伴い、予約済み容量の引き上げが必要になる場合があります。拡張処理の実行後にリザーブ容量を増やすことを検討してください。

Data Assurance（DA）に対応していないプールまたはボリュームグループに容量を追加するときは、DA対応のドライブは使用しないでください。DA対応ドライブの機能をプールまたはボリュームグループで利用することはできません。DAに対応していないドライブの使用を検討してください。

手順

1. 管理ページで、プールまたはボリュームグループを含むストレージアレイを選択します。
2. メニューを選択します。Provisioning（プロビジョニング）[Configure Pools and Volume Groups]（プールとボリュームグループの構成）。
3. ドライブを追加するプールまたはボリュームグループを選択し、*容量の追加*をクリックします。

   Add Capacityダイアログボックスが表示されます。プールまたはボリュームグループと互換性がある未割り当てのドライブのみが表示されます。

4. ドライブの選択…*で、既存のプールまたはボリュームグループに追加するドライブを1つ以上選択します。

   ドライブのリストは、より適した未割り当てのドライブから順に表示されます。プールまたはボリュームグループに追加された合計空き容量が、選択した合計容量*のリストの下に表示されます。

フィールドの詳細

フィールド	説明
シェルフ	ドライブのシェルフの場所を示します。
ベイ	ドライブのベイの場所を示します
容量（GiB）	ドライブの容量を示します。 • できるだけ、プールまたはボリュームグループ内の既存のドライブと同じ容量のドライブを選択してください。 • 容量が小さい未割り当てのドライブを追加する必要がある場合は、プールまたはボリュームグループに現在含まれている各ドライブの使用可能容量が削減されることに注意してください。したがって、ドライブ容量はプールまたはボリュームグループ全体で同じになります。 • 容量が大きい未割り当てのドライブを追加する必要がある場合は、現在プールまたはボリュームグループに含まれているドライブの容量に合わせて、追加する未割り当てのドライブの使用可能容量が削減されることに注意してください。
セキュリティ対応	ドライブがセキュリティ対応かどうかを示します。 • プールやボリュームグループはドライブセキュリティ機能を使用して保護できますが、この機能を使用するには、すべてのドライブがセキュリティ対応である必要があります。 • セキュリティ対応とセキュリティ対応でないドライブが混在したプールまたはボリュームグループを作成することは可能ですが、ドライブセキュリティ機能を有効にすることはできません。 • すべてのセキュリティ対応ドライブを備えたプールまたはボリュームグループは、暗号化機能が使用されていない場合でも、スペアリングまたは拡張のために非セキュア対応ドライブを受け入れることはできません。 • セキュリティ対応ドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。FIPSドライブは、レベル140-2または140–3のいずれかで、レベル140-3がより高いセキュリティレベルです。140-2レベルと140-3レベルのドライブを組み合わせて選択した場合、プールまたはボリュームグループは下位のセキュリティレベル（140-2）で動作します。

フィールド	説明
DA対応	ドライブがData Assurance（DA）対応かどうかを示します。 • DAに対応していないドライブを使用してDAに対応したプールまたはボリュームグループに容量を追加することは推奨されません。プールまたはボリュームグループのDA機能は無効になり、プールまたはボリュームグループに新たに作成したボリュームでDAを有効にすることもできなくなります。 • DA対応のドライブを使用してDAに対応していないプールまたはボリュームグループに容量を追加することは推奨されません。DA対応ドライブの機能をプールまたはボリュームグループで利用することはできないためです（ドライブの属性が一致しません）。DAに対応していないドライブの使用を検討してください。
DULBE対応	ドライブにDeallocated or Unwritten Logical Block Error（DULBE）に対応したオプションがあるかどうかを示します。DULBEはNVMeドライブのオプションです。このオプションにより、EF300またはEF600ストレージアレイでリソースプロビジョニングボリュームをサポートできます。

5. [追加（ Add ）] をクリックします。

   プールまたはボリュームグループにドライブを追加する場合、プールまたはボリュームグループの次の属性が無効になるようなドライブを選択すると、確認のダイアログボックスが表示されます。

   - シェルフ損失の保護
   - ドロワー損失の保護
   - Full Disk Encryption機能
   - Data Assurance機能
   - DULBE機能

6. 続行するには、[はい]をクリックします。それ以外の場合は、[キャンセル]をクリックします。

結果

プールまたはボリュームグループに未割り当てのドライブを追加したあと、追加のドライブを含めるためにプールまたはボリュームグループの各ボリューム内のデータが再配置されます。

SSDキャッシュを作成する

システムパフォーマンスを向上させるために、SSDキャッシュ機能を使用して、アクセス頻度が特に高いデータ（「ホット」データ）を低レイテンシのソリッドステートドライブ（SSD）にキャッシュすることができます。SSDキャッシュは、ホスト読み取りにのみ使用されます。

作業を開始する前に

ストレージアレイにSSDドライブが含まれている必要があります。

SSDキャッシュは、EF600またはEF300ストレージシステムでは使用できません。

このタスクについて

SSDキャッシュを作成するときは、1つまたは複数のドライブを使用することができます。読み取りキャッシュはストレージアレイ内にあるため、ストレージアレイを使用するすべてのアプリケーションでキャッシュが共有されます。キャッシュするボリュームを選択すると、あとは動的に自動でキャッシングが実行されます。

SSDキャッシュを作成する際は、次のガイドラインに従ってください。

- SSDキャッシュのセキュリティを有効にできるのは作成時だけで、あとから有効にすることはできません。
- SSDキャッシュはストレージアレイごとに1つだけサポートされます。
- ストレージアレイ上で使用可能なSSDキャッシュの最大容量は、コントローラのプライマリキャッシュ容量によって異なります。
- SSDキャッシュはSnapshotイメージではサポートされません。
- SSDキャッシュが有効になっているボリュームや無効になっているボリュームをインポートまたはエクスポートしても、キャッシュデータはインポートまたはエクスポートされません。
- コントローラのSSDキャッシュを使用するように割り当てられたボリュームは、自動ロードバランシングによる転送の対象外となります。
- 関連するボリュームがセキュリティ有効の場合は、セキュリティ有効のSSDキャッシュを作成してください。

手順

1. Manage（管理）ページで、キャッシュのストレージアレイを選択します。
2. メニューを選択します。Provisioning（プロビジョニング）[Configure Pools and Volume Groups]（プールとボリュームグループの構成）。
3. メニューをクリックします：Create [SSD Cache]。

   SSDキャッシュの作成ダイアログボックスが表示されます。

4. SSDキャッシュの名前を入力します。
5. 次の特性に基づいて使用するSSDキャッシュ候補を選択します。

フィールドの詳細

特性	使用
容量	使用可能な容量がGiB単位で表示されます。アプリケーションのストレージニーズに合わせて容量を選択します。SSDキャッシュの最大容量は、コントローラのプライマリキャッシュ容量によって異なります。SSDキャッシュに最大容量を超える容量を割り当てた場合、超過した容量は使用できません。SSDキャッシュの容量は、全体の割り当て容量にカウントされます。
合計ドライブ数	このSSDキャッシュで使用できるドライブの数を示します。必要なドライブ数のSSD候補を選択します
セキュリティ対応	SSDキャッシュがセキュリティ対応ドライブだけで構成されているかどうかを示します。セキュリティ対応ドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。セキュリティ有効SSDキャッシュを作成する場合は、「セキュア対応」列で「はい- FDE」または「はい- FIPS」を探します。
セキュリティを有効化	セキュリティ対応ドライブでドライブセキュリティ機能を有効にするオプションです。セキュリティ有効SSDキャッシュを作成する場合は、*セキュリティを有効にする*チェックボックスをオンにします。注：一度有効にすると、セキュリティを無効にすることはできません。SSDキャッシュのセキュリティを有効にできるのは作成時だけで、あとから有効にすることはできません。
DA対応	このSSDキャッシュ候補でData Assurance（DA）を使用できるかどうかを示します。Data Assurance（DA）は、データがコントローラ経由でドライブに転送される際に発生する可能性があるエラーをチェックして修正します。DAを使用する場合は、DAに対応したSSDキャッシュ候補を選択します。このオプションはDA機能が有効になっている場合にのみ使用できます。SSDキャッシュにはDAに対応したドライブとDAに対応していないドライブの両方を含めることができますが、DAを使用するためにはすべてのドライブがDAに対応している必要があります。

6. SSD読み取りキャッシュを実装するボリュームにSSDキャッシュを関連付けます。互換性のあるボリュームでSSDキャッシュをすぐに有効にするには、*ホストにマップされている既存の互換性のあるボリュームでSSDキャッシュを有効にする*チェックボックスをオンにします。

   互換性があるボリュームとは、ドライブセキュリティ機能とDA機能の設定が同じボリュームです。

7. [作成（ Create ）] をクリックします。

プールの設定を変更します

プールの名前、容量アラートの設定、変更の優先順位、予約済み容量などのプールの設定を編集できます。

このタスクについて

このタスクでは、プールの構成設定を変更する方法について説明します。

プラグインインターフェイスを使用してプールのRAIDレベルを変更することはできません。プラグインは、プールを自動的にRAID 6として構成します。

手順

1. [管理]ページで、プールがあるストレージアレイを選択します。
2. メニューを選択します。Provisioning（プロビジョニング）[Configure Pools and Volume Groups]（プールとボリュームグループの構成）。
3. 編集するプールを選択し、*表示/設定の編集*をクリックします。

   Pool Settings（プール設定）ダイアログボックスが表示されます。

4. [設定]タブを選択し、必要に応じてプール設定を編集します。

フィールドの詳細

設定	説明
名前	ユーザが指定したプールの名前を変更できます。プールの名前は必ず指定する必要があります。
容量アラート	プールの空き容量が指定したしきい値以上になったときにアラート通知を送信できます。プールに格納されたデータが指定したしきい値を超えると、プラグインはメッセージを送信します。このため、ストレージスペースを追加したり、不要なオブジェクトを削除したりすることができます。アラートは、ダッシュボードの通知領域に表示され、サーバから管理者にEメールおよびSNMPトラップメッセージで送信できます。次の容量アラートを定義できます。 • 重大アラート：プールの空き容量が指定したしきい値以上になったときに通知されます。しきい値の割合はスピンボックスで調整できます。この通知を無効にするには、チェックボックスをオンにします。 • 早期アラート：プールの空き容量が指定したしきい値に達したときに通知されます。しきい値の割合はスピンボックスで調整できます。この通知を無効にするには、チェックボックスをオンにします。
修正の優先順位	システムパフォーマンスと比較したプールの変更処理の優先度レベルを指定できます。プールの変更処理の優先度を高くすると処理は高速に完了しますが、ホストのI/Oパフォーマンスは低下します。優先度を低くすると処理には時間がかかりますが、ホストのI/Oパフォーマンスへの影響は小さくなります。優先度レベルは、lowest、low、medium、high、highestの5つから選択できます。優先度レベルが高いほど、ホストのI/Oパフォーマンスとシステムパフォーマンスへの影響は大きくなります。 • 重大の再構築優先度-このスライダバーは、複数のドライブに障害が発生した場合のデータ再構築処理の優先度を決定します。この状況では、一部のデータの冗長性が失われ、別のドライブ障害が発生した場合はデータの損失を招くおそれがあります。 • デグレード再構築優先度-このスライダバーは、ドライブ障害が発生した場合のデータ再構築処理の優先度を決定します。この状況では、データの冗長性は失われておらず、別のドライブ障害が発生してもデータの損失が発生することはありません。 • バックグラウンド処理の優先度-このスライダバーは、プールが最適な状態のときに実行されるバックグラウンド処理の優先度を決定します。たとえば、Dynamic Volume Expansion（DVE）、Instant Availability Format（IAF）、交換または追加したドライブへのデータの移行などがあります。

設定	説明
予約済み容量（EF600またはEF300の場合は「最適化容量」）	予約済み容量-ドライブ数を定義して、ドライブ障害に備えてプールに確保されている容量を特定できます。ドライブ障害が発生すると、予約済み容量を使用して再構築されたデータが格納されます。プールのデータ再構築プロセスでは、ボリュームグループで使用されるホットスペアドライブではなく、予約済み容量が使用されます。ドライブ数はスピンボックスで調整します。指定したドライブ数に応じて、スピンボックスの横にプールの予約済み容量が表示されます。予約済み容量については、次の点に注意してください。 • 予約済み容量はプールの合計空き容量から差し引かれるため、確保する容量がボリュームの作成に使用できる空き容量に影響します。予約済み容量に0を指定すると、プールのすべての空き容量がボリュームの作成に使用されます。 • 予約済み容量を減らすと、プールボリュームに使用できる容量が増えます。 追加の最適化容量（**EF600**および**EF300**アレイのみ）--プールの作成時に、使用可能容量とパフォーマンスおよびドライブ寿命とのバランスが取れた、推奨される最適化容量が生成されます。このバランスを調整するには、使用可能容量を犠牲にしてパフォーマンスの向上とドライブ寿命の延長を図る場合はスライダを右に、パフォーマンスとドライブ寿命を犠牲にして使用可能容量を増やす場合は左に動かします。SSDドライブでは、その容量の一部が未割り当ての場合に寿命が長くなり、最大書き込みパフォーマンスが向上します。プールに関連付けられているドライブの未割り当て容量は、プールの予約済み容量、空き容量（ボリュームで使用されていない容量）、および使用可能容量のうちの最適化容量として確保された容量で構成されます。この最適化容量は使用可能容量を減らすことで最小レベルの最適化容量を確保するため、ボリュームの作成には使用できません。

5. [保存（ Save ）] をクリックします。

ボリュームグループの設定を変更します

名前やRAIDレベルなど、ボリュームグループの設定を編集できます。

作業を開始する前に

ボリュームグループにアクセスするアプリケーションが必要とするパフォーマンスを確保できるようにRAIDレベルを変更する場合は、次の前提条件を満たしていることを確認してください。

- ボリュームグループのステータスが最適である必要があります。
- ボリュームグループに、新しいRAIDレベルに変換するための十分な容量が必要です。

手順

1. 管理ページで、ボリュームグループを含むストレージアレイを選択します。
2. メニューを選択します。Provisioning（プロビジョニング）[Configure Pools and Volume Groups]（プールとボリュームグループの構成）。

3. 編集するボリュームグループを選択し、*表示/設定の編集*をクリックします。

   Volume Group Settings（ボリュームグループ設定）ダイアログボックスが表示されます。

4. 「* Settings *」（設定）タブを選択し、必要に応じてボリュームグループの設定を編集します。

フィールドの詳細

設定	説明
名前	ユーザが指定したボリュームグループの名前を変更できます。ボリュームグループの名前は必ず指定する必要があります。
RAIDレベル	ドロップダウンメニューから新しいRAIDレベルを選択します。 • **RAID 0**ストライピング--ハイパフォーマンスを提供しますが'データの冗長性は提供しませんボリュームグループ内の1本のドライブで障害が発生すると、関連付けられているすべてのボリュームで障害が発生し、すべてのデータが失われます。ストライピングRAIDグループは、2つ以上のドライブを1つの大容量論理ドライブにまとめます。 • **RAID 1**ミラーリング--高いパフォーマンスと最高のデータ可用性を提供し、企業レベルまたは個人レベルで機密データを保存するのに適しています。一方のドライブの内容をミラーペアのもう一方のドライブに自動的にミラーリングすることで、データを保護します。単一のドライブ障害からの保護を提供します。 • **RAID 10**ストライピング/ミラーリング-- RAID 0 (ストライピング)とRAID 1(ミラーリング)を組み合わせたもので'4台以上のドライブを選択した場合に実現されますRAID 10は、高いパフォーマンスとフォールトトレランスが必要な、データベースなどの大量のトランザクションを処理するアプリケーションに適しています。 • **RAID 5**--標準的なI/Oサイズが小さく読み取り処理の割合が高いマルチユーザー環境(データベースやファイルシステムストレージなど)に最適 • **RAID 6**-- RAID 5を超える冗長性を必要とするが'高い書き込みパフォーマンスは必要としない環境に最適ですRAID 3をボリュームグループに割り当てるには、コマンドラインインターフェイスを使用する必要があります。RAIDレベルの変更はキャンセルできません。変更中もデータは引き続き使用できます。
最適化容量（EF600アレイのみ）	ボリュームグループの作成時に、使用可能容量とパフォーマンスおよびドライブの寿命とのバランスに基づいて、推奨される最適化容量が決定されます。このバランスを調整するには、使用可能容量を犠牲にしてパフォーマンスの向上とドライブ寿命の延長を図る場合はスライダを右に、パフォーマンスとドライブ寿命を犠牲にして使用可能容量を増やす場合は左に動かします。SSDドライブでは、その容量の一部が未割り当ての場合に寿命が長くなり、最大書き込みパフォーマンスが向上します。ボリュームグループに関連付けられているドライブの未割り当て容量は、グループの空き容量（ボリュームで使用されていない容量）と、使用可能容量のうちの最適化容量として確保された容量で構成されます。この最適化容量は使用可能容量を減らすことで最小レベルの最適化容量を確保するため、ボリュームの作成には使用できません。

5. [保存（ Save ）] をクリックします。

RAIDレベルの変更によって容量が減ったり、ボリュームの冗長性が失われたり、シェルフ/ドロワー損失の保

護が失われた場合は、確認ダイアログボックスが表示されます。続行するには*はい*を選択し、続行しない場合は*いいえ*をクリックします。

結果

ボリュームグループのRAIDレベルを変更すると、プラグインはボリュームグループを構成するすべてのボリュームのRAIDレベルを変更します。処理の実行中は、パフォーマンスが若干低下することがあります。

SSDキャッシュの設定を変更する

SSDキャッシュの名前を編集し、そのステータス、最大容量と現在の容量、ドライブセキュリティとData Assuranceのステータス、および関連付けられているボリュームとドライブを表示できます。

この機能は、EF600またはEF300ストレージシステムでは使用できません。

手順

1. 管理ページで、SSDキャッシュを搭載したストレージアレイを選択します。
2. メニューを選択します。Provisioning（プロビジョニング）[Configure Pools and Volume Groups]（プールとボリュームグループの構成）。
3. 編集するSSDキャッシュを選択し、*表示/設定の編集*をクリックします。

   SSD Cache Settings（SSDキャッシュ設定）ダイアログボックスが表示されます。

4. SSDキャッシュ設定を確認するか、必要に応じて編集します。

フィールドの詳細

設定	説明
名前	SSDキャッシュの名前が表示されます。この名前は変更できます。SSDキャッシュの名前は必ず指定する必要があります。
特性	SSDキャッシュのステータスが表示されます。ステータスは次のいずれかです。 • 最適 • 不明です • デグレード • 失敗（重大なMELイベントが生成されます） • 中断しました
容量	SSDキャッシュの現在の容量と使用可能な最大容量が表示されます。SSDキャッシュの最大容量は、コントローラのプライマリキャッシュサイズによって異なります。 • 1 GiB以下 • 1GiBから2GiB • 2GiB ~ 4GiB • 4 GiB超
セキュリティおよびDA	SSDキャッシュのドライブセキュリティとData Assuranceのステータスが表示されます。 • セキュリティ対応-- SSDキャッシュがセキュリティ対応ドライブだけで構成されているかどうかを示しますセキュリティ対応ドライブは自己暗号化ドライブで、データを不正アクセスから保護できます。 • * Secure-enabled *- SSDキャッシュでセキュリティが有効になっているかどうかを示します。 • *DA Capable *-- SSDキャッシュがDA対応ドライブだけで構成されているかどうかを示しますDA対応ドライブでは、ホストとストレージアレイの間でデータをやり取りするときに発生する可能性があるエラーをチェックして修正できます。
関連付けられているオブジェクト	SSDキャッシュに関連付けられているボリュームとドライブが表示されます。

5. [保存（ Save ）] をクリックします。

SSDキャッシュの統計を表示します

SSDキャッシュについて、読み取り、書き込み、キャッシュヒット、キャッシュ割り当ての割合、 キャッシュ使用率です。

この機能は、EF600またはEF300ストレージシステムでは使用できません。

このタスクについて

詳細統計のサブセットである一般統計は、View SSD Cache Statisticsダイアログボックスに表示されます。SSDキャッシュの詳細統計は、すべてのSSD統計を.csvファイルにエクスポートした場合にのみ表示できます。

統計を確認および解釈する際には、複数の統計を組み合わせることで見えてくる情報もあることに注意してください。

手順

1. 管理ページで、SSDキャッシュを搭載したストレージアレイを選択します。
2. メニューを選択します。Provisioning（プロビジョニング）[Configure Pools and Volume Groups]（プールとボリュームグループの構成）。
3. 統計を表示するSSDキャッシュを選択し、メニューをクリックします。More [View SSD Cache] statistics

   View SSD Cache Statistics（SSDキャッシュ統計の表示）ダイアログボックスが表示され、選択したSSDキャッシュの公称統計が表示されます。

フィールドの詳細

設定	説明
読み取り	SSDキャッシュが有効なボリュームに対するホストの読み取りの合計数が表示されます。書き込みに対する読み取りの比率が大きいほど、キャッシュ処理が向上します。
書き込み	SSDキャッシュが有効なボリュームに対するホストの書き込みの合計数。書き込みに対する読み取りの比率が大きいほど、キャッシュ処理が向上します。
キャッシュヒット	キャッシュヒット数が表示されます。
キャッシュヒット率	キャッシュヒット率が表示されます。この値は、「キャッシュヒット数/（読み取り数+書き込み数）」の式で算出されます。効果的なSSDキャッシュ処理には、キャッシュヒットの割合が50%より高いことが必要です。
キャッシュ割り当て率	割り当てられているSSDキャッシュストレージの割合が表示されます。この値は、このコントローラで使用できるSSDキャッシュストレージの割合で表したもので、割り当てられているバイト数/使用可能なバイト数から導き出されます。
キャッシュ使用率	有効なボリュームのデータが格納されているSSDキャッシュストレージの割合が表示されます。この値は、割り当てられているSSDキャッシュストレージの割合で表したものです。この値はSSDキャッシュの利用率または密度を表し、割り当てられたバイト数を使用可能なバイト数で割った値です。
すべてエクスポート（**Export All**）	SSDキャッシュのすべての統計をCSV形式にエクスポートします。エクスポートされたファイルには、SSDキャッシュの使用可能なすべての統計（一般統計と詳細統計の両方）が含まれます。

4. 「キャンセル」をクリックして、ダイアログボックスを閉じます。

ボリュームの冗長性をチェックします

テクニカルサポートから指示があった場合やRecovery Guruに記載されている場合は、プールまたはボリュームグループ内のボリュームの冗長性をチェックし、そのボリュームのデータに整合性があるかどうかを確認できます。

冗長性データは、プールまたはボリュームグループ内のいずれかのドライブで障害が発生した場合に、交換用ドライブに迅速に情報を再構築するために使用されます。

作業を開始する前に

- プールまたはボリュームグループのステータスが最適である必要があります。
- プールまたはボリュームグループで実行中の変更処理がないことを確認する必要があります。
- RAID 0にはデータの冗長性がないため、RAID 0以外のすべてのRAIDレベルで冗長性をチェックできます。（プールはRAID 6としてのみ構成されます）。

ボリュームの冗長性チェックは、Recovery Guruに記載されている場合にかぎり、テクニカルサポートの指示に従って実行してください。

このタスクについて

このチェックは、一度に1つのプールまたはボリュームグループでのみ実行できます。ボリュームの冗長性チェックでは、次の処理が実行されます。

- RAID 3ボリューム、RAID 5ボリューム、またはRAID 6ボリューム内のデータブロックがスキャンされ、各ブロックの冗長性情報がチェックされます。（RAID 3をボリュームグループに割り当てるには、コマンドラインインターフェイスを使用する必要があります）。
- RAID 1のミラーリングされたドライブ上のデータブロックが比較されます。
- コントローラファームウェアがデータに整合性がないと判断した場合は、冗長性エラーが返されます。

> 同じプールまたはボリュームグループですぐに冗長性チェックを実行すると、原因 でエラーが発生する場合があります。この問題を回避するには、同じプールまたはボリュームグループで別の冗長性チェックを実行する前に、1~2分待ってください。

手順

1. 管理ページで、プールまたはボリュームグループを含むストレージアレイを選択します。
2. メニューを選択します。Provisioning（プロビジョニング）[Configure Pools and Volume Groups]（プールとボリュームグループの構成）。
3. メニューから[一般的でないタスク]を選択します。[ボリュームの冗長性をチェック]。

   [Check Redundancy]ダイアログボックスが表示されます。

4. チェックするボリュームを選択し、checkと入力して、この処理を実行することを確定します。
5. [*チェック（Check）]をクリックする。

   ボリュームの冗長性チェック処理が開始されます。プールまたはボリュームグループ内のボリュームが、ダイアログボックスの表の一番上から順番にスキャンされます。各ボリュームがスキャンされるたびに、次の操作が実行されます。

   - ボリュームテーブルでボリュームが選択されます。
   - 冗長性チェックのステータスがStatus列に表示されます。
   - メディアエラーまたはパリティエラーが発生するとチェックが停止され、エラーが報告されます。次の表に、冗長性チェックのステータスの詳細を示します。

フィールドの詳細

ステータス	説明
保留中です	これはスキャン対象の最初のボリュームです。冗長性チェックを開始するには、Start（開始）をクリックしていません。-or -プールまたはボリュームグループ内の他のボリュームで冗長性チェック処理が実行されています。
チェック中です	ボリュームは冗長性チェック中です。
合格	ボリュームは冗長性チェックにパスしました。冗長性情報に不整合は見つかりませんでした。
失敗しました	ボリュームは冗長性チェックに失敗しました。冗長性情報に不整合が見つかりました。
メディアエラー	ドライブメディアが故障しており、読み取り不能です。Recovery Guruに表示される手順に従います。
パリティエラー	データの一部でパリティが想定される値ではありません。パリティエラーは深刻な問題を招く可能性があり、原因 によってデータが永久に失われる可能性があります。

6. プールまたはボリュームグループ内の最後のボリュームをチェックした後、「* Done *」をクリックします。

プールまたはボリュームグループを削除します

プールまたはボリュームグループを削除して未割り当て容量を増やし、アプリケーションのストレージニーズを満たすように再構成することができます。

作業を開始する前に

- プールまたはボリュームグループに含まれるすべてのボリューム上のデータをバックアップしておく必要があります。
- すべての入出力（I/O）を停止しておく必要があります。
- ボリュームのファイルシステムをアンマウントする必要があります。
- プールまたはボリュームグループのミラー関係を削除しておく必要があります。
- プールまたはボリュームグループに対して実行中のボリュームコピー処理を停止しておく必要があります。
- プールまたはボリュームグループが非同期ミラーリング処理の対象になっていないことを確認する必要があります。
- ボリュームグループのドライブに永続的予約が設定されていないことを確認する必要があります。

手順

1. 管理ページで、プールまたはボリュームグループを含むストレージアレイを選択します。
2. メニューを選択します。Provisioning（プロビジョニング）[Configure Pools and Volume Groups]（プールとボリュームグループの構成）。
3. リストからプールまたはボリュームグループを1つ選択します。

プールまたはボリュームグループは一度に1つだけ選択できます。リストを下にスクロールして、他のプールまたはボリュームグループを確認します。

4. [メニュー]、[一般的でないタスク]、[削除]の順に選択し、確認します

結果

システムは次の処理を実行します。

- プールまたはボリュームグループ内のすべてのデータを削除します。
- プールまたはボリュームグループに関連付けられているすべてのドライブを削除します。
- 関連付けられているドライブの割り当てを解除し、新規または既存のプールやボリュームグループで再利用できるようにします。

ボリュームグループの空き容量を統合します

選択したボリュームグループ上の既存の空きエクステントを統合するには、空き容量の統合オプションを使用します。この操作を実行すると、追加ボリュームを作成する際にボリュームグループ内の空き容量を最大限使用できるようになります。

作業を開始する前に

- ボリュームグループに少なくとも1つの空き容量領域が含まれている必要があります。
- ボリュームグループ内のすべてのボリュームがオンラインで、ステータスが最適Iである必要があります。
- ボリュームのセグメントサイズの変更など、実行中のボリューム変更処理がないことを確認してください。

このタスクについて

この処理は開始後にキャンセルすることはできません。統合処理の実行中もデータには引き続きアクセスできます。

次のいずれかの方法を使用して、[Consolidate Free Capacity]ダイアログボックスを起動できます。

- ボリュームグループに対して1つ以上の空き容量領域が検出されると、通知領域のホームページに空き容量の統合に関する推奨事項が表示されます。[空き容量の統合（Consolidate free capacity）]リンクをクリックして、ダイアログボックスを起動します。
- 次のタスクで説明するように、[Pools & Volume Groups]ページから[Consolidate Free Capacity]ダイアログボックスを起動することもできます。

空き容量領域についての詳細はこちらをご覧ください

空き容量領域は、ボリュームを削除した場合や、ボリュームの作成時に使用可能なすべての空き容量を使用しなかった場合に発生する空き容量です。1つ以上の空き容量領域があるボリュームグループでボリュームを作成する場合、ボリュームの容量はそのボリュームグループ内で最も大きい空き容量領域以内に制限されます。たとえば、ボリュームグループに合計15GiBの空き容量があり、最も大きい空き容量領域が10GiBであるとすると、作成できるボリュームのサイズは最大10GiBです。

ボリュームグループの空き容量を統合すると、書き込みパフォーマンスが向上します。ボリュームグループの空き容量は、ホストがファイルを書き込み、変更、削除するうちに徐々に断片化されていきます。最終的に、使用可能な容量は1つの連続したブロックに存在するのではなく、小さなフラグメントに分断されてボリュームグループ全体に分散した状態になります。これにより、ホストは新しいファイルを空きクラスタの使用可能な範囲に収まるフラグメントとして書き込む必要があるため、ファイルの断片化がさらに進みます。

選択したボリュームグループの空き容量を統合することで、ホストが新しいファイルを書き込む際のファイルシステムのパフォーマンスが向上します。また、統合プロセスは、新しいファイルが以降に断片化されないようにするのにも役立ちます。

手順

1. 管理ページで、ボリュームグループを含むストレージアレイを選択します。
2. メニューを選択します。Provisioning（プロビジョニング）[Configure Pools and Volume Groups]（プールとボリュームグループの構成）。
3. 統合する空き容量があるボリュームグループを選択し、メニューから「Uncommon Tasks [ボリュームグループの空き容量を統合する]」を選択します。

   [Consolidate Free Capacity]ダイアログボックスが表示されます。

4. この操作を実行するかどうかを確認するには’consolidateと入力します
5. [*統合（Consolidate）]をクリックし

結果

ボリュームグループの空き容量領域の統合（デフラグ）が開始され、以降のストレージ設定タスク用に1つの連続した容量になります。

完了後

ナビゲーションサイドバーで、* Operations *を選択して、空き容量の統合操作の進行状況を表示します。この処理には時間がかかることがあり、システムのパフォーマンスに影響する可能性があります。

ロケーターライトを点灯します

ドライブを検索して、選択したプール、ボリュームグループ、またはSSDキャッシュを構成するすべてのドライブを物理的に特定できます。選択したプール、ボリュームグループ、またはSSDキャッシュ内の各ドライブのLEDインジケータが点灯します。

手順

1. 管理ページで、ストレージアレイを選択します。

2. メニューを選択します。Provisioning（プロビジョニング）[Configure Pools and Volume Groups]（プールとボリュームグループの構成）。
3. 特定するプール、ボリュームグループ、またはSSDキャッシュを選択し、メニューをクリックします。More [ロケーターライトを点灯]。

   選択したプール、ボリュームグループ、またはSSDキャッシュを構成するドライブのライトが点灯されたことを示すダイアログボックスが表示されます。

4. ドライブが正常に検出されたら、*電源をオフにする*をクリックします。

容量を削除

ドライブを削除することで、既存のプールまたはSSDキャッシュの容量を減らすことができます。

ドライブを削除したあと、プールまたはSSDキャッシュの各ボリューム内のデータは残りのドライブに再配置されます。削除されたドライブは割り当てが解除され、その容量はストレージアレイの合計空き容量に加算されます。

このタスクについて

容量を削除する際のガイドラインを次に示します。

- SSDキャッシュ内の最後のドライブを削除するには、まずSSDキャッシュを削除する必要があります。
- プール内のドライブの数を11本より少なくすることはできません。
- 一度に削除できるドライブは最大12本です。12本を超えるドライブを削除する必要がある場合は、手順を繰り返します。
- 削除したドライブのデータがプールまたはSSDキャッシュ内の残りのドライブに再配置される際に、プールまたはSSDキャッシュにそのデータを十分に格納できる空き容量がない場合、ドライブは削除できません。

パフォーマンスへの影響は次のとおりです。

- プールまたはSSDキャッシュからドライブを削除すると、ボリュームのパフォーマンスが低下する可能性があります。
- プールまたはSSDキャッシュから容量を削除しても、予約済み容量は消費されません。ただし、プールまたはSSDキャッシュに残っているドライブの数に基づいて、予約済み容量が減少する可能性があります。

セキュリティ対応ドライブには、次のような影響があります。

- セキュリティ対応でない最後のドライブを削除すると、プール内に残るのはすべてセキュリティ対応のドライブになります。この場合、プールのセキュリティを有効にするオプションが表示されます。
- Data Assurance（DA）対応でない最後のドライブを削除すると、プール内に残るのはすべてDA対応のドライブになります。
- このプールに作成する新しいボリュームはすべてDA対応になります。既存のボリュームをDA対応にする場合は、ボリュームを削除してから再作成する必要があります。

手順

1. 管理ページで、ストレージアレイを選択します。

メニューを選択します。Provisioning（プロビジョニング）[Configure Pools and Volume Groups]（プールとボリュームグループの構成）。

2. プールまたはSSDキャッシュを選択し、メニューをクリックします。More [容量の削除]

   Remove Capacityダイアログボックスが表示されます。

3. リストから1つ以上のドライブを選択します。

   リストでドライブを選択または選択解除すると、選択した容量の合計フィールドが更新されます。このフィールドには、選択したドライブを削除後のプールまたはSSDキャッシュの合計容量が表示されます。

4. [*削除]をクリックし、ドライブを削除することを確認します。

結果

プールまたはSSDキャッシュの新しく削減された容量は、プールおよびボリュームグループビューに反映されます。

プールまたはボリュームグループのセキュリティを有効にします

プールまたはボリュームグループのドライブセキュリティを有効にして、プールまたはボリュームグループに含まれているドライブ上のデータへの不正アクセスを防止できます。

ドライブの読み取りおよび書き込みアクセスは、セキュリティキーが設定されたコントローラからのみ可能です。

作業を開始する前に

- ドライブセキュリティ機能を有効にする必要があります。
- セキュリティキーを作成する必要があります。
- プールまたはボリュームグループの状態が最適Iである必要があります。
- プールまたはボリュームグループ内のすべてのドライブがセキュリティ対応である必要があります。

このタスクについて

ドライブセキュリティを使用する場合は、セキュリティ対応のプールまたはボリュームグループを選択します。プールまたはボリュームグループにはセキュリティ対応とセキュリティ対応でないドライブの両方を含めることができますが、暗号化機能を使用するためにはすべてのドライブがセキュリティ対応である必要があります。

一度有効にしたセキュリティを解除するには、プールまたはボリュームグループを削除してからドライブを消去する必要があります。

手順

1. 管理ページで、プールまたはボリュームグループを含むストレージアレイを選択します。
2. メニューを選択します。Provisioning（プロビジョニング）[Configure Pools and Volume Groups]（プールとボリュームグループの構成）。
3. セキュリティを有効にするプールまたはボリュームグループを選択し、[メニュー:その他のセキュリティの有効化]をクリックします。

[セキュリティの有効化の確認]ダイアログボックスが表示されます。

4. 選択したプールまたはボリュームグループのセキュリティを有効にすることを確認し、*有効*をクリックします。

vCenter 向けストレージプラグインを削除します

vCenter Server Appliance からプラグインを削除し、アプリケーションホストからプラグイン Web サーバをアンインストールできます。

これらは、任意の順序で実行できる 2 つのステップです。ただし、プラグインの登録を解除する前にプラグイン Web サーバをアプリケーションホストから削除することを選択した場合、登録スクリプトはその処理中に削除され、方法 1 を使用して登録を解除することはできません。

vCenter Server Appliance からプラグインの登録を解除します

vCenter Server Appliance からプラグインの登録を解除するには、次のいずれかの方法を選択します。

- [方法1:登録スクリプトを実行します]
- 方法2：vCenter Serverのモブページを使用する

方法**1:**登録スクリプトを実行します

1. コマンドラインでプロンプトを開き、次のディレクトリに移動します。

   `< インストールディレクトリ >\vcenter-register-bin'

2. 「 vcenter-register.bat 」ファイルを実行します。

   vcenter-register.bat

   ```
   -action unregisterPlugin^

   -vcenterHostname <vCenter FQDN>^

   -username <Administrator Username>^
   ```

3. スクリプトが正常に実行されたことを確認します。

   ログは '%install_dir%/working/logs/vc-registration.log' に保存されます

方法**2：vCenter Server**のモブページを使用する

1. Web ブラウザを開き、次の URL を入力します。

   https://<FQDN[] vCenter Server の数 >/mob

2. 管理者のクレデンシャルでログインします。
3. extensionManager のプロパティ名を探し ' そのプロパティに関連付けられているリンクをクリックします

4. [* 詳細 * …] をクリックして、プロパティリストを展開します。 リンクをクリックします。
5. 拡張子「 plugin.netapp.eseries` 」がリストに含まれていることを確認します。
6. このメソッドが存在する場合は 'UnregisterExtension' メソッドをクリックします
7. ダイアログに「 plugin.netapp.eseries` 」という値を入力し、 * invoke method * をクリックします。
8. ダイアログを閉じ、 Web ブラウザをリフレッシュします。
9. plugin.netapp.eseries` 拡張子がリストにないことを確認します

> この手順は、 vCenter Server Appliance からプラグインの登録を解除しますが、サーバからプラグインパッケージファイルを削除することはありません。パッケージファイルを削除するには、SSHを使用してvCenter Server Applianceにアクセスし、「etc/vmware/vsphere-clientui/vc-packages/vsphere-client-serenity」ディレクトリに移動します。次に、プラグインに関連付けられているディレクトリを削除します。

アプリケーションホストからプラグイン **Web** サーバを削除します

プラグインソフトウェアをアプリケーションホストから削除するには、次の手順を実行します。

1. アプリケーションサーバーから、 * コントロールパネル * に移動します。
2. 「 * Apps & Features * 」に移動し、「 * SANtricity Storage Plugin for vCenter * 」を選択します。
3. [アンインストール / 変更 *] をクリックします。

   確認ダイアログが開きます。

4. [アンインストール] をクリックします。

   アンインストールが完了すると、確認メッセージが表示されます。

5. [完了（ Done ）] をクリックします。

よくある質問です

どの設定がインポートされますか？

設定のインポート機能は、1つのストレージアレイから複数のストレージアレイに構成をロードするバッチ処理です。

この処理でインポートされる設定は、System Managerでソースストレージアレイがどのように設定されているかによって異なります。複数のストレージアレイにインポートできる設定は次のとおりです。

- **Email alerts**--メールサーバのアドレスとアラート受信者の電子メールアドレスを設定します
- **Syslog**アラート-- syslogサーバのアドレスとUDPポートを含む設定。
- *snmp alerts *-- SNMPサーバのコミュニティ名とIPアドレスを含む設定。
- * AutoSupport *--個別の機能（Basic AutoSupport 、AutoSupport OnDemand、Remote Diagnostics）、メンテナンス時間、配信方法、 およびディスパッチスケジュール。

- ディレクトリサービス-- LDAP (Lightweight Directory Access Protocol)サーバーのドメイン名とURL、およびLDAPサーバーのユーザーグループとストレージアレイの定義済みロールとのマッピングが含まれます。
- ストレージ構成--ボリューム(リポジトリボリューム以外のシックボリュームのみ)、ボリュームグループ、プール、およびホットスペアドライブの割り当てが含まれます。
- システム設定--ボリュームのメディアスキャン設定、コントローラのSSDキャッシュ、および自動ロードバランシングが含まれます(ホスト接続レポートは含まれません)。

ストレージアレイが一部表示されないのはなぜですか？

設定のインポート処理の際、ターゲットの選択ダイアログボックスに一部のストレージアレイが表示されないことがあります。

ストレージアレイが表示されない理由は次のとおりです。

- ファームウェアのバージョンが8.50未満である。
- ストレージアレイがオフラインになっている。
- システムがそのアレイと通信できません（アレイに証明書、パスワード、ネットワークの問題がある場合など）。

これらのボリュームがワークロードに関連付けられていないのはなぜですか？

ボリュームをコマンドラインインターフェイス（CLI）を使用して作成した場合や別のストレージアレイから移行（インポート/エクスポート）した場合、それらのボリュームはワークロードに関連付けられません。

選択したワークロードはボリュームの作成にどのように影響しますか？

ボリュームの作成中に、ワークロードの使用状況に関する情報を入力するように求められます。この情報に基づいて最適なボリューム構成が作成されるため、必要に応じて編集することができます。必要に応じて、ボリューム作成のこの手順をスキップできます。

ワークロードは、アプリケーションをサポートするストレージオブジェクトです。アプリケーションごとに1つ以上のワークロードまたはインスタンスを定義できます。一部のアプリケーションでは、特性が似たボリュームで構成されるようにワークロードが設定されます。これらのボリューム特性は、ワークロードがサポートするアプリケーションのタイプに基づいて最適化されます。たとえば、Microsoft SQL Serverアプリケーションをサポートするワークロードを作成し、そのワークロード用のボリュームを作成すると、Microsoft SQL Serverをサポートするようにボリューム特性が最適化されます。

- アプリケーション固有--アプリケーション固有のワークロードを使用してボリュームを作成する場合、アプリケーションワークロードのI/Oとアプリケーションインスタンスからの他のトラフィックの競合を最小限に抑えるために最適化されたボリューム構成が推奨される場合があります。I/Oタイプ、セグメントサイズ、コントローラ所有権、読み取り/書き込みキャッシュなどのボリューム特性が自動的に推奨され、次のアプリケーションタイプ用に作成されるワークロードに合わせて最適化されます。
  - Microsoft SQL Server の場合
  - Microsoft Exchange Server の略

- ビデオ監視アプリケーション
- VMware ESXi（ボリュームをVirtual Machine File Systemで使用する場合）

  ボリュームの追加/編集ダイアログボックスを使用して、推奨されるボリューム構成を確認し、システムで推奨されるボリュームや特性を編集、追加、削除できます。

- その他（または特定のボリューム作成サポートのないアプリケーション）- 特定のアプリケーションに関連付けられていないワークロードを作成する場合や、ストレージアレイで使用する予定のアプリケーションに対する最適化が組み込まれていない場合は、その他のワークロードではボリューム構成を手動で指定する必要があります。ボリュームの追加/編集ダイアログボックスを使用して、ボリューム構成を手動で指定する必要があります。

ボリューム、ホスト、またはホストクラスタが一部表示されないのはなぜですか？

ベースボリュームでData Assurance（DA）が有効なSnapshotボリュームを、DA対応でないホストに割り当てることはできません。DA対応でないホストにSnapshotボリュームを割り当てるには、ベースボリュームのDAを無効にする必要があります。

Snapshotボリュームを割り当てるホストについては、次のガイドラインを考慮してください。

- DA対応でないI/Oインターフェイスを使用してストレージアレイに接続されているホストは、DA対応ではありません。
- ホストメンバーが1つでもDA対応でないホストクラスタは、DA対応ではありません。

> Snapshot（整合性グループ、Snapshotグループ、Snapshotイメージ、Snapshotボリューム）、ボリュームコピーに関連付けられているボリュームでは、DAを無効にできません。 ミラーリングも可能です。ベースボリュームのDAを無効にするには、最初に関連付けられているすべてのリザーブ容量とSnapshotオブジェクトを削除する必要があります。

選択したワークロードを削除できないのはなぜですか？

このワークロードは、コマンドラインインターフェイス（CLI）を使用して作成されたボリューム、または別のストレージアレイから移行（インポート/エクスポート）されたボリュームのグループで構成されています。そのため、このワークロード内のボリュームはアプリケーション固有のワークロードに関連付けられておらず、ワークロードを削除することはできません。

アプリケーション固有のワークロードはストレージアレイの管理にどのように役立ちますか？

アプリケーション固有のワークロードのボリューム特性は、ワークロードがストレージアレイのコンポーネントとやり取りする方法を決定し、特定の構成下での環境のパフォーマンスを判断するのに役立ちます。

アプリケーションとは、SQL ServerやExchangeなどのソフトウェアです。アプリケーションごとに、サポートするワークロードを1つ以上定義します。一部のアプリケーションについては、ストレージを最適化するボリューム構成が自動的に提示されます。ボリューム構成には、I/Oタイプ、セグメントサイズ、コントローラ所有権、読み取りと書き込みのキャッシュなどの特性が含まれます。

拡張後の容量を認識させるにはどうすればよいですか？

ボリュームの容量を拡張した場合、その拡張した容量がホストですぐに認識されないことがあります。

ほとんどのオペレーティングシステムでは、拡張されたボリューム容量を認識し、ボリューム拡張の開始後に自動的に拡張が行われます。ただし、この処理が行われない場合もあります。拡張されたボリューム容量をOSが自動的に認識しない場合は、ディスクの再スキャンまたはリブートが必要になる可能性があります。

ボリュームの容量を拡張したら、それに応じてファイルシステムのサイズを手動で拡張する必要があります。方法は、使用しているファイルシステムによって異なります。

詳細については、ホストオペレーティングシステムのドキュメントを参照してください。

ホストの割り当てをあとで実行する場合に選択します。

ボリューム作成プロセスの速度を上げる場合は、ホスト割り当ての手順を省略して、新しく作成したボリュームをオフラインにすることができます。

新しく作成するボリュームを初期化する必要があります。システムは、Immediate Available Format（IAF）バックグラウンド初期化プロセスまたはオフラインプロセスのいずれかのモードを使用して初期化できます。

ボリュームをホストにマッピングすると、そのグループ内のすべての初期化中のボリュームがバックグラウンド初期化に強制的に移行します。このバックグラウンド初期化プロセスにより、同時ホストI/Oが可能になりますが、これには時間がかかることがあります。

ボリュームグループ内のいずれのボリュームもマッピングされていない場合、オフライン初期化が実行されます。オフラインプロセスはバックグラウンドプロセスよりもはるかに高速です。

ホストブロックサイズの要件について、どのような点に注意する必要がありますか？

EF300システムとEF600システムの場合は、ボリュームを設定して512バイトまたは4KiBのブロックサイズ（「セクターサイズ」とも呼ばれる）をサポートすることができます。ボリュームの作成時に正しい値を設定する必要があります。可能であれば、適切なデフォルト値が推奨されます。

ボリュームのブロックサイズを設定する前に、次の制限事項とガイドラインを確認してください。

- 一部のオペレーティングシステムと仮想マシン（現時点ではVMwareなど）は512バイトのブロックサイズを必要とし、4KiBをサポートしないため、ボリュームを作成する前にホストの要件を確認してください。通常、最適なパフォーマンスを得るには、ボリュームを4KiBのブロックサイズに設定します。ただし、ホストで4KiB（または「4Kn」）のブロックを使用できることを確認します。
- プールまたはボリュームグループ用に選択したドライブのタイプによって、サポートされるボリュームブロックサイズも次のように決まります。
  - 512バイトブロックに書き込むドライブを使用してボリュームグループを作成する場合、作成できるのは512バイトブロックのボリュームのみです。
  - 4KiBブロックに書き込むドライブを使用してボリュームグループを作成する場合は、512バイトまたは4KiBブロックでボリュームを作成します。

- アレイにiSCSIホストインターフェイスカードが搭載されている場合、すべてのボリュームは（ボリュームグループのブロックサイズに関係なく）512バイトブロックに制限されます。これは、特定のハードウェアの実装が原因です。
- 一度設定したブロックサイズは変更できません。ブロックサイズを変更する必要がある場合は、ボリュームを削除して再作成する必要があります。

ホストクラスタを作成する必要があるのはどのような場合ですか？

複数のホストから同じボリュームセットにアクセスする場合は、ホストクラスタを作成する必要があります。通常、個々のホストには、ボリュームへのアクセスを調整するためのクラスタリングソフトウェアがインストールされています。

正しいホストオペレーティングシステムタイプを特定するにはどうすればよいですか？

Host Operating System Typeフィールドには、ホストのオペレーティングシステムが表示されます。推奨されるホストタイプをドロップダウンリストから選択できます。

ドロップダウンリストに表示されるホストタイプは、ストレージアレイのモデルとファームウェアバージョンによって異なります。最新バージョンでは、最も一般的なオプションが最初に表示されますが、これは最も適切なオプションです。このリストに表示されるオプションが完全にサポートされているとは限りません。

> ホストのサポートの詳細については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

リストに表示されるホストタイプは次のとおりです。

ホストオペレーティングシステムのタイプ	オペレーティングシステム（**OS**）とマルチパスドライバ
Linux DM-MP（カーネル3.10以降）	Device Mapper Multipathのフェイルオーバー解決策と3.10以降のカーネルを使用するLinuxオペレーティングシステムをサポートします。
VMware ESXi	VMwareに組み込みのストレージアレイタイプポリシーモジュールであるSATP_ALUAを使用してNative Multipathing Plug-in（NMP）アーキテクチャを実行するVMware ESXiオペレーティングシステムをサポートします。
Windows（クラスタまたは非クラスタ）	ATTOマルチパスドライバを実行しないWindowsクラスタ構成または非クラスタ構成をサポートします。
ATTOクラスタ（すべてのオペレーティングシステム）	ATTO Technology、Inc.のマルチパスドライバを使用するすべてのクラスタ構成をサポートします。
Linux（Veritas DMP）	Veritas DMPマルチパス解決策 を使用するLinuxオペレーティングシステムをサポートします。
Linux（ATTO）	ATTO Technology、Inc.のマルチパスドライバを使用するLinuxオペレーティングシステムをサポートします。

ホストオペレーティングシステムのタイプ	オペレーティングシステム（**OS**）とマルチパスドライバ
Mac OS の場合	ATTO Technology、Inc.のマルチパスドライバを使用するMac OSバージョンをサポートします。
Windows（ATTO）	ATTO Technology、Inc.のマルチパスドライバを使用するWindowsオペレーティングシステムをサポートします。
FlexArray （ALUA）	マルチパスにALUAを使用するNetApp FlexArray システムをサポートします。
IBM SVCの場合	IBM SAN Volume Controller構成をサポートします。
工場出荷時のデフォルト	ストレージアレイの初回起動用です。ホストオペレーティングシステムのタイプが工場出荷時のデフォルトに設定されている場合は、接続先ホストで実行されているホストオペレーティングシステムとマルチパスドライバに合わせて変更します。
Linux DM-MP（カーネル3.9以前）	Device Mapper Multipathのフェイルオーバー解決策と3.9以前のカーネルを使用するLinuxオペレーティングシステムをサポートします。
Windowsクラスタ（廃止）	ホストオペレーティングシステムのタイプがこの値に設定されている場合は、代わりにWindows（クラスタまたは非クラスタ）の設定を使用します。

ホストポートをホストに一致させるにはどうすればよいですか？

ホストを手動で作成する場合は、まずホストで利用可能な適切なHost Bus Adapter（HBA；ホストバスアダプタ）ユーティリティを使用して、ホストにインストールされている各HBAに関連付けられているホストポート識別子を特定する必要があります。

この情報を確認したら、Create Hostダイアログのリストから、ストレージアレイにログインしているホストポート識別子を選択します。

> 作成するホストに適したホストポート識別子を選択してください。誤ったホストポート識別子を関連付けると、別のホストからこのデータへの原因 の意図しないアクセスが発生する可能性があります。

デフォルトクラスタとは何ですか？

デフォルトクラスタはシステム定義のエンティティです。ストレージアレイにログインしたホストポート識別子が関連付けられていない場合、そのポートはデフォルトクラスタに割り当てられているボリュームにアクセスできます。

関連付けられていないホストポート識別子は、特定のホストに論理的に関連付けられておらず、ホストに物理的に搭載されてストレージアレイにログインしているホストポートです。

> ホストがストレージアレイ内の特定のボリュームにアクセスできるようにする場合は、デフォルトクラスタを使用しないでください。代わりに、ホストポート識別子を対応するホストに関連付ける必要があります。このタスクは、ホスト作成処理中に手動で実行できます。その後、ボリュームを個々のホストまたはホストクラスタに割り当てます。

デフォルトクラスタは、外部ストレージ環境がすべてのホストにアクセスできるようにし、ストレージアレイに接続されているすべてのログイン済みホストポート識別子がすべてのボリュームにアクセスできるようにする（フルアクセスモード）場合にのみ使用してください。 特にストレージアレイやユーザインターフェイスでホストが認識されないようにする必要があります。

最初にボリュームをデフォルトクラスタに割り当てる際には、コマンドラインインターフェイス（CLI）を使用する必要があります。ただし、ボリュームを少なくとも1つデフォルトクラスタに割り当てると、このエンティティを管理できるユーザインターフェイスに表示されます（デフォルトクラスタ）。

冗長性チェックとは何ですか？

冗長性チェックでは、プールまたはボリュームグループ内のボリューム上のデータに整合性があるかどうかが判別されます。冗長性データは、プールまたはボリュームグループ内のいずれかのドライブで障害が発生した場合に、交換用ドライブに迅速に情報を再構築するために使用されます。

このチェックは、一度に1つのプールまたはボリュームグループでのみ実行できます。ボリュームの冗長性チェックでは、次の処理が実行されます。

- RAID 3ボリューム、RAID 5ボリューム、またはRAID 6ボリューム内のデータブロックがスキャンされ、各ブロックの冗長性情報がチェックされます。（RAID 3をボリュームグループに割り当てるには、コマンドラインインターフェイスを使用する必要があります）。
- RAID 1のミラーリングされたドライブ上のデータブロックが比較されます。
- データに整合性がないことがコントローラファームウェアで確認された場合は、冗長性エラーが返されます。

> 同じプールまたはボリュームグループですぐに冗長性チェックを実行すると、原因 でエラーが発生する場合があります。この問題を回避するには、同じプールまたはボリュームグループで別の冗長性チェックを実行する前に、1~2分待ってください。

予約済み容量とは何ですか？

予約済み容量は、ドライブ障害に備えてプール内に確保されている容量（ドライブ数）です。

プールが作成されると、プール内のドライブ数に応じて自動的にデフォルトの予約済み容量が確保されます。

プールの予約済み容量は再構築時に使用されますが、ボリュームグループでは同じ目的でホットスペアドライブが使用されます。予約済み容量を使用する方式は、再構築の時間を短縮できるため、ホットスペアドライブよりも優れています。予約済み容量は、ホットスペアドライブの場合は1本のドライブに確保されるのではなく、プール内の複数のドライブに分散されるため、特定のドライブの速度や可用性に制限されません。

アプリケーションに最適な**RAID**レベルはどれですか？

ボリュームグループのパフォーマンスを最大限に高めるには、適切なRAIDレベルを選択する必要があります。

適切なRAIDレベルを特定するには、ボリュームグループにアクセスしているアプリケーションでの読み取りと書き込みの割合を把握します。これらの割合を取得するには、[パフォーマンス]ページを使用します。

RAIDレベルとアプリケーションパフォーマンス

RAIDには、レベルと呼ばれる一連の構成が採用されており、ユーザデータと冗長性データのドライブに対する書き込み/読み出し方法が決定されます。RAIDレベルごとにパフォーマンス機能が異なります。読み取り比率が高いアプリケーションの場合、RAID 5ボリュームまたはRAID 6ボリュームを使用するとパフォーマンスが向上します。これは、RAID 5およびRAID 6構成の読み取りパフォーマンスが優れているためです。

読み取り比率が低い（書き込み中心の）アプリケーションの場合、RAID 5ボリュームまたはRAID 6ボリュームでは同様のパフォーマンスを実現できません。パフォーマンスの低下は、コントローラがデータと冗長性データをRAID 5ボリュームグループまたはRAID 6ボリュームグループのドライブに書き込む方法に起因します。

次の情報に基づいてRAIDレベルを選択します。

RAID 0

概要 ：

- 冗長性なし、ストライピングモード。
- RAID 0は、ボリュームグループ内のすべてのドライブにデータをストライピングします。

データ保護機能：

- 高可用性が求められる場合、RAID 0は推奨されません。RAID 0は重要度の低いデータに適しています。
- ボリュームグループ内の1本のドライブで障害が発生すると、関連付けられているすべてのボリュームで障害が発生し、すべてのデータが失われます。

必要なドライブ数：

- RAIDレベル0には少なくとも1本のドライブが必要です。
- RAID 0ボリュームグループには30本を超えるドライブを含めることができます。
- ストレージアレイのすべてのドライブを含むボリュームグループを作成できます。

RAID 1または**RAID 10**

概要 ：

- ストライピング/ミラーモード。

どのように機能するか:

- RAID 1では、ディスクミラーリングを使用して、2本のディスクに同時にデータが書き込まれます。

- RAID 10は、ドライブストライピングを使用して、複数のミラーリングされたドライブペアにデータをストライピングします。

データ保護機能：

- RAID 1とRAID 10は、ハイパフォーマンスと最高のデータ可用性を提供します。
- RAID 1とRAID 10は、ドライブミラーリングを使用して、あるドライブから別のドライブにまったく同じコピーを作成します。
- ドライブペアの一方のドライブで障害が発生した場合、ストレージアレイはデータやサービスを失うことなくもう一方のドライブに即座に切り替えることができます。
- 単一ドライブ障害が発生すると、関連付けられているボリュームはデグレード状態になります。ミラードライブがデータへのアクセスを許可します。
- ボリュームグループ内のドライブペアで障害が発生すると、関連付けられているすべてのボリュームで障害が発生し、データが失われる可能性があります。

必要なドライブ数：

- RAID 1には、ユーザデータ用に1本、ミラーデータ用に1本、合計2本以上のドライブが必要です。
- 4本以上のドライブを選択すると、ボリュームグループ全体でRAID 10が自動的に設定されます。ユーザデータ用にドライブが2本、ミラーデータ用にドライブが2本です。
- ボリュームグループのドライブ数は偶数でなければなりません。ドライブ数が偶数ではなく未割り当てのドライブが残っている場合は、「* Pools & Volume Groups」に移動してボリュームグループにドライブを追加し、処理を再試行します。
- RAID 1とRAID 10のボリュームグループは、30本を超えるドライブで構成できます。ストレージアレイのすべてのドライブを含むボリュームグループを作成できます。

RAID 5

概要 ：

- 高I/Oモード。

どのように機能するか:

- ユーザデータと冗長性情報（パリティ）が複数のドライブにストライピングされます。
- 冗長性情報を格納するために、ドライブ1本分の容量が使用されます。

データ保護機能

- RAID 5ボリュームグループで1本のドライブに障害が発生すると、関連付けられているすべてのボリュームがデグレード状態になります。冗長な情報があるので、データには引き続きアクセスできます。
- RAID 5ボリュームグループで複数のドライブに障害が発生すると、関連付けられているすべてのボリュームに障害が発生し、すべてのデータが失われます。

必要なドライブ数：

- ボリュームグループには最低3本のドライブが必要です。
- 通常、ボリュームグループのドライブ数は最大30本に制限されます。

RAID 6

概要 ：

- 高I/Oモード。

どのように機能するか:

- ユーザデータと冗長性情報（デュアルパリティ）が複数のドライブにストライピングされます。
- 冗長性情報を格納するために、ドライブ2本分の容量が使用されます。

データ保護機能：

- RAID 6ボリュームグループで1本または2本のドライブに障害が発生すると、関連付けられているすべてのボリュームがデグレード状態になりますが、冗長性情報があるためデータには引き続きアクセスできます。
- RAID 6ボリュームグループで3本以上のドライブに障害が発生すると、関連付けられているすべてのボリュームに障害が発生し、すべてのデータが失われます。

必要なドライブ数：

- ボリュームグループには最低5本のドライブが必要です。
- 通常、ボリュームグループのドライブ数は最大30本に制限されます。

> プールのRAIDレベルは変更できません。ユーザーインタフェースは’プールを自動的にRAID 6として構成します

RAIDレベルとデータ保護

RAID 1、RAID 5、およびRAID 6は、フォールトトレランス用に冗長性データをドライブメディアに書き込みます。冗長性データには、データのコピー（ミラー）、またはデータから導出されたエラー修正コードがあります。ドライブで障害が発生した場合は、冗長性データを使用して交換用ドライブに迅速に情報を再構築できます。

単一のボリュームグループ全体で単一のRAIDレベルを設定します。そのボリュームグループの冗長性データは、すべてボリュームグループ内に格納されます。ボリュームグループの容量は、メンバードライブのアグリゲート容量から冗長性データ用に確保された容量を引いた値です。冗長性を確保するために必要な容量は、使用するRAIDレベルによって異なります。

一部のドライブが表示されないのはなぜですか？

容量の追加ダイアログで、既存のプールまたはボリュームグループに容量を追加できるドライブがすべて表示されるわけではありません。

ドライブを追加できない理由は次のとおりです。

- 未割り当てで、セキュリティ有効でないドライブを指定する必要があります。すでに別のプールやボリュームグループに含まれているドライブ、またはホットスペアとして設定されているドライブは使用できません。未割り当てだが、セキュリティ有効なドライブは、手動で消去すると使用可能になります。
- 最適な状態でないドライブは使用できません。

- 容量が小さすぎるドライブは使用できません。
- プールまたはボリュームグループ内でドライブのメディアタイプが一致している必要があります。次のものを混在させることはできません。
  - ソリッドステートディスク（SSD）搭載のハードディスクドライブ（HDD）
  - NVMeとSASドライブ
  - ボリュームブロックサイズが512バイトおよび4KiBのドライブ
- プールまたはボリュームグループに含まれているドライブがすべてセキュリティ対応の場合は、セキュリティ対応でないドライブは表示されません。
- プールまたはボリュームグループに含まれているドライブがすべて連邦情報処理標準（FIPS）ドライブの場合、非FIPSドライブは表示されません。
- プールまたはボリュームグループに含まれているドライブがすべてData Assurance（DA）対応で、プールまたはボリュームグループにDA有効ボリュームが1つ以上ある場合は、DA非対応のドライブは使用できないためプールまたはボリュームグループに追加できません。ただし、プールまたはボリュームグループにDA有効ボリュームがない場合は、DA非対応のドライブをプールまたはボリュームグループに追加できます。DA対応と非対応のドライブが混在している場合は、DA対応ボリュームを作成できないことに注意してください。

> ストレージアレイの容量は、新しいドライブを追加するか、プールまたはボリュームグループを削除することで増やすことができます。

予約済み容量を増やせない場合、どのような理由が考えられますか？

使用可能なすべての容量でボリュームを作成した場合は、予約済み容量を増やせないことがあります。

予約済み容量は、ドライブ障害に備えてプール内に確保されている容量（ドライブ数）です。プールが作成されると、プール内のドライブ数に応じて自動的にデフォルトの予約済み容量が確保されます。使用可能なすべての容量でボリュームを作成している場合は、ドライブを追加するかボリュームを削除してプールに容量を追加しないと、予約済み容量を増やすことはできません。

予約済み容量は、プールおよびボリュームグループから変更できます。編集するプールを選択します。[設定の表示/編集]をクリックし、[設定]タブを選択します。

> 予約済み容量はプール内の複数のドライブに分散されますが、予約するときはドライブ数で指定します。

Data Assuranceとは何ですか？

Data Assurance（DA）はT10 Protection Information（PI）標準を実装しています。I/Oパスでデータが転送される際に発生する可能性のあるエラーをチェックして修正することで、データの整合性が向上します。

Data Assurance機能の一般的な用途として、コントローラとドライブ間のI/Oパスがチェックされます。DA機能はプールおよびボリュームグループのレベルで提供されます。

この機能を有効にすると、ボリューム内の各データブロックに巡回冗長検査（CRC）と呼ばれるエラーチェ

ック用のコードが付加されます。データブロックが移動されると、ストレージアレイはこれらのCRCコードを使用して、転送中にエラーが発生したかどうかを判断します。破損している可能性があるデータはディスクに書き込まれず、ホストにも返されません。DA機能を使用する場合は、新しいボリュームを作成するときにDAに対応したプールまたはボリュームグループを選択します（プールとボリュームグループの候補の表で、「* DA *」の横の「*はい」*を探します）。

これらのDA対応ボリュームは、必ずDAに対応したI/Oインターフェイスを使用しているホストに割り当ててください。DAに対応したI/Oインターフェイスには、ファイバチャネル、SAS、iSCSI over TCP/IP、NVMe/FC、NVMe/IB、 NVMe/RoCEとiSER over InfiniBand（iSCSI Extensions for RDMA/IB）：SRP over InfiniBandではDAはサポートされていません。

FDE / FIPSセキュリティとは何ですか？

FDE / FIPSセキュリティとは、一意の暗号化キーを使用して書き込み時にデータを暗号化し、読み取り時に復号化するセキュリティ対応ドライブを指します。

セキュリティ対応ドライブは、ストレージアレイから物理的に取り外されたドライブ上のデータへの不正アクセスを防止します。セキュリティ対応ドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。FIPSドライブは認定テストをパスしたドライブです。

> FIPSのサポートが必要なボリュームには、FIPSドライブのみを使用します。ボリュームグループまたはプールにFIPSドライブとFDEドライブが混在している場合、すべてのドライブがFDEドライブとして扱われます。また、FIPSドライブのみを含むボリュームグループまたはプールでは、FDEドライブを追加したりスペアとして使用したりすることはできません。

セキュリティ対応（ドライブセキュリティ）とは何ですか？

ドライブセキュリティは、セキュリティ有効ドライブをストレージアレイから取り外したときに、そのドライブ上のデータへの不正アクセスを防止する機能です。

対応するドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。

SSDキャッシュのすべての統計情報を表示するにはどうすればよいですか？また、何が

SSDキャッシュについては、一般統計と詳細統計を表示できます。

一般統計は詳細統計のサブセットです。詳細統計は、すべてのSSD統計を.csvファイルにエクスポートした場合にのみ表示できます。統計を確認および解釈する際には、複数の統計を組み合わせることで見えてくる情報もあることに注意してください。

一般統計

SSDキャッシュの統計を表示するには、* Manage *ページに移動します。メニューを選択します。Provisioning [プールとボリュームグループの構成]。統計を表示するSSDキャッシュを選択し、メニューを選択します。More [View Statistics]公称統計はView SSD Cache Statistics（SSDキャッシュ統計の表示）ダイアログに表示されます。

> この機能は、EF600またはEF300ストレージシステムでは使用できません。

このリストには、詳細統計のサブセットである一般統計が表示されます。

詳細統計

詳細統計は、一般統計とその他の統計で構成されます。これらの追加統計は一般統計とともに保存されますが、一般統計とは異なり、View SSD Cache Statistics（SSDキャッシュ統計の表示）ダイアログには表示されません。詳細統計を表示するには、統計を.csvファイルにエクスポートする必要があります。

一般統計のあとに詳細統計が表示されます。

シェルフ損失の保護およびドロワー損失の保護とは何ですか？

シェルフ損失の保護とドロワー損失の保護は、シェルフまたはドロワーで単一障害が発生した場合にデータアクセスを維持するためのプールとボリュームグループの属性です。

シェルフ損失の保護

シェルフは、ドライブまたはドライブとコントローラを格納するエンクロージャです。シェルフ損失の保護が有効な場合、1台のドライブシェルフとの通信が完全に失われた場合でもプールまたはボリュームグループ内のボリューム上のデータへのアクセスが保証されます。通信が完全に失われるケースには、ドライブシェルフの電源喪失や、両方のI/Oモジュール（IOM）の障害などがあります。

> プールまたはボリュームグループですでにドライブに障害が発生している場合は、シェルフ損失の保護は保証されません。この状況で、ドライブシェルフへのアクセス、さらにその結果プールまたはボリュームグループ内の別のドライブへのアクセスを失うと、データが失われます。

シェルフ損失の保護の条件は、次の表で説明するように、保護の手法によって異なります。

レベル	シェルフ損失の保護の条件	必要なシェルフの最小数
プール	プールには少なくとも5つのシェルフのドライブが含まれている必要があり、各シェルフで同じ数のドライブが必要です。シェルフ損失の保護は大容量シェルフには適用されません。大容量シェルフがあるシステムの場合は、ドロワー損失の保護を参照してください。	5.
RAID 6	ボリュームグループに同じドロワーのドライブが3本以上含まれない。	3.
RAID 3またはRAID 5	ボリュームグループ内のドライブがすべて別々のシェルフに配置されている。	3.
RAID 1	RAID 1ペアのドライブがそれぞれ別のシェルフに配置されている。	2.
RAID 0	シェルフ損失の保護は実現できない。	該当なし

ドロワーはシェルフのコンパートメントの1つで、引き出してドライブを設置します。ドロワーを備えているのは大容量シェルフのみです。ドロワー損失の保護が有効な場合、1つのドロワーとの通信が完全に失われた場合でもプールまたはボリュームグループ内のボリューム上のデータへのアクセスが保証されます。通信が完全に失われるケースには、ドロワーの電源喪失や、ドロワー内のコンポーネント障害などがあります。

> プールまたはボリュームグループですでにドライブに障害が発生している場合は、ドロワー損失の保護は保証されません。この状況でドロワーにアクセスできなくなると（その結果プールまたはボリュームグループ内の別のドライブにアクセスできなくなると）、データが失われます。

ドロワー損失の保護の条件は、次の表で説明するように、保護の手法によって異なります。

レベル	ドロワー損失の保護の基準	必要なドロワーの最小数
プール	プール候補にはすべてのドロワーのドライブを含める必要があり、各ドロワーに同じ数のドライブが必要です。プールには少なくとも5つのドロワーのドライブが含まれている必要があり、各ドロワーに同じ数のドライブが必要です。60ドライブのシェルフでは、プールに含まれる15、20、25、30、35でドロワー損失の保護を実現できます。 40、45、50、55、または60ドライブ。初回作成後に、5の倍数でプールに追加できます。	5.
RAID 6	ボリュームグループに同じドロワーのドライブが3本以上含まれない。	3.
RAID 3または5	ボリュームグループ内のドライブがすべて別々のドロワーに配置されている	3.
RAID 1	ミラーペアのドライブがそれぞれ別のドロワーに配置されている。	2.
RAID 0	ドロワー損失の保護は実現できない。	該当なし

シェルフ損失およびドロワー損失の保護を維持するにはどうすればよいですか？

プールまたはボリュームグループのシェルフ損失およびドロワー損失の保護を維持するには、次の表の基準を使用します。

レベル	シェルフ/ドロワー損失の保護の基準	必要なシェルフ/ドロワーの最小数
プール	シェルフの場合、プールに同じシェルフのドライブが3本以上含まれない。ドロワーの場合、プールに各ドロワーから同数のドライブが含まれている。	ドロワー用のシェルフ5の場合は6
RAID 6	ボリュームグループに同じシェルフまたはドロワーのドライブが3本以上含まれない。	3.
RAID 3またはRAID 5	ボリュームグループ内のドライブがすべて別々のシェルフまたはドロワーに配置されている。	3.
RAID 1	ミラーペア内のドライブがそれぞれ別のシェルフまたはドロワーに配置されている。	2.
RAID 0	シェルフ/ドロワー損失の保護は実現できない。	該当なし

プールまたはボリュームグループですでにドライブに障害が発生している場合は、シェルフ/ドロワー損失の保護は維持されません。この状況で、ドライブシェルフまたはドロワーへのアクセス、さらにその結果プールまたはボリュームグループ内の別のドライブへのアクセスを失うと、データが失われます。

プールの最適化容量とは何ですか？

SSDドライブでは、その容量の一部が未割り当ての場合に寿命が長くなり、最大書き込みパフォーマンスが向上します。

プールに関連付けられているドライブの未割り当て容量は、プールの予約済み容量、空き容量（ボリュームで使用されていない容量）、および使用可能容量のうちの最適化容量として確保された容量で構成されます。この最適化容量は使用可能容量を減らすことで最小レベルの最適化容量を確保するため、ボリュームの作成には使用できません。

プールの作成時に、パフォーマンス、ドライブの寿命、使用可能容量のバランスに基づいて、推奨される最適化容量が決定されます。プール設定ダイアログにある追加の最適化容量スライダを使用すると、プールの最適化容量を調整できます。スライダを動かすことで、使用可能容量を犠牲にしてパフォーマンスの向上とドライブ寿命の延長を図るか、またはパフォーマンスとドライブ寿命を犠牲にして使用可能容量を増やすことができます。

追加の最適化容量スライダは、EF600およびEF300ストレージシステムに対してのみ使用できます。

ボリュームグループの最適化容量とは何ですか？

SSDドライブでは、その容量の一部が未割り当ての場合に寿命が長くなり、最大書き込みパフォーマンスが向上します。

ボリュームグループに関連付けられているドライブの未割り当て容量は、ボリュームグループの空き容量（ボリュームで使用されていない容量）と、使用可能容量のうちの最適化容量として確保された容量で構成されます。この最適化容量は使用可能容量を減らすことで最小レベルの最適化容量を確保するため、ボリュームの作成には使用できません。

ボリュームグループの作成時に、パフォーマンス、ドライブの寿命、使用可能容量のバランスに基づいて、推奨される最適化容量が決定されます。ボリュームグループ設定ダイアログの最適化容量のスライダを使用して、ボリュームグループの最適化容量を調整できます。スライダを動かすことで、使用可能容量を犠牲にしてパフォーマンスの向上とドライブ寿命の延長を図るか、またはパフォーマンスとドライブ寿命を犠牲にして使用可能容量を増やすことができます。

追加の最適化容量のスライダは、EF600およびEF300ストレージシステムに対してのみ使用できます。

リソースプロビジョニング機能とは何ですか？

リソースプロビジョニングは、EF300およびEF600ストレージアレイで使用できる機能です。これにより、バックグラウンドの初期化プロセスを実行せずに、ボリュームをただちに使用できます。

リソースプロビジョニングボリュームは、SSDグループまたはプール内のシックボリュームです。ボリュームの作成時にはドライブ容量が割り当てられますが（ボリュームに割り当てられます）、ドライブブロックは割り当て解除されます（マッピング解除されます）。これに対し、従来のシックボリュームでは、Data Assurance保護情報のフィールドを初期化し、各RAIDストライプでデータとRAIDパリティの整合性を確保するために、すべてのドライブブロックがバックグラウンドボリューム初期化処理中にマッピングまたは割り当てられます。リソースプロビジョニングボリュームでは、時間制限付きのバックグラウンド初期化は実行されません。代わりに、各RAIDストライプは、ストライプ内のボリュームブロックへの最初の書き込み時に初期化されます。

リソースプロビジョニングボリュームはSSDボリュームグループおよびプールでのみサポートされます。グループまたはプール内のすべてのドライブでNVMeのDeallocated or Unwritten Logical Block Error（DULBE）エラーリカバリ機能がサポートされます。リソースでプロビジョニングされたボリュームを作成すると、そのボリュームに割り当てられていたすべてのドライブブロックが割り当て解除（マッピング解除）されます。また、ホストではNVMe Dataset Managementコマンドを使用して、ボリューム内の論理ブロックの割り当てを解除できます。ブロックの割り当てを解除すると、SSDの消耗度が改善され、書き込みパフォーマンスが最大化されます。向上率はドライブのモデルと容量によって異なります。

リソースでプロビジョニングされるボリューム機能について、どのような点に注意する必要がありますか？

リソースプロビジョニングは、EF300およびEF600ストレージアレイで使用できる機能です。これにより、バックグラウンドの初期化プロセスを実行せずに、ボリュームをただちに使用できます。

リソースプロビジョニング機能は現在使用できません。ビューによっては、コンポーネントがリソースプロビジョニング対応と報告される場合がありますが、リソースプロビジョニングボリュームを作成する機能は、あとで更新するまで無効になっています。

リソースでプロビジョニングされたボリューム

リソースプロビジョニングボリュームは、SSDグループまたはプール内のシックボリュームです。ボリュームの作成時にはドライブ容量が割り当てられますが（ボリュームに割り当てられます）、ドライブブロックは割り当て解除されます（マッピング解除されます）。これに対し、従来のシックボリュームでは、Data Assurance保護情報のフィールドを初期化し、各RAIDストライプでデータとRAIDパリティの整合性を確保するために、すべてのドライブブロックがバックグラウンドボリューム初期化処理中にマッピングまたは割り当てられます。リソースプロビジョニングボリュームでは、時間制限付きのバックグラウンド初期化は実行されません。代わりに、各RAIDストライプは、ストライプ内のボリュームブロックへの最初の書き込み時に初期化されます。

リソースプロビジョニングボリュームはSSDボリュームグループおよびプールでのみサポートされます。グループまたはプール内のすべてのドライブでNVMeのDeallocated or Unwritten Logical Block Error（DULBE）エラーリカバリ機能がサポートされます。リソースでプロビジョニングされたボリュームを作成すると、そのボリュームに割り当てられていたすべてのドライブブロックが割り当て解除（マッピング解除）されます。また、ホストではNVMe Dataset Managementコマンドを使用して、ボリューム内の論理ブロックの割り当てを解除できます。ブロックの割り当てを解除すると、SSDの消耗度が改善され、書き込みパフォーマンスが最大化されます。向上率はドライブのモデルと容量によって異なります。

機能の有効化と無効化

DULBEがサポートされているシステムでは、リソースプロビジョニングがデフォルトで有効になっています。このデフォルト設定は、プールとボリュームグループで無効にできます。リソースプロビジョニングの無効化は、既存のボリュームに対する永続的な処理であり、元に戻すことはできません（つまり、これらのボリュームグループおよびプールのリソースプロビジョニングを再度有効にすることはできません）。

新しいボリュームのリソースプロビジョニングを再度有効にするには、[設定][システム]メニューを使用します。リソースのプロビジョニングを再度有効にすると、新しく作成したボリュームグループとプールのみに影響する点に注意してください。既存のボリュームグループおよびプールは変更されません。必要に応じて、[設定][システム]メニューからリソースプロビジョニングを再度無効にすることもできます。

内部セキュリティキー管理と外部セキュリティキー管理の違いは何ですか？

ドライブセキュリティ機能を実装している場合は、内部セキュリティキーまたは外部セキュリティキーを使用して、セキュリティ有効ドライブがストレージアレイから取り外されたときにデータをロックダウンすることができます。

セキュリティキーは、ストレージアレイのセキュリティ有効ドライブとコントローラで共有される文字列です。内部キーは、コントローラの永続的メモリに保持されます。外部キーは、Key Management Interoperability Protocol（KMIP）を使用して別のキー管理サーバに保持されます。

セキュリティキーを作成するときは、どのような点に注意する必要がありますか？

セキュリティキーは、ストレージアレイ内のコントローラとセキュリティ有効ドライブによって共有されます。セキュリティ有効ドライブをストレージアレイから取り外すと、セキュリティキーによってデータが不正アクセスから保護されます。

セキュリティキーは次のいずれかの方法で作成および管理できます。

- コントローラの永続的メモリ上での内部キー管理。
- 外部キー管理サーバでの外部キー管理

内部キー管理

コントローラの永続的メモリ上のアクセスできない場所に内部キーが保持され、「非表示」になります。内部セキュリティキーを作成する前に、次の作業を行う必要があります。

1. ストレージアレイにセキュリティ対応ドライブを取り付けます。対応するドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。
2. ドライブセキュリティ機能が有効になっていることを確認します。ドライブセキュリティ機能を有効にする手順については、必要に応じてストレージベンダーに問い合わせてください。

識別子とパスフレーズを定義して、内部セキュリティキーを作成します。識別子は、セキュリティキーに関連付けられる文字列で、コントローラとキーに関連付けられたすべてのドライブに格納されます。パスフレーズは、バックアップ用にセキュリティキーを暗号化するために使用されます。作成したセキュリティキーは、コントローラ上のアクセスできない場所に格納されます。これで、セキュリティ有効のボリュームグループまたはプールを作成したり、既存のボリュームグループまたはプールでセキュリティを有効にしたりできます。

外部キー管理

外部キーは、Key Management Interoperability Protocol（KMIP）を使用して別のキー管理サーバに保持されます。外部セキュリティキーを作成する前に、次の作業を行う必要があります。

1. ストレージアレイにセキュリティ対応ドライブを取り付けます。対応するドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。
2. ドライブセキュリティ機能が有効になっていることを確認します。ドライブセキュリティ機能を有効にする手順については、必要に応じてストレージベンダーに問い合わせてください
3. 署名済みのクライアント証明書ファイルを取得します。クライアント証明書は、キー管理サーバがKMIP要求を信頼できるよう、ストレージアレイのコントローラを検証します。
   a. まず、クライアント証明書署名要求（CSR）を生成してダウンロードします。メニューに移動します。Settings [証明書]、[キー管理]、[CSRの作成]の順に選択します。
   b. 次に、キー管理サーバで信頼されているCAから署名済みのクライアント証明書を要求します。（ダウンロードしたCSRファイルを使用して、キー管理サーバからクライアント証明書を作成およびダウンロードすることもできます）。
   c. クライアント証明書ファイルを作成したら、System Managerにアクセスしているホストにそのファイルをコピーします。
4. キー管理サーバから証明書ファイルを取得し、System Managerにアクセスしているホストにそのファイルをコピーします。キー管理サーバ証明書は、ストレージアレイがサーバのIPアドレスを信頼できるよう、キー管理サーバを検証します。キー管理サーバには、ルート証明書、中間証明書、またはサーバ証明書を使用できます。

キー管理サーバのIPアドレスとKMIP通信に使用するポート番号を定義して、外部キーを作成します。このプロセスでは、証明書ファイルもロードします。作成が完了すると、入力したクレデンシャルを使用してキー管理サーバに接続されます。これで、セキュリティ有効のボリュームグループまたはプールを作成したり、既存のボリュームグループまたはプールでセキュリティを有効にしたりできます。

パスフレーズを定義する必要があるのはなぜですか？

パスフレーズは、ローカルの管理クライアントに格納されているセキュリティキーファイルの暗号化と復号化に使用されます。パスフレーズがないとセキュリティキーを復号化できず、セキュリティ有効ドライブが別のストレージアレイに再設置された場合、デ

ータのロック解除にセキュリティキーを使用できません。

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権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

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