SANtricityソフトウェアのドキュメント11.80

SANtricity 11.8

NetApp
December 16, 2024

目次

SANtricityソフトウェアのドキュメント11.80 . . . 1
リリースノート . . . 2
SANtricity OS 11.80の新機能 . . . 2
リリースノート . . . 5
開始する . . . 6
SANtricityソフトウェアの概要 . . . 6
サポートされるブラウザとオペレーティングシステム . . . 9
System Managerのセットアップ . . . 10
Unified Managerセットアップ . . . 14
System Manager 11.8による単一アレイの管理 . . . 16
メインインターフェイス . . . 16
プールとボリュームグループ . . . 39
ボリュームとワークロード . . . 106
ホストとホストクラスタ . . . 161
スナップショット . . . 181
ミラーリング . . . 226
リモートストレージ . . . 271
ハードウェアコンポーネント . . . 283
Unified Manager 6による複数のアレイの管理 . . . 588
メインインターフェイス . . . 588
ストレージアレイ . . . 591
設定のインポート . . . 599
アレイクルウフ . . . 606
アップグレード . . . 609

SANtricityソフトウェアのドキュメント11.80

リリースノート

SANtricity OS 11.80の新機能

次の表に、SANtricity System Manager 11.8の新機能を示します。

バージョン**11.80.1R1**の新機能

新機能	製品説明
新しい自己署名およびCA署名管理証明書のキーサイズが拡張されました。	SANtricity System ManagerおよびUnified Managerアプリケーションの自己署名証明書の管理証明書キーサイズが、2、048ビットから3、072ビットに変更されました。この変更は、SANtricityアプリケーションから新しく生成された自己署名証明書とCA署名証明書に適用されます。キーの長さは固定であり、NVSRAMのデフォルトのキーサイズ定義の影響を受けません。

バージョン**11.80.1**の新機能

新機能	製品説明
`-identifyDevices` パラメータ	SMcliで新しい `-identifyDevices`パラメータを使用できるようになりました。この新しいパラメータを使用すると、ストレージアレイに関連付けられているすべてのSCSIネイティブブロックデバイスを検索できます。詳細については、を参照してください "ダウンロード可能なSMcliコマンドラインパラメータ"。
イーサネットカーネル統計	System Managerの[iSCSI統計パッケージの表示]ページに、新しい[イーサネットカーネル統計]オプションが追加されました。この新しいオプションを使用すると、iSCSIデバイスのプラットフォームカーネルドライバの統計を表示できます。詳細については、を参照してください "iSCSI統計パッケージの表示"。
REST APIエンドポイントを使用してIPアドレスをブロックする機能を追加	ユーザは、[Settings]エンドポイントを使用して特定のIPアドレスをブロックできるようになりまし(`/devmgr/v2/settings`た）。[Settings]エンドポイントで設定すると、ホワイトリストで指定したIPアドレスだけがストレージデバイスと通信できます。この新機能では、IPv4およびIPv6アドレスリストがサポートされます。
vCenterストレージプラグイン	vCenter Storageプラグインは、Eシリーズ11.80.1リリースとの互換性を考慮して更新されています。
Web Services Proxy	Web Services Proxyは、Eシリーズ11.80.1リリースとの互換性を確保するためにバージョン6.1に更新されています。

バージョン**11.80**の新機能

新機能	製品説明
強化されたボリュームパリティスキャン	REST APIまたはCLIを使用して、ボリュームパリティスキャンをバックグラウンドプロセスとして起動できるようになりました。パリティスキャンは、スキャン処理を完了するために必要な限りバックグラウンドで実行されます。スキャン処理は、コントローラのリブートおよびフェイルオーバー処理の間も維持されます。
Unified ManagerのSAMLサポート	Unified ManagerでSecurity Assertion Markup Language（SAML）がサポートされるようになりました。Unified ManagerでSAMLを有効にすると、ユーザインターフェイスを操作するために、アイデンティティプロバイダに対して多要素認証を使用する必要があります。Unified ManagerでSAMLを有効にすると、IdPを経由せずにREST APIを使用して要求を認証することはできません。
自動構成機能	アレイの初期セットアップ時に自動構成機能で使用するボリュームのブロックサイズパラメータを設定できるようになりました。この機能は、CLIでは「blocksize」パラメータとしてのみ使用できます。
コントローラファームウェアの暗号化署名	コントローラファームウェアは暗号署名されています。シグネチャは、初回ダウンロード時および各コントローラのブート時にチェックされます。エンドユーザへの影響はありません。署名は、CAによって発行された拡張検証証明書によって裏付けられます。
ドライブファームウェアの暗号化署名	ドライブファームウェアは暗号署名されています。署名は最初のダウンロード時にチェックされ、CAによって発行された拡張検証証明書によってバックアップされます。ドライブファームウェアの内容がZIPファイルとして提供されるようになりました。ZIPファイルには、署名済みの古いファームウェアと署名済みの新しいファームウェアが含まれています。ユーザーは、ターゲットシステムで実行されているコードのリリースバージョンに基づいて適切なファイルを選択する必要があります。

新機能	製品説明

外部キーサーバ管理-証明書のキーサイズ	新しいデフォルトの証明書キーサイズは3072ビット（2048から）です。最大4096ビットのキーサイズがサポートされます。デフォルト以外のキーサイズをサポートするには、NVSRAMビットを変更する必要があります。
	
	キーサイズの選択値は次のとおりです。
	
	• デフォルト= 0
	• 長さ2048 = 1
	• 長さ3072 = 2
	• 長さ4096 = 3
	
	SMcliを使用してキーサイズを4096に変更するには、次の手順を実行します。
	
	`set controller[b] globalnvsrambyte[0xc0]=3;`
	`set controller[a] globalnvsrambyte[0xc0]=3;`
	
	キーのサイズを調べます。
	
	`show allcontrollers globalnvsrambyte[0xc0];`

ディスクプールの改善	11.80以降を実行しているコントローラで作成されたディスクプールは、_Version 0_poolsではなく_Version 1_poolsになります。_Version 1_diskプールが存在する場合、ダウングレード操作は制限されます。 ストレージアレイプロファイルでディスクプールのバージョンを特定できます。
System ManagerとUnified Managerは、ブラウザの最小要件を満たしていないと起動しません。	System ManagerまたはUnified Managerを起動するには、少なくともバージョンのブラウザが必要です。サポートされる最小バージョンは次のとおりです。 • Firefoxの最小バージョン80 • Chrome最小バージョン89 • エッジ最小バージョン90 • Safariの最小バージョン14
FIPS 140-3 NVMe SSDドライブのサポート	NetApp認定のFIPS 140-3 NVMe SSDドライブがサポートされるようになりました。これらは、ストレージアレイプロファイルおよびSystem Managerで正しく識別されます。
EF300およびEF600でのSSD読み取りキャッシュのサポート	SAS拡張構成のHDDを使用するEF300およびEF600コントローラでSSD読み取りキャッシュがサポートされるようになりました。

新機能	製品説明
EF300およびEF600でのiSCSIとFibre Channelの非同期リモートミラーリングのサポート	NVMeおよびSASベースのボリュームを使用するEF300およびEF600コントローラで非同期リモートミラーリング（ARVM）がサポートされるようになりました。
ベーストレイにドライブを搭載しないEF300およびEF600をサポート	ベーストレイにNVMeドライブを搭載しないEF300およびEF600コントローラ構成がサポートされるようになりました。
すべてのプラットフォームでUSBポートが無効になっている	すべてのプラットフォームでUSBポートが無効になりました。

リリースノート

リリースノートはこのサイト以外でも入手できます。NetAppサポートサイトのクレデンシャルを使用してログインするように求められます。

- "11.80リリースノート"
- "11.70リリースノート"
- "11.60リリースノート"
- "11.50リリースノート"

開始する

SANtricityソフトウェアの概要

E シリーズシステムには、ストレージプロビジョニングとその他のタスクを行うための SANtricity ソフトウェアが搭載されています。

このサイトでは、次のSANtricity管理インターフェイスの使用方法について説明します。

- System Manager --ネットワーク内の個 々 のストレージアレイの管理に使用するWebベースのインターフェイス。
- Unified Manager --ネットワーク内のすべてのストレージアレイの表示と管理に使用するWebベースのインターフェイス。

EF600およびEF300ストレージアレイでは、同期ミラーリングまたはシンボリュームはサポートされません。

SANtricityシステムマネージャ

System Managerは、Webベースの管理ソフトウェアで、各コントローラに組み込まれています。ユーザインターフェイスにアクセスするには、ブラウザでコントローラのIPアドレスを指定します。セットアップウィザードを使用して、システム設定を開始できます。

System Managerには、次のようなさまざまな管理機能があります。

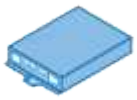
パフォーマンス

I/O レイテンシ、 IOPS 、 CPU 利用率、スループットなど、最大 30 日分のパフォーマンスデータを表示します。

ストレージ

プールまたはボリュームグループを使用してストレージをプロビジョニングし、アプリケーションワークロードを作成

データ保護

Snapshot 、ボリュームコピー、リモートミラーリングを使用してバックアップやディザスタリカバリを実行できます。
 ハードウェア
コンポーネントのステータスを確認し、ホットスペアドライブの割り当てなど、コンポーネントに関連するいくつかの機能を実行します。
 アラート
ストレージアレイで発生している重要なイベントを管理者に通知します。Eメール、SNMPトラップ、syslogを使用してアラートを送信できます。
 アクセス管理
ユーザ認証を設定し、ユーザがシステムにログインする際に割り当てられたクレデンシャルの入力を求めます。
 システム設定
SSD キャッシュや自動ロードバランシングなど、その他のシステムパフォーマンス機能を設定します。
 サポート
診断データを表示し、アップグレードを管理します。また、ストレージアレイの健常性を監視してテクニカルサポートに自動ディスパッチを送信する AutoSupport を設定します。

SANtricity Unified Manager

Unified Manager は、ドメイン全体の管理に使用する Web ベースのソフトウェアです。EシリーズおよびEFシリーズの新しいすべてのアレイ（E2800、EF280、EF300、E5700、EF570、EF600など）のステータスをまとめて確認できます。選択したストレージアレイに対してバッチ処理を実行することもできます。

Unified Manager は、 Web Services Proxy とともに管理サーバにインストールされます。Unified Manager にアクセスするには、ブラウザを開き、 Web Services Proxy がインストールされているサーバの URL を入力します。

Unified Managerには、次のようなさまざまな管理機能があります。

 ストレージアレイの検出
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索および追加します。1 つのページですべてのストレージアレイのステータスを確認できます。
 発売開始
System Manager のインスタンスを開き、特定のストレージアレイについての管理操作を個別に実行します。
 設定のインポート
アラート、 AutoSupport 、ディレクトリサービスなどの設定を 1 つのストレージアレイから複数のアレイに一括でインポートします。
 ミラーリング
2つのストレージアレイ間で非同期ミラーペアまたは同期ミラーペアを設定します。
 グループの管理
管理しやすいようにストレージアレイをグループにまとめます。

 アップグレードセンター
複数のストレージアレイのSANtricity OSソフトウェアをアップグレードします。
 証明書
複数のストレージアレイについて、証明書署名要求（ CSR ）の作成、証明書のインポート、既存の証明書の管理を行います。
 アクセス管理
ユーザ認証を設定し、ユーザが Unified Manager にログインする際に割り当てられたクレデンシャルの入力を求めます。

サポートされるブラウザとオペレーティングシステム

SANtricityソフトウェアは、いくつかの種類のブラウザとオペレーティングシステムをサポートしています。

ブラウザ

サポートされるブラウザとバージョンを次に示します。

ブラウザ	最小バージョン
Google Chrome	89
Mozilla Firefox	80
Safari	14
Microsoft Edge	90

Unified Managerの場合は、Web Services Proxyがインストールされていて、ブラウザから使用できる必要があります。詳細については、を参照してください。 "SANtricity Web Services Proxyの概要"

オペレーティングシステム

次のオペレーティングシステムとバージョンがサポートされています。

オペレーティングシステム	最小バージョン/アーキテクチャ
Red Hat Enterprise Linux（RHEL）	7.x、8.x/64ビット
SUSE Linux Enterprise Server（SLES）	12.x、15.x/64ビット
Oracle Linux（OL）	7.x、8.x/64ビット
Windows Server	2016年、2019年、2022年/ 64ビット
Ubuntu	18.04、20.04/64ビット

System Managerのセットアップ

System Managerへのアクセス

System Managerのユーザインターフェイスにアクセスするには、ブラウザでコントローラのIPアドレスを指定します。セットアップウィザードを使用して、システム設定を開始できます。

開始する前に

- 次のいずれかのエクスプレス構成ガイドの説明に従って、ハードウェアを設置して設定します。
  - "Linuxの簡単な設定"
  - "VMwareの簡単な設定"
  - "Windowsの簡単な設定"
- 次の要件を満たす管理ステーションを設定します。
  - 1Gbps以上の速度のネットワークに接続されている。
  - ストレージ管理ポートと同じサブネットに接続されています。
  - データ管理に使用するホスト（I/O接続）ではなく、別のステーションとして使用します。
  - アウトオブバンド管理用にセットアップします。アウトオブバンド管理では、ストレージ管理ステーションからコントローラへのイーサネット接続を介してストレージシステムにコマンドが送信されます。
  - サポートされているブラウザを使用してをセットアップします。を参照して "サポートされるブラウザとオペレーティングシステム"

手順

1. ブラウザで、次のURLを入力します。 `https://<IPAddress>`

   `IPAddress`は、いずれかのストレージアレイコントローラのアドレスです。

設定されていないアレイでSystem Managerを初めて起動すると、[Set Administrator Password]プロンプトが表示されます。

2. 管理者パスワードの設定フィールドとパスワードの確認フィールドに管理者ロールの System Manager パスワードを入力し、 * パスワードの設定 * をクリックします。

   初回ログイン時にセットアップウィザードが起動します。

3. セットアップウィザードを使用して次のタスクを実行します。
   - * ハードウェア（コントローラとドライブ）の確認 * — ストレージアレイ内のコントローラとドライブの数を確認しますアレイに名前を割り当てます。
   - * ホストとオペレーティング・システムの確認 * — ストレージ・アレイがアクセスできるホストとオペレーティング・システムの種類を確認します
   - *Accept pools * — 高速インストール方法の推奨されるプール構成を受け入れますプールはドライブの論理グループです。
   - * アラートの設定 * — ストレージアレイで問題が発生した場合に、 System Manager が自動通知を受信できるようにします。
   - * AutoSupport を有効にする * — ストレージアレイの状態を自動的に監視し、テクニカルサポートにディスパッチを送信します。

セットアップ・ウィザードの詳細については、を参照してください"セットアップウィザードの概要"。

セットアップウィザードの概要

セットアップウィザードを使用して、ストレージアレイ（ハードウェア、ホスト、アプリケーション、ワークロード、プール、アラート、AutoSupportなど）を設定します。

初回セットアップ

System Managerを初めて開いたときは、セットアップウィザードが起動します。セットアップウィザードでは、画面の指示に従って、ストレージアレイの名前の設定、ホストの設定、アプリケーションの選択、ストレージのプールの作成など、基本的な設定タスクを実行します。

> 初期セットアップを続行する前に、アップグレードセンター（メニュー：サポート[Upgrade Center]）に移動し、SANtricity OSソフトウェアが最新であることを確認します。必要に応じて最新バージョンにアップグレードし、ブラウザの表示を更新してセットアップを続行します。詳細については、を参照してください "アップグレードセンターの概要"。

ウィザードをキャンセルした場合、手動で再起動することはできません。ウィザードは、 System Manager を開くかブラウザを更新したときに、次の条件の少なくとも 1 つに該当していれば自動的に再度起動されます。

- プールとボリュームグループが検出されていません。
- ワークロードが検出されていません。
- 通知が設定されていません。

用語

セットアップウィザードでは、次の用語を使用します。

期間	製品説明
アプリケーション	アプリケーションとは、Microsoft SQL ServerやMicrosoft Exchangeなどのソフトウェアプログラムです。
アラート	アラートは、ストレージアレイで発生した重要なイベントについて管理者に通知します。Eメール、SNMPトラップ、またはsyslogを使用してアラートを送信できます。
AutoSupport	AutoSupport機能は、ストレージアレイの健常性を監視し、テクニカルサポートに自動ディスパッチを送信します。
ハードウェア	ストレージシステムハードウェアには、ストレージアレイ、コントローラ、およびドライブが含まれます。
ホスト	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。
オブジェクト	オブジェクトとは、任意の論理または物理ストレージコンポーネントのことです。論理オブジェクトには、ボリュームグループ、プール、ボリュームがあります。物理オブジェクトには、ストレージアレイ、アレイコントローラ、ホスト、ドライブがあります。
プール	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。プールを使用して、ホストにアクセスできる1つ以上のボリュームを作成できます。（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します）。
ボリューム	ボリュームは、アプリケーション、データベース、およびファイルシステムがデータを格納するコンテナです。ホストがストレージアレイのストレージにアクセスするために作成される論理コンポーネントです。 ボリュームは、プールまたはボリュームグループの使用可能な容量から作成します。ボリュームごとに容量が定義されています。ボリュームは複数のドライブで構成される場合もありますが、ホストでは1つの論理コンポーネントとして認識されます。
ボリュームグループ	ボリュームグループは、同じ特性を持つボリュームのコンテナです。ボリュームグループには容量とRAIDレベルが定義されています。ボリュームグループを使用して、ホストにアクセスできる1つ以上のボリュームを作成できます。（ボリュームはボリュームグループまたはプールから作成します）。

期間	製品説明
ワークロード	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（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。

FAQ

すべてのハードウェアコンポーネントが表示されない場合はどうすればよいですか？

[ハードウェアの確認]ダイアログボックスにすべてのハードウェアコンポーネントが表示されない場合は、ドライブシェルフが正しく接続されていないか、互換性のないシェルフがストレージアレイに取り付けられている可能性があります。

すべてのドライブシェルフが正しく接続されていることを確認します。互換性があるドライブシェルフが不明な場合は、テクニカルサポートにお問い合わせください。

すべてのホストが表示されない場合はどうすればよいですか？

接続されているホストが表示されない場合は、自動検出に失敗したか、ホストが正しく接続されていないか、または現在接続されているホストがありません。

ホストは、セットアップの完了後に設定できます。ホストを手動で作成するには、次の手順を実行します。

- ホストを手動で作成し、次のメニューから適切なホストポート識別子を関連付けることができます：Storage [Hosts]。手動で作成したホストは、*初期セットアップ*ウィザードにも表示されます。
- 自動検出が機能するためには、ターゲットとホストにホストポートタイプ（iSCSIやNVMe over RoCEなど）が設定されており、ストレージへのセッションが確立されている必要があります。

アプリケーションを特定すると、ストレージアレイの管理にどのように役立ちますか？

アプリケーションを特定すると、アプリケーションタイプに基づいてストレージを最適化するボリューム構成がSystem Managerによって自動的に提示されます。

アプリケーション別にボリュームを最適化することで、データストレージの運用効率を高めることができます。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、読み取りキャッシュと書き込みキャッシュなどの特性が含まれます。また、アプリケーション別およびワークロード別のパフォーマンスデータを表示して、アプリケーションおよび関連するワークロードのレイテンシ、IOPS、MiB/秒を評価できます。

ワークロードとは

ネットワーク内の一部のアプリケーション（SQL ServerやExchangeなど）については、そのアプリケーションのストレージを最適化するワークロードを定義できます。

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（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。

ボリュームの作成時には、ワークロードの用途に関する情報を入力するように求められます。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ボリュームの最適な構成が作成され、必要に応じて編集することもできます。

AutoSupportの配信方法を設定するにはどうすればよいですか。

AutoSupport 配信方法の設定タスクにアクセスするには、[Support]（サポートセンター）のメニューに移動し、AutoSupport *]タブをクリックします。

サポートされているプロトコルは、HTTPS、HTTP、およびSMTPです。

推奨されるプール構成を承認するかどうかを判断するにはどうすればよいですか。

推奨されるプール構成を承認するかどうかは、いくつかの要因によって決まります。

次の質問に答えて、要件に最適なストレージのタイプを特定します。

- 最大のプールではなく、容量の小さいプールを複数使用することを希望しますか。
- プールよりもRAIDボリュームグループを使用することを希望しますか？
- 推奨される構成ではなく、ドライブを手動でプロビジョニングすることを希望しますか？

これらの質問のいずれかに「はい」と回答した場合は、推奨されるプール構成を拒否することを検討してください。

ホストが検出されませんでした。どうすればいいですか？

接続されているホストが表示されない場合は、自動検出に失敗したか、ホストが正しく接続されていないか、または現在接続されているホストがありません。

ホストは、セットアップの完了後に設定できます。ホストを手動で作成するには、次の手順を実行します。

- ホストを手動で作成し、次のメニューから適切なホストポート識別子を関連付けることができます：Storage [Hosts]。手動で作成したホストは、*初期セットアップ*ウィザードにも表示されます。
- 自動検出が機能するためには、ターゲットとホストにホストポートタイプ（iSCSIやNVMe over RoCEなど）が設定されており、ストレージへのセッションが確立されている必要があります。

Unified Managerセットアップ

Unified Managerをインストールする

Unified ManagerはWebサービスプロキシに含まれています。Webサービスプロキシは、NetApp Eシリーズストレージシステムを管理するためにホストシステムに別途インストールするRESTful APIサーバです。

Web Services ProxyとUnified Managerをインストールするには、EシリーズおよびSANtricityドキュメントセンターで次の手順を参照してください。

1. "インストールとアップグレードの要件を確認する"
2. "Web Services Proxyファイルをダウンロードしてインストールする"

Unified Managerへのアクセス

Web Services Proxyをインストールしたら、Unified Managerにアクセスして Webベースのインターフェイスで複数のストレージシステムを管理できます。

サポートされるブラウザについては、を参照してください"サポートされるブラウザとオペレーティングシステム"。

手順

1. ブラウザを開き、次のURLを入力します。

   `http[s]://<server>:<port>/um`

   このURLで、 `<server>`はWeb Services ProxyがインストールされているサーバのアドレスまたはFQDN、 `<port>`はリスニングポート番号（デフォルトはHTTPの場合は8080、HTTPSの場合は8443）です。

   Unified Managerのログインページが開きます。

2. 初回ログインの場合は、ユーザ名にと入力し `admin`、adminユーザのパスワードを設定して確認します。

   パスワードには最大30文字を使用できます。

ユーザとパスワードの詳細については、を参照してください"アクセス管理の仕組み"。

System Manager 11.8による単一アレイの管理

メインインターフェイス

System Managerインターフェイスの概要

System Managerは、ストレージアレイを1つのビューで管理できるWebベースのインターフェイスです。

ホームページ

[ホーム]ページには、ストレージアレイの日 々 の管理用にダッシュボードビューが表示されます。System Managerにログインすると、最初に表示される画面がホームページになります。

ダッシュボードビューは4つの概要領域で構成され、ストレージアレイの状態と健全性に関する重要な情報が表示されます。詳細については、サマリー領域を参照してください。

面積	製品説明
通知	[通知]領域には、ストレージアレイとそのコンポーネントのステータスを示す問題の通知が表示されます。また、自動アラートが表示され、ストレージ環境の他の領域に影響が及ぶ前に問題をトラブルシューティングできます。
パフォーマンス	[パフォーマンス]領域では、リソース使用量の推移を比較できます。応答時間（IOPS）、転送速度（MiB/秒）、使用中の処理容量（CPU）について、ストレージアレイのパフォーマンス指標を表示できます。
容量	[容量]領域には、ストレージアレイ内の割り当て済み容量、空きストレージ容量、未割り当てのストレージ容量がグラフで表示されます。
ストレージ階層	[Storage Hierarchy]領域には、ストレージアレイで管理されているさまざまなハードウェアコンポーネントやストレージオブジェクトがまとめて表示されます。ドロップダウン矢印をクリックして、ハードウェアコンポーネントまたはストレージオブジェクトに対して特定の操作を実行します。

インターフェイス設定

メインインターフェイスから表示設定やその他の設定を変更できます。

設定	製品説明
表示環境設定	インターフェイスの右上にある[Preferences]ドロップダウンから容量の値と期間を変更します。
セツシヨンタイムアウト	非アクティブな状態が一定の時間続いたユーザセッションは切断されるようにタイムアウトを設定します。

設定	製品説明
ヘルプ	インターフェイスの右上にあるドロップダウンから、ヘルプドキュメントやその他のリソースにアクセスできます。

ユーザログインとパスワード

システムにログインしている現在のユーザがインターフェイスの右上に表示されます。

ユーザとパスワードの詳細については、次を参照してください。

- "管理者パスワード保護の設定"
- "パスワードの変更"

パフォーマンスデータの表示

パフォーマンスの概要

[パフォーマンス]ページでは、ストレージアレイのパフォーマンスを簡単に監視できます。

パフォーマンスデータから何を学ぶことができますか？

パフォーマンスのグラフと表にはパフォーマンスデータがほぼリアルタイムで表示されるため、ストレージアレイで問題が発生しているかどうかを確認できます。また、パフォーマンスデータを保存してストレージアレイの履歴を確認し、問題の発生時期や原因を特定することもできます。

詳細：

- "パフォーマンスのグラフとガイドライン"
- "パフォーマンスの用語"

パフォーマンスデータを表示するにはどうすればよいですか？

パフォーマンスデータには、の[ホーム]ページと[ストレージ]ページからアクセスできます。

詳細：

- "グラフィカルなパフォーマンスデータの表示"
- "表形式のパフォーマンスデータの表示と保存"
- "パフォーマンスデータの解釈"

パフォーマンスのグラフとガイドライン

[パフォーマンス]ページに表示されるデータのグラフと表を使用して、いくつかの重要な領域におけるストレージアレイのパフォーマンスを評価できます。

パフォーマンス機能を使用すると、次のタスクを実行できます。

- パフォーマンスデータをほぼリアルタイムで表示し、ストレージアレイに問題が発生しているかどうかを確認できます。
- パフォーマンスデータをエクスポートしてストレージアレイの履歴を確認し、問題の発生時期や原因を特定できます。
- 表示するオブジェクト、パフォーマンス指標、期間を選択します。
- 指標を比較する。

パフォーマンスデータは次の3つの形式で表示できます。

- リアルタイムのグラフ--パフォーマンスデータをほぼリアルタイムでグラフに出力します。
- ほぼリアルタイムの表--パフォーマンスデータをほぼリアルタイムで表に表示します。
- エクスポートされた**CSV**ファイル--表形式のパフォーマンスデータを'さらに表示および分析するためにカンマ区切りのファイルに保存できます

パフォーマンスデータ形式の特徴

パフォーマンス監視のタイプ	サンプリング間隔	表示時間の長さ	表示されるオブジェクトの最大数	データの保存機能
リアルタイムのグラフ、ライブ リアルタイムのグラフ、履歴	10秒（ライブ） 5分（履歴） 表示されるデータポイントは選択した期間によって異なる	デフォルトの期間は1時間です。 選択肢： • 5分 • 1時間 • 8時間 • 1日 • 7日 • 30日	5	いいえ
ほぼリアルタイムの表形式（表形式）	10秒~1時間	最新の値	無制限	はい
カンマ区切り値（CSV）ファイル	選択した期間によって異なる	選択した期間によって異なる	無制限	はい

パフォーマンスデータの表示に関するガイドライン

- パフォーマンスデータの収集は常にオンになっています。オフにするオプションはありません。
- サンプリング間隔が経過するたびに、ストレージアレイが照会され、データが更新されます。
- グラフデータの場合は、5分間隔で10秒の間隔で5分間の平均値が更新されます。それ以外の期間はすべて5分ごとに更新され、選択した期間の平均が計算されます。
- グラフビューのパフォーマンスデータはリアルタイムで更新されます。表形式のパフォーマンスデータ

は、ほぼリアルタイムで更新されます。

- データの収集中に監視対象オブジェクトが変更された場合は、選択した期間にわたるデータポイントの完全なセットがオブジェクトに存在しない可能性があります。たとえば、ボリュームが作成、削除、割り当て、割り当て解除されるたびにボリュームセットが変更されたり、ドライブが追加、削除、障害状態になったりする可能性があります。

パフォーマンスの用語

ストレージアレイに関連するパフォーマンスの用語を次に示します。

期間	製品説明
アプリケーション	アプリケーションとは、SQLやExchangeなどのソフトウェアプログラムです。
CPU	CPUは、Central Pocessing Unit（中央処理装置）の略です。ストレージ アレイの処理能力のうち使用中の割合を示します。
ホスト	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。
IOPS	IOPSは、1秒あたりのI/O処理数です。
レイテンシ	レイテンシは、読み取りや書き込みコマンドなどの要求を送信してから、ホストまたはストレージアレイから応答が返されるまでの時間です。
LUN	Logical Unit Number（LUN；論理ユニット番号）は、ホストがボリュームへのアクセスに使用する番号で、アドレススペースに割り当てられます。ボリュームは、LUNの形式で容量としてホストに提示されます。 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を異なるホストで使用して、異なるボリュームにアクセスできます。
MIB	MiBは、メビバイト（メガバイナリバイト）の略です。1MiBは220、つまり1、048、576バイトです。10を基数とするMBとは異なる単位です。1MBは1、024バイトです。
オブジェクト	オブジェクトとは、任意の論理または物理ストレージコンポーネントのことです。 論理オブジェクトには、ボリュームグループ、プール、ボリュームがあります。物理オブジェクトには、ストレージアレイ、アレイコントローラ、ホスト、ドライブがあります。
プール	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。プールを使用して、ホストにアクセスできる1つ以上のボリュームを作成できます。（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します）。
読み取り	読み取りは「読み取り処理」では省略されます。読み取り処理は、ホストがストレージアレイにデータを要求したときに行われます。

期間	製品説明
ボリューム	ボリュームは、アプリケーション、データベース、およびファイルシステムがデータを格納するコンテナです。ホストがストレージアレイのストレージにアクセスするために作成される論理コンポーネントです。 ボリュームは、プールまたはボリュームグループの使用可能な容量から作成します。ボリュームごとに容量が定義されています。ボリュームは複数のドライブで構成される場合もありますが、ホストでは1つの論理コンポーネントとして認識されます。
ボリューム名	ボリューム名は、ボリュームの作成時に割り当てられる文字列です。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。
ボリュームグループ	ボリュームグループは、同じ特性を持つボリュームのコンテナです。ボリュームグループには容量とRAIDレベルが定義されています。ボリュームグループを使用して、ホストにアクセスできる1つ以上のボリュームを作成できます。（ボリュームはボリュームグループまたはプールから作成します）。
ワークロード	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（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。
書き込み	書き込みは、ホストからストレージ用のアレイにデータが送信されるときの「書き込み処理」には適していません。

グラフィカルなパフォーマンスデータの表示

論理オブジェクト、物理オブジェクト、アプリケーション、およびワークロードのパフォーマンスグラフデータを表示できます。

タスクの内容

パフォーマンスグラフには、履歴データとキャプチャ中のライブデータが表示されます。「ライブ更新」というラベルの付いたグラフ上の縦線は、履歴データとライブデータを区別します。

ホームページ表示

ホームページには、ストレージアレイレベルのパフォーマンスを示すグラフが表示されます。このビューから限定された指標を選択することも、「*パフォーマンスの詳細を表示」をクリックして利用可能なすべての指標を選択することもできます。

詳細表示

詳細なパフォーマンスビューに表示されるグラフは、次の3つのタブに分かれています。

- 論理ビュー--ボリュームグループおよびプール別にグループ化された論理オブジェクトのパフォーマンスデータを表示します論理オブジェクトには、ボリュームグループ、プール、ボリュームがあります。
- 物理ビュー--コントローラ、ホストチャネル、ドライブチャネル、ドライブのパフォーマンスデータを表示します。
- アプリケーションとワークロードビュー-定義したアプリケーションタイプとワークロード別にグループ化された論理オブジェクト（ボリューム）のリストが表示されます。

手順

1. 「* Home *」を選択します。
2. アレイレベルのビューを選択するには、[IOPS]、[MiB/秒]、または[CPU]ボタンをクリックします。
3. 詳細を表示するには、*パフォーマンスの詳細を表示*をクリックします。
4. 論理ビュー*タブ、*物理ビュー*タブ、または*アプリケーションとワークロードの表示*タブを選択します。

   オブジェクトタイプに応じて、各タブに異なるグラフが表示されます。

ビューのタブ	各オブジェクトタイプについて表示されるパフォーマンスデータ
論理ビュー	• ストレージアレイ：IOPS、MiB/秒 • プール：レイテンシ、IOPS、MiB/秒 • ボリュームグループ：レイテンシ、IOPS、MiB/秒 • ボリューム：レイテンシ、IOPS、MiB/秒
物理ビュー	• コントローラ：IOPS、MiB/秒、CPU、ヘッドルーム • ホストチャネル：レイテンシ、IOPS、MiB/秒、ヘッドルーム • ドライブチャネル：レイテンシ、IOPS、MiB/秒 • ドライブ：レイテンシ、IOPS、MiB/秒
アプリケーションとワークロードビュー	• ストレージアレイ：IOPS、MiB/秒 • アプリケーション：レイテンシ、IOPS、MiB/秒 • ワークロード：レイテンシ、IOPS、MiB/秒 • ボリューム：レイテンシ、IOPS、MiB/秒

5. オプションを使用して、必要なオブジェクトと情報を表示します。

オプション

オブジェクトを表示するためのオプション	製品説明
ドロワーを展開すると、オブジェクトのリストが表示されます。	_Navigationドロワー_には、プール、ボリュームグループ、ドライブなどのストレージオブジェクトが含まれます。 ドロワーをクリックすると、ドロワー内のオブジェクトのリストが表示されます。
表示するオブジェクトを選択します。	各オブジェクトの左側にあるチェックボックスをオンにして、表示するパフォーマンスデータを選択します。
フィルタを使用して、オブジェクト名または名前の一部を検索します。	[フィルタ]ボックスに、オブジェクトの名前または名前の一部を入力して、それらのオブジェクトだけをドロワーに表示します。
オブジェクトを選択した後、*グラフの更新*をクリックします。	ドロワーからオブジェクトを選択した後、[グラフの更新]を選択して、選択した項目のグラフデータを表示します。
グラフの表示/非表示	グラフの表示と非表示を切り替えるには、グラフのタイトルを選択します。

6. 必要に応じて、パフォーマンスデータを表示するための追加のオプションを使用します。

その他のオプション

オプション	製品説明
期間	表示する時間の長さ（5分、1時間、8時間、1日、7日、または30日）を選択します。デフォルトは1時間です。 30日間のパフォーマンスデータのロードには数分かかることがあります。データのロード中は、Webページから移動したり、Webページを更新したり、ブラウザを閉じたりしないでください。
データポイントの詳細	グラフにカーソルを合わせると、特定のデータポイントの指標が表示されます。
スクロールバー	グラフの下にあるスクロールバーを使用して、前後の期間を表示します。
ズームバー	グラフの下にあるズームバーハンドルをドラッグして、期間をズームアウトします。ズームバーが広いほど、グラフの詳細は細分化されません。 グラフをリセットするには、いずれかの期間のオプションを選択します。
ドラッグアンドドロップ	グラフ上で、カーソルをある時点から別の時点にドラッグすると、特定の期間を拡大表示できます。 グラフをリセットするには、いずれかの期間のオプションを選択します。

表形式のパフォーマンスデータの表示と保存

パフォーマンスグラフのデータを表形式で表示および保存できます。これにより、表示するデータをフィルタできます。

手順

1. 任意のパフォーマンスデータグラフから、[テーブルビューの起動*]をクリックします。

   選択したオブジェクトのすべてのパフォーマンスデータがリストされたテーブルが表示されます。

2. 必要に応じて、オブジェクト選択のプルダウンとフィルタを使用します。
3. [列の表示/非表示*]ボタンをクリックして、テーブルに含める列を選択します。

   各チェックボックスをクリックすると、項目を選択または選択解除できます。

4. 画面下部の* Export *（エクスポート）を選択して、表形式ビューをカンマ区切り値（CSV）のファイルに保存します。

   [テーブルのエクスポート]ダイアログボックスが表示され、エクスポートする行の数とエクスポートのファイル形式（カンマ区切り値またはCSV形式）が示されます。

5. 「* Export（エクスポート）」をクリックしてダウンロードを続行するか、「 Cancel（キャンセル）*」をクリックします。

   ブラウザの設定に応じて、ファイルが保存されるか、ファイルの名前と場所を選択するように求められます。

   デフォルトのファイル名の形式はで、 `performanceStatistics-yyyy-mm-dd_hh-mm-ss.csv`ファイルがエクスポートされた日時が含まれます。

パフォーマンスデータの解釈

パフォーマンスデータは、ストレージアレイのパフォーマンスの調整に役立ちます。

パフォーマンスデータを解釈するときは、いくつかの要因がストレージアレイのパフォーマンスに影響することに注意してください。次の表に、考慮すべき主な領域を示します。

パフォーマンスデータ	パフォーマンス調整の関連事項
レイテンシ（ミリ秒、ms ）	特定のオブジェクトのI/Oアクティビティを監視します。 ボトルネックになっているオブジェクトを特定できる可能性があります。 • ボリュームグループを複数のボリュームで共有する場合は、ドライブのシーケンシャルパフォーマンスを向上させてレイテンシを低減するために、個 々のボリュームに独自のボリュームグループが必要になることがあります。 • プールではレイテンシが大きくなり、ドライブ間でワークロードが不均一な場合があるため、レイテンシの値はあまり意味がなく、一般的に高くなります。 • ドライブのタイプと速度はレイテンシに影響します。ランダムI/Oを使用すると、回転式ドライブが高速であるため、ディスク上のさまざまな場所への移動にかかる時間が短縮されます。 • ドライブの数が少なすぎると、キューに登録されるコマンドが多くなり、ドライブがコマンドを処理する時間が長くなり、システムの一般的なレイテンシが増加します。 • I/Oが大きいほど、データ転送にかかる時間が長くなるため、レイテンシが大きくなります。 • レイテンシが高い場合は、I/Oパターンが本質的にランダムである可能性があります。ランダムI/Oのドライブは、シーケンシャルストリームのドライブよりもレイテンシが高くなります。 • 共通のボリュームグループのドライブ間またはボリューム間でレイテンシが異なる場合は、ドライブが低速であることを示している可能性があります。

パフォーマンスデータ	パフォーマンス調整の関連事項
IOPS	1秒あたりの入出力処理（IOPSまたはIO/秒）に影響する要因には、次の項目があります。 • アクセスパターン（ランダムまたはシーケンシャル） • I/Oサイズ • RAIDレベル • キャッシュブロックサイズ • 読み取りキャッシュが有効かどうか • 書き込みキャッシュが有効かどうか • 動的キャッシュ読み取りプリフェッチ • セグメントサイズ • ボリュームグループまたはストレージアレイ内のドライブ数 キャッシュヒット率が高いほど、I/O速度は高くなります。書き込みキャッシュが有効な場合の方が、無効な場合に比べて書き込みI/O速度が高くなります。個々のボリュームの書き込みキャッシュを有効にするかどうかを判断するときは、現在のIOPSと最大IOPSを確認します。シーケンシャルI/Oパターンの方が、ランダムI/Oパターンよりも高速です。I/Oパターンに関係なく、書き込みキャッシュを有効にしてI/O速度を最大化し、アプリケーションの応答時間を短縮します。 ボリュームのIOPS統計では、セグメントサイズの変更によるパフォーマンスの向上を確認できます。実験して最適なセグメントサイズを決定するか、ファイルシステムサイズまたはデータベースブロックサイズを使用します。
MiB/秒	転送またはスループットの速度は、アプリケーションのI/Oサイズと I/O速度によって決まります。一般に、アプリケーションのI/O要求が小さいと転送速度は低下しますが、I/O速度は速く、応答時間は短くなります。アプリケーションのI/O要求のサイズが大きい場合は、スループットが高速になる可能性があります。 一般的なアプリケーションのI/Oパターンを理解しておくと、特定のストレージアレイの最大I/O転送速度を決定するのに役立ちます。
CPU	使用中の処理能力の割合を示します。 同じタイプのオブジェクトのCPU使用率に差異がある場合があります。たとえば、一方のコントローラのCPU使用率が高いか、時間の経過とともに増加している一方で、もう一方のコントローラのCPU使用率は低く安定しています。この場合、1つ以上のボリュームのコントローラ所有権を、CPU使用率の低いコントローラに変更できます。 ストレージアレイ全体でCPUを監視できます。時間の経過とともにアプリケーションのパフォーマンスが低下する場合は、ストレージアレイの追加が必要になることがあります。ストレージアレイを企業に追加することで、許容可能なパフォーマンスレベルでアプリケーションのニーズを引き続き満たすことができます。

パフォーマンスデータ	パフォーマンス調整の関連事項
ヘッドルーム	ヘッドルームとは、コントローラ、コントローラホストチャネル、およびコントローラドライブチャネルの残りのパフォーマンス容量のことです。この値はパーセンテージで表され、これらのオブジェクトが提供できる最大パフォーマンスと現在のパフォーマンスレベルの差を表します。 • コントローラの場合、ヘッドルームは最大限可能なIOPSの割合です。 • チャネルの場合、ヘッドルームは最大スループット（MiB/秒）の割合です。計算には、読み取りスループット、書き込みスループット、双方向スループットが含まれています。

ストレージ階層の表示

メインインターフェイスのストレージ階層には、ストレージアレイで管理されているさまざまなハードウェアコンポーネントやストレージオブジェクトがまとめて表示されます。

ストレージ階層を表示するには、[ホーム]ページに移動し、ストレージアレイコンポーネントまたはストレージオブジェクトのドロップダウン矢印をクリックします。ストレージアレイは、物理コンポーネントと論理コンポーネントの両方の集合で構成されます。

物理コンポーネント

この表では、ストレージアレイの物理コンポーネントについて説明します。

コンポーネント	製品説明
コントローラ	コントローラは、ボード、ファームウェア、ソフトウェアで構成されます。ドライブを制御し、System Managerの機能を実装します。
シェルフ	シェルフは、キャビネットまたはラックに設置されるエンクロージャです。ストレージアレイのハードウェアコンポーネントが含まれています。シェルフには、コントローラシェルフとドライブシェルフの2種類があります。コントローラシェルフにはコントローラとドライブが搭載されます。ドライブシェルフには、入出力モジュール（IOM）とドライブが搭載されています。 ストレージアレイのメディアタイプやインターフェイスタイプが異なる場合は、ドライブタイプごとにドライブシェルフが表示されます。
ドライブ	ドライブは、データの物理ストレージメディアとして使用される、電磁的な機械デバイスまたはソリッドステートメモリデバイスです。
ホスト	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。
ホストバスアダプタ（HBA）	ホストバスアダプタ（HBA）はホストに搭載されるボードで、1つ以上のホストポートが搭載されています。

コンポーネント	製品説明
ホストポート	ホストポートは、コントローラに物理的に接続されるホストバスアダプタ（HBA）のポートで、I/O処理に使用されます。
管理クライアント	管理クライアントは、System Managerにアクセスするためのブラウザがインストールされたコンピュータです。

論理コンポーネント

ストレージアレイ内のドライブは、データ用の物理ストレージ容量を提供します。System Managerを使用して、物理容量をプール、ボリュームグループ、ボリュームなどの論理コンポーネントに設定します。これらのコンポーネントは、ストレージアレイのデータの設定、格納、保守、保持に使用するツールです。次の表では、ストレージアレイの論理コンポーネントについて説明します。

コンポーネント	製品説明
プール	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。プールを使用して、ホストにアクセスできる1つ以上のボリュームを作成できます。（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します）。
ボリュームグループ	ボリュームグループは、同じ特性を持つボリュームのコンテナです。ボリュームグループには容量とRAIDレベルが定義されています。ボリュームグループを使用して、ホストにアクセスできる1つ以上のボリュームを作成できます。（ボリュームはボリュームグループまたはプールから作成します）。
ボリューム	ボリュームは、アプリケーション、データベース、およびファイルシステムがデータを格納するコンテナです。ホストがストレージアレイのストレージにアクセスするために作成される論理コンポーネントです。
論理ユニット番号（LUN）	Logical Unit Number（LUN；論理ユニット番号）は、ホストがボリュームへのアクセスに使用する番号で、アドレススペースに割り当てられます。ボリュームは、LUNの形式で容量としてホストに提示されます。 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を異なるホストで使用して、異なるボリュームにアクセスできます。

インターフェイス設定の管理

パスワード保護の管理

不正なアクセスから保護するために、ストレージアレイにパスワードを設定する必要があります。

パスワードの設定と変更

System Managerの初回起動時に、管理者パスワードを設定するように求められます。adminパスワードを持つユーザは、オブジェクトや設定の追加、変更、削除など、ストレージアレイの設定を変更できます。初回起動時にadminパスワードを設定するには、を参照してください"System Managerへのアクセス"。

セキュリティ上の理由から、パスワードの入力を試行できるのは5回までです。この回数を超えると、ストレージアレイは「ロックアウト」状態になります。この状態の場合、ストレージアレイは以降のパスワードの入力を拒否します。パスワードをもう一度入力するには、ストレージアレイが「通常」の状態にリセットされるまで10分待つ必要があります。

ストレージアレイには、adminパスワードに加えて、1つ以上のロールがマッピングされた事前定義されたユーザプロファイルが含まれています。詳細については、を参照してください "マッピングされたロールの権限"。ユーザプロファイルとマッピングは変更できません。変更できるのはパスワードのみです。adminパスワードまたはその他のユーザパスワードを変更する場合は、を参照してください"パスワードの変更"。

セッションタイムアウト後のパスワードの再入力

パスワードの入力を求めるプロンプトは、1つの管理セッションで1回だけ表示されます。ただし、30分間操作を行わないとセッションはタイムアウトし、その時点でパスワードを再入力する必要があります。セッションの実行中に別の管理クライアントから同じストレージアレイを管理している別のユーザがパスワードを変更した場合は、次回の設定処理または表示処理でパスワードの入力を求められます。

セッションタイムアウトを調整することも、セッションタイムアウトを完全に無効にすることもできます。を参照して "セッションタイムアウトの管理"

ドライブまたはパスワードによる保護の解除

パスワードで保護されたドライブを取り外す場合、またはパスワード保護を無効にする場合は、次の点に注意してください。

- *パスワード保護が設定されたドライブを取り外すと、パスワードはストレージアレイの各ドライブの予約領域に保存されます。ストレージアレイからすべてのドライブを取り外すと、そのパスワードは機能しなくなります。この状況を修正するには、元のドライブの1つをストレージアレイに再取り付けします。
- パスワード保護を解除する場合--コマンドのパスワード保護を解除する場合は'現在の管理者パスワードを入力し'新しいパスワードのテキストボックスを空白のままにします

> ストレージアレイで設定コマンドを実行すると、データ損失などの重大な損傷が発生する可能性があります。そのため、ストレージアレイには管理者パスワードを常に設定する必要があります。セキュリティを強化するために、英数字15文字以上の長い管理者パスワードを使用してください。

容量値のデフォルトの単位を設定

System Managerでは、容量値をギビバイト（GiB）またはテビバイト（TiB）で表示できます。

すべてのユーザが独自の設定を使用できるように、設定はブラウザのローカルストレージに保存されます。

手順

1. メニューを選択します。環境設定[環境設定]。
2. 「ギビバイト」または「テビバイト」のラジオボタンをクリックして、処理を実行することを確認します。

   略語と値については、次の表を参照してください。

略語	値
GIB	1、024 [3]バイト
TiB	1、024[4]バイト

パフォーマンスグラフのデフォルト期間の設定

パフォーマンスグラフに表示されるデフォルトの期間を変更できます。

タスクの内容

[ホーム]ページと[パフォーマンス]ページのパフォーマンスグラフに最初に表示される期間は1時間です。すべてのユーザが独自の設定を使用できるように、設定はブラウザのローカルストレージに保存されます。

手順

1. メニューを選択します。環境設定[環境設定]。
2. ドロップダウンリストから、* 5分*、* 1時間*、* 8時間*、* 1日*、または* 7日*のいずれかを選択します。処理を確定します。

ログインバナーの設定

ユーザがSystem Managerでセッションを確立する前に表示されるログインバナーを作成できます。バナーには、注意事項と同意メッセージを含めることができます。

タスクの内容

作成したバナーは、ログイン画面の前にダイアログボックスに表示されます。

手順

1. メニューを選択します。[設定][システム]。
2. [全般]セクションで、[ログインバナーの設定*]を選択します。

   Configure Login Bannerダイアログボックスが開きます。

3. ログインバナーに表示するテキストを入力します。

   書式設定にHTMLやその他のマークアップタグを使用しないでください。

4. [保存（ Save ）] をクリックします。

結果

ユーザが次回System Managerにログインすると、このテキストがダイアログボックスに表示されます。ログイン画面に進むには、*OK*をクリックする必要があります。

セッションタイムアウトの管理

非アクティブな状態が一定の時間続いたユーザセッションは切断されるよう、System

Managerでタイムアウトを設定できます。

タスクの内容

デフォルトでは、System Managerのセッションタイムアウトは30分です。この時間を調整したり、セッションタイムアウトを無効にしたりすることができます。

> アレイに組み込みのSecurity Assertion Markup Language（SAML）機能を使用してアクセス管理を設定している場合、ユーザのSSOセッションが最大数に達したときにセッションタイムアウトが発生することがあります。これは、System Managerのセッションタイムアウトより前に発生することがあります。

手順

1. メニューを選択します。[設定][システム]。
2. [全般]セクションで、[セッションタイムアウトの有効化/無効化]を選択します。

   セッションタイムアウトの有効化/無効化ダイアログボックスが開きます。
3. スピナーコントロールを使用して、時間を分単位で増減します。

   System Managerに設定できる最小のタイムアウトは15分です。

   > セッションタイムアウトを無効にするには、*時間の長さを設定*チェックボックスの選択を解除します。
4. [保存（ Save ）] をクリックします。

通知の管理

問題通知の概要

System Managerは、アイコンおよびその他のいくつかの方法を使用して、ストレージアレイに問題が存在することを通知します。

アイコン

System Managerでは、以下のアイコンを使用してストレージアレイおよびそのコンポーネントのステータスが表示されます。

をクリックします。	製品説明
	最適
	最適でない、または障害が発生している
	対応または修正が必要
	注意

これらのアイコンはSystem Managerのさまざまな場所に表示されます。

- [ホーム]ページの[通知]領域に、失敗したアイコンとメッセージが表示されます。
- ナビゲーション領域の[ホーム]ページアイコンに障害アイコンが表示されます。
- [コンポーネント]ページでは、ドライブとコントローラのグラフィックに障害アイコンが表示されます。

アラートと**LED**

System Managerでは、アイコン以外の方法でも問題が通知されます。

- System ManagerはSNMP通知またはEメールのエラーメッセージを送信します。
- ハードウェアの保守操作必要LEDが点灯します。

問題の通知を受け取ったら、Recovery Guruを使用して問題を修正します。必要に応じて、リカバリ手順を記載したハードウェアのドキュメントを参照して、障害が発生したコンポーネントを交換します。

実行中の処理を表示して処理を実行する

長時間の処理を表示して対処するには、[実行中の処理]ページを使用します。

タスクの内容

[実行中の処理]ページに表示された各処理について、完了率と完了までの推定残り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。完了したボリュームコピー処理をリストから消去することもできます。

手順

1. ホームページで、*進行中の操作を表示*を選択します。

   [Operations in Progress]ページが表示されます。

2. 必要に応じて、[アクション]列のリンクを使用して、処理を停止または優先度を変更します。

   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。

   ボリュームコピー処理を停止したり、優先度を変更したりできます。

3. ボリュームコピー処理が完了したら、「クリア」を選択してリストから削除できます。

   ホームページの上部には、処理が完了すると、情報メッセージと黄色のレンチアイコンが表示されます。このメッセージには、[Operations in Progress]ページから操作をクリアできるリンクが含まれています。

[実行中の処理]ページに表示される処理は次のとおりです。

操作	処理のステータス	対処方法
ボリュームコピー	完了	クリア

操作	処理のステータス	対処方法
ボリュームコピー	実行中	• 優先度の変更 • 停止
ボリュームコピー	保留中	クリア
ボリュームコピー	失敗	• クリア • 再コピー
ボリュームコピー	停止	• クリア • 再コピー
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	_ 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	_ なし _
非同期ミラーグループの初期同期	実行中	中断
非同期ミラーグループの初期同期	中断	再開
同期ミラーリング	実行中	中断
同期ミラーリング	中断	再開
Snapshotイメージのロールバック	実行中	キャンセル
Snapshotイメージのロールバック	保留中	キャンセル
Snapshotイメージのロールバック	一時停止	• キャンセル • 再開
ドライブの退避	実行中	キャンセル（ドライブの退避タイプによる）
プールまたはボリュームグループへの容量の追加	実行中	_ なし _
ボリュームのRAIDレベルの変更	実行中	_ なし _
プールの容量削減	実行中	_ なし _

操作	処理のステータス	対処方法
シンボリュームの再生	実行中	_ 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する	実行中	_ なし _
ボリュームグループのデータ冗長性チェック	実行中	_ なし _
ボリュームグループのデフラグ	実行中	_ なし _
ボリュームの初期化	実行中	_ なし _
ボリュームの容量の拡張	実行中	_ なし _
ボリュームのセグメントサイズを変更する	実行中	_ なし _
ドライブコピー	実行中	_ なし _
データ再構築	実行中	_ なし _
コピーバック	実行中	_ なし _
ドライブ消去	実行中	_ なし _
リモートストレージインポート	実行中	• 優先度の変更 • 停止
リモートストレージインポート	停止	• 再開 • 切断
リモートストレージインポート	失敗	• 再開 • 切断
リモートストレージインポート	完了	切断

Recovery Guruを使用した問題からのリカバリ

Recovery GuruはSystem Managerのコンポーネントです。ストレージアレイの問題を診断し、問題を修正するリカバリ手順を推奨します。

手順

1. 「* Home *」を選択します。
2. ウィンドウの中央上部にある*Recover from_n_problems *というリンクをクリックします。

   Recovery Guruダイアログボックスが表示されます。

3. 概要リストに表示された最初の問題を選択し、リカバリ手順の指示に従って問題を修正します。必要に応じて、交換手順を使用して障害のあるコンポーネントを交換します。リストされている問題ごとに、この手順を繰り返します。

   ストレージアレイ内の複数の問題が関連している可能性があります。この場合、問題を修正する順序が結果に影響する可能性があります。サマリーリストに表示されている順序で問題を選択して修正します。

   電源装置キャニスターに複数の障害がある場合、概要リストには1つの問題としてまとめて表示されます。ファンキャニスターで複数の障害が発生した場合も、1つの問題としてリストされます。

4. リカバリ手順 が正常に完了したことを確認するには、*再チェック*をクリックします。

   非同期ミラーグループまたは非同期ミラーグループのメンバーに問題を選択した場合は、最初に* Clear をクリックしてコントローラの障害を解消し、次に Check *をクリックしてRecovery Guruからイベントを削除します。

   すべての問題が修正されると、ストレージアレイアイコンは最終的にNeeds AttentionからOptimalに変わります。一部の問題では、再構築などの処理の実行中に修正アイコンが表示されます。

5. *オプション：Recovery Guruの情報をファイルに保存するには、*保存*アイコンをクリックします。

   ブラウザのDownloadsフォルダにという名前でファイルが保存されます `recovery-guru-failure-yyyy-mm-dd-hh-mm-ss-mmm.html`。

6. Recovery Guruの情報を印刷するには、*印刷*アイコンをクリックします。

FAQ

サポートされているブラウザを教えてください。

System Managerでサポートされるブラウザとバージョンは次のとおりです。

ブラウザ	最小バージョン
Google Chrome	89
Mozilla Firefox	80
Safari	14
Microsoft Edge	90

System Managerをキーボードだけで操作できます。

全体的なナビゲーション

アクション	キーボードショートカット
次の項目に移動する。	タブ
前の項目に移動する。	Shift + Tabキーを押します
項目を選択します。	入力
ドロップダウンリスト—次のアイテムまたは前のアイテムに移動します	下矢印または上矢印
チェックボックス—アイテムを選択します	スペースキー
ラジオボタン—項目間の切り替え	下矢印または上矢印
展開可能なテキスト—アイテムを展開または縮小します	入力

テーブルナビゲーション

アクション	キーボードショートカット
行を選択します。	Tabキーを押して行を選択し、Enterキーを押します。
上下にスクロールします。	下矢印/上矢印またはPage Down / Page Up
列のソート順序を変更します。	Tabキーを押して列見出しを選択し、Enterキーを押します。

カレンダーのナビゲーション

アクション	キーボードショートカット
前の月に移動する。	ページ上へ
次の月に移動する。	ページを下に移動
前の年に移動する。	Ctrl + Page Upキーを押します

アクション	キーボードショートカット
次の年に移動する。	Ctrl + Page Downキーを押します
閉じている場合は、日付ピッカーを開きます。	Ctrl + Homeキー
現在の月に移動する。	Ctrl / Command + Home
前の日に移動する。	Ctrl / Command +左矢印
次の日に移動する。	Ctrl / Command +右矢印
前の週に移動する。	Ctrl / Command +上矢印
次の週に移動する。	Ctrl / Command +下矢印
フォーカスした日付を選択します。	入力
日付ピッカーを閉じて日付を消去します。	Ctrl / Command + End
選択せずに日付ピッカーを閉じます。	エスケープ

個 々 のボリュームのパフォーマンス統計と合計の関係を教えてください。

プールとボリュームグループの統計は、リザーブ容量ボリュームを含むすべてのボリュームを集計して計算されます。

リザーブ容量は、シンボリューム、Snapshot、非同期ミラーリングをサポートするためにストレージシステムによって内部的に使用され、I/Oホストには表示されません。そのため、プール、コントローラ、およびストレージアレイの統計が、表示可能なボリュームの合計ではない場合があります。

ただし、アプリケーションとワークロードの統計については、表示されるボリュームのみが集計されます。

グラフや表にデータがゼロと表示されるのはなぜですか。

グラフや表のデータポイントにゼロが表示されている場合は、その時点でオブジェクトのI/Oアクティビティがないことを意味します。ホストがそのオブジェクトへのI/Oを開始していないか、オブジェクト自体に問題がある可能性があります。

オブジェクトの履歴データは引き続き表示できます。オブジェクトに対してI/Oアクティビティの発生が開始されると、ゼロ以外のデータがグラフと表に表示されます。

次の表に、任意のオブジェクトでデータポイントの値がゼロになる最も一般的な理由を示します。

アレイレベルのオブジェクトタイプ	データがゼロと表示される理由
ボリューム	• ボリュームにホストが割り当てられていない。
ボリュームグループ	• ボリュームグループをインポートしています。 • ボリュームグループにホストに割り当てられているボリュームがありません。*と*のボリュームグループにリザーブ容量が含まれていません。
ドライブ	• ドライブで障害が発生している。 • ドライブが取り外されている。 • ドライブの状態が不明である。
コントローラ	• コントローラがオフラインです。 • コントローラで障害が発生している。 • コントローラが取り外されている。 • コントローラの状態が不明である。
ストレージアレイ	• ストレージアレイにボリュームが含まれていません。

[レイテンシ**]**グラフには何が表示されますか？

レイテンシのグラフには、ボリューム、ボリュームグループ、プールについて、レイテンシの統計がミリ秒（ms）単位で表示されます。 アプリケーション、ワークロードこのグラフは、[Logical View]、[Physical View]、[Applications & Workloads View]の各タブに表示されます。

レイテンシとは、データの読み取りまたは書き込み時に発生する遅延のことです。グラフの特定のポイントにカーソルを合わせると、その時点における次の値（ミリ秒）が表示されます。

- 読み取り時間
- 書き込み時間
- 平均I/Oサイズ

[IOPS]グラフには何が表示されますか？

IOPSグラフには、1秒あたりの入出力処理数の統計が表示されます。ホームページのこのグラフには、ストレージアレイの統計が表示されます。このグラフには、パフォーマンスタイルの論理ビュー、物理ビュー、およびアプリケーションとワークロードのビュータブに、ストレージアレイ、ボリューム、ボリュームグループ、プール、アプリケーションの統計が表示されます。 ワークロードを管理できます。

IOPSは、1秒あたりの入出力（I/O）処理数の略です。グラフの特定のポイントにカーソルを合わせると、その時点における次の値が表示されます。

- 読み取り処理の数
- 書き込み処理の数
- 読み取り処理と書き込み処理の合計数

[MiB/秒]グラフには何が表示されますか。

MiB/秒のグラフでは、転送速度の統計が1秒あたりのメビバイトで表示されます。ホームページのこのグラフには、ストレージアレイの統計が表示されます。このグラフには、パフォーマンスタイルの論理ビュー、物理ビュー、およびアプリケーションとワークロードのビュータブに、ストレージアレイ、ボリューム、ボリュームグループ、プール、アプリケーションの統計が表示されます。 ワークロードを管理できます。

MiB/秒は、1秒あたりのメビバイト数、つまり1秒あたり1、048、576バイト数です。グラフの特定のポイントにカーソルを合わせると、その時点における次の値が表示されます。

- 読み取られたデータの量
- 書き込まれたデータの量
- 読み取られたデータと書き込まれたデータの合計量

[CPU]グラフには何が表示されますか。

[CPU]グラフには、各コントローラ（コントローラAとコントローラB）の処理容量の統計が表示されます。CPUは、_central processing unit_の省略形です。ホームページのこのグラフには、ストレージアレイの統計が表示されます。パフォーマンスタイルの物理ビュータブには、ストレージアレイとドライブの統計が表示されます。

[CPU]グラフには、アレイでの処理に対するCPU処理容量の割合が表示されます。外部I/Oが発生していない場合でも、ストレージオペレーティングシステムがバックグラウンドで処理や監視を実行している可能性があるため、CPU利用率がゼロ以外になることがあります。グラフの特定のポイントにカーソルを合わせると、その時点で使用されている処理機能の割合が表示されます。

[ヘッドルーム]グラフには何が表示されますか？

[ヘッドルーム]グラフには、ストレージアレイコントローラの残りのパフォーマンス容量が表示されます。このグラフは、ホームページおよびパフォーマンスタイルの物理ビュータブに表示されます。

[ヘッドルーム]グラフには、ストレージシステム内の物理オブジェクトの残りのパフォーマンス容量が表示されます。グラフの特定のポイントにカーソルを合わせると、コントローラAとコントローラBの残りのIOPSおよびMiB/秒能力の割合が表示されます。

表示設定に関する詳しい情報は、どこで入手できますか。

使用可能な表示オプションに関する情報を検索するには、次の手順に従います。

- 容量値を表示するためのデフォルトの単位の詳細については、を参照してください"容量値のデフォルトの単位を設定"。

- パフォーマンスグラフを表示するデフォルトの期間の詳細については、を参照してください"パフォーマンスグラフのデフォルト期間の設定"。

プールとボリュームグループ

プールとボリュームグループの概要

ストレージアレイ内の未割り当てドライブのサブセットから論理ストレージ容量を作成できます。この論理容量は、環境のニーズに応じてプールまたはボリュームグループのどちらかになります。

プールとボリュームグループとは

a_pool_は、論理的にグループ化されたドライブのセットです。a_volume group_は、特性が共有されているボリュームのコンテナです。プールまたはボリュームグループを使用して、ホストにアクセスできるボリュームを作成できます。

詳細：

- "プールとボリュームグループの機能"
- "容量に関する用語"
- "プールとボリュームグループのどちらを使用するかを決定する"

プールはどのように作成しますか？

System Managerでストレージアレイ内に未割り当て容量が検出されたときにプールを自動的に作成することができます。最適な構成を自動作成で判断できない場合は、ストレージ[プールとボリュームグループ]メニューからプールを手動で作成することもできます。

詳細：

- "プールの自動作成と手動作成"
- "プールの自動作成"
- "プールの手動作成"
- "プールまたはボリュームグループへの容量の追加"

ボリュームグループはどのようにして作成しますか？

メニューからボリュームグループを作成できます。Storage [Pools & Volume Groups]

詳細：

- "ボリュームグループの作成"
- "プールまたはボリュームグループへの容量の追加"

関連情報

プールとボリュームグループに関連する概念については、以下を参照してください。

- "リザーブ容量の仕組み"
- "SSDキャッシュの仕組み"

概念

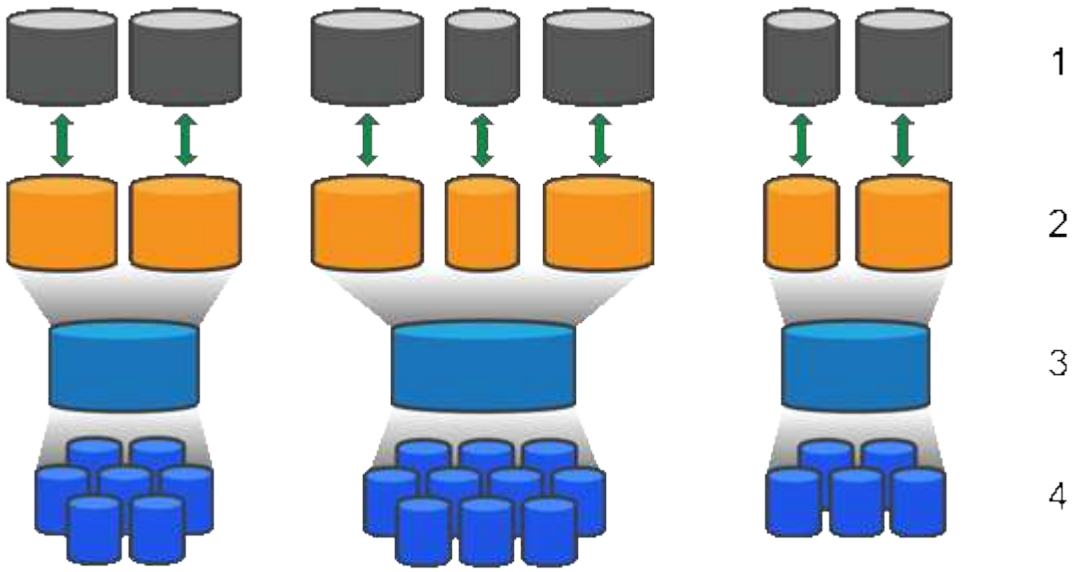
プールとボリュームグループの機能

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）ドライブを含むプールまたはボリュームグループを作成します。

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
- RAID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分割に分割します。これらの論理区分内には、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。次の図は、この概念を示しています。



^1 ホストLUN；2ボリューム；3ボリュームグループまたはプール；4^ HDDまたはSSDドライブ

ストレージシステムを導入したら、最初に次の方法で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。

- 十分な容量を備えたプールまたはボリュームグループの作成
- パフォーマンス要件を満たすために必要なドライブ数をプールまたはボリュームグループに追加
- 特定のビジネス要件を満たすために必要なレベルのRAID保護を選択する（ボリュームグループを使用す

る場合）

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含めることはできますが、1つ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含めることはできません。次に、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用にホストに提供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大きなストレージスペースに集約し、RAID保護を強化するよう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。ドライブを紛失したり追加したりした場合、System Managerによって、アクティブなドライブ全体にわたってデータのリバランシングが動的に行われます。

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。System Managerは、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レベルを自動的に6に設定します。

ドライブの一致

プールにはHDDまたはSSDのどちらかを選択できます。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で同じテクノロジを使用する必要があります。対象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、ドライブで障害が発生した場合のスペア容量用に1ドライブ分の容量がリザーブされます。この予備容量は「予約済み容量」と呼ばれます。

プールが作成されると、緊急時に使用するために一定量の容量が保持されます。この容量はSystem Managerではドライブ数で表されますが、実際の実装はドライブプール全体に分散されます。デフォルトで保持される容量は、プール内のドライブの数によって決まります。

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。保持できる最大容量（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、使用可能な容量は少なくなる場合があります。

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ボリュームに容量を割り当てる方法を定義します。ディスクドライブはRAIDグループに編成され、ボリュームはRAIDグループ内の複数のドライブにまたがって配置されます。したがって、ボリュームグループの構成設定によって、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、グループに含めるドライブが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ものです。

ドライブの一致

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

プ内のドライブのサイズが小さい場合は、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に低速のドライブがある場合は、すべてのドライブが最も低速のドライブとして認識されます。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ドライブと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格納されず、ストレージアレイの冗長性が強化されます。

ストレージアレイ内のドライブで障害が発生した場合は、障害が発生したドライブの代わりにホットスペアドライブが自動的に使用されます。物理的に交換する必要はありません。ドライブに障害が発生したときにホットスペアドライブを使用できる場合、コントローラは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を再構築します。

容量に関する用語

ストレージアレイに関連する容量の用語を次に示します。

ストレージオブジェクト

次の用語は、ストレージアレイを操作できるさまざまなタイプのストレージオブジェクトを示しています。

ストレージオブジェクト	製品説明
ホスト	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。
LUN	Logical Unit Number（LUN；論理ユニット番号）は、ホストがボリュームへのアクセスに使用する番号で、アドレススペースに割り当てられます。ボリュームは、LUNの形式で容量としてホストに提示されます。 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を異なるホストで使用して、異なるボリュームにアクセスできます。
ミラー整合性グループ	ミラー整合性グループは、1つ以上のミラーペアのコンテナです。非同期ミラーリング処理では、ミラー整合性グループを作成する必要があります。
ミラーボリュームペア	ミラーペアは、プライマリボリュームとセカンダリボリュームの2つのボリュームで構成されます。
プール	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。プールを使用して、ホストにアクセスできる1つ以上のボリュームを作成できます。（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します）。

ストレージオブジェクト	製品説明
Snapshot整合性グループ	Snapshot整合性グループは、Snapshotイメージが作成されるときに1つのエンティティとして扱われるボリュームの集まりです。各ボリュームには独自のSnapshotイメージがありますが、すべてのイメージは同じ時点で作成されます。
Snapshotグループ	Snapshotグループは、1つのベースボリュームのSnapshotイメージの集まりです。
Snapshotボリューム	Snapshotボリュームを使用すると、ホストはSnapshotイメージのデータにアクセスできます。Snapshotボリュームには独自のリザーブ容量が含まれているため、元のSnapshotイメージに影響を与えることなくベースボリュームへの変更が保存されます。
ボリューム	ボリュームは、アプリケーション、データベース、およびファイルシステムがデータを格納するコンテナです。ホストがストレージアレイのストレージにアクセスするために作成される論理コンポーネントです。
ボリュームグループ	ボリュームグループは、同じ特性を持つボリュームのコンテナです。ボリュームグループには容量とRAIDレベルが定義されています。ボリュームグループを使用して、ホストにアクセスできる1つ以上のボリュームを作成できます。（ボリュームはボリュームグループまたはプールから作成します）。

ストレージ容量

次の用語は、ストレージアレイで使用されているさまざまなタイプの容量を示しています。

容量タイプ	製品説明
割り当て容量	割り当て容量は、プールまたはボリュームグループ内のドライブから割り当てられた物理容量です。 割り当て容量は、ボリュームの作成やコピーサービス処理に使用します。
空き容量	空き容量は、ボリュームの作成処理やコピーサービス処理、およびストレージオブジェクトにまだ割り当てられていないプールまたはボリュームグループ内の使用可能な容量です。
プールまたはボリュームグループの容量	プール、ボリューム、またはボリュームグループの容量は、プールまたはボリュームグループに割り当てられているストレージアレイ内の容量です。この容量は、ボリュームを作成し、コピーサービス処理やストレージオブジェクトで必要とされるさまざまな容量に対応するために使用されます。
プールの使用不可容量	プールの使用不可容量は、ドライブサイズの不一致が原因で使用できないプール内のスペースです。

容量タイプ	製品説明
予約済み容量	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。
レポート容量	レポート容量は、ホストに報告され、ホストからアクセスできる容量です。
リザーブ容量	リザーブ容量は、コピーサービス処理やストレージオブジェクトに使用される物理割り当て容量です。ホストから直接読み取ることはできません。
SSD キャッシュ	SSDキャッシュは、ストレージアレイ内で論理的にグループ化したソリッドステートディスク（SSD）ドライブのセットです。SSDキャッシュ機能は、アクセス頻度が最も高いデータ（「ホット」データ）を低レイテンシのSSDドライブにキャッシュすることで、アプリケーションワークロードを動的に高速化します。
未割り当て容量	未割り当て容量は、ストレージアレイ内のスペースのうち、プールまたはボリュームグループに「割り当てられていない」スペースです。
書き込み済み容量	書き込み済み容量は、シンボリュームに割り当てられたリザーブ容量のうちの書き込み済みの容量です。

プールとボリュームグループのどちらを使用するかを決定する

ボリュームはプールまたはボリュームグループを使用して作成できます。最適な選択は、主に、想定されるI/Oワークロードなどの主なストレージ要件、パフォーマンス要件、データ保護要件によって異なります。

プールまたはボリュームグループを選択する理由

プールを選択

- 高速なドライブリビルドやストレージ管理の簡易化が必要な場合、シンボリュームが必要な場合、大量のランダムワークロードを実行する場合。
- 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

- システム帯域幅の最大化、ストレージ設定の調整、大量のシーケンシャルワークロードが必要な場合。
- 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の作成時に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順次書き込む場合。

プールはボリュームグループと共存できるため、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。

プールとボリュームグループの機能の違い

次の表に、ボリュームグループとプールの機能の比較を示します。

使用	プール	ボリュームグループ
ランダムワークロード	より良い	良い
シーケンシャルワークロード	良い	より良い
ドライブのリビルド時間	高速化	遅い
パフォーマンス（最適モード）	Good：小規模ブロックのランダムワークロードに最適です。	良好：大規模ブロックのシーケンシャルワークロードに最適
パフォーマンス（ドライブリビルドモード）	優れている：通常はRAID 6よりも優れている	デグレード：パフォーマンスが最大40%低下
複数のドライブ障害	データ保護機能に優れる：リビルドを優先し、高速に処理	データ保護機能が劣る：リビルドが遅く、データ損失のリスクが大きい
ドライブの追加	高速：オンザフライでプールに追加	低速：Dynamic Capacity Expansion処理が必要
シンボリュームのサポート	はい	いいえ
ソリッドステートディスク（SSD）のサポート	はい	はい
管理の簡易化	はい：構成するホットスペアやRAID設定はありません	いいえ：ホットスペアを割り当て、RAIDを構成する必要がある
パフォーマンスの調整	いいえ	はい

プールとボリュームグループの機能比較

プールとボリュームグループの機能と目的は同じです。どちらのオブジェクトも、ストレージアレイ内に論理的にグループ化された一連のドライブであり、ホストがアクセスできるボリュームの作成に使用されます。

次の表は、プールとボリュームグループのどちらがストレージのニーズに適しているかを判断する際に役立ちます。

機能	プール	ボリュームグループ
異なるRAIDレベルのサポート	×（System ManagerではRAID 6のみ）	はい。RAID 0、1、10、5、6を使用可能
シンボリュームのサポート	はい	いいえ
Full Disk Encryption（FDE）のサポート	はい	はい
Data Assurance（DA）のサポート	はい	はい
シェルフ損失の保護のサポート	はい	はい
ドロワー損失の保護のサポート	はい	はい
ドライブ速度混在のサポート	同じにすることをお勧めしますが、必須ではありません。一番低速のドライブにすべてのドライブの速度が合わせられます。	同じにすることをお勧めしますが、必須ではありません。一番低速のドライブにすべてのドライブの速度が合わせられます。
ドライブ容量混在のサポート	同じにすることをお勧めしますが、必須ではありません。一番容量の少ないドライブにすべてのドライブの容量が合わせられます。	同じにすることをお勧めしますが、必須ではありません。一番容量の少ないドライブにすべてのドライブの容量が合わせられます。
最小ドライブ数	11	RAIDレベルによって異なります。RAID 0には1が必要です。RAID 1または10には2本（偶数）必要。RAID 5の最小構成は3です。RAID 6の最小構成は5です。
最大ドライブ数	ストレージアレイの上限まで	RAID 1および10：ストレージアレイの上限までRAID 5、6～30ドライブ
ボリューム作成時にドライブを個別に選択可能	いいえ	はい
ボリューム作成時にセグメントサイズを指定可能	はい。128Kをサポート。	はい
ボリューム作成時にI/O特性を指定可能	いいえ	はい。ファイルシステム、データベース、マルチメディア、カスタムをサポート。

機能	プール	ボリュームグループ
ドライブ障害からの保護	プール内の各ドライブの予約済み容量を使用し、再構築にかかる時間を短縮。	ホットスペアドライブを使用します。再構築はドライブのIOPSによって制限されます。
容量制限に達したときの警告	はい。使用済み容量が最大容量の割合に達したときにアラートを設定できます。	いいえ
別のストレージアレイへの移行のサポート	×（まずボリューム グループに移行する必要がある）	はい
動的セグメントサイズ（DSS）	いいえ	はい
RAIDレベルを変更可能	いいえ	はい
ボリュームの拡張（容量の拡張）	はい	はい
容量の拡張（容量の追加）	はい	はい
容量の削減	はい	いいえ

プールまたはボリュームグループでは、ドライブタイプ（HDD、SSD）の混在はサポートされていません。

プールの自動作成と手動作成

プールを自動または手動で作成して物理ストレージをグループ化し、必要に応じて動的に割り当てることができます。プールを作成すると、物理ドライブを追加できます。

自動作成

プールの自動作成は、System Managerがストレージアレイ内に未割り当て容量を検出すると開始されます。未割り当て容量が検出されると、プールを作成するか、未割り当て容量を既存のプールに追加するか、またはその両方を行うようにSystem Managerから自動的に要求されます。

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、新しいプールを作成するのに十分な数のドライブがあります。
- 少なくとも1つのプールを含むストレージアレイに新しいドライブが追加される。

プール内の各ドライブは、ドライブタイプ（HDDまたはSSD）が同じで、容量がほぼ同じである必要があります。System Managerでは、次のタスクを実行するように求められます。

- 同じタイプの十分な数のドライブがある場合は、単一のプールを作成します。
- 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、複数のプールを作成します。

- ストレージアレイでプールが定義済みの場合は既存のプールにドライブを追加し、同じドライブタイプの新しいドライブをプールに追加します。
- 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ます。新しいドライブタイプが異なる場合は、他のドライブタイプを使用して別のプールを作成します。

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ます。
- 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ない。

ストレージアレイ上の複数のアプリケーションが同じドライブリソースを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。この場合は、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代わりに、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し、競合を軽減できます。

ストレージを設定する

プールの自動作成

プールの作成は、System Managerがストレージアレイ内に未割り当てのドライブを検出すると自動的に開始されます。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。

開始する前に

[プールの自動構成]ダイアログボックスは、次のいずれかの条件に該当する場合に起動できます。

- 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少なくとも1本検出されました。
- 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本以上検出されました（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）。

タスクの内容

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、System Managerで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。
- プールがすで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System Managerで自動的に表示されます。新しいドライブが既存のプールに追加されると、System Managerによって新しい容量（追加した新しいドライブを含む）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構成する場合は、各コントローラが最初の12スロットの同数のドライブと最後の12スロットの同数のドライブにアクセスできることを確認してください。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。

プールの自動構成（Pool Auto-Configuration）ダイアログボックスは、次のいずれかの方法で起動できます。

- 未割り当て容量が検出されると、通知領域のホームページにプールの自動構成に関する推奨事項が表示されます。View Pool Auto-Configuration *（プールの自動構成の表示）をクリックして、ダイアログボックスを起動します。
- プールとボリュームグループページからプールの自動構成ダイアログボックスを起動することもできます。これには次のタスクを実行します。

手順

1. 選択メニュー：Storage（Pool & Volume Groups）
2. 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。

   System Managerは次のタスクを実行します。

   - ドライブタイプ（HDDまたはSSD）が同じで容量がほぼ同じ十分な数のドライブがある場合は、単一のプールを作成します。
   - 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。
   - ストレージアレイでプールが定義済みの場合は、既存のプールにドライブを追加し、同じドライブタイプの新しいドライブをプールに追加します。
   - 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ます。新しいドライブタイプが異なる場合は、他のドライブタイプを使用して別のプールを作成します。
3. 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。
4. 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、* Details *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ストレージアレイの場合は、リソースプロビジョニングとボリュームのブロックサイズの設定も表示されます。

5. [* 同意する *] をクリックします。

プールの手動作成

プールの自動構成機能でニーズに合ったプールが提供されない場合は、プールを（一連の候補から）手動で作成できます。

プールは必要な論理ストレージ容量を提供します。この容量から個々のボリュームを作成し、アプリケーションをホストすることができます。

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11本以上必要です。
- 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、同じドライブシェルフのドライブが3本以下である必要があります。
- 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構成する場合は、各コントローラが最初の12スロットの同数のドライブと最後の12スロットの同数のドライブにアクセスできることを確認してください。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。現在のところ、System Managerでは、ボリュームグループを作成するときに[アドバンスト]機能でドライブを選択できます。プールを作成する場合は、ストレージアレイ内のすべてのドライブを使用することを推奨します。

手順

1. 選択メニュー：Storage（Pool & Volume Groups）
2. メニュー：[Create Pool（プールの作成）]をクリックします。

   [Create Pool]ダイアログボックスが表示されます。

3. プールの名前を入力します。
4. *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。

5. 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。

特性	使用
空き容量	プール候補の空き容量（GiB）が表示されます。アプリケーションのストレージニーズに対応する容量を持つプール候補を選択します。 予約済み（スペア）容量もプール全体に分散され、空き容量には含まれません。
合計ドライブ数	プール候補で使用可能なドライブの数が表示されます。 System Managerは、できるだけ多くのドライブを予約済み容量として自動的に確保します（System Managerではプール内の6本につき1本のドライブを予約済み容量として確保します）。 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み可能なブロックサイズ（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。

特性	使用
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レベルドライブと140-3レベルドライブが混在していることを示します。これらのレベルを混合して使用する場合は、プールはより低い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を提供します。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は、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。
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は、すべてのドライブがDA対応の場合は有効になります。DAは、ボリュームの作成後にメニューを選択して無効にすることができます。Storage [Volumes]、[View/Edit Settings]、[Advanced]、[Permanently disable Data Assurance（データ保護を完全に無効にする）]。DAが無効になっているボリュームでは、再度有効にすることはできません。
リソースプロビジョニング対応（EF300およびEF600のみ）	この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。この機能を使用すると、ボリュームをバックグラウンドの初期化プロセスなしですぐに使用できるようになります。
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。

特性	使用
ドロワー損失の保護	ドロワー損失の保護を使用できる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）	に、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を示します。 • 512n — 512バイトネイティブ。 • 512e — 512バイトエミュレート。 • 4k — 4,096バイト

ボリュームグループの作成

ボリュームグループを使用して、ホストにアクセス可能な1つ以上のボリュームを作成します。ボリュームグループは、RAIDレベルや容量などの特性が共有されたボリュームのコンテナです。

大容量のドライブとコントローラ間でボリュームを分散できるので、ストレージ容量を活用してデータを保護するには、ボリュームグループごとに複数のボリュームを作成すると効果的です。

開始する前に

ボリュームグループを作成する前に、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数には制限があります。これらの制限はRAIDレベル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、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（RAID 1ではシェルフ/ドロワーが2台以上）。
- EF600またはEF300ストレージアレイを使用していて、ボリュームグループを手動で作成する場合は、各コントローラが最初の12スロットの同数のドライブと最後の12スロットの同数のドライブにアクセスできることを確認してください。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。現在のところ、System Managerでは、ボリュームグループを作成するときに[アドバンスト]機能でドライブを選択できます。
- 選択したRAIDレベルがボリュームグループの容量にどのように影響するかを確認します。
  - RAID 1を選択した場合は、一度に2本のドライブを追加してミラーペアを選択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を選択した場合は、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を選択した場合は、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。

手順

1. 選択メニュー：Storage（Pool & Volume Groups）
2. 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]ダイアログボックスが表示されます。

3. ボリュームグループの名前を入力します。
4. 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のみが表示されます。

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。

   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のみが表示されます。

6. *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特定の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。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ストレージアレイに含まれている場合は、1つのドライブタイプに対して未設定の容量のみを選択して新しいボリュームグループを作成できます。

   手動方式を使用するのは、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エキスパートだけです。

7. 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。

自動方式のドライブ特性

特性	使用
空き容量	使用可能な容量（GiB）を示します。アプリケーションのストレージニーズに対応する容量を備えたボリュームグループ候補を選択してください。
合計ドライブ数	このボリュームグループで使用可能なドライブの数が表示されます。必要なドライブ数のボリュームグループ候補を選択します。
ドライブブロックサイズ（EF300およびEF600のみ）	グループ内のドライブが書き込み可能なブロックサイズ（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	このボリュームグループ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。 • ボリュームグループ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のみのボリュームグループを作成する場合は、SecureCapable列で「* Yes-fde」が検索されています。FIPSのみのボリュームグループを作成する場合は、「はい- FIPS *」または「はい- FIPS（混在）」を探します。「Mixed」 は 、140-2レベルドライブと140-3レベルドライブが混在していることを示します。これらのレベルが混在している場合は、ボリュームグループが下位のセキュリティレベル（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ボリュームグループや、セキュリティレベルが異なるドライブが混在したボリュームグループを作成することもできます。ボリュームグループ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、ボリュームグループ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を提供します。ボリュームグループがセキュリティ対応で、セキュリティキーを設定している場合、チェックボックスを選択してドライブ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、ボリュームグループ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	このグループで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に対応したボリュームグループを選択します。（DA対応ドライブの場合、プール内に作成されたボリュームではDAが自動的に有効になります）。 ボリュームグループには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）	このグループ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。この機能を使用すると、ボリュームをバックグラウンドの初期化プロセスなしですぐに使用できるようになります。
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、シェルフとの通信が完全に失われた場合でも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。
ドロワー損失の保護	ドロワー損失の保護を使用できる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。
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）	グループ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バイトエミュレート。 • 4k — 4,096バイト

手動方式のドライブの特性

特性	使用
メディアタイプ	メディアタイプを示します。次のメディアタイプがサポートされています。 • ハードドライブ • ソリッドステートディスク（SSD） ボリュームグループ内のすべてのドライブのメディアタイプ（すべてのSSDまたはすべてのハードドライブ）が同じである必要があります。ボリュームグループでメディアタイプやインターフェイスタイプを混在させることはできません。
ドライブブロックサイズ（EF300およびEF600のみ）	グループ内のドライブが書き込み可能なブロックサイズ（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。
ドライブ容量	ドライブの容量を示します。 • 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可能なかぎり選択してください。 • 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、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、ボリュームグループに現在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。
トレイ	ドライブのトレイの場所を示します。
スロット	ドライブのスロットの場所を示します。
速度（rpm）	ドライブの速度を示します。
論理セクターサイズ	セクターサイズとフォーマットを示します。

特性	使用
セキュリティ対応	このボリュームグループ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。 • ボリュームグループ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のみのボリュームグループを作成する場合は、SecureCapable列で「* Yes-fde」が検索されています。FIPSのみのボリュームグループを作成する場合は、「はい- FIPS *」または「はい- FIPS（混在）」を探します。「Mixed」 は 、140-2レベルドライブと140-3レベルドライブが混在していることを示します。これらのレベルが混在している場合は、ボリュームグループが下位のセキュリティレベル（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ボリュームグループや、セキュリティレベルが異なるドライブが混在したボリュームグループを作成することもできます。ボリュームグループ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、ボリュームグループをセキュリティ対応にすることはできません。
DA 対応	このグループでData Assurance（DA）を使用できるかどうかを示します。Data Assurance（DA）は、コントローラ経由でドライブと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します。 DAを使用する場合は、DAに対応したボリュームグループを選択します。（DA対応ドライブの場合、プール内に作成されたボリュームではDAが自動的に有効になります）。 ボリュームグループには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。
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）	グループ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バイトエミュレート。 • 4k — 4,096バイト
リソースプロビジョニング対応（EF300およびEF600のみ）	このグループ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。この機能を使用すると、ボリュームをバックグラウンドの初期化プロセスなしですぐに使用できるようになります。

ドライブを追加して、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できます。

拡張すると、プールまたはボリュームグループに追加の空き容量が含まれます。この空き容量を使用して、追加のボリュームを作成できます。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。

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Iである必要があります。
- 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。
- プールに含めることができるボリュームの最大数は、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（E2800シリーズ）
- 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ドライブの場合は、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のみを追加してください。

  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。

タスクの内容

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、同じ手順を繰り返します。（プールにはストレージシステム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。拡張処理のあと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場合は、DAに対応したドライブは使用しないでください。プールまたはボリュームグループでDA対応ドライブの機能を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. 選択メニュー：Storage（Pool & Volume Groups）
2. 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。

   [容量の追加]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。

3. 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	製品説明
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。 • 可能なかぎり、プールまたはボリュームグループ内の現在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。 • 容量の大きい未割り当て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内のドライブの現在の容量に合わせて、追加する未割り当て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。 • プールまたはボリュームグループをドライブセキュリティ機能で保護するには、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。 • セキュリティ対応ドライブのみのプールまたはボリュームグループでは、暗号化機能を使用していなくても、スペアまたは拡張用にセキュリティ対応でないドライブを使用す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ドライブにはレベル140-2または140-3を指定でき、レベル140-3が上位の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混在させる場合、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	製品説明
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しく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。 • Data Assurance（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。プールまたはボリュームグループでDA対応ドライブの機能を利用できない（ドライブ属性が一致しない）ためです。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。このオプションを使用すると、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。

4. [追加]*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は、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

   *現在、シェルフ損失の保護またはドロワー損失の保護が有効なプールにドライブを追加する場合、確認のダイアログボックスは表示されません。

1. 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すると、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て追加のドライブが追加されます。

ストレージの管理

ボリュームの冗長性チェック

テクニカルサポートから指示があった場合、または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て、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。

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ボリューム変更処理がないことを確認します。
- RAID 0にはデータの冗長性がないため、RAID 0以外のどのRAIDレベルでも冗長性をチェックできます。

> 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のみ、テクニカルサポートの指示に従って実行してください。

タスクの内容

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ボリュームのデータブロックをスキャンし、各ブロックの冗長性情報をチェックします。（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）。
- は、RAID 1ミラードライブ上のデータブロックを比較します。
- 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、冗長性エラーを返します。

> 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、エラーが発生することがあります。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. 選択メニュー：Storage（Pool & Volume Groups）
2. 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。
3. 確認するボリュームを選択し、と入力して `check`この処理を実行します。
4. [*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テーブル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と、次の処理が実行されます。

   - 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は、*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、チェックが停止し、エラーが報告されます。

冗長性チェックのステータスの詳細

ステータス	製品説明
保留中	これは最初にスキャンされるボリュームであり、冗長性チェックを開始するために[Start]をクリックしていません。 または 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を実行中です。
カクニン	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	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、読み取りできません。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。パリティエラーは重大な問題であり、データが永久に失われる可能性があります。

5. 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の削除

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追加で作成し、アプリケーションのストレージニーズに合わせて再設定することができます。

開始する前に

- プールまたはボリュームグループ内の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内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してください。

- 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必要があります。

手順

1. 選択メニュー：Storage（Pool & Volume Groups）
2. 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。

3. [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

System Manager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ドライブをすべて削除します。
- 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の統合

[空き容量の統合]オプションを使用して、選択したボリュームグループの既存の空きエクステントを統合します。この操作を実行すると、ボリュームグループ内の最大空き容量から追加ボリュームを作成できます。

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l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ようにする必要があります。

タスクの内容

この処理は開始後にキャンセルすることはできません。データへのアクセスは、統合処理中も維持されます。

[空き容量の統合]ダイアログボックスは、次のいずれかの方法で起動できます。

- ボリュームグループで少なくとも1つの空き容量領域が検出されると、[ホーム]ページの[通知]領域に「空き容量の統合」という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、[プールとボリュームグループ]ページから[空き容量の統合]ダイアログボックスを開くこともできます。

空き容量領域について

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に制限されます。たとえば、ボリュームグループの合計空き容量が15GiBで、最も大きい空き容量領域が10GiBの場合、作成できるボリュームの最大サイズは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、削除するにつれて徐 々 に断片化されます。最終的には、使用可能な容量は単一の連続するブロックに配置されるのではなく、小さなフラグメントに分割されてボリュームグループ全体に分散されます。これにより、ホストは新しいファイルを空きクラスタの利用可能な範囲に収まるように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。統合プロセスは、将来的に新しいファイルが断片化されるのを防ぐのにも役立ちます。

手順

1. 選択メニュー：Storage（Pool & Volume Groups）
2. 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。

   [空き容量の統合]ダイアログボックスが表示されます。

3. と入力して、 `consolidate`この処理を実行します。
4. [*統合（Consolidate）]をクリックし

   System Managerは、以降のストレージ設定タスクで使用できるように、ボリュームグループの空き容量領域の統合（デフラグ）を開始します。

終了後

[MENU]：[Home（ホーム）][View Operations in Progress]（進行中の操作の表示）を選択して、[Consolidate Free Capacity（空き容量の統合）]操作の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。

ボリュームグループのエクスポート/インポート

ボリュームグループの移行では、ボリュームグループをエクスポートして、ボリュームグループを別のストレージアレイにインポートすることができます。

エクスポート/インポート機能は、SANtricity System Managerユーザインターフェイスではサポートされていません。ボリュームグループを別のストレージアレイにエクスポート/インポートするには、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。

プール、ボリュームグループ、または**SSD**キャッシュでのロケーターライトの点灯

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. 選択メニュー：Storage（Pool & Volume Groups）
2. 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していることを示すダイアログボックスが表示されます。

3. 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。

プールまたは**SSD**キャッシュからの容量の削除

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。削除したドライブは未割り当てになり、その容量はストレージアレイの合計空き容量に含まれます。

タスクの内容

容量を削除する際は、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、同じ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

- 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応じて、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への影響

- 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. 選択メニュー：Storage（Pool & Volume Groups）
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]

   [容量の削除]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。

   リストからドライブを選択または選択解除すると、[**Total capacity selected**]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。

   プールまたはSSDキャッシュで新たに削減された容量が、[プールとボリュームグループ]ビューに反映されます。

プールとグループの設定を変更します。

プールの構成設定の変更

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

タスクの内容

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。

System Manager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。System Managerはプールを自動的にRAID 6として構成します。

手順

1. 選択メニュー：Storage（Pool & Volume Groups）
2. 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。

   [プール設定]ダイアログボックスが表示されます。

3. [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	製品説明
名前	ユーザが指定したプールの名前を変更できます。プールの名前を指定する必要があります。
容量のアラート	プールの空き容量が指定したしきい値に達したとき、または超えたときにアラート通知を送信できます。プールに格納されているデータが指定したしきい値を超えるとSystem Managerからメッセージが送信されるため、前もって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できます。 アラートはダッシュボードの[Notifications]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。スピナコントロールを使用して、しきい値の割合を調整します。この通知を無効にするには、この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。スピナコントロールを使用して、しきい値の割合を調整します。この通知を無効にするには、この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に対するプール内の変更処理の優先度レベルを指定できます。プール内の変更処理の優先度を高くすると処理は短時間で完了しますが、ホストのI/Oパフォーマンスが低下することがあります。優先度を低くすると処理にかかる時間は長くなりますが、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I/O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	製品説明
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。プールでは、データの再構築プロセスで、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の代わりに予約済み容量が使用されます。 スピンボックスを使用してドライブ数を調整します。ドライブ数に基づいて、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。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削って確保され、この容量をボリュームの作成に使用することはできません。

4. [保存（ Save ）] をクリックします。

ボリュームグループの設定の変更

ボリュームグループの名前やRAIDレベルなどの設定を編集できます。

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のパフォーマンスニーズに合わせて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必要があります。

- ボリュームグループのステータスが最適I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. 選択メニュー：Storage（Pool & Volume Groups）
2. 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]ダイアログボックスが表示されます。

3. 「* 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	製品説明
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。単一ドライブ障害が発生した場合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を必要とする、データベースなどの大量のトランザクション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（CLI）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寿命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削って確保され、この容量をボリュームの作成に使用することはできません。

4. [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、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レベルがSystem Managerによって変更されます。処理中はパフォーマンスに多少影響することがあります。

既存のボリュームグループおよびプールでリソースプロビジョニングを有効または無効にする

DULBE対応ドライブについては、プールまたはボリュームグループ内の既存のボリュームでリソースプロビジョニングを有効または無効にすることができます。

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。この機能を使用すると、ボリュームをバックグラウンドの初期化プロセスなしですぐに使用できるようになります。ボリュームに割り当てられているドライブブロックはすべて割り当て解除（マッピング解除）されるため、SSDの摩耗度が向上し、最大書き込みパフォーマンスが向上します。

デフォルトでは、ドライブがDULBEをサポートするシステムでリソースプロビジョニングが有効になっています。以前にリソースプロビジョニングを無効にしていないかぎり、リソースプロビジョニングを有効にする必要はありません。

開始する前に

- EF300またはEF600ストレージアレイが必要です。
- NVMeのDeallocated or Unwritten Logical Block Error（DULBE）エラーリカバリ機能がすべてのドライブでサポートされているSSDボリュームグループまたはプールが必要です。そうしないと、リソースプロビジョニングオプションは使用できません。

タスクの内容

既存のボリュームグループおよびプールに対してリソースプロビジョニングを有効にすると、選択したボリュームグループまたはプール内のすべてのボリュームが変更されてブロックの割り当てが解除されます。このプロセスには、UNMAPの粒度で一貫した割り当てを確保するためのバックグラウンド処理が含まれる場合があります。この処理では、スペースのマッピングは解除されません。バックグラウンド処理が完了したら、オペレーティングシステムは未使用のブロックのマッピングを解除して空きスペースを確保する必要があります。

既存のボリュームグループまたはプールのリソースプロビジョニングを無効にすると、バックグラウンド処理によってすべてのボリューム内のすべての論理ブロックが書き換えられます。既存のデータはそのまま維持されます。書き込みでは、ボリュームグループまたはプールに関連付けられたドライブのブロックがマッピングまたはプロビジョニングされます。

> 新しいボリュームグループおよびプールについては、メニューからリソースのプロビジョニングを有効または無効にできます。設定[システム]、[追加設定]、[リソースプロビジョニングボリュームの有効化/無効化]の順に選択します。

手順

1. 選択メニュー：Storage（Pool & Volume Groups）
2. 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。

3. [一般的でないタスク]を選択し、[リソースプロビジョニングを有効にする]または[リソースプロビジョニングを無効にする]のいずれかを選択します。
4. ダイアログボックスで、処理を確認します。

*DULBEを再度有効にした場合—バックグラウンド処理が完了した後'ホストを再起動してDULBE設定の変更を検出し'すべてのファイルシステムを再マウントする必要がある場合があります

新しいボリュームグループまたはプールのリソースプロビジョニングを有効または無効にする

リソースプロビジョニングのデフォルト機能を無効にしていた場合は、作成する新しいSSDボリュームグループまたはプールに対して再度有効にすることができます。設定を再度無効にすることもできます。

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。この機能を使用すると、ボリュームをバックグラウンドの初期化プロセスなしですぐに使用できるようになります。ボリュームに割り当てられているドライブブロックはすべて割り当て解除（マッピング解除）されるため、SSDの摩耗度が向上し、最大書き込みパフォーマンスが向上します。

デフォルトでは、ドライブがDULBEをサポートするシステムでリソースプロビジョニングが有効になっています。

開始する前に

- EF300またはEF600ストレージアレイが必要です。
- NVMeのDeallocated or Unwritten Logical Block Error（DULBE）エラーリカバリ機能がすべてのドライブでサポートされているSSDボリュームグループまたはプールが必要です。

タスクの内容

新しいボリュームグループまたはプールのリソース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が影響を受けます。リソースプロビジョニングが有効になっている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。

手順

1. メニューを選択します。[設定][システム]。
2. 下にスクロールして「* Additional Settings 」(追加設定)を選択し、「*リソースプロビジョニングボリュームの有効化/無効化」をクリックします。

   設定の説明には、リソースプロビジョニングが現在有効になっているか無効になっているかが示されます。

3. ダイアログボックスで、処理を確認します。

結果

リソースプロビジョニングの有効化と無効化は、作成した新しいSSDプールまたはボリュームグループにのみ影響します。既存のプールまたはボリュームグループは変更されません。

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

プールまたはボリュームグループに対してドライブセキュリティを有効にすると、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/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使用できます。

開始する前に

- ドライブセキュリティ機能が有効になっている必要があります。
- 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l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ドライブである必要があります。

タスクの内容

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両方のドライブを含めることができますが、暗号化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。

セキュリティを有効にしたあとに削除するには、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. 選択メニュー：Storage（Pool & Volume Groups）
2. 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。

   [Confirm Enable Security]ダイアログボックスが表示されます。

3. 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。

SSDキャッシュの管理

SSDキャッシュの仕組み

SSDキャッシュ機能は、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でシステムのパフォーマンスを動的に向上させるコントローラベースの解決策 です。SSDキャッシュは、ホスト読み取りにのみ使用されます。

SSDキャッシュとプライマリキャッシュ

SSDキャッシュはセカンダリキャッシュであり、コントローラの動的ランダムアクセスメモリ（DRAM）にあるプライマリキャッシュと組み合わせて使用されます。

SSDキャッシュはプライマリキャッシュとは動作が異なります。

- プライマリキャッシュの場合、I/O処理ごとにキャッシュを介してデータをステージングする必要があります。

  プライマリキャッシュでは、ホスト読み取り後にデータがDRAMに格納されます。

- SSDキャッシュは、データをキャッシュに配置してシステムの全体的なパフォーマンスを向上できる場合にのみ使用されます。

  SSDキャッシュでは、データはボリュームからコピーされて2つの内部RAIDボリューム（コントローラごとに1つ）に格納されます。RAIDボリュームはSSDキャッシュの作成時に自動的に作成されます。

内部RAIDボリュームは、内部的なキャッシュ処理に使用されます。これらのボリュームにはアクセスできず、ユーザインターフェイスにも表示されません。ただし、ストレージアレイで許可されるボリュームの総数には、これら2つのボリュームが含まれます。

SSDキャッシュの使用方法

インテリジェントキャッシングは、低レイテンシのドライブにデータを配置するため、そのデータに対する以降の要求への応答時間を大幅に短縮できます。キャッシュ内のデータをプログラムが要求すると(キャッシュヒットと呼ばれます)'低遅延ドライブはそのトランザクションを処理できますそれ以外の場合は「キャッシュミス」が発生し、元の低速ドライブからデータにアクセスする必要があります。キャッシュヒット数が増えると、全体的なパフォーマンスが向上します。

ホストプログラムがストレージアレイのドライブにアクセスすると、データはSSDキャッシュに格納されます。ホストプログラムが再度同じデータにアクセスすると、そのデータはハードドライブではなくSSDキャッシュから読み取られます。よくアクセスされるデータはSSDキャッシュに格納されます。ハードドライブは、SSDキャッシュからデータを読み取ることができない場合にのみアクセスされます。

SSDキャッシュは、データをキャッシュに配置して全体的なシステムパフォーマンスを向上できる場合にのみ使用されます。

CPUが読み取りデータを処理する必要がある場合は、次の手順に従います。

1. DRAMキャッシュをチェックします。
2. DRAMキャッシュで検出されない場合は、SSDキャッシュをチェックします。
3. SSDキャッシュで見つからない場合は、ハードドライブから取得します。データをキャッシュする価値があると判断された場合は、SSDキャッシュにコピーします。

パフォーマンスの向上

最もアクセス頻度の高いデータ（ホットスポット）をSSDキャッシュにコピーすることで、ハードディスクの処理効率が向上し、レイテンシが低減され、読み取りと書き込みの速度が向上します。ハイパフォーマンスのSSDを使用してHDDボリュームのデータをキャッシュすると、I/Oパフォーマンスと応答時間が向上します。

SSDキャッシュとの間のデータの移動には、単純なボリュームI/Oのメカニズムが使用されます。データがキャッシュされてSSDに格納されると、そのデータの以降の読み取りはSSDキャッシュで実行されるため、HDDボリュームにアクセスする必要はありません。

SSDキャッシュとドライブセキュリティ機能

ドライブセキュリティを使用している（セキュリティ有効）ボリュームでSSDキャッシュを使用する場合は、

そのボリュームとSSDキャッシュのドライブセキュリティ機能が同じである必要があります。同じでない場合、ボリュームはセキュリティ有効になりません。

SSDキャッシュの実装

SSDキャッシュを実装するには、次の手順を実行します。

1. SSDキャッシュを作成します。
2. 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。

> 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転送の対象になりません。

SSDキャッシュの制限事項

ストレージアレイでSSDキャッシュを使用する場合の制限事項について説明します。

制限事項

- 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転送の対象になりません。
- 現時点では、1つのストレージアレイでサポートされるSSDキャッシュは1つだけです。
- ストレージアレイで使用可能なSSDキャッシュの最大容量は10TBです。
- SSDキャッシュはSnapshotイメージではサポートされません。
- SSDキャッシュが有効または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た場合、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。
- 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。

ドライブセキュリティに関する制限事項

- SSDキャッシュでセキュリティを有効にすることができるのは、SSDキャッシュの作成時のみです。ボリューム上のようにセキュリティをあとから有効にすることはできません。
- セキュリティ対応のドライブとセキュリティ対応でないドライブをSSDキャッシュで混在させる場合、それらのドライブに対してドライブセキュリティを有効にすることはできません。
- セキュリティ有効ボリュームには、セキュリティが有効なSSDキャッシュが必要です。

SSDキャッシュの作成

システムパフォーマンスを動的に高速化するには、SSDキャッシュ機能を使用して、アクセス頻度が最も高いデータ（「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）にキャッシュします。SSDキャッシュは、ホスト読み取りにのみ使用されます。

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。

タスクの内容

新しいSSDキャッシュを作成するときに、1つまたは複数のドライブを使用できます。読み取りキャッシュはストレージアレイにあるため、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。

新しいSSDキャッシュを作成するときは、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。
- 1つのストレージアレイでサポートされるSSDキャッシュは1つだけです。
- SSDキャッシュが有効になっているボリュームが1つだけの場合は、SSDキャッシュ全体がそのボリュームを所有するコントローラに割り当てられます。
- ストレージアレイで使用可能な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決まります。
- SSDキャッシュはSnapshotイメージではサポートされません。
- SSDキャッシュが有効または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た場合、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転送の対象になりません。
- 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. 選択メニュー：Storage（Pool & Volume Groups）
2. 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。

3. SSDキャッシュの名前を入力します。
4. 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。

特性	使用
容量	使用可能な容量（GiB）を示します。アプリケーションのストレージニーズに応じ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が表示されます。必要なドライブ数のSSD候補を選択します。

特性	使用
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を提供します。セキュリティ有効SSDキャッシュを作成する場合は、セキュリティの有効化チェックボックスをオンにします。 いったん有効にすると、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。

5. 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。

   ドライブセキュリティとDAの機能が同じボリュームであれば互換性があります。

6. [作成（ Create ）] をクリックします。

SSDキャッシュ設定の変更

SSDキャッシュの名前を編集して、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確認できます。

手順

1. 選択メニュー：Storage（Pool & Volume Groups）
2. 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キャッシュ設定]ダイアログボックスが表示されます。

3. 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	製品説明
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須です。
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 • デグレード • 失敗（重大なMELイベントが生成されます） • 中断
容量	SSDキャッシュの現在の容量と許容される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から4GiB • 4 GiB超
セキュリティと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、データへの不正アクセスを防止できる自己暗号化ドライブです。 • * 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。

4. [保存（ Save ）] をクリックします。

SSDキャッシュの統計の表示

SSDキャッシュの統計（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、キャッシュ利用率など）を表示できます。

詳細統計のサブセットである一般統計は、[SSDキャッシュの統計を表示]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統計をファイルにエクスポートした場合にのみ表示できます `.csv`。

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. 選択メニュー：Storage（Pool & Volume Groups）
2. 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 [SSD Cache statistics（SSDキャッシュ統計の表示）]

   [SSDキャッシュの統計を表示]ダイアログボックスが表示され、選択したSSDキャッシュの一般統計が表示されます。

フィールドの詳細

設定	製品説明
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総数。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を表示します。
キャッシュヒット率	キャッシュヒットの割合が表示されます。この値は、キャッシュヒット数/（読み取り+書き込み）から算出されます。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%以上である必要があります。
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可能なSSDキャッシュストレージの割合で表され、割り当て済みバイト数/使用可能バイト数から算出されます。
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。割り当てられているSSDキャッシュストレージの割合として表されます。この量は、SSDキャッシュの利用率または密度を表します。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。
すべてエクスポート	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。

3. 「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。

リザーブ容量の管理

リザーブ容量の仕組み

リザーブ容量は、Snapshotや非同期ミラーリング処理などのコピーサービス処理がボリュームに提供されている場合に自動的に作成されます。

リザーブ容量の目的は、何らかの不具合が発生した場合に備えて、これらのボリューム上のデータ変更を保存することです。ボリュームと同様に、リザーブ容量はプールまたはボリュームグループから作成されます。

リザーブ容量を使用するコピーサービスオブジェクト

リザーブ容量は、次のコピーサービスオブジェクトで使用される基盤となるストレージメカニズムです。

- Snapshotクルウフ
- 読み取り/書き込みSnapshotボリューム
- 整合性グループメンバーボリューム
- ミラアヘアホリユウム

これらのコピーサービスオブジェクトを作成または拡張するときは、プールまたはボリュームグループから新しいリザーブ容量を作成する必要があります。リザーブ容量は、通常、Snapshot処理の場合はベースボリュームの40%、非同期ミラーリング処理の場合はベースボリュームの20%です。ただし、リザーブ容量は元のデータに対する変更の回数によって異なります。

シンボリュームとリザーブ容量

シンボリュームの場合、最大レポート容量の256TiBに達していると容量を拡張できません。シンボリュームのリザーブ容量が最大レポート容量よりも大きいサイズに設定されていることを確認してください。（シンボリュームは常にシンプロビジョニングされます。つまり、ボリュームにデータが書き込まれるときに容量が割り当てられます）。

プール内のシンボリュームを使用してリザーブ容量を作成する場合は、リザーブ容量に関する次の操作と結果を確認してください。

- シンボリュームのリザーブ容量に障害が発生した場合、シンボリューム自体は自動的に失敗状態に移行しません。ただし、シンボリュームに対するI/O処理はすべてリザーブ容量ボリュームにアクセスする必要があるため、I/O処理では常にCheck Conditionが要求元ホストに返されます。リザーブ容量ボリュームの根本的な問題を解決できる場合は、リザーブ容量ボリュームが最適な状態に戻り、シンボリュームが再び機能するようになります。
- 既存のシンボリュームを使用して非同期ミラーペアを作成する場合、そのシンボリュームは新しいリザーブ容量ボリュームで再初期化されます。初期同期プロセス中は、プライマリ側のプロビジョニングされたブロックのみが転送されます。

容量のアラート

コピーサービスオブジェクトには、容量の警告とアラートのしきい値を設定できるほか、リザーブ容量がフルになったときの応答も設定できます。

コピーサービスオブジェクトボリュームのリザーブ容量が上限に近づくと、ユーザにアラートが発行されます。デフォルトでは、リザーブ容量ボリュームの使用率が75%に達したときにこのアラートが生成されますが、必要に応じて増減できます。このアラートを受け取った場合は、その時点でリザーブ容量ボリュームの容量を増やすことができます。この点で、各コピーサービスオブジェクトは個別に設定できます。

孤立したリザーブ容量ボリューム

孤立したリザーブ容量ボリュームは、関連付けられているコピーサービスオブジェクトが削除されたため、コピーサービス処理のデータを格納しなくなったボリュームです。コピーサービスオブジェクトが削除されたときにリザーブ容量ボリュームも削除されている必要があります。ただし、リザーブ容量ボリュームを削除できませんでした。

孤立したリザーブ容量ボリュームは、どのホストからもアクセスできないため、再生候補となります。孤立したリザーブ容量ボリュームを手動で削除して、その容量を他の処理で使用できるようにします。

System Managerは、[ホーム]ページの[通知]領域に「未使用容量の再生」というメッセージを表示して、孤立したリザーブ容量ボリュームについて警告します。未使用容量を再利用する*をクリックすると、未使用容量

の再生ダイアログボックスが表示され、孤立したリザーブ容量ボリュームを削除できます。

リザーブ容量の特性

- 十分な空き容量を保持するために、ボリュームの作成時にはリザーブ容量に割り当てられる容量を考慮する必要があります。
- リザーブ容量はベースボリュームよりも小さくすることができます（最小サイズは8MiB）。
- 一部のスペースはメタデータによって消費されますが、ごくわずか（192KiB）なので、リザーブ容量ボリュームのサイズを特定する際に考慮する必要はありません。
- リザーブ容量は、ホストから直接読み取りまたは書き込みすることはできません。
- リザーブ容量は、読み取り/書き込みSnapshotボリューム、Snapshotグループ、整合性グループメンバーボリューム、ミラーペアボリュームごとに確保されます。

リザーブ容量の拡張

リザーブ容量を増やすことができます。リザーブ容量は、ストレージオブジェクトに対する任意のコピーサービス処理に使用される物理的に割り当てられた容量です。

Snapshot処理の場合は、通常はベースボリュームの40%、非同期ミラーリング処理の場合は通常はベースボリュームの20%です。一般に、ストレージオブジェクトのリザーブ容量がフルに近づいているという警告が表示されたときにリザーブ容量を拡張します。

開始する前に

- プールまたはボリュームグループ内のボリュームのステータスが最適で、変更処理の実行中でないことを確認してください。
- プールまたはボリュームグループに容量の拡張に使用する空き容量が必要です。

  プールまたはボリュームグループに空き容量がない場合は、未割り当て容量を未使用ドライブの形式でプールまたはボリュームグループに追加できます。

タスクの内容

次のストレージオブジェクトのリザーブ容量は8GiB単位でのみ拡張できます。

- Snapshotグループ
- Snapshotボリューム
- 整合性グループメンバーボリューム
- ミラーペアボリューム

プライマリボリュームで多数の変更が行われる可能性がある場合や、特定のコピーサービス処理の寿命が非常に長い場合は、割合を高くします。

読み取り専用のSnapshotボリュームのリザーブ容量は増やすことはできません。リザーブ容量が必要なのは、読み取り/書き込みのSnapshotボリュームだけです。

手順

1. 選択メニュー：Storage（Pool & Volume Groups）

2. 予約容量*タブを選択します。
3. リザーブ容量を増やすストレージオブジェクトを選択し、*容量の拡張*をクリックします。

   リザーブ容量の拡張ダイアログボックスが表示されます。

4. スピンボックスを使用して容量の割合を調整します。

   選択したストレージオブジェクトを含むプールまたはボリュームグループに空き容量がなく、ストレージアレイに未割り当て容量がある場合は、新しいプールまたはボリュームグループを作成できます。その後、そのプールまたはボリュームグループの新しい空き容量を使用してこの処理を再試行できます。

5. [* 拡大（ * ）] をクリックします

結果

System Managerは次の処理を実行します。

- ストレージオブジェクトのリザーブ容量を拡張します。
- 新たに追加したリザーブ容量を表示します。

リザーブ容量の削減

[容量の削減]オプションを使用して、Snapshotグループ、Snapshotボリューム、および整合性グループのメンバーボリュームのリザーブ容量を削減します。リザーブ容量は、拡張に使用した量だけ削減できます。

開始する前に

- ストレージオブジェクトに複数のリザーブ容量ボリュームが含まれている必要があります。
- ストレージオブジェクトがミラーペアボリュームでないことを確認してください。
- ストレージオブジェクトがSnapshotボリュームの場合は、無効になっているSnapshotボリュームである必要があります。
- ストレージオブジェクトがSnapshotグループの場合は、関連付けられているSnapshotイメージが含まれていないことを確認してください。

タスクの内容

次のガイドラインを確認してください。

- リザーブ容量ボリュームは、追加したときと逆の順序でのみ削除できます。
- 読み取り専用のSnapshotボリュームについては、関連付けられたリザーブ容量がないため、リザーブ容量を削減することはできません。リザーブ容量が必要なのは、読み取り/書き込みのSnapshotボリュームだけです。

手順

1. 選択メニュー：Storage（Pool & Volume Groups）
2. 予約容量*タブをクリックします。
3. リザーブ容量を削減するストレージオブジェクトを選択し、*容量の削減*をクリックします。

リザーブ容量の削減ダイアログボックスが表示されます。

4. リザーブ容量を削減する容量を選択し、*削減*をクリックします。

結果

System Managerは次の処理を実行します。

- ストレージオブジェクトの容量を更新します。
- ストレージオブジェクトの更新された新しいリザーブ容量が表示されます。
- Snapshotボリュームの容量を削減すると、System ManagerはSnapshotボリュームを自動的に無効状態に移行します。無効は、Snapshotボリュームが現在Snapshotイメージに関連付けられていないため、I/O処理でホストに割り当てることができないことを意味します。

Snapshotグループのリザーブ容量設定の変更

Snapshotグループの設定では、グループ名、自動削除設定、許可されるSnapshotイメージの最大数、System Managerがリザーブ容量のアラート通知を送信する割合、またはリザーブ容量が最大使用率に達したときに使用するポリシーを変更できます。

Snapshotグループの作成時に、グループに含まれるすべてのSnapshotイメージのデータを格納するためのリザーブ容量が作成されます。

手順

1. 選択メニュー：Storage（Pool & Volume Groups）
2. 予約容量*タブをクリックします。
3. 編集するSnapshotグループを選択し、*表示/設定の編集*をクリックします。

   スナップショットグループ設定ダイアログボックスが表示されます。

4. Snapshotグループの設定を適宜変更します。

フィールドの詳細

設定	製品説明
• Snapshotグループの設定*	名前
Snapshotグループの名前。Snapshotグループの名前は必ず指定する必要があります。	自動削除
グループ内のSnapshotイメージの総数をユーザ定義の最大数以下に抑えるための設定。このオプションを有効にすると、グループで許可されているSnapshotイメージの最大数に準拠するために、System Managerは新しいSnapshotが作成されるたびに最も古いSnapshotイメージを自動的に削除します。	Snapshotイメージの上限
Snapshotグループに許可されるSnapshotイメージの最大数（設定可能）。	Snapshotスケジュール
[Yes]の場合は、Snapshotを自動的に作成するスケジュールが設定されます。	リザーブ容量の設定
アラートを受け取るタイミング…	このスピンボックスを使用して、Snapshotグループのリザーブ容量が残り少なくなったときにSystem Managerからアラート通知を送信する割合を調整します。 Snapshotグループのリザーブ容量が指定したしきい値を超えるとSystem Managerからアラートが送信されるため、前もってリザーブ容量を増やしたり不要なオブジェクトを削除したりできます。

設定	製品説明
リザーブ容量がフルになった場合のポリシー	次のいずれかのポリシーを選択できます。 • 最も古い**Snapshot**イメージをパージする- System Managerはスナップショットグループ内の最も古いスナップショットイメージを自動的にパージし、そのスナップショットイメージのリザーブ容量を解放してグループ内で再利用します。 • ベースボリュームへの書き込みを拒否--リザーブ容量の割合が定義された上限に達すると、System Managerはリザーブ容量へのアクセスをトリガーしたベースボリュームに対するI/O書き込み要求をすべて拒否します。
関連付けられたオブジェクト	ベースボリューム
グループに使用されるベースボリュームの名前。ベースボリュームは、Snapshotイメージの作成元のボリュームです。シックボリュームでもシンボリュームでもかまいません。通常はホストに割り当てられます。ベースボリュームはボリュームグループまたはディスクプールのどちらかに配置できます。	Snapshotイメエシ

5. [保存]をクリックして'スナップショット・グループの設定に変更を適用します

Snapshotボリュームのリザーブ容量の設定の変更

Snapshotボリュームの設定を変更して、Snapshotボリュームのリザーブ容量が残り少なくなったときにシステムからアラート通知を送信する割合を調整できます。

手順

1. 選択メニュー：Storage（Pool & Volume Groups）
2. 予約容量*タブをクリックします。
3. 編集するSnapshotボリュームを選択し、*表示/設定の編集*をクリックします。

   Snapshot Volume Reserved Capacity Settingsダイアログボックスが表示されます。

4. Snapshotボリュームのリザーブ容量設定を適宜変更します。

フィールドの詳細

設定	製品説明
アラートを受け取るタイミング…	このスピンボックスを使用して、メンバーボリュームのリザーブ容量が残り少なくなったときにシステムからアラート通知を送信する割合を調整します。 Snapshotボリュームのリザーブ容量が指定したしきい値を超えるとシステムからアラートが送信されるため、前もってリザーブ容量を増やしたり不要なオブジェクトを削除したりできます。

5. 保存*をクリックして、スナップショットボリュームの予約容量設定に変更を適用します。

整合性グループのメンバーボリュームのリザーブ容量設定の変更

整合性グループのメンバーボリュームの設定を変更して、メンバーボリュームのリザーブ容量が残り少なくなったときにSystem Managerからアラート通知を送信する割合を調整したり、リザーブ容量が最大定義に達したときに使用するポリシーを変更したりできます 割合。

タスクの内容

個 々 のメンバーボリュームのリザーブ容量設定を変更すると、整合性グループに関連付けられているすべてのメンバーボリュームのリザーブ容量設定も変更されます。

手順

1. 選択メニュー：Storage（Pool & Volume Groups）
2. 予約容量*タブをクリックします。
3. 編集する整合性グループのメンバーボリュームを選択し、*表示/設定の編集*をクリックします。

   Member Volume Reserved Capacity Settings（メンバーボリュームのリザーブ容量設定）ダイアログボックスが表示されます。

4. メンバーボリュームのリザーブ容量の設定を適宜変更します。

フィールドの詳細

設定	製品説明
アラートを受け取るタイミング…	このスピンボックスを使用して、メンバーボリュームのリザーブ容量が残り少なくなったときにSystem Managerからアラート通知を送信する割合を調整します。 メンバーボリュームのリザーブ容量が指定したしきい値を超えるとSystem Managerからアラートが送信されるため、前もってリザーブ容量を増やしたり不要なオブジェクトを削除したりできます。 1つのメンバーボリュームのアラート設定を変更すると、同じ整合性グループに属する_ALL_MEMBER_VOLUMESのアラート設定が変更されます。
リザーブ容量がフルになった場合のポリシー	次のいずれかのポリシーを選択できます。 • 最も古い**Snapshot**イメージをパージする- System Managerは整合性グループの最も古いSnapshotイメージを自動的にパージします。これにより、メンバーのリザーブ容量が解放され、グループ内で再利用できます。 • ベースボリュームへの書き込みを拒否--リザーブ容量の割合が定義された上限に達すると、System Managerはリザーブ容量へのアクセスをトリガーしたベースボリュームに対するI/O書き込み要求をすべて拒否します。

5. [保存（Save）]をクリックして、変更を適用します。

結果

System Managerはメンバーボリュームのリザーブ容量設定だけでなく、整合性グループ内のすべてのメンバーボリュームのリザーブ容量設定を変更します。

ミラーペアボリュームのリザーブ容量設定の変更

ミラーペアボリュームの設定を変更して、ミラーペアボリュームのリザーブ容量が残り少なくなったときにSystem Managerからアラート通知を送信する割合を調整できます。

手順

1. 選択メニュー：Storage（Pool & Volume Groups）
2. 予約容量*タブを選択します。
3. 編集するミラーペアボリュームを選択し、*表示/設定の編集*をクリックします。

   ミラーペアボリュームのリザーブ容量の設定ダイアログボックスが表示されます。
4. ミラーペアボリュームのリザーブ容量の設定を適宜変更します。

フィールドの詳細

設定	製品説明
アラートを受け取るタイミング…	このスピンボックスを使用して、ミラーペアのリザーブ容量が残り少なくなったときにSystem Managerからアラート通知を送信する割合を調整します。 ミラーペアのリザーブ容量が指定したしきい値を超えるとSystem Managerからアラートが送信されるため、前もってリザーブ容量を増やすことができます。 1つのミラーペアのアラート設定を変更すると、同じミラー整合性グループに属するすべてのミラーペアのアラート設定が変更されます。

5. [保存（Save）]をクリックして、変更を適用します。

保留中の**Snapshot**イメージのキャンセル

保留中のSnapshotイメージを完了前にキャンセルすることができます。Snapshotは非同期的に作成され、作成が完了するまでSnapshotのステータスは「保留中」になります。Snapshotイメージは同期処理が完了するとすぐに作成されます。

タスクの内容

Snapshotイメージが保留状態になるのは、次の条件が同時に発生する場合です。

- Snapshotグループのベースボリューム、またはこのSnapshotイメージを含む整合性グループの1つ以上のメンバーボリュームが非同期ミラーグループのメンバーである。
- 現在、1個または複数のボリュームが非同期ミラーリングの同期処理中である。

手順

1. 選択メニュー：Storage（Pool & Volume Groups）
2. 予約容量*タブをクリックします。
3. 保留中のSnapshotイメージをキャンセルするSnapshotグループを選択し、メニューの[一般的でないタスク][保留中のSnapshotイメージのキャンセル]をクリックします。
4. 「* Yes」をクリックして、保留中のSnapshotイメージをキャンセルすることを確認します。

Snapshotグループの削除

Snapshotグループの削除は、グループのデータを完全に削除してシステムから削除する場合に実行します。Snapshotグループを削除すると、リザーブ容量が再生されてプールまたはボリュームグループで再利用できます。

タスクの内容

Snapshotグループを削除すると、グループ内のすべてのSnapshotイメージも削除されます。

手順

1. 選択メニュー：Storage（Pool & Volume Groups）
2. 予約容量*タブをクリックします。
3. 削除するSnapshotグループを選択し、メニューから「一般的でないタスク」「Snapshotグループの削除」をクリックします。

   Confirm Delete Snapshot Groupダイアログボックスが表示されます。
4. と入力し `delete`て確認します。

結果

System Managerは次の処理を実行します。

- Snapshotグループに関連付けられているSnapshotイメージをすべて削除します。
- Snapshotグループのイメージに関連付けられているSnapshotボリュームを無効化します。
- Snapshotグループ用のリザーブ容量を削除します。

FAQ

ボリュームグループとは何ですか？

ボリュームグループは、同じ特性を持つボリュームのコンテナです。ボリュームグループには容量とRAIDレベルが定義されています。ボリュームグループを使用して、ホストにアクセスできる1つ以上のボリュームを作成できます。（ボリュームはボリュームグループまたはプールから作成します）。

プールとは

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。プールを使用して、ホストにアクセスできる1つ以上のボリュームを作成できます。（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します）。

プールを使用すると、管理者が各ホストの使用状況を監視してストレージスペースが不足する可能性があるかどうかを判断する必要がなくなり、従来のディスクサイズ変更によるシステム停止を回避できます。プールの枯渇が近づくと、システムを停止することなくプールにドライブを追加でき、ホストからは透過的に容量の拡張が行われます。

プールを使用すると、データは自動的に再分散されてバランスが維持されます。パリティ情報とスペア容量をプール全体に分散することで、プール内のすべてのドライブを障害が発生したドライブのリビルドに使用できます。このアプローチでは専用のホットスペアドライブを使用しません。代わりに、予約済み（スペア）容量がプール全体でリザーブされます。ドライブ障害が発生すると、他のドライブのセグメントが読み取られてデータが再作成されます。次に、新しいドライブが選択され、障害が発生したドライブにあった各セグメントが書き込まれます。これにより、ドライブ間でのデータの分散が維持されます。

リザーブ容量とは何ですか？

リザーブ容量は、Snapshotイメージ、整合性グループメンバーボリューム、ミラーペア

ボリュームなどのコピーサービスオブジェクトのデータを格納する物理的に割り当てられた容量です。

コピーサービス処理に関連付けられているリザーブ容量ボリュームは、プールまたはボリュームグループに配置されます。リザーブ容量はプールまたはボリュームグループから作成します。

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受けています。

> 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のみのボリュームグループまたはプールで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。

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の整合性がチェックされます。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ボリュームのデータブロックをスキャンし、各ブロックの冗長性情報をチェックします。（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）。
- は、RAID 1ミラードライブ上のデータブロックを比較します。
- 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、エラーが発生することがあります。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。

プールとボリュームグループの違いは何ですか？

プールはボリュームグループに似ていますが、次の点が異なります。

- プール内のデータはプール内のすべてのドライブにランダムに格納されますが、ボリュームグループ内のデータは同じ一連のドライブに格納されます。

- プールでは、ドライブ障害時のパフォーマンスの低下や再構築にかかる時間が少なくて済みます。
- プールには予約済み容量が組み込まれているため、専用のホットスペアドライブは必要ありません。
- プールでは多数のドライブをグループ化できます。
- プールには指定されたRAIDレベルは必要ありません。

プールを手動で設定するのはどのような場合ですか？

次の例は、プールを手動で設定する理由を示しています。

- ストレージアレイに複数のアプリケーションがあり、それらのアプリケーションが同じドライブリソースについて競合しないようにする場合は、1つ以上のアプリケーション用に小さい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代わりに、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し、競合を軽減できます。

  プールを手動で作成するには、「* Storage 」を選択し、「 Pools & Volume Groups」を選択します。All Capacity（すべての容量）タブで、MENU（メニュー）：Create（プール）をクリックします。

- 同じドライブタイプのプールが複数ある場合は、System Managerでプールに使用するドライブが自動的に推奨されないことを示すメッセージが表示されます。ただし、既存のプールに手動でドライブを追加することはできます。

  既存のプールにドライブを手動で追加するには：プールとボリュームグループページでプールを選択し、*容量の追加*をクリックします。

容量アラートが重要なのはなぜですか？

容量アラートは、ドライブをプールに追加するタイミングを示します。ストレージアレイの処理を正常に実行するには、プールに十分な空き容量が必要です。プールの空き容量が指定した割合を超えたときにアラートを送信するようにSystem Managerを設定すると、これらの処理の中断を回避できます。

プールの作成時にこの割合を設定するには、* Pool auto-configuration オプションまたは Create pool *オプションを使用します。自動オプションを選択すると、アラート通知を受信するタイミングはデフォルト設定によって自動的に決まります。プールを手動で作成する場合は、アラート通知を設定できます。デフォルトの設定を使用することもできます。これらの設定は、後で「Settings [Alerts]」（設定[Alerts]）メニューで調整できます。

プールの空き容量が指定した割合に達すると、アラート設定に指定した方法でアラート通知が送信されます。

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、予約済み容量を増やすことができ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た場合、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* Pools & Volume Groups 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ドライブに分散されますが、予約済み容量はドライブ数で指定します。

プールから削除できるドライブの数に制限はありますか。

System Managerでは、プールから削除できるドライブ数が制限されています。

- 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。
- 削除対象のドライブに含まれるデータがプール内の残りのドライブに再配置される場合、そのデータを十分に格納できる空き容量がプール内にない場合は、そのドライブは削除できません。
- 一度に削除できるドライブは最大60本です。60本を超えるドライブを選択した場合、ドライブの削除オプションは無効になります。60本を超えるドライブを取り外す必要がある場合は、ドライブの取り外し処理を繰り返します。

ドライブではどのようなメディアタイプがサポートされていますか。

サポートされているメディアタイプは、ハードディスクドライブ（HDD）とソリッドステートディスク（SSD）です。

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、すべてのドライブを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。

- 未割り当ての、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。すでに別のプールまたはボリュームグループに属しているドライブ、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）搭載ハードディスクドライブ（HDD）
  - SASドライブ搭載のNVMe
  - 512バイトおよび4KiBのボリュームブロックサイズのドライブ
- 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ドライブの場合、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、FIPS以外の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Data Assurance（DA）対応ドライブが含まれていて、プールまたはボリュームグループにDA対応ボリュームが1つ以上ある場合は、DA対応でないドライブは使用できないため、そのプールまたはボリュームグループに追加することはできません。ただし、プールまたはボリュームグループにDA対応ボリュームがない場合は、DA対応でない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。これらのドライブを混在させる場合は、DA対応ボリュームは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して増やすことができます。

シェルフ/ドロワー損失の保護を維持する方法を教えてください。

プールまたはボリュームグループのシェルフ/ドロワー損失の保護を維持するには、次の表の条件を使用します。

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本以上含まれないようにする必要があります。 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。	シェルフの場合は6 ドロワーの場合は5
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それぞれ別 々 のシェルフまたはドロワーに配置されている。	3
RAID 1	ミラーペアの各ドライブが別 々 のシェルフまたはドロワーに配置されている必要があります。	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で障害が発生している場合、シェルフ/ドロワー損失の保護は維持されません。この場合、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。

プールとボリュームグループに最適なドライブの配置はどれですか？

プールとボリュームグループを作成する場合は、上部と下部のドライブスロットの間でドライブ選択のバランスを取るようにしてください。

EF600およびEF300コントローラでは、ドライブスロット0 11を1つのPCIブリッジに接続し、スロット12 23を別のPCIブリッジに接続します。最適なパフォーマンスを実現するには、上部スロットと下部スロットのドライブ数がほぼ同じになるように、ドライブ選択のバランスを調整する必要があります。この配置により、ボリュームが必要以上に早く帯域幅制限に達しないようにします。

アプリケーションに最適な**RAID**レベルを教えてください。

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レベルを判断するには、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。これらの割合は、[Performance]ページで確認できます。

RAIDレベルとアプリケーションパフォーマンス

RAIDには、_levels _という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レベルごとに異なるパフォーマンス機能が提供されます。読み取り率が高いアプリケーションでは、RAID 5ボリュームまたはRAID 6ボリュームを使用すると、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、パフォーマンスが向上します。

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が原因です。

次の情報に基づいてRAIDレベルを選択します。

- RAID 0*
- * 概要 *
  - 非冗長、ストライピングモード。
- どのように機能するか
  - RAID 0は、ボリュームグループ内のすべてのドライブにわたって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。
  - ストレージアレイ内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は、ディスクミラーリングを使用して、2つの重複ディスクに同時にデータを書き込みます。
  - RAID 10は、ドライブストライピングを使用して、ミラーリングされた一連の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、高い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およびRAID 10では、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完全な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ても、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がデグレード状態になります。ミラードライブはデータへのアクセスを許可します。
  - ボリュームグループ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には少なくとも2つのドライブが必要です。1つはユーザデータ用、もう1つはミラーリングされたデータ用です。
  - 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（ユーザデータ用に2本、ミラーリングされたデータ用に2本）でRAID 10が自動的に設定されます。
  - ボリュームグループには偶数個のドライブが必要です。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。ストレージアレイ内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がデグレード状態になります。冗長な情報により、データに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
  - ボリュームグループには少なくとも3本のドライブが必要です。

- 通常、ボリュームグループ内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、冗長性情報を使用することで引き続きデータにアクセスできます。
  - 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
  - ボリュームグループには少なくとも5本のドライブが必要です。
  - 通常、ボリュームグループ内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。プールは、ユーザインターフェイスによって自動的にRAID 6として構成されます。

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のため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（ミラーリング）や、データから導き出されたエラー修正コードなどがあります。ドライブで障害が発生した場合に、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ている容量を引いたものです。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。

Data Assuranceとは

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、ストレージアレイはボリューム内の各データブロックにエラーチェックコード（巡回冗長性チェック（CRC）とも呼ばれます）を追加します。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

ボリュームの作成時にDA対応のプールまたはボリュームグループ（[候補]の表で[DA]が[はい]になっている）を選択します。

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、Fibre Channel、SAS、iSCSI over TCP/IP、NVMe/FC、NVMe/IB、NVMe/RoCE、iSER over InfiniBand（iSCSI Extensions for RDMA/IB）があります。SRP over InfiniBandではDAはサポートされていません。

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す際に、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。

リザーブ容量を増やすときは、どのような点に注意する必要がありますか？

通常は、リザーブ容量がフルに近づく危険性があるという警告が表示されたときに容量を拡張します。リザーブ容量は8GiB単位でのみ拡張できます。

- 必要に応じて拡張できるように、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。

  プールまたはボリュームグループに空き容量がない場合は、未割り当て容量を未使用ドライブの形式でプールまたはボリュームグループに追加できます。

- プールまたはボリュームグループ内のボリュームのステータスが最適で、変更処理の実行中でないことを確認してください。
- プールまたはボリュームグループに容量の拡張に使用する空き容量が必要です。
- 読み取り専用のSnapshotボリュームのリザーブ容量は増やすことはできません。リザーブ容量が必要なのは、読み取り/書き込みのSnapshotボリュームだけです。

Snapshot処理のリザーブ容量は、通常はベースボリュームの40%です。非同期ミラーリング処理では、リザーブ容量は通常ベースボリュームの20%です。ベースボリュームで多くの変更が見込まれる場合や、ストレージオブジェクトのコピーサービス処理の使用期間が非常に長くなることが想定される場合は、これよりも割合を増やしてください。

削減する量を選択できないのはなぜですか？

リザーブ容量は、増やしたときの分量ずつしか減らすことができません。メンバーボリュームのリザーブ容量は、追加したときと逆の順序でのみ削除できます。

次のいずれかの条件に該当する場合、ストレージオブジェクトのリザーブ容量を削減することはできません。

- ストレージオブジェクトがミラーペアボリュームの場合。
- ストレージオブジェクトにリザーブ容量用のボリュームが1つだけ含まれている場合。ストレージオブジェクトにリザーブ容量用のボリュームが少なくとも2つ含まれている必要があります。
- ストレージオブジェクトが無効なSnapshotボリュームである場合。
- ストレージオブジェクトに関連付けられているSnapshotイメージが1つ以上含まれている場合。

リザーブ容量用のボリュームは、追加したときと逆の順序でのみ削除できます。

読み取り専用のSnapshotボリュームについては、関連付けられたリザーブ容量がないため、リザーブ容量を削減することはできません。リザーブ容量が必要なのは、読み取り/書き込みのSnapshotボリュームだけです。

メンバーボリュームごとにリザーブ容量が必要なのはなぜですか？

Snapshot整合性グループ内の各メンバーボリュームには、参照される整合性グループSnapshotイメージに影響を与えることなく、ホストアプリケーションによる変更をベースボリュームに保存するための独自のリザーブ容量が必要です。リザーブ容量は、読み取り/書き込み用に指定されたメンバーボリュームに含まれているデータのコピーへの書き込みアクセスをホストアプリケーションに提供します。

整合性グループSnapshotイメージに対するホストからの直接の読み取りや書き込みはできません。Snapshotイメージは、ベースボリュームからキャプチャされたデータのみを保存するために使用されます。

読み取り/書き込み用の整合性グループSnapshotボリュームの作成時に、System Managerは整合性グループのメンバーボリュームごとにリザーブ容量を作成します。このリザーブ容量により、ホストアプリケーションは、整合性グループSnapshotイメージに含まれているデータのコピーへの書き込みアクセスが可能になります。

SSDキャッシュのすべての統計を表示および表示するにはどうすればよいですか？

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統計をファイルにエクスポートした場合にのみ表示でき`.csv`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、次のメニューを選択します。Storage [Pools & Volume Groups]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]一般統計は[SSDキャッシュの統計を表示]ダイアログに表示されます。

次に、詳細統計のサブセットである一般統計を示します。

一般統計	製品説明
読み取り/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読み取りと書き込みの合計数。読み取り数を書き込み数と比較します。効率的なSSDキャッシュ処理には、読み取り数が書き込み数より多いことが必要です。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。
キャッシュヒット	キャッシュヒットの数。

一般統計	製品説明
キャッシュヒット(%)	キャッシュヒット数を読み取り+書き込み数で割った値。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%以上である必要があります。数値が小さい場合は、次のような場合があります。 • 書き込みに対する読み取りの比率が小さすぎる • 読み取りが繰り返されない • キャッシュ容量が小さすぎる
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量。このコントローラで使用可能なSSDキャッシュストレージの割合として表されます。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。キャッシュ割り当ての割合は、通常は100%と表示されます。この数値が100%未満の場合は、キャッシュがウォームアップされていないか、アクセスされているすべてのデータよりもSSDキャッシュ容量が大きいことを意味します。後者の場合は、SSDキャッシュ容量を小さくしても同じレベルのパフォーマンスを提供できます。この値は、キャッシュされたデータがSSDキャッシュに配置されたことを示しているわけではなく、SSDキャッシュにデータを配置可能となる前の準備手順にすぎません。
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量。割り当てられているSSDキャッシュストレージの割合として表されます。この値はSSDキャッシュの利用率または密度を表し、ユーザデータのバイト数を割り当てられているバイト数で割った値です。キャッシュ使用率のパーセンテージは通常100%より低く、おそらくはるかに低くなります。この数値は、SSDキャッシュ容量のうち、キャッシュデータが書き込まれている割合を示します。SSDキャッシュの各割り当て単位（SSDキャッシュブロック）はサブブロックと呼ばれる小さい単位に分割され、サブブロックにはある程度独立してデータが格納されるため、この数値は100%未満です。数値が大きいほど一般的には優れていますが、数値が小さい場合でもパフォーマンスが大幅に向上する可能性があります。

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。これらの追加の統計は一般統計と一緒に保存されますが、一般統計とは異なり、[SSDキャッシュの統計を表示]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、統計をファイルにエクスポートする `.csv`必要があります。

ファイルを表示する `.csv`と、一般統計のあとに詳細統計が表示されます。

詳細統計	製品説明
読み取りブロック	ホスト読み取りのブロック数。
書き込みブロック	ホスト書き込みのブロック数。
フルヒットブロック	キャッシュヒットのブロック数。フルヒットブロックは、SSDキャッシュから完全に読み取られたブロックの数を示します。SSDキャッシュのパフォーマンスが向上するのは、フルキャッシュヒットの処理に対してのみです。

詳細統計	製品説明
部分ヒット	すべてのブロックではなく、少なくとも1つのブロックがSSDキャッシュ内にあったホスト読み取りの数。部分ヒットはSSDキャッシュ*ミス*で、読み取りはベースボリュームから行われています。
部分ヒット-ブロック	[部分ヒット]のブロック数。部分キャッシュヒットと部分キャッシュヒットブロックは、SSDキャッシュにデータの一部しかない処理の結果として発生します。この場合、キャッシュされたハードディスクドライブ（HDD）ボリュームからデータを取得する必要があります。このタイプのヒットの場合、SSDキャッシュから得られるパフォーマンス上のメリットはありません。部分キャッシュヒットブロック数が完全キャッシュヒットブロック数よりも多い場合は、別のI/O特性タイプ（ファイルシステム、データベース、またはWebサーバ）を使用するとパフォーマンスが向上する可能性があります。SSDキャッシュのウォームアップ中は、[キャッシュヒット]と比較して[部分キャッシュヒット]と[キャッシュミス]の数が多くなることが想定されます。
ミス	SSDキャッシュ内にブロックがなかったホスト読み取りの数。SSDキャッシュミスは、ベースボリュームから読み取りが行われた場合に発生します。SSDキャッシュのウォームアップ中は、[キャッシュヒット]と比較して[部分キャッシュヒット]と[キャッシュミス]の数が多くなることが想定されます。
ミス-ブロック	[キャッシュミス]のブロック数。
取り込み処理（ホスト読み取り）	ベースボリュームからSSDキャッシュにデータがコピーされたホスト読み取りの数。
取り込み処理（ホスト読み取り）-ブロック	[取り込み処理（ホスト読み取り）]のブロック数。
取り込み処理（ホスト書き込み）	ベースボリュームからSSDキャッシュにデータがコピーされたホスト書き込みの数。書き込みI/O処理でキャッシュに書き込まないキャッシュ設定の場合、[取り込み処理（ホスト書き込み）]の数がゼロになることがあります。
取り込み処理（ホスト書き込み）-ブロック	[取り込み処理（ホスト書き込み）]のブロック数。
無効化処理	データが無効化された、またはSSDキャッシュから削除された回数。キャッシュの無効化処理は、各ホスト書き込み要求、Forced Unit Access（FUA）によるホスト読み取り要求、確認要求、およびその他一部の状況で実行されます。
リサイクル処理	別のベースボリュームや別の論理ブロックアドレス（LBA）範囲にSSDキャッシュブロックが再利用された回数。キャッシュ処理を効果的に行うには、読み取り処理と書き込み処理の合計数と比較して、再利用の数を少なくする必要があります。[リサイクル処理]の数が読み取りと書き込みの合計数に近い場合は、SSDキャッシュでスラッシングが発生しています。キャッシュ容量を増やす必要があります。または、ワークロードがSSDキャッシュの使用に適していません。

詳細統計	製品説明
使用可能バイト数	SSDキャッシュ内でこのコントローラによって使用可能なバイト数。
割り当てバイト数	このコントローラによってSSDキャッシュから割り当てられたバイト数。SSDキャッシュから割り当てられたバイトは、空の場合もあれば、ベースボリュームのデータが含まれている場合もあります。
ユーザデータバイト数	SSDキャッシュ内の、ベースボリュームのデータを含む割り当て済みバイト数。[Available Bytes]、[Allocated Bytes]、および[User Data Bytes]を使用して、キャッシュ割り当ての割合とキャッシュ使用率が計算されます。

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削って確保され、この容量をボリュームの作成に使用することはできません。

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]ダイアログの[追加の最適化容量]スライダを使用して、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。

[Additional Optimization Capacity]スライダは、EF600およびEF300ストレージシステムでのみ使用できます。

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削って確保され、この容量をボリュームの作成に使用することはできません。

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[追加の最適化容量]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。

[Additional Optimization Capacity]スライダは、EF600およびEF300ストレージシステムでのみ使用できます。

リソースプロビジョニング対応とは何ですか？

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。この機能を使用すると、ボリュームをバックグラウンドの初期化プロセスなしですぐに使用できるようになります。

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またはプール内のシックボリュームで、ボリュームの作成時に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）。一方、従来のシックボリュームでは、Data Assurance保護の情報フィールドを初期化し、各RAIDストライプでデータとRAIDパリティを整合させるために、すべてのドライブブロックがバックグラウンドのボリューム初期化処理で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の場合、バックグラウンドの初期化は時間に制限されません。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、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。リソースプロビジョニング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るすべてのドライブブロックの割り当てが解除されます（マッピングが解除されます）。また、ホストではNVMe Dataset ManagementコマンドまたはSCSI Unmap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の消耗度が向上し、最大書き込みパフォーマンスが向上します。どの程度向上するかは、ドライブのモデルや容量によって異なります。

リソースプロビジョニング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。この機能を使用すると、ボリュームをバックグラウンドの初期化プロセスなしですぐに使用できるようになります。

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またはプール内のシックボリュームで、ボリュームの作成時に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）。一方、従来のシックボリュームでは、Data Assurance保護の情報フィールドを初期化し、各RAIDストライプでデータとRAIDパリティを整合させるために、すべてのドライブブロックがバックグラウンドのボリューム初期化処理で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の場合、バックグラウンドの初期化は時間に制限されません。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、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。リソースプロビジョニング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るすべてのドライブブロックの割り当てが解除されます（マッピングが解除されます）。また、ホストではNVMe Dataset ManagementコマンドまたはSCSI Unmap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の消耗度が向上し、最大書き込みパフォーマンスが向上します。どの程度向上するかは、ドライブのモデルや容量によって異なります。

リソースプロビジョニングは、ドライブがDULBEをサポートするシステムでは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、* Pools & Volume Groups *で無効にできます。

ボリュームとワークロード

ボリュームとワークロードの概要

アプリケーション、データベース、およびファイルシステムがデータを格納するコンテナとしてボリュームを作成できます。ボリュームを作成するときは、特定のアプリケーション用にワークロードを選択してストレージアレイの構成をカスタマイズすることもできます。

ボリュームとワークロードとは

a_volume_は、ホストがアクセスするための特定の容量で作成される論理コンポーネントです。ボリュームは複数のドライブで構成される場合もありますが、ホストでは1つの論理コンポーネントとして認識されます。定義したボリュームは、ワークロードに追加できます。a_workload _は、SQL ServerやExchangeなどの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、このアプリケーションのストレージを最適化するために使用できます。

詳細：

- "ボリュームの機能"
- "ワークロードの仕組み"
- "ボリュームに関する用語"
- "ボリュームの容量の割り当て方法"
- "ボリュームで実行できる操作"

ボリュームとワークロードをどのように作成しますか？

まず、ワークロードを作成します。メニュー「Storage [Volumes]」に移動し、手順を示すウィザードを開きます。次に、プールまたはボリュームグループの使用可能な容量からボリュームを作成し、作成したワークロードを割り当てます。

詳細：

- "ボリュームを作成するためのワークフロー"
- "ワークロードの作成"
- "ボリュームの作成"
- "ワークロードへのボリュームの追加"

関連情報

ボリュームに関連する概念の詳細については、以下を参照してください。

- "ボリュームのデータ整合性とデータセキュリティ"
- "SSDキャッシュとボリューム"
- "シンボリュームの監視"

概念

ボリュームの機能

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し、システムのリソースを簡単に整理して使用できます。この概念は、コンピュータ上のフォルダ/ディレクトリを使用してファイルを整理し、簡単かつ迅速にアクセスできるようにするのと似ています。

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、論理ユニット番号（LUN）にマッピングされたボリュームをホストから認識できます。LUNには、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（FC、iSCSI、SASなど）を使用してアクセス可能なユーザデータが格納されます。

プールおよびボリュームグループから作成できるボリュームタイプ

ボリュームは、プールまたはボリュームグループから容量を取得します。ストレージアレイ上のプールまたはボリュームグループから次のタイプのボリュームを作成できます。

- プールから--プールからは、フルプロビジョニング（シック）ボリューム_または_シンプロビジョニング（シン）ボリュームとしてボリュームを作成できます。

> System Manager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。シンボリュームを作成する場合は、コマンドラインインターフェイス（CLI）を使用します。

- ボリュームグループから--ボリュームグループからボリュームを作成できるのは_完全にプロビジョニングされた（シック）ボリューム_のみです。

シックボリュームとシンボリュームは、次の方法でストレージアレイから容量を取得します。

- シックボリュームの容量は、ボリュームの作成時に割り当てられます。
- シンボリュームの容量は、ボリュームへの書き込み時にデータとして割り当てられます。

シンプロビジョニングを使用すると、容量の無駄な割り当てを回避し、ストレージの先行投資を抑えることができます。ただし、シックボリュームの作成時にすべてのストレージが一度に割り当てられるため、フルプロビジョニングの場合はレイテンシが低減されます。

> EF600およびEF300ストレージシステムでは、シンプロビジョニングはサポートされません。

ボリュームの特性

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、格納するデータのタイプに基づいた独自の特性があります。次のような特徴があります。

- 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。セグメントサイズがボリュームグループの容量以下である。プールのセグメントサイズは固定であり、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て、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ある必要があります。
- 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が1台のコントローラで管理されます。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分散の問題が修正されます。自動ロードバランシングは、I/Oワークロードを自動で分散し、ホストからの受信I/Oトラフィックを動的に管理して両方のコントローラに分散します。
- 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、Logical Unit Number（LUN；論理ユニット番号）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、すべてのホストでボリュームを使用できるようにします。

  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を制限できます。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。

- 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割り当てられます。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。

ワークロードの仕組み

ボリュームを作成する際には、特定のアプリケーション用のワークロードを選択して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（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。

ボリュームの作成時には、ワークロードの用途に関する情報を入力するように求められます。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ボリュームの最適な構成が作成され、必要に応じて編集することもできます。必要に応じて、ボリューム作成のこの手順を省略できます。

ワークロードの種類

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ことがあります。I/Oタイプ、セグメントサイズ、コントローラ所有権、読み取りキャッシュと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™
- Microsoft®Exchange Server™
- ビデオ監視アプリケーション
- VMware ESXi™（仮想マシンファイルシステムで使用するボリューム用）

  推奨されるボリューム構成を確認し、[ボリュームの追加/編集]ダイアログボックスを使用して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。

- 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システムに組み込まれていない場合は、「その他」のワークロードで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、SANtricity System Managerを起動します。このインターフェイスから、次の2つの方法で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表示できます。

- ボリュームのタイルで「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*タブを選択すると、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一定の間隔で収集することで、ベースラインの測定値を設定して傾向を分析できます。これは、I/Oパフォーマンスに関連する問題の調査に役立ちます。

ボリュームに関する用語

ストレージアレイに関連するボリュームの用語を次に示します。

すべてのボリュームタイプ

期間	製品説明
割り当て容量	割り当て容量は、ボリュームの作成やコピーサービス処理に使用します。 割り当て容量とレポート容量はシックボリュームでは同じですが、シンボリュームでは異なります。シックボリュームの場合、物理的に割り当てられたスペースは、ホストに報告されるスペースと同じになります。シンボリュームの場合、レポート容量はホストに報告される容量であり、割り当て容量はデータの書き込み用に現在割り当てられているドライブスペースの量です。

期間	製品説明
アプリケーション	アプリケーションとは、SQL ServerやExchangeなどのソフトウェアのことです。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、読み取りキャッシュと書き込みキャッシュなどの特性が含まれます。
容量	容量は、ボリュームに格納できるデータの量です。
コントローラ所有権	コントローラ所有権は、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。ボリュームは'ボリュームを所有する優先コントローラ（AまたはB）を持つことができますボリューム所有権は、自動ロードバランシング機能を使用して自動的に調整され、コントローラ間でワークロードが移動する際の負荷分散の問題が修正されます。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し、ホストからの受信I/Oトラフィックを動的に管理して両方のコントローラに分散します。
動的キャッシュ読み取りプリフェッチ	動的キャッシュ読み取りプリフェッチでは、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することができます。このキャッシュにより、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。ランダムアクセスでは、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。 動的キャッシュ読み取りプリフェッチはシンボリュームに対しては常に無効で、変更することはできません。
空き容量領域	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に制限されます。たとえば、ボリュームグループの合計空き容量が15GiBで、最も大きい空き容量領域が10GiBの場合、作成できるボリュームの最大サイズは10GiBです。 空き容量を統合することで、ボリュームグループ内の空き容量を最大限に増やして追加ボリュームを作成できます。
ホスト	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。
ホストクラスタ	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。

期間	製品説明
ホットスペアドライブ	ホットスペアドライブはボリュームグループでのみサポートされます。ホットスペアドライブにはデータは格納されておらず、ボリュームグループに含まれるRAID 1、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のスタンバイとして機能します。ホットスペアドライブを使用すると、ストレージアレイの冗長性が向上します。
LUN	Logical Unit Number（LUN；論理ユニット番号）は、ホストがボリュームへのアクセスに使用する番号で、アドレススペースに割り当てられます。ボリュームは、LUNの形式で容量としてホストに提示されます。 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を異なるホストで使用して、異なるボリュームにアクセスできます。
メテイアスキヤン	メディアスキャンは、ドライブに対する通常の読み取り/書き込みの際に、ドライブメディアのエラーが検出される前に検出する機能です。メディアスキャンはバックグラウンド処理として実行され、定義されたユーザボリューム内のすべてのデータと冗長性情報がスキャンされます。
ネームスペース	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、ストレージアレイ内のボリュームに関連します。
プール	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。プールを使用して、ホストにアクセスできる1つ以上のボリュームを作成できます。（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します）。
プールまたはボリュームグループの容量	プール、ボリューム、またはボリュームグループの容量は、プールまたはボリュームグループに割り当てられているストレージアレイ内の容量です。この容量は、ボリュームを作成し、コピーサービス処理やストレージオブジェクトで必要とされるさまざまな容量に対応するために使用されます。
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。
レポート容量	レポート容量は、ホストに報告され、ホストからアクセスできる容量です。 レポート容量と割り当て容量はシックボリュームでは同じですが、シンボリュームでは異なります。シックボリュームの場合、物理的に割り当てられたスペースは、ホストに報告されるスペースと同じになります。シンボリュームの場合、レポート容量はホストに報告される容量であり、割り当て容量はデータの書き込み用に現在割り当てられているドライブスペースの量です。

期間	製品説明
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。セグメントサイズがボリュームグループの容量以下である。プールのセグメントサイズは固定であり、変更することはできません。
ストライピング	ストライピングは、ストレージアレイにデータを格納する方法の1つです。ストライピングでは、データフローが特定のサイズ（「ブロックサイズ」）のブロックに分割され、それらのブロックがドライブに1つずつ書き込まれます。このデータ格納方法は、複数の物理ドライブにデータを分散して格納する場合に使用されます。ストライピングはRAID 0と同義で、パリティを使用せずにRAIDグループ内のすべてのドライブにデータを分散します。
ボリューム	ボリュームは、アプリケーション、データベース、およびファイルシステムがデータを格納するコンテナです。ホストがストレージアレイのストレージにアクセスするために作成される論理コンポーネントです。
ボリュームの割り当て	ボリューム割り当てとは、ホストLUNのボリュームへの割り当てです。
ボリューム名	ボリューム名は、ボリュームの作成時に割り当てられる文字列です。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。
ボリュームグループ	ボリュームグループは、同じ特性を持つボリュームのコンテナです。ボリュームグループには容量とRAIDレベルが定義されています。ボリュームグループを使用して、ホストにアクセスできる1つ以上のボリュームを作成できます。（ボリュームはボリュームグループまたはプールから作成します）。
ワークロード	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（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。
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。データは、ドライブに書き込まれるまで書き込みキャッシュに残ります。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。

期間	製品説明
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る場合に発生します。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。
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設定すると、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継続されます。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。

シンボリューム固有

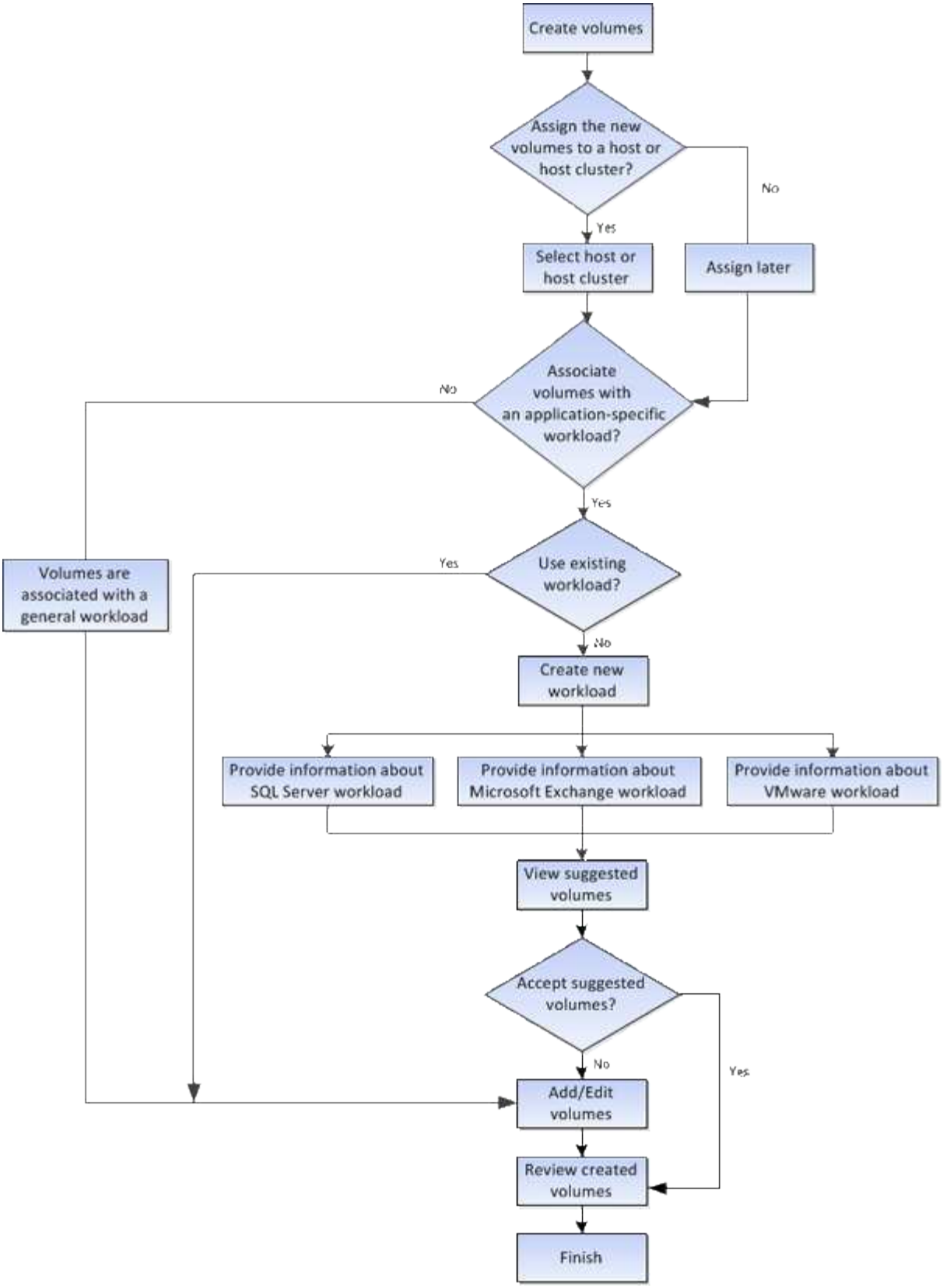
System Managerには、シンボリュームを作成するオプションはありません。シンボリュームを作成する場合は、コマンドラインインターフェイス（CLI）を使用してください。

シンボリュームはEF600またはEF300ストレージシステムでは使用できません。

期間	製品説明
割り当て容量の制限	割り当て容量の制限は、シンボリュームの拡張時に割り当てることができる物理容量の上限です。
書き込み済み容量	書き込み済み容量は、シンボリュームに割り当てられたリザーブ容量のうちの書き込み済みの容量です。
警告しきい値	警告しきい値アラートは、シンボリュームの割り当て容量がしきい値に達したときに発行されるように設定できます（警告しきい値）。

ボリュームを作成するためのワークフロー

System Managerでは、次の手順でボリュームを作成します。



ボリュームのデータ整合性とデータセキュリティ

ボリュームでData Assurance（DA）機能とドライブセキュリティ機能を有効にして使用することができます。これらの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。

Data Assurance

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、ストレージアレイはボリューム内の各データブロックにエラーチェックコード（巡回冗長性チェック（CRC）とも呼ばれます）を追加します。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、新しいボリュームの作成時にDA対応のプールまたはボリュームグループ（[候補]の表で[DA]が[はい]になっている）を選択します。

ドライブセキュリティ

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す際に、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）140-2レベル2に準拠したドライブ（FIPSドライブ）があります。

ドライブレベルでのドライブセキュリティの動作

セキュリティ対応ドライブであるFDEまたはFIPSでは、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。この暗号化と復号化は、パフォーマンスやユーザのワークフローには影響しません。各ドライブには固有の暗号化キーがあり、ドライブから転送することはできません。

ボリュームレベルでのドライブセキュリティの動作

セキュリティ対応ドライブからプールまたはボリュームグループを作成する場合、そのプールまたはボリュームグループに対してドライブセキュリティを有効にすることもできます。ドライブセキュリティを有効にすると、ドライブとそれに関連付けられているボリュームグループおよびプールがsecure-_enabled_になります。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両方のドライブを含めることができますが、暗号化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。

ドライブセキュリティの実装方法

ドライブセキュリティを実装するには、次の手順を実行します。

1. ストレージアレイにセキュリティ対応のFDEドライブまたはFIPSドライブを取り付けます（FIPSのサポートが必要なドライブには、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のみのボリュームグループまたはプールで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）。
2. セキュリティキーを作成します。セキュリティキーは、読み取り/書き込みアクセス用にコントローラとドライブで共有される文字列です。コントローラの永続的メモリから内部キーを作成するか、キー管理サーバから外部キーを作成できます。外部キー管理の場合は、キー管理サーバとの間で認証を確立する必要があります。
3. プールおよびボリュームグループに対してドライブ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を作成します（受験者テーブルの「Secure Capable 」列で「 Yes」を検索してください）。
   - 新しいボリュームを作成するときにプールまたはボリュームグループを選択します（Pool and volume

group Candidatesテーブルで、「* SecureCapable 」の横の「 Yes」*を探します）。

ドライブセキュリティ機能を使用する場合、セキュリティ有効ドライブとストレージアレイのコントローラで共有されるセキュリティキーを作成します。ドライブの電源をオフにしてオンにするたびに、コントローラがセキュリティキーを適用するまでセキュリティ有効ドライブはセキュリティロック状態になります。

SSDキャッシュとボリューム

読み取り専用のパフォーマンスを向上させる方法として、SSDキャッシュにボリュームを追加できます。SSDキャッシュは、ストレージアレイ内で論理的にグループ化した一連のソリッドステートディスク（SSD）ドライブで構成されます。

ボリューム

SSDキャッシュとの間のデータの移動には、単純なボリュームI/Oのメカニズムが使用されます。データがキャッシュされてSSDに格納されると、そのデータの以降の読み取りはSSDキャッシュで実行されるため、HDDボリュームにアクセスする必要はありません。

SSDキャッシュはセカンダリキャッシュであり、コントローラの動的ランダムアクセスメモリ（DRAM）にあるプライマリキャッシュと組み合わせて使用されます。

- プライマリキャッシュでは、ホスト読み取り後にデータがDRAMに格納されます。
- SSDキャッシュでは、データはボリュームからコピーされて2つの内部RAIDボリューム（コントローラごとに1つ）に格納されます。RAIDボリュームはSSDキャッシュの作成時に自動的に作成されます。

内部RAIDボリュームは、内部的なキャッシュ処理に使用されます。これらのボリュームにはアクセスできず、ユーザインターフェイスにも表示されません。ただし、ストレージアレイで許可されるボリュームの総数には、これら2つのボリュームが含まれます。

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転送の対象になりません。

ドライブセキュリティ機能

ドライブセキュリティを使用している（セキュリティ有効）ボリュームでSSDキャッシュを使用する場合は、そのボリュームとSSDキャッシュのドライブセキュリティ機能が同じである必要があります。同じでない場合、ボリュームはセキュリティ有効になりません。

ボリュームで実行できる操作

ボリュームに対しては、容量の拡張、削除、コピー、初期化、再配置、所有権の変更、キャッシュ設定の変更、メディアスキャン設定の変更など、さまざまな操作を実行できます。

容量の拡張

ボリュームの容量は次の2つの方法で拡張できます。

- プールまたはボリュームグループの使用可能な空き容量を使用します。

ボリュームに容量を追加するには、メニューからStorage（Pool and Volume Groups）> Add Capacity（容量の追加）を選択します。

- ボリュームのプールまたはボリュームグループに未割り当て容量（未使用ドライブ）を追加します。このオプションは、プールまたはボリュームグループに空き容量がない場合に使用します。

  プールまたはボリュームグループに未割り当て容量を追加するには、メニューからStorage（Pool and Volume Groups）> Add Capacity（容量の追加）を選択します。

  プールまたはボリュームグループに使用可能な空き容量がない場合、ボリュームの容量を拡張することはできません。先にプールまたはボリュームグループのサイズを拡張するか、未使用のボリュームを削除する必要があります。

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。

削除

ボリュームを削除する一般的な状況としては、作成したボリュームのパラメータや容量に誤りがあった場合、ストレージ構成のニーズを満たさなくなった場合、バックアップやアプリケーションのテストに必要なくなったSnapshotイメージがある場合などがあります。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。ボリュームを削除すると、関連付けられているSnapshotイメージ、スケジュール、Snapshotボリュームも削除され、ミラーリング関係も削除されます。

コピー

ボリュームをコピーすると、ソースボリュームとターゲットボリュームの2つのボリュームのポイントインタイムコピーが同じストレージアレイ上に作成されます。ボリュームをコピーするには、メニューから「Storage [Volumes]> Copy Services > Copy volume」を選択します。

初期化

ボリュームを初期化すると、ボリュームからすべてのデータが消去されます。ボリュームは、最初に作成された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。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、割り当て容量、およびリザーブ容量の設定は維持されます。Data Assurance（DA）設定とセキュリティ設定も同じままです。

ボリュームを初期化するには、メニューからStorage [Volumes]> More > Initialize volumesを選択します。

再配置

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で問題が発生すると、マルチパスドライバによって優先コントローラ所有者からボリュームが移動されます。

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った場合は、ホストのマルチパスドライバが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。

ボリュームを再配置するには、メニューを選択します。Storage [Volumes]>[More]> redistribute volumes]

ボリューム所有権の変更

ボリュームの所有権を変更すると、ボリュームの優先コントローラ所有権が変更されます。ボリュームの優先コントローラ所有者は、メニューの下に表示されます。Storage [Volumes]、[View/Edit Settings]、[Advanced]タブ

ボリュームの所有権を変更するには、メニューから次のいずれかを選択します。Storage [Volumes]、[More（その他）]、[Change ownership（所有権の変更）]。

ミラーリングとボリューム所有権

ミラーペアのプライマリボリュームがコントローラAに所有されている場合、セカンダリボリュームもリモートストレージアレイのコントローラAに所有されます。プライマリボリュームの所有者を変更すると、セカンダリボリュームの所有者が自動的に変更され、両方のボリュームが同じコントローラで所有されるようになります。プライマリ側で現在の所有権が変更されると、セカンダリ側の対応する所有権も自動的に変更されます。

ミラー整合性グループにローカルのセカンダリボリュームが含まれている場合にコントローラ所有権が変更されると、セカンダリボリュームは最初の書き込み処理時に自動的に元のコントローラ所有者に戻されます。所有権の変更*オプションを使用してセカンダリボリュームのコントローラ所有権を変更することはできません。

ボリュームのコピーとボリューム所有権

ボリュームのコピー処理では、ソースボリュームとターゲットボリュームの両方を同じコントローラが所有している必要があります。ボリュームコピー処理の開始時に、両方のボリュームの優先コントローラが同じでないことがあります。そのため、ターゲットボリュームの所有権がソースボリュームの優先コントローラに自動的に転送されます。ボリュームコピーが完了するか停止すると、ターゲットボリュームの所有権は優先コントローラにリストアされます。

ボリュームのコピー処理中にソースボリュームの所有権が変更された場合は、ターゲットボリュームの所有権も変更されます。特定のオペレーティングシステム環境では、I/Oパスを使用する前に、マルチパスホストドライバの再設定が必要になる場合があります。（一部のマルチパスドライバでは、I/Oパスを認識するために編集が必要です。詳細については、ドライバのマニュアルを参照してください）。

キャッシュ設定の変更

キャッシュメモリは、ドライブメディアよりもアクセス時間が速い、コントローラ上の一時的な揮発性ストレージ（RAM）の領域です。キャッシュメモリを使用すると、次の理由により全体的なI/Oパフォーマンスを向上させることができます。

- 読み取り用にホストから要求されたデータは、以前の処理ですでにキャッシュに格納されている可能性があるため、ドライブにアクセスする必要はありません。
- 書き込みデータは最初にキャッシュに書き込まれるため、データがドライブに書き込まれるのを待つことなくアプリケーションが処理を続行できます。

メニューを選択します。Storage [Volumes]、[More（その他）]、[Change cache settings]（キャッシュ設定の

変更）。次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--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。データは、ドライブに書き込まれるまで書き込みキャッシュに残ります。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。

- 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たときに発生しますそのため、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。
- 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設定により、バッテリがない、故障している、完全に放電されている、またはフル充電されていない場合でも書き込みキャッシュを続行できます。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。

  この設定は、書き込みキャッシュを有効にしている場合にのみ使用できます。この設定はシンボリュームに対しては使用できません。

- 動的キャッシュ読み取りプリフェッチ--動的キャッシュ読み取りプリフェッチにより'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'追加のシーケンシャル・データ・ブロックをキャッシュにコピーすることができますこのキャッシュにより、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。ランダムアクセスでは、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。

  動的キャッシュ読み取りプリフェッチはシンボリュームに対しては常に無効で、変更することはできません。

メディアスキャン設定の変更

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。このスキャンを実行すると、プールまたはボリュームグループ内の他のドライブで障害が発生した場合に、障害ドライブのデータが冗長性情報とプールまたはボリュームグループ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、データ損失が発生するのを防ぐことができます。

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、同じ速度で再開されます。

メディアスキャンの実行期間を有効にして設定するには、メニューを選択します。Storage [Volumes]、[More]、[Change media scan settings]の順に選択します。

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。そのボリュームに対して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がある場合は、ボリューム内の冗長性情報がデータとの整合性がチェックされます。メディアスキャンと冗長性チェックは、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は、冗長性情報を使用してデータが修復されます（使用可能な場合）。たとえば、冗長性情報は、最適なRAID 5ボリューム、最適なRAID 6ボリューム、または1つのドライブだけで障害が発生したRAID 6ボリュームで確認できます。冗長性情報を使用してリカバリ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の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ると、イベントログに報告されます。

ボリュームの容量の割り当て方法

ストレージアレイ内のドライブは、データの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は、ストレージアレイのデータの設定、格納、保守、保持に使用します。

容量を使用したボリュームの作成と拡張

ボリュームは、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。

シックボリュームとシンボリュームの容量タイプ

シックボリュームまたはシンボリュームを作成できます。レポート容量と割り当て容量はシックボリュームでは同じですが、シンボリュームでは異なります。

- シックボリュームの場合、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になります。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たスペースは、ホストに報告されるスペースと同じです。

  通常、シックボリュームのレポート容量は、ボリュームが拡張されると予想される最大容量に設定します。シックボリュームは、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るためです。

- シンボリュームの場合、レポート容量はホストに報告される容量であり、割り当て容量はデータの書き込み用に現在割り当てられているドライブスペースの量です。

  レポート容量は、ストレージアレイで割り当てられた容量よりも大きくなることがあります。シンボリュームは、現在使用可能な資産に関係なく、拡張に応じてサイズを設定できます。

SANtricity System Manager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。シンボリュームを作成する場合は、コマンドラインインターフェイス（CLI）を使用します。

シックボリュームの容量制限

シックボリュームの最小容量は1MiBで、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。

シックボリュームのレポート容量を拡張する場合は、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容量以下の容量を指定する必要があります。

  ボリュームを作成すると、セグメントサイズの動的変更（DSS）用に追加の容量が事前に割り当てられます。DSS移行は、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、一部のホストオペレーティングシステムでは、最大128TiBのボリュームがサポートされます。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。

シンボリュームの容量制限

レポート容量が大きく、割り当て容量が比較的小さいシンボリュームを作成できます。これは、ストレージの利用率と効率を高めるのに役立ちます。シンボリュームを使用すると、アプリケーションの中断を伴わずにアプリケーションのニーズの変化に応じて割り当て容量を増やすことができるため、ストレージ管理が簡易化され、ストレージ利用率が向上します。

シンボリュームには、レポート容量と割り当て容量に加えて、書き込み済み容量も含まれます。書き込み済み容量は、シンボリュームに割り当てられたリザーブ容量のうちの書き込み済みの容量です。

次の表に、シンボリュームの容量制限を示します。

容量のタイプ	最小サイズ	最大サイズ
レポート済み	32MiB	256 TiB
割り当て済み	4MiB	64TiB

シンボリュームの場合、最大レポート容量の256TiBに達していると容量を拡張できません。シンボリュームのリザーブ容量が最大レポート容量よりも大きいサイズに設定されていることを確認してください。

割り当て容量は、割り当て容量の制限に基づいて自動的に拡張されます。割り当て容量の制限を使用すると、シンボリュームの自動拡張をレポート容量未満に制限できます。書き込まれるデータの量が割り当て容量に近付いたときは、割り当て容量の制限を変更することができます。

割り当て容量の制限を変更するには、メニューを選択します。Storage [Volumes]> Thin Volume Monitoringタブ> Change Limit]

System Managerでは、シンボリュームの作成時にフル容量を割り当てないため、プールの空き容量が不足する可能性があります。スペースが不足していると、シンボリュームだけでなく、プールの容量を必要とするそ

の他の処理（SnapshotイメージやSnapshotボリュームなど）でもプールへの書き込みがブロックされる可能性があります。ただし、プールからの読み取り処理は引き続き実行できます。この状況が発生すると、アラートしきい値の警告が表示されます。

シンボリュームの監視

シンボリュームのスペースを監視して適切なアラートを生成することで、容量不足を回避できます。

シンプロビジョニング環境では、基盤となる物理ストレージよりも多くの論理スペースを割り当てることができます。メニューから「Storage [Volumes]> Thin Volume Monitoring]タブを選択すると、シンボリュームが割り当て容量の上限に達するまでの増加量を監視できます。

Thin Monitoringビューを使用して、次の操作を実行できます。

- シンボリュームを自動的に拡張できる割り当て容量を制限する制限を定義します。
- シンボリュームが割り当て容量の上限に近づいたときに[ホーム]ページの[通知]領域にアラート（警告しきい値の超過）が送信される割合を設定します。

シンボリュームの容量を拡張するには、レポート容量を拡張してください。

> System Manager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。シンボリュームを作成する場合は、コマンドラインインターフェイス（CLI）を使用します。

> シンボリュームはEF600またはEF300ストレージシステムでは使用できません。

シックボリュームとシンボリュームの比較

シックボリュームは常にフルプロビジョニングされます。つまり、ボリュームの作成時にすべての容量が割り当てられます。シンボリュームは常にシンプロビジョニングされます。つまり、ボリュームにデータが書き込まれるときに容量が割り当てられます。

> System Manager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。シンボリュームを作成する場合は、コマンドラインインターフェイス（CLI）を使用します。

ボリュームタイプ	製品説明
シックボリューム	• シックボリュームは、プールまたはボリュームグループから作成されます。 • シックボリュームでは、将来のストレージニーズに備えて、大量のストレージスペースが事前に確保されます。 • シックボリュームは、ボリューム作成時に物理ストレージに事前に割り当てられたボリュームのサイズ全体を使用して作成されます。つまり、100GiBのボリュームを作成すると、ドライブ上で割り当てられた100GiBの容量が実際に消費されます。ただし、スペースが未使用のままになり、ストレージ容量の利用率が低下する可能性があります。 • シックボリュームを作成する場合は、1つのボリュームに容量を過剰に割り当てないようにしてください。1つのボリュームに容量を過剰に割り当てると、システム内の物理ストレージをすぐに使い果たしてしまう可能性があります。 • 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、非同期ミラーリング）用のストレージ容量も必要なため、シックボリュームにすべての容量を割り当てないでください。スペースが不足していると、プールまたはボリュームグループへの書き込みがブロックされる可能性があります。この状況が発生すると、空き容量アラートしきい値の警告が表示されます。
シンボリューム	• シンボリュームはプールからのみ作成され、ボリュームグループからは作成されません。 • シンボリュームはRAID 6である必要があります。 • シンボリュームはEF600またはEF300ストレージシステムでは使用できません。 • シンボリュームを作成するにはCLIを使用する必要があります。 • シックボリュームとは異なり、シンボリュームに必要なスペースは作成時に割り当てられず、必要に応じてあとから提供されます。 • シンボリュームでは、サイズを過剰に割り当てることができます。つまり、ボリュームのサイズよりも大きいLUNサイズを割り当てることができます。その後、LUNのサイズを拡張することなく、ユーザを切断することなく、必要に応じてボリュームを拡張できます（必要に応じてドライブを追加します）。 • シンプロビジョニングブロックのスペース再生（UNMAP）を使用すると、ホストからSCSI UNMAPコマンドを実行して、ストレージアレイ上のシンプロビジョニングされたボリュームのブロックを再生できます。シンプロビジョニングをサポートするストレージアレイでは、再生されたスペースを同じストレージアレイ内の他のシンプロビジョニングされたボリュームの割り当て要求に使用できます。これにより、ディスクスペースの消費状況が適切にレポートされ、リソースがより効率的に使用されるようになります。

シンボリュームの制限事項

シンボリュームでは、次の例外を除き、シックボリュームとしてのすべての処理がサポートされます。

- シンボリュームのセグメントサイズは変更できません。

- シンボリュームに対して読み取り前冗長性チェックを有効にすることはできません。
- シンボリュームをボリュームコピー処理のターゲットボリュームとして使用することはできません。
- シンボリュームの割り当て容量制限と警告しきい値は、非同期ミラーペアのプライマリ側でのみ変更できます。プライマリ側でこれらのパラメータを変更すると、自動的にセカンダリ側に反映されます。

ストレージを設定する

ワークロードの作成

あらゆるタイプのアプリケーションのワークロードを作成できます。

タスクの内容

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（インスタンス）を定義できます。

手順

1. 選択メニュー： Storage [Volumes]
2. メニューを選択します。Create [Workload]。

   [Create Application Workload]ダイアログボックスが表示されます。

3. 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。
4. [作成（ Create ）] をクリックします。

終了後

ワークロードを作成したら、そのワークロードにストレージ容量を追加できます。アプリケーション用に1つ以上のボリュームを作成し、各ボリュームに特定の量の容量を割り当てるには、* Create Volume *オプションを使用します。

ボリュームの作成

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から認識されるようにします。また、ボリューム作成手順では、作成する各ボリュームに特定の容量を割り当てることもできます。

タスクの内容

ほとんどのアプリケーションタイプでは、ユーザ定義のボリューム構成がデフォルトで適用されます。一部のアプリケーションタイプでは、ボリュームの作成時にスマートな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。System Managerでは、この情報に基づいてボリュームの構成を最適化します。この構成は、必要に応じて編集することもできます。

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ます。

手順1：ボリュームのホストを選択する

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から認識されるようにします。また、ボリューム作成手順では、作成する各ボリュームに特定の容量を割り当てることもできます。

開始する前に

- ホストタイルの下に、有効なホストまたはホストクラスタが存在します。
- 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のいずれかのホスト接続でDAがサポートされていない場合、関連付けられているホストはDA対応ボリュームのデータにアクセスできません。

タスクの内容

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。
- 割り当ては、ストレージアレイ内のボリュームごとに1つずつ定義できます。
- 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。
- 1つのホストまたはホストクラスタが、同じ論理ユニット番号（LUN）を2回使用してボリュームにアクセス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。
- ボリュームの作成にかかる時間を短縮するには、ホストの割り当て手順を省略して、新しく作成したボリュームをオフラインで初期化します。

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

手順

1. 選択メニュー： Storage [Volumes]
2. メニューから[ボリュームの作成]を選択します。

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

3. ドロップダウンリストから、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。
4. 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進めるには、*[次へ]*をクリックし、に進みます[手順2：ボリュームのワークロードを選択する]。

   [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2：ボリュームのワークロードを選択する

Microsoft SQL Server、Microsoft Exchange、ビデオ監視アプリケーション、VMwareなど、特定のアプリケーション用のワークロードを選択してストレージアレイの構成をカスタマイズします。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表示されない場合は、[その他のアプリケーション]を選択します。

タスクの内容

このタスクでは、既存の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。

- 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ることがあります。推奨されるボリューム構成を確認し、[ボリュームの追加/編集]ダイアログボックスを使用して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。
- _"other"_applications (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)を使用してボリュームを作成する場合は'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を作成する場合は、「*既存のワークロード用のボリュームを作成する」オプションを選択します。
   - 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」オプションを選択します。
     - 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ない場合は、いずれかの[その他]エントリを選択します。

     - 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、必要な情報を入力します。関連付けられていない場合は、に進みます。[手順3：ボリュームを追加または編集する]

手順**3**：ボリュームを追加または編集する

選択したアプリケーションまたはワークロードに基づいて、推奨されるボリューム構成がSystem Managerから提示されることがあります。このボリューム構成は、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ています。推奨されるボリューム構成をそのまま使用することも、必要に応じて編集することもできます。「その他」のいずれかのアプリケーションを選択した場合は、作成するボリュームと特性を手動で指定する必要があります。

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。
- 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。
- プールに含めることができるボリュームの最大数は、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（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。

セキュリティ対応のプールまたはボリュームグループの選択

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）。

System Managerでは、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、エラーがあれば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のいずれかのホスト接続でDAがサポートされていない場合、関連付けられているホストは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。

セキュリティ対応のプールまたはボリュームグループの選択

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）。

System Managerでは、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両方のドライブを含めることができますが、暗号化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。

- 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）オプションが設定されたNVMeドライブである必要があります。

タスクの内容

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します。Add/Edit Volumes（ボリュームの追加/編集）ダイアログボックスには、ストレージアレイ上の使用可能なすべてのプールとボリュームグループが表示されます。対応す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。

一部のアプリケーション固有のワークロードについては、対象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く容量が提示され、残りの空き容量（GiB）が表示されます。それ以外のワークロードの場合は、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. [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

フィールドの詳細

フィールド	製品説明
ボリューム名	ボリュームには、作成時にSystem Managerによって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使用する容量の単位（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、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。 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、リモートミラー）用のストレージ容量も必要であるため、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。 プール内の容量は、ドライブタイプに応じて4GiBまたは8GiB単位で割り当てられます。4GiBまたは8GiBの倍数でない容量は割り当てられていますが、使用できません。すべての容量を使用できるようにするには、4GiBまたは8GiB単位で容量を指定します。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	製品説明
セグメントサイズ	セグメントサイジング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。セグメントサイズを変更してパフォーマンスを最適化できます。 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System Managerで判別されます。現在のセグメントサイズからの移行に適していないセグメントサイズは、ドロップダウンリストに表示されません。通常、許容されるトランジションは、現在のセグメントサイズの2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の場合は、16KiBまたは64KiBの新しいボリュームセグメントサイズが許可されます。 • 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（I/Oブロックサイズが16KiB以下など）を処理する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容量ブロックのシーケンシャル処理を処理する場合、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、データは引き続き使用できます。
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に属する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おり、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両方のドライブを含めることができますが、暗号化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。

フィールド	製品説明
DA	• 「 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で発生する可能性があるエラー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、エラーがすべて検出されます。
リソースプロビジョニング（EF300およびEF600のみ）	*はい*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、[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。この機能を使用すると、ボリュームをバックグラウンドの初期化プロセスなしですぐに使用できるようになります。

◦ 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	製品説明
ボリューム名	ボリュームには、作成時にSystem Managerによって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使用する容量の単位（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、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。 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、リモートミラー）用のストレージ容量も必要であるため、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。 プール内の容量は、ドライブタイプに応じて4GiBまたは8GiB単位で割り当てられます。4GiBまたは8GiBの倍数でない容量は割り当てられていますが、使用できません。すべての容量を使用できるようにするには、4GiBまたは8GiB単位で容量を指定します。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	製品説明
セグメントサイズ	セグメントサイジング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。セグメントサイズを変更してパフォーマンスを最適化できます。 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System Managerで判別されます。現在のセグメントサイズからの移行に適していないセグメントサイズは、ドロップダウンリストに表示されません。通常、許容されるトランジションは、現在のセグメントサイズの2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の場合は、16KiBまたは64KiBの新しいボリュームセグメントサイズが許可されます。 • 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（I/Oブロックサイズが16KiB以下など）を処理する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容量ブロックのシーケンシャル処理を処理する場合、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	製品説明
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に属する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両方のドライブを含めることができますが、暗号化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。
DA	• 「 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で発生する可能性があるエラー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、エラーがすべて検出されます。
リソースプロビジョニング（EF300およびEF600のみ）	*はい*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、[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。この機能を使用すると、ボリュームをバックグラウンドの初期化プロセスなしですぐに使用できるようになります。

2. 選択したアプリケーションのボリューム作成手順を進めるには、*[次へ]*をクリックし、に進みます[手順4：ボリュームの構成を確認する]。

手順**4**：ボリュームの構成を確認する

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。[戻る]をクリックして変更を行います。
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。

結果

選択したプールとボリュームグループに新しいボリュームが作成され、All Volumes（すべてのボリューム）テーブルに新しいボリュームが表示されます。

終了後

- 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で必要なオペレーティングシステムの変更を実行します。
- 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が提供）を実行してから、SMcliコマンドを実行し `-identifyDevices`てボリューム名をホストストレージアレイ名に関連付けます。

  SMcliは、SANtricityシステムマネージャから直接使用できます。SMcliのダウンロード版は、EF600、EF300、E5700、EF570、E2800、EF280の各コントローラで使用できます。SANtricity システムマネージャからSMcliをダウンロードするには、* Settings > System * and * Add-ons > Command Line Interface * を選択します。

ワークロードへのボリュームの追加

現在ワークロードに関連付けられていないボリュームについては、既存または新規のワークロードに1つ以上のボリュームを追加できます。

タスクの内容

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）されたボリュームは、ワークロードに関連付けられません。

手順

1. 選択メニュー： Storage [Volumes]
2. [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。

3. 「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。

4. 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。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、このワークロードに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。
5. 「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]ダイアログボックスが表示されます。

6. ワークロードに追加するボリュームを選択します。
7. 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。
8. 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。

ボリュームの管理

ボリュームの容量の拡張

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。

開始する前に

- 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ある。
- ボリュームが最適な状態であり、変更中の状態ではありません。
- シンボリュームの最大レポート容量である256TiBに達していません。
- ボリュームでホットスペアドライブが使用されていません。（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）。

ボリューム容量は一度に最大128TiBまで拡張できます。

タスクの内容

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対する今後の容量要件に注意してください。Snapshotイメージ、Snapshotボリューム、またはリモートミラーを作成するための十分な空き容量を確保してください。

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ます。サポート対象外のホストオペレーティングシステム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はできません。

手順

1. 選択メニュー： Storage [Volumes]
2. 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。

3. 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で使用可能な空き容量が表示されます。

4. 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）、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。

5. [* 拡大（ * ）] をクリックします

結果

- System Managerは、選択に基づいてボリュームの容量を拡張します。
- メニューを選択します。Home [View Operations in Progress]は、選択したボリュームで現在実行中の容量増加処理の進捗状況を表示します。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。

終了後

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。

ボリュームの初期化

ボリュームは、最初に作成された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。このオプションは、必ずテクニカルサポートから指示があった場合に使用してください。初期化するボリュームは1つ以上選択できます。

開始する前に

- すべてのI/O処理が停止されている。
- 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。
- ボリュームのステータスが最適であり、ボリュームで実行中の変更処理はありません。

この処理は開始後に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で指示された場合を除き、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。

タスクの内容

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、割り当て容量、およびリザーブ容量の設定は維持されます。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

このトピックは、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. 選択メニュー： Storage [Volumes]
2. 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]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すべてのボリュームがこのダイアログボックスに表示されます。

3. 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

System Manager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をクリアします。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見えます）。

メニューを選択します。Home [View Operations in Progress]は、選択したボリュームに対して現在実行中の初期化処理の進捗状況を表示します。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。

ボリュームの再配置

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で問題が発生すると、マルチパスドライバによって優先コントローラ所有者からボリュームが移動されます。

開始する前に

- 再配置するボリュームが使用中でない場合、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ないと、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、再配置処理の実行中に_VOLUMESへの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。

タスクの内容

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った場合は、ホストのマルチパスドライバが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. 選択メニュー： Storage [Volumes]
2. 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。

3. 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

System Managerによって、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の変更

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。

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パスが変更されたときにアプリケーションエラーが発生するのを防ぐことができます。

タスクの内容

プールまたはボリュームグループ内の1つ以上のボリュームのコントローラ所有権を変更できます。

手順

1. 選択メニュー： Storage [Volumes]
2. 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。ストレージアレイ上のすべてのボリュームがこのダイアログボックスに表示されます。

3. [* 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

- System Managerによってボリュームのコントローラ所有権が変更されます。これで、ボリュームへのI/OがこのI/Oパス経由で転送されます。
- 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ことがあります。この操作は通常5分未満で完了します。

ボリュームの削除

ボリュームを削除する一般的な状況としては、作成したボリュームのパラメータや容量に誤りがあった場合、ストレージ構成のニーズを満たさなくなった場合、バックアップやアプリケーションのテストに必要なくなったSnapshotイメージがある場合などがあります。

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。削除するボリュームを1つ以上選択できます。

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。

タスクの内容

次のいずれかの条件のボリュームは削除できません。

- 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」の場合を除き、ボリュームで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のソースボリュームまたはターゲットボリュームで、ステータスが「保留」、「実行中」、「失敗」のいずれかです。

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。

ボリュームのサイズが一定（現在は128TB）を超えた場合、削除はバックグラウンドで実行されており、解放されたスペースをすぐに使用できるとは限りません。

手順

1. 選択メニュー： Storage [Volumes]
2. [削除（ Delete ）] をクリックします。

   [Delete Volumes]ダイアログボックスが表示されます。

3. 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。
4. [削除（ Delete ）] をクリックします。

結果

System Managerは次の処理を実行します。

- 関連付けられているSnapshotイメージ、スケジュール、およびSnapshotボリュームを削除します。
- ミラーリング関係を削除します。
- プールまたはボリュームグループの空き容量を増やします。

シンボリュームの割り当て容量制限の変更

オンデマンドでスペースを割り当てることができるシンボリュームでは、シンボリュームを自動的に拡張できる割り当て容量の制限を変更できます。

シンボリュームが割り当て容量の制限に近づいたときに[ホーム]ページの[通知]領域にアラート（警告しきい値の超過）が送信される割合を変更することもできます。このアラート通知を有効にするか無効にするかを選択できます。

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。

割り当て容量は、割り当て容量の制限に基づいて自動的に拡張されます。割り当て容量の制限を使用すると、シンボリュームの自動拡張をレポート容量未満に制限できます。書き込まれるデータの量が割り当て容量に近付いたときは、割り当て容量の制限を変更することができます。

シンボリュームの割り当て容量の制限と警告しきい値を変更する場合は、ボリュームのユーザデータとコピーサービスデータの両方で消費されるスペースを考慮する必要があります。

手順

1. 選択メニュー： Storage [Volumes]
2. [* Thin Volume Monitoring]タブを選択します。

   シンボリュームの監視ビューが表示されます。

3. 変更するシンボリュームを選択し、*制限の変更*を選択します。

   [制限の変更]ダイアログボックスが表示されます。選択したシンボリュームの割り当て容量の制限と警告しきい値の設定がこのダイアログボックスに表示されます。

4. 割り当て容量の制限と警告しきい値を必要に応じて変更します。

   フィールドの詳細

設定	製品説明
割り当て容量の制限を変更…	書き込みが失敗し、シンボリュームが追加のリソースを消費しないようにするしきい値。このしきい値は、ボリュームのレポート容量サイズの割合です。
アラートを受け取るタイミング…（警告しきい値）	シンボリュームが割り当て容量の制限に近づいたときにシステムでアラートを生成する場合は、このチェックボックスを選択します。アラートが[ホーム]ページの[通知]領域に送信されます。このしきい値は、ボリュームのレポート容量サイズの割合です。 警告しきい値のアラート通知を無効にするには、このチェックボックスをオフにします。

5. [保存（ Save ）] をクリックします。

設定の管理

ボリュームの設定の変更

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。

開始する前に

変更するボリュームのステータスは「最適」である必要があります。

ボリューム設定の変更の実行中は、一部の処理を使用できない可能性があります

手順

1. 選択メニュー： Storage [Volumes]
2. 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]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。

3. 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	製品説明
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。 レポート容量と割り当て容量はシックボリュームでは同じですが、シンボリュームでは異なります。シックボリュームの場合、物理的に割り当てられたスペースは、ホストに報告されるスペースと同じになります。シンボリュームの場合、レポート容量はホストに報告される容量であり、割り当て容量はデータの書き込み用に現在割り当てられているドライブスペースの量です。
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、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の形式で容量としてホストに提示されます。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を異なるホストで使用して、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、ストレージアレイ内の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に対する一意の識別子で、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。

設定	製品説明
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）*-ボリュームの一意な16進数の識別子。 • * Extended Unique Identifier（EUI）*--ボリュームの識別子EUI-64。 • 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識別子。

4. 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	製品説明
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。
サービス品質の設定	• 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を無効にすると、このボリュームで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。この機能が有効になっているボリュームでは、コントローラファームウェアでデータの整合性が確保されていないと判断されると、読み取りエラーが返されます。
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。コントローラは、I/O全体でできるだけバランスよく配置する必要があります。

設定	製品説明
セグメントサイジング	セグメントサイジング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。セグメントサイズを変更してパフォーマンスを最適化できます。 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System Managerで判別されます。現在のセグメントサイズからの移行に適していないセグメントサイズは、ドロップダウンリストに表示されません。通常、許容されるトランジションは、現在のセグメントサイズの2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の場合は、16KiBまたは64KiBの新しいボリュームセグメントサイズが許可されます。 • 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（I/Oブロックサイズが16KiB以下など）を処理する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容量ブロックのシーケンシャル処理を処理する場合、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	修正の優先度に関する設定が表示されます。この設定は、ボリュームグループ内のボリュームに対してのみ表示されます。 変更の優先度は、ボリューム変更処理に割り当てる処理時間を、システムパフォーマンスに対する相対的な割合で定義します。変更の優先度を上げることができますが、システムパフォーマンスに影響する可能性があります。 スライダバーを移動して優先度レベルを選択します。 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変更処理には影響しますが、システムパフォーマンスが低下する可能性があります。

設定	製品説明
キャッシュ	キャッシュ設定が表示されます。キャッシュ設定は、ボリュームの全体的なI/Oパフォーマンスに影響するように変更できます。
SSD キャッシュ	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。ドライブセキュリティとData Assuranceの設定が同じボリュームは互換性があります。 • 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の読み取り時間が短縮されるため、アプリケーションの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。

5. [保存（ Save ）] をクリックします。

   選択内容に基づいて、System Managerがボリュームの設定を変更します。

終了後

選択したボリュームで現在実行されている変更処理の進捗状況を表示するには、[MENU]：[View Operations in Progress]を選択します。

ワークロード設定の変更

ワークロードの名前を変更して、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。現在の名前が適切でない場合はワークロードの名前を変更します。

手順

1. 選択メニュー： Storage [Volumes]
2. [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。

3. 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。

4. *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。
5. [保存（ Save ）] をクリックします。

ボリュームのキャッシュ設定の変更

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

パフォーマンスに影響を与えることができます。

タスクの内容

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あと、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、新しいバッテリの充電中、コントローラが取り外された場合、またはコントローラでキャッシュサイズの不一致が検出された場合に発生することがあります。条件がクリアされると、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、1つ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。すべての標準ボリュームまたはすべてのシンボリュームのキャッシュ設定を同時に変更できます。

手順

1. 選択メニュー： Storage [Volumes]
2. 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。ストレージアレイ上のすべてのボリュームがこのダイアログボックスに表示されます。

3. [**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	製品説明
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。データは、ドライブに書き込まれるまで書き込みキャッシュに残ります。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、ボリュームに対して*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。

4. 「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。詳細な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

キャッシュ設定	製品説明
動的キャッシュ読み取りプリフェッチ	動的キャッシュ読み取りプリフェッチでは、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することができます。このキャッシュにより、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。ランダムアクセスでは、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。 動的キャッシュ読み取りプリフェッチはシンボリュームに対しては常に無効で、変更することはできません。
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設定すると、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継続されます。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。 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*バッテリなしの書き込みキャッシュ*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。 この設定は、書き込みキャッシュを有効にしている場合にのみ使用できます。この設定はシンボリュームに対しては使用できません。
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る場合に発生します。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。 この設定は、書き込みキャッシュを有効にしている場合にのみ使用できます。この設定はシンボリュームに対しては使用できません。

5. [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の変更

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。

開始する前に

次の点を理解してください。

- 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、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。そのボリュームに対して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がある場合は、ボリューム内の冗長性情報がデータとの整合性がチェックされます。メディアスキャンと冗長性チェックは、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は、冗長性情報を使用してデータが修復されます（使用可能な場合）。

  たとえば、冗長性情報は、最適なRAID 5ボリューム、最適なRAID 6ボリューム、または1つのドライブだけで障害が発生したRAID 6ボリュームで確認できます。冗長性情報を使用してリカバリ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の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ると、イベントログに報告されます。

タスクの内容

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た場合にデータが失われることがあります。これは、障害が発生した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です。

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する
- ストレージアレイ全体のスキャン期間を変更する
- 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する
- 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する

手順

1. 選択メニュー： Storage [Volumes]
2. 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]。

   [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。ストレージアレイ上のすべてのボリュームがこのダイアログボックスに表示されます。

3. 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。

メディアスキャンのチェックボックスを無効にすると、すべてのメディアスキャン設定が一時停止されます。

4. メディアスキャンを実行する日数を指定します。
5. 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。

   System Managerでは、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。

6. [保存（ Save ）] をクリックします。

   選択内容に基づいて、System Managerで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。

コピーサービスの使用

ボリュームコピーの概要

ボリュームコピー機能を使用すると、ソースボリュームとターゲットボリュームという2つのボリュームを同じストレージアレイに作成して、ボリュームのポイントインタイムコピーを作成できます。

ソースボリュームからターゲットボリュームへの1バイトずつコピーが実行され、ターゲットボリュームのデータがソースボリュームのデータと同一になります。

データコピーによるアクセスの向上

ボリュームのストレージ要件の変化に応じて、ボリュームコピー機能を使用して、小容量のドライブを使用するプールまたはボリュームグループから大容量のドライブを使用するプールまたはボリュームグループにデータをコピーできます。たとえば、ボリュームコピー機能を使用して次の処理を実行できます。

- 大容量ドライブにデータを移動
- データ転送速度の高いドライブに変更します。
- パフォーマンスを向上させるために、新しいテクノロジを使用するドライブに変更してください。
- シンボリュームをシックボリュームに変更します。

コピーのソースボリュームとターゲットボリュームで、報告されるホストアドレス指定可能/論理ブロックサイズ（セクターサイズ）が同じである必要があります。

報告されるボリュームのブロックサイズは次のとおりです。

- ネイティブブロックサイズ–ボリュームのブロックサイズは、ドライブのブロックサイズ（512または4K）と同じです。
- エミュレートされた**512**ブロックサイズ-ドライブは4Kですが、報告されるブロックサイズは512です。

シンボリュームからシックボリュームへの変更

シンボリュームをシックボリュームに変更する場合は、ボリュームコピー処理を使用してシンボリュームのコ

ピーを作成します。ボリュームコピー処理のターゲットは常にシックボリュームです。

> System Manager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。シンボリュームを作成する場合は、コマンドラインインターフェイス（CLI）を使用します。

バックアップデータ

ボリュームコピー機能を使用すると、ボリュームのデータを同じストレージアレイ上の別のボリュームにコピーしてボリュームをバックアップできます。ターゲットボリュームは、ソースボリュームのバックアップ、システムのテスト、またはテープドライブなどの別のデバイスへのバックアップとして使用できます。

Snapshotボリュームのデータをベースボリュームにリストア

ベースボリュームに関連付けられているSnapshotボリュームからデータをリストアする必要がある場合は、ボリュームコピー機能を使用してSnapshotボリュームからベースボリュームにデータをコピーできます。Snapshotボリューム上のデータのボリュームコピーを作成し、そのデータをベースボリュームにコピーできます。

ソースボリュームとターゲットボリューム

次の表に、ボリュームコピー機能でソースボリュームとターゲットボリュームに使用できるボリュームのタイプを示します。

ボリュームタイプ	オフラインボリュームコピーのソースボリュームを指定します	オンラインボリュームコピーのソースボリューム	オンラインおよびオフラインのターゲットボリューム
プール内のシックボリューム	はい	はい	はい
ボリュームグループ内のシックボリューム	はい	はい	はい
シンボリューム	はい^1です	はい	いいえ
Snapshotボリューム	はい[2]	いいえ	いいえ
Snapshotベースボリューム	はい	はい	いいえ
リモートミラープライマリボリューム	はい[3]	はい	いいえ

[1]ターゲットボリュームの容量はシンボリュームのレポート容量以上である必要があります。

[2]オンラインコピー処理が完了するまでは、Snapshotボリュームコピーを使用できません。

[3]ソースボリュームがプライマリボリュームの場合、ターゲットボリュームの容量はソースボリュームの使用可能容量以上である必要があります。

オフラインの_ボリュームコピー操作または_オンラインの_ボリュームコピー操作のいずれかを実行できます。オフライン処理では、ソースボリュームからデータを読み取り、ターゲットボリュームにコピーします。オンライン処理では、Snapshotボリュームをソースとして使用し、そのデータをターゲットボリュームにコピーします。

データの整合性を確保するために、どちらのタイプのボリュームコピー処理でも、ターゲットボリュームに対するすべてのI/Oアクティビティが中断されます。この一時停止は、手順が完了するまでターゲットボリューム上のデータの状態が不整合であるために発生します。

以下に、オフラインとオンラインのボリュームコピー処理について説明します。

オフラインノボリュームコヒイシヨリ

オフラインのボリュームコピー関係は、ソースボリュームとターゲットボリュームの間の関係です。オフラインコピーでは、ソースボリュームからデータを読み取り、ターゲットボリュームにコピーします。コピーの実行中は、ソースボリュームに対するすべての更新が一時停止されます。ソースボリュームに対するすべての更新は、時間的な不整合がターゲットボリュームで作成されるのを防ぐために中断されます。

オフラインコピー処理に関する重要なポイント	
読み取り要求と書き込み要求	• ボリュームコピー処理のステータスが実行中または保留の間は、オフラインコピーに参加しているソースボリュームを読み取り専用のI/Oアクティビティに使用できます。 • 書き込み要求はオフラインコピーの完了後に許可されます。 • 書き込み禁止のエラーメッセージが表示されないようにするには、ステータスが実行中のボリュームコピー処理に参加しているソースボリュームにはアクセスしないでください。
ジャーナリングファイルシステム	• ソースボリュームがジャーナリングファイルシステムでフォーマットされている場合、ソースボリュームに対する読み取り要求を発行しようとすると、ストレージアレイコントローラによって拒否され、エラーメッセージが表示されることがあります。 • ジャーナリングファイルシステムドライバは、読み取り要求の発行を試行する前に書き込み要求を発行します。コントローラは書き込み要求を拒否します。書き込み要求が拒否されたために、読み取り要求が発行されない可能性があります。その場合、ソースボリュームが書き込み禁止になっていることを示すエラーメッセージが表示されることがあります。 • この問題が発生しないようにするには、ボリュームコピー処理のステータスが実行中である間は、オフラインコピーに参加しているソースボリュームにはアクセスしないでください。

オンラインのボリュームコピー処理

オンラインのボリュームコピー関係は、Snapshotボリュームとターゲットボリュームの間の関係です。ソースボリュームがオンラインでデータの書き込みに使用できる状態で、ボリュームコピー処理を開始できます。この機能は、ボリュームのSnapshotを作成し、そのSnapshotをコピーの実際のソースボリュームとして使用することで実現されます。

ソースボリュームに対してボリュームコピー処理を開始すると、System Managerはベースボリュームのスナップショットイメージおよびベースボリュームとターゲットボリュームのスナップショットイメージ間のコピー関係を作成します。スナップショットイメージをソースボリュームとして使用すると、ストレージアレイはコピーの実行中もソースボリュームへの書き込みを継続できます。

オンラインコピー処理では、copy-on-write手順が原因でパフォーマンスが低下します。オンラインコピーが完了すると、ベースボリュームのパフォーマンスが元に戻ります。

オンラインコピー処理に関する重要なポイント	
どのような種類のボリュームを使用できますか？	• ポイントインタイムイメージの作成対象となるボリュームはベースボリュームと呼ばれ、ストレージアレイ上の標準ボリュームまたはシンボリュームである必要があります。 • ターゲットボリュームは、ボリュームグループ内の標準ボリュームまたはプール内の標準ボリュームです。ターゲットボリュームをシンボリュームやスナップショットグループ内のベースボリュームにすることはできません。 • オンラインのボリュームコピー機能を使用して、シンボリュームから同じストレージアレイ内のプール内の標準ボリュームにデータをコピーできます。ただし、ボリュームコピー機能を使用して標準ボリュームからシンボリュームにデータをコピーすることはできません。
ベースボリュームのパフォーマンス	• コピーソースとして使用されるスナップショットボリュームがアクティブな場合は、copy-on-write処理が原因でベースボリュームのパフォーマンスが低下します。コピーが完了すると、スナップショットは無効になり、ベースボリュームのパフォーマンスがリストアされます。スナップショットは無効ですが、リザーブ容量ボリュームとコピー関係はそのまま残ります。
作成されるボリュームのタイプ	• スナップショットボリュームとリザーブ容量ボリュームは、オンラインコピー処理中に作成されます。 • スナップショットボリュームは、データを格納する実際のボリュームではなく、特定の時点でボリュームに格納されていたデータへの参照です。 • 作成されるスナップショットごとに、そのスナップショットのデータを保持するためのリザーブ容量ボリュームが作成されます。リザーブ容量ボリュームは、スナップショットイメージの管理にのみ使用されます。
リザーブ容量ボリューム	• ソースボリューム上のデータブロックが変更される前に、変更対象のブロックの内容が保護用のリザーブ容量ボリュームにコピーされます。 • リザーブ容量ボリュームには元のデータブロックのコピーが格納されるため、これらのデータブロックに対する以降の変更はソースボリュームにのみ書き込まれます。 • リザーブ容量ボリュームに格納されるのはスナップショットの作成後に変更されたデータブロックだけであるため、オンラインコピー処理で使用されるディスクスペースは完全な物理コピーよりも少なくなります。

ボリュームコピー

1つのボリュームから同じストレージアレイ内の別のボリュームにデータをコピーし、ソ

ースボリュームのポイントインタイムの物理的な複製（クローン）を作成できます。

開始する前に

- ソースボリュームとターゲットボリュームに対するすべてのI/Oアクティビティを停止する必要があります。
- ソースボリュームとターゲットボリュームのすべて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。
- ターゲットボリュームを以前にボリュームコピー処理で使用したことがある場合は、そのデータが不要になるか、データをバックアップしておく必要があります。

タスクの内容

ソースボリュームは、ホストI/Oを受け入れてアプリケーションデータを格納するボリュームです。ボリュームコピーを開始すると、ソースボリュームのデータ全体がターゲットボリュームにコピーされます。

ターゲットボリュームは、ソースボリュームのデータのコピーを保持する標準ボリュームです。ボリュームコピー処理の完了後、ターゲットボリュームはソースボリュームと同じになります。ターゲットボリュームの容量はソースボリュームと同じかそれ以上である必要がありますが、RAIDレベルは異なる場合があります。

オンラインコピーとオフラインコピーの詳細

オンラインコピー

オンラインコピーでは、ストレージアレイ内の任意のボリュームのポイントインタイムコピーが作成されますが、コピーの実行中もボリュームへの書き込みは可能です。この機能は、ボリュームのSnapshotを作成し、そのSnapshotをコピーの実際のソースボリュームとして使用することで実現されます。ポイントインタイムイメージの作成対象となるボリュームはベースボリュームと呼ばれ、ストレージアレイ内の標準ボリュームまたはシンボリュームを使用できます。

オフラインコピー

オフラインコピーでは、ソースボリュームからデータを読み取り、ターゲットボリュームにコピーします。コピーの実行中は、ソースボリュームに対するすべての更新が一時停止されます。ソースボリュームに対するすべての更新は、時間的な不整合がターゲットボリュームで作成されるのを防ぐために中断されます。オフラインボリュームコピー関係は、ソースボリュームとターゲットボリュームの間の関係です。

ボリュームコピー処理では、ターゲットボリュームのデータが上書きされ、ターゲットボリュームに関連付けられているSnapshotボリュームがある場合はすべて使用停止になります。

手順

1. 選択メニュー： Storage [Volumes]
2. ボリュームコピー処理のソースとして使用するボリュームを選択し、メニューからコピーサービス[Copy Volume]を選択します。

   Copy Volume - Select Target（ボリュームのコピー-ターゲットの選択）ダイアログボックスが表示されます。

3. データのコピー先となるターゲットボリュームを選択します。

このダイアログボックスの表には、対応するターゲットボリュームがすべて表示されます。

4. スライダバーを使用して、ボリュームコピー処理のコピー優先度を設定します。

   コピー優先度は、I/O要求の処理と比較して、ボリュームコピー処理を完了するために使用されるシステムリソースの量を決定します。

   コピー優先度について

   コピー優先度は5段階で設定できます。

   - 最低
   - 低
   - 中
   - 高
   - 最高

   [最低]に設定すると、I/Oアクティビティが優先され、ボリュームコピー処理にかかる時間が長くなります。[最高]に設定すると、ボリュームコピー処理が優先されますが、ストレージアレイのI/Oアクティビティに影響する可能性があります。

5. オンラインコピーとオフラインコピーのどちらを作成するかを選択します。オンライン・コピーを作成するには'[コピー・オペレーション中にソース・ボリュームをオンラインにしておく]チェック・ボックスを選択します

6. 次のいずれかを実行します。

   - online_copy操作を実行するには、* Next をクリックして、 Reserve Capacity *ダイアログボックスに進みます。
   - _offline_copy操作を実行するには'[終了]をクリックしてオフライン・コピーを開始します

7. オンラインコピーの作成を選択した場合は、オンラインコピーのデータおよびその他の情報を保存するために必要なリザーブ容量を設定し、[**Finish**]をクリックしてオンラインコピーを開始します。

   [ボリューム候補]の表には、指定したリザーブ容量をサポートする候補のみが表示されます。リザーブ容量は、コピーサービス処理やストレージオブジェクトに使用される物理割り当て容量です。ホストから直接読み取ることはできません。

   次のガイドラインに従ってリザーブ容量を割り当てます。

   - リザーブ容量のデフォルト設定はベースボリュームの容量の40%で、通常はこの容量で十分です。
   - ただし、リザーブ容量は元のデータに対する変更の回数によって異なります。ストレージオブジェクトがアクティブになっている時間が長いほど、リザーブ容量を大きくする必要があります。

結果

System Managerにより、ソースボリュームのすべてのデータがターゲットボリュームにコピーされます。ボリュームコピー処理が完了すると、ターゲットボリュームは自動的にホストに対して読み取り専用になります。

終了後

メニューHome（ホーム）[View Operations in Progress]（進行中の操作の表示）を選択して、ボリュームコピー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。

ボリュームコピー処理に対する操作の実行

実行中のボリュームコピー処理の表示、ボリュームコピー処理の停止、優先度の変更、再コピー、クリアを行うことができます。

手順

1. メニューを選択します。ホーム[進行中の操作を表示]。

   [処理を実行中]ダイアログボックスが表示されます。

2. 処理を実行するボリュームコピー処理を探し、* Actions *列のリンクをクリックして、次のいずれかの操作を実行します。

   特に、処理を停止する場合は、ダイアログ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。

アクション	製品説明
停止	ステータスが実行中、保留、または失敗のボリュームコピー処理を停止できます。 ボリュームコピーが停止すると、マッピングされているすべてのホストがソースボリュームに書き込みアクセスできるようになります。ソースボリュームにデータが書き込まれると、ターゲットボリュームのデータはソースボリュームのデータと一致しなくなります。
優先度の変更	ステータスが実行中であるボリュームコピー処理の優先度を変更して、ボリュームコピー処理が完了する速度を選択できます。
再コピー	停止したボリュームコピー処理を再開する場合や、ボリュームコピー処理が失敗または停止した場合に、ボリュームを再コピーできます。ボリュームコピー処理が最初から開始されます。 再コピー操作では、ターゲットボリュームの既存のデータが上書きされ、ターゲットボリュームに関連付けられているSnapshotボリュームがある場合はすべて使用停止になります。
クリア	ステータスが実行中、保留、または失敗のボリュームコピー処理を削除できます。 この操作は必ず、「クリア」を選択する前に実行してください。確認ダイアログは表示されません。

FAQ

ボリュームとは何ですか？

ボリュームは、アプリケーション、データベース、およびファイルシステムがデータを格納するコンテナです。ホストがストレージアレイのストレージにアクセスするために作成される論理コンポーネントです。

ボリュームは、プールまたはボリュームグループの使用可能な容量から作成します。ボリュームごとに容量が定義されています。ボリュームは複数のドライブで構成される場合もありますが、ホストでは1つの論理コンポーネントとして認識されます。

ボリュームグループにボリュームの作成に十分な空き容量があると、容量の過剰割り当てエラーが表示されるのはなぜですか？

選択したボリュームグループには1つ以上の空き容量領域がある可能性があります。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に制限されます。たとえば、ボリュームグループの合計空き容量が15GiBで、最も大きい空き容量領域が10GiBの場合、作成できるボリュームの最大サイズは10GiBです。

ボリュームグループに空き容量領域がある場合は、ボリュームグループのグラフに、既存の空き容量領域の数を示すリンクが表示されます。リンクを選択すると、各領域の容量を示すポップアップが表示されます。

空き容量を統合することで、ボリュームグループ内の空き容量を最大限に増やして追加ボリュームを作成できます。次のいずれかの方法を使用して、選択したボリュームグループの既存の空き容量を統合できます。

- ボリュームグループで少なくとも1つの空き容量領域が検出されると、[ホーム]ページの[通知]領域に「空き容量の統合」という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。
- メニューから[プールとボリュームグループ[一般的でないタスク]>[ボリュームグループの空き容量の統合]を選択して、ダイアログボックスを起動することもできます。

最大の空き容量領域ではなく特定の空き容量領域を使用する場合は、コマンドラインインターフェイス（CLI）を使用してください。

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？

ボリュームの作成時に、ワークロードの用途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ボリュームの最適な構成が作成され、必要に応じて編集することもできます。必要に応じて、ボリューム作成のこの手順を省略できます。

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（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、読み取りキャッシュと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™
- Microsoft®Exchange Server™
- ビデオ監視アプリケーション
- VMware ESXi™（仮想マシンファイルシステムで使用するボリューム用）

推奨されるボリューム構成を確認し、[ボリュームの追加/編集]ダイアログボックスを使用して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。

- 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？

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）されたボリュームは、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どのように対話するかを決定し、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のことです。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。

この情報はストレージの作成にどのように役立ちますか？

ワークロード情報は、選択したワークロードのI/Oタイプ、セグメントサイズ、読み取り/書き込みキャッシュなどのボリューム特性を最適化するために使用されます。最適化された特性によって、ワークロードとストレージアレイコンポーネントの連携方法が決まります。

指定したワークロード情報に基づいて、System Managerによって適切なボリュームが作成され、システム上の現在の使用可能なプールまたはボリュームグループに配置されます。選択したワークロードの最新のベストプラクティスに基づいて、ボリュームが作成され、その特性が最適化されます。

特定のワークロード用のボリュームの作成が完了する前に、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。

ベストプラクティスの情報については、アプリケーション固有のドキュメントを参照してください。

拡張された容量を認識するには、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が認識され、ボリューム拡張の開始後に自動的に拡張されます。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。

プールやボリュームグループが一部表示されないのはなぜですか？

ボリュームの移動先として指定できないプールまたはボリュームグループはリストに表示されません。

プールまたはボリュームグループを使用できない理由は次のとおりです。

- プールまたはボリュームグループのData Assurance（DA）機能が一致しません。
- プールまたはボリュームグループの状態が最適でない。
- プールまたはボリュームグループの容量が小さすぎます。

セグメントサイズとは何ですか？

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にのみ適用され、プールには適用されません。

セグメントサイズは、セグメントに含まれるデータブロックの数で定義されます。セグメントサイズを決定するときは、ボリュームに格納するデータのタイプを把握しておく必要があります。アプリケーションが一般にスモールランダムリードとスモールランダムライト（IOPS）を使用する場合は、一般に小さいセグメントサイズが適しています。また、アプリケーションが大容量のシーケンシャルリード/ライト（スループット）を実行している場合は、一般に大きなセグメントサイズの方が適しています。

アプリケーションがスモールランダムリード/ライトを使用する場合でも、ラージシーケンシャルリード/ライトを使用する場合でも、セグメントサイズが一般的なデータブロックのチャンクサイズよりも大きいと、ストレージアレイのパフォーマンスが向上します。これにより、ドライブからのデータへのアクセスがより簡単か

つ高速になります。これは、ストレージアレイのパフォーマンスを向上させるために重要です。

IOPSパフォーマンスが重視される環境

IOPS（1秒あたりのI/O処理数）環境では、ドライブに対して読み書きされる標準的なデータブロックサイズ（「チャンク」）よりもセグメントサイズを大きくすると、ストレージアレイのパフォーマンスが向上します。こうすることで、各チャンクが確実に1つのドライブに書き込まれます。

スループットが重視される環境

スループット環境では、セグメントサイズは、データ用ドライブの総数および一般的なデータチャンクサイズ（I/Oサイズ）の偶数になります。これにより、データが単一のストライプとしてボリュームグループ内のドライブに分散されるため、読み取りと書き込みが高速になります。

優先コントローラ所有権とは何ですか？

優先コントローラ所有権は、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。コントローラは、I/O全体でできるだけバランスよく配置する必要があります。

たとえば、一方のコントローラが主に大容量のシーケンシャルデータブロックを読み取り、もう一方のコントローラが小さいデータブロックを頻繁に読み書きする場合、負荷は大きく異なります。どのボリュームにどのタイプのデータが含まれているかを把握しておくと、両方のコントローラでI/O転送を均等に分散できます。

[ホストをあとで割り当てる**]**オプションはどのような場合に使用しますか？

ボリュームの作成にかかる時間を短縮するには、ホストの割り当て手順を省略して、新しく作成したボリュームをオフラインで初期化します。

新しく作成した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、そのグループ内の初期化中のボリュームは強制的にバックグラウンド初期化に移行されます。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にマッピングされているボリュームがない場合は、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。

ホストの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およびEF600システムでは、ボリュームのブロックサイズ（「セクターサイズ」とも呼ばれます）を512バイトまたは4KiBに設定できます。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。可能な場合は、適切なデフォルト値が提示されます。

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および仮想マシン（現時点ではVMwareなど）では512バイトのブロックサイズが必要であり、4KiBをサポートしていないため、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実現するには、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。

- サポートされるボリュームのブロックサイズは、次のように、プールまたはボリュームグループに対して選択するドライブのタイプによっても決まります。
  - 512バイトの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、512バイトのブロックを含むボリュームのみを作成できます。
  - 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バイトブロックまたは4KiBブロックのボリュームを作成できます。
- 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、ボリュームグループのブロックサイズに関係なく、すべてのボリュームのブロック数が512バイトに制限されます。これは、特定のハードウェアの実装によるものです。
- 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。

ホストとホストクラスタ

ホストおよびホストクラスタの概要

ホストとホストクラスタを設定して、ストレージアレイとデータサーバの間の接続を定義できます。

ホストとホストクラスタとは

a_host_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。a_host cluster_は ホストのグループであり、複数のホストに同じボリュームを割り当てるために作成できます。

詳細：

- "ホストの用語"
- "アクセスホリユウム"
- "LUNの最大数"

ホストとホストクラスタを設定するにはどうすればよいですか？

ホスト接続を定義するには、メニュー[ストレージ][ホスト]に移動してホストを手動で設定します。複数のホストで同じボリュームセットへのアクセスを共有する場合は、クラスタを定義してそのクラスタにボリュームを割り当てることができます。

詳細：

- "ホストの手動作成"
- "ホストおよびホストクラスタへのボリュームの割り当て方法"
- "ホストの作成とボリュームの割り当てのワークフロー"
- "ホストの手動作成"
- "ホストクラスタの作成"

- "ホストへのボリュームの割り当て"

関連情報

ホストに関連するタスクの詳細については、以下を参照してください。

- "自動ロードバランシングの設定"
- "ホスト接続レポートの設定"
- "デフォルトのホストタイプの変更"

概念

ホストの用語

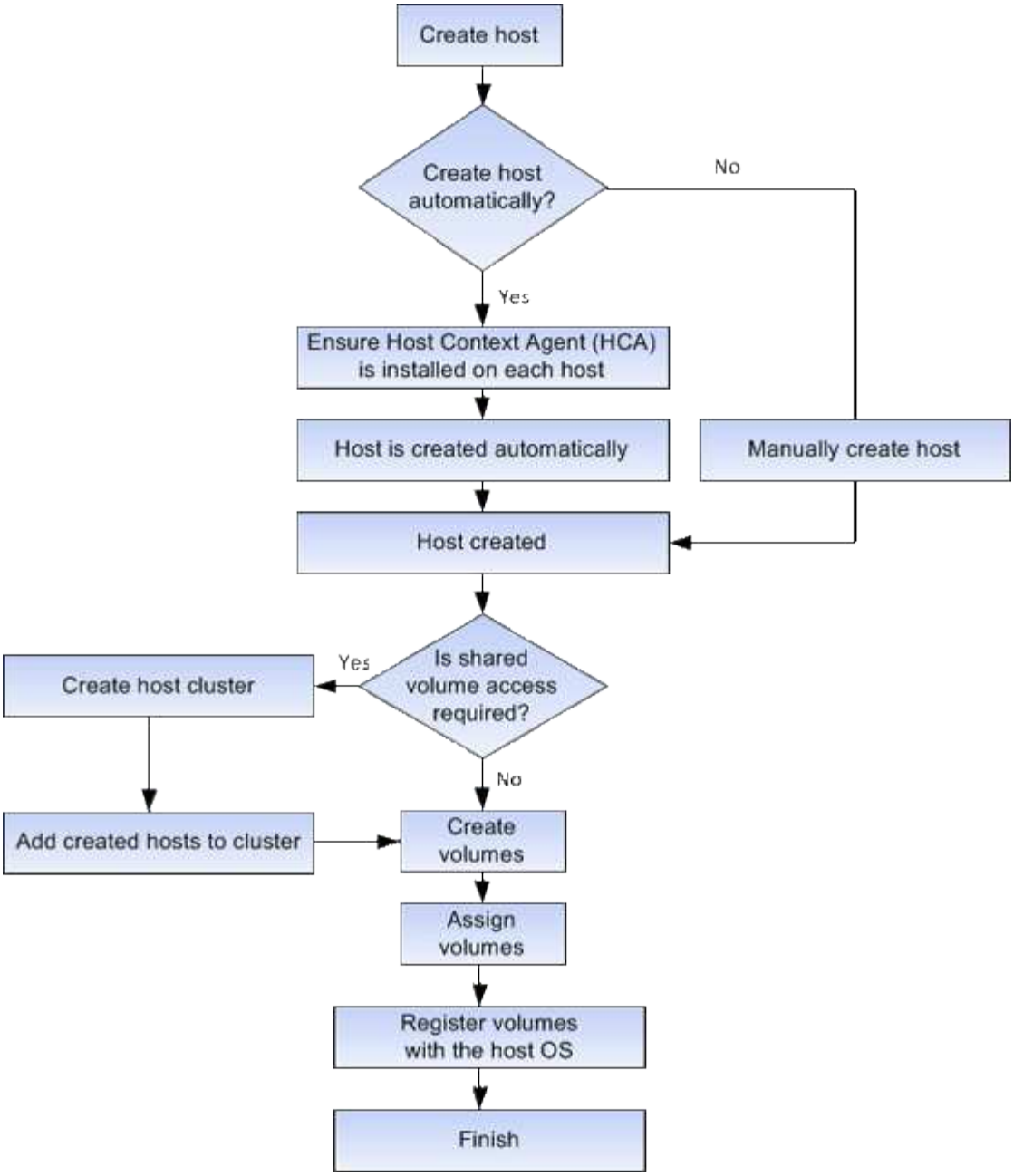
ストレージアレイに関連するホストの用語を次に示します。

コンポーネント	定義
ホスト	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。
ホスト名	ホスト名は、ホストのシステム名に相当します。
ホストクラスタ	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。
ホストインターフェイスプロトコル	ホストインターフェイスプロトコルは、コントローラとホストの間の接続（Fibre ChannelやiSCSIなど）です。
HBAまたはネットワークインターフェイスカード（NIC）	ホストバスアダプタ（HBA）はホストに搭載されるボードで、1つ以上のホストポートが搭載されています。
ホストポート	ホストポートは、コントローラに物理的に接続されるホストバスアダプタ（HBA）のポートで、I/O処理に使用されます。
ホストポート識別子	ホストポート識別子は、ホストバスアダプタ（HBA）上の各ホストポートに関連付けられた一意のワールドワイド名です。 • Internet Small Computer System Interface（iSCSI）ホストポート識別子は、1 ~ 233文字で指定する必要があります。iSCSIホストポート識別子は、標準のIQN形式（など）で表示されます。 `iqn.xxx.com.xxx:8b3ad` • Fibre ChannelやSerial Attached SCSI（SAS；シリアル接続SCSI）など、iSCSI以外のホストポート識別子は、2文字ごとにコロンで区切って表示されます（など） `xx:yy:zz`。Fibre Channelのホストポート識別子は16文字にする必要があります。

コンポーネント	定義
ホストオペレーティングシステムタイプ	ホストオペレーティングシステムタイプは、ホストのオペレーティングシステム（またはそのバージョン）に応じて、ストレージアレイ内のコントローラによるI/Oの処理方法を定義する設定です。これは、_host type_for shortとも呼ばれます。
コントローラのホストポート	コントローラホストポートは、ホストに物理的に接続されるコントローラのポートで、I/O処理に使用されます。
LUN	Logical Unit Number（LUN；論理ユニット番号）は、ホストがボリュームへのアクセスに使用する番号で、アドレススペースに割り当てられます。ボリュームは、LUNの形式で容量としてホストに提示されます。 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を異なるホストで使用して、異なるボリュームにアクセスできます。

ホストの作成とボリュームの割り当てのワークフロー

次の図に、ホストアクセスの設定方法を示します。



ホストの手動作成

ホストの作成は、ストレージアレイに接続されているホストを認識させ、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。ホストは手動でのみ作成できます。

手動作成

ホストを手動で作成すると、ストレージアレイコントローラで検出されたホストポート識別子がホストに正しく関連付けられていることを確認できます。

ホストの手動作成時には、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。作成したホストにボリュームを割り当てたり、ボリュームへのアクセスを共有する場合はホストクラスタに追加したりできます。

ホストおよびホストクラスタへのボリュームの割り当て方法

ホストまたはホストクラスタからボリュームにI/Oを送信するには、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。

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、あとでホストまたはホストクラスタにボリュームを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このボリュームには、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、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」の役割を果たします。LUNはボリュームが作成されたあとに変更できます。

アクセスホリユウム

アクセスボリュームは、ストレージアレイ上の工場出荷時に設定されたボリュームで、ホストI/O接続を介したストレージアレイおよびホストとの通信に使用されます。アクセスボリュームには論理ユニット番号（LUN）が必要です。

アクセスボリュームは次のインスタンスで使用されます。

- インバンド管理--インバンド接続でストレージアレイを管理するために使用されるアクセスボリューム。これは、ストレージアレイをコマンドラインインターフェイス（CLI）で管理している場合にのみ実行できます。

> インバンド管理は、EF600またはEF300ストレージシステムでは使用できません。

アクセスボリュームは、ホストに初めてボリュームを割り当てるときに自動的に作成されます。たとえば、Volume_1とVolume_2をホストに割り当てた場合、その割り当ての結果を表示すると、3つのボリューム（Volume_1、Volume_2、Access）が表示されます。

ホストを自動的に作成しない場合や、CLIを使用してストレージアレイをインバンドで管理しない場合は、アクセスボリュームが不要であるため、アクセスボリュームを削除してLUNを解放できます。この処理を実行すると、ボリュームとLUNの割り当てが解除されるだけでなく、ホストへのインバンド管理接続もすべて削除されます。

LUNの最大数

ストレージアレイには、各ホストで使用できる論理ユニット番号（LUN）の最大数があります。

最大数は、ホストのオペレーティングシステムによって異なります。ストレージアレイは、使用されているLUNの数を追跡します。LUNの最大数を超えるホストにボリュームを割り当てようとすると、そのホストはボリュームにアクセスできません。

デフォルトのホストオペレーティングシステムタイプ

デフォルトのホストタイプは、ホストの初期接続時にストレージアレイで使用されます。ボリュームへのアクセス時にストレージアレイ内のコントローラがホストのオペレーティングシステムとどのように連携するかを定義します。

接続されているホストに応じてストレージアレイの動作を変更する必要がある場合は、ホストタイプを変更できます。通常、デフォルトのホストタイプは、ホストをストレージアレイに接続する前、または追加のホストを接続するときに変更します。

次のガイドラインに注意してください。

- ストレージアレイに接続するすべてのホストのオペレーティングシステムが同じ場合（同種のホスト環境）は、オペレーティングシステムに合わせてホストタイプを変更します。
- ストレージアレイに接続するホストに異なるオペレーティングシステムのホストが混在している場合は（異機種ホスト環境）、ホストのオペレーティングシステムの大部分に一致するホストタイプに変更します。

  たとえば、8つの異なるホストをストレージアレイに接続し、そのうち6つでWindowsオペレーティングシステムを実行している場合は、Windowsをデフォルトのホストオペレーティングシステムタイプとして選択する必要があります。

- 接続されているホストの大部分でオペレーティングシステムが異なる場合は、ホストタイプを[工場出荷時のデフォルト]に変更します。

  たとえば、8つの異なるホストをストレージアレイに接続し、そのうち2つでWindowsオペレーティングシステムを実行している場合、3つでVMwareオペレーティングシステムを実行しています。 さらに、別の3つのOSでLinuxオペレーティングシステムを実行している場合は、デフォルトのホストオペレーティングシステムタイプとしてFactory Defaultを選択する必要があります。

ホストアクセスの設定

ホストの手動作成

自動で検出できないホストについては、手動で作成することができます。ホストの作成は、ストレージアレイに接続されているホストを認識させ、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。

タスクの内容

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ている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、この処理は成功しません。
- 名前の最大文字数は30文字です。

手順

1. メニューから「 Storage [Hosts] 」を選択します。
2. メニュー： Create [Host] をクリックします。

   [ホストの作成]ダイアログボックスが表示されます。

3. 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	製品説明
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は、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 * を選択します 通常、ホストポートはログイン済みで、ドロップダウンリストに表示されます。リストからホストポート識別子を選択できます。 • * 手動で追加 * 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ません。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（一度に1つずつ）から* Host Ports *フィールドにコピーアンドペーストできます。 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はいくつでも選択できます。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。

設定	製品説明
CHAPイニシエータ	（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、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、* CHAP initiator *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したものと同じCHAPシークレットを入力します。双方向CHAP認証（ホストがストレージアレイに対して自身を検証し、ストレージアレイがホストに対して自身を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時または設定の変更時に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。 現在のところ、System Managerで使用されるiSCSI認証方式はCHAPだけです。

4. [作成（ Create ）] をクリックします。

結果

ホストが正常に作成されると、ホストに設定された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、用に作成された最初のポートのデフォルトエイリアス `host IPT is IPT_1`です。

ホストクラスタの作成

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します。

タスクの内容

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る場合があります（異機種混在）。
- ホストクラスタにNVMeホストとNVMe以外のホストを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のいずれかのホスト接続でDAがサポートされていない場合、関連付けられているホストは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、この処理は成功しません。
- 名前の最大文字数は30文字です。

手順

1. メニューから「 Storage [Hosts] 」を選択します。
2. メニューから「Create [Host Cluster]」を選択します。

   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。

3. ホストクラスタ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	製品説明
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	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。ホストクラスタにまだ含まれていないホストだけがリストに表示されます。

4. [作成（ Create ）] をクリックします。

   接続されているインターフェイスタイプのData Assurance（DA）機能が選択したホストで異なる場合は、ホストクラスタでDAを使用できなくなる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、DA対応ボリュームをホストクラスタに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整合性が向上します。DAを使用すると、ホストとドライブの間でデータを移動するときに発生する可能性があるエラーがストレージアレイでチェックされます。新しいボリュームにDAを使用すると、エラーがすべて検出されます。

結果

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

ホストへのボリュームの割り当て

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。これにより、ストレージアレイ内の1つ以上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。

タスクの内容

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。
- 1つのホストまたはホストクラスタが、同じ論理ユニット番号（LUN）を2回使用してボリュームにアクセス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の場合、すべてのボリュームが作成されて初期化されてから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、_ALL_VOLUMESを使用すると、初期化の速度が遅くなります。初期化の進捗状況は、ホーム[処理実行中]メニューから確認できます。

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。
- ホストにホストポート識別子が定義されていません。
- すべてのボリューム割り当てが定義されている。

このタスクでは未割り当てのボリュームがすべて表示されますが、ホストにData Assurance（DA）があるかどうかは次のようになります。

- DA対応ホストの場合は、DAが有効なボリュームとDAが有効でないボリュームを選択できます。
- DA対応でないホストでDAが有効なボリュームを選択すると、ボリュームをホストに割り当てる前にボリュームのDAを自動的にオフにする必要があることを示す警告が表示されます。

手順

1. メニューから「 Storage [Hosts] 」を選択します。
2. 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。任意の列をソートしたり、 * Filter * ボックスに何かを入力すると、特定のボリュームを簡単に見つけることができます。

3. 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、テーブルヘッダーの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。
4. [**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番号が割り当てられます。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。該当する場合は、ホストに関連付けられているボリュームの一覧に、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。

ホストとクラスタの管理

デフォルトのホストタイプの変更

ストレージアレイレベルでデフォルトのホストタイプを変更するには、[デフォルトのホストオペレーティングシステムの変更]設定を使用します。通常、デフォルトのホストタ

イプは、ホストをストレージアレイに接続する前、または追加のホストを接続するときに変更します。

タスクの内容

次のガイドラインに注意してください。

- ストレージアレイに接続するすべてのホストのオペレーティングシステムが同じ場合（同種のホスト環境）は、オペレーティングシステムに合わせてホストタイプを変更します。
- ストレージアレイに接続するホストに異なるオペレーティングシステムのホストが混在している場合は（異機種ホスト環境）、ホストのオペレーティングシステムの大部分に一致するホストタイプに変更します。

  たとえば、8つの異なるホストをストレージアレイに接続し、そのうち6つでWindowsオペレーティングシステムを実行している場合は、Windowsをデフォルトのホストオペレーティングシステムタイプとして選択する必要があります。

- 接続されているホストの大部分でオペレーティングシステムが異なる場合は、ホストタイプを[工場出荷時のデフォルト]に変更します。

  たとえば、8つの異なるホストをストレージアレイに接続し、そのうち2つでWindowsオペレーティングシステムを実行している場合、3つでVMwareオペレーティングシステムを実行しています。 さらに、別の3つのOSでLinuxオペレーティングシステムを実行している場合は、デフォルトのホストオペレーティングシステムタイプとしてFactory Defaultを選択する必要があります。

手順

1. メニューを選択します。[設定][システム]。
2. 下にスクロールして「その他の設定」を選択し、「デフォルトのホストOSタイプの変更」をクリックします。
3. デフォルトとして使用するホストオペレーティングシステムタイプを選択します。
4. [変更（ Change ）] をクリックします。

ボリュームの割り当て解除

ホストまたはホストクラスタからボリュームへの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からボリュームの割り当てを解除します。

タスクの内容

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。

- 最後に割り当てられ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、最後に割り当てられたボリュームを削除する前にそれらの割り当て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、それらのノードを削除する前に登録をクリアする必要があります。

手順

1. メニューから「 Storage [Hosts] 」を選択します。

2. 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。

3. 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、テーブルヘッダーの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。
4. 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は、ボリュームはホストオペレーティングシステムで認識されたままです。

ホストまたはホストクラスタの削除

ホストまたはホストクラスタを削除できます。

タスクの内容

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。
- ホストが属しているホストクラスタに固有の割り当てがある場合、ホストクラスタは影響を受けません。ただし、ホストが属しているホストクラスタに他の割り当てがない場合は、ホストクラスタと他の関連付けられた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は未定義になります。

手順

1. メニューから「 Storage [Hosts] 」を選択します。
2. 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。

   確認のダイアログボックスが表示されます。

3. 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、システムによって次の処理が実行されます。

- 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。

ホスト接続レポートの設定

ホスト接続レポートを有効にすると、コントローラと設定されているホストの間の接続がストレージアレイで継続的に監視され、接続が中断された場合にアラートが表示されるようになります。この機能はデフォルトで有効になっています。

タスクの内容

ホスト接続レポートを無効にすると、接続またはストレージアレイに接続されているホストに関するマルチパスドライバの問題は監視されなくなります。

ホスト接続レポートを無効にすると、コントローラのリソース利用率を監視および調整する自動ロードバランシングも無効になります。

手順

1. メニューを選択します。[設定][システム]。
2. 下にスクロールして「* Additional Settings 」(その他の設定)を表示し、「* Enable / Disable Host Connectivity Reporting *」(ホスト接続レポートの有効化/無効化

   このオプションの下のテキストは、現在有効になっているか無効になっているかを示します。

   確認のダイアログボックスが開きます。
3. 続行するには、 [はい] をクリックします。

   このオプションを選択すると、機能の有効と無効を切り替えることができます。

設定の管理

ホストの設定の変更

ホストの名前、ホスト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. メニューから「 Storage [Hosts] 」を選択します。
2. 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表示され、現在のホスト設定が表示されます。
3. まだ選択されていない場合は、*プロパティ*タブをクリックします。
4. 必要に応じて設定を変更します。

フィールドの詳細

設定	製品説明
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	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た場合は、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. [保存（ Save ）] をクリックします。

ホストクラスタの設定の変更

ホストクラスタ名を変更したり、ホストクラスタ内のホストを追加または削除したりできます。

手順

1. メニューから「 Storage [Hosts] 」を選択します。
2. 編集するホストクラスタを選択し、*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表示され、現在のホストクラスタ設定が表示されます。

3. ホストクラスタの設定を適宜変更します。

   フィールドの詳細

設定	製品説明
名前	ホストクラスタの名前をユーザが指定できます。クラスタ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	ホストを追加するには、[**Associated Hosts**]ボックスをクリックし、ドロップダウンリストからホスト名を選択します。ホスト名を手動で入力することはできません。 ホストを削除するには、ホスト名の横にある* X *をクリックします。

4. [保存（ Save ）] をクリックします。

ホストのホストポート識別子の変更

ホストポート識別子のユーザラベルを変更する場合、ホストに新しいホストポート識別子を追加する場合、またはホストからホストポート識別子を削除する場合は、ホストポート識別子を変更します。

タスクの内容

ホストポート識別子を変更するときは、次のガイドラインに注意してください。

- *-ホストポートを追加すると、ストレージアレイに接続するために作成したホストにホストポート識別子が関連付けられます。ホストバスアダプタ（HBA）ユーティリティを使用して、ポート情報を手動で入力できます。
- 編集--ホストポートを編集して’ホストポートを別のホストに移動(関連付け)することができますホストバスアダプタまたはiSCSIイニシエータを別のホストに移動した可能性があるため、ホストポートを新しいホストに移動（関連付ける）必要があります。
- 削除--ホストポートを削除して’ホストからホストポートを削除(関連付けを解除)することができます

手順

1. メニューから「 Storage [Hosts] 」を選択します。
2. ポートを関連付けるホストを選択し、 * 表示 / 設定の編集 * をクリックします。

   ホストクラスタ内のホストにポートを追加する場合は、ホストクラスタを展開して目的のホストを選択します。ホストクラスタレベルでポートを追加することはできません。

   ダイアログボックスが表示され、現在のホスト設定が表示されます。

3. [ホストポート *] タブをクリックします。

   ダイアログボックスに現在のホストポート識別子が表示されます。

4. ホストポート識別子の設定を必要に応じて変更します。

設定	製品説明
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、ホストポートはコントローラで認識されたままです。 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は解除されます。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。 System Manager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。

5. [保存（ Save ）] をクリックします。

FAQ

ホストとホストクラスタとは

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。

ホストは個別に定義します。独立したエンティティにすることも、ホストクラスタに追加することもできます。個 々 のホストにボリュームを割り当てることも、ホストをホストクラスタの一部として構成して、1つ以上のボリュームへのアクセスをホストクラスタ内の他のホストと共有することもできます。

ホストクラスタは、SANtricity System Managerで作成する論理エンティティです。ボリュームを割り当てる

前に、ホストクラスタにホストを追加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？

同じボリュームセットへのアクセスを複数のホストで共有する場合は、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確認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。最も適切なオプションが表示されます。このリストの表示は、このオプションが完全にサポートされていることを意味するものではありません。

ホストサポートの詳細については、を参照して "NetApp Interoperability Matrix Tool"ください。

次のホストタイプの一部がリストに表示されます。

ホストオペレーティングシステムタイプ	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マルチパスフェイルオーバーソリューションと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ビルトインのストレージアレイタイプポリシーモジュール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マルチパスソリューションを使用する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。
Mac OS（ATTO）	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。

ホストオペレーティングシステムタイプ	オペレーティングシステム（**OS**）とマルチパスドライバ
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	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期起動用に予約されています。ホストオペレーティングシステムタイプが[工場出荷時のデフォルト]に設定されている場合は、接続されている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マルチパスフェイルオーバーソリューションと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）設定を使用します。

HBAおよびアダプタポートとは何ですか。

ホストバスアダプタ（HBA）はホストに搭載されるボードで、1つ以上のホストポートが搭載されています。ホストポートは、コントローラに物理的に接続されるホストバスアダプタ（HBA）のポートで、I/O処理に使用されます。

HBAのアダプタポートはホストポートと呼ばれます。ほとんどのHBAには、1つまたは2つのホストポートがあります。HBAには一意のWorld Wide Identifier（WWID）が割り当てられ、各HBAホストポートには一意のWWIDが割り当てられます。ホストポート識別子は、SANtricity System Managerからホストを手動で作成するときに、適切なHBAを物理ホストに関連付けるために使用されます。

ホストポートをホストに一致させる方法を教えてください。

ホストを手動で作成する場合は、まず、ホストで使用可能な適切な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。

この情報が手元にある場合は、[ホストの作成]ダイアログに表示されるリストから、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。

作成するホストに対応する適切な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に意図せずアクセスする可能性があります。

CHAPシークレットを作成するにはどうすればよいですか？

ストレージアレイに接続されているiSCSIホストでチャレンジハンドシェイク認証プロトコル（CHAP）認証を設定する場合は、iSCSIホストごとにイニシエータCHAPシークレットを再入力する必要があります。

これを行うには、System Managerをホスト作成処理の一環として使用するか、[設定の表示/編集]オプションを使用します。

CHAP相互認証を使用している場合は、[設定]ページでストレージアレイのターゲットCHAPシークレットを定義し、各iSCSIホストでそのターゲットCHAPシークレットを再入力する必要もあります。

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、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に、デフォルトクラスタに割り当てられているボリュームへのアクセスを許可します。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いないが、ホストに物理的に設置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する_は_しない_選択します。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。次に、個 々 のホストまたはホストクラスタにボリュームを割り当てます。

デフォルトクラスタは、すべてのホストとストレージアレイに接続された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ための外部ストレージ環境を構築する場合にのみ使用してください（フルアクセスモード） 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、ユーザインターフェイスに表示されて管理できるようになります。

ホスト接続レポートとは何ですか？

ホスト接続レポートを有効にすると、ストレージアレイはコントローラと設定されているホストの間の接続を継続的に監視し、接続が中断された場合に警告します。

ケーブルの緩み、損傷、紛失、またはホストに別の問題がある場合は、接続が中断される可能性があります。これらの状況では、Recovery Guruメッセージが発行されることがあります。

- ホストの冗長性が失われました--どちらかのコントローラがホストと通信できない場合に開きます
- ホストタイプが正しくありません--ストレージアレイでホストタイプが正しく指定されていないと'フェイルオーバーの問題が発生する可能性があります

コントローラのリブートにかかる時間が接続タイムアウトよりも長くなる可能性がある場合は、ホスト接続レポートを無効にすることができます。この機能を無効にすると、Recovery Guruメッセージが生成されなくなります。

ホスト接続レポートを無効にすると、自動ロードバランシングも無効になります。自動ロードバランシングは、コントローラのリソース使用量を監視および調整します。ただし、ホスト接続レポートを再度有効にしても、自動ロードバランシング機能は自動的には有効になりません。

スナップショット

Snapshotの概要

Snapshot機能を使用すると、ストレージアレイボリュームのポイントインタイムイメージを作成して、バックアップやテストに使用できます。

Snapshotイメージとは

a_snapshot image_は 特定の時点でキャプチャされたボリュームデータの論理コピーです。リストアポイントと同様に、 Snapshot イメージを使用して既知の正常なデータセットにロールバックできます。ホストはSnapshotイメージにアクセスできますが、Snapshotイメージの読み取りや書き込みを直接行うことはできません。

詳細：

- "Snapshotストレージの仕組み"
- "Snapshotに関する用語"
- "ベースボリューム、リザーブ容量、およびSnapshotグループ"
- "Snapshotスケジュールと整合性グループ"
- "Snapshotホリユウム"

スナップショットを作成するにはどうすればよいですか?

ベースボリュームまたはSnapshot整合性グループからSnapshotイメージを手動で作成できます。この手順 は次のメニューから使用できます。Storage [Snapshots]。

詳細：

- "Snapshotの要件とガイドライン"
- "Snapshotイメージとボリュームの作成ワークフロー"
- "Snapshotイメージの作成"
- "Snapshotイメージのスケジュール設定"
- "Snapshot整合性グループの作成"
- "Snapshotボリュームの作成"

スナップショットからデータをロールバックする方法を教えてください。

a_rollback_は、ベースボリューム内のデータを過去の特定の時点に戻すプロセスです。メニューからSnapshotデータをロールバックできます。Storage [Snapshots]。

詳細：

- "Snapshotのロールバック"
- "ベースボリュームのSnapshotイメージのロールバックの開始"
- "整合性グループメンバーのSnapshotイメージのロールバックの開始"

関連情報

スナップショットに関連するタスクの詳細については、以下を参照してください。

- "Snapshotボリュームのリザーブ容量の変更"
- "Snapshotグループのリザーブ容量の変更"

概念

Snapshotストレージの仕組み

Snapshot機能では、copy-on-writeテクノロジを使用してSnapshotイメージを格納し、割り当てられたリザーブ容量を使用します。

Snapshotイメージの使用方法

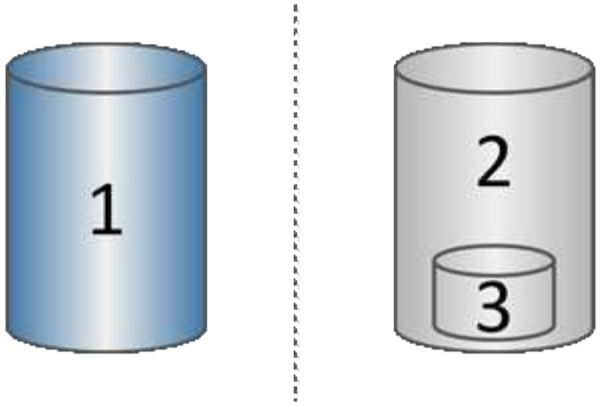
Snapshotイメージは、特定の時点でキャプチャされた、ボリュームの内容の論理的な読み取り専用コピーです。Snapshotを使用してデータ損失を防ぐことができます。

Snapshotイメージはテスト環境でも役立ちます。データの仮想コピーを作成することで、実際のボリューム自体を変更することなく、Snapshotを使用してデータをテストできます。また、ホストにはSnapshotイメージへの書き込みアクセス権がないため、Snapshotは常にセキュアなバックアップリソースです。

Snapshotの作成

Snapshotが作成されると、Snapshot機能はイメージデータを次のように格納します。

- Snapshotイメージが作成されると、ベースボリュームと完全に一致します。Snapshot機能はcopy-on-writeテクノロジを使用します。Snapshotの作成後、ベースボリューム上のブロックまたはブロックセットへの最初の書き込みによって、新しいデータがベースボリュームに書き込まれる前に元のデータがリザーブ容量にコピーされます。
- 以降のSnapshotには変更されたデータブロックのみが含まれます。ベースボリュームのデータが上書きされる前に、Snapshot機能はcopy-on-writeテクノロジを使用して、影響を受けるセクターの必要なイメージをSnapshotのリザーブ容量に保存します。



1基本ボリューム（物理ディスク容量）；2スナップショット（論理ディスク容量）；3^予約容量（物理ディスク容量）

- リザーブ容量には、ベースボリュームのSnapshotの作成後に変更された部分の元のデータブロックと、変更を追跡するためのインデックスが格納されます。通常、リザーブ容量のデフォルトサイズはベースボリュームの40%です。（リザーブ容量が足りない場合は拡張できます）。
- Snapshotイメージは、タイムスタンプに基づいて特定の順序で格納されます。手動で削除できるのはベースボリュームの最も古いSnapshotイメージのみです。

Snapshotのリストア

ベースボリュームにデータをリストアするには、SnapshotボリュームまたはSnapshotイメージを使用できます。

- スナップショット・ボリューム--削除されたファイルを取得する必要がある場合は'既知の正常なスナップショット・イメージからスナップショット・ボリュームを作成してから'それをホストに割り当てます
- * Snapshotイメージ*--ベースボリュームを特定の時点にリストアする必要がある場合は、以前のSnapshotイメージを使用してデータをベースボリュームにロールバックします。

Snapshotに関する用語

ストレージアレイに関連するSnapshotの用語を次に示します。

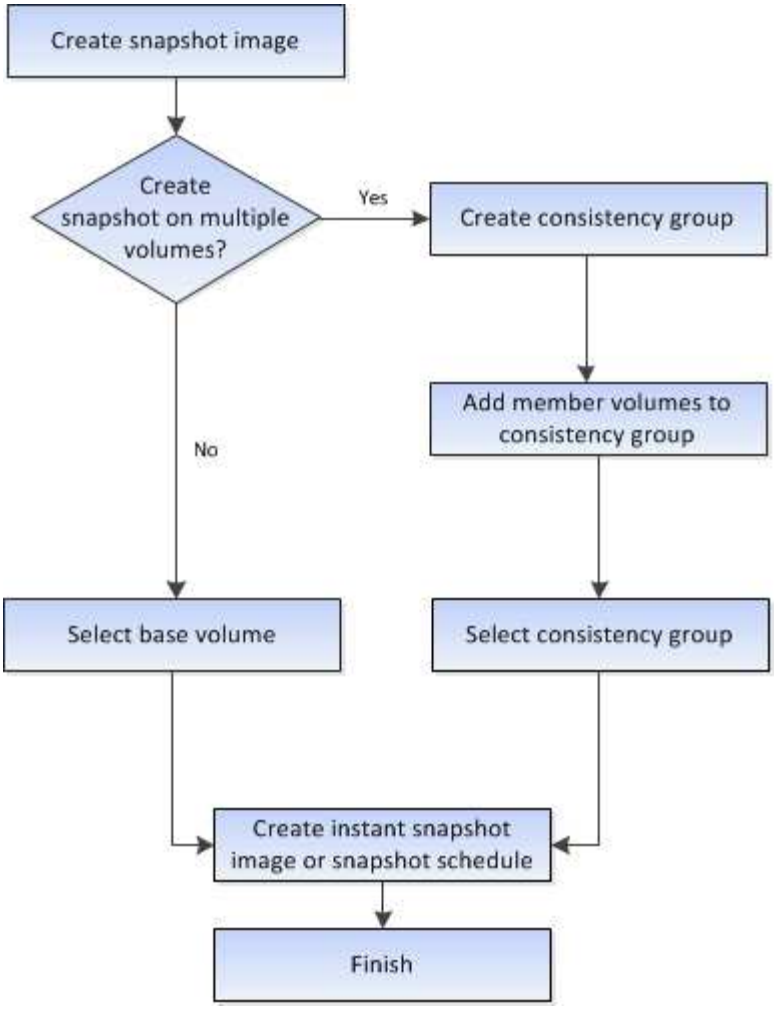
期間	製品説明
Snapshot機能	Snapshot機能は、ボリュームのイメージの作成と管理に使用されます。
Snapshotイメージ	Snapshot イメージは、ボリュームのデータを特定の時点でキャプチャした論理コピーです。リストアポイントと同様に、 Snapshot イメージを使用して既知の正常なデータセットにロールバックできます。ホストはSnapshotイメージにアクセスできますが、Snapshotイメージの読み取りや書き込みを直接行うことはできません。
ベースボリューム	ベースボリュームは、Snapshotイメージの作成元のボリュームです。シックボリュームでもシンボリュームでもかまいません。通常はホストに割り当てられます。ベースボリュームはボリュームグループまたはディスクプールのどちらかに配置できます。

期間	製品説明
Snapshotボリューム	Snapshotボリュームを使用すると、ホストはSnapshotイメージのデータにアクセスできます。Snapshotボリュームには独自のリザーブ容量が含まれているため、元のSnapshotイメージに影響を与えることなくベースボリュームへの変更が保存されます。
Snapshotグループ	Snapshotグループは、1つのベースボリュームのSnapshotイメージの集まりです。
リザーブ容量ボリューム	リザーブ容量ボリュームは、ベースボリュームのうちどのデータブロックが上書きされるか、およびそれらのブロックの保持される内容を追跡します。
Snapshotスケジュール	Snapshotスケジュールは、Snapshotイメージの自動作成に使用するタイムテーブルです。イメージを作成する頻度を制御することができます。
Snapshot整合性グループ	Snapshot整合性グループは、Snapshotイメージが作成されるときに1つのエンティティとして扱われるボリュームの集まりです。各ボリュームには独自のSnapshotイメージがありますが、すべてのイメージは同じ時点で作成されます。
Snapshot整合性グループメンバーボリューム	Snapshot整合性グループに属する各ボリュームをメンバーボリュームと呼びます。ボリュームをSnapshot整合性グループに追加すると、System Managerはそのメンバーボリュームに対応する新しいSnapshotグループを自動的に作成します。
ロールバック	ロールバックとは、ベースボリュームのデータを過去のある時点に戻すプロセスです。
リザーブ容量	リザーブ容量は、コピーサービス処理やストレージオブジェクトに使用される物理割り当て容量です。ホストから直接読み取ることはできません。

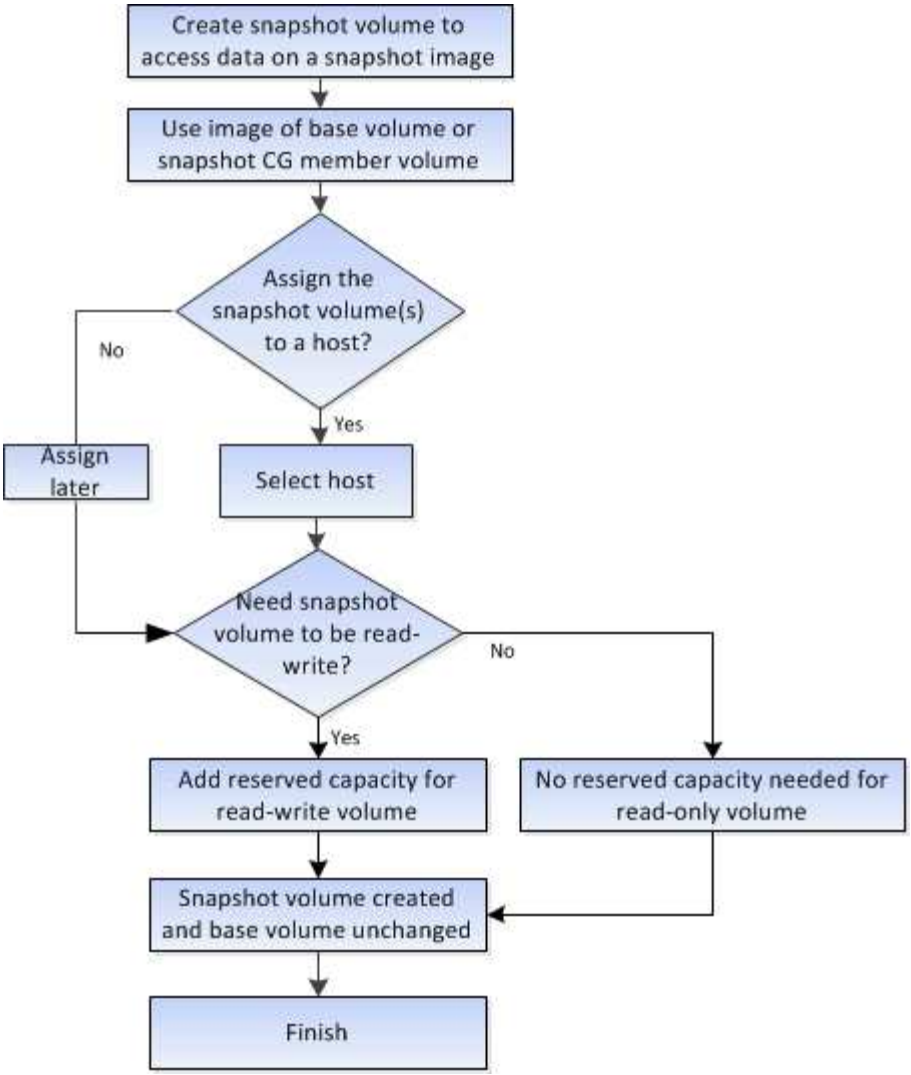
Snapshotイメージと**Snapshot**ボリュームの作成ワークフロー

System Managerでは、次の手順でSnapshotイメージとSnapshotボリュームを作成します。

Snapshotイメージの作成ワークフロー



Snapshotボリュームの作成ワークフロー



Snapshotの要件とガイドライン

スナップショットを作成して使用する場合は、次の要件とガイドラインを確認してください。

Snapshotイメージと**Snapshot**グループ

- 各Snapshotイメージは1つのSnapshotグループに関連付けられます。
- Snapshotグループは、関連オブジェクトのスケジュールされたSnapshotイメージまたはインスタントSnapshotイメージを初めて作成したときに作成されます。これにより、リザーブ容量が作成されます。

  Snapshotグループは、Pools & Volume Groupsページで表示できます。

- スケジュールされたSnapshotイメージは、ストレージアレイがオフラインのときや電源がオフのときは作成されません。
- Snapshotスケジュールが設定されたSnapshotグループを削除すると、Snapshotスケジュールも削除されます。
- 不要になったSnapshotボリュームは、削除する代わりに、関連付けられているリザーブ容量とともに再利用できます。これにより、同じベースボリュームの別のSnapshotボリュームが作成されます。Snapshotイメージが同じベースボリューム内にあるかぎり、SnapshotボリュームまたはSnapshot整合性グループ

のSnapshotボリュームを同じSnapshotイメージまたは別のSnapshotイメージに再度関連付けることができます。

Snapshot整合性グループ

- Snapshot整合性グループには、Snapshot整合性グループのメンバーであるボリュームごとにSnapshotグループが1つ含まれます。
- Snapshot整合性グループは1つのスケジュールにのみ関連付けることができます。
- Snapshotスケジュールが設定されたSnapshot整合性グループを削除すると、Snapshotスケジュールも削除されます。
- Snapshot整合性グループに関連付けられているSnapshotグループを個別に管理することはできません。管理処理（Snapshotイメージの作成、SnapshotイメージまたはSnapshotグループの削除、Snapshotイメージのロールバック）は、Snapshot整合性グループレベルで実行する必要があります。

ベースボリューム

- SnapshotボリュームのData Assurance（DA）とセキュリティ設定は、関連付けられているベースボリュームと同じである必要があります。
- 障害が発生したベースボリュームのSnapshotボリュームは作成できません。
- ベースボリュームがボリュームグループに含まれている場合は、関連付けられているSnapshot整合性グループのメンバーボリュームをプールまたはボリュームグループに配置できます。
- ベースボリュームがプールに含まれている場合は、関連付けられているSnapshot整合性グループのすべてのメンバーボリュームをベースボリュームと同じプールに配置する必要があります。

リザーブ容量

- リザーブ容量は1つのベースボリュームにのみ関連付けられます。
- スケジュールを使用すると、Snapshotイメージが大量に作成される可能性があります。スケジュールされたSnapshot用の十分なリザーブ容量があることを確認してください。
- Snapshot整合性グループのリザーブ容量ボリュームのData Assurance（DA）とセキュリティの設定は、Snapshot整合性グループのメンバーボリュームの関連付けられているベースボリュームと同じである必要があります。

保留中の**Snapshot**イメージ

次の状況では、Snapshotイメージの作成が保留状態のままになることがあります。

- このSnapshotイメージを含むベースボリュームが非同期ミラーグループのメンバーである。
- ベースボリュームで同期処理を実行中です。同期処理が完了するとすぐにSnapshotイメージの作成が完了します。

Snapshotイメージの最大数

- ボリュームがSnapshot整合性グループのメンバーである場合、System Managerはそのメンバーボリュームのスナップショットグループを作成します。このSnapshotグループは、ベースボリュームあたりのSnapshotグループの許容最大数にカウントされます。
- SnapshotグループまたはSnapshot整合性グループにSnapshotイメージを作成しようとしていて、関連付けられているグループがSnapshotイメージの最大数に達している場合は、次の2つのオプションがありま

す。

- SnapshotグループまたはSnapshot整合性グループの自動削除を有効にします。
- SnapshotグループまたはSnapshot整合性グループから1つ以上のSnapshotイメージを手動で削除し、処理を再試行します。

自動削除

SnapshotグループまたはSnapshot整合性グループで自動削除が有効になっている場合、グループに新しいSnapshotイメージが作成されると、最も古いSnapshotイメージがSystem Managerによって削除されます。

ロールバック処理

- ロールバック処理の実行中は、次の操作を実行できません。
  - ロールバックに使用されているSnapshotイメージを削除します。
  - ロールバック処理の対象となるベースボリュームの新しいSnapshotイメージを作成します。
  - 関連付けられているSnapshotグループのRepository-Fullポリシーの変更
- 次のいずれかの処理が実行中の場合は、ロールバック処理を開始できません。
  - 容量の拡張（プールまたはボリュームグループへの容量の追加）
  - ボリュームの拡張（ボリュームの容量の拡張）
  - ボリュームグループのRAIDレベルの変更
  - ボリュームのセグメントサイズの変更
- ベースボリュームがボリュームコピーに含まれている場合は、ロールバック処理を開始できません。
- ベースボリュームがリモートミラーのセカンダリボリュームである場合は、ロールバック処理を開始できません。
- 関連付けられているSnapshotリポジトリボリュームの使用済み容量に読み取り不能セクターがある場合、ロールバック処理は失敗します。

ベースボリューム、リザーブ容量、および**Snapshot**グループ

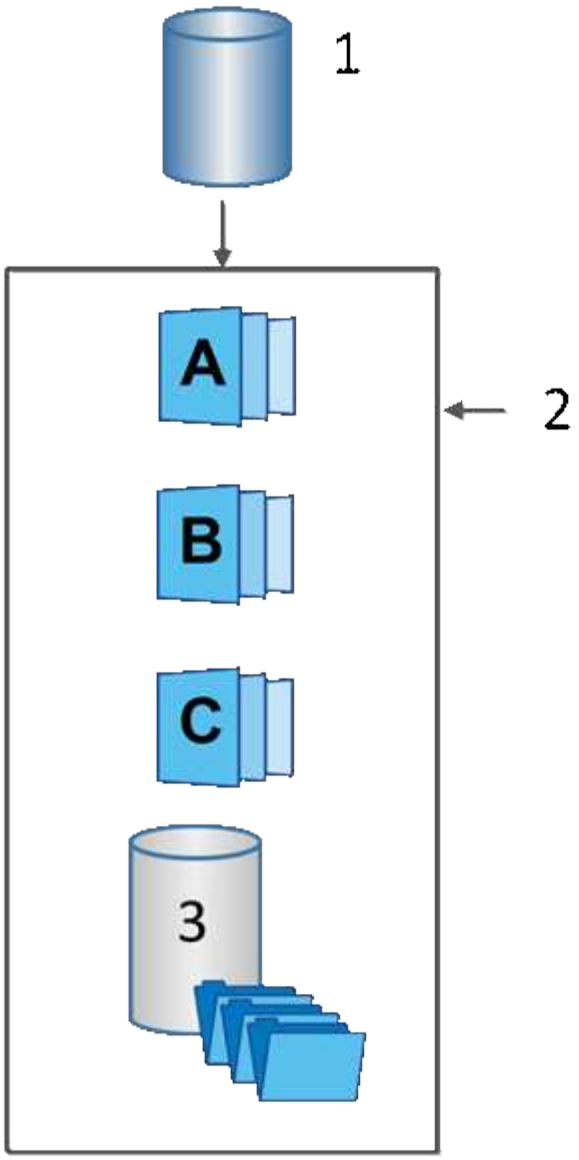
Snapshot機能では、ベースボリューム、リザーブ容量、およびSnapshotグループが使用されます。

ヘエスホリユウム

a_base volume_は、Snapshotイメージのソースとして使用されるボリュームです。ベースボリュームはシックボリュームでもシンボリュームでもかまいません。ベースボリュームはプールまたはボリュームグループに配置できます。

ベースボリュームのSnapshotを作成するには、いつでもインスタントイメージを作成したり、Snapshotの定期的なスケジュールを定義してプロセスを自動化したりできます。

次の図は、Snapshotオブジェクトとベースボリュームの関係を示しています。



1基本ボリューム；2グループ内のSnapshotオブジェクト（イメージおよびリザーブ容量）；3^ Snapshotグループのリザーブ容量。

リザーブ容量と**Snapshot**グループ

System Managerでは、Snapshotイメージを_ Snapshotグループ_に編成します。System Managerは、Snapshotグループの確立時に、グループのSnapshotイメージを保持し、追加のSnapshotに対する以降の変更を追跡するために、Associated _reserved capacity _を自動的に作成します。

ベースボリュームがボリュームグループに含まれている場合は、リザーブ容量をプールまたはボリュームグループに配置できます。ベースボリュームがプールに含まれている場合は、リザーブ容量をベースボリュームと同じプールに配置する必要があります。

Snapshotグループに対するユーザの操作は必要ありませんが、Snapshotグループではリザーブ容量をいつでも調整できます。また、次の条件に該当する場合は、リザーブ容量の作成を求められることがあります。

- Snapshotグループがまだ作成されていないベースボリュームのSnapshotを作成すると、System ManagerによってSnapshotグループが自動的に作成されます。この操作では、以降のSnapshotイメージの格納に

使用されるベースボリュームのリザーブ容量も作成されます。

- ベースボリュームのSnapshotスケジュールを作成すると、System ManagerによってSnapshotグループが自動的に作成されます。

自動削除

Snapshotを使用する場合は、デフォルトオプションを使用して自動削除をオンにします。Snapshotグループの上限である32個のイメージに達すると、自動削除によって最も古いSnapshotイメージが自動的に削除されます。自動削除を無効にすると、最終的にはSnapshotグループの制限を超えるため、Snapshotグループの設定やリザーブ容量の管理を手動で行う必要があります。

Snapshotスケジュールと**Snapshot**整合性グループ

Snapshotイメージの収集スケジュールを使用し、Snapshot整合性グループを使用して複数のベースボリュームを管理します。

ベースボリュームのSnapshot処理を簡単に管理するために、次の機能を使用できます。

- **Snapshot**スケジュール-- 1つのベース・ボリュームのスナップショットを自動化します
- スナップショット・コンシステンシ・グループ--複数のベース・ボリュームを1つのエンティティとして管理する

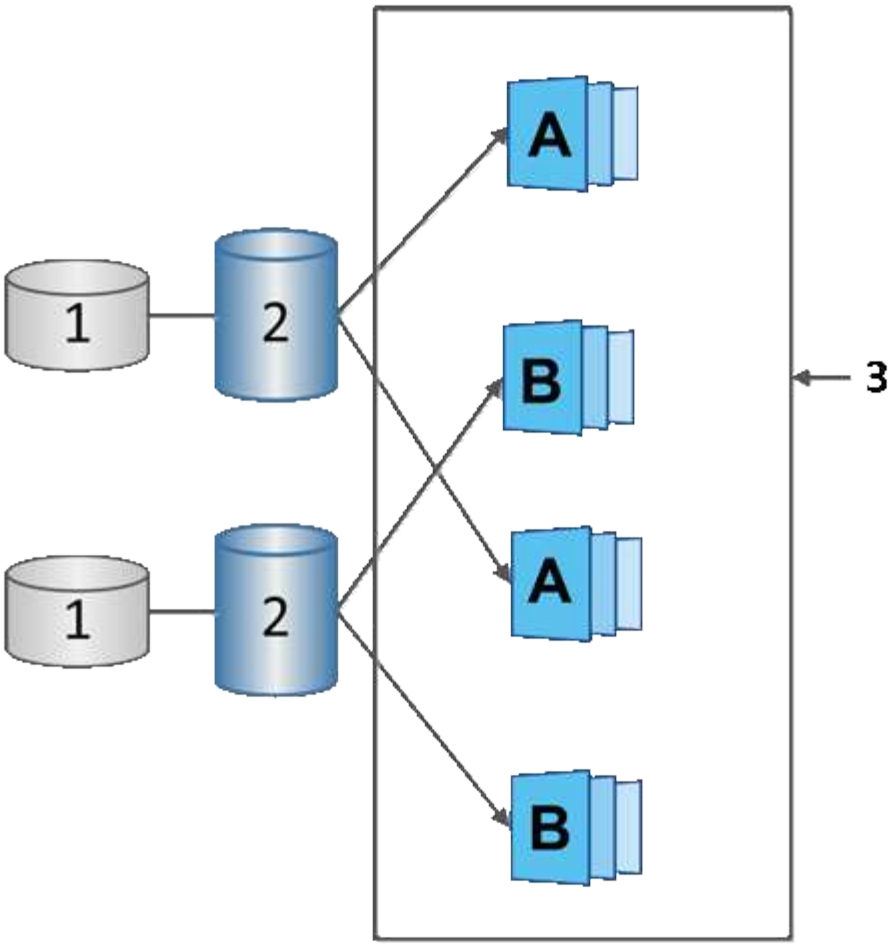
Snapshotスケジュール

ベースボリュームのSnapshotを自動的に作成する場合は、スケジュールを作成できます。たとえば、毎月第1土曜日の午前0時にSnapshotイメージを作成するスケジュールを定義できます。任意の日時を指定することもできます。1つのスケジュールにつき最大32個のSnapshotに達すると、スケジュールされたSnapshotを一時停止して追加のリザーブ容量を作成したり、Snapshotを削除したりできます。Snapshotは、手動で削除することも、削除プロセスを自動化することもできます。Snapshotイメージが削除されると、追加のリザーブ容量を再利用できます。

Snapshot整合性グループ

複数のボリュームに同時にSnapshotイメージが作成されるようにするには、Snapshot整合性グループを作成します。Snapshotイメージの操作は、Snapshot整合性グループ全体に対して実行されます。たとえば、タイムスタンプが同じすべてのボリュームの同期されたSnapshotのスケジュールを設定できます。Snapshot整合性グループは、複数のボリュームにまたがるアプリケーション（あるボリュームにログを格納し、別のボリュームにデータベースファイルを格納するデータベースアプリケーションなど）に最適です。

Snapshot整合性グループに含まれるボリュームはメンバーボリュームと呼ばれます。整合性グループにボリュームを追加すると、そのメンバーボリュームに対応する新しいリザーブ容量がSystem Managerによって自動的に作成されます。各メンバーボリュームのSnapshotイメージを自動的に作成するスケジュールを定義できます。



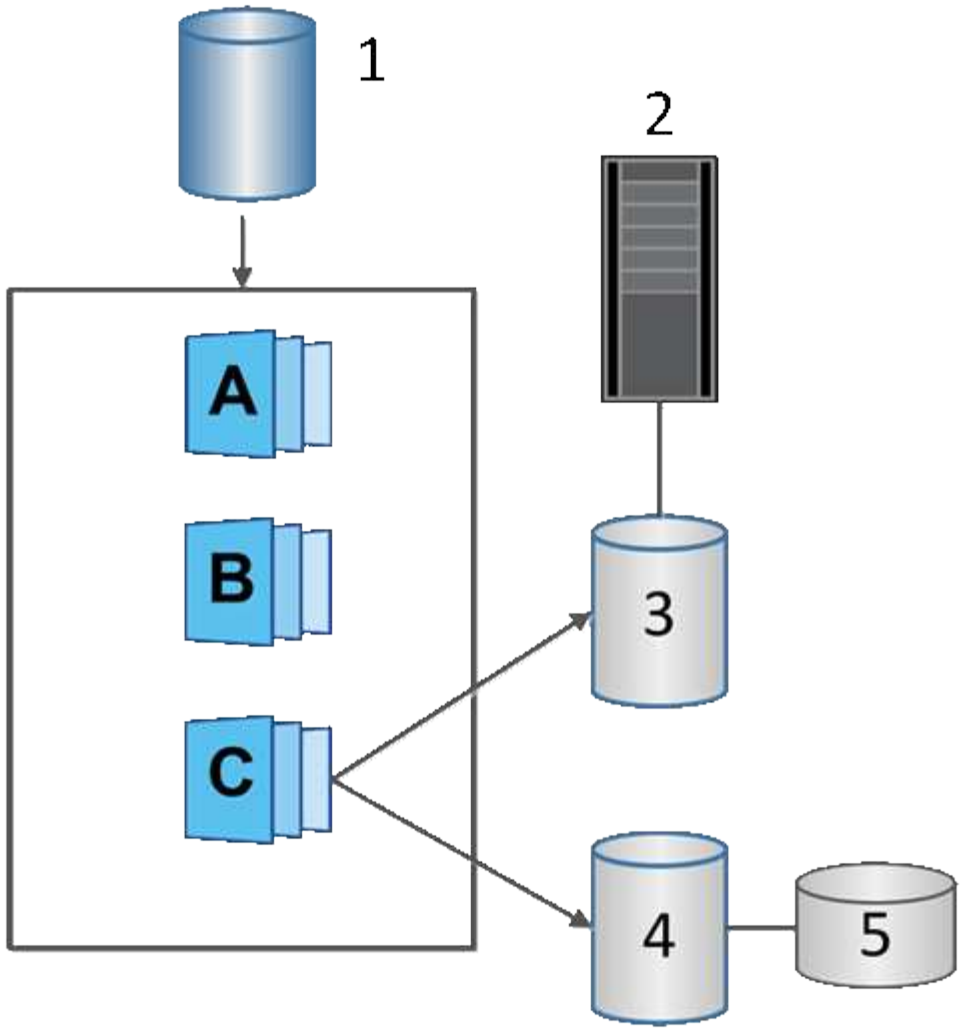
[1]リザーブ容量；[2]メンバーボリューム；3^整合グループSnapshotイメージ

Snapshotホリユウム

Snapshotデータの読み取りまたは書き込みを行う場合は、Snapshotボリュームを作成してホストに割り当てることができます。Snapshotボリュームはベースボリュームと同じ特性（RAIDレベル、I/O特性など）を共有します。

作成したSnapshotボリュームは、____トク ミシユリ_onl_yまたは_read-write accessible _として指定できます。

読み取り専用Snapshotボリュームを作成する場合は、リザーブ容量を追加する必要はありません。読み書き可能Snapshotボリュームを作成する場合は、リザーブ容量を追加して書き込みアクセスを許可する必要があります。



1基本ボリューム；2ホスト；3読み取り専用Snapshotボリューム；4読み取り/書き込みSnapshotボリューム；5^リザーブ容量

Snapshotのロールバック

ロールバック処理では、ベースボリュームが選択したSnapshotで指定された以前の状態に戻ります。

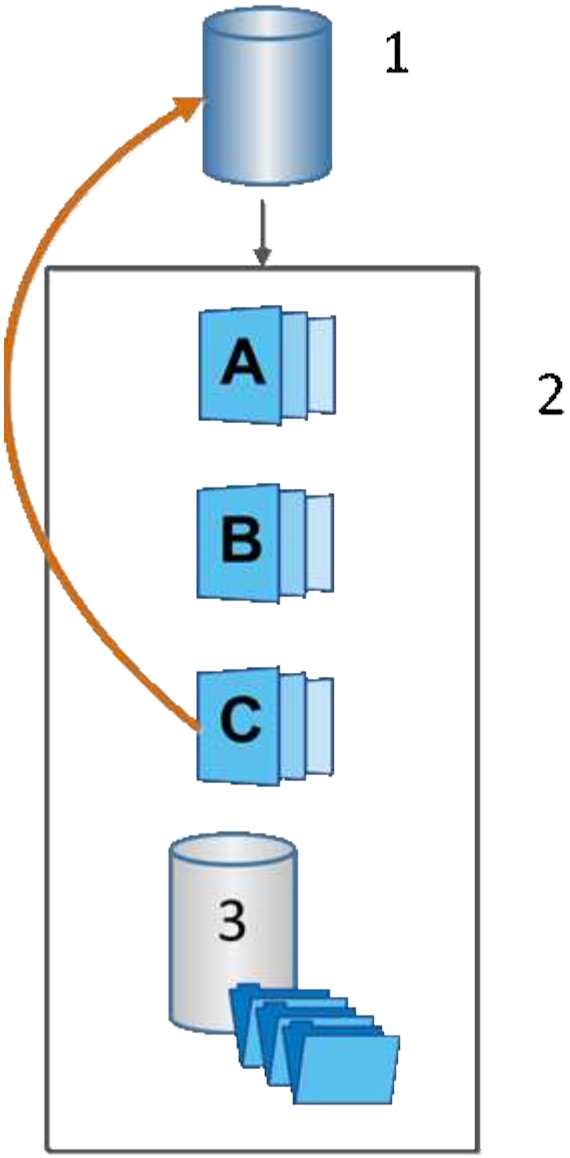
ロールバックでは、次のいずれかのソースからSnapshotイメージを選択できます。

- * Snapshotイメージのロールバック*：ベース・ボリュームのフル・リストア用
- * Snapshot整合性グループのロールバック*。1つ以上のボリュームのロールバックに使用できます。

ロールバック中は、Snapshot機能によってグループ内のすべてのSnapshotイメージが保持されます。また、I/O処理に必要な場合は、このプロセス中にホストからベースボリュームにアクセスすることもできます。

ロールバックが開始されると、バックグラウンドプロセスによってベースボリュームの論理ブロックアドレス（LBA）が検索され、リストア対象のcopy-on-writeデータがロールバックSnapshotイメージから検出されます。ベースボリュームは読み取りと書き込みのためにホストからアクセスでき、以前に書き込まれたすべてのデータをすぐに使用できるため、ロールバック処理中のすべての変更を格納できる十分な容量がリザーブ容量

ボリュームに必要です。データ転送は、ロールバックが完了するまでバックグラウンド処理として続行されます。



1基本ボリューム；2グループ内のSnapshotオブジェクト；3^ Snapshotグループのリザーブ容量

SnapshotとSnapshotオブジェクトの作成

Snapshotイメージの作成

ベースボリュームまたはSnapshot整合性グループからSnapshotイメージを手動で作成できます。これは_インスタント・スナップショット_または_インスタント・イメージ_とも呼ばれます

開始する前に

- ベースボリュームが最適Iである必要があります。

- ドライブが最適lである必要があります。
- スナップショット・グループを予約済みとして指定することはできません
- リザーブ容量ボリュームのData Assurance（DA）設定は、関連付けられているSnapshotグループのベースボリュームと同じである必要があります。

手順

1. 次のいずれかの操作を実行してSnapshotイメージを作成します。
   - 選択メニュー： Storage [Volumes]オブジェクト（ベースボリュームまたはSnapshot整合性グループ）を選択し、メニュー：コピーサービス[インスタントSnapshotの作成]を選択します。
   - メニューを選択します。Storage [Snapshots]。「スナップショットイメージ」タブを選択し、メニューから「Create [Instant snapshot]」を選択します。

     Create Snapshot Image（スナップショットイメージの作成）ダイアログボックスが表示されます。オブジェクト（ベースボリュームまたはSnapshot整合性グループ）を選択し、* Next *をクリックします。ボリュームまたはSnapshot整合性グループに対して以前にSnapshotイメージが作成されている場合は、インスタントSnapshotがただちに作成されます。それ以外の場合は、ボリュームまたはSnapshot整合性グループのSnapshotイメージが初めて作成されるときに、Confirm Snapshot Imageダイアログボックスが表示されます。

2. Create *をクリックしてリザーブ容量が必要であることを通知し、Reserve Capacityステップに進みます。

   Reserve Capacityダイアログボックスが表示されます。

3. スピンボックスを使用して容量の割合を調整し、*次へ*をクリックして、テーブルで強調表示されている候補ボリュームを受け入れます。

   設定の編集ダイアログボックスが表示されます。

4. Snapshotイメージの設定を必要に応じて選択し、処理を確定します。

フィールドの詳細

設定	製品説明
• Snapshotイメージの設定*	Snapshotイメージの上限
指定した上限を超えたSnapshotイメージを自動的に削除する場合は、チェックボックスをオンのままにします。上限を変更するには、スピンボックスを使用します。このチェックボックスをオフにすると、32個のイメージが作成された時点でSnapshotイメージの作成が停止します。	リザーブ容量の設定
アラートを受け取るタイミング…	このスピンボックスを使用して、Snapshotグループのリザーブ容量が残り少なくなったときにシステムからアラート通知を送信する割合を調整します。 Snapshotグループのリザーブ容量が指定したしきい値を超えた場合は、事前通知を使用して、残りのスペースがなくなる前にリザーブ容量を増やしたり、不要なオブジェクトを削除したりします。
リザーブ容量がフルになった場合のポリシー	次のいずれかのポリシーを選択します。 • 最も古い**Snapshot**イメージをパージする- Snapshotグループ内の最も古いSnapshotイメージが自動的にパージされ、そのSnapshotイメージのリザーブ容量が解放されてグループ内で再利用されます。 • ベースボリュームへの書き込みを拒否--リザーブ容量の割合が定義された上限に達すると'リザーブ容量へのアクセスをトリガーしたベースボリュームに対するI/O書き込み要求はすべて拒否されます

結果

- System ManagerのSnapshot Imagesテーブルに、新しいSnapshotイメージが表示されます。新しいイメージがタイムスタンプおよび関連付けられているベースボリュームまたはSnapshot整合性グループ別にリストされます。
- 次の状況に該当する場合は、Snapshotの作成が保留状態になることがあります。
  - このSnapshotイメージを含むベースボリュームが非同期ミラーグループのメンバーである。
  - ベースボリュームで同期処理を実行中です。同期処理が完了するとすぐにSnapshotイメージの作成が完了します。

Snapshotイメージのスケジュール設定

Snapshotスケジュールを作成して、ベースボリュームに問題が発生した場合のリカバリを有効にし、スケジュールされたバックアップを実行します。ベースボリュームまたはSnapshot整合性グループのSnapshotは、日単位、週単位、または月単位のスケジュールでいつでも作成できます。

開始する前に

ベースボリュームが最適lである必要があります。

タスクの内容

このタスクでは、既存のSnapshot整合性グループまたはベースボリュームのSnapshotスケジュールを作成する方法について説明します。

ベースボリュームまたはSnapshot整合性グループのSnapshotイメージの作成と同時にSnapshotスケジュールを作成することもできます。

手順

1. 次のいずれかの操作を実行して、Snapshotスケジュールを作成します。
   - 選択メニュー： Storage [Volumes]

     このSnapshotスケジュールのオブジェクト（ボリュームまたはSnapshot整合性グループ）を選択し、メニュー：コピーサービス[Snapshotスケジュールの作成]を選択します。

   - メニューを選択します。Storage [Snapshots]。

     [スケジュール]タブを選択し、[作成]をクリックします。

2. このSnapshotスケジュールのオブジェクト（ボリュームまたはSnapshot整合性グループ）を選択し、* Next *をクリックします。

   Create Snapshot Schedule（スナップショットスケジュールの作成）ダイアログボックスが表示されます。

3. 次のいずれかを実行します。
   - *別のSnapshotオブジェクト*から以前に定義されたスケジュールを使用します。

     詳細オプションが表示されていることを確認します。[詳細オプションを表示]をクリックします。[スケジュールのインポート]をクリックし、インポートするスケジュールのあるオブジェクトを選択して、[インポート]をクリックします。

   - *基本オプションまたは詳細オプション*を変更します。

     ダイアログボックスの右上にある*その他のオプションを表示*をクリックしてすべてのオプションを表示し、次の表を参照してください。

フィールドの詳細

フィールド	製品説明
基本設定	日を選択
Snapshotイメージの個々の曜日を選択します。	開始時刻
ドロップダウンリストから、日単位のSnapshotの新しい開始時間を選択します（30分単位で選択できます）。デフォルトでは、開始時刻は現在時刻の30分前に設定されます。	タイムゾーン
ドロップダウンリストから、アレイのタイムゾーンを選択します。	• 詳細設定 *
日/月	次のいずれかのオプションを選択します。 • 毎日/毎週--同期スナップショットの個々の曜日を選択します日次スケジュールを設定する場合は、右上の[すべての日を選択]チェックボックスをオンにすることもできます。 • 毎月/毎年--同期スナップショットの個々の月を選択します[* on day(s)]フィールドに、同期を実行する月の日を入力します。有効なエントリは 1 ~* 31 および Last *です。複数の日にちをカンマまたはセミコロンで区切ることができます。日にちの範囲を入力するには、ハイフンを使用します。たとえば、「1、3、4」、「10-15」、「Last」のようになります。月単位のスケジュールを設定する場合は、右上の[すべての月を選択]チェックボックスをオンにすることもできます。
開始時刻	ドロップダウンリストから、日単位のSnapshotの新しい開始時間を選択します（30分単位で選択できます）。デフォルトでは、開始時刻は現在時刻の30分前に設定されます。
タイムゾーン	ドロップダウンリストから、アレイのタイムゾーンを選択します。
1日あたりのSnapshot数/ Snapshotの作成間隔	1日に作成するSnapshotイメージの数を選択します。複数を選択する場合は、Snapshotイメージの作成間隔も選択します。複数のSnapshotイメージを作成する場合は、リザーブ容量が十分にあることを確認してください。

フィールド	製品説明
Snapshotイメージを今すぐ作成？	スケジュールする自動イメージに加えてインスタントイメージを作成するには、このチェックボックスをオンにします。
開始日/終了日または終了日なし	同期の開始日を入力します。終了日を入力するか、「終了日なし」を選択してください。

4. 次のいずれかを実行します。
   - オブジェクトがSnapshot整合性グループの場合は、* Create *をクリックして設定を受け入れ、スケジュールを作成します。
   - オブジェクトがボリュームの場合は、* Next *をクリックして、Snapshotイメージにリザーブ容量を割り当てます。

     [ボリューム候補]の表には、指定したリザーブ容量をサポートする候補のみが表示されます。リザーブ容量は、コピーサービス処理やストレージオブジェクトに使用される物理割り当て容量です。ホストから直接読み取ることはできません。
5. スピンボックスを使用して、Snapshotイメージにリザーブ容量を割り当てます。次のいずれかを実行します。
   - デフォルト設定を受け入れます。

     デフォルト設定を使用してSnapshotイメージにリザーブ容量を割り当てるには、この推奨オプションを使用します。
   - データストレージのニーズに合わせて独自の設定でリザーブ容量を割り当てることができます。

     デフォルトのリザーブ容量設定を変更した場合は、*候補の更新*をクリックして、指定したリザーブ容量の候補リストを更新します。

     次のガイドラインに従ってリザーブ容量を割り当てます。
     - リザーブ容量のデフォルト設定はベースボリュームの容量の40%です。通常はこの容量で十分です。
     - 必要な容量は、ボリュームに対するI/O書き込みの頻度とサイズ、およびSnapshotイメージを収集する数と期間によって異なります。
6. 「 * 次へ * 」をクリックします。

   設定の編集ダイアログボックスが表示されます。
7. 必要に応じてスナップショットスケジュールの設定を編集し、*完了*をクリックします。

フィールドの詳細

設定	製品説明
• Snapshotイメージの上限*	次の場合にSnapshotイメージの自動削除を有効にする…
指定した上限を超えたSnapshotイメージを自動的に削除する場合は、チェックボックスをオンのままにします。上限を変更するには、スピンボックスを使用します。このチェックボックスをオフにすると、32個のイメージが作成された時点でSnapshotイメージの作成が停止します。	リザーブ容量の設定
アラートを受け取るタイミング…	このスピンボックスを使用して、スケジュールのリザーブ容量が残り少なくなったときにシステムからアラート通知を送信する割合を調整します。 スケジュールのリザーブ容量が指定したしきい値を超えた場合は、事前通知を使用して、残りのスペースがなくなる前にリザーブ容量を増やしたり、不要なオブジェクトを削除したりします。
リザーブ容量がフルになった場合のポリシー	次のいずれかのポリシーを選択します。 • 最も古い**Snapshot**イメージをパージする--システムは最も古いSnapshotイメージを自動的にパージし、そのSnapshotイメージのリザーブ容量を解放して、Snapshotグループ内で再利用します。 • ベースボリュームへの書き込みを拒否--リザーブ容量の割合が定義された上限に達すると'リザーブ容量へのアクセスをトリガーしたベースボリュームに対するI/O書き込み要求はすべて拒否されます

Snapshot整合性グループの作成

整合性のあるコピーを保持するために、Snapshot整合性グループ_という名前の複数のボリュームのセットを作成できます。

このグループを使用すると、すべてのボリュームのSnapshotイメージを同時に作成して整合性を確保できます。Snapshot整合性グループに属する各ボリュームのことを「*member volume_*」と呼びます。Snapshot整合性グループにボリュームを追加すると、そのメンバーボリュームに対応する新しいSnapshotグループが自動的に作成されます。

タスクの内容

Snapshot整合性グループ作成手順では、グループのメンバーボリュームを選択し、メンバーボリュームに容量を割り当てることができます。

Snapshot整合性グループを作成するプロセスは複数の手順で構成されます。

手順1：Snapshot整合性グループにメンバーを追加する

メンバーを選択し、Snapshot整合性グループを構成する一連のボリュームを指定します。Snapshot整合性グループに対して実行する操作はすべて、選択したメンバーボリュームに対して均一に実行されます。

開始する前に

メンバーボリュームが最適Iである必要があります。

手順

1. メニューを選択します。Storage [Snapshots]。
2. スナップショット・コンシステンシ・グループ*タブをクリックします
3. メニューを選択します。Create [Snapshot consistency group].

   Create Snapshot Consistency Group（Snapshot整合グループの作成）ダイアログボックスが表示されます。

4. Snapshot整合性グループにメンバーボリュームとして追加するボリュームを選択します。
5. [次へ]*をクリックし、に進みます手順2：Snapshot整合性グループ用の容量をリザーブします。

手順2：Snapshot整合性グループ用の容量をリザーブします

Snapshot整合性グループにリザーブ容量を関連付けます。Snapshot整合性グループのプロパティに基づいて、System Managerから推奨されるボリュームと容量が提示されます。推奨されるリザーブ容量の設定をそのまま使用することも、割り当てられたストレージをカスタマイズすることもできます。

タスクの内容

ボリューム候補の表には、リザーブ容量ダイアログボックスで、指定したリザーブ容量をサポートする候補だけが表示されます。リザーブ容量は、コピーサービス処理やストレージオブジェクトに使用される物理割り当て容量です。ホストから直接読み取ることはできません。

手順

1. スピンボックスを使用して、Snapshot整合性グループにリザーブ容量を割り当てます。次のいずれかを実行します。
   - デフォルトの設定をそのまま使用します。

     各メンバーボリュームにデフォルトの設定でリザーブ容量を割り当てるには、このオプションを使用します（推奨）。

   - データストレージのニーズに合わせて独自の設定でリザーブ容量を割り当てることができます。

     次のガイドラインに従ってリザーブ容量を割り当てます。

     - リザーブ容量のデフォルト設定はベースボリュームの容量の40%です。通常はこの容量で十分です。

- 必要な容量は、ボリュームに対するI/O書き込みの頻度とサイズ、およびSnapshotイメージを収集する数と期間によって異なります。

2. *オプション：*デフォルトのリザーブ容量設定を変更した場合は、*候補の更新*をクリックして、指定したリザーブ容量の候補リストを更新します。
3. [次へ]*をクリックし、に進みます手順3：Snapshot整合性グループの設定を編集する。

手順3：Snapshot整合性グループの設定を編集する

Snapshot整合性グループの自動削除に関する設定とリザーブ容量に関するアラートのしきい値を確認し、必要に応じて変更します。

タスクの内容

Snapshot整合性グループ作成手順では、グループのメンバーボリュームを選択し、メンバーボリュームに容量を割り当てることができます。

手順

1. Snapshot整合性グループのデフォルトの設定をそのまま使用するか、必要に応じて変更します。

フィールドの詳細

設定	製品説明
• Snapshot整合グループ設定*	名前
Snapshot整合性グループの名前を指定します。	次の場合にSnapshotイメージの自動削除を有効にする…
指定した上限を超えたSnapshotイメージを自動的に削除する場合は、チェックボックスをオンのままにします。上限を変更するには、スピンボックスを使用します。このチェックボックスをオフにすると、32個のイメージが作成された時点でSnapshotイメージの作成が停止します。	リザーブ容量の設定
アラートを受け取るタイミング…	このスピンボックスを使用して、Snapshot整合性グループのリザーブ容量が残り少なくなったときにシステムからアラート通知を送信する割合を調整します。 Snapshot整合性グループのリザーブ容量が指定したしきい値を超えると、事前の通知が表示され、残りのスペースがなくなる前にリザーブ容量を増やしたり不要なオブジェクトを削除したりできます。
リザーブ容量がフルになった場合のポリシー	次のいずれかのポリシーを選択します。 • 最も古い**Snapshot**イメージをパージする- Snapshot整合性グループ内の最も古いSnapshotイメージが自動的にパージされ、そのSnapshotイメージのリザーブ容量が解放されてグループ内で再利用されます。 • ベースボリュームへの書き込みを拒否--リザーブ容量の割合が定義された上限に達すると'リザーブ容量へのアクセスをトリガーしたベースボリュームに対するI/O書き込み要求はすべて拒否されます

2. Snapshot整合性グループの設定が完了したら、「*完了」をクリックします。

Snapshotボリュームの作成

ボリュームまたはSnapshot整合性グループのSnapshotイメージへのホストアクセスを提供するには、Snapshotボリュームを作成します。Snapshotボリュームは読み取り専用ま

たは読み取り/書き込みのいずれかに指定できます。

タスクの内容

Snapshotボリュームの作成手順では、SnapshotイメージからSnapshotボリュームを作成し、ボリュームが読み取り/書き込みの場合にリザーブ容量を割り当てることができます。Snapshotボリュームは次のいずれかとして指定できます。

- 読み取り専用のSnapshotボリュームは、Snapshotイメージに格納されたデータへの読み取りアクセスをホストアプリケーションに提供しますが、Snapshotイメージを変更することはできません。読み取り専用のSnapshotボリュームには、関連付けられたリザーブ容量はありません。
- 読み書き可能なSnapshotボリュームは、Snapshotイメージに含まれているデータのコピーへの書き込みアクセスをホストアプリケーションに提供します。専用のリザーブ容量が割り当てられ、ホストアプリケーションがベースボリュームに対して行った以降の変更を、参照元のSnapshotイメージに影響を与えることなく保存するために使用されます。

Snapshot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ます。

手順**1**：**Snapshot**ボリュームのメンバーを確認します

ベースボリュームまたはSnapshot整合性グループのSnapshotイメージを選択します。Snapshot整合性グループのSnapshotイメージを選択すると、確認用にSnapshot整合性グループのメンバーボリュームが表示されます。

手順

1. メニューを選択します。Storage [Snapshots]。
2. スナップショットボリューム*タブを選択します。
3. 「 * Create * 」を選択します。

   Create Snapshot Volume（スナップショットボリュームの作成）ダイアログボックスが表示されます。

4. Snapshotボリュームに変換するSnapshotイメージ（ボリュームまたはSnapshot整合性グループ）を選択し、* Next（次へ）をクリックします。**[*Filter**]フィールドのテキスト・エントリを使用して、リストを絞り込みます。

   Snapshot整合性グループのSnapshotイメージを選択した場合は、[メンバーの確認]ダイアログボックスが表示されます。

   [メンバーの確認]ダイアログ・ボックスで'スナップショット・ボリュームへの変換に選択したボリュームのリストを確認し'[次へ]をクリックします

5. にアクセスします。

手順**2**：**Snapshot**ボリュームをホストに割り当てる

特定のホストまたはホストクラスタを選択してSnapshotボリュームに割り当てます。これにより、Snapshot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。必要に応じて、あとでホストを割り当てることもできます。

開始する前に

- 有効なホストまたはホストクラスタがHostsページに表示されています。

- ホストに対してホストポート識別子を定義しておく必要があります。
- DA対応ボリュームを作成する前に、予定しているホスト接続でData Assurance（DA）機能がサポートされていることを確認してください。ストレージアレイのコントローラのいずれかのホスト接続でDAがサポートされていない場合、関連付けられているホストはDA対応ボリュームのデータにアクセスできません。

タスクの内容

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。
- ホスト割り当ては、ストレージアレイ内のSnapshotボリュームごとに1つずつ定義できます。
- 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。
- 1つのホストまたはホストクラスタからSnapshotボリュームにアクセスする際に、同じ論理ユニット番号（LUN）を2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。

ホストクラスタにボリュームを割り当てようとすると、すでに確立されている割り当てと競合しているホストクラスタへのボリュームの割り当ては失敗します。

手順

1. [ホストへの割り当て]ダイアログ・ボックスで'新しいボリュームに割り当てるホストまたはホスト・クラスタを選択しますホストを割り当てずにボリュームを作成する場合は、ドロップダウンリストから* Assign later *を選択します。
2. アクセスモードを選択します。次のいずれかを選択します。
   - 読み取り/書き込み-このオプションは、Snapshotボリュームへの読み取り/書き込みアクセスをホストに提供し、リザーブ容量を必要とします。
   - 読み取り専用-このオプションは、Snapshotボリュームへの読み取り専用アクセスをホストに提供し、リザーブ容量は不要です。
3. 「次へ」をクリックして、次のいずれかの操作を行います。
   - Snapshotボリュームが読み取り/書き込みの場合は、Review Capacity（容量の確認）ダイアログボックスが表示されます。にアクセスします。
   - Snapshotボリュームが読み取り専用の場合は、Edit Priorityダイアログボックスが表示されます。にアクセスします。

手順3：Snapshotボリューム用の容量をリザーブする

読み取り/書き込みのSnapshotボリュームにリザーブ容量を関連付けます。ベースボリュームまたはSnapshot整合性グループのプロパティに基づいて、System Managerから推奨されるボリュームと容量が提示されます。推奨されるリザーブ容量の設定をそのまま使用することも、割り当てられたストレージをカスタマイズすることもできます。

タスクの内容

Snapshotボリュームのリザーブ容量を必要に応じて増やしたり減らしたりできます。Snapshotのリザーブ容量が必要よりも多い場合は、サイズを縮小することで他の論理ボリュームに必要なスペースを解放できます。

手順

1. スピンボックスを使用して、Snapshotボリュームにリザーブ容量を割り当てます。

   [ボリューム候補]の表には、指定したリザーブ容量をサポートするボリュームだけが候補として表示されます。

   次のいずれかを実行します。

   - デフォルトの設定をそのまま使用します。

     Snapshotボリュームにデフォルトの設定でリザーブ容量を割り当てるには、このオプションを使用します（推奨）。

   - データストレージのニーズに合わせて、独自の設定でリザーブ容量を割り当てます。

     デフォルトのリザーブ容量設定を変更した場合は、*候補の更新*をクリックして、指定したリザーブ容量の候補リストを更新します。

     次のガイドラインに従ってリザーブ容量を割り当てます。

     - リザーブ容量のデフォルト設定はベースボリュームの容量の40%で、通常はこの容量で十分です。
     - 必要な容量は、ボリュームに対するI/O書き込みの頻度とサイズ、およびSnapshotイメージを収集する数と期間によって異なります。

2. *オプション：Snapshot整合性グループのSnapshotボリュームを作成する場合は、「候補の変更」オプションがリザーブ容量候補の表に表示されます。[候補の変更]をクリックして、代替リザーブ容量候補を選択します。
3. [次へ]*をクリックし、に進みます手順4：Snapshotボリュームの設定を編集する。

手順4：Snapshotボリュームの設定を編集する

名前、キャッシュ、リザーブ容量に関するアラートしきい値など、Snapshotボリュームの設定を変更します。

タスクの内容

読み取り専用のパフォーマンスを向上させる方法として、ソリッドステートディスク（SSD）キャッシュにボリュームを追加することができます。SSDキャッシュは、ストレージアレイ内で論理的にグループ化した一連のSSDドライブで構成されます。

手順

1. Snapshotボリュームの設定をそのまま使用するか、必要に応じて変更します。

フィールドの詳細

設定	製品説明
• Snapshotボリューム設定*	名前
Snapshotボリュームの名前を指定します。	SSDキャッシュの有効化
SSDで読み取り専用キャッシュを有効にする場合は、このオプションを選択します。	リザーブ容量の設定
アラートを受け取るタイミング…	*読み取り/書き込みのSnapshotボリューム*にのみ表示されます。 このスピンボックスを使用して、Snapshotグループのリザーブ容量が残り少なくなったときにシステムからアラート通知を送信する割合を調整します。 Snapshotグループのリザーブ容量が指定したしきい値を超えた場合は、事前通知を使用して、残りのスペースがなくなる前にリザーブ容量を増やしたり、不要なオブジェクトを削除したりします。

2. Snapshotボリュームの設定を確認します。[戻る]をクリックして変更を行います。
3. スナップショット・ボリュームの構成に問題がなければ'[終了]をクリックします

Snapshotスケジュールの管理

Snapshotスケジュールの設定の変更

Snapshotスケジュールでは、自動収集時間または収集の頻度を変更できます。

タスクの内容

既存のSnapshotスケジュールから設定をインポートするか、必要に応じて設定を変更できます。

SnapshotスケジュールはSnapshotグループまたはSnapshot整合性グループに関連付けられているため、スケジュールの設定を変更するとリザーブ容量に影響を及ぼす場合があります。

手順

1. メニューを選択します。Storage [Snapshots]。
2. [* Schedules （スケジュール）]タブをクリックします
3. 変更するSnapshotスケジュールを選択し、* Edit *をクリックします。

   Edit Snapshot Schedule（スナップショットスケジュールの編集）ダイアログボックスが表示されます。

4. 次のいずれかを実行します。
   - 別のスナップショットオブジェクトから以前に定義したスケジュールを使用する--*スケジュールのインポート*をクリックし、インポートするスケジュールのあるオブジェクトを選択して、*インポート*をクリックします。
   - スケジュール設定を編集--下記のフィールド詳細を参照してください。

     フィールドの詳細

設定	製品説明
日/月	次のいずれかのオプションを選択します。 • 毎日/毎週--同期スナップショットの個々の曜日を選択します日次スケジュールを設定する場合は、右上の[すべての日を選択]チェックボックスをオンにすることもできます。 • 毎月/毎年--同期スナップショットの個々の月を選択します[* on day(s)]フィールドに、同期を実行する月の日を入力します。有効なエントリは 1 ~* 31 および Last *です。複数の日にちをカンマまたはセミコロンで区切ることができます。日にちの範囲を入力するには、ハイフンを使用します。たとえば、「1、3、4」、「10-15」、「Last」のようになります。月単位のスケジュールを設定する場合は、右上の[すべての月を選択]チェックボックスをオンにすることもできます。
開始時刻	ドロップダウンリストから、日単位のSnapshotの新しい開始時刻を選択します。30分単位で選択できます。デフォルトでは、開始時刻は現在時刻の30分前に設定されます。
タイムゾーン	ドロップダウンリストから、ストレージアレイのタイムゾーンを選択します。
1日あたりのSnapshot数 Snapshotの作成間隔	1日に作成するSnapshotイメージの数を選択します。 複数を選択した場合は、復元ポイント間の時間も選択します。複数のリストアポイントを使用する場合は、十分なリザーブ容量があることを確認してください。
開始日 終了日 終了日なし	同期の開始日を入力します。終了日を入力するか、「終了日なし」を選択してください。

5. [保存（ Save ）] をクリックします。

Snapshotスケジュールのアクティブ化と一時停止

ストレージスペースを節約する必要がある場合は、スケジュールされているSnapshotイメージの収集を一時的に中断できます。この方法は、Snapshotスケジュールを削除して作成し直すよりも効率的です。

タスクの内容

スケジュールされたスナップショットアクティビティを再開するために* Activate *オプションを使用するまで'スナップショットスケジュールの状態は一時停止のままになります

手順

1. メニューを選択します。Storage [Snapshots]。
2. 表示されていない場合は、* Schedules （スケジュール）タブをクリックします。

   スケジュールの一覧が表示されます。

3. サスペンドするアクティブなスナップショットスケジュールを選択し、[**Activate/Suspend**]をクリックします。

   State列のステータスが* suspended *に変わり、SnapshotスケジュールがすべてのSnapshotイメージの収集を停止します。

4. Snapshotイメージの収集を再開するには、再開する一時停止中のSnapshotスケジュールを選択し、* Activate / Suspend *をクリックします。

   状態列のステータスが*アクティブ*に変わります。

Snapshotスケジュールの削除

Snapshotイメージを収集する必要がなくなった場合は、既存のSnapshotスケジュールを削除できます。

タスクの内容

Snapshotスケジュールを削除しても、関連付けられているSnapshotイメージは削除されません。ある時点でSnapshotイメージの収集が再開される可能性がある場合は、Snapshotスケジュールを削除するのではなく一時停止してください。

手順

1. メニューを選択します。Storage [Snapshots]。
2. [* Schedules （スケジュール）]タブをクリックします
3. 削除するSnapshotスケジュールを選択し、処理を確定します。

結果

ベースボリュームまたはSnapshot整合性グループからすべてのスケジュール設定が削除されます。

Snapshotイメージの管理

Snapshotイメージ設定の表示

各Snapshotイメージに割り当てられているプロパティ、ステータス、リザーブ容量、および関連オブジェクトを表示できます。

タスクの内容

Snapshotイメージの関連オブジェクトには、このSnapshotイメージがリストアポイントであるベースボリュームまたはSnapshot整合性グループ、関連するSnapshotグループ、およびSnapshotイメージから作成されたSnapshotボリュームが含まれます。Snapshotの設定を使用して、Snapshotイメージをコピーするか変換するかを決定します。

手順

1. メニューを選択します。Storage [Snapshots]。
2. スナップショットイメージ*タブをクリックします。
3. 表示するSnapshotイメージを選択し、* View Settings *をクリックします。

   スナップショットイメージ設定ダイアログボックスが表示されます。

4. Snapshotイメージの設定を確認します。

ベースボリュームのSnapshotイメージのロールバックの開始

ロールバック処理を実行して、Snapshotイメージに保存されている内容と一致するようにベースボリュームの内容を変更できます。

ロールバック処理では、ベースボリュームに関連付けられているSnapshotイメージの内容は変更されません。

開始する前に

- ロールバック処理を開始するための十分なリザーブ容量があります。
- 選択したSnapshotイメージとボリュームがどちらも最適な状態である必要があります。
- 選択したボリュームですでに実行中のロールバック処理がないことを確認します。

タスクの内容

ロールバックの開始手順では、ベースボリュームのSnapshotイメージに対してロールバックを開始すると同時に、ストレージ容量を追加することもできます。1つのベースボリュームに対して複数のロールバック処理を同時に開始することはできません。

ホストはロールバックされた新しいベースボリュームにすぐにアクセスできますが、ロールバックの開始後は既存のベースボリュームに読み取り/書き込みアクセスできません。リカバリ用にロールバック前のベースボリュームを保持するには、ロールバックを開始する直前にベースボリュームのSnapshotを作成します。

手順

1. メニューを選択します。Storage [Snapshots]。

2. 「* Snapshot Images *」タブを選択します。
3. Snapshotイメージを選択し、メニューからロールバック[開始]を選択します。

   ロールバックの開始の確認ダイアログボックスが表示されます。

4. *オプション：*必要に応じて、*容量を増やす*オプションを選択します。

   リザーブ容量の拡張ダイアログボックスが表示されます。

   a. スピンボックスを使用して容量の割合を調整します。

      選択したストレージオブジェクトを含むプールまたはボリュームグループに空き容量がなく、ストレージアレイに未割り当て容量がある場合は、容量を追加できます。新しいプールまたはボリュームグループを作成し、そのプールまたはボリュームグループの新しい空き容量を使用してこの処理を再試行できます。

   b. [* 拡大（ * ）] をクリックします
5. この処理を実行することを確認し、*ロールバック*をクリックします。

結果

System Managerは次の処理を実行します。

- 選択したSnapshotイメージに保存された内容を使用してボリュームをリストアします。
- ホストからロールバックされたボリュームにすぐにアクセスできるようにします。ロールバック処理が完了するまで待つ必要はありません。

終了後

ロールバック処理の進捗状況を表示するには、MENU（ホーム）：[View Operations in Progress]（進行中の処理の表示）を選択します。

ロールバック処理が失敗すると、処理は一時停止します。一時停止した処理を再開できます。それでも失敗する場合は、Recovery Guruの手順に従って問題を解決するか、テクニカルサポートにお問い合わせください。

Snapshot整合性グループメンバーボリュームの**Snapshot**イメージのロールバックの開始

ロールバック処理を実行して、Snapshotイメージに保存されている内容と一致するようにSnapshot整合性グループメンバーボリュームの内容を変更することができます。

ロールバック処理では、Snapshot整合性グループに関連付けられているSnapshotイメージの内容は変更されません。

開始する前に

- ロールバック処理を開始するための十分なリザーブ容量があります。
- 選択したSnapshotイメージとボリュームがどちらも最適な状態である必要があります。
- 選択したボリュームですでに実行中のロールバック処理がないことを確認します。

タスクの内容

ロールバックの開始手順によって、Snapshot整合性グループのSnapshotイメージに対してロールバックが開

始されます。このとき、ストレージ容量を追加することもできます。Snapshot整合性グループに対して複数のロールバック処理を同時に開始することはできません。

> ホストはロールバックされた新しいボリュームにすぐにアクセスできますが、ロールバックの開始後は既存のメンバーボリュームに読み取り/書き込みアクセスできなくなります。リカバリ用にロールバック前のベースボリュームを保持するには、ロールバックを開始する直前にメンバーボリュームのSnapshotイメージを作成します。

Snapshot整合性グループのSnapshotイメージのロールバックを開始するプロセスは複数の手順で構成されます。

手順**1**：メンバーを選択します

ロールバックするメンバーボリュームを選択する必要があります。

手順

1. メニューを選択します。Storage [Snapshots]。
2. 「* Snapshot Images *」タブを選択します。
3. Snapshot整合性グループのSnapshotイメージを選択し、メニュー：ロールバック[開始]を選択します。

   ロールバックの開始ダイアログボックスが表示されます。
4. 1つ以上のメンバーボリュームを選択します。
5. 「次へ」をクリックして、次のいずれかの操作を行います。
   - 選択したいずれかのメンバーボリュームが、Snapshotイメージを格納する複数のリザーブ容量オブジェクトに関連付けられている場合は、Review Capacity（容量の確認）ダイアログボックスが表示されます。にアクセスします。
   - 選択したメンバーボリュームのいずれも、Snapshotイメージを格納する複数のリザーブ容量オブジェクトに関連付けられていない場合は、優先度の編集ダイアログボックスが表示されます。にアクセスします。

手順**2**：容量を確認する

複数のリザーブ容量オブジェクト（Snapshotグループやリザーブ容量ボリュームなど）に関連付けられているメンバーボリュームを選択した場合は、ロールバックされたボリュームのリザーブ容量を確認して拡張できます。

手順

1. 予約済み容量が非常に少ない（またはゼロの）メンバーボリュームの横にある* Edit *列で*容量の増加*リンクをクリックします。

   リザーブ容量の拡張ダイアログボックスが表示されます。
2. スピンボックスを使用して容量の割合を調整し、*増加*をクリックします。

   選択したストレージオブジェクトを含むプールまたはボリュームグループに空き容量がなく、ストレージアレイに未割り当て容量がある場合は、容量を追加できます。新しいプールまたはボリュームグループを作成し、そのプールまたはボリュームグループの新しい空き容量を使用してこの処理を再試行できます。

3. [次へ]*をクリックし、に進みます[手順3：優先度を編集する]。

   [優先度の編集]ダイアログボックスが表示されます。

手順**3**：優先度を編集する

必要に応じて、ロールバック処理の優先度を編集できます。

タスクの内容

ロールバックの優先度によって、システムパフォーマンスを犠牲にしてロールバック処理専用に使用するシステムリソースの数が決まります。

手順

1. スライダを使用して、ロールバックの優先度を必要に応じて調整します。
2. この操作を実行することを確認し、[完了]をクリックします。

結果

System Managerは次の処理を実行します。

- 選択したSnapshotイメージに保存されている内容を使用してSnapshot整合性グループのメンバーボリュームをリストアします。
- ホストからロールバックされたボリュームにすぐにアクセスできるようにします。ロールバック処理が完了するまで待つ必要はありません。

終了後

ロールバック処理の進捗状況を表示するには、MENU（ホーム）：[View Operations in Progress]（進行中の処理の表示）を選択します。

ロールバック処理が失敗すると、処理は一時停止します。一時停止した処理を再開できます。それでも失敗する場合は、Recovery Guruの手順に従って問題を解決するか、テクニカルサポートにお問い合わせください。

Snapshotイメージのロールバックの再開

Snapshotイメージのロールバック処理中にエラーが発生した場合は、処理が自動的に一時停止します。一時停止状態のロールバック処理を再開することができます。

手順

1. メニューを選択します。Storage [Snapshots]。
2. スナップショットイメージ*タブをクリックします。
3. 一時停止中のロールバックを強調表示し、メニューからロールバック[再開]を選択します。

   処理が再開されます。

結果

System Managerは次の処理を実行します。

- ロールバック処理が正常に再開された場合は、Operations in Progressウィンドウでロールバック処理の進

捗状況を確認できます。

- ロールバック処理が失敗すると、処理は再び一時停止します。Recovery Guruの手順に従って問題を修正するか、テクニカルサポートにお問い合わせください。

Snapshotイメージのロールバックのキャンセル

進行中のアクティブなロールバック（データのアクティブなコピー）、保留中のロールバック（リソースの開始を待機している保留キュー内）、またはエラーによって一時停止されたロールバックをキャンセルできます。

タスクの内容

実行中のロールバック処理をキャンセルすると、ベースボリュームは使用できない状態に戻り、「失敗」と表示されます。したがって、ベースボリュームの内容をリストアするためのリカバリオプションがある場合にのみロールバック処理をキャンセルすることを検討してください。

> Snapshotグループに含まれている1つ以上のSnapshotイメージが自動的にパージされた場合は、ロールバック処理に使用されるSnapshotイメージを今後のロールバックで使用できなくなる可能性があります。

手順

1. メニューを選択します。Storage [Snapshots]。
2. スナップショットイメージ*タブをクリックします。
3. アクティブまたは一時停止中のロールバックを選択し、メニューからロールバック[キャンセル]を選択します。

   [ロールバックのキャンセルの確認]ダイアログボックスが表示されます。

4. 「 * はい * 」をクリックして確定します。

結果

System Managerがロールバック処理を停止します。ベースボリュームは使用可能ですが、データに整合性がないか完全でない可能性があります。

終了後

ロールバック処理をキャンセルしたら、次のいずれかの操作を実行する必要があります。

- ベースボリュームの内容を再初期化します。
- 新しいロールバック処理を実行して、ロールバックのキャンセル処理と同じSnapshotイメージまたは別のSnapshotイメージを使用してベースボリュームをリストアします。

Snapshotイメージの削除

Snapshotイメージの削除は、SnapshotグループまたはSnapshot整合性グループから最も古いSnapshotイメージをクリーンアップする場合に行います。

タスクの内容

Snapshotイメージは1つだけ削除することも、作成時のタイムスタンプが同じSnapshotイメージをSnapshot

整合性グループから削除することもできます。SnapshotグループからSnapshotイメージを削除することもできます。

関連付けられているベースボリュームまたはSnapshot整合性グループの最も古いSnapshotイメージでないSnapshotイメージは削除できません。

手順

1. メニューを選択します。Storage [Snapshots]。
2. スナップショットイメージ*タブをクリックします。
3. 削除するSnapshotイメージを選択し、処理を確定します。

   Snapshot整合性グループのSnapshotイメージを選択した場合は、削除する各メンバーボリュームを選択し、処理を確定します。

4. [削除（ Delete ）] をクリックします。

結果

System Managerは次の処理を実行します。

- ストレージアレイからSnapshotイメージを削除します。
- SnapshotグループまたはSnapshot整合性グループ内で再利用できるようにリザーブ容量が解放されます。
- 削除したSnapshotイメージに関連付けられていたSnapshotボリュームがすべて無効化されます。
- Snapshot整合性グループから削除すると、削除されたSnapshotイメージに関連付けられているメンバーボリュームが停止状態になります。

Snapshot整合性グループの管理

Snapshot整合性グループへのメンバーボリュームの追加

既存のSnapshot整合性グループに新しいメンバーボリュームを追加できます。新しいメンバーボリュームを追加する場合は、そのメンバーボリュームの容量もリザーブする必要があります。

開始する前に

- メンバーボリュームが最適lである必要があります。
- Snapshot整合性グループのボリューム数は、許容される最大ボリューム数（構成で定義）よりも少なくする必要があります。
- 各リザーブ容量ボリュームのData Assurance（DA）とセキュリティの設定は、関連付けられているメンバーボリュームと同じである必要があります。

タスクの内容

Snapshot整合性グループには、標準ボリュームまたはシンボリュームを追加できます。ベースボリュームはプールまたはボリュームグループのいずれかに配置できます。

手順

1. メニューを選択します。Storage [Snapshots]。
2. スナップショット・コンシステンシ・グループ*タブを選択します

   ストレージアレイに関連付けられているすべてのSnapshot整合性グループが表に表示されます。

3. 変更するSnapshot整合性グループを選択し、*メンバーの追加*をクリックします。

   メンバーの追加（Add Members）ダイアログボックスが表示されます。

4. 追加するメンバーボリュームを選択し、*次へ*をクリックします。

   [容量のリザーブ]手順が表示されます。[ボリューム候補]の表には、指定したリザーブ容量をサポートするボリュームだけが候補として表示されます。

5. スピンボックスを使用して、メンバーボリュームにリザーブ容量を割り当てます。次のいずれかを実行します。
   - デフォルト設定を受け入れます。

     メンバーボリュームにデフォルトの設定でリザーブ容量を割り当てるには、このオプションを使用します（推奨）。

   - データストレージのニーズに合わせて独自の設定でリザーブ容量を割り当てることができます。

     デフォルトのリザーブ容量設定を変更した場合は、*候補の更新*をクリックして、指定したリザーブ容量の候補リストを更新します。

     次のガイドラインに従ってリザーブ容量を割り当てます。

     - リザーブ容量のデフォルト設定はベースボリュームの容量の40%で、通常はこの容量で十分です。
     - 必要な容量は、ボリュームに対するI/O書き込みの頻度とサイズ、およびSnapshotイメージを収集する数と期間によって異なります。
6. [完了]をクリックして、メンバーボリュームを追加します。

Snapshot整合性グループからのメンバーボリュームの削除

既存のSnapshot整合性グループからメンバーボリュームを削除できます。

タスクの内容

Snapshot整合性グループからメンバーボリュームを削除すると、そのメンバーボリュームに関連付けられているSnapshotオブジェクトがSystem Managerによって自動的に削除されます。

手順

1. メニューを選択します。Storage [Snapshots]。
2. スナップショット・コンシステンシ・グループ*タブをクリックします
3. 変更するSnapshot整合性グループの横にあるプラス記号（+）を選択して展開します。
4. 削除するメンバーボリュームを選択し、*削除*をクリックします。
5. 操作を実行することを確認し、[削除]をクリックします。

結果

System Managerは次の処理を実行します。

- メンバーボリュームに関連付けられているSnapshotイメージとSnapshotボリュームをすべて削除します。
- メンバーボリュームに関連付けられているSnapshotグループを削除します。
- それ以外の方法でメンバーボリュームが変更または削除されることはありません。

Snapshot整合性グループの設定の変更

Snapshot整合性グループの設定では、グループ名、自動削除設定、許可されるSnapshotイメージの最大数を変更できます。

手順

1. メニューを選択します。Storage [Snapshots]。
2. スナップショット・コンシステンシ・グループ*タブをクリックします
3. 編集するSnapshot整合性グループを選択し、*表示/設定の編集*をクリックします。

   [Snapshot整合性グループ設定]ダイアログボックスが表示されます。

4. Snapshot整合性グループの設定を適宜変更します。

フィールドの詳細

設定	製品説明
• Snapshot整合グループ設定*	名前
Snapshot整合性グループの名前を変更できます。	自動削除
指定した上限を超えたSnapshotイメージを自動的に削除する場合は、チェックボックスをオンのままにします。上限を変更するには、スピンボックスを使用します。このチェックボックスをオフにすると、32個のイメージが作成された時点でSnapshotイメージの作成が停止します。	Snapshotイメージの上限
Snapshotグループで許可されるSnapshotイメージの最大数を変更できます。	Snapshotスケジュール
Snapshot整合性グループにスケジュールが関連付けられているかどうかを示します。	関連付けられたオブジェクト
メンバーボリューム	Snapshot整合性グループに関連付けられているメンバーボリュームの数を表示できます。

5. [保存（ Save ）] をクリックします。

Snapshot整合性グループの削除

不要になったSnapshot整合性グループを削除することができます。

開始する前に

すべてのメンバーボリュームのイメージがバックアップまたはテストに必要なくなったことを確認します。

タスクの内容

この処理を実行すると、Snapshot整合性グループに関連付けられているSnapshotイメージまたはスケジュールがすべて削除されます。

手順

1. メニューを選択します。Storage [Snapshots]。
2. スナップショット・コンシステンシ・グループ*タブを選択します
3. 削除するSnapshot整合性グループを選択し、メニューから「一般的でないタスク」「削除」を選択します。

   Confirm Delete Snapshot Consistency Group（スナップショット整合グループの削除の確認）ダイアログボックスが表示されます。

4. この処理を実行することを確認し、* Delete *をクリックします。

結果

System Managerは次の処理を実行します。

- Snapshot整合性グループから既存のSnapshotイメージとSnapshotボリュームをすべて削除します。
- Snapshot整合性グループの各メンバーボリュームに関連付けられているSnapshotイメージをすべて削除します。
- Snapshot整合性グループの各メンバーボリュームに関連付けられているSnapshotボリュームをすべて削除します。
- Snapshot整合性グループの各メンバーボリュームに関連付けられているリザーブ容量をすべて削除します（選択した場合）。

Snapshotボリュームの管理

Snapshotボリュームの読み取り/書き込みモードへの変換

必要に応じて、読み取り専用のSnapshotボリュームまたはSnapshot整合性グループのSnapshotボリュームを読み取り/書き込みモードに変換できます。

読み取り/書き込みアクセス可能に変換されたSnapshotボリュームには、独自のリザーブ容量が含まれます。この容量は、ホストアプリケーションによるベースボリュームに対する以降の変更を、参照元のSnapshotイメージに影響を与えることなく保存するために使用されます。

手順

1. メニューを選択します。Storage [Snapshots]。
2. スナップショットボリューム*タブを選択します。

   [Snapshotボリューム]の表に、ストレージアレイに関連付けられているすべてのSnapshotボリュームが表示されます。

3. 変換する読み取り専用Snapshotボリュームを選択し、*読み取り/書き込みに変換*をクリックします。

   読み取り/書き込みに変換ダイアログボックスが開き、予約容量*ステップが有効になります。[ボリューム候補]の表には、指定したリザーブ容量をサポートするボリュームだけが候補として表示されます。

4. 読み取り/書き込みSnapshotボリュームにリザーブ容量を割り当てるには、次のいずれかを実行します。
   - デフォルト設定を受け入れます-この推奨オプションを使用して、Snapshotボリュームのリザーブ容量をデフォルト設定で割り当てます。
   - データストレージのニーズに合わせて独自の設定でリザーブ容量を割り当てる--次のガイドラインに従ってリザーブ容量を割り当てます
     - リザーブ容量のデフォルト設定はベースボリュームの容量の40%で、通常はこの容量で十分です。
     - 必要な容量は、ボリュームに対するI/O書き込みの頻度とサイズによって異なります。
5. 設定を確認または編集するには、「次へ」を選択します。

   設定の編集ダイアログボックスが表示されます。

6. 必要に応じてSnapshotボリュームの設定をそのまま使用するか指定し、「完了」を選択してSnapshotボリュームを変換します。

   フィールドの詳細

設定	製品説明
リザーブ容量の設定	アラートを受け取るタイミング…

Snapshotボリュームのボリューム設定の変更

SnapshotボリュームまたはSnapshot整合性グループのSnapshotボリュームの設定を変更して、Snapshotボリュームの名前を変更したり、SSDキャッシングを有効または無効にしたり、ホスト、ホストクラスタ、論理ユニット番号（LUN）の割り当てを変更したりできます。

手順

1. メニューを選択します。Storage [Snapshots]。
2. スナップショットボリューム*タブをクリックします。
3. 変更するSnapshotボリュームを選択し、*表示/設定の編集*をクリックします。

   Snapshot Volume Settings（スナップショットボリューム設定）ダイアログボックスが表示されます。

4. Snapshotボリュームの設定を必要に応じて表示または編集します。

フィールドの詳細

設定	製品説明
• Snapshotボリューム*	名前
Snapshotボリュームの名前を変更できます。	割り当て先
Snapshotボリュームのホストまたはホストクラスタの割り当てを変更できます。	LUN
Snapshotボリュームのlunの割り当てを変更できます。	SSD キャッシュ
ソリッドステートディスク（SSD）の読み取り専用キャッシュを有効または無効にすることができます。	関連付けられたオブジェクト
Snapshotイメージ	Snapshotボリュームに関連付けられているSnapshotイメージを表示できます。Snapshot イメージは、ボリュームのデータを特定の時点でキャプチャした論理コピーです。リストアポイントと同様に、 Snapshot イメージを使用して既知の正常なデータセットにロールバックできます。ホストはSnapshotイメージにアクセスできますが、Snapshotイメージの読み取りや書き込みを直接行うことはできません。
ベースボリューム	Snapshotボリュームに関連付けられているベースボリュームを表示できます。ベースボリュームは、Snapshotイメージの作成元のボリュームです。シックボリュームでもシンボリュームでもかまいません。通常はホストに割り当てられます。ベースボリュームはボリュームグループまたはディスクプールのどちらかに配置できます。
Snapshotグループ	Snapshotボリュームに関連付けられているSnapshotグループを表示できます。Snapshotグループは、1つのベースボリュームのSnapshotイメージの集まりです。

Snapshotボリュームのコピー

SnapshotボリュームまたはSnapshot整合性グループのSnapshotボリュームに対して、ボリュームコピープロセスを実行できます。

タスクの内容

Snapshotボリュームは、通常のボリュームコピー処理と同様にターゲットボリュームにコピーできます。ただし、Snapshotボリュームをオンラインのままコピーすることはできません。

手順

1. メニューを選択します。Storage [Snapshots]。
2. スナップショットボリューム*タブを選択します。

   [Snapshotボリューム]の表に、ストレージアレイに関連付けられているすべてのSnapshotボリュームが表示されます。

3. コピーするSnapshotボリュームを選択し、*ボリュームコピー*を選択します。

   ボリュームコピーダイアログボックスが表示され、ターゲットを選択するように求められます。

4. コピー先として使用するターゲット・ボリュームを選択し'[終了]をクリックします

Snapshotボリュームの再作成

以前に無効にしたSnapshotボリュームまたはSnapshot整合性グループのSnapshotボリュームを再作成できます。Snapshotボリュームの再作成は、新しいボリュームを作成するよりも短時間で完了します。

開始する前に

- Snapshotボリュームの状態が最適または無効である必要があります。
- Snapshot整合性グループのSnapshotボリュームを再作成するには、メンバーであるSnapshotボリュームがすべて無効の状態である必要があります。

タスクの内容

メンバーSnapshotボリュームを個別に再作成することはできません。再作成できるのは、Snapshot整合性グループのSnapshotボリューム全体のみです。

> SnapshotボリュームまたはSnapshot整合性グループのSnapshotボリュームがオンラインコピー関係の一部である場合、ボリュームに対して再作成オプションを実行することはできません。

手順

1. メニューを選択します。Storage [Snapshots]。
2. スナップショットボリューム*タブを選択します。

   [Snapshotボリューム]の表に、ストレージアレイに関連付けられているすべてのSnapshotボリュームが表示されます。

3. 再作成するSnapshotボリュームを選択し、メニューから「一般的でないタスク」「再作成」を選択します。

   Recreate Snapshot Volume（スナップショットボリュームの再作成）ダイアログボックスが表示されます

4. 次のいずれかのオプションを選択します。

- *ボリューム<name>*から作成された既存のSnapshotイメージ

  既存のSnapshotイメージを指定してからSnapshotボリュームを再作成する場合は、このオプションを選択します。

- *ボリューム<name>*の新しい（インスタント）Snapshotイメージ

  新しいSnapshotイメージを作成してからSnapshotボリュームを再作成する場合は、このオプションを選択します。

5. [* Recreate *（再作成）]を

結果

System Managerは次の処理を実行します。

- 関連付けられているSnapshotリポジトリボリューム上のすべてのデータを削除します `write`。
- SnapshotボリュームまたはSnapshot整合性グループのSnapshotボリュームのパラメータは、以前に無効にしたボリュームのパラメータと同じままです。
- SnapshotボリュームまたはSnapshot整合性グループのSnapshotボリュームの元の名前は変更しません。

Snapshotボリュームの無効化

Snapshotボリューム、またはSnapshot整合性グループのSnapshotボリュームが不要になった場合や一時的に使用を停止する場合は、それらのボリュームを無効にすることができます。

タスクの内容

次のいずれかの条件に該当する場合は、[Disable]オプションを使用します。

- SnapshotボリュームまたはSnapshot整合性グループのSnapshotボリュームをしばらく使用しない。
- あとでSnapshotボリュームまたはSnapshot整合性グループのSnapshotボリューム（読み取り/書き込み用）を再作成する予定があり、再度作成する必要がないように関連付けられているリザーブ容量を残したい。
- 読み書き可能なSnapshotボリュームへの書き込みアクティビティを停止して、ストレージアレイのパフォーマンスを向上させたい。

SnapshotボリュームまたはSnapshot整合性グループのSnapshotボリュームが読み取り/書き込みの場合、このオプションを使用すると、関連付けられているリザーブ容量ボリュームへの以降の書き込みアクティビティも停止できます。SnapshotボリュームまたはSnapshot整合性グループのSnapshotボリュームを再作成する場合は、同じベースボリュームからSnapshotイメージを選択する必要があります。

SnapshotボリュームまたはSnapshot整合性グループのSnapshotボリュームがオンラインコピー関係の一部である場合、[無効化]オプションは実行できません。

手順

1. メニューを選択します。Storage [Snapshots]。
2. スナップショットボリューム*タブを選択します。

ストレージアレイに関連付けられているすべてのSnapshotボリュームが表示されます。

3. 無効にするSnapshotボリュームを選択し、メニューから「一般的でないタスク」「無効」を選択します。
4. 操作を実行することを確認し、[**Disable**]をクリックします。

結果

- Snapshotボリュームのベースボリュームへの関連付けは維持されます。
- SnapshotボリュームのWorld Wide Name（WWN；ワールドワイド名）は保持されます。
- 読み取り/書き込みの場合、Snapshotボリュームに関連付けられているリザーブ容量は保持されます。
- Snapshotボリュームのホストの割り当てとアクセスは保持されます。ただし、読み取り/書き込み要求は失敗します。
- SnapshotボリュームのSnapshotイメージとの関連付けは解除されます。

Snapshotボリュームの削除

バックアップまたはソフトウェアアプリケーションのテストに不要になったSnapshotボリュームまたはSnapshot整合性グループのSnapshotボリュームを削除できます。

Snapshotボリュームに関連付けられているSnapshotリザーブ容量ボリュームを削除するか、またはSnapshotリザーブ容量ボリュームを未割り当てボリュームとして残すかを指定することもできます `read-write`。

タスクの内容

ベースボリュームを削除すると、関連付けられているSnapshotボリュームまたは整合性グループのSnapshotボリュームが自動的に削除されます。ステータスが「実行中」のボリュームコピーの対象になっているSnapshotボリュームは削除できません。

手順

1. メニューを選択します。Storage [Snapshots]。
2. スナップショットボリューム*タブを選択します。

   ストレージアレイに関連付けられているすべてのSnapshotボリュームが表示されます。

3. 削除するSnapshotボリュームを選択し、メニューから「一般的でないタスク」「削除」を選択します。
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

System Managerは次の処理を実行します。

- メンバーであるSnapshotボリュームをすべて削除します（Snapshot整合性グループのSnapshotボリュームの場合）。
- 関連付けられているホスト割り当てをすべて削除します。

FAQ

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DAが有効なSnapshotボリュームをData Assurance（DA）に対応していないホストに割り当てることはできません。DAに対応していないホストにSnapshotボリュームを割り当てるには、ベースボリュームで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に対応していないI/Oインターフェイスを介してストレージアレイに接続されているホストはDAに対応していません。
- ホストメンバーが1つでもDA対応でない場合、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、およびミラーに関連付けられているボリュームでは、DAを無効にすることはできません。ベースボリュームでDAを無効にする前に、関連付けられているリザーブ容量とSnapshotオブジェクトをすべて削除する必要があります。

Snapshotイメージとは何ですか？

Snapshotイメージは、ボリュームの内容を特定の時点でキャプチャした論理コピーです。Snapshotイメージは最小限のストレージスペースを使用します。

Snapshotイメージのデータは次のように格納されます。

- Snapshotイメージが作成されると、ベースボリュームと完全に一致します。Snapshotの作成後、ベースボリューム上のいずれかのブロックまたはブロックセットに対する最初の書き込み要求が発生すると、新しいデータがベースボリュームに書き込まれる前に元のデータがSnapshotリザーブ容量にコピーされます。
- 以降のSnapshotには、最初のSnapshotイメージの作成後に変更されたデータブロックのみが含まれます。以降のcopy-on-write処理では、新しいデータがベースボリュームに書き込まれる前に、ベースボリュームで上書きされる元のデータがSnapshotリザーブ容量に保存されます。

Snapshotイメージを使用する理由

Snapshotを使用すると、偶然または悪意のある行為によるデータの損失や破損からデータを保護し、リカバリすることができます。

ベースボリュームまたはベースボリュームのグループ（Snapshot整合性グループ）を選択し、次のいずれかの方法でSnapshotイメージをキャプチャします。

- 1つのベースボリューム、または複数のベースボリュームで構成されるSnapshot整合性グループのSnapshotイメージを作成できます。
- 手動でSnapshotを作成するか、ベースボリュームまたはSnapshot整合性グループのスケジュールを作成して定期的なSnapshotイメージを自動的にキャプチャすることができます。
- ホストからアクセス可能なSnapshotイメージのSnapshotボリュームを作成できます。
- ロールバック処理を実行してSnapshotイメージをリストアできます。

複数のSnapshotイメージがリストアポイントとして保持され、特定の時点の既知の有効なデータセットにロ

ールバックできます。ロールバック機能により、偶発的なデータ削除やデータ破損からデータを保護できます。

Snapshotにはどのような種類のボリュームを使用できますか。

Snapshotイメージの格納に使用できるボリュームは、標準ボリュームとシンボリュームだけです。標準以外のボリュームは使用できません。ベースボリュームはプールまたはボリュームグループのいずれかに配置できます。

Snapshot整合性グループを作成するのはどのような場合ですか？

複数のボリュームに同時にSnapshotイメージが作成されるようにするには、Snapshot整合性グループを作成します。

たとえば、リカバリ目的で整合性を保つ必要がある複数のボリュームで構成されるデータベースが該当します。この場合、すべてのボリュームのSnapshotを同時に収集し、収集したSnapshotを使用してデータベース全体をリストアするために、Snapshot整合性グループが必要です。

Snapshot整合性グループに含まれるボリュームのことを_member volume__と呼びます。

Snapshot整合性グループに対して次のSnapshot処理を実行できます。

- メンバーボリュームの同時イメージを取得するには、Snapshot整合性グループのSnapshotイメージを作成します。
- メンバーボリュームの定期的な同時イメージを自動的にキャプチャするように、Snapshot整合性グループのスケジュールを作成します。
- ホストからアクセス可能なSnapshot整合性グループイメージのSnapshotボリュームを作成します。
- Snapshot整合性グループのロールバック処理を実行する。

Snapshotボリュームとは何ですか？また、リザーブ容量が必要になるのはいつですか？

Snapshotボリュームを使用すると、ホストはSnapshotイメージのデータにアクセスできます。Snapshotボリュームには独自のリザーブ容量が含まれているため、元のSnapshotイメージに影響を与えることなくベースボリュームへの変更が保存されます。Snapshotイメージに対するホストからの読み取りまたは書き込みはできません。Snapshotデータの読み取りまたは書き込みを行う場合は、Snapshotボリュームを作成してホストに割り当てます。

2種類のSnapshotボリュームを作成できます。Snapshotボリュームのタイプによって、リザーブ容量を使用するかどうかが決まります。

- 読み取り専用--読み取り専用として作成されたスナップショット・ボリュームは'スナップショット・イメージに含まれるデータのコピーへの読み取りアクセスをホスト・アプリケーションに提供します読み取り専用のSnapshotボリュームはリザーブ容量を使用しません。
- 読み取り/書き込み-読み書き可能として作成されたSnapshotボリュームでは、参照されているSnapshotイメージに影響を与えることなくSnapshotボリュームに変更を加えることができます。読み書き可能なSnapshotボリュームは、リザーブ容量を使用してこの変更を格納します。読み取り専用のSnapshotボリュームは、いつでも読み書き可能ボリュームに変換できます。

Snapshotグループとは何ですか？

Snapshotグループは、関連付けられている1つのベースボリュームのポイントインタイムSnapshotイメージの集まりです。

System Managerでは、Snapshotイメージを_ Snapshotグループ_に編成します。Snapshotグループに対するユーザの操作は必要ありませんが、Snapshotグループではリザーブ容量をいつでも調整できます。また、次の条件に該当する場合は、リザーブ容量の作成を求められることがあります。

- Snapshotグループがまだ作成されていないベースボリュームのSnapshotを作成すると、System ManagerによってSnapshotグループが自動的に作成されます。これにより、ベースボリューム用のリザーブ容量が作成され、以降のSnapshotイメージの格納に使用されます。
- ベースボリュームのSnapshotスケジュールを作成すると、System ManagerによってSnapshotグループが自動的に作成されます。

Snapshotボリュームを無効にするのはどのような場合ですか？

Snapshotイメージに別のSnapshotボリュームを割り当てる場合は、Snapshotボリュームを無効にします。無効にしたSnapshotボリュームは、あとで使用できます。

Snapshotボリュームまたは整合性グループのSnapshotボリュームが不要になり、あとで再作成する予定がない場合は、無効にする代わりにボリュームを削除してください。

Disabled状態とは何ですか。

無効状態のSnapshotボリュームは、現在Snapshotイメージに割り当てられていません。Snapshotボリュームを有効にするには、再作成処理を使用して無効なSnapshotボリュームに新しいSnapshotイメージを割り当てる必要があります。

Snapshotボリュームの特性は、割り当てられているSnapshotイメージによって定義されます。無効ステータスのSnapshotボリュームで読み取り/書き込みアクティビティが中断されています。

Snapshotスケジュールを一時停止するのはどのような場合ですか？

スケジュールを一時停止すると、スケジュールされたSnapshotイメージの作成は実行されません。ストレージスペースを節約するためにSnapshotスケジュールを一時停止してから、スケジュールされたSnapshotをあとから再開できます。

Snapshotスケジュールが不要な場合は、スケジュールを一時停止するのではなく削除してください。

ミラーリング

概要

非同期ミラーリングの概要

非同期ミラーリング機能は、ローカルストレージアレイとリモートストレージアレイの間でデータをレプリケーションするための、コントローラレベルのファームウェアベー

スのメカニズムを提供します。

非同期ミラーリングとは

非同期ミラーリング_は、特定の時点におけるプライマリボリュームの状態をキャプチャし、前回のイメージキャプチャ以降に変更されたデータのみをコピーします。プライマリサイトはただちに更新でき、セカンダリサイトは帯域幅の許す限り更新できます。情報はキャッシュされ、あとでネットワークリソースが利用可能になると送信されます。

非同期ミラーリングはボリューム単位で作成されますが、グループレベルで管理されるため、個別のリモートミラーボリュームを特定のストレージアレイ上の任意のプライマリボリュームに関連付けることができます。このタイプのミラーリングはノンストップオペレーションの要求を満たすのに最適です。一般に、定期的なプロセスをはるかに効率的に実行できます。

詳細：

- "非同期ミラーリングの仕組み"
- "非同期ミラーリングに関する用語"
- "非同期ミラーのステータス"
- "ボリューム所有権"
- "ミラー整合性グループのロール変更"

非同期ミラーリングを設定するにはどうすればよいですか？

アレイ間の初期ミラーリングの設定は、Unified Managerインターフェイスを使用して実行する必要があります。設定が完了したら、System Managerでミラーペアと整合グループを管理できます。

詳細：

- "非同期ミラーリングを使用するための要件"
- "ホリユウムノヒトウキミラアリンクワアクフロオ"
- "非同期ミラーペアの作成（Unified Manager）"

関連情報

非同期ミラーリングに関連する概念の詳細については、以下を参照してください。

- "ミラー整合性グループを作成する際の注意事項"
- "ミラーペアを作成する際の注意事項"
- "非同期ミラーリングと同期ミラーリングの違い"

同期ミラーリングの概要

同期ミラーリング機能は、遠隔地にあるストレージアレイ間で、オンラインのリアルタイムデータレプリケーションを提供します。

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。

同期ミラーリングとは

_Synchronousミラーリング_データボリュームをリアルタイムで複製して、継続的な可用性を確保します。ミラーリング処理はストレージアレイコントローラによって管理され、ホストマシンやソフトウェアアプリケーションからは透過的に実行されます。

このタイプのミラーリングは、ディザスタリカバリなどのビジネス継続性の目的に最適です。

詳細：

- "同期ミラーリングの仕組み"
- "同期ミラーリングに関する用語"
- "同期ミラーリングのステータス"
- "ボリューム所有権"
- "ミラーペア内のボリューム間でのロール変更"

同期ミラーリングを設定するにはどうすればよいですか？

アレイ間の初期ミラーリングの設定は、Unified Managerインターフェイスを使用して実行する必要があります。設定後は、System Managerでミラーペアを管理できます。

詳細：

- "同期ミラーリングを使用するための要件"
- "ボリュームを同期的にミラーリングするためのワークフロー"
- "同期ミラーペアの作成（Unified Manager）"

関連情報

同期ミラーリングに関連する概念の詳細については、以下を参照してください。

- "ミラーペアを作成する際の注意事項"
- "非同期ミラーリングと同期ミラーリングの違い"

非同期の概念

非同期ミラーリングの仕組み

非同期ミラーリングでは、データボリュームがオンデマンドまたはスケジュールに基づいてコピーされるため、データの破損や損失が原因で発生するダウンタイムを最小限または回避できます。

非同期ミラーリングでは、特定の時点におけるプライマリボリュームの状態がキャプチャされ、前回のイメージキャプチャ以降に変更されたデータだけがコピーされます。プライマリサイトはただちに更新でき、セカンダリサイトは帯域幅の許す限り更新できます。情報はキャッシュされ、あとでネットワークリソースが利用可能になると送信されます。

このタイプのミラーリングはノンストップオペレーションの要求を満たすのに最適であり、一般に、バックア

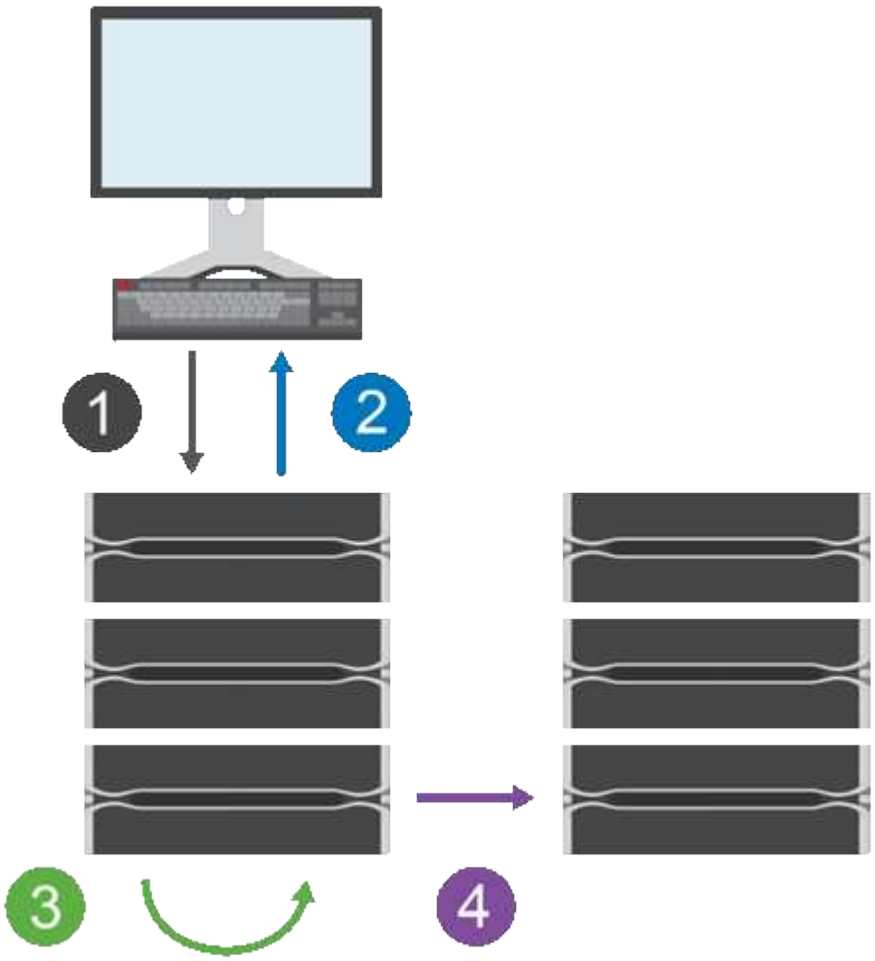
ップやアーカイブなどの定期的なプロセスをはるかにネットワーク効率よく実行できます。非同期ミラーリングを使用する理由は次のとおりです。

- リモートバックアップの統合：
- 局地災害や広域災害に対する保護
- 本番データのある時点におけるイメージを使用したアプリケーションの開発とテスト

非同期ミラーリングセッション

非同期ミラーリングでは、特定の時点におけるプライマリボリュームの状態がキャプチャされ、前回のイメージキャプチャ以降に変更されたデータだけがコピーされます。非同期ミラーリングを使用すると、プライマリサイトはただちに更新でき、セカンダリサイトは帯域幅に余裕があれば更新できます。情報はキャッシュされ、あとでネットワークリソースが利用可能になると送信されます。

アクティブな非同期ミラーリングセッションには、主に4つの手順があります。



1. 書き込み処理は最初にプライマリボリュームのストレージアレイで実行されます。
2. 処理のステータスがホストに返されます。
3. プライマリボリュームでのすべての変更がログに記録され、追跡されます。
4. すべての変更が、バックグラウンドプロセスとしてセカンダリボリュームのストレージアレイに送信されます。

これらの手順は、定義した同期間隔で繰り返されます。また、間隔が定義されていない場合は、手動で繰り返すこともできます。

非同期ミラーリングでは、設定された間隔でのみデータがリモートサイトに転送されるため、ローカルI/Oへの影響は低速なネットワーク接続による影響と同程度で済みます。この転送はローカルI/Oには関連付けられないため、アプリケーションのパフォーマンスには影響しません。したがって、非同期ミラーリングでは、iSCSIなどの低速な接続を使用して、ローカルとリモートのストレージシステム間で長距離にわたって実行することができます。

ストレージアレイのファームウェアバージョンが7.84以上である必要があります。（それぞれ異なるOSバージョンを実行できます）。

ミラー整合性グループとミラーペア

ミラー整合性グループを作成して、ローカルストレージアレイとリモートストレージアレイの間にミラーリング関係を確立します。非同期ミラーリング関係は、ミラーペア（あるストレージアレイ上のプライマリボリュームと別のストレージアレイ上のセカンダリボリューム）で構成されます。

プライマリボリュームを含むストレージアレイは、通常はプライマリサイトにあり、アクティブなホストに対応します。セカンダリボリュームを含むストレージアレイは、通常はセカンダリサイトにあり、データのレプリカを格納します。セカンダリボリュームには通常、データのバックアップコピーが格納され、ディザスタリカバリに使用されます。

同期の設定

ミラーペアを作成するときは、同期優先度と再同期ポリシーも定義します。通信が中断した場合、ミラーペアはこれらを使用して再同期処理を完了します。

ミラー整合性グループを作成するときは、グループ内のすべてのミラーペアの同期優先度と再同期ポリシーも定義します。ミラーペアは、同期優先度と再同期ポリシーを使用して、通信の中断後に再同期処理を完了します。

プライマリボリュームのストレージアレイがセカンダリボリュームにデータを書き込むことができない場合、ミラーペアのプライマリボリュームとセカンダリボリュームが非同期になる可能性があります。この状況は、次の問題が原因で発生する可能性があります。

- ローカルストレージアレイとリモートストレージアレイ間のネットワークの問題。
- セカンダリボリュームに障害が発生した。
- ミラーペアの同期を手動で中断しています。
- ミラーグループのロールの競合。

リモートストレージアレイ上のデータは、手動または自動で同期できます。

リザーブ容量と非同期ミラーリング

リザーブ容量は、同期が行われていないときにプライマリボリュームとセカンダリボリュームの間の差異を追跡するために使用します。また、各ミラーペアの同期の統計も追跡します。

ミラーペアのボリュームごとに専用のリザーブ容量が必要です。

2つのアレイ間のミラーリングを有効にして設定するには、Unified Managerインターフェイスを使用する必要があります。ミラーリングを有効にすると、System Managerでミラーペアと同期設定を管理できます。

非同期ミラーリングに関する用語

ストレージアレイに関連する非同期ミラーリングの用語を次に示します。

期間	製品説明
ローカルストレージアレイ	ローカルストレージアレイは、操作の対象となるストレージアレイです。 Local Role列に* Primary と表示された場合は、ミラー関係のプライマリロールが割り当てられたボリュームがストレージアレイに含まれていることを示しています。**Local Role**列に「 Secondary」と表示されている場合、ストレージアレイにミラー関係のセカンダリロールが割り当てられたボリュームが含まれていることを示しています。
ミラー整合性グループ	ミラー整合性グループは、1つ以上のミラーペアのコンテナです。非同期ミラーリング処理では、ミラー整合性グループを作成する必要があります。
ミラーペア	ミラーペアは、プライマリボリュームとセカンダリボリュームの2つのボリュームで構成されます。 非同期ミラーリングでは、ミラーペアは常にミラー整合性グループに属します。書き込み処理は最初にプライマリボリュームに対して実行され、次にセカンダリボリュームにレプリケートされます。ミラー整合性グループ内の各ミラーペアでは、同じ同期設定が共有されます。
プライマリボリューム	ミラーペアのプライマリボリュームは、ミラーリングするソースボリュームです。
リモートストレージアレイ	通常、リモートストレージアレイはセカンダリサイトとして指定され、セカンダリサイトにはミラーリング構成のデータのレプリカが格納されます。
リザーブ容量	リザーブ容量は、コピーサービス処理やストレージオブジェクトに使用される物理割り当て容量です。ホストから直接読み取ることはできません。
ロール変更	ロール変更では、セカンダリボリュームにプライマリロールが割り当てられ、セカンダリボリュームにプライマリロールが割り当てられます。
セカンダリボリューム	ミラーペアのセカンダリボリュームは、通常はセカンダリサイトに配置され、データのレプリカが格納されます。

期間	製品説明
同期	同期は、ローカルストレージアレイとリモートストレージアレイの間の初期同期で実行されます。同期は、通信の中断後にプライマリボリュームとセカンダリボリュームが同期されていない状態になった場合にも実行されます。通信リンクの動作が再開されると、レプリケートされていないデータがセカンダリボリュームのストレージアレイに同期されます。

ホリユウムノヒトウキミラアリンクワアクフロオ

次のワークフローを使用して非同期ミラーリングを設定します。

1. Unified Managerで初期設定を実行します。
   a. データ転送元としてローカルストレージアレイを選択します。
   b. ミラー整合性グループを作成または選択します。ミラー整合性グループは、ローカルアレイ上のプライマリボリュームとリモートアレイ上のセカンダリボリュームのコンテナです。プライマリ ボリュームとセカンダリ ボリュームは「ミラー ペア」と呼ばれます。ミラー整合性グループを初めて作成する場合は、実行する同期方法（手動またはスケジュール）を指定します。
   c. ローカルストレージアレイからプライマリボリュームを選択し、リザーブ容量を確認します。リザーブ容量は、コピー処理に使用される物理割り当て容量です。
   d. 転送先としてリモートストレージアレイを選択し、セカンダリボリュームを選択して、リザーブ容量を確認します。
   e. プライマリボリュームからセカンダリボリュームへの初回のデータ転送を開始します。ボリュームサイズによっては、この初回転送に数時間かかることがあります。
2. 初期同期の進捗状況を確認します。
   a. Unified Managerで、ローカルアレイのSystem Managerを起動します。
   b. System Managerで、ミラーリング処理のステータスを確認します。ミラーリングが完了すると、ミラーペアのステータスは「最適」になります。
3. *オプション：*以降のデータ転送については、System Managerでスケジュールを再設定したり、手動で実行したりできます。新しいブロックと変更されたブロックだけがプライマリボリュームからセカンダリボリュームに転送されます。

> 非同期レプリケーションは定期的に行われるため、変更されたブロックを統合してネットワーク帯域幅を節約できます。書き込みスループットと書き込みレイテンシへの影響は最小限に抑えられます。

非同期ミラーリングを使用するための要件

非同期ミラーリングを使用する場合は、次の要件に注意してください。

Unified Manager

2つのアレイ間のミラーリングを有効にして設定するには、Unified Managerインターフェイスを使用する必要があります。Unified Managerは、Web Services Proxyとともにホストシステムにインストールされます。

- Web Services Proxyサービスが実行されている必要があります。

- Unified ManagerがHTTPS接続経由でローカルホストで実行されている必要があります。
- Unified Managerにストレージアレイの有効なSSL証明書が表示されている必要があります。Unified Managerのメニューから「Certificate Management」に移動し、自己署名証明書を受け入れるか、独自のセキュリティ証明書をインストールできます。

ストレージアレイ

- 2つのストレージアレイが必要です。
- 各ストレージアレイに2台のコントローラが必要です。
- Unified Managerで2つのストレージアレイが検出されている必要があります。
- プライマリアレイとセカンダリアレイの両方の各コントローラにイーサネット管理ポートが設定され、ネットワークに接続されている必要があります。
- ストレージアレイに必要なファームウェアの最小バージョンは7.84です（それぞれ異なるOSバージョンを実行できます）。
- ローカルとリモートのストレージアレイのパスワードを確認しておく必要があります。
- ミラーリングするプライマリボリューム以上のセカンダリボリュームを作成するには、リモートストレージアレイに十分な空き容量が必要です。
- ローカルとリモートのストレージアレイをFibre ChannelファブリックまたはiSCSIインターフェイスを介して接続します。

サポートされる接続

非同期ミラーリングでは、ローカルとリモートのストレージシステム間の通信にFC接続、iSCSI接続、またはその両方を使用できます。ミラー整合性グループを作成するときに、リモートストレージアレイにFCとiSCSIの両方が接続されている場合は、そのグループでどちらかを選択できます。1つのチャネルタイプからもう1つのチャネルタイプへのフェールオーバーはありません。

非同期ミラーリングでは、ストレージアレイのホスト側I/Oポートを使用して、ミラーリングされたデータがプライマリ側からセカンダリ側に転送されます。

- * Fibre Channel（FC）インターフェイス経由のミラーリング*

  ストレージアレイの各コントローラでは、最も番号が大きいFCホストポートがミラーリング処理の専用ポートとして使用されます。

  ベースのFCポートとホストインターフェイスカード（HIC）のFCポートの両方があるコントローラでは、HICの最も番号が大きいポートが使用されます。専用ポートにログオンしたホストはログアウトされ、ホストログイン要求は許可されません。このポートでのI/O要求は、ミラーリング処理の対象となるコントローラからのみ許可されます。

  専用のミラーリングポートは、ディレクトリサービスとネームサービスのインターフェイスをサポートするFCファブリック環境に接続されている必要があります。特に、FC-ALおよびポイントツーポイントはミラー関係が確立されたコントローラ間の接続オプションとしてサポートされないことに注意してください。

- * iSCSIインターフェイス経由のミラーリング*

  FCとは異なり、iSCSIでは専用のポートを必要としません。iSCSI環境で非同期ミラーリングを使用する場合、ストレージアレイのどのフロントエンドiSCSIポートも非同期ミラーリング専用にする必要はあり

ません。これらのポートは、非同期ミラーリングのトラフィックとホスト/アレイ間のI/O接続で共有されます。

コントローラはリモートストレージシステムのリストを管理しており、iSCSIイニシエータはこのリストを使用してセッションの確立を試みます。iSCSI接続の確立に成功した最初のポートは、そのリモートストレージアレイとの以降のすべての通信に使用されます。通信に失敗すると、使用可能なすべてのポートを使用して新しいセッションの確立が試行されます。

iSCSIポートは、アレイレベルでポート単位で設定します。設定メッセージおよびデータ転送用のコントローラ間通信では、次の設定を含むグローバル設定が使用されます。

- VLAN：ローカルシステムとリモートシステムが通信するためには、両方のシステムでVLAN設定が同じである必要があります
- iSCSIリスニングポート
- ジャンボフレーム
- イーサネットの優先順位

> コントローラ間のiSCSI通信には、管理イーサネットポートではなくホスト接続ポートを使用する必要があります。

非同期ミラーリングでは、ストレージアレイのホスト側I/Oポートを使用して、ミラーリングされたデータがプライマリ側からセカンダリ側に転送されます。非同期ミラーリングは高レイテンシで低コストのネットワーク向けであるため、iSCSI接続（つまりTCP/IPベース）が適しています。iSCSI環境で非同期ミラーリングを使用する場合、アレイのどのフロントエンドiSCSIポートも非同期ミラーリング専用にする必要はありません。これらのポートは、非同期ミラーリングのトラフィックとホスト/アレイ間のI/O接続で共有されます。

ミラーボリュームの候補

- 非同期ミラーペアのプライマリボリュームとセカンダリボリュームでは、RAIDレベル、キャッシングパラメータ、およびセグメントサイズが異なる場合があります。

> EF600およびEF300コントローラでは、非同期ミラーペアのプライマリボリュームとセカンダリボリュームのプロトコル、トレイレベル、セグメントサイズ、セキュリティタイプ、およびRAIDレベルが同じである必要があります。対応していない非同期ミラーペアは、使用可能なボリュームのリストに表示されません。

- セカンダリボリュームは、プライマリボリュームと同じサイズ以上である必要があります。
- ボリュームに設定できるミラー関係は1つだけです。
- ボリュームの候補は、同じデータセキュリティ機能を共有する必要があります。
  - プライマリボリュームがFIPSに対応している場合、セカンダリボリュームはFIPSに対応している必要があります。
  - プライマリボリュームがFDEに対応している場合、セカンダリボリュームはFDEに対応している必要があります。
  - プライマリボリュームでドライブセキュリティを使用していない場合、セカンダリボリュームでドライブセキュリティを使用していない必要があります。
- プライマリボリュームとセカンダリボリュームで同じドライブタイプを共有する必要があります。プライ

マリボリュームとセカンダリボリュームにNVMeドライブとSASドライブを混在させることはできません。

リザーブ容量

- コントローラのリセットおよびその他の一時的な中断からリカバリするための書き込み情報をログに記録するには、ミラーペアのプライマリボリュームとセカンダリボリュームにリザーブ容量ボリュームが必要です。
- ミラーペアのプライマリボリュームとセカンダリボリュームには追加のリザーブ容量が必要であるため、ミラー関係にある両方のストレージアレイに空き容量が確保されていることを確認してください。
- リザーブ容量ボリュームは、関連付けられているミラーボリュームと同じドライブタイプを共有する必要があります。
  - リザーブ容量ボリュームをNVMeドライブに作成する場合は、そのミラーボリュームもNVMeドライブに作成する必要があります。
  - リザーブ容量ボリュームをSASドライブに作成する場合は、そのミラーボリュームもSASドライブに作成する必要があります。

ドライブセキュリティ機能

- セキュリティ対応ドライブを使用する場合、プライマリボリュームとセカンダリボリュームのセキュリティ設定に互換性がある必要があります。この制限は強制的には適用されないため、自分で確認する必要があります。
- セキュリティ対応ドライブを使用する場合、プライマリボリュームとセカンダリボリュームで同じタイプのドライブを使用する必要があります。この制限は強制的には適用されないため、自分で確認する必要があります。
- Data Assurance（DA）を使用する場合、プライマリボリュームとセカンダリボリュームでDA設定を同じにする必要があります。

非同期ミラーのステータス

ミラーステータスは、ミラー整合性グループとミラーボリュームペアの状態を定義します。

ミラー整合性グループのステータス

ステータス	製品説明
同期（初期同期）	ミラーボリュームペア間で完了した初期データ同期の進捗状況。 初期同期中に、ボリュームは、デグレード/失敗/最適/不明の各状態に移行できます。
同期（間隔同期）	ミラーボリュームペア間で完了した定期的なデータ同期の進捗状況。

ステータス	製品説明
システム中断	ミラー整合性グループレベルで、すべてのミラーペアについて、データの同期がストレージシステムによって一時停止された状態。 ミラー整合性グループ内の少なくとも1つのミラーペアが停止または障害状態です。
ユーザによる中断	ミラー整合性グループレベルで、すべてのミラーペアについて、データの同期がユーザによって一時停止されました。 この状態は、ホストアプリケーションのパフォーマンスへの影響（ローカルストレージアレイで変更されたデータがリモートストレージアレイにコピーされるときに発生する可能性があります）を削減するのに役立ちます。
一時停止	リモートストレージアレイへのアクセス中にエラーが発生したため、データ同期プロセスが一時停止しました。
孤立	孤立したミラーペアボリュームは、整合性ミラーグループの一方（プライマリまたはセカンダリ）で整合性ミラーグループのメンバーボリュームが削除され、もう一方では削除されていない場合に発生します。 孤立したミラーペアボリュームは、アレイ間の通信がリストアされ、ミラー構成の両サイドでミラーパラメータが調整されたときに検出されます。 ミラーペアを削除すると、孤立したミラーペアの状態を修正できます。
ロール変更を保留中/実行中	ミラー整合性グループ間のロールの変更が保留中または進行中です。 ロールを（プライマリロールまたはセカンダリロールに）反転すると、選択したミラー整合性グループ内のすべての非同期ミラーペアに反映されます。 保留中のロール変更はキャンセルできますが、進行中のロール変更はキャンセルできません。
ロールの競合	ロール変更処理中にローカルストレージアレイとリモートストレージアレイの間の通信に問題が発生したため、ミラー整合性グループ間でロールの競合が発生しました。 通信の問題が解決されると、ロールの競合が発生します。Recovery Guruを使用してこのエラーを解決してください。 ロールの競合を解決する場合、強制昇格は許可されません。

ミラアヘアノステエタス

ミラーペアのステータスは、プライマリボリュームとセカンダリボリュームのデータが同期されているかどうかを示します。

ステータス	製品説明
トウキ	ミラーペア間で完了した初期または定期的なデータ同期の進捗状況。 同期には、初期同期と定期的同期の2種類があります。初期同期の進捗状況は、[Long Running Operations]ダイアログボックスにも表示されます。
最適	ミラーペア内のボリュームが同期されています。これは、ストレージアレイ間の接続が動作していて、各ボリュームが適切な動作状態にあることを示しています。
不完全	System Managerでサポートされていないストレージアレイでミラーペアの作成手順が開始され、セカンダリでミラーペアが完了していないため、リモートストレージアレイ上の非同期ミラーペアが不完全です。 ミラーペアの作成プロセスは、リモートストレージアレイ上のミラー整合性グループにボリュームを追加すると完了します。このボリュームが非同期ミラーペアのセカンダリボリュームになります。 リモートストレージアレイがSystem Managerで管理されている場合、ミラーペアは自動的に完了します。
失敗	プライマリボリューム、セカンダリボリューム、またはミラーのリザーブ容量で障害が発生したため、非同期ミラーリング処理を正常に実行できません。
孤立	孤立したミラーペアボリュームは、整合性ミラーグループの一方（プライマリまたはセカンダリ）で整合性ミラーグループのメンバーボリュームが削除され、もう一方では削除されていない場合に発生します。 孤立したミラーペアボリュームは、2つのストレージアレイ間の通信がリストアされ、ミラー構成の両側でミラーパラメータが調整されると検出されます。 ミラーペアを削除すると、孤立したミラーペアの状態を修正できます。
停止	ミラー整合性グループがシステムによって中断された状態であるため、ミラーペアは停止状態です。

ボリューム所有権

ミラーペアの優先コントローラ所有者を変更できます。

ミラーペアのプライマリボリュームがコントローラAに所有されている場合、セカンダリボリュームもリモートストレージアレイのコントローラAに所有されます。プライマリボリュームの所有者を変更すると、セカンダリボリュームの所有者が自動的に変更され、両方のボリュームが同じコントローラで所有されるようになります。プライマリ側で現在の所有権が変更されると、セカンダリ側の対応する所有権も自動的に変更されます。

たとえば、コントローラAが所有するプライマリ ボリュームの所有者をコントローラBに変更したとします。この場合、次回のリモート書き込み時に、セカンダリ ボリュームの所有者がコントローラAからコントローラBに切り替わります。セカンダリ側のコントローラ所有権の切り替えはプライマリ側で制御されるため、ス

トレージ管理者による特別な対応は必要ありません。

コントローラのリセット

コントローラをリセットすると、プライマリ側でボリューム所有権が優先コントローラ所有者からストレージアレイ内の代替コントローラに変更されます。

セカンダリボリュームへの書き込み前に、コントローラのリセットやストレージアレイの電源の再投入によってリモート書き込みが中断されることがあります。この場合、コントローラでミラーペアの完全同期を実行する必要はありません。

コントローラのリセット中にリモートの書き込みが中断されると、プライマリ側の新しいコントローラ所有者は、優先コントローラ所有者のリザーブ容量ボリューム内のログファイルに格納されている情報を読み取ります。その後、新しいコントローラ所有者は、影響を受けたデータブロックをプライマリボリュームからセカンダリボリュームにコピーします。これにより、ミラーボリュームの完全な同期が不要になります。

ミラー整合性グループのロール変更

ミラー整合性グループ内のミラーペア間でロールを変更できます。そのためには、プライマリミラー整合性グループをセカンダリロールに降格するか、セカンダリミラー整合性グループをプライマリロールに昇格します。

ロール変更処理に関する次の情報を確認してください。

- ロール変更は、選択したミラー整合性グループ内のすべてのミラーペアに反映されます。
- ミラー整合性グループがセカンダリロールに降格されると、そのミラー整合性グループ内のすべてのミラーペアもセカンダリロールに降格されます。その逆も同様です。
- プライマリミラー整合性グループがセカンダリロールに降格されると、そのグループ内のメンバーボリュームに割り当てられているホストはそのグループに書き込みアクセスできなくなります。
- ミラー整合性グループがプライマリロールに昇格されると、そのグループ内のメンバーボリュームにアクセスしているホストがそのグループに書き込むことができるようになります。
- ローカルストレージアレイがリモートストレージアレイと通信できない場合は、ローカルストレージアレイで強制的にロールを変更できます。

強制的なロール変更

ローカルストレージアレイとリモートストレージアレイ間の通信の問題により、セカンダリミラー整合性グループ内のメンバーボリュームの昇格やプライマリミラー整合性グループ内のメンバーボリュームの降格を実行できない場合は、ミラー整合性グループ間で強制的にロールを変更できます。

セカンダリ側のミラー整合性グループを強制的にプライマリロールに移行できます。これで、リカバリホストはそのミラー整合性グループ内で新しく昇格されたメンバーボリュームにアクセスできるようになり、業務を続行できます。

強制昇格が許可される場合と許可されない場合

ミラー整合性グループの強制昇格は、ミラー整合性グループのすべてのメンバーボリュームが同期され、整合性のあるリカバリポイントがある場合にのみ許可されます。

次の状況では、ミラー整合性グループの強制昇格が許可されません。

- ミラー整合性グループのいずれかのメンバーボリュームが初期同期中です。
- ミラー整合性グループのメンバーボリュームにリカバリポイントのポイントインタイムイメージがない（リザーブ容量のフルエラーなどが原因）。
- ミラー整合性グループにメンバーボリュームが含まれていません。
- ミラー整合性グループが失敗、Role-Change-Pending、Role-Change-In-Progressのいずれかの状態であるか、関連付けられているいずれかのメンバーボリュームまたはリザーブ容量ボリュームで障害が発生している。

ミラーグループロールの競合

ローカルストレージアレイとリモートストレージアレイ間の通信の問題が解決すると、Mirror Group Role Conflict状態が発生します。Recovery Guruを使用してこのエラーを解決してください。二重ロールの競合の解決時に、強制昇格は許可されません。

Mirror Group Role Conflict状態とそれ以降のリカバリ手順を回避するには、ストレージアレイ間の接続が確立されてから強制的にロールを変更してください。

ロール変更実行中の状態

ミラーリング構成内の2つのストレージアレイが切断され、ミラー整合性グループのプライマリ側が強制的にセカンダリロールに降格され、ミラー整合性グループのセカンダリ側が強制的にプライマリロールに昇格されると、通信が回復すると、両方のストレージアレイのミラー整合性グループがRole-Change-In-Progress状態になります。

システムでは、変更ログを転送し、再同期を実行し、ミラー整合性グループを通常の動作状態に戻して、定期的な同期を続行することで、ロール変更プロセスを完了します。

同期の概念

同期ミラーリングの仕組み

同期ミラーリングでは、データボリュームがリアルタイムでレプリケートされるため、継続的な可用性が確保されます。

> 同期ミラーリングはEF600またはEF300ストレージアレイでは使用できません。

同期ミラーリングでは、2つのストレージアレイのいずれかで災害が発生した場合に重要なデータのコピーを確保することで、データ損失ゼロの目標復旧時点（RPO）を達成します。プライマリボリュームに書き込みが行われるたびにセカンダリボリュームにも書き込みが行われるため、コピーは常に本番環境のデータと同じです。プライマリボリュームで行われた変更でセカンダリボリュームが更新されるまで、ホストは書き込みが成功したという確認応答を受信しません。

このタイプのミラーリングは、ディザスタリカバリなどのビジネス継続性の目的に最適です。

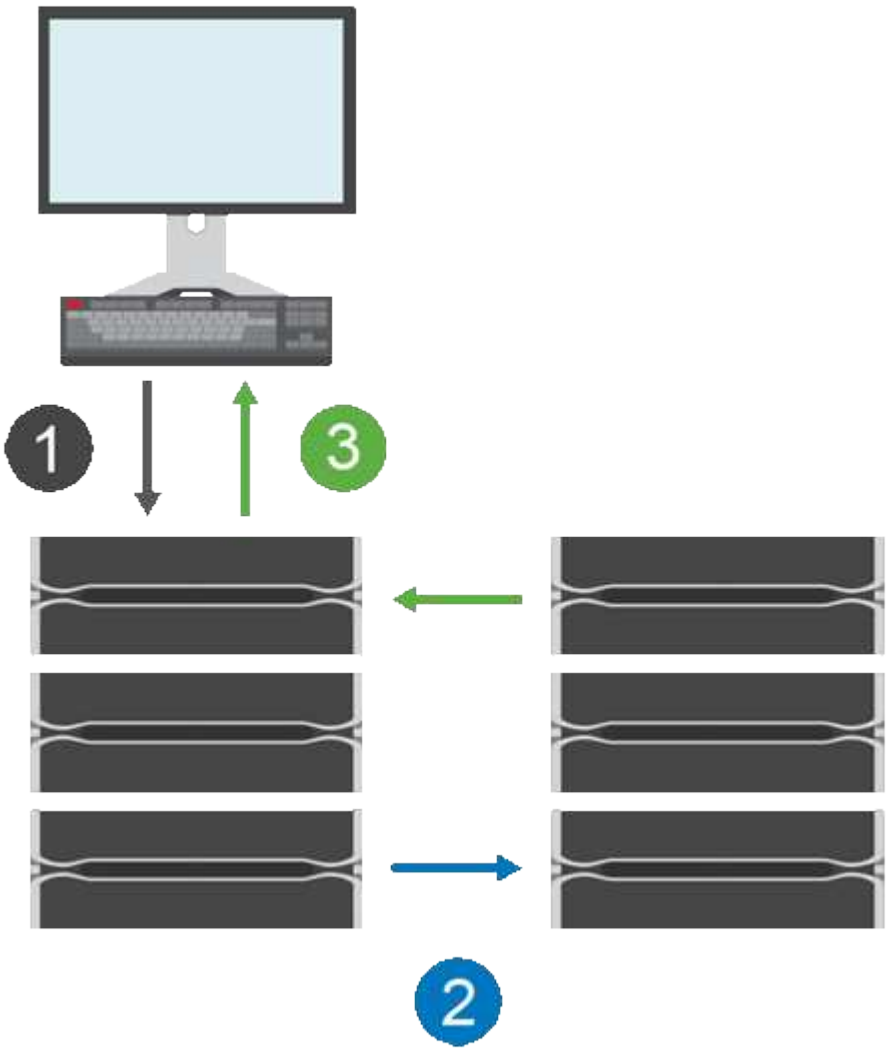
同期ミラー関係

同期ミラーリング関係は、別 々 のストレージアレイ上のプライマリボリュームとセカンダリボリュームで構成されます。プライマリボリュームを含むストレージアレイは、通常はプライマリサイトにあり、アクティブなホストに対応します。セカンダリボリュームを含むストレージアレイは、通常はセカンダリサイトにあり、データのレプリカを格納します。セカンダリボリュームは、プライマリサイトで完全な停電、火災、ハードウ

ェア障害が発生した場合など、プライマリボリュームのストレージアレイが使用できなくなった場合に使用されます。

同期ミラーリングセッション

同期ミラーリングの構成プロセスには、ボリュームをペアとして構成することが含まれます。一方のストレージアレイのプライマリボリュームともう一方のストレージアレイのセカンダリボリュームで構成されるミラーペアを作成したら、同期ミラーリングを開始できます。同期ミラーリングの手順を次に示します。



1. ホストから書き込みが行われます。
2. 書き込みはプライマリボリュームにコミットされ、リモートシステムに伝播され、セカンダリボリュームにコミットされます。
3. プライマリボリュームのストレージアレイからホストsystem_after_both書き込み処理が完了したときに、I/O完了メッセージが送信されます。

リザーブ容量は、ホストからの書き込み要求に関する情報の記録に使用されます。

プライマリボリュームの現在のコントローラ所有者がホストからの書き込み要求を受け取ると、コントローラはまず書き込みに関する情報をプライマリボリュームのリザーブ容量に記録します。次に、プライマリボリュームにデータを書き込みます。次に、コントローラがリモート書き込み処理を開始し、影響を受けたデータブロックをリモートストレージアレイのセカンダリボリュームにコピーします。

ホストアプリケーションは、ローカルストレージアレイおよびリモートストレージアレイ上のネットワークで書き込みが行われるまで待機する必要があるため、 ローカルのI/Oパフォーマンスを大幅に低下させることなくミラー関係を維持するには、ローカルストレージアレイとリモートストレージアレイの間に非常に高速な接続が必要です。

ディザスタリカバリ

同期ミラーリングでは、データが存在するサイトから物理的に離れた場所にデータのコピーが保持されます。停電や洪水などの災害がプライマリサイトで発生した場合、すぐにセカンダリサイトからデータにアクセスできます。

同期ミラーリング処理の進行中は、ホストアプリケーションはセカンダリボリュームを使用できないため、ローカルストレージアレイで災害が発生した場合はリモートストレージアレイにフェイルオーバーできます。フェイルオーバーするには、セカンダリボリュームをプライマリロールに昇格します。これで、新しく昇格されたボリュームにリカバリホストがアクセスできるようになり、業務を続行できます。

同期の設定

ミラーペアを作成するときは、同期優先度と再同期ポリシーも定義します。通信が中断した場合、ミラーペアはこれらを使用して再同期処理を完了します。

2つのストレージアレイ間の通信リンクが停止しても、ホストはローカルストレージアレイからの確認応答を引き続き受信し、アクセスが失われるのを防ぎます。通信リンクの動作が再開したら、レプリケートされていないデータを自動的に、または手動で、リモートストレージアレイに再同期できます。

データが自動的に再同期されるかどうかは、ミラーペアの再同期ポリシーによって異なります。自動再同期ポリシーを使用すると、リンクの再同期が完了した時点でミラーペアが自動的に再同期されます。手動再同期ポリシーを使用している場合は、通信問題の発生後に同期を手動で再開する必要があります。手動再同期ポリシーが推奨されるポリシーです。

ミラーペアの同期設定は、プライマリボリュームを含むストレージアレイでのみ編集できます。

非同期のデータ

プライマリボリュームのストレージアレイがセカンダリボリュームにデータを書き込むことができなくなった場合、プライマリボリュームとセカンダリボリュームは非同期状態になります。これは、次の問題が原因で発生する可能性があります。

- ローカルストレージアレイとリモートストレージアレイ間のネットワークの問題
- セカンダリボリュームの障害
- ミラーペアの同期を手動で中断しています

孤立したミラーペア

孤立したミラーペアボリュームは、一方（プライマリまたはセカンダリ）でメンバーボリュームが削除され、もう一方では削除されていない場合に発生します。

孤立したミラーペアボリュームは、アレイ間の通信がリストアされ、ミラー構成の両サイドでミラーパラメータが調整されたときに検出されます。

ミラーペアを削除すると、孤立したミラーペアの状態を修正できます。

2つのアレイ間のミラーリングを有効にして設定するには、Unified Managerインターフェイスを使用する必要があります。ミラーリングを有効にすると、System Managerでミラーペアと同期設定を管理できます。

同期ミラーリングに関する用語

ストレージアレイに関連する同期ミラーリングの用語を次に示します。

期間	製品説明
ローカルストレージアレイ	ローカルストレージアレイは、操作の対象となるストレージアレイです。 Local Role列に* Primary と表示された場合は、ミラー関係のプライマリロールが割り当てられたボリュームがストレージアレイに含まれていることを示しています。**Local Role**列に「 Secondary」と表示されている場合、ストレージアレイにミラー関係のセカンダリロールが割り当てられたボリュームが含まれていることを示しています。
ミラーペア	ミラーペアは、プライマリボリュームとセカンダリボリュームの2つのボリュームで構成されます。
プライマリボリューム	ミラーペアのプライマリボリュームは、ミラーリングするソースボリュームです。
目標復旧時点（RPO）	目標復旧時点（RPO）は、ミラーペアのプライマリボリュームとセカンダリボリュームの間で許容される差異の目標値です。RPOがゼロの場合は、プライマリボリュームとセカンダリボリュームの差が許容されません。RPOがゼロより大きい場合は、セカンダリボリュームの方がプライマリボリュームよりも最新でないか遅延しています。
リモートストレージアレイ	通常、リモートストレージアレイはセカンダリサイトとして指定され、セカンダリサイトにはミラーリング構成のデータのレプリカが格納されます。
リザーブ容量	リザーブ容量は、コピーサービス処理やストレージオブジェクトに使用される物理割り当て容量です。ホストから直接読み取ることはできません。
ロール変更	ロール変更では、セカンダリボリュームにプライマリロールが割り当てられ、セカンダリボリュームにプライマリロールが割り当てられます。
セカンダリボリューム	ミラーペアのセカンダリボリュームは、通常はセカンダリサイトに配置され、データのレプリカが格納されます。
同期	同期は、ローカルストレージアレイとリモートストレージアレイの間の初期同期で実行されます。同期は、通信の中断後にプライマリボリュームとセカンダリボリュームが同期されていない状態になった場合にも実行されます。通信リンクの動作が再開されると、レプリケートされていないデータがセカンダリボリュームのストレージアレイに同期されます。

ボリュームを同期的にミラーリングするためのワークフロー

次のワークフローを使用して同期ミラーリングを設定します。

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。

1. Unified Managerで初期設定を実行します。
   a. データ転送元としてローカルストレージアレイを選択します。
   b. ローカルストレージアレイからプライマリボリュームを選択します。
   c. データ転送先としてリモートストレージアレイを選択し、セカンダリボリュームを選択します。
   d. 同期と再同期の優先度を選択します。
   e. プライマリボリュームからセカンダリボリュームへの初回のデータ転送を開始します。ボリュームサイズによっては、この初回転送に数時間かかることがあります。
2. 初期同期の進捗状況を確認します。
   a. Unified Managerで、ローカルアレイのSystem Managerを起動します。
   b. System Managerで、ミラーリング処理のステータスを確認します。ミラーリングが完了すると、ミラーペアのステータスは「最適」になります。2つのアレイは、通常の処理を通じて同期状態が維持されます。新しいブロックと変更されたブロックだけがプライマリボリュームからセカンダリボリュームに転送されます。
3. オプション： System Managerで同期設定を変更できます。

同期レプリケーションは継続的であるため、2つのサイト間のレプリケーションリンクで十分な帯域幅機能を提供する必要があります。

同期ミラーリングを使用するための要件

同期ミラーリングを使用する場合は、次の要件に注意してください。

Unified Manager

2つのアレイ間のミラーリングを有効にして設定するには、Unified Managerインターフェイスを使用する必要があります。Unified Managerは、Web Services Proxyとともにホストシステムにインストールされます。

- Web Services Proxyサービスが実行されている必要があります。
- Unified ManagerがHTTPS接続経由でローカルホストで実行されている必要があります。
- Unified Managerにストレージアレイの有効なSSL証明書が表示されている必要があります。Unified Managerのメニューから「Certificate Management」に移動し、自己署名証明書を受け入れるか、独自のセキュリティ証明書をインストールできます。

ストレージアレイ

同期ミラーリングはEF300またはEF600ストレージアレイでは使用できません。

- 2つのストレージアレイが必要です。

- 各ストレージアレイに2台のコントローラが必要です。
- Unified Managerで2つのストレージアレイが検出されている必要があります。
- プライマリアレイとセカンダリアレイの両方の各コントローラにイーサネット管理ポートが設定され、ネットワークに接続されている必要があります。
- ストレージアレイに必要なファームウェアの最小バージョンは7.84です（それぞれ異なるOSバージョンを実行できます）。
- ローカルとリモートのストレージアレイのパスワードを確認しておく必要があります。
- ミラーリングするプライマリボリューム以上のセカンダリボリュームを作成するには、リモートストレージアレイに十分な空き容量が必要です。
- ローカルとリモートのストレージアレイをFibre Channelファブリックを介して接続します。

サポートされる接続

同期ミラーリングの通信は、Fibre Channel（FC）ホストポートを搭載したコントローラでのみサポートされます。

同期ミラーリングでは、ローカルストレージアレイとリモートストレージアレイの両方にある各コントローラで最も大きい番号のホストポートが使用されます。通常、コントローラのホストバスアダプタ（HBA）ホストポート4は、データ送信のミラーリング用に予約されています。

ミラーボリュームの候補

- 同期ミラーペアのプライマリボリュームとセカンダリボリュームでは、RAIDレベル、キャッシングパラメータ、およびセグメントサイズが異なる場合があります。
- 同期ミラーペアのプライマリボリュームとセカンダリボリュームは標準ボリュームである必要があります。シンボリュームやSnapshotボリュームは使用できません。
- セカンダリボリュームは、プライマリボリュームと同じサイズ以上である必要があります。
- Snapshotを関連付けることができるのはプライマリボリュームのみです。また、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として使用できるのもプライマリボリュームのみです。
- ボリュームに設定できるミラー関係は1つだけです。
- 特定のストレージアレイでサポートされるボリュームの数には制限があります。ストレージアレイに設定されているボリュームの数がサポートされている制限よりも少ないことを確認してください。同期ミラーリングがアクティブな場合は、作成された2つのリザーブ容量ボリュームがボリュームの制限に含まれます。

リザーブ容量

- コントローラのリセットおよびその他の一時的な中断からリカバリするための書き込み情報をログに記録するには、プライマリボリュームとセカンダリボリュームにリザーブ容量が必要です。
- 同期ミラーリングがアクティブ化されると、リザーブ容量ボリュームが自動的に作成されます。ミラーペアのプライマリボリュームとセカンダリボリュームにはリザーブ容量が必要であるため、同期ミラー関係にある両方のストレージアレイに十分な空き容量が確保されていることを確認してください。

ドライブセキュリティ機能

- セキュリティ対応ドライブを使用する場合、プライマリボリュームとセカンダリボリュームのセキュリティ設定に互換性がある必要があります。この制限は強制的には適用されないため、自分で確認する必要が

あります。

- セキュリティ対応ドライブを使用する場合、プライマリボリュームとセカンダリボリュームで同じタイプのドライブを使用する必要があります。この制限は強制的には適用されないため、自分で確認する必要があります。
  - プライマリボリュームでFull Disk Encryption（FDE）ドライブを使用する場合、セカンダリボリュームでもFDEドライブを使用する必要があります。
  - プライマリボリュームで連邦情報処理標準（FIPS）140-2準拠ドライブを使用する場合、セカンダリボリュームでもFIPS 140-2準拠ドライブを使用する必要があります。
- Data Assurance（DA）を使用する場合、プライマリボリュームとセカンダリボリュームでDA設定を同じにする必要があります。

同期ミラーリングのステータス

同期ミラーペアのステータスは、プライマリボリュームとセカンダリボリュームのデータが同期されているかどうかを示します。ミラーステータスは、ミラーペア内のボリュームのコンポーネントステータスとは関係ありません。

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。

同期ミラーペアのステータスは次のいずれかになります。

- 最適

  ミラーペア内のボリュームが同期されていることを示します。つまり、ストレージアレイ間のファブリック接続が動作していて、各ボリュームが適切な動作状態にあることを示します。

- 同期中

  ミラーペア間のデータ同期の進捗状況が表示されます。このステータスは、初期同期中にも表示されます。

  通信リンクの中断後、リンクの中断中にプライマリボリュームで変更されたデータブロックのみがセカンダリボリュームにコピーされます。

- 非同期

  プライマリボリュームのストレージアレイがリモートアレイに受信データを書き込めないことを示します。ローカルホストはプライマリボリュームへの書き込みを継続できますが、リモート書き込みは行われません。次のようなさまざまな状況によって、プライマリボリュームのストレージアレイがセカンダリボリュームに受信データを書き込めない場合があります。

  - セカンダリボリュームにアクセスできません。
  - リモートストレージアレイにアクセスできません。
  - ストレージアレイ間のファブリック接続にアクセスできません。
  - セカンダリボリュームを新しいWorld Wide Identifier（WWID）で更新することはできません。

- 一時停止

  同期ミラーリング処理がユーザによって中断されたことを示します。ミラーペアが中断されている場合、

セカンダリボリュームへの接続は試行されません。プライマリボリュームへの書き込みは、ミラーのリザーブ容量ボリュームに永続的に記録されます。

- 失敗

  プライマリボリューム、セカンダリボリューム、またはミラーのリザーブ容量の障害が原因で、同期ミラーリング処理を正常に実行できないことを示します。

ボリューム所有権

ミラーペアの優先コントローラ所有者を変更できます。

この機能は、EF600またはEF300ストレージシステムの同期ミラーリングでは使用できません。

ミラーペアのプライマリボリュームがコントローラAに所有されている場合、セカンダリボリュームもリモートストレージアレイのコントローラAに所有されます。プライマリボリュームの所有者を変更すると、セカンダリボリュームの所有者が自動的に変更され、両方のボリュームが同じコントローラで所有されるようになります。プライマリ側で現在の所有権が変更されると、セカンダリ側の対応する所有権も自動的に変更されます。

たとえば、コントローラAが所有するプライマリ ボリュームの所有者をコントローラBに変更したとします。この場合、次回のリモート書き込み時に、セカンダリ ボリュームの所有者がコントローラAからコントローラBに切り替わります。セカンダリ側のコントローラ所有権の切り替えはプライマリ側で制御されるため、ストレージ管理者による特別な対応は必要ありません。

コントローラのリセット

コントローラをリセットすると、プライマリ側でボリューム所有権が優先コントローラ所有者からストレージアレイ内の代替コントローラに変更されます。

セカンダリボリュームへの書き込み前に、コントローラのリセットやストレージアレイの電源の再投入によってリモート書き込みが中断されることがあります。この場合、コントローラでミラーペアの完全同期を実行する必要はありません。

コントローラのリセット中にリモートの書き込みが中断されると、プライマリ側の新しいコントローラ所有者は、優先コントローラ所有者のリザーブ容量ボリューム内のログファイルに格納されている情報を読み取ります。その後、新しいコントローラ所有者は、影響を受けたデータブロックをプライマリボリュームからセカンダリボリュームにコピーします。これにより、ミラーボリュームの完全な同期が不要になります。

ミラーペア内のボリューム間でのロール変更

ミラーペア内のボリューム間でロールを変更できます。そのためには、プライマリボリュームをセカンダリロールに降格するか、セカンダリボリュームをプライマリロールに昇格します。

同期ミラーリングは、EF600またはEF300ストレージシステムでは使用できません。

ロール変更処理に関する次の情報を確認してください。

- プライマリボリュームがセカンダリロールに降格されると、そのミラーペアのセカンダリボリュームがプ

ライマリロールに昇格されます。その逆も同様です。

- プライマリボリュームがセカンダリロールに降格されると、そのボリュームに割り当てられているホストはボリュームに書き込みアクセスできなくなります。
- セカンダリボリュームがプライマリロールに昇格されると、そのボリュームにアクセスしているすべてのホストがボリュームに書き込むことができるようになります。
- ローカルストレージアレイがリモートストレージアレイと通信できない場合は、ローカルストレージアレイで強制的にロールを変更できます。

強制的なロール変更

ローカルストレージアレイとリモートストレージアレイ間の通信の問題によってセカンダリボリュームの昇格またはプライマリボリュームの降格を実行できない場合は、ミラーペアのボリューム間で強制的にロールを変更できます。

セカンダリ側のボリュームを強制的にプライマリロールに移行できます。これで、新しく昇格されたボリュームにリカバリホストがアクセスできるようになり、業務を続行できます。

リモートストレージアレイがリカバリされ、通信の問題が解決されると、「同期ミラーリング-プライマリボリュームが競合しています」状態が発生します。リカバリ手順にはボリュームの再同期が含まれます。Recovery Guruを使用してこのエラーを解決してください。

強制昇格が許可される場合と許可されない場合

次の状況では、ミラーペアのボリュームの強制昇格は許可されません。

- ミラーペア内のいずれかのボリュームで初期同期中です。
- ミラーペアが失敗、Role-Change-Pending、Role-Change-In-Progressのいずれかの状態であるか、関連付けられているいずれかのリザーブ容量ボリュームで障害が発生している。

ロール変更実行中の状態

ミラーリング構成の2つのストレージアレイが切断され、ミラーペアのプライマリボリュームが強制的にセカンダリロールに降格され、ミラーペアのセカンダリボリュームが強制的にプライマリロールに昇格された場合、通信が回復すると、両方のストレージアレイのボリュームがRole-Change-In-Progress状態になります。

システムは、変更ログを転送し、再同期し、ミラーペアを通常の動作状態に戻し、同期を続行することで、ロール変更プロセスを完了します。

非同期ミラー整合性グループを管理します。

ミラー整合性グループの通信のテスト

通信リンクをテストして、ミラー整合性グループに関連付けられているローカルストレージアレイとリモートストレージアレイの間の通信の問題を診断できます。

開始する前に

テストするミラー整合性グループがローカルとリモートのストレージアレイに存在している必要があります。

タスクの内容

次の4つのテストを実行できます。

- 接続-- 2台のコントローラに通信パスがあることを確認します接続テストでは、ストレージアレイ間でメッセージを送信し、リモートストレージアレイに対応するミラー整合性グループが存在するかどうかを検証します。また、リモートストレージアレイ上のミラー整合性グループのメンバーボリュームがローカルストレージアレイ上のミラー整合性グループのメンバーボリュームと一致するかどうかも検証されます。
- * Latency *--ミラー整合性グループに関連付けられたリモートストレージアレイ上の各ミラーボリュームにSCSI Test Unitコマンドを送信して、最小、平均、最大のレイテンシをテストします。
- **bandwidth**-- 2つのアレイ間メッセージをリモートストレージアレイに送信して、最小、平均、最大の帯域幅、およびテストを実行しているアレイ上のポートのネゴシエートされたリンク速度をテストします。
- ポート接続--ローカルストレージアレイ上のミラーリングに使用されているポート'およびリモートストレージアレイ上のミラーデータを受信しているポートを表示します

手順

1. メニューを選択します。Storage [非同期ミラーリング]。
2. ミラー整合性グループ*タブを選択し、テストするミラー整合性グループを選択します。
3. [通信のテスト]を選択します。

   [Test Communication]ダイアログボックスが表示されます。
4. 選択したミラー整合性グループに関連付けられているローカルとリモートのストレージアレイ間で実行する通信テストを1つ以上選択し、* Test *をクリックします。
5. [結果]ウィンドウに表示される情報を確認します。

通信テストのステータス	製品説明
正常（エラーなし）	ミラー整合性グループが正常に通信しています。
合格（ただし、正常ではない）	考えられるネットワークまたは接続の問題を確認してから、テストを再試行してください。
失敗ステータス	エラーの理由が示されます。問題を修正するには、Recovery Guruを参照してください。
ポート接続エラー	ローカルストレージアレイが接続されていないか、リモートストレージアレイに接続できない可能性があります。問題を修正するには、Recovery Guruを参照してください。

結果

通信テストが完了すると、このダイアログボックスにNormal、Passed、Failedのいずれかのステータスが表示されます。

通信テストから失敗ステータスが返された場合は、このダイアログボックスを閉じたあと、ミラー整合性グループ間の通信が回復するまでテストが続行されます。

ミラー整合性グループの同期の中断または再開

ミラー整合性グループ内のすべてのミラーペアでデータの同期を中断または再開できます。これは、個 々 のミラーペアで同期を中断または再開するよりも効率的です。

タスクの内容

グループに対する同期の一時停止と再開は、ホストアプリケーションのパフォーマンスへの影響（ローカルストレージアレイで変更されたデータがリモートストレージアレイにコピーされるときに発生する可能性があります）を軽減するのに役立ちます。

ミラー整合性グループとそのミラーペアの状態は、[再開]オプションを使用して同期アクティビティを再開するまで中断されたままです。

手順

1. メニューを選択します。Storage [非同期ミラーリング]。
2. [ミラー整合性グループ*（Mirror Consistency Groups *）]タブを選択します。

   [ミラー整合性グループ]の表に、ストレージアレイに関連付けられているすべてのミラー整合性グループが表示されます。

3. 中断または再開するミラー整合性グループを選択し、メニュー：その他[中断]またはメニュー：その他[再開]を選択します。

   確認メッセージが表示されます。

4. 「はい」を選択して確定します。

結果

System Managerは次の処理を実行します。

- ミラー関係を削除せずに、ミラー整合性グループ内のすべてのミラーペア間のデータ転送を中断または再開します。
- ミラーグループの中断中にミラー整合性グループのプライマリ側に書き込まれたデータをログに記録し、ミラーグループが再開されるとミラー整合性グループのセカンダリ側にデータを自動的に書き込みます。完全同期は必要ありません。
- a_suspended_mirror整合性グループの場合、Mirror Consistency Groupsテーブルに* user-suspended *が表示されます。
- 再開されたミラー整合性グループでは、ミラー整合性グループの中断中にプライマリボリュームに書き込まれたデータがセカンダリボリュームにただちに書き込まれます。自動同期間隔が設定されている場合は、定期的な同期が再開されます。

ミラー整合性グループの同期設定の変更

ローカルストレージアレイ上のミラー整合性グループが、データが最初に同期されたときや非同期ミラーリング処理中にデータが再同期されたときに使用する同期設定と警告しきい値を変更できます。

タスクの内容

同期設定を変更すると、ミラー整合性グループ内のすべてのミラーペアの同期処理に反映されます。

手順

1. メニューを選択します。Storage [非同期ミラーリング]。
2. [ミラー整合性グループ*（Mirror Consistency Groups *）]タブを選択します。

   [ミラー整合性グループ]の表に、ストレージアレイに関連付けられているすべてのミラー整合性グループが表示されます。

3. 編集するミラー整合性グループを選択し、メニューから[More（詳細）][Edit Settings（設定の編集）]を選択します。

   [設定の編集]ダイアログボックスが表示されます。

4. 必要に応じて同期とアラートの設定を編集し、*保存*をクリックします。

   フィールドの詳細

フィールド	製品説明
ミラーペアを同期…	リモートストレージアレイのミラーペアの同期を手動で行うか自動で行うかを指定します。 • 手動–リモートストレージアレイ上のミラーペアを手動で同期する場合に選択します • 自動、–リモートストレージアレイのミラーペアを自動的に同期する場合は、前の更新の開始から次の更新の開始までの間隔を指定します。デフォルトの間隔は10分です。
アラートを受け取る条件を選択…	同期方法を自動的に実行するように設定した場合は、次のアラートを設定します。 • 同期–同期が完了していないというアラートがSystem Managerから送信されるまでの時間を設定します。 • リモートリカバリポイント–リモートストレージアレイのリカバリポイントデータが指定した制限時間より古くなったことを示すアラートがSystem Managerから送信されるまでの時間制限を設定します。期限は、前回の更新の終了時点からの経過時間で定義します。 • リザーブ容量のしきい値–リザーブ容量が指定した値を超えるとSystem Managerからアラートが送信され、リザーブ容量のしきい値に近づいていることが通知されます。しきい値は残りの容量の割合で定義します。

結果

System Managerによって、ミラー整合性グループ内のすべてのミラーペアの同期設定が変更されます。

ミラー整合性グループの手動による再同期

ミラー整合性グループ内のすべてのミラーペアの再同期を手動で開始できます。

手順

1. メニューを選択します。Storage [非同期ミラーリング]。
2. [ミラー整合性グループ*（Mirror Consistency Groups *）]タブを選択します。

   [ミラー整合性グループ]の表に、ストレージアレイに関連付けられているすべてのミラー整合性グループが表示されます。

3. 再同期するミラー整合性グループを選択し、メニューを選択します。More [Manually resynchronize]

   確認メッセージが表示されます。

4. 「はい」を選択して確定します。

結果

システムは次の処理を実行します。

- 選択したミラー整合性グループ内のすべてのミラーペアでデータの再同期が開始されます。
- ローカルストレージアレイからリモートストレージアレイに変更されたデータを更新します。

ミラー整合性グループ間で同期されていないデータ量の表示

ローカルストレージアレイとリモートストレージアレイ上のミラー整合性グループ間で同期されていないデータの量を表示できます。ミラー整合性グループのステータスが非同期の間は、ミラーリングアクティビティは実行されません。

タスクの内容

このタスクは、選択したミラー整合性グループにミラーペアが含まれている場合、および同期が実行中でない場合に実行できます。

手順

1. メニューを選択します。Storage [非同期ミラーリング]。
2. [ミラー整合性グループ*（Mirror Consistency Groups *）]タブを選択します。

   [ミラー整合性グループ]の表に、ストレージアレイに関連付けられているすべてのミラー整合性グループが表示されます。

3. メニューをクリックします。More [同期されていないデータ量の表示]

   同期されていないデータが存在する場合は、テーブルの値に反映されます。データ量の列には、同期されていないデータの量がMiB単位で表示されます。

リモート**IP**アドレスの更新

リモートストレージアレイのiSCSI IPアドレスを更新して、ローカルストレージアレイ

との接続を再確立できます。

開始する前に

iSCSI接続を使用した非同期ミラーリング用にローカルストレージアレイとリモートストレージアレイの両方が設定されている必要があります。

手順

1. メニューを選択します。Storage [非同期ミラーリング]。
2. [ミラー整合性グループ*（Mirror Consistency Groups *）]タブを選択します。

   [ミラー整合性グループ]の表には、ストレージアレイに関連付けられているすべてのミラー整合性グループが表示されます。

3. 更新するミラー整合性グループを選択し、メニューを選択します。More [Update remote IP address].

   [Update Remote IP Address]ダイアログボックスが表示されます。

4. 「* Update *」を選択して、リモートストレージアレイのiSCSI IPアドレスを更新します。

結果

リモートストレージアレイのIPアドレスがリセットされ、ローカルストレージアレイとの接続が再確立されます。

ミラー整合性グループのロール変更（プライマリまたはセカンダリ）

管理目的で、またはローカルストレージアレイで災害が発生した場合に、ミラー整合性グループ間でロールを変更できます。

タスクの内容

ローカルストレージアレイに作成されたミラー整合性グループには、プライマリロールが割り当てられます。リモートストレージアレイに作成されたミラー整合性グループには、セカンダリロールが割り当てられます。ローカルのミラー整合性グループのロールをセカンダリに降格するか、リモートのミラー整合性グループのロールをプライマリに昇格することができます。

手順

1. メニューを選択します。Storage [非同期ミラーリング]。
2. [ミラー整合性グループ*（Mirror Consistency Groups *）]タブを選択します。

   [ミラー整合性グループ]の表に、ストレージアレイに関連付けられているすべてのミラー整合性グループが表示されます。

3. ロールを変更するミラー整合性グループを選択し、メニューを選択します。More **>>**。

   確認メッセージが表示されます。

4. ミラー整合性グループのロールを変更することを確認し、* Change Role *をクリックします。

ロールの変更が要求されてもリモートストレージアレイに接続できない場合、[ストレージアレイに接続できません]ダイアログボックスが表示されます。[はい]をクリックして、強制的にロールを変更します。

結果

System Managerは次の処理を実行します。

- [ミラー整合性グループ]テーブルで、ロール変更を実行中のミラー整合性グループの横にステータスが「保留」または「実行中」と表示されます。テーブルセル内にある*Cancel*リンクをクリックすると、保留中のロール変更操作をキャンセルできます。
- 関連付けられたミラー整合性グループにアクセスできる場合は、ミラー整合性グループ間でロールが変更されます。選択した内容に応じて、System Managerはセカンダリミラー整合性グループのロールをプライマリに昇格するか、プライマリミラー整合性グループのロールをセカンダリに降格します。ロール変更は、選択したミラー整合性グループ内のすべてのミラーペアに反映されます。

ミラー整合性グループの削除

ローカルストレージアレイとリモートストレージアレイで不要になったミラー整合性グループを削除できます。

開始する前に

ミラー整合性グループからすべてのミラーペアを削除する必要があります。

手順

1. メニューを選択します。Storage [非同期ミラーリング]。
2. [ミラー整合性グループ*（Mirror Consistency Groups *）]タブを選択します。

   [ミラー整合性グループ]の表に、ストレージアレイに関連付けられているすべてのミラー整合性グループが表示されます。

3. 削除するミラー整合性グループを選択し、メニューから「一般的でないタスク[削除]」を選択します。

   確認メッセージが表示されます。

4. 「* Yes」を選択してミラー整合性グループを削除します。

結果

System Managerは次の処理を実行します。

- 最初にローカルストレージアレイから、次にリモートストレージアレイからミラー整合性グループを削除します。
- [ミラー整合性グループ]テーブルからミラー整合性グループを削除します。

終了後

ローカルストレージアレイからミラー整合性グループが削除されたあとに通信エラーが発生してリモートストレージアレイからミラー整合性グループが削除されないことがあります。この場合、リモートストレージアレイにアクセスして対応するミラー整合性グループを削除する必要があります。

非同期ミラーペアを管理します。

非同期ミラー関係の削除

ミラーペアを削除して、ローカルストレージアレイ上のプライマリボリュームとリモートストレージアレイ上のセカンダリボリュームからミラー関係を削除します。

タスクの内容

孤立したミラーペアに関する次の情報を確認します。

- 孤立したミラーペアは、一方（ローカルストレージアレイ側またはリモートストレージアレイ側）でミラー整合性グループのメンバーボリュームが削除され、もう一方では削除されていない場合に発生します。
- 孤立したミラーペアは、アレイ間の通信がリストアされ、ミラー構成の両側でミラーパラメータが調整されたときに検出されます。
- ミラーペアを削除すると、孤立したミラーペアの状態を修正できます。

手順

1. メニューを選択します。Storage [非同期ミラーリング]。
2. [ミラーペア*（Mirrored Pair *）]タブを選択します。

   [ミラーペア]の表に、ストレージアレイに関連付けられているすべてのミラーペアが表示されます。

3. 削除するミラーペアを選択し、* Remove *をクリックします。
4. ミラーペアの削除を確認し、* Remove *をクリックします。

結果

System Managerは次の処理を実行します。

- ローカルストレージアレイとリモートストレージアレイのミラー整合性グループからミラー関係を削除し、リザーブ容量を削除します。
- ホストがアクセス可能でミラーされていないボリュームにプライマリボリュームとセカンダリボリュームを戻します。
- 非同期ミラーペアの削除を反映して[非同期ミラーリング]タイルを更新します。

リザーブ容量の拡張

リザーブ容量を増やすことができます。リザーブ容量は、ストレージオブジェクトに対する任意のコピーサービス処理に使用される物理的に割り当てられた容量です。

Snapshot処理の場合は、通常はベースボリュームの40%、非同期ミラーリング処理の場合は通常はベースボリュームの20%です。一般に、ストレージオブジェクトのリザーブ容量がフルに近づいているという警告が表示されたときにリザーブ容量を拡張します。

開始する前に

- プールまたはボリュームグループ内のボリュームのステータスが最適で、変更処理の実行中でないことを確認してください。

- プールまたはボリュームグループに容量の拡張に使用する空き容量が必要です。

  プールまたはボリュームグループに空き容量がない場合は、未割り当て容量を未使用ドライブの形式でプールまたはボリュームグループに追加できます。

タスクの内容

次のストレージオブジェクトのリザーブ容量は8GiB単位でのみ拡張できます。

- Snapshotグループ
- Snapshotボリューム
- 整合性グループメンバーボリューム
- ミラーペアボリューム

プライマリボリュームで多数の変更が行われる可能性がある場合や、特定のコピーサービス処理の寿命が非常に長い場合は、割合を高くします。

読み取り専用のSnapshotボリュームのリザーブ容量は増やすことはできません。リザーブ容量が必要なのは、読み取り/書き込みのSnapshotボリュームだけです。

手順

1. 選択メニュー：Storage（Pool & Volume Groups）
2. 予約容量*タブを選択します。
3. リザーブ容量を増やすストレージオブジェクトを選択し、*容量の拡張*をクリックします。

   リザーブ容量の拡張ダイアログボックスが表示されます。

4. スピンボックスを使用して容量の割合を調整します。

   選択したストレージオブジェクトを含むプールまたはボリュームグループに空き容量がなく、ストレージアレイに未割り当て容量がある場合は、新しいプールまたはボリュームグループを作成できます。その後、そのプールまたはボリュームグループの新しい空き容量を使用してこの処理を再試行できます。

5. [* 拡大（ * ）] をクリックします

結果

System Managerは次の処理を実行します。

- ストレージオブジェクトのリザーブ容量を拡張します。
- 新たに追加したリザーブ容量を表示します。

ミラーペアボリュームのリザーブ容量設定の変更

ミラーペアボリュームの設定を変更して、ミラーペアボリュームのリザーブ容量が残り少なくなったときにSystem Managerからアラート通知を送信する割合を調整できます。

手順

1. 選択メニュー：Storage（Pool & Volume Groups）
2. 予約容量*タブを選択します。
3. 編集するミラーペアボリュームを選択し、*表示/設定の編集*をクリックします。

   ミラーペアボリュームのリザーブ容量の設定ダイアログボックスが表示されます。

4. ミラーペアボリュームのリザーブ容量の設定を適宜変更します。

   フィールドの詳細

設定	製品説明
アラートを受け取るタイミング…	このスピンボックスを使用して、ミラーペアのリザーブ容量が残り少なくなったときにSystem Managerからアラート通知を送信する割合を調整します。 ミラーペアのリザーブ容量が指定したしきい値を超えるとSystem Managerからアラートが送信されるため、前もってリザーブ容量を増やすことができます。 1つのミラーペアのアラート設定を変更すると、同じミラー整合性グループに属するすべてのミラーペアのアラート設定が変更されます。

5. [保存（Save）]をクリックして、変更を適用します。

従来型システムで作成されたプライマリボリュームのミラーペアの作成

System Managerで管理できない従来型ストレージアレイにプライマリボリュームを作成した場合は、System Managerでこのアレイにセカンダリボリュームを作成できます。

タスクの内容

別のインターフェイスを使用する従来のアレイとSystem Managerで管理可能な新しいアレイの間で、非同期ミラーリングを実行できます。

- System Managerを使用する2つのストレージアレイをミラーリングする場合は、ミラーペア作成手順ですでにミラーペアの作成が完了しているため、このタスクはスキップできます。
- このタスクはリモートストレージアレイで実行します。

手順

1. メニューを選択します。Storage [非同期ミラーリング]。
2. [ミラーペア*（Mirrored Pair *）]タブを選択します。

   [ミラーペア]の表に、ストレージアレイに関連付けられているすべてのミラーペアが表示されます。

3. ステータスが「Incomplete」のミラーペアボリュームを探し、ミラーペアの列に表示された「* Complete Mirrored pair *」リンクをクリックします。

4. 次のいずれかのラジオボタンを選択して、ミラーペア作成手順を自動で実行するか手動で実行するかを選択します。
   - 自動--新しいセカンダリボリュームを作成します

     セカンダリボリュームを作成する既存のプールまたはボリュームグループを選択して、ミラーペアのリモート側のデフォルト設定を受け入れます。セカンダリボリュームにデフォルトの設定でリザーブ容量を割り当てるには、このオプションを使用します（推奨）。

   - 手動--既存のボリュームを選択します

     セカンダリボリュームのパラメータを独自に定義します。

     i. Next（次へ）*をクリックして、セカンダリボリュームを選択します。
     ii. セカンダリボリュームとして使用する既存のボリュームを選択し、* Next *をクリックしてリザーブ容量を割り当てます。
     iii. リザーブ容量を割り当てます。次のいずれかを実行します。
        - デフォルト設定をそのまま使用します。

          リザーブ容量のデフォルト設定はベースボリュームの容量の20%で、通常はこの容量で十分です。

        - 非同期ミラーリングに関連するデータストレージのニーズに合わせて、独自の設定でリザーブ容量を割り当てます。

          必要な容量は、プライマリボリュームに対するI/O書き込みの頻度とサイズ、およびその容量を維持する必要がある期間によって異なります。一般に、次のいずれかまたは両方に該当する場合は、リザーブ容量を大きくします。

          - ミラーペアを長期間保持する場合。
          - 大量のI/Oアクティビティにより、プライマリボリュームのデータブロックの大部分で変更が発生する場合。プライマリボリュームに対する一般的なI/Oアクティビティを判断するには、過去のパフォーマンスデータやその他のオペレーティングシステムユーティリティを使用します。
5. [*Complete]を選択します。

結果

System Managerは次の処理を実行します。

- リモートストレージアレイにセカンダリボリュームを作成し、ミラーペアのリモート側にリザーブ容量を割り当てます。
- ローカルストレージアレイとリモートストレージアレイの間の初期同期を開始します。
- ミラーリング対象のボリュームがシンボリュームの場合、初期同期では割り当てられたブロックのみがセカンダリボリュームに転送されます。この転送により、初期同期を完了するために転送する必要のあるデータ量が削減されます。
- ローカルストレージアレイとリモートストレージアレイにミラーペア用のリザーブ容量を作成します。

同期ミラーペアの管理

同期ミラーリングの通信のテスト

ローカルストレージアレイとリモートストレージアレイの間の通信をテストして、同期ミラーリングに参加しているミラーペアで発生する可能性のある通信の問題を診断できます。

タスクの内容

次の2つのテストが実行されます。

- 通信-- 2つのストレージアレイに通信パスがあることを確認します通信テストでは、ローカルストレージアレイがリモートストレージアレイと通信できるかどうか、およびミラーペアに関連付けられているセカンダリボリュームがリモートストレージアレイに存在するかどうかを検証します。
- * Latency *--ミラーペアに関連付けられたリモートストレージアレイ上のセカンダリボリュームにSCSIテストユニットコマンドを送信して、最小、平均、最大のレイテンシをテストします。

手順

1. 選択メニュー：Storage [Synchronous Mirroring]
2. テストするミラーペアを選択し、「*通信のテスト」を選択します。
3. [結果]ウィンドウに表示された情報を確認し、必要に応じて、示された対処方法に従います。

> ⓘ 通信テストに失敗した場合は、このダイアログを閉じたあと、ミラーペア間の通信が回復するまでテストが続行されます。

ミラーペアの同期の中断と再開

[中断]オプションと[再開]オプションを使用して、ミラーペアのプライマリボリュームとセカンダリボリュームのデータを同期するタイミングを制御できます。

タスクの内容

ミラーペアを手動で中断した場合、手動で再開するまでミラーペアは同期されません。

手順

1. 選択メニュー：Storage [Synchronous Mirroring]
2. 中断または再開するミラーペアを選択し、メニューから[More [Suspend]（その他の中断）またはメニュー：More [Resume]（その他の再開）のいずれかを選択します。

   確認メッセージが表示されます。
3. 「はい」を選択して確定します。

結果

System Managerは次の処理を実行します。

- ミラー関係を削除せずに、ミラーペア間のデータ転送を中断または再開します。

- 中断されたミラーペアの場合：
  - ミラーペアテーブルに「* suspended」と表示されます。
  - 同期の中断中にミラーペアのプライマリボリュームに書き込まれたデータを記録します。
- 再開されたミラーペアでは、同期が再開されたときにミラーペアのセカンダリボリュームにデータを自動的に書き込みます。完全同期は必要ありません。

ミラーペア内のボリューム間でのロールの変更

同期ミラーリングに参加しているミラーペア内の2つのボリューム間でロール反転を実行できます。このタスクは、管理目的やローカルストレージアレイで災害が発生した場合に必要になることがあります。

タスクの内容

プライマリボリュームをセカンダリロールに降格するか、セカンダリボリュームをプライマリロールに昇格できます。プライマリボリュームにアクセスしているホストには、そのボリュームに対する読み取り/書き込みアクセス権があります。プライマリボリュームがセカンダリボリュームになると、プライマリコントローラによって開始されたリモート書き込みだけがボリュームに書き込まれます。

手順

1. 選択メニュー：Storage [Synchronous Mirroring]
2. ロールを変更するボリュームが含まれているミラーペアを選択し、メニューから[More]（その他）[Change Role]（ロールの変更）を選択します。

   確認メッセージが表示されます。
3. ボリュームのロールを変更することを確認し、*ロールの変更*を選択します。

> ローカルストレージアレイがリモートストレージアレイと通信できない場合、ロールの変更が要求されたときにシステムに[ストレージアレイにアクセスできません]ダイアログボックスが表示されますが、リモートストレージアレイにアクセスできません。[はい]をクリックして、強制的にロールを変更します。

結果

System Managerは次の処理を実行します。

- ミラーペア内の関連付けられているボリュームにアクセスできる場合は、ボリューム間でロールが変更されます。選択内容に応じて、ミラーペアのセカンダリボリュームのロールがプライマリに昇格されるか、プライマリボリュームのロールがセカンダリに降格されます。

ミラーペアの同期設定の変更

ミラーペアが通信の中断後に再同期処理を完了するために使用する同期優先度と再同期ポリシーを変更できます。

タスクの内容

ミラーペアの同期設定は、プライマリボリュームを含むストレージアレイでのみ編集できます。

手順

1. 選択メニュー：Storage [Synchronous Mirroring]
2. 編集するミラーペアを選択し、メニューから[More（詳細）][Edit settings（設定の編集）]を選択します。

   [設定の表示/編集]ダイアログボックスが表示されます。

3. スライダバーを使用して同期優先度を編集します。

   同期優先度は、I/O要求の処理と比較して、通信中断後の再同期処理を完了するために使用されるシステムリソースの量を決定します。

   同期レートの詳細

   同期優先度は5段階で設定できます。

   - 最低
   - 低
   - 中
   - 高
   - 最高

   同期優先度を最低に設定すると、I/Oアクティビティが優先され、再同期処理にかかる時間が長くなります。同期優先度が最高に設定されている場合は再同期処理が優先されますが、ストレージアレイのI/Oアクティビティに影響する可能性があります。

4. 再同期ポリシーを適宜編集します。

   リモートストレージアレイのミラーペアを手動または自動で再同期できます。

   - 手動（推奨オプション）-ミラーペアとの通信が回復したあとに同期を手動で再開する場合に選択します。このオプションは、データをリカバリするための最良の機会を提供します。
   - 自動--ミラーペアとの通信が回復した後、再同期を自動的に開始する場合に選択します。

5. [保存（ Save ）] を選択します。

同期ミラー関係の削除

ミラーペアを削除して、ローカルストレージアレイ上のプライマリボリュームとリモートストレージアレイ上のセカンダリボリュームからミラー関係を削除します。

タスクの内容

孤立したミラーペアの状態を修正するために、ミラーペアを削除することもできます。孤立したミラーペアに関する次の情報を確認します。

- 孤立したミラーペアは、一方（ローカル/リモート）でメンバーボリュームが削除され、もう一方では削除されていない場合に発生します。
- 孤立したミラーペアは、アレイ間の通信がリストアされたときに検出されます。

手順

1. 選択メニュー：Storage [Synchronous Mirroring]
2. 削除するミラーペアを選択し、メニューから「一般的でないタスク[削除]」を選択します。

   [ミラー関係の削除]ダイアログボックスが表示されます。

3. ミラーペアの削除を確認し、* Remove *をクリックします。

結果

System Managerは次の処理を実行します。

- ローカルストレージアレイとリモートストレージアレイのミラーペアからミラー関係を削除します。
- ホストがアクセス可能でミラーされていないボリュームにプライマリボリュームとセカンダリボリュームを戻します。
- 同期ミラーペアの削除を反映して[同期ミラーリング]タイルを更新します。

ミラーリングをアクティブ化

非同期ミラーリングの非アクティブ化

ローカルとリモートのストレージアレイで非同期ミラーリングを非アクティブ化すると、ストレージアレイの専用ポートを通常の用途に戻すことができます。

開始する前に

- すべてのミラー関係を削除しておく必要があります。ローカルとリモートのストレージアレイからすべてのミラー整合性グループとミラーペアが削除されていることを確認します。
- ローカルストレージアレイとリモートストレージアレイがFibre ChannelファブリックまたはiSCSIインターフェイスを介して接続されている必要があります。

タスクの内容

非同期ミラーリングを非アクティブ化すると、ローカルとリモートのストレージアレイでミラー処理が実行されなくなります。

手順

1. メニューを選択します。Storage [非同期ミラーリング]。
2. メニューから[一般的でないタスク]を選択します。

   確認メッセージが表示されます。

3. 「はい」を選択して確定します。

結果

- 非同期ミラーリング通信専用で使用されていたコントローラのHBAホストチャネルで、ホストの読み取り要求と書き込み要求を受け付けることができるようになります。
- このストレージアレイのどのボリュームも、プライマリボリュームまたはセカンダリボリュームとしてミラー関係に参加できません。

ストレージアレイで同期ミラーリング機能を非アクティブ化すると、ミラーデータの転送用に予約されていたホストバスアダプタ（HBA）ホストポート4の通常の使用を再確立できます。

開始する前に

すべての同期ミラー関係を削除しておく必要があります。ストレージアレイからすべてのミラーペアが削除されていることを確認します。

手順

1. 選択メニュー：Storage [Synchronous Mirroring]
2. メニューから[一般的でないタスク]を選択します。

   確認メッセージが表示されます。

3. 「はい」を選択して確定します。

結果

- 同期ミラーリング通信専用に使用されていたコントローラのHBAホストポート4が、ホストの読み取り要求と書き込み要求を受け入れるようになりました。
- ストレージアレイのリザーブ容量ボリュームが削除されます。

非同期に関する**FAQ**

非同期ミラーリングと同期ミラーリングの違いは何ですか？

非同期ミラーリング機能と同期ミラーリング機能の重要な点は、非同期ミラーリング機能がソースボリュームの特定の時点の状態をキャプチャし、前回のイメージキャプチャ以降に変更されたデータのみをコピーするという点です。

同期ミラーリングでは、プライマリボリュームの状態はある時点でキャプチャされるのではなく、プライマリボリュームで行われたすべての変更がセカンダリボリュームに反映されます。このタイプのミラーでは、プライマリボリュームへの書き込みが行われるたびにセカンダリボリュームへの書き込みが行われるため、セカンダリボリュームは常にプライマリボリュームと同一です。プライマリボリュームで行われた変更でセカンダリボリュームが更新されるまで、ホストは書き込みが成功したという確認応答を受信しません。

非同期ミラーリングでは、リモートストレージアレイはローカルストレージアレイと完全に同期されません。そのため、ローカルストレージアレイの損失によってアプリケーションをリモートストレージアレイに移行する必要がある場合、一部のトランザクションが失われる可能性があります。

ミラーリングフィーチャー間の比較：

非同期ミラーリング	同期ミラーリング
レプリケーション方法	• ポイントインタイム ミラーリングはオンデマンドで、またはユーザ定義のスケジュールに従って自動的に行われます。スケジュールは分単位で定義できます。同期の最小間隔は10分です。
• 連続 ミラーリングは継続して自動的に実行され、ホストに書き込みがあるたびにデータがコピーされます。	リザーブ容量
• 複数 ミラーペアごとにリザーブ容量ボリュームが1つ必要です。	• * シングル * すべてのミラーボリュームにリザーブ容量ボリュームが1つ必要です。
通信	• * iSCSIおよびファイバ・チャネル* ストレージアレイ間でiSCSIインターフェイスとFibre Channelインターフェイスをサポートします。
• ファイバ・チャネル ストレージアレイ間でFibre Channelインターフェイスのみがサポートされます。	距離
• 無制限 ローカルストレージアレイとリモートストレージアレイの間でサポートされる距離は事実上無制限で、通常はネットワークとチャネル拡張テクノロジの機能によってのみ距離が制限されます。	• 制限付き レイテンシとアプリケーションパフォーマンスの要件を満たすために、通常はローカルストレージアレイから約10km（6.2マイル）以内である必要があります。

選択したミラーリング機能にアクセスできないのはなぜですか？

ミラーリングはUnified Managerインターフェイスで設定されます。

同期ミラーリングはEF600またはEF300ストレージアレイでは使用できません。

2つのアレイ間のミラーリングを有効にして設定するには、次の点を確認します。

- Web Services Proxyサービスが実行されている必要があります。（Unified Managerは、Web Services Proxyとともにホストシステムにインストールされます）。
- Unified ManagerがHTTPS接続経由でローカルホストで実行されている必要があります。
- ミラーリングに使用する2つのストレージアレイがUnified Managerで検出されている必要があります。
- Unified Managerには、ストレージアレイの有効なSSL証明書が必要です。自己署名証明書を受け入れることも、Unified ManagerからCA署名証明書をインストールすることもできます。

設定手順については、次を参照してください。

- "非同期ミラーペアの作成（Unified Manager）"
- "同期ミラーペアの作成（Unified Manager）"

ミラー整合性グループを作成するときは、どのような点に注意する必要がありますか？

ミラー整合性グループを作成する際は、次のガイドラインに従ってください。

同期ミラーリングは、EF600またはEF300ストレージシステムでは使用できません。

Unified Managerのミラーペアの作成ウィザードで整合性グループを作成しておきます。

Unified Managerに関する次の要件を満たしている必要があります。

- Web Services Proxyサービスが実行されている必要があります。
- Unified ManagerがHTTPS接続経由でローカルホストで実行されている必要があります。
- Unified Managerにストレージアレイの有効なSSL証明書が表示されている必要があります。Unified Managerのメニューから「Certificate Management」に移動し、自己署名証明書を受け入れるか、独自のセキュリティ証明書をインストールできます。

また、ストレージアレイに関する次の要件も満たしている必要があります。

- Unified Managerで2つのストレージアレイが検出されている必要があります。
- 各ストレージアレイに2台のコントローラが必要です。
- プライマリアレイとセカンダリアレイの両方の各コントローラにイーサネット管理ポートが設定され、ネットワークに接続されている必要があります。
- ストレージアレイに必要なファームウェアの最小バージョンは7.84です（それぞれ異なるOSバージョンを実行できます）。
- ローカルとリモートのストレージアレイのパスワードを確認しておく必要があります。
- ローカルとリモートのストレージアレイをFibre ChannelファブリックまたはiSCSIインターフェイスを介して接続します。

非同期ミラーリング-ミラーペアを作成するときは、どのような点に注意する必要がありますか？

ミラーペアはUnified Managerインターフェイスで設定し、System Managerで管理します。

ミラーペアを作成する前に、次のガイドラインに従ってください。

- 2つのストレージアレイが必要です。
- 各ストレージアレイに2台のコントローラが必要です。
- プライマリアレイとセカンダリアレイの両方の各コントローラにイーサネット管理ポートが設定され、ネットワークに接続されている必要があります。
- ローカルとリモートのストレージアレイをFibre Channelファブリックまたはiscsiインターフェイスを介して接続します。
- ストレージアレイに必要なファームウェアの最小バージョンは7.84です（それぞれ異なるOSバージョンを実行できます）。
- ローカルとリモートのストレージアレイのパスワードを確認しておく必要があります。
- ミラーリングするプライマリボリューム以上のセカンダリボリュームを作成するには、リモートストレージアレイに十分な空き容量が必要です。
- Web Services ProxyとUnified Managerをインストールしておきます。Unified Managerインターフェイスでミラーペアが設定されている必要があります。
- Unified Managerで2つのストレージアレイが検出されている必要があります。
- ストレージアレイに少なくとも1つのミラー整合性グループが含まれている必要があります。Unified Managerのミラーペアの作成ウィザードで整合性グループを作成しておきます。

ミラーペアボリュームでリザーブ容量を増やすときは、どのような点に注意する必要がありますか？

通常は、ミラーペアのリザーブ容量がフルに近づいているという警告が表示されたときにリザーブ容量を拡張します。リザーブ容量は8GiB単位でのみ拡張できます。

非同期ミラーリング処理のリザーブ容量は、通常はベースボリュームの20%です。次のいずれかまたは両方に該当する場合は、リザーブ容量を大きくします。

- ミラーペアを長期間保持する場合。
- 大量のI/Oアクティビティにより、プライマリボリュームのデータブロックの大部分で変更が発生する場合。プライマリボリュームに対する一般的なI/Oアクティビティを判断するには、過去のパフォーマンスデータやその他のオペレーティングシステムユーティリティを使用します。

ミラーペアのリザーブ容量を増やすには、次のいずれかを実行します。

- ミラーペアボリュームの容量の割合を調整するには、メニューからStorage（Pool and Volumes Groups）を選択し、* Reserved Capacity *タブをクリックします。
- プールまたはボリュームグループの使用可能な空き容量を使用して新しいボリュームを作成します。

  プールまたはボリュームグループに空き容量がない場合は、未設定の容量を未使用ドライブの形式でプールまたはボリュームグループに追加できます。

リザーブ容量を要求した量で増やせない場合、どのような理由が考えられますか？

リザーブ容量は4GiB単位でのみ拡張できます。

次のガイドラインを確認してください。

- 必要に応じて拡張できるように、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。

  プールまたはボリュームグループに空き容量がない場合は、未割り当て容量を未使用ドライブの形式でプールまたはボリュームグループに追加できます。

- プールまたはボリュームグループ内のボリュームのステータスが最適で、変更処理の実行中でないことを確認してください。
- プールまたはボリュームグループに容量の拡張に使用する空き容量が必要です。

非同期ミラーリング処理では、リザーブ容量は通常ベースボリュームの20%です。ベースボリュームで多くの変更が見込まれる場合や、ストレージオブジェクトのコピーサービス処理の使用期間が非常に長くなることが想定される場合は、これよりも割合を増やしてください。

この割合を変更するのはなぜですか？

リザーブ容量は、通常、Snapshot処理の場合はベースボリュームの40%、非同期ミラーリング処理の場合はベースボリュームの20%です。

通常はこの容量で十分です。必要な容量は、ベースボリュームに対するI/O書き込みの頻度とサイズ、およびストレージオブジェクトのコピーサービス処理を使用する期間によって異なります。

一般に、次のいずれかまたは両方に該当する場合は、リザーブ容量の割合を大きくします。

- 特定のストレージオブジェクトのコピーサービス処理の期間が非常に長い場合。
- 大量のI/Oアクティビティにより、ベースボリュームのデータブロックの大部分で変更が発生する場合。ベースボリュームに対する一般的なI/Oアクティビティを判断するには、過去のパフォーマンスデータやその他のオペレーティングシステムユーティリティを使用します。

リザーブ容量の候補が複数表示されるのはなぜですか？

プールまたはボリュームグループ内にストレージオブジェクトに対して選択した容量の割合を満たすボリュームが複数ある場合は、複数の候補が表示されます。

ベースボリューム上でコピーサービス処理用にリザーブする物理ドライブスペースの割合を変更すると、推奨される候補のリストを更新できます。選択に基づいて最適な候補が表示されます。

表に「**Not available values**」と表示されるのはなぜですか？

リモートストレージアレイにあるデータを表示できない場合は、テーブルにNot availableという値が表示されます。

リモートストレージアレイのデータを表示するには、Unified ManagerからSystem Managerを起動します。

プールとボリュームグループが一部表示されないのはなぜですか？

非同期ミラーペアのセカンダリボリュームを作成すると、その非同期ミラーペアに対応するすべてのプールとボリュームグループのリストが表示されます。使用できないプールまたはボリュームグループはリストに表示されません。

次のいずれかの理由で、プールまたはボリュームグループを使用できない可能性があります。

- プールまたはボリュームグループのセキュリティ機能が一致しません。
- プールまたはボリュームグループの状態が最適でない。
- プールまたはボリュームグループの容量が小さすぎます。

非同期ミラーリング-ボリュームが一部表示されないのはなぜですか？

ミラーペアのプライマリボリュームを選択すると、対応するすべてのボリュームのリストが表示されます。

使用できないボリュームはリストに表示されません。次のいずれかの理由でボリュームを使用できない可能性があります。

- 最適状態でない。
- すでにミラー関係に参加している。
- シンボリュームの場合は、自動拡張を有効にする必要があります。

> EF600およびEF300コントローラでは、非同期ミラーペアのプライマリボリュームとセカンダリボリュームのプロトコル、トレイレベル、セグメントサイズ、セキュリティタイプ、およびRAIDレベルが同じである必要があります。対応していない非同期ミラーペアは、使用可能なボリュームのリストに表示されません。

非同期ミラーリング-リモートストレージアレイのボリュームが一部表示されないのはなぜですか？

リモートストレージアレイ上のセカンダリボリュームを選択すると、そのミラーペアに対応するすべてのボリュームのリストが表示されます。

使用できないボリュームはリストに表示されません。次のいずれかの理由で、ボリュームが対象外になっている可能性があります。

- 最適状態でない。
- すでにミラー関係に参加している。
- シンボリュームの属性がプライマリボリュームとセカンダリボリュームで一致しません。
- Data Assurance（DA）を使用する場合、プライマリボリュームとセカンダリボリュームでDA設定を同じにする必要があります。
  - プライマリボリュームでDAを有効にする場合、セカンダリボリュームでもDAを有効にする必要があります。
  - プライマリボリュームでDAを有効にしない場合、セカンダリボリュームでもDAを無効にする必要があります。

リモートストレージアレイのIPアドレスを更新するのはどのような場合ですか？

リモートストレージアレイのIPアドレスを更新するのは、iSCSIポートのIPアドレスが変わってローカルストレージアレイがリモートストレージアレイと通信できなくなった場合です。

iSCSI接続を使用して非同期ミラーリング関係を確立すると、ローカルストレージアレイとリモートストレージアレイの両方で、リモートストレージアレイのIPアドレスのレコードが非同期ミラーリング構成に保存されます。iSCSIポートのIPアドレスが変わると、そのポートを使用しようとしているリモートストレージアレイで通信エラーが発生します。

IPアドレスが変更されたストレージアレイは、iSCSI接続を介してミラーリングするように設定されたミラー整合性グループに関連付けられている各リモートストレージアレイにメッセージを送信します。このメッセージを受け取ったストレージアレイは、リモートターゲットのIPアドレスを自動的に更新します。

IPアドレスが変更されたストレージアレイがアレイ間メッセージをリモートストレージアレイに送信できない場合は、接続問題 のアラートが送信されます。Update Remote IP Addressオプションを使用して、ローカルストレージアレイとの接続を再確立します。

同期に関するFAQ

非同期ミラーリングと同期ミラーリングの違いは何ですか？

非同期ミラーリング機能と同期ミラーリング機能の重要な点は、非同期ミラーリング機能がソースボリュームの特定の時点の状態をキャプチャし、前回のイメージキャプチャ以降に変更されたデータのみをコピーするという点です。

同期ミラーリングでは、プライマリボリュームの状態はある時点でキャプチャされるのではなく、プライマリボリュームで行われたすべての変更がセカンダリボリュームに反映されます。このタイプのミラーでは、プライマリボリュームへの書き込みが行われるたびにセカンダリボリュームへの書き込みが行われるため、セカンダリボリュームは常にプライマリボリュームと同一です。プライマリボリュームで行われた変更でセカンダリボリュームが更新されるまで、ホストは書き込みが成功したという確認応答を受信しません。

非同期ミラーリングでは、リモートストレージアレイはローカルストレージアレイと完全に同期されません。そのため、ローカルストレージアレイの損失によってアプリケーションをリモートストレージアレイに移行する必要がある場合、一部のトランザクションが失われる可能性があります。

ミラーリングフィーチャー間の比較：

非同期ミラーリング	同期ミラーリング
レプリケーション方法	• ポイントインタイム ミラーリングはオンデマンドで、またはユーザ定義のスケジュールに従って自動的に行われます。スケジュールは分単位で定義できます。同期の最小間隔は10分です。
• 連続 ミラーリングは継続して自動的に実行され、ホストに書き込みがあるたびにデータがコピーされます。	リザーブ容量

非同期ミラーリング	同期ミラーリング
• 複数 ミラーペアごとにリザーブ容量ボリュームが1つ必要です。	• * シングル * すべてのミラーボリュームにリザーブ容量ボリュームが1つ必要です。
通信	• * iSCSIおよびファイバ・チャネル* ストレージアレイ間でiSCSIインターフェイスとFibre Channelインターフェイスをサポートします。
• ファイバ・チャネル ストレージアレイ間でFibre Channelインターフェイスのみがサポートされます。	距離
• 無制限 ローカルストレージアレイとリモートストレージアレイの間でサポートされる距離は事実上無制限で、通常はネットワークとチャネル拡張テクノロジの機能によってのみ距離が制限されます。	• 制限付き レイテンシとアプリケーションパフォーマンスの要件を満たすために、通常はローカルストレージアレイから約10km（6.2マイル）以内である必要があります。

同期ミラーリング-ボリュームが一部表示されないのはなぜですか？

ミラーペアのプライマリボリュームを選択すると、対応するすべてのボリュームのリストが表示されます。

使用できないボリュームはリストに表示されません。次のいずれかの理由で、ボリュームが対象外になっている可能性があります。

- 標準以外のボリューム（Snapshotボリュームやシンボリュームなど）である。
- 最適状態でない。
- すでにミラー関係に参加している。

同期ミラーリング-リモートストレージアレイのボリュームが一部表示されないのはなぜですか？

リモートストレージアレイ上のセカンダリボリュームを選択すると、そのミラーペアに対応するすべてのボリュームのリストが表示されます。

使用できないボリュームはリストに表示されません。次のいずれかの理由で、ボリュームが対象外になっている可能性があります。

- 標準以外のボリューム（Snapshotボリュームやシンボリュームなど）である。

- 最適状態でない。
- すでにミラー関係に参加している。
- Data Assurance（DA）を使用する場合、プライマリボリュームとセカンダリボリュームでDA設定を同じにする必要があります。
  - プライマリボリュームでDAを有効にする場合、セカンダリボリュームでもDAを有効にする必要があります。
  - プライマリボリュームでDAを有効にしない場合、セカンダリボリュームでもDAを無効にする必要があります。

同期ミラーリング-ミラーペアを作成するときは、どのような点に注意する必要がありますか？

ミラーペアはUnified Managerインターフェイスで設定し、System Managerで管理します。

ミラーペアを作成する前に、次のガイドラインに従ってください。

- 2つのストレージアレイが必要です。
- 各ストレージアレイに2台のコントローラが必要です。
- プライマリアレイとセカンダリアレイの両方の各コントローラにイーサネット管理ポートが設定され、ネットワークに接続されている必要があります。
- ローカルとリモートのストレージアレイをFibre Channelファブリックを介して接続します。
- ストレージアレイに必要なファームウェアの最小バージョンは7.84です（それぞれ異なるOSバージョンを実行できます）。
- ローカルとリモートのストレージアレイのパスワードを確認しておく必要があります。
- ミラーリングするプライマリボリューム以上のセカンダリボリュームを作成するには、リモートストレージアレイに十分な空き容量が必要です。
- Web Services ProxyとUnified Managerをインストールしておきます。Unified Managerインターフェイスでミラーペアが設定されている必要があります。
- Unified Managerで2つのストレージアレイが検出されている必要があります。

同期優先度は同期速度にどのような影響を与えますか？

同期優先度は、システムパフォーマンスに対する同期アクティビティに割り当てる処理時間を定義します。

プライマリボリュームのコントローラ所有者はこの処理をバックグラウンドで実行します。同時にコントローラ所有者は、プライマリボリュームへのローカルのI/O書き込みと、対応するセカンダリボリュームへのリモートの書き込みを処理します。再同期には、I/Oアクティビティに使用されるはずのコントローラの処理リソースが使用されるため、再同期がホストアプリケーションのパフォーマンスに影響する可能性があります。

同期優先度に応じた所要時間や、同期優先度がシステムパフォーマンスに与える影響を特定する際には、次のガイドラインに注意してください。

同期優先度について

次のプライオリティレートを使用できます。

- 最低
- 低
- 中
- 高
- 最高

優先度が最低の場合はシステムパフォーマンスがサポートされますが、再同期にかかる時間は長くなります。最も優先度が高い場合は再同期がサポートされますが、システムパフォーマンスが低下する可能性があります。

これらのガイドラインは、優先度の大まかな違いを示しています。

完全同期の優先度	最高の同期速度と比較した経過時間
最低	最高プライオリティレートの約8倍の長さになります。
低	最高プライオリティレートの約6倍の長さになります。
中	最高プライオリティレートの約3.5倍の長さになります。
高	最高プライオリティレートの約2倍の時間がかかります。

同期の所要時間には、ボリュームサイズとホストのI/O速度が影響します。

手動同期ポリシーの使用が推奨されるのはなぜですか。

手動再同期が推奨されるのは、データがリカバリされる可能性が最も高い方法で再同期プロセスを管理できるためです。

自動再同期ポリシーを使用していて、再同期中に通信が中断する問題が発生した場合は、セカンダリボリューム上のデータが一時的に破損する可能性があります。再同期が完了すると、データは修正されます。

リモートストレージ

リモートストレージ機能の概要

リモートストレージ機能が搭載されている場合は、リモートストレージシステムからストレージアレイにデータをインポートできます。

リモートストレージ機能とは何ですか？

リモートストレージ機能を使用すると、リモートストレージシステムからローカルのEシリーズストレージシステムにデータをインポートできます。リモートシステムには、別のEシリーズシステムを使用することも、別のベンダーのシステムを使用することもできます。この機能は、機器のアップグレード時など、ダウンタイムを最小限に抑えながらデータ移行を合理化したい場合に役立ちます。

リモートストレージを使用するには、サブモデルID（SMID）でこの機能を有効にする必要があります。

詳細：

- "リモートストレージの仕組み"
- "リモートストレージの用語"
- "リモートストレージの要件"
- "リモートストレージボリュームの要件"

この機能を使用してデータをインポートする方法を教えてください。

リモートストレージウィザードを使用して、リモートストレージデバイス（データのインポート元）をEシリーズシステム上のターゲットボリュームにマッピングします。このウィザードは、ストレージ[リモートストレージ]メニューから使用できます。

詳細：

- "リモートストレージのインポート"
- "データインポートの進行状況を管理します。"

概念

リモートストレージの仕組み

リモートストレージ機能を使用すると、リモートストレージシステムからローカルのEシリーズストレージシステムにデータをインポートできます。この機能は、機器のアップグレード時など、ダウンタイムを最小限に抑えながらデータ移行を合理化したい場合に役立ちます。

リモートストレージ機能を設定するには、ハードウェアをセットアップし、System Managerを使用してリモートストレージオブジェクトを作成する必要があります。この設定が完了すると、インポートプロセスが開始されます。

ハードウェアのセットアップ

次のワークフローを使用して、ハードウェア接続を準備します。

これらの手順の詳細については、リモートストレージ機能のユーザガイドを参照してください。このユーザガイドは、EシリーズおよびSANtricityのドキュメントセンター、およびで "Remote Storageテクニカルレポート"入手でき "Remote Storage Volumesの概要"ます。

ローカルのEシリーズストレージシステムで、次の手順を実行します。

1. 各コントローラからリモートストレージシステムへのiSCSI接続が確立されていることを確認します。この接続では、ローカルのEシリーズシステムがiSCSIイニシエータとして機能し、リモートシステムでホストとしてセットアップできます。
2. インポート処理のデスティネーションボリュームを作成します。ボリュームの容量がリモートストレージシステムのソースボリューム以上で、ブロックサイズが同じで、マッピングされていないことを確認してください。を参照して "ボリュームの作成"
3. System Managerインターフェイスから、ローカルのEシリーズシステムのiSCSI Qualified Name（IQN）を収集します。このIQNは、あとでローカルのEシリーズシステムをリモートストレージシステムのホストとしてセットアップする際に使用します。System Managerで、次のメニューに移動します。Settings（システム）> iSCSI settings（iSCSI設定）> Target IQN（ターゲットIQN）の順に選択します。

リモート・ストレージ・システム：

1. IQNを使用して、ローカルのEシリーズシステムをリモートシステムのホストとしてセットアップします。適切なホストタイプを次のように設定してください。
   - リモートシステムがEシリーズモデルの場合は、を参照してください"ホストおよびホストクラスタの概要"。「工場出荷時のデフォルト」のホストタイプを使用します。
   - リモートシステムが別のベンダーのものである場合は、使用可能なオプションに基づいて適切なホストタイプを選択します。
2. ソースボリュームのすべてのI/Oを停止し、ファイルシステムをアンマウントし、ホストまたはアプリケーションへの割り当てをすべて削除します。
3. 新しく作成したローカルのEシリーズストレージシステムホストにボリュームを割り当てます。
4. 選択したソースボリュームについて、インポートを作成できるように、リモートストレージシステムから次の情報を収集します。
   - iSCSI Qualified Name（IQN）
   - iSCSI IPアドレス
   - ソースボリュームのLUN番号

System Managerのセットアップ

インポート用のリモートストレージオブジェクトを作成するには、次のワークフローを使用します。

1. System Managerインターフェイスのリモートストレージウィザードを使用して、リモートストレージデバイス（データのインポート元）をEシリーズシステム上のターゲットボリュームにマッピングします。「完了」を選択すると、インポート処理が開始されます。
2. [処理を表示]ダイアログまたは[実行中の処理]パネルからインポートを監視します。必要に応じて、プロセスを一時停止および再開することもできます。
3. 必要に応じて、インポートの完了時にソースボリュームとターゲットボリュームの間の接続を切断するか、以降のインポート用に接続を維持します。

リモートストレージの用語

ストレージアレイに関連するリモートストレージの用語を次に示します。

期間	製品説明
IQN	iSCSI Qualified Name（IQN）識別子。iSCSIイニシエータまたはターゲットの一意の名前です。
LUN	論理ユニット番号。アクセス用にホストに提供できる論理ユニットを識別するために使用されます。
リモートストレージシステム	データが最初に格納されているストレージシステム。リモートストレージシステムは、Eシリーズモデルでも別のベンダーのシステムでもかまいません。
リモートストレージデバイス	データが最初にリモートシステムに保存される物理デバイスまたは論理デバイス。Eシリーズストレージシステムでは、これを「ボリューム」と呼びます。
リモートストレージオブジェクト	Eシリーズシステムがリモートストレージシステムを識別して接続できるようにする情報を含むオブジェクト。これには、リモートストレージシステムのIQNおよびIPアドレスが含まれます。リモートストレージオブジェクトは、リモートストレージシステムとEシリーズシステム間の通信を表します。
リモートストレージボリューム	リモートストレージデバイスへのデータアクセスを許可する、Eシリーズシステム上の標準ボリューム。
ボリューム	データが格納されるコンテナ。ホストがデータにアクセスするために作成される論理コンポーネントです。

リモートストレージ機能の要件

リモートストレージ機能を使用する前に、次の要件および制限事項を確認してください。

サポートされるプロトコル

サポートされるプロトコルは次のとおりです。

- iSCSI
- IPv4

Eシリーズの最新のサポートおよび設定情報については、を参照してください "NetApp Interoperability Matrix Tool"。

ハードウェア要件

Eシリーズストレージシステムには次のものが含まれている必要があります。

- コントローラ×2（デュプレックスモード）
- 両方のEシリーズコントローラのiSCSI接続（1つ以上のiSCSI接続を介してリモートストレージシステムと通信する場合）
- SANtricity OS 11.71以降

- サブモデルID（SMID）でリモートストレージ機能が有効になっている

リモートシステムには、Eシリーズストレージシステムを使用することも、別のベンダーのシステムを使用することもできます。以下を含む必要があります。

- iSCSI対応インターフェイス

制限事項

リモートストレージ機能には、次の制限事項があります。

- ミラーリングを無効にする必要があります。
- EシリーズシステムのデスティネーションボリュームにSnapshotを含めることはできません。
- インポートを開始する前に、Eシリーズシステム上のデスティネーションボリュームをホストにマッピングしないでください。
- Eシリーズシステムのデスティネーションボリュームで、リソースプロビジョニングを無効にする必要があります。
- リモートストレージボリュームを1つのホストまたは複数のホストに直接マッピングすることはできません。
- Web Services Proxyはサポートされません。
- iSCSI CHAPシークレットはサポートされません。
- SMcliはサポートされていません。
- VMwareデータストアはサポートされません。
- インポートペアが存在する場合、関係/インポートペアに含まれるストレージシステムは一度に1つだけアップグレードできます。

リモートストレージボリュームの要件

インポートに使用するボリュームは、サイズ、ステータス、その他の条件を満たしている必要があります。

リモートストレージボリューム

インポートのソース ボリュームは「リモート ストレージ ボリューム」と呼ばれます。このボリュームは次の基準を満たす必要があります。

- 別のインポートに含めることはできません
- オンラインステータスである必要があります

インポートが開始されると、コントローラファームウェアはバックグラウンドでリモートストレージボリュームを作成します。そのため、リモートストレージボリュームはSystem Managerで管理できず、インポート処理にのみ使用できます。

作成されたリモートストレージボリュームは、次の例外を除き、Eシリーズシステム上の他の標準ボリュームと同様に扱われます。

- リモートストレージデバイスのプロキシとして使用できます。

- 他のボリュームコピーまたはSnapshotの候補として使用することはできません。
- インポートの実行中はData Assurance設定を変更することはできません。
- はどのホストにもマッピングできません。インポート処理用にのみ予約されています。

各リモートストレージボリュームは1つのリモートストレージオブジェクトにのみ関連付けられますが、1つのリモートストレージオブジェクトを複数のリモートストレージボリュームに関連付けることができます。リモートストレージボリュームは、次の組み合わせを使用して一意に識別されます。

- リモートストレージオブジェクトID
- リモートストレージデバイスのLUN番号

ターゲットボリューム候補

ターゲットボリュームは、ローカルのEシリーズシステムのデスティネーションボリュームです。デスティネーションボリュームは次の条件を満たしている必要があります。

- RAID / DDPボリュームである必要があります。
- リモートストレージボリューム以上の容量が必要です。
- ブロックサイズがリモートストレージボリュームと同じである必要があります。
- 有効な状態（最適）である必要があります。
- ボリュームコピー、Snapshotコピー、非同期ミラーリング、同期ミラーリングのいずれの関係も確立できません。
- 再設定処理を実行できません：動的ボリューム拡張、動的容量拡張、動的セグメントサイズ、動的 RAID 移行、動的な容量削減、 最適化。
- インポートの開始前にホストにマッピングすることはできません（ただし、インポートの完了後にマッピングすることはできます）。
- Flash Read Cached（FRC）を有効にできません。

これらの要件は、System Managerのリモートストレージインポートウィザードで自動的に確認されます。デスティネーションボリュームの選択には、すべての要件を満たすボリュームのみが表示されます。

リモートストレージの管理

リモートストレージのインポート

リモートシステムからローカルのEシリーズストレージシステムへのストレージのインポートを開始するには、リモートストレージのインポートウィザードを使用します。

開始する前に

- Eシリーズストレージシステムがリモートストレージシステムと通信するように設定されている必要があります。

ハードウェア構成については、リモートストレージ機能のユーザガイドを参照してください。このユーザガイドは、EシリーズおよびSANtricityのドキュメントセンター、およびで"Remote Storageテクニカルレポート"入手でき "ハードウェアの設定"ます。

- リモートストレージシステムについて、次の情報を収集します。
  - iSCSI IQN
  - iSCSI IPアドレス
  - リモートストレージデバイス（ソースボリューム）のLUN番号
- ローカルのEシリーズストレージシステムの場合、データのインポートに使用するボリュームを作成または選択します。を参照して "ボリュームの作成"ターゲットボリュームは次の要件を満たしている必要があります。
  - リモートストレージデバイス（ソースボリューム）のブロックサイズと一致します。
  - リモートストレージデバイスと同等以上の容量がある。
  - は最適な状態で使用可能です。

要件の完全なリストについては、を参照してください"リモートストレージボリュームの要件"。

- *推奨：*インポート処理を開始する前に、リモートストレージシステムのボリュームをバックアップしてください。

タスクの内容

このタスクでは、リモートストレージデバイスとローカルのEシリーズストレージシステム上のボリュームの間にマッピングを作成します。設定が完了すると、インポートが開始されます。

> 多くの変数がインポート操作とその完了時間に影響を与える可能性があるため、最初に小さい「テスト」インポートを実行することをお勧めします。これらのテストを使用して、すべての接続が想定どおりに機能し、インポート処理が適切な時間で完了することを確認します。

手順

1. 「ストレージ[リモートストレージ]」メニューを選択します。
2. [リモートストレージのインポート] をクリックします。

   リモートストレージをインポートするためのウィザードが表示されます。

3. ソースの設定パネルの*手順1a *で、接続情報を入力します。別のiSCSI接続を追加する場合は、*別のIPアドレスを追加*をクリックして、リモートストレージのIPアドレスを追加します。完了したら、 * 次へ * をクリックします。

フィールドの詳細

設定	製品説明
名前	System Managerインターフェイスでリモートストレージデバイスを識別するための名前を入力します。 名前には最大30文字を使用できます。使用できる文字は、アルファベット、数字、およびアンダースコア（_）、ダッシュ（-）、ハッシュ記号（#）のみです。名前にスペースを含めることはできません。
iSCSI接続プロパティ	リモートストレージデバイスの接続プロパティを入力します。 • * iSCSI Qualified Name（IQN）*：iSCSI IQNを入力します。 • **IP**アドレス: IPv4アドレスを入力します。 • ポート：ソース・デバイスとターゲット・デバイス間の通信に使用するポート番号を入力します。デフォルトでは、ポート番号は3260です。

「次へ」をクリックすると、ソースの設定パネルの*ステップ1b *が表示されます。

4. [**LUN**]フィールドで'ソースとして使用するリモート・ストレージ・デバイスのLUN番号を選択し'[次へ]をクリックします

   [ターゲットの設定]パネルが開き、インポートのターゲットとして使用するボリューム候補が表示されます。ブロックサイズ、容量、またはボリュームの可用性が原因で、一部のボリュームが候補のリストに表示されません。

5. テーブルから、Eシリーズストレージシステム上のターゲットボリュームを選択します。必要に応じて、スライダを使用してインポートの優先度を変更します。「 * 次へ * 」をクリックします。次のダイアログボックスでと入力し、* Continue *をクリックして操作を確定します `continue`。

   ターゲットボリュームの容量がソースボリュームよりも大きい場合、その追加容量はEシリーズシステムに接続されたホストには報告されません。新しい容量を使用するには、インポート処理が完了して切断されたあとに、ホストでファイルシステムの拡張処理を実行する必要があります。

   ダイアログで構成を確認すると、[Review]パネルが表示されます。

6. [レビュー]パネルで、設定が正しいことを確認し、[完了]をクリックしてインポートを開始します。

   別のインポートを開始するかどうかを確認するダイアログボックスが表示されます。

7. 必要に応じて、 * はい * をクリックして別のリモートストレージインポートを作成します。[ソースの設定]パネルの[はい]をクリックすると、[手順1a*]に戻ります。ここで、既存の構成を選択するか、新しい構成を追加できます。別のインポートを作成しない場合は、[いいえ（* No *）]をクリックしてダイアログボックスを終了します。

   インポートプロセスが開始されると、コピーしたデータでターゲットボリューム全体が上書きされます。このプロセス中にホストがターゲットボリュームに新しいデータを書き込むと、その新しいデータはリモートデバイス（ソースボリューム）に伝播されます。

8. 処理の進捗状況は、[リモートストレージ]パネルの[処理の表示]ダイアログで確認します。

結果

インポート処理が完了するまでの時間は、リモートストレージシステムのサイズ、インポートの優先度設定、およびストレージシステムと関連ボリュームの両方のI/O負荷によって異なります。

インポートが完了すると、ローカルボリュームはリモートストレージデバイスの複製になります。

終了後

2つのボリューム間の関係を解除する準備ができたら、インポートオブジェクトの「処理を実行中」ビューで「*切断」を選択します。関係を切断すると、ローカルボリュームのパフォーマンスは正常に戻り、リモート接続による影響はなくなります。

リモートストレージインポートの進捗状況を管理します。

インポートプロセスが開始されたら、その進行状況を表示して対処できます。

タスクの内容

[実行中の処理]ダイアログには、インポート処理ごとに完了率と推定残り時間が表示されます。処理には、インポート優先度の変更、処理の停止と再開、処理からの切断が含まれます。

進行中の処理は、ホームページ（メニュー：ホーム[進行中の処理を表示]）から表示することもできます。

手順

1. [リモートストレージ]ページで、[オペレーションの表示]を選択します。

   [実行中の処理]ダイアログボックスが表示されます。

2. 必要に応じて、[アクション*（* Actions *）]列のリンクを使用して、オペレーションの停止と再開、優先度の変更、またはオペレーションからの切断を行います。
   - 優先度の変更--進行中または保留中のオペレーションの処理優先度を変更するには'*Change Priority*を選択しますオペレーションに優先度を適用し、 * OK * をクリックする。
   - 停止--リモートストレージデバイスからのデータのコピーを一時停止するには'*Stop*を選択しますインポートペア間の関係はそのままです。インポート操作を続行する準備ができたら、 * 再開 * を選択できます。
   - 再開--停止したプロセスまたは停止したプロセスを'停止したプロセスまたは停止したプロセスを開始するには'*Resume*を選択します次に、レジューム操作に優先度を適用し、 * OK * をクリックします。この操作は'インポートを最初から再開しない（_not_restart）最初からプロセスを再開する場合は、「 * 切断」を選択し、リモートストレージのインポートウィザードを使用してインポートを再作成する必要があります。
   - 切断-停止、完了、または失敗したインポート処理のソースボリュームとデスティネーションボリュームの関係を解除するには、「*切断」を選択します。

リモートストレージの接続設定を変更します。

[設定の表示/編集]オプションを使用して、リモートストレージ構成の接続設定を編集、追加、削除できます。

タスクの内容

接続プロパティを変更すると、実行中のインポートに影響します。接続プロパティの変更は、インポートが実行されていないときにのみ行ってください。

手順

1. 「ストレージ[リモートストレージ]」メニューを選択します。
2. 変更するリモートストレージオブジェクトをリストから選択します。
3. [* 設定の表示 / 編集 *] をクリックします。

   [リモートストレージ設定]ダイアログボックスが表示されます。

4. [接続のプロパティ *] タブをクリックします。

   リモートストレージインポート用に設定されているIPアドレスとポートの設定が表示されます。

5. 次のいずれかを実行します。
   - 編集--リモートストレージオブジェクトの対応する行アイテムの横にある*編集*をクリックします変更したIPアドレスまたはポート情報をフィールドに入力します。
   - *追加--*Add*をクリックして、表示されたフィールドに新しいIPアドレスとポート情報を入力します。[* 追加] をクリックして確定すると、リモートストレージオブジェクトのリストに新しい接続が表示されます。
   - 削除--リストから目的の接続を選択し、**Delete***をクリックします。表示されたフィールドにと入力して処理を確認し **`delete`**、[削除]*をクリックします。リモートストレージオブジェクトのリストから接続が削除されます。
6. [保存（ Save ）] をクリックします。

   変更した接続設定がリモートストレージオブジェクトに適用されます。

リモートストレージオブジェクトの削除

ローカルデバイスとリモートデバイス間でデータをコピーしない場合は、インポートの完了後にリモートストレージオブジェクトを削除できます。

開始する前に

削除するリモートストレージオブジェクトにインポートが関連付けられていないことを確認します。

タスクの内容

リモートストレージオブジェクトを削除すると、ローカルデバイスとリモートデバイス間の接続が削除されます。

手順

1. 「ストレージ[リモートストレージ]」メニューを選択します。
2. リストから、削除するリモートストレージオブジェクトを選択します。
3. [削除（ Remove ）] をクリックします。

   [リモートストレージ接続の削除の確認]ダイアログボックスが表示されます。

4. と入力し、*[削除]*をクリックして処理を確定します `remove`。

   選択したリモートストレージオブジェクトが削除されます。

FAQ

リモートストレージ接続を作成するときは、どのような点に注意する必要がありますか？

リモートストレージ機能を設定するには、リモートデバイスとターゲットストレージシステムをiSCSI経由で直接接続する必要があります。

iSCSIシステム接続をセットアップするには、以下を参照してください。

- "iSCSIポートの設定"
- "Remote Storageテクニカルレポート"

リモートボリュームの削除を求めるプロンプトが表示されるのはなぜですか？

リモートボリュームの最大数に達すると、使用されていないリモートボリュームがストレージシステムによって自動的に検出され、削除するように求められます。

一部のケースでは、使用されていないリモートボリュームが作成プロセスでクリーンアップされないことがあります。追加のインポート処理を開始する前に、システムが最適でネットワーク接続が安定していることを確認してください。

デスティネーションアレイにボリュームが一部表示されないのはなぜですか？

リモートストレージ機能のインポートを設定するときに、ブロックサイズ、容量、またはボリュームの可用性が原因で、一部のボリュームがターゲット候補のリストに表示されないことがあります。

ボリューム候補をリストに表示するには、次の条件が満たされている必要があります。

- リモートボリューム以上の容量。
- ブロックサイズがリモートボリュームと同じ。
- 最適の現在のステータス。

ボリュームの候補が次の条件を満たしている場合は、リストから除外されます。

- ボリュームコピー、Snapshot、ミラーリングのいずれかの関係。
- 再設定処理を実行中です。
- 別のデバイス（ホストまたはホストクラスタ）にマッピングしています。
- 読み取りフラッシュキャッシュが有効になりました。

インポートするリモートボリュームについて、どのような点に注意する必要がありますか？

リモートストレージ機能を使用する場合は、データのソースがリモートボリュームであることに注意してください。

インポートの実行中は、リモートボリュームからデスティネーションストレージシステム上のターゲットボリュームにデータが転送されます。これら2つのボリュームは、同じブロックサイズである必要があります。

リモートストレージのインポートを開始するときは、どのような点に注意する必要がありますか？

リモートストレージ機能を使用すると、リモートストレージシステムからローカルのEシリーズストレージシステム上のボリュームにデータをコピーできます。この機能を使用する前に、次のガイドラインを確認してください。

構成

リモートストレージインポートを作成する前に、次の操作を完了し、次の条件を確認する必要があります。

- ローカルのEシリーズストレージシステムの各コントローラにリモートストレージシステムへのiSCSI接続が確立されていることを確認します。
- ローカルのEシリーズストレージシステムで、インポート処理のターゲットボリュームを作成します。ボリュームの容量がソースボリューム以上で、ブロックサイズがソースボリュームと同じで、マッピングされていないことを確認してください。を参照して "ボリュームの作成"
- iSCSI Qualified Name（IQN）を使用して、ローカルのEシリーズストレージシステムをリモートシステムのホストとしてセットアップします。IQNは次のメニューから確認できます。Settings（システム）> iSCSI settings（iSCSI設定）> Target IQN（ターゲットIQN）。また、使用するシステムに基づいて適切なホストタイプを設定してください。
- リモートストレージシステム上の選択したボリュームについて、すべてのI/Oを停止し、ファイルシステムをアンマウントし、ホストまたはアプリケーションへの割り当てをすべて削除します。
- 新しく作成したローカルのEシリーズストレージシステムホストにボリュームを割り当てます。
- インポートを作成できるように、リモートストレージシステムから次の情報を収集します。
  - iSCSI Qualified Name（IQN）
  - iSCSI IPアドレス
  - ソースデータの発信元であるリモートストレージデバイスのLUN番号
- インポートプロセスが開始されると、ローカルデスティネーションボリューム全体がコピーされたデータで上書きされます。インポートの作成後、ローカルデスティネーションボリュームに新たに書き込まれたデータは、リモートストレージデバイス上のボリュームに伝播されます。そのため、インポートプロセスを開始する前に、リモートストレージシステム上のボリュームをバックアップすることを推奨します。

インポートプロセス

次の手順では、インポートプロセスの概要を説明します。

1. System Managerインターフェイスにアクセスし、* Remote Storage ページに移動します。「*読み込み」を選択して、新しいインポートの作成を開始します。詳細については、を参照してください"リモートストレージのインポート"。

オフラインインポートを実行する場合は、インポートが完了するまでデスティネーションボリュームをマッピングしないでください。

2. インポートの進捗状況を監視します。

   インポートが開始されたら、ターゲットボリュームをマッピングできます。インポート処理が完了するまでの時間は、リモートストレージデバイス（ソースボリューム）のサイズ、インポートの優先度の設定、ストレージシステムと関連付けられたボリュームの両方のI/O負荷によって異なります。

   インポートが完了すると、ターゲットボリュームはソースと同じボリュームになります。

3. マッピング関係を解除する準備ができたら、インポートオブジェクトに対して*操作実行中*パネルから*切断*を実行します。

インポートが切断されると、ローカルデスティネーションのパフォーマンスは通常の状態に戻り、リモート接続による影響はなくなります。

制限事項

リモートストレージ機能には、次の制限事項があります。

- ミラーリングを無効にする必要があります。
- EシリーズシステムのデスティネーションボリュームにSnapshotを含めることはできません。
- インポートを開始する前に、Eシリーズシステム上のデスティネーションボリュームをホストにマッピングしないでください。
- Eシリーズシステムのデスティネーションボリュームで、リソースプロビジョニングを無効にする必要があります。
- リモートストレージボリュームを1つのホストまたは複数のホストに直接マッピングすることはできません。
- Web Services Proxyはサポートされません。
- iSCSI CHAPシークレットはサポートされません。
- SMcliはサポートされていません。
- VMwareデータストアはサポートされません。
- インポートペアが存在する場合、関係/インポートペアに含まれるストレージシステムは一度に1つだけアップグレードできます。

追加情報

リモートストレージ機能の詳細については、を参照してください "Remote Storageテクニカルレポート"。

ハードウェアコンポーネント

ハードウェアコンポーネントの概要

[ハードウェア]ページでコンポーネントのステータスを確認し、それらのコンポーネントに関連するいくつかの機能を実行できます。

管理できるコンポーネント

コンポーネントのステータスを確認し、これらのコンポーネントに関連するいくつかの機能を実行できます。

- シェルフ--a_shelf_は、ストレージアレイのハードウェア(コントローラ、電源/ファンキャニスター、ドライブ)を含むコンポーネントです。シェルフのサイズは3つあり、それぞれ最大で12本、24本、60本のドライブを収容できます。
- コントローラ--a_controller_は'ストレージ・アレイと管理機能を実装するハードウェアとファームウェアの組み合わせですキャッシュメモリ、ドライブのサポート、およびホスト接続用のポートが含まれます。
- ドライブ--a_drive_に は、ハードディスクドライブ（HDD）またはソリッドステートドライブ（SSD）を使用できます。シェルフのサイズに応じて、最大12本、24本、または60本のドライブをシェルフに設置できます。

詳細：

- "ハードウェアページ"
- "ハードウェアの用語"

ハードウェアコンポーネントの表示方法を教えてください。

[ハードウェア]ページに移動します。このページには、ストレージアレイの物理コンポーネントが図で示されています。アレイシェルフの前面ビューと背面ビューを切り替えるには、シェルフビューの右上にある*タブまたは[コントローラ]*タブを選択します。

詳細：

- "シェルフコンポーネントのステータスと設定の表示"
- "コントローラ設定の表示"
- "ドライブのステータスと設定の表示"

関連情報

ハードウェアに関連する概念の詳細については、以下を参照してください。

- "コントローラの状態"
- "ドライブの状態"
- "シェルフ損失の保護とドロワー損失の保護"

概念

ハードウェアページとコンポーネント

[ハードウェア]ページには、ストレージアレイの物理コンポーネントがグラフィカルに表示されます。ここから、コンポーネントのステータスを確認し、それらのコンポーネントに関連するいくつかの機能を実行できます。

シェルフ

シェルフは、ストレージアレイのハードウェア（コントローラ、電源/ファンキャニスター、ドライブ）を搭載したコンポーネントです。シェルフには次の2種類があります。

- コントローラシェルフ-ドライブ、電源/ファンキャニスター、コントローラが搭載されています。
- ドライブシェルフ（または*拡張シェルフ*）--ドライブ、電源/ファンキャニスター、および入出力モジュール（IOM）2台が搭載されています。IOMは環境サービスモジュール（ESM）とも呼ばれ、ドライブシェルフをコントローラシェルフに接続するSASポートが搭載されています。

シェルフのサイズは3つあり、それぞれ最大で12本、24本、60本のドライブを収容できます。各シェルフには、コントローラファームウェアによって割り当てられたID番号が含まれています。IDはシェルフビューの左上に表示されます。

[ハードウェア]ページのシェルフビューには、前面または背面のコンポーネントが表示されます。ビューを切り替えるには、シェルフビューの右上から*タブまたは[コントローラ]タブを選択します。また、ページの下部から Show all front または Show all back *を選択することもできます。前面ビューと背面ビューには次の情報が表示されます。

- 前面コンポーネント--ドライブおよび空のドライブベイ。
- 背面コンポーネント--コントローラと電源/ファンキャニスター(コントローラシェルフ用)、またはIOMと電源/ファンキャニスター(ドライブシェルフ用)。

シェルフに関連して次の機能を実行できます。

- キャビネットまたはラック内でシェルフの物理的な場所を確認できるように、シェルフのロケーターライトを点灯します。
- シェルフビューの左上に表示されるID番号を変更します。
- 設置されているドライブのタイプやシリアル番号など、シェルフの設定を表示します。
- ストレージアレイの物理レイアウトに合わせて、シェルフビューを上下に移動します。

コントローラ

コントローラは、ハードウェアとファームウェアを組み合わせたもので、ストレージアレイと管理機能を実装します。キャッシュメモリ、ドライブのサポート、およびホストインターフェイスのサポートが含まれます。

コントローラに関連して次の機能を実行できます。

- 管理ポートのIPアドレスと速度を設定します。
- iSCSIホスト接続を設定します（iSCSIホストがある場合）。
- Network Time Protocol（NTP；ネットワークタイムプロトコル）サーバとDomain Name System（DNS；ドメインネームシステム）サーバを設定します。
- コントローラのステータスと設定を表示します。
- ローカルエリアネットワークの外部のユーザがコントローラのSSHセッションを開始し、設定を変更できるようにします。
- コントローラをオフライン、オンライン、またはサービスモードに切り替えます。

ドライブ

ストレージアレイには、ハードディスクドライブ（HDD）またはソリッドステートドライブ（SSD）を含めることができます。シェルフのサイズに応じて、最大12本、24本、または60本のドライブをシェルフに設置できます。

ドライブに関連して次の機能を実行できます。

- シェルフ内のドライブの物理的な場所を確認できるように、ドライブのロケーターライトを点灯します。
- ドライブのステータスと設定を表示します。
- ドライブを再割り当て（障害が発生したドライブを未割り当てのドライブに論理的に交換）し、必要に応じてドライブを手動で再構築します。
- 交換できるように、ドライブを手動で使用停止にします。（ドライブを使用停止にすると、交換前にドライブの内容をコピーできます）。
- ホットスペアを割り当てまたは割り当て解除します。
- ドライブを消去します。

ハードウェアの用語

ストレージアレイに関連するハードウェアの用語を次に示します。

一般的なハードウェア用語：

コンポーネント	製品説明
ベイ	ベイは、ドライブやその他のコンポーネントを取り付けるシェルフのスロットです。
コントローラ	コントローラは、ボード、ファームウェア、ソフトウェアで構成されます。ドライブを制御し、System Managerの機能を実装します。
コントローラシェルフ	コントローラシェルフには、一連のドライブと1つ以上のコントローラキャニスターが搭載されています。コントローラキャニスターには、コントローラ、ホストインターフェイスカード（HIC）、バッテリが搭載されます。
ドライブ	ドライブは、データの物理ストレージメディアとして使用される、電磁的な機械デバイスまたはソリッドステートメモリデバイスです。
ドライブシェルフ	ドライブシェルフは、拡張シェルフとも呼ばれ、一連のドライブと2つの入出力モジュール（IOM）が搭載されます。IOMにはSASポートが搭載されており、ドライブシェルフをコントローラシェルフまたは他のドライブシェルフに接続します。
IOM（ESM）	IOMは、ドライブシェルフをコントローラシェルフに接続するためのSASポートを含む入出力モジュールです。以前のコントローラモデルでは、IOMは環境サービスモジュール（ESM）と呼ばれていました。
電源/ファンキャニスター	電源/ファンキャニスターは、シェルフに挿入するアセンブリです。電源装置と一体型ファンで構成されます。
SFP	SFPは、Small Form-factor Pluggable（SFP）トランシーバです。
シェルフ	シェルフは、キャビネットまたはラックに設置されるエンクロージャです。ストレージアレイのハードウェアコンポーネントが含まれています。シェルフには、コントローラシェルフとドライブシェルフの2種類があります。コントローラシェルフにはコントローラとドライブが搭載されます。ドライブシェルフには、入出力モジュール（IOM）とドライブが搭載されています。
ストレージアレイ	ストレージアレイには、シェルフ、コントローラ、ドライブ、ソフトウェア、およびファームウェアが含まれます。

コントローラの用語：

コンポーネント	製品説明
コントローラ	コントローラは、ボード、ファームウェア、ソフトウェアで構成されます。ドライブを制御し、System Managerの機能を実装します。
コントローラシェルフ	コントローラシェルフには、一連のドライブと1つ以上のコントローラキャニスターが搭載されています。コントローラキャニスターには、コントローラ、ホストインターフェイスカード（HIC）、バッテリが搭載されます。
DHCP	Dynamic Host Configuration Protocol（DHCP；動的ホスト構成プロトコル）は、IPアドレスなどのネットワーク構成パラメータを動的に配布するためにインターネットプロトコル（IP）ネットワークで使用されるプロトコルです。
DNS	Domain Name System（DNS；ドメインネームシステム）は、インターネットまたはプライベートネットワークに接続されたデバイスの命名システムです。DNSサーバはドメイン名のディレクトリを維持し、インターネットプロトコル（IP）アドレスに変換します。
デュプレックス構成	デュプレックスは、ストレージアレイ内に2台のコントローラモジュールを配置した構成です。デュプレックスシステムでは、コントローラ、論理ボリュームパス、およびディスクパスに関して完全な冗長性が確保されます。一方のコントローラで障害が発生した場合、そのI/Oがもう一方のコントローラに引き継がれて可用性が維持されます。デュプレックスシステムには、ファンと電源装置も冗長構成になっています。
全二重/半二重接続	全二重と半二重は、接続モードを指します。全二重モードでは、2つのデバイスが両方向で同時に通信できます。半二重モードでは、デバイスは一度に一方向に通信できます（一方のデバイスはメッセージを送信し、もう一方のデバイスはメッセージを受信します）。
HIC	ホストインターフェイスカード（HIC）は、コントローラキャニスターにオプションで取り付けることができます。コントローラに搭載されたホストポートはベースボードホストポートと呼ばれます。HICに組み込まれているホストポートは、HICポートと呼ばれます。
ICMP PING応答	Internet Control Message Protocol（ICMP）は、ネットワークに接続されたコンピュータのオペレーティングシステムでメッセージの送信に使用されるプロトコルです。ICMPメッセージを送信することで、ホストに到達できるかどうかや、そのホストとのパケットの送受信にどれくらいの時間がかかるかが確認されます。
MACアドレス	メディアアクセス制御（MAC）アドレスはイーサネットで使用される識別子で、同じ物理トランスポートネットワークインターフェイス上の2つのポートを接続する別々の論理チャネルを区別します。

コンポーネント	製品説明
管理クライアント	管理クライアントは、System Managerにアクセスするためのブラウザがインストールされたコンピュータです。
MTU	Maximum Transmission Unit（MTU；最大伝送ユニット）は、ネットワークで送信できるパケットまたはフレームの最大サイズです。
NTP	Network Time Protocol（NTP；ネットワークタイムプロトコル）は、データネットワーク内のコンピュータシステム間でクロック同期を行うためのネットワークプロトコルです。
シンフレツクスコウセイ	シンプレックスは、ストレージアレイ内に1つのコントローラモジュールを配置した構成です。シンプレックスシステムでは、コントローラやディスクパスは冗長化されませんが、ファンと電源装置は冗長化されます。
VLAN	仮想ローカルエリアネットワーク（VLAN）は、同じデバイス（スイッチ、ルータなど）でサポートされる他のネットワークから物理的に分離されているかのように動作する論理ネットワークです。

ドライブの用語：

コンポーネント	製品説明
DA	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する機能です。Data Assuranceは、Fibre ChannelなどのDA対応I/Oインターフェイスを使用するホストで、プールまたはボリュームグループのレベルで有効にすることができます。
ドライブセキュリティ機能	ドライブセキュリティは、 Full Disk Encryption （ FDE ）ドライブまたは連邦情報処理標準（ FIPS ）ドライブを使用してセキュリティを強化するストレージアレイの機能です。これらのドライブをドライブセキュリティ機能と組み合わせて使用すると、データにアクセスするためのセキュリティキーが必要になります。ドライブをアレイから物理的に取り外した場合、別のアレイに取り付けるまでドライブは動作しません。別のアレイに取り付けると、正しいセキュリティキーを指定するまでセキュリティロック状態になります。
ドライブシェルフ	ドライブシェルフは、拡張シェルフとも呼ばれ、一連のドライブと2つの入出力モジュール（IOM）が搭載されます。IOMにはSASポートが搭載されており、ドライブシェルフをコントローラシェルフまたは他のドライブシェルフに接続します。
DULBE	Deallocated or Unwritten Logical Block Error（DULBE）はNVMeドライブのオプションです。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。
FDEトライフ	Full Disk Encryption（FDE）ドライブは、ハードウェアレベルでディスクドライブの暗号化を実行します。ハードドライブには、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ASICチップが搭載されています。
FIPSトライフ	FIPSドライブは、連邦情報処理標準（FIPS）140-2レベル2に準拠しています。基本的な概念はFDEドライブと同じですが、米国政府の基準に従って強力な暗号化アルゴリズムと暗号化方式を実装しています。FIPSドライブにはFDEドライブよりも高度なセキュリティ基準が採用されています。
HDD	ハードディスクドライブ（ HDD ）は、磁気コーティングを施した金属製の回転式ディスクを使用するデータストレージデバイスです。
ホットスペアドライブ	ホットスペアは、RAID 1、RAID 5、またはRAID 6のボリュームグループで、スタンバイドライブとして機能します。問題なく動作するドライブですが、データは格納されていません。ボリュームグループ内のドライブに障害が発生すると、障害が発生したドライブのデータがホットスペアに自動的に再構築されます。

コンポーネント	製品説明
NVMe	Non-Volatile Memory Express（NVMe）は、SSDドライブなどのフラッシュベースのストレージデバイス向けに設計されたインターフェイスです。NVMeは、以前の論理デバイスインターフェイスと比較してI/Oオーバーヘッドを削減し、パフォーマンスを向上させます。
SAS	Serial Attached SCSI （ SAS ）は、コントローラをディスクドライブに直接リンクするポイントツーポイントのシリアルプロトコルです。
セキュリティ対応ドライブ	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。これらのドライブでは、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。ドライブセキュリティ機能を使用したセキュリティの強化に使用できるため、これらのドライブはsecured_capable_とみなされます。これらのドライブを使用するボリュームグループやプールでドライブセキュリティ機能を有効にすると、ドライブはsecure-_enabled_になります。
セキュリティ有効ドライブ	セキュリティ有効ドライブは、ドライブセキュリティ機能で使用されます。ドライブセキュリティ機能を有効にし、かつsecured_caped_drivesのプールまたはボリュームグループにドライブセキュリティを適用すると、ドライブはsecure*enable*になります。読み取り/書き込みアクセスは、正しいセキュリティキーが設定されたコントローラからのみ実行できます。この追加のセキュリティ機能により、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。
SSD	ソリッドステートディスク（ SSD ）は、ソリッドステートメモリ（フラッシュ）を使用してデータを永続的に格納するデータストレージデバイスです。SSD は従来のハードドライブをエミュレートしたものであり、ハードドライブと同じインターフェイスで利用できます。

iSCSIの用語：

期間	製品説明
CHAP（CHAP）	Challenge Handshake Authentication Protocol（CHAP；チャレンジハンドシェイク認証プロトコル）方式では、最初のリンク時にターゲットとイニシエータのIDが検証されます。認証は、CHAP_secret__という共有セキュリティキーに基づいて行われます。
コントローラ	コントローラは、ボード、ファームウェア、ソフトウェアで構成されます。ドライブを制御し、System Managerの機能を実装します。
DHCP	Dynamic Host Configuration Protocol（DHCP；動的ホスト構成プロトコル）は、IPアドレスなどのネットワーク構成パラメータを動的に配布するためにインターネットプロトコル（IP）ネットワークで使用されるプロトコルです。
IB	InfiniBand （ IB ）は、ハイパフォーマンスのサーバとストレージシステムの間のデータ転送用の通信標準です。
ICMP PING応答	Internet Control Message Protocol（ICMP）は、ネットワークに接続されたコンピュータのオペレーティングシステムでメッセージの送信に使用されるプロトコルです。ICMPメッセージを送信することで、ホストに到達できるかどうかや、そのホストとのパケットの送受信にどれくらいの時間がかかるかが確認されます。
IQN	iSCSI Qualified Name（IQN）は、iSCSIイニシエータまたはiSCSIターゲットの一意の名前です。
iSER	iSCSI Extensions for RDMA（iSER）は、InfiniBandやイーサネットなどのRDMAトランスポートを使用する処理用にiSCSIプロトコルを拡張したプロトコルです。
iSNS	Internet Storage Name Service（iSNS）は、TCP/IPネットワーク上のiSCSIデバイスとFibre Channelデバイスの自動検出、管理、構成を可能にするプロトコルです。
MACアドレス	メディアアクセス制御（MAC）アドレスはイーサネットで使用される識別子で、同じ物理トランスポートネットワークインターフェイス上の2つのポートを接続する別々の論理チャネルを区別します。
管理クライアント	管理クライアントは、System Managerにアクセスするためのブラウザがインストールされたコンピュータです。
MTU	Maximum Transmission Unit（MTU；最大伝送ユニット）は、ネットワークで送信できるパケットまたはフレームの最大サイズです。

期間	製品説明
RDMA	リモートダイレクトメモリアクセス（RDMA）は、ネットワークコンピュータがいずれかのコンピュータのオペレーティングシステムを介さずにメインメモリ内のデータを交換できるようにするテクノロジです。
名前のない検出セッション	名前のない検出セッションのオプションが有効な場合、iSCSIイニシエータは、コントローラの情報を取得するためにターゲットIQNを指定する必要はありません。

NVMeの用語：

期間	製品説明
InfiniBand	InfiniBand （ IB ）は、ハイパフォーマンスのサーバとストレージシステムの間のデータ転送用の通信標準です。
ネームスペース	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、ストレージアレイ内のボリュームに関連します。
ネームスペースID	ネームスペースIDは、NVMeコントローラのネームスペースに対する一意の識別子で、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。
NQN	NVMe Qualified Name（NQN）は、リモートストレージターゲット（ストレージアレイ）を識別するために使用します。
NVM	Non-Volatile Memory（NVM；不揮発性メモリ）は、さまざまなタイプのストレージデバイスで使用される永続的メモリです。
NVMe	Non-Volatile Memory Express（NVMe）は、SSDドライブなどのフラッシュベースのストレージデバイス向けに設計されたインターフェイスです。NVMeは、以前の論理デバイスインターフェイスと比較してI/Oオーバーヘッドを削減し、パフォーマンスを向上させます。
NVMe-oF	Non-Volatile Memory Express over Fabrics（NVMe-oF）は、NVMeコマンドとデータをホストとストレージ間でネットワーク経由で転送するための仕様です。
NVMeコントローラ	NVMeコントローラはホスト接続プロセス中に作成されます。ホストとストレージアレイ内のネームスペースの間のアクセスパスを提供します。
NVMeキュー	NVMeインターフェイス経由でのコマンドやメッセージの受け渡しに使用されるキューです。
NVMeサブシステム	NVMeホストに接続されているストレージアレイ。
RDMA	Remote Direct Memory Access（RDMA；リモートダイレクトメモリアクセス）は、ネットワークインターフェイスカード（NIC）ハードウェアに転送プロトコルを実装することで、サーバとの間でより直接的なデータ移動を可能にします。
RoCE	RDMA over Converged Ethernet （ RoCE ）は、イーサネットネットワークを介したリモートダイレクトメモリアクセス（ RDMA ）を可能にするネットワークプロトコルです。

期間	製品説明
SSD	ソリッドステートディスク（ SSD ）は、ソリッドステートメモリ（フラッシュ）を使用してデータを永続的に格納するデータストレージデバイスです。SSD は従来のハードドライブをエミュレートしたものであり、ハードドライブと同じインターフェイスで利用できます。

シェルフコンポーネントを管理します。

ハードウェアコンポーネントの表示

[ハードウェア]ページには、コンポーネントの検索を容易にするソートとフィルタの機能が用意されています。

手順

1. 「* ハードウェア * 」を選択します。
2. 次の表に示す機能を使用して、ハードウェアコンポーネントを表示します。

機能	製品説明
ドライブ、コントローラ、およびコンポーネントのビュー	シェルフ前面ビューと背面ビューを切り替えるには、右端から*または[コントローラとコンポーネント]を選択します（表示されるリンクは現在のビューによって異なります）。**[**ドライブ**]**ビューには、ドライブと空のドライブベイが表示されます。**[**コントローラとコンポーネント**]***ビューには、コントローラ、**IOM**（**ESM**）モジュール、電源**/**ファンキャニスター、または空のコントローラベイが表示されます。ページの下部で、[すべてのドライブを表示]*を選択することもできます。
ドライブ表示のフィルタ	ストレージアレイに物理属性と論理属性が異なるドライブが含まれている場合、ハードウェア*ページにはドライブ表示フィルタが含まれています。これらのフィルタフィールドでは、ページに表示されるドライブタイプを制限することで、特定のドライブをすばやく特定できます。**[Show drives that are…]**で、左側のフィルタフィールド(デフォルトでは*any drive type*)をクリックすると、物理属性(容量や速度など)のドロップダウンリストが表示されます。右側のフィルタフィールド（デフォルトではストレージアレイ内に「* Anywhere」と表示されます）をクリックすると、論理属性（ボリュームグループ割り当てなど）のドロップダウンリストが表示されます。これらのフィルタは一緒に使用することも別 々に使用することもできます ストレージアレイに同じ物理属性を共有するドライブがすべて含まれている場合、左側の*いずれかのドライブタイプ*フィールドは表示されません。すべてのドライブが同じ論理的な場所にある場合、右側のストレージアレイ*フィールドに「* Anywhere」と表示されません。
凡例	各コンポーネントは、ロールの状態を示すために特定の色で表示されます。これらの状態の説明を展開または折りたたむには、*凡例*をクリックします。

機能	製品説明
ステータスアイコンの詳細を表示	ステータスインジケータには、可用性状態の説明を含めることができます。[ステータスアイコンの詳細を表示する*]をクリックして、このステータステキストを表示または非表示にします。
シェルフ/シェルフアイコン	各シェルフビューには、関連するコマンドのリストと、プロパティおよびステータスが表示されます。[**Shelf-**]をクリックすると、コマンドのドロップダウンリストが表示されます。上部にあるいずれかのアイコンを選択して、個 々 のコンポーネント（コントローラ、IOM（ESM）、電源装置、ファン、温度、バッテリ、SFP）のステータスとプロパティを表示することもできます。
シェルフの順序	シェルフはハードウェアページで再配置できます。各シェルフビューの右上にある上下の矢印を使用して、シェルフの上下の順序を変更します。

コンポーネントステータスの表示/非表示

ドライブ、コントローラ、ファン、電源装置のステータスに関する説明を表示できます。

手順

1. 「 * ハードウェア * 」を選択します。
2. 背面または前面のコンポーネントを確認するには、次の手順を実行します。
   - コントローラおよび電源/ファンキャニスターコンポーネントを確認する際にドライブが表示される場合は、*[コントローラとコンポーネント]*タブをクリックします。
   - ドライブを表示する際にコントローラおよび電源/ファンキャニスターコンポーネントが表示される場合は、*[ドライブ]*タブをクリックします。
3. ポップオーバーステータスの説明を表示または非表示にするには：
   - ステータスアイコンの上にある概要 を表示するには、シェルフビューの右上にあるステータスアイコンの詳細を表示*をクリックします（チェックボックスを選択します）。
   - ポップオーバーの説明を非表示にするには、*ステータスアイコンの詳細を表示*をもう一度クリックします（チェックボックスをオフにします）。
4. ステータスの詳細をすべて表示するには、シェルフビューでコンポーネントを選択し、* View settings *を選択します。
5. 色の付いたコンポーネントの説明を表示するには、*凡例*を選択します。

前面ビューと背面ビューを切り替える

[ハードウェア]ページでは、シェルフの前面と背面のどちらかを表示できます。

タスクの内容

背面ビューには、コントローラ/ IOMと電源/ファンキャニスターが表示されます。前面ビューにはドライブが表示されます。

手順

1. 「 * ハードウェア * 」を選択します。
2. 図にドライブが表示された場合は、*[コントローラとコンポーネント]*タブをクリックします。

   図の表示が切り替わり、ドライブではなくコントローラが表示されます。

3. 図にコントローラが表示された場合は、*[ドライブ]*タブをクリックします。

   図の表示が切り替わり、コントローラではなくドライブが表示されます。

4. 必要に応じて、ページの下部にある「* Show all front 」または「 Show all back *」を選択できます。

シェルフの表示順序を変更

[ハードウェア]ページに表示されるシェルフの順序は、キャビネット内のシェルフの物理的な順序と同じになるように変更できます。

手順

1. 「 * ハードウェア * 」を選択します。
2. シェルフビューの右上から、上下の矢印を選択して、ハードウェアページに表示されるシェルフの順序を変更します。

シェルフのロケーターライトを点灯

[ハードウェア]ページに表示されたシェルフの物理的な場所を確認するには、シェルフのロケーターライトを点灯します。

手順

1. 「 * ハードウェア * 」を選択します。
2. コントローラシェルフまたはドライブシェルフのドロップダウンリストを選択し、*ロケーターライトを点灯*を選択します。

   シェルフのロケーターライトが点灯します。

3. シェルフを物理的に配置したら、ダイアログボックスに戻り、*電源をオフにする*を選択します。

シェルフ**ID**の変更

シェルフIDは、ストレージアレイ内のシェルフを一意に識別する番号です。シェルフに00または01から始まる連番が振られており、シェルフ画面の左上に表示されます。

タスクの内容

シェルフIDはコントローラファームウェアによって自動的に割り当てられますが、別の順序付けを作成する場合は変更できます。

手順

1. 「 * ハードウェア * 」を選択します。
2. コントローラシェルフまたはドライブシェルフのドロップダウンリストを選択し、* Change ID *を選択します。

3. Change Shelf ID（シェルフIDの変更）ダイアログボックスで、ドロップダウンリストを選択して、使用可能な番号を表示します。

   このダイアログボックスには、アクティブなシェルフに現在割り当てられているIDは表示されません。

4. 使用可能な番号を選択し、*保存*をクリックします。

   選択した番号によっては、ハードウェアページでシェルフの順序が変更される場合があります。必要に応じて、各シェルフの右上にある上下の矢印を使用して順序を調整できます。

シェルフコンポーネントのステータスと設定の表示

[ハードウェア]ページには、シェルフコンポーネント（電源装置、ファン、バッテリなど）のステータスと設定が表示されます。

タスクの内容

使用可能なコンポーネントはシェルフのタイプによって異なります。

- ドライブシェルフ--ドライブ、電源/ファンキャニスター、入出力モジュール（IOM）、およびその他のサポートコンポーネントが1台のシェルフに収容されます。
- コントローラシェルフ--一連のドライブ、1つまたは2つのコントローラキャニスター、電源/ファンキャニスター、およびその他のサポートコンポーネントが1つのシェルフに格納されています。

手順

1. 「 * ハードウェア * 」を選択します。
2. コントローラシェルフまたはドライブシェルフのドロップダウンリストを選択し、* View Settings *を選択します。

   Shelf Components Settingsダイアログボックスが開き、シェルフコンポーネントに関連するステータスと設定がタブに表示されます。選択したシェルフのタイプによっては、表に記載されている一部のタブが表示されない場合があります。

タブ	製品説明
シェルフ	[* Shelf *]タブには、次のプロパティが表示されます。 • * Shelf ID *：ストレージ・アレイ内のシェルフを一意に識別しますこの番号はコントローラファームウェアによって割り当てられますが、変更するにはメニューから「Shelf [Change ID]」を選択します。 • * Shelf path redundancy *-シェルフとコントローラ間の接続の代替方法があるかどうか（「はい」または「いいえ」）を示します。 • 現在のドライブタイプ--ドライブに組み込まれているテクノロジのタイプを表示します(たとえば'セキュリティ対応のSASドライブ)ドライブタイプが複数ある場合は、両方のテクノロジが表示されます。 • * Serial Number *-シェルフのシリアル番号が表示されます。

タブ	製品説明
IOM（ESM）	IOM（ESM）*タブには、環境サービスモジュール（ESM）とも呼ばれる入出力モジュール（IOM）のステータスが表示されます。ドライブシェルフ内のコンポーネントのステータスを監視し、ドライブトレイとコントローラの間の接続ポイントとして機能します。 ステータスは最適、失敗、最適（誤配線）、未認定のいずれかです。その他の情報には、ファームウェアのバージョンと設定のバージョンが含まれます。 「詳細設定を表示」を選択すると、最大および現在のデータレートとカード通信の状態（「はい」または「いいえ」）が表示されます。  [シェルフ]ドロップダウンリストの横にある[IOM]アイコンを選択してこのステータスを表示することもできます。
電源装置	電源装置*タブには、電源装置キャニスターと電源装置自体のステータスが表示されます。ステータスは最適、失敗、取り外し、不明のいずれかです。電源装置のパーツ番号も表示されます。  [シェルフ]ドロップダウンリストの横にある[電源装置]アイコンを選択してこのステータスを表示することもできます。
ファン	ファン*タブには、ファンキャニスターとファン自体のステータスが表示されます。ステータスは最適、失敗、取り外し、不明のいずれかです。  [シェルフ]ドロップダウンリストの横にある[ファン]アイコンを選択してこのステータスを表示することもできます。
温度	温度*タブには、センサー、コントローラ、電源/ファンキャニスターなどのシェルフコンポーネントの温度ステータスが表示されます。ステータスは最適、公称温度を超過、最大温度を超過、不明のいずれかです。  [シェルフ]ドロップダウンリストの横にある[温度]アイコンを選択してこのステータスを表示することもできます。
ハツテリ	バッテリ*タブには、コントローラのバッテリのステータスが表示されます。ステータスは最適、失敗、取り外し、不明のいずれかです。その他の情報には、バッテリの寿命、交換までの日数、学習サイクル、および学習サイクル間の週の数が含まれます。  [シェルフ]ドロップダウンリストの横にある[バッテリ]アイコンを選択してこのステータスを表示することもできます。

タブ	製品説明
SFP	[SFP *]タブには、コントローラのSmall Form-factor Pluggable（SFP）トランシーバのステータスが表示されます。ステータスは最適、失敗、不明のいずれかです。 [Show more settings]を選択して、SFPのパーツ番号、シリアル番号、ベンダーを確認します。 [シェルフ]ドロップダウンリストの横にある[SFP]アイコンを選択してこのステータスを表示することもできます。

3. [* 閉じる *] をクリックします。

バッテリ学習サイクルの更新

学習サイクルは、スマートバッテリーゲージを較正するための自動サイクルです。サイクルは、コントローラごとに8週間の間隔で、同じ日時に自動的に開始されるようにスケジュールされます。別のスケジュールを設定する場合は、学習サイクルを調整できます。

タスクの内容

学習サイクルの更新は両方のコントローラのバッテリに影響します。

手順

1. 「 * ハードウェア * 」を選択します。
2. コントローラシェルフのドロップダウンリストを選択し、* View settings *を選択します。
3. 「バッテリ*」タブを選択します。
4. 「バッテリ学習サイクルの更新」を選択します。

   バッテリ学習サイクルの更新ダイアログボックスが開きます。

5. ドロップダウンリストから新しい日時を選択します。
6. [保存（ Save ）] をクリックします。

コントローラの管理

コントローラの状態

コントローラは、オンライン、オフライン、およびサービスモードの3つの状態に切り替えることができます。

オンライン状態

オンライン状態は、コントローラの通常動作時の状態です。コントローラが正常に動作しており、I/O処理に使用できることを意味します。

コントローラをオンラインにすると、ステータスが最適になります。

オフライン状態

オフライン状態は、通常、ストレージアレイにコントローラが2台ある場合にコントローラを交換する準備に使用します。コントローラは、明示的なコマンドを実行した場合とコントローラで障害が発生した場合の2つの方法でオフライン状態になります。コントローラのオフライン状態は、別の明示的なコマンドを実行するか、障害が発生したコントローラを交換するまで解消されません。コントローラをオフラインにできるのは、ストレージアレイにコントローラが2台ある場合だけです。

コントローラがオフライン状態のときは次の状況になります。

- コントローラをI/Oに使用できません。
- そのコントローラでストレージアレイを管理することはできません。
- そのコントローラが現在所有しているボリュームは、もう一方のコントローラに移動されます。
- キャッシュミラーリングが無効になり、すべてのボリュームがライトスルーキャッシュモードに変更されます。

サービスモード

サービスモードは通常、テクニカルサポートのみが使用し、ストレージアレイのすべてのボリュームを一方のコントローラに移動して、もう一方のコントローラを診断できるようにします。コントローラは手動でサービスモードにする必要があり、サービス処理の完了後に手動でオンラインに戻す必要があります。

コントローラがサービスモードの場合は、次の状況になります。

- コントローラをI/Oに使用できません。
- テクニカルサポートは、シリアルポートまたはネットワーク接続経由でコントローラにアクセスし、潜在的な問題を分析できます。
- そのコントローラが現在所有しているボリュームは、もう一方のコントローラに移動されます。
- キャッシュミラーリングが無効になり、すべてのボリュームがライトスルーキャッシュモードに変更されます。

IPアドレスの割り当てに関する考慮事項

デフォルトでは、コントローラは両方のネットワークポートでDHCPを有効にした状態で出荷されます。静的IPアドレスを割り当てるか、デフォルトの静的IPアドレスを使用するか、またはDHCPによって割り当てられたIPアドレスを使用できます。IPv6のステートレス自動設定を使用することもできます。

> IPv6は新しいコントローラではデフォルトで無効になっていますが、別の方法で管理ポートのIPアドレスを設定し、System Managerを使用して管理ポートでIPv6を有効にすることができます。

ネットワークポートが「リンク停止」状態、つまりLANから切断されている場合、システムは設定を静的として報告するか（以前のリリース）、DHCPが有効でIPアドレスが報告されないか（以降のリリース）と報告します。ネットワークポートが「リンクアップ」状態（LANに接続）になると、DHCP経由でIPアドレスを取得しようとします。

コントローラの特定のネットワークポートでDHCPアドレスを取得できない場合はデフォルトのIPアドレスに戻りますが、これには3分ほどかかることがあります。デフォルトのIPアドレスは次のとおりです。

```
Controller 1 (port 1): IP Address: 192.168.128.101
```

```
Controller 1 (port 2): IP Address: 192.168.129.101
```

```
Controller 2 (port 1): IP Address: 192.168.128.102
```

```
Controller 2 (port 2): IP Address: 192.168.129.102
```

IPアドレスを割り当てる場合：

- コントローラのポート2をカスタマーサポート用に予約します。デフォルトのネットワーク設定（DHCPが有効な状態）を変更しないでください。
- E2800およびE5700のコントローラに静的IPアドレスを設定するには、SANtricity System Managerを使用します。E2700およびE5600のコントローラに静的IPアドレスを設定するには、SANtricity Storage Managerを使用します。静的IPアドレスを設定すると、リンクの停止/停止イベントが発生しても設定されたままになります。
- DHCPを使用してコントローラのIPアドレスを割り当てるには、DHCP要求を処理できるネットワークにコントローラを接続します。永続的なDHCPリースを使用してください。

> デフォルトアドレスは、リンク停止イベントが発生しても維持されません。コントローラのネットワークポートでDHCPを使用するように設定されている場合、ケーブルの挿入、リブート、電源の再投入など、リンク稼働イベントのたびにDHCPアドレスの取得が試行されます。DHCPの試行に失敗すると、そのポートのデフォルトの静的IPアドレスが使用されます。

管理ポートを設定

コントローラには、システム管理に使用するイーサネットポートが搭載されています。必要に応じて、送信パラメータとIPアドレスを変更できます。

タスクの内容

この手順では、ポート1を選択し、速度とポートアドレス指定方法を決定します。ポート1は、管理クライアントがコントローラとSystem Managerにアクセスできるネットワークに接続します。

> どちらのコントローラでもポート2は使用しないでください。ポート2はテクニカルサポート用に予約されています。

手順

1. 「 * ハードウェア * 」を選択します。

2. 図にドライブが表示された場合は、*[コントローラとコンポーネント]*タブをクリックします。

   図の表示が切り替わり、ドライブではなくコントローラが表示されます。

3. 管理ポートを設定するコントローラをクリックします。

   コントローラのコンテキストメニューが表示されます。

4. ［管理ポートの設定］を選択します。

   Configure Management Portsダイアログボックスが開きます。

5. ポート1が表示されていることを確認し、*次へ*をクリックします。
6. 構成ポートの設定を選択し、 * 次へ * をクリックします。

   フィールドの詳細

フィールド	製品説明
速度と二重モード	System Managerでストレージアレイとネットワークの間の転送パラメータを決定する場合、またはネットワークの速度とモードを確認したい場合は、自動ネゴシエーション設定を維持します。ネットワークのパラメータをドロップダウンリストから選択することもできます。有効な速度とデュプレックスの組み合わせだけがリストに表示されます。
IPv4を有効にする/ IPv6を有効にする	IPv4およびIPv6ネットワークのサポートを有効にするには、一方または両方のオプションを選択します。

   「* IPv4を有効にする*」を選択すると、「次へ」をクリックした後でIPv4設定を選択するためのダイアログボックスが開きます。「* IPv6を有効にする*」を選択すると、「次へ」をクリックした後でIPv6設定を選択するためのダイアログボックスが開きます。両方のオプションを選択した場合は、IPv4設定のダイアログボックスが最初に開き、*次へ*をクリックすると、IPv6設定のダイアログボックスが開きます。

7. IPv4 / IPv6を自動または手動で設定します。

フィールドの詳細

フィールド	製品説明
DHCPサーバから自動的に設定を取得	設定を自動的に取得するには、このオプションを選択します。
静的設定を手動で指定する	このオプションを選択し、コントローラのIPアドレスを入力します。（必要に応じて、カット アンド ペーストでアドレスをフィールドに貼り付けることもできます）。IPv4の場合は、ネットワークのサブネットマスクとゲートウェイを指定します。IPv6の場合は、ルーティング可能なIPアドレスとルータのIPアドレスを指定します。 IPアドレスの設定を変更すると、ストレージアレイへの管理パスが失われます。SANtricity Unified Managerを使用してネットワーク内のアレイをグローバルに管理する場合は、ユーザインターフェイスを開き、メニューから「Manage [Discover]」に移動します。SANtricity Storage Managerを使用している場合は、Enterprise Management Window（EMW）からデバイスを削除し、メニューのEdit [Add Storage Array]を選択してEMWに再び追加し、新しいIPアドレスを入力する必要があります。

8. [完了] をクリックします。

結果

管理ポートの設定は、コントローラの設定の管理ポートタブに表示されます。

NTPサーバアドレスの設定

ネットワークタイムプロトコル（NTP）サーバへの接続を設定すると、コントローラがNTPサーバを定期的に照会して内部の時刻クロックを更新できるようになります。

開始する前に

- ネットワークにNTPサーバをインストールし、設定する必要があります。
- プライマリNTPサーバとオプションのバックアップNTPサーバのアドレスを確認しておく必要があります。これらのアドレスには、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスを使用できます。

NTPサーバのドメイン名を1つ以上入力する場合は、NTPサーバアドレスを解決するようにDNSサーバも設定する必要があります。DNSサーバの設定が必要となるのは、NTPを設定してドメイン名を指定したコントローラだけです。

タスクの内容

NTPを使用すると、ストレージアレイがSimple Network Time Protocol（SNTP；簡易ネットワークタイムプロトコル）を使用してコントローラのクロックを外部ホストと自動的に同期できます。コントローラは設定されたNTPサーバを定期的に照会し、その結果を使用して内部のクロックを更新します。一方のコントローラだけでNTPが有効になっている場合、代替コントローラのクロックはNTPが有効なコントローラと定期的に同期されます。どちらのコントローラでもNTPが有効になっていない場合は、定期的にコントローラ間で相互にクロ

ックが同期されます。

両方のコントローラでNTPを設定する必要はありませんが、設定すると、ハードウェア障害や通信障害が発生した場合にストレージアレイの同期度が向上します。

手順

1. 「 * ハードウェア * 」を選択します。
2. 図にドライブが表示された場合は、*[コントローラとコンポーネント]*タブをクリックします。

   図の表示が切り替わり、ドライブではなくコントローラが表示されます。

3. 設定するコントローラをクリックします。

   コントローラのコンテキストメニューが表示されます。

4. [Configure NTP server*]を選択します。

   Configure Network Time Protocol（NTP）Server（ネットワークタイムプロトコル（NTP）サーバの設定）ダイアログボックスが開きます。

5. [* I want to enable NTP on Controller （ A * or * B *）]を選択します。

   ダイアログボックスに追加の選択肢が表示されます。

6. 次のいずれかのオプションを選択します。
   - **DHCP**サーバから自動的に**NTP**サーバアドレスを取得--検出されたNTPサーバアドレスが表示されます

     静的なNTPアドレスを使用するようにストレージ アレイが設定されている場合、NTPサーバは表示されません。

   - * NTPサーバ・アドレスを手動で指定*--プライマリNTPサーバ・アドレスとバックアップNTPサーバ・アドレスを入力しますバックアップサーバはオプションです。（アドレス フィールドはラジオ ボタンを選択すると表示されます）。サーバアドレスには、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスを使用できます。
7. *オプション：*バックアップNTPサーバのサーバ情報と認証クレデンシャルを入力します。
8. [保存（ Save ）] をクリックします。

結果

NTPサーバの設定は、コントローラの設定の* DNS/NTP *タブに表示されます。

DNSサーバアドレスの設定

ドメインネームシステム（DNS）は、コントローラとネットワークタイムプロトコル（NTP）サーバの完全修飾ドメイン名を解決するために使用します。ストレージアレイの管理ポートでは、IPv4プロトコルとIPv6プロトコルを同時にサポートできます。

開始する前に

- ネットワークにDNSサーバをインストールし、設定する必要があります。

- プライマリDNSサーバとオプションのバックアップDNSサーバのアドレスを確認しておきます。IPv4アドレスまたはIPv6アドレスを指定できます。

タスクの内容

この手順では、プライマリおよびバックアップのDNSサーバアドレスを指定する方法について説明します。バックアップDNSサーバは、プライマリDNSサーバに障害が発生した場合に使用するようにオプションで設定できます。

> ストレージアレイの管理ポートを動的ホスト構成プロトコル（DHCP）ですでに設定していて、1つ以上のDNSサーバまたはNTPサーバをDHCPセットアップに関連付けている場合は、DNSまたはNTPを手動で設定する必要はありません。この場合、DNS / NTPサーバのアドレスはストレージアレイですでに自動的に取得されているはずです。ただし、以下の手順に従ってダイアログボックスを開き、正しいアドレスが検出されていることを確認する必要があります。

手順

1. 「 * ハードウェア * 」を選択します。
2. 図にドライブが表示された場合は、*[コントローラとコンポーネント]*タブをクリックします。

   図の表示が切り替わり、ドライブではなくコントローラが表示されます。
3. 設定するコントローラを選択します。

   コントローラのコンテキストメニューが表示されます。
4. [Configure DNS server*]を選択します。

   ドメインネームシステム（DNS）サーバの設定ダイアログボックスが開きます。
5. 次のいずれかのオプションを選択します。
   - **DHCP**サーバから自動的に**DNS**サーバアドレスを取得--検出されたDNSサーバアドレスが表示されます

     > 静的DNSアドレスを使用するようにストレージアレイが設定されている場合、DNSサーバは表示されません。

   - **DNS**サーバアドレスを手動で指定する--プライマリDNSサーバのアドレスとバックアップDNSサーバのアドレスを入力しますバックアップサーバはオプションです。（アドレス フィールドはラジオ ボタンを選択すると表示されます）。IPv4アドレスまたはIPv6アドレスを指定できます。
6. [保存（ Save ）] をクリックします。
7. もう一方のコントローラに対して上記の手順を繰り返します。

結果

DNS設定は、コントローラ設定の* DNS/NTP *タブに表示されます。

コントローラ設定の表示

コントローラに関する情報（ホストインターフェイス、ドライブインターフェイス、管

理ポートのステータスなど）を表示できます。

手順

1. 「 * ハードウェア * 」を選択します。
2. 図にドライブが表示された場合は、*[コントローラとコンポーネント]*タブをクリックします。

   図の表示が切り替わり、ドライブではなくコントローラが表示されます。

3. 次のいずれかの操作を実行して、コントローラの設定を表示します。
   - コントローラをクリックしてコンテキストメニューを表示し、*設定の表示*を選択します。
   - コントローラアイコン（「* Shelf 」ドロップダウン・リストの横）を選択します。デュプレックス構成の場合は、ダイアログボックスから Controller A*または* Controller B*を選択し、* Next *をクリックします。

     Controller Settings（コントローラ設定）ダイアログボックスが開きます。

4. プロパティ設定間を移動するタブを選択します。

   一部のタブには、右上に[詳細設定を表示]*のリンクがあります。

フィールドの詳細

タブ	製品説明
ベース	コントローラのステータス、モデル名、交換パーツ番号、現在のファームウェアバージョン、および不揮発性静的ランダムアクセスメモリ（NVSRAM）のバージョンが表示されます。
キャッシュ	コントローラのキャッシュ設定が表示されます。これには、データキャッシュ、プロセッサキャッシュ、およびキャッシュバックアップデバイスが含まれます。キャッシュバックアップデバイスは、コントローラへの電源が失われた場合にキャッシュ内のデータをバックアップするために使用されます。ステータスは、最適、失敗、削除、不明、書き込み禁止、互換性なしのいずれかです。
ホストインターフェイス	ホストインターフェイスの情報と各ポートのリンクステータスが表示されます。ホストインターフェイスは、コントローラとホスト間の接続（Fibre ChannelやiSCSIなど）です。 ホストインターフェイスカード（HIC）の場所は、ベースボード内またはスロット（ベイ）内です。「Baseboard」は、HICポートがコントローラに組み込まれていることを示します。「Slot」ポートはオプションのHICに搭載されています。
ドライブインターフェイス	ドライブインターフェイス情報と各ポートのリンクステータスが表示されます。ドライブインターフェイスは、コントローラとドライブ（SASなど）の間の接続です。
管理ポート	管理ポートの詳細（コントローラへのアクセスに使用するホスト名、リモートログインが有効になっているかどうかなど）が表示されます。管理ポートは、コントローラと管理クライアントを接続します。このポートには、System Managerにアクセスするためのブラウザがインストールされています。
DNS / NTP	は、DNSサーバとNTPサーバがSystem Managerで設定されている場合のアドレス指定方法とIPアドレスを示しています。 Domain Name System（DNS；ドメインネームシステム）は、インターネットまたはプライベートネットワークに接続されたデバイスの命名システムです。DNSサーバはドメイン名のディレクトリを維持し、インターネットプロトコル（IP）アドレスに変換します。 Network Time Protocol（NTP；ネットワークタイムプロトコル）は、データネットワーク内のコンピュータシステム間でクロック同期を行うためのネットワークプロトコルです。

5. [* 閉じる *] をクリックします。

リモートログインを有効にすると、ローカルエリアネットワークの外部のユーザがコントローラのSSHセッションを開始し、設定にアクセスできるようになります。

SANtricityバージョン11.74以降では、ユーザにSSHキーやSSHパスワードの入力を要求することで、多要素認証（MFA）を設定することもできます。SANtricity バージョン11.73以前の場合、この機能には、SSHキーとパスワードを使用した多要素認証のオプションは含まれません。

セキュリティ上のリスク--セキュリティ上の理由から、リモートログイン機能を使用するのはテクニカルサポート担当者だけにしてください。

手順

1. 「 * ハードウェア * 」を選択します。
2. 図にドライブが表示された場合は、*[コントローラとコンポーネント]*タブをクリックします。

   図の表示が切り替わり、ドライブではなくコントローラが表示されます。

3. リモートログインを設定するコントローラをクリックします。

   コントローラのコンテキストメニューが表示されます。

4. Configure remote login (SSH)*を選択します。（SANtricity バージョン11.73以前の場合、このメニュー項目は*リモートログインの変更*です）。

   リモートログインを有効にするためのダイアログボックスが開きます。

5. [リモートログインを有効にする*]チェックボックスをオンにします。

   この設定により、リモートログインに許可の3つのオプションが提供されます。

   - パスワードのみ。このオプションでは、完了し、[保存（Save）]をクリックできます。デュプレックスシステムの場合は、前の手順に従って2台目のコントローラでリモートログインを有効にすることができます。
   - * SSHキーまたはパスワード*。このオプションでは、次の手順に進みます。
   - パスワードと**SSH**キー*の両方。このオプションでは、**[**リモートログインに許可された公開鍵とパスワードを要求する]チェックボックスをオンにして、次の手順に進みます。

6. [**Authorized public key**]フィールドに値を入力します。このフィールドには、OpenSSH * authorized_keys *ファイルの形式の、許可された公開鍵のリストが含まれます。

   [**Authorized public key**]フィールドに入力する場合は、次のガイドラインに注意してください。

   - Authorized Public Key *フィールド環境 は両方のコントローラを対象としており、1台目のコントローラでのみ構成する必要があります。
   - authorized_keys *ファイルには、1行に1つのキーのみを含める必要があります。#で始まる行と空行は無視されます。ファイル形式の詳細については、を参照してください"OpenSSHの認証済みキーの設定"。
   - *authorized_keys *ファイルは、次の例のようになります。

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDJlG20rYTk4ok+xFjkPHYp/R0LfJqEYDLXA5AJ4
9w3DvAWLrUg+1CpNq76WSqmQBmoG9jgbcAB5ABGdswdeMQZHilJcu29iJ3OKKv6SlCulA
j1tHymwtbdhPuipd2wIDAQAB
```

7. 完了したら、*保存*をクリックします。
8. デュプレックスシステムの場合、上記の手順に従って2台目のコントローラでリモートログインを有効にすることができます。パスワードとSSHキーの両方のオプションを設定する場合は、「リモートログインに許可された公開鍵とパスワードを要求する」チェックボックスを再度選択してください。
9. テクニカルサポートのトラブルシューティングが完了したら、リモートログインの設定ダイアログボックスに戻り、*リモートログインを有効にする*チェックボックスの選択を解除することで、リモートログインを無効にできます。2台目のコントローラでリモートログインが有効になっている場合は、確認ダイアログが開き、2台目のコントローラでもリモートログインを無効にすることができます。

   リモートログインを無効にすると、現在のSSHセッションはすべて終了され、新しいログイン要求はすべて拒否されます。

コントローラをオンラインにする

コントローラがオフライン状態またはサービスモードの場合は、オンラインに戻すことができます。

手順

1. 「 * ハードウェア * 」を選択します。
2. 図にドライブが表示された場合は、*[コントローラとコンポーネント]*タブをクリックします。

   図の表示が切り替わり、ドライブではなくコントローラが表示されます。

3. オフライン状態またはサービスモードのコントローラをクリックします。

   コントローラのコンテキストメニューが表示されます。

4. 「オンラインにする」を選択し、処理を実行することを確認します。

結果

リストアされた優先パスがマルチパスドライバで検出されるまでに最大10分かかることがあります。

このコントローラが元 々 所有していたボリュームは、各ボリュームに対するI/O要求を受信すると自動的にコントローラに戻されます。場合によっては、* redistribute volumes *コマンドを使用して手動でボリュームを再配分する必要があります。

コントローラをオフラインにする

指示があった場合は、コントローラをオフラインに切り替えることができます。

開始する前に

- ストレージアレイにコントローラが2台必要です。オフラインに切り替えないコントローラはオンライン

（最適状態）である必要があります。

- 使用中のボリュームがないこと、またはそれらのボリュームを使用す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ことを確認します。

タスクの内容

```
[CAUTION]
====
Recovery
Guruまたはテクニカルサポートの指示がないかぎり、コントローラをオフラインにしないでください。

====
.手順
. 「 * ハードウェア * 」を選択します。
. 図にドライブが表示された場合は、*[コントローラとコンポーネント]*タブをクリックします。
+
図の表示が切り替わり、ドライブではなくコントローラが表示されます。

. オフラインに切り替えるコントローラをクリックします。
+
コントローラのコンテキストメニューが表示されます。

. 「*オフラインに切り替え」を選択し、操作を確定します。


.結果
System
Managerでコントローラのステータスがオフラインに更新されるまで数分かかることがあります。ステータスの更新が完了するまでは、他の処理を開始しないでください。



[[ID081c1d83a913939bf47491d8912ebcbb]]
= コントローラをサービスモードにする
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
指示があった場合は、コントローラをサービスモードに切り替えることができます。

.開始する前に
* ストレージアレイにコントローラが
2台必要です。サービスモードに切り替えないコントローラがオンライン（最適状態）である必要が
```

あります。
*
使用中のボリュームがないこと、またはそれらのボリュームを使用す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ことを確認します。

[NOTE]
====
コントローラをサービスモードにすると、パフォーマンスが大幅に低下する可能性があります。テクニカルサポートから指示がないかぎり、コントローラをサービスモードにしないでください。

====
.手順
. 「 * ハードウェア * 」を選択します。
. 図にドライブが表示された場合は、*[コントローラとコンポーネント]*タブをクリックします。
+
図の表示が切り替わり、ドライブではなくコントローラが表示されます。

. サービスモードにするコントローラをクリックします。
+
コントローラのコンテキストメニューが表示されます。

. [サービスモードに切り替え]を選択し、操作を確定します。

[[IDb9780e3f38c5a1fce76dd89257607030]]
= コントローラのリセット（リブート）
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
一部の問題に対処するには、コントローラのリセット（リブート）が必要です。コントローラに物理的にアクセスできない場合でも、コントローラをリセットできます。

.開始する前に
* ストレージアレイにコントローラが
2台必要です。リセットしないコントローラがオンライン（最適状態）である必要があります。
*
使用中のボリュームがないこと、またはそれらのボリュームを使用す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ことを確認します。

.手順
. 「 * ハードウェア * 」を選択します。
. 図にドライブが表示された場合は、*[コントローラとコンポーネント]*タブをクリックします。
+
図の表示が切り替わり、ドライブではなくコントローラが表示されます。

. リセットするコントローラをクリックします。
+
コントローラのコンテキストメニューが表示されます。

. 「* Reset *」を選択し、処理を確定します。

:leveloffset: -1

= iSCSIポートを管理します。

:leveloffset: +1

[[ID56df316820b3d03ae9f98244f2196d05]]
= iSCSIポートの設定
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
コントローラにiSCSIホスト接続が搭載されている場合は、[ハードウェア]ページからiSCSIポートを設定できます。

.開始する前に
* コントローラにiSCSIポートが搭載されている必要があります。そうでない場合、iSCSI設定は使用できません。
* ネットワーク速度（ポートとホストの間のデータ転送率）を把握しておく必要があります。

[NOTE]
====
iSCSIの設定と機能は、ストレージアレイがiSCSIをサポートしている場合にのみ表示されます。

====
.手順

. 「 * ハードウェア * 」を選択します。
. 図にドライブが表示された場合は、*[コントローラとコンポーネント]*タブをクリックします。
+
図の表示が切り替わり、ドライブではなくコントローラが表示されます。

. iSCSIポートを設定するコントローラをクリックします。
+
コントローラのコンテキストメニューが表示されます。

. Configure iSCSI Port* （ iSCSI ポートの設定）を選択します。
+
[NOTE]
====
Configure iSCSI Ports *オプションは、System Managerがコントローラで
iSCSIポートを検出した場合にのみ表示されます。

====
+
[iSCSIポートの設定]ダイアログボックスが開きます。

. ドロップダウンリストで、設定するポートを選択し、 * Next * をクリックします。
. 構成ポートの設定を選択し、 * 次へ * をクリックします。
+
すべてのポート設定を表示するには、ダイアログボックスの右側にある * Show more port settings * リンクをクリックします。

+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| ポート設定 | 製品説明

 a|
設定されているイーサネットポート速度（特定のタイプのホストインターフェイスカードでのみ表示されます）
 a|
ポートのSFPの速度と同じ速度を選択します。

 a|
Forward Error Correction （
FEC）モード（特定のタイプのホストインターフェイスカードでのみ表示されます）
 a|

必要に応じて、指定したホストポートのいずれかのFECモードを選択します。

NOTE: Reed Solomonモードでは、25Gbpsのポート速度はサポートされません。

a|
IPv4を有効にする/ IPv6を有効にする
a|
IPv4およびIPv6ネットワークのサポートを有効にするには、一方または両方のオプションを選択します。

NOTE: ポートアクセスをディセーブルにする場合は、両方のチェックボックスをオフにします。

a|
TCP リスニングポート（ [Show more port settings] をクリックすると使用可能）
a|
必要に応じて、新しいポート番号を入力します。

リスニングポートは、コントローラがホストiSCSIイニシエータからのiSCSIログインをリスンするために使用するTCPポート番号です。デフォルトのリスニングポートは3260です。3260または49152~65535の値を入力する必要があります。

a|
MTU サイズ（ * Show more port settings* をクリックすると使用可能）
a|
必要に応じて、Maximum Transmission Unit（
MTU；最大転送単位）の新しいサイズをバイト単位で入力します。

デフォルトのMaximum Transmission Unit（MTU；最大伝送ユニット）サイズは1500バイト/フレームです。1500 ~ 9000の値を入力する必要があります。

a|
ICMP PING応答をイネーブルにする
a|
Internet Control Message Protocol（
ICMP）を有効にするには、このオプションを選択します。ネットワーク接続されたコンピュータのオペレーティングシステムは、このプロトコルを使用してメッセージを送信します。これらのICMPメッセージは、ホストに到達できるかどうか、およびそのホストとのパケットの送受信にかかる時

間を決定します。

|===
====
+
[*IPv4 を有効にする *] を選択した場合、 [次へ *] をクリックすると、 IPv4 設定を選択するためのダイアログボックスが開きます。[*IPv6 を有効にする *] を選択した場合、 [次へ *] をクリックすると、 IPv6 設定を選択するためのダイアログボックスが開きます。両方のオプションを選択した場合は、 IPv4 設定のダイアログボックスが最初に開き、 * 次へ * をクリックすると、 IPv6 設定のダイアログボックスが開きます。

. IPv4 / IPv6を自動または手動で設定します。すべてのポート設定を表示するには、ダイアログボックスの右側にある * Show more settings * リンクをクリックします。
+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| ポート設定 | 製品説明

a|
設定を自動的に取得
a|
設定を自動的に取得するには、このオプションを選択します。

a|
静的設定を手動で指定する
a|
このオプションを選択し、フィールドに静的アドレスを入力します。（必要に応じて、カットアンド ペーストでアドレスをフィールドに貼り付けることもできます）。
IPv4の場合は、ネットワークのサブネットマスクとゲートウェイを指定します。IPv6の場合は、ルーティング可能なIPアドレスとルータのIPアドレスを指定します。

a|
VLAN サポートを有効にします（ * Show more settings * をクリックして使用可能）。
a|
VLANを有効にしてそのIDを入力するには、このオプションを選択します。VLANは、同じスイッチ、同じルータ、またはその両方でサポートされる他の物理LANや仮想LANから物理的に分離されているかのように動作する論理ネットワークです。

a|
イーサネットの優先順位を有効にする（ [詳細設定を表示する *] をクリックして使用可能）。
a|
ネットワークアクセスの優先度を決定するパラメータを有効にするには、このオプションを選択します。スライダを使用して優先度を1（最も低い）から7（最も高い）の間で選択します。

イーサネットなどの共有ローカルエリアネットワーク（LAN）環境では、多くのステーションがネットワークへのアクセスを争う場合があります。アクセスは先に行われたものから順に処理されます。2つのステーションが同時にネットワークにアクセスしようとすると、両方のステーションがオフになり、再試行する前に待機します。このプロセスは、スイッチポートに1つのステーションだけが接続されているスイッチドイーサネットでは最小限に抑えられます。

|===
====
. [完了] をクリックします。

[[IDac78a8268f0d76b2abf9d621f548c81d]]
= iSCSI認証の設定
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
iSCSIネットワークのセキュリティを強化するために、コントローラ（ターゲット）とホスト（イニシエータ）の間に認証を設定できます。

System Manager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、a_chap secret_という共有セキュリティキーに基づいて行われます。

.開始する前に
イニシエータ（iSCSIホスト）のCHAPシークレットは、ターゲット（コントローラ）のCHAPシークレットを設定する前でもあとでも設定できます。このタスクの手順を実行する前に、ホストがiSCSI接続を確立するのを待ってから、個々のホストでCHAPシークレットを設定する必要があります。接続が確立されると、iSCSI認証のダイアログボックス（このタスクで説明）にホストのIQN名とCHAPシークレットが表示されるため、手動で入力する必要はありません。

.タスクの内容

次のいずれかの認証方法を選択できます。

* *一方向認証*--コントローラがiSCSIホストの識別情報を認証できるようにするには
'この設定を使用します(一方向認証)
* *双方向認証*--コントローラとiSCSIホストの両方が認証(双方向認証
)を実行できるようにするには'この設定を使用しますこの設定は、コントローラがiSCSIホストの識別情報を認証し、iSCSIホストがコントローラの識別情報を認証できるようにすることで、第2レベルのセキュリティを提供します。

[NOTE]
====
iSCSIの設定と機能は、ストレージアレイがiSCSIをサポートしている場合にのみ[設定]ページに表示されます。

====
.手順
. メニューを選択します。[設定][システム]。
. [iSCSI設定]で、[*認証の設定*]をクリックします。
+
[Configure
Authentication]ダイアログボックスが表示され、現在設定されている方法が示されます。CHAPシークレットが設定されているホストがあるかどうかも表示されます。

. 次のいずれかを選択します。
+
** *認証なし*--コントローラがiSCSIホストのIDを認証しないようにするには
'このオプションを選択して'完了*をクリックしますダイアログボックスが閉じ、設定が完了します。
** *一方向認証*--コントローラがiSCSIホストのIDを認証できるようにするには
'このオプションを選択して'次へをクリックします*ターゲットCHAPの構成ダイアログ・ボックスを表示します
** *双方向認証*--コントローラとiSCSIホストの両方が認証を実行できるようにするには
'このオプションを選択して'次へ*をクリックし'ターゲットCHAPの構成ダイアログ・ボックスを表示します

. 一方向認証または双方向認証について、コントローラ（ターゲット）の
CHAPシークレットを入力または確認します。CHAPシークレットは12~57文字の印刷可能なASCII文字で指定する必要があります。
+
[NOTE]
====
コントローラのCHAPシークレットがすでに設定されている場合は、フィールド内の文字は表示されません。必要に応じて、既存の文字を置き換えることができます（新しい文字はマスクされません）。

====
. 次のいずれかを実行します。
+
** 一方向認証を設定する場合は、*完了
*をクリックします。ダイアログボックスが閉じ、設定が完了します。
** _2Way _authenticationを設定する場合は、* Next *をクリックしてConfigure Initiator CHAPダイアログボックスを表示します。

. 双方向認証の場合、いずれかのiSCSIホスト（イニシエータ）のCHAPシークレット（12~57文字の印刷可能なASCII文字）を入力または確認します。特定のホストに双方向認証を設定しない場合は、Initiator CHAP Secretフィールドを空白のままにします。
+
[NOTE]
====
ホストのCHAPシークレットがすでに設定されている場合は、フィールド内の文字は表示されません。必要に応じて、既存の文字を置き換えることができます（新しい文字はマスクされません）。

====
. [完了] をクリックします。

.結果
認証なしを指定した場合を除き、iSCSIログインシーケンス中にコントローラとiSCSIホストの間で認証が行われます。

[[ID29942e2ddc87785628c5cd630831efe0]]
= iSCSI検出設定の有効化
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
iSCSIネットワーク内のストレージデバイスの検出に関連する設定を有効にすることができます。

[ターゲット検出設定]では、Internet Storage Name Service（iSNS）プロトコルを使用してストレージアレイのiSCSI情報を登録し、名前のない検出セッションを許可するかどうかを決定できます。

.開始する前に
iSNSサーバで静的IPアドレスが使用されている場合は、そのアドレスをiSNSの登録に使用できる必要があります。IPv4とIPv6の両方がサポートされます。

.タスクの内容
iSCSI検出に関連する次の設定を有効にすることができます。

* * iSNSサーバによるターゲットの登録を有効にする*--有効にすると'
ストレージ・アレイはiSNSサーバからiSCSI Qualified Name（
IQN）とポート情報を登録しますこの設定は、イニシエータがiSNSサーバからIQNとポート情報を取得できるように、iSNS検出を許可します。
* *名前のない検出セッションを有効にする*--名前のない検出セッションを有効にすると
'イニシエータ（iSCSIホスト）は'検出タイプ接続のログインシーケンス中にターゲットのIQN（
コントローラ）を指定する必要はありません無効な場合、ホストはIQNを指定してコントローラへの検出セッションを確立する必要があります。ただし、通常の（I/Oベアリング）セッションでは常にターゲットIQNが必要です。この設定を無効にすると、権限のないiSCSIホストがIPアドレスのみを使用してコントローラに接続することを防止できます。

[NOTE]
====
iSCSIの設定と機能は、ストレージアレイがiSCSIをサポートしている場合にのみ[設定]ページに表示されます。

====
.手順
. メニューを選択します。[設定][システム]。
. [* iSCSI settings]で、[*ターゲット検出設定の表示/編集]をクリックします。
+
Target Discovery Settings
（ターゲット検出設定）ダイアログボックスが表示されます。[Enable iSNS
server*...]フィールドの下に、コントローラがすでに登録されているかどうかを示すダイアログボックスが表示されます。

. コントローラを登録するには、[iSNSサーバーを有効にしてターゲットを登録する
*]を選択し、次のいずれかを選択します。
+
** * DHCPサーバから自動的に設定を取得*--動的ホスト構成プロトコル(DHCP)
サーバを使用してiSNSサーバを設定する場合は'このオプションを選択しますこのオプションを使用する場合は、コントローラのすべてのiSCSIポートでDHCPを使用するように設定する必要があることに注意してください。必要に応じて、コントローラのiSCSIポートの設定を更新して、このオプションを有効にします。
+
[NOTE]
====
DHCPサーバでiSNSサーバのアドレスを指定するには'オプション43のベンダー固有の情報を使用するようにDHCPサーバを設定する必要があります このオプションでは、iSNSサーバの
IPv4アドレスをデータバイト0xa-0xd（10-13）に含める必要があります。

====

** *静的な設定を手動で指定*-- iSNSサーバの静的IPアドレスを入力する場合は
'このオプションを選択します（必要に応じて、カット アンド
ペーストでアドレスをフィールドに貼り付けることもできます）。IPv4アドレスまたはIPv6アドレスをフィールドに入力します。両方を設定した場合は、IPv4がデフォルトです。TCPリスニングポートも入力します（デフォルトの3205を使用するか、49152~65535の値を入力します）。

. ストレージアレイを名前のない検出セッションの対象にするには、
*名前のない検出セッションを有効にする*を選択します。
+
** 有効にすると、iSCSIイニシエータは、コントローラの情報を取得するためにターゲット
IQNを指定する必要はありません。
** 無効にすると、イニシエータがターゲット
IQNを指定しないかぎり、検出セッションは実行されません。名前のない検出セッションを無効にすると、セキュリティが強化されます。

. [保存（ Save ）] をクリックします。

.結果
System Managerがコントローラを
iSNSサーバに登録しようとする間、進捗状況バーが表示されます。このプロセスには最大で5分かかることがあります。

[[IDf214abb682ae80bf17adc0c9edc59ee1]]
= iSCSI統計パッケージの表示
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ストレージアレイへのiSCSI接続に関するデータを表示できます。

.タスクの内容
System Managerには、次のタイプの
iSCSI統計が表示されます。すべての統計は読み取り専用であり、設定することはできません。

NOTE: System
Managerに表示される統計のタイプは、ストレージアレイで使用可能な統計に基づきます。

* *イーサネットMAC統計*--メディアアクセス制御(MAC)の統計情報を提供します。
MACは、物理アドレスまたはMACアドレスと呼ばれるアドレス指定メカニズムも提供します。MACアドレスは、各ネットワークアダプタに割り当てられる一意のアドレスです。MACアドレスは、データパケットをサブネットワーク内の宛先に配信するのに役立ちます。
* *イーサネットTCP/IP統計*-- iSCSIデバイスのTCP (Transmission Control Protocol)とIP (Internet Protocol)のTCP/IPの統計情報を提供します
TCPを使用すると、ネットワーク接続されたホスト上のアプリケーションが相互に接続を作成し、その上でパケットでデータを交換できます。IPは、パケット交換されたネットワーク間でデータを通信するデータ指向プロトコルです。IPv4統計とIPv6統計は個別に表示されます。
* *イーサネットカーネル統計*--
iSCSIデバイスのプラットフォームカーネルドライバの統計を提供します。カーネル統計には、TCP/IP統計オプションと同様のネットワークデータが表示されます。ただし、カーネル統計データは、iSCSIハードウェアから直接ではなく、プラットフォームのカーネルドライバから収集されます。
* *ローカル・ターゲット/イニシエータ（プロトコル）統計
*：ストレージ・メディアへのブロック・レベルのアクセスを提供するiSCSIターゲットの統計情報を表示します非同期ミラーリング処理でイニシエータとして使用される場合は'ストレージ・アレイのiSCSI統計情報を表示します
* *DCBXの運用状態統計*--さまざまなData Center Bridging Exchange（DCBX）機能の運用状態を表示します。
* *LLDP TLV statistics *-- Link Layer Discovery Protocol (LLDP) Type Length Value (TLTLV)統計を表示します。
* *DCBX TLV統計*-- Data Center Bridging（DCB）環境内のストレージアレイのホストポートを識別する情報が表示されます。この情報は、識別および機能の目的でネットワークピアと共有されます。

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

.手順
. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
. [View iSCSI Statistics Packages]を選択します。
. タブをクリックして、さまざまな統計を表示します。
. ベースラインを設定するには、*新しいベースラインを設定*をクリックします。
+
ベースラインを設定すると、統計を収集するための新しい開始ポイントが設定されます。すべてのiSCSI統計に同じベースラインが使用されます。

[[ID8388533cfdf437d7be72d5885fbfed12]]
= iSCSIセッションの表示
:allow-uri-read:
:experimental:

```
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
ストレージ アレイへのiSCSI接続に関する詳細情報を表示できます。
iSCSIセッションは、非同期ミラー関係にあるホストまたはリモート ストレージ
アレイとの間で発生します。

.手順
. メニューを選択します。[設定][システム]。
. 「* iSCSIセッションの表示/終了*」を選択します。
+
現在のiSCSIセッションのリストが表示されます。

. *オプション：特定のiSCSIセッションに関する追加情報
を表示するには、セッションを選択し、*詳細の表示*をクリックします。
+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| 項目 | 製品説明


 a|
セッション識別子（SSID）
 a|
iSCSIイニシエータとiSCSIターゲット間のセッションを識別する16進数の文字列。SSIDは、ISI
DとTPGTで構成されます。



 a|
イニシエータSession ID（ISID）
 a|
セッション識別子のイニシエータの部分。イニシエータはログイン時にISIDを指定します。



 a|
ターゲットポータルグループ
 a|
iSCSIターゲット。
```

a|
ターゲットポータルグループタグ（TPGT）
a|
セッション識別子のターゲットの部分。iSCSIターゲットポータルグループの16ビットの数値識別子。

a|
イニシエータのiSCSI名
a|
世界規模で一意なイニシエータの名前。

a|
イニシエータのiSCSIラベル
a|
System Managerで設定されたユーザラベル。

a|
イニシエータのiSCSIエイリアス
a|
iSCSIノードにも関連付けることができる名前。エイリアスを使用すると、組織がユーザにわかりやすい文字列をiSCSI名に関連付けることができます。ただし、エイリアスはiSCSI名に代わるものではありません。イニシエータのiSCSIエイリアスは、System Managerではなく、ホストでのみ設定できます

a|
ホスト
a|
ストレージアレイに入出力を送信するサーバ。

a|
接続ID（CID）
a|
イニシエータとターゲット間のセッション内における接続の一意の名前。イニシエータがこのIDを生成し、ログイン要求の際にターゲットに提供します。接続IDは、接続を閉じるログアウト時にも表示されます。

a|
ポート識別子
a|
接続に関連付けられているコントローラポート。

a|
イニシエータIPアドレス
a|
イニシエータのIPアドレス。

a|
ネゴシエーション済みのログインパラメータ
a|
iSCSIセッションのログイン時に処理されるパラメータ。

a|
認証方式
a|
iSCSIネットワークへのアクセスを必要とするユーザを認証する手法。有効な値は* chap *
および* None *です。

a|
ヘッダーダイジェスト方式
a|
iSCSIセッションに有効なヘッダー値を表示する手法。HeaderDigestおよびDataDigestには、*
None *または* CRC32C *を使用できます。両方のデフォルト値は* None *です。

a|
データダイジェスト方式
a|
iSCSIセッションに有効なデータ値を表示する手法。HeaderDigestおよびDataDigestには、*
None *または* CRC32C *を使用できます。両方のデフォルト値は* None *です。

a|
最大接続数
a|
iSCSIセッションに許可される接続の最大数。接続の最大数は1~4です。デフォルト値は*1*です。

a|
ターゲットエイリアス
a|
ターゲットに関連付けられているラベル。

a|
イニシエータエイリアス
a|
イニシエータに関連付けられているラベル。

a|
ターゲットIPアドレス
a|
iSCSIセッションのターゲットのIPアドレス。DNS名はサポートされません。

a|
初期R2T
a|
最初の転送準備完了ステータス。ステータスは「* Yes *」または「* No *」のいずれかになります。

a|
最大バースト長
a|
このiSCSIセッションの最大SCSIペイロード（バイト）。512~262、144（256KB）を最大バースト長として指定できます。デフォルト値は*262,144（256KB）*です。

a|
第1バースト長

a|
このiSCSIセッションの未承諾データのSCSIペイロード（バイト）。512~131、072（128KB）を第1バースト長として指定できます。デフォルト値は*65,536（64KB）*です。

a|
デフォルトの待機時間
a|
接続が終了した後、または接続がリセットされた後、接続を試行するまでに待機する最小秒数。デフォルトの待機時間の値は、0～3600です。デフォルトは* 2 *です。

a|
デフォルトの保持時間
a|
接続の終了または接続のリセット後も接続が可能な最大秒数。デフォルトの保持時間は、0～3600です。デフォルト値は*20*です。

a|
最大未処理R2T
a|
このiSCSIセッションの未処理の「準備が完了した転送」の最大数。未処理の転送準備完了の最大値は1～16です。デフォルトは* 1 *です。

a|
エラーリカバリレベル
a|
このiSCSIセッションのエラーリカバリのレベル。エラーリカバリレベルの値は常に* 0 *に設定されています。

a|
受信データ最大セグメント長
a|
イニシエータまたはターゲットが任意のiSCSIペイロードデータユニット（PDU）で受信できるデータの最大量。

a|

ターゲット名
 a|
ターゲットの正式名（エイリアスではありません）。iqn形式のターゲット名です。

 a|
イニシエータ名
 a|
イニシエータの正式名（エイリアスではありません）。iqn形式または_eui_formatを使用するイニシエータ名です。

|===
====
. *オプション：*レポートをファイルに保存するには、*保存*をクリックします。
+
ブラウザのDownloadsフォルダにファイル名が付けられて保存され `iscsi-session-connections.txt`ます。

[[IDc3c0fc842eeb95caa0cbb4b4b09e723a]]
= iSCSIセッションの終了
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
不要になったiSCSIセッションを終了できます。iSCSIセッションは、非同期ミラー関係にあるホストまたはリモート ストレージ アレイとの間で発生します。

.タスクの内容
iSCSIセッションを終了する理由には、次のようなものがあります。

* *不正アクセス*-- iSCSI
イニシエータがログオンされていて、アクセスできない場合は、iSCSIセッションを終了して、iSCSIイニシエータをストレージアレイから強制的に切断できます。[なし]認証方式を使用できたため、iSCSIイニシエータがログオンできた可能性があります。
* *システムダウンタイム*--ストレージアレイを停止する必要があり
'iSCSIイニシエータがまだログオンしている場合は'iSCSIセッションを終了してiSCSIイニシエータをストレージアレイから切断できます

.手順
. メニューを選択します。[設定][システム]。
. 「* iSCSIセッションの表示/終了*」を選択します。
+
現在のiSCSIセッションのリストが表示されます。

. 終了するセッションを選択します。
. [セッションの終了]をクリックし、操作を実行することを確認します。

[[ID4205ac0b2c3dc09407918a98eadc120a]]
= iSER over InfiniBandポートの設定
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
コントローラにiSER over InfiniBandポートが搭載されている場合は、ホストとのネットワーク接続を設定できます。

.開始する前に
* コントローラにiSER over InfiniBandポートが搭載されている必要があります。そうでないと、System ManagerでiSER over InfiniBand設定を使用できません。
* ホスト接続のIPアドレスを確認しておく必要があります。

.手順
. 「 * ハードウェア * 」を選択します。
. 図にドライブが表示された場合は、*[コントローラとコンポーネント]*タブをクリックします。
+
図の表示が切り替わり、ドライブではなくコントローラが表示されます。

. iSER over InfiniBandポートを設定するコントローラをクリックします。
+
コントローラのコンテキストメニューが表示されます。

. iSER over InfiniBandポートの設定*を選択します。
+
[iSER over InfiniBandポートの設定]ダイアログボックスが開きます。

. ドロップダウンリストで設定するHICポートを選択し、ホストのIPアドレスを入力します。

. [*Configure*] をクリックします。
. 設定を完了したら、* Yes *をクリックしてiSER over InfiniBandポートをリセットします。

[[IDf3f87d8d4d42aab63dfc775401446fcb]]
= iSER over InfiniBandの統計の表示
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ストレージアレイのコントローラにiSER over InfiniBandポートが搭載されている場合は、ホスト接続に関するデータを表示できます。

.タスクの内容
System Managerには、次のタイプのiSER over InfiniBand統計が表示されます。すべての統計は読み取り専用であり、設定することはできません。

* *ローカルターゲット（プロトコル）統計*- iSER over InfiniBandターゲットの統計を提供し、ストレージメディアへのブロックレベルのアクセスが表示されます。
* * iSER over InfiniBandインターフェイス統計*- InfiniBandインターフェイス上のすべてのiSERポートの統計が提供され、各スイッチポートに関連付けられているパフォーマンス統計とリンクエラー情報が含まれます。

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

.手順
. メニューを選択します。[設定][システム]。
. View iSER over InfiniBand Statistics *を選択します。
. タブをクリックして、さまざまな統計を表示します。
. *オプション：*ベースラインを設定するには、*新しいベースラインの設定*をクリックします。
+
ベースラインを設定すると、統計を収集するための新しい開始ポイントが設定されます。すべてのiSER over InfiniBand統計に同じベースラインが使用されます。

```
:leveloffset: -1


= NVMeポートを管理します。

:leveloffset: +1


[[ID3f6c4f88a27aa9e30b5229c9d321f7ae]]
= NVMeの概要
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
一部のコントローラには、NVMe（Non-Volatile Memory Express）over
Fabricsを実装するためのポートが搭載されています。NVMeを使用すると、ホストとストレージアレイの間でハイパフォーマンスな通信が可能になります。



== NVMeとは

_NVM
_は「不揮発性メモリ」を表し、多くのタイプのストレージデバイスで使用されている永続的メモリです。_NVM_（NVM Express）は、
NVMデバイスとのハイパフォーマンスなマルチキュー通信に特化して設計された、標準インターフェイスまたはプロトコルです。



== NVMe over Fabricsとは

_NVMe over Fabrics（NVMe-oF）_は、
NVMeメッセージベースのコマンドおよびデータをホストコンピュータとストレージの間でネットワーク経由で転送できるようにするテクノロジ仕様です。NVMeストレージアレイ（a_subsystem
_）には、ファブリックを使用してホストからアクセスできます。NVMeコマンドは、ホスト側とサブシステム側の両方のトランスポート抽象化レイヤで有効化され、カプセル化されます。これにより、ハイパフォーマンスなNVMeインターフェイスがホストからストレージまでエンドツーエンドで拡張され、コマンドセットが標準化および簡易化されます。

NVMe-
```

oFストレージは、ローカルのブロックストレージデバイスとしてホストに提供されます。ボリューム（a_namespac_）は、他のブロックストレージデバイスと同様にファイルシステムにマウントできます。必要に応じて、REST API、SMcli、またはSANtricity System Managerを使用してストレージをプロビジョニングできます。

== NVMe Qualified Name（NQN）とは

NVMe Qualified Name（NQN）は、リモートストレージターゲットを識別するために使用します。ストレージアレイのNVMe修飾名は常にサブシステムによって割り当てられ、変更することはできません。NVMe Qualified Nameはアレイ全体で1つです。NVMe Qualified Nameは最大223文字です。iSCSI Qualified Nameと比較してみてください。

== ネームスペースとネームスペースIDとは何ですか？

ネームスペースはSCSIの論理ユニットに相当し、アレイ内のボリュームに関連付けられています。ネームスペースID（NSID）は、SCSIの論理ユニット番号（LUN）に相当します。NSIDはネームスペースの作成時に作成し、1~255の値を設定できます。

== NVMeコントローラとは

SCSI I_T nexus（ホストのイニシエータからストレージシステムのターゲットへのパス）と同様に、ホストの接続プロセス中に作成されるNVMeコントローラは、ホストとストレージアレイ内のネームスペースの間のアクセスパスを提供します。NVMeコントローラは、ホストのNQNとホストポート識別子によって一意に識別されます。NVMeコントローラは1つのホストにしか関連付けることができませんが、複数のネームスペースにアクセスできます。

SANtricity System Managerを使用して、どのホストがどのネームスペースにアクセスできるかを設定し、ホストのネームスペースIDを設定します。その後、NVMeコントローラが作成されると、NVMeコントローラからアクセス可能なネームスペースIDのリストが作成され、許可される接続の設定に使用されます。

[[ID8273c94615f5187b0c8ed18c4b6fb819]]
= NVMe over InfiniBandポートの設定
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
コントローラにNVMe over InfiniBand接続が搭載されている場合は、[ハードウェア]ページからNVMeポートを設定できます。

.開始する前に
* コントローラにNVMe over InfiniBandホストポートが搭載されている必要があります。そうでないと、System ManagerでNVMe over InfiniBand設定を使用できません。
* ホスト接続のIPアドレスを確認しておく必要があります。

[NOTE]
====
NVMe over InfiniBandの設定と機能は、ストレージアレイのコントローラにNVMe over InfiniBandポートが搭載されている場合にのみ表示されます。

====
.手順
. 「 * ハードウェア * 」を選択します。
. 図にドライブが表示された場合は、*[コントローラとコンポーネント]*タブをクリックします。
+
図の表示が切り替わり、ドライブではなくコントローラが表示されます。

. NVMe over InfiniBandポートを設定するコントローラをクリックします。
+
コントローラのコンテキストメニューが表示されます。

. Configure NVMe over InfiniBand ports] を選択します。
+
[NVMe over InfiniBandポートの設定]ダイアログボックスが開きます。

. 設定するHICポートをドロップダウンリストから選択し、IPアドレスを入力します。
+
200Gb対応のHICを使用してEF600ストレージアレイを設定する場合、このダイアログボックスには、2つのIPアドレスフィールドが表示されます。1つは物理ポート（外部）用のフィールドで、もう1つは仮想ポート（内部）用のフィールドです。両方のポートに一意のIPアドレスを割り当てる必要があります。これらの設定を使用すると、ホストで各ポート間のパスを確立し、HICのパフォーマンスを最大限に高めることができます。仮想ポートにIPアドレスを割り当てない場合、HICの実行速度は約半分になります。

. [*Configure*] をクリックします。
. 設定を完了したら、「* Yes」をクリックしてNVMe over InfiniBandポートをリセットします。

```
[[ID7c5261698bf75023943fc4db2cf0ca9a]]
= NVMe over RoCEポートの設定
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
コントローラにNVMe over RoCE（RDMA over Converged
Ethernet）の接続が搭載されている場合は、[ハードウェア]ページからNVMeポートを設定できます。

.開始する前に
* コントローラにNVMe over
RoCEホストポートが搭載されている必要があります。そうでないと、System ManagerでNVMe over RoCE設定を使用できません。
* ホスト接続のIPアドレスを確認しておく必要があります。


.手順
. 「 * ハードウェア * 」を選択します。
. 図にドライブが表示された場合は、*[コントローラとコンポーネント]*タブをクリックします。
+
図の表示が切り替わり、ドライブではなくコントローラが表示されます。

. NVMe over RoCEポートを設定するコントローラをクリックします。
+
コントローラのコンテキストメニューが表示されます。

. NVMe over RoCE ポートの設定 * を選択します。
+
[NVMe over RoCEポートの設定]ダイアログボックスが開きます。

. ドロップダウンリストで、設定するHICポートを選択します。
. 「 * 次へ * 」をクリックします。
+
すべてのポート設定を表示するには、ダイアログボックスの右側にある * Show more port settings * リンクをクリックします。

+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
```

```
|===
| ポート設定 | 製品説明


 a|
設定されたイーサネットポート速度
 a|
ポートのSFPの速度と同じ速度を選択します。




 a|
IPv4を有効にする/ IPv6を有効にする
 a|
IPv4およびIPv6ネットワークのサポートを有効にするには、一方または両方のオプションを選択します。


NOTE: ポートアクセスをディセーブルにする場合は、両方のチェックボックスをオフにします。




 a|
MTU サイズ（ * Show more port settings* をクリックすると使用可能）
 a|
必要に応じて、Maximum Transmission Unit（
MTU；最大転送単位）の新しいサイズをバイト単位で入力します。

デフォルトのMaximum Transmission Unit（MTU；最大伝送ユニット）サイズは1500バイト/フレームです。1500 ~ 9000の値を入力する必要があります。

|===
====
+
[*IPv4 を有効にする *] を選択した場合、 [ 次へ *] をクリックすると、 IPv4
設定を選択するためのダイアログボックスが開きます。[*IPv6 を有効にする *]
を選択した場合、 [ 次へ *] をクリックすると、 IPv6
設定を選択するためのダイアログボックスが開きます。両方のオプションを選択した場合は、
IPv4 設定のダイアログボックスが最初に開き、 * 次へ * をクリックすると、 IPv6
設定のダイアログボックスが開きます。

. IPv4 / IPv6を自動または手動で設定します。
+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
```

```
|===
| ポート設定 | 製品説明


 a|
設定を自動的に取得
 a|
設定を自動的に取得するには、このオプションを選択します。



 a|
静的設定を手動で指定する
 a|
このオプションを選択し、フィールドに静的アドレスを入力します。（必要に応じて、カットアンド ペーストでアドレスをフィールドに貼り付けることもできます）。
IPv4の場合は、ネットワークのサブネットマスクとゲートウェイを指定します。IPv6の場合は、ルーティング可能なIPアドレスとルータのIPアドレスを指定します。200Gb対応のHICを使用してEF600ストレージアレイを設定する場合、このダイアログボックスには、ネットワークパラメータの2セットのフィールドが表示されます。1つは物理ポート（外部）用のフィールドで、もう1つは仮想ポート（内部）用のフィールドです。両方のポートに一意のパラメータを割り当てる必要があります。これらの設定を使用すると、ホストで各ポート間のパスを確立し、HICのパフォーマンスを最大限に高めることができます。仮想ポートにIPアドレスを割り当てない場合、HICの実行速度は約半分になります。

|===
====
. [ 完了 ] をクリックします。



[[ID4cfbe7bdb104348b1a32bf761d169665]]
= NVMe over Fabrics統計の表示
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
ストレージアレイへのNVMe over Fabrics接続に関するデータを表示できます。

.タスクの内容
System Managerには、次のタイプのNVMe over Fabrics統計が表示されます。すべての統計は読み取り専用であり、設定することはできません。
```

* * nvmeサブシステム統計*- NVMeコントローラとそのキューの統計が表示されます。NVMeコントローラは、ストレージアレイ内のネームスペースとホストの間のアクセスパスを提供します。NVMeサブシステム統計では、接続障害、リセット、シャットダウンなどの項目を確認できます。
* * rdma Interface statistics *-- RDMAインターフェイス上のすべてのNVMe over Fabricsポートの統計を提供します。各スイッチポートに関連付けられているパフォーマンス統計とリンクエラー情報が含まれます。このタブは、NVMe over Fabricsポートが使用可能な場合にのみ表示されます。

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

.手順
. メニューを選択します。[設定][システム]。
. View NVMe over Fabrics Statistics *を選択します。
. *オプション：*ベースラインを設定するには、*新しいベースラインの設定*をクリックします。
+
ベースラインを設定すると、統計を収集するための新しい開始ポイントが設定されます。すべてのNVMe統計に同じベースラインが使用されます。

:leveloffset: -1

= ドライブの管理

:leveloffset: +1

[[ID614edfd345983dec11f162cb130c66bc]]
= ドライブの状態
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
System Managerでは、ドライブについてさまざまな状態が報告されます。

== アクセスの状態

[cols="25h,~"]
|===
| 都道府県 | 定義

 a|
バイパス
 a|
ドライブは物理的に存在しますが、コントローラがどちらのポートでもドライブと通信できません。

 a|
互換性なし
 a|
次のいずれかの状況に該当します。

* ドライブはストレージアレイでの使用が認定されていません。
* ドライブのセクターサイズが異なります。
*
ドライブに古いバージョンまたは新しいバージョンのファームウェアから使用できない構成データがあります。

 a|
削除済み
 a|
ドライブがストレージアレイから適切に取り外されていません。

 a|
現在
 a|
コントローラは両方のポートでドライブと通信できます。

 a|
応答なし
 a|

ドライブがコマンドに応答していません。

|===

== ロールの状態

[cols="25h,~"]
|===
| 都道府県 | 定義

a|
割り当て済み
a|
プールまたはボリュームグループのメンバーである。

a|
使用中のホットスペア
a|
障害が発生したドライブの交換用ドライブとして使用中です。ホットスペアはボリュームグループでのみ使用され、プールでは使用されません。

a|
スタンバイのホットスペア
a|
障害が発生したドライブの交換用ドライブとして使用可能な状態です。ホットスペアはボリュームグループでのみ使用され、プールでは使用されません。

a|
未割り当て
a|
プールまたはボリュームグループのメンバーではありません。

|===

== 可用性の状態

[cols="25h,~"]
|===

| 都道府県 | 定義

a|
失敗
a|
ドライブは動作していません。ドライブ上のデータを使用できません。

a|
障害の兆候
a|
ドライブで障害の前兆が検出されています。ドライブ上のデータはまだ使用できます。

a|
オフライン
a|
ドライブをデータの格納に使用できません。通常、ドライブがエクスポート中のボリュームグループに属しているか、ファームウェアのアップグレード中です。

a|
最適
a|
ドライブは正常に動作しています。

|===

[[ID3b948cc25690a7341437eb129d0861e8]]
= ソリッドステートディスク（SSD）
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ソリッドステートディスク（ SSD
）は、ソリッドステートメモリ（フラッシュ）を使用してデータを永続的に格納するデータストレージデバイスです。SSD
は従来のハードドライブをエミュレートしたものであり、ハードドライブと同じインターフェイス

で利用できます。

== SSDのメリット

ハードドライブと比較した場合のSSDの利点は次のとおりです。

* 高速起動（スピンアップなし）
* レイテンシの低減
* 1秒あたりのI/O処理数（IOPS）が増加
* 可動部品の数を減らして信頼性を向上
* 消費電力の削減
* 発熱量の削減と冷却の必要性の低減

== SSDの識別

[ハードウェア]ページのシェルフ前面ビューでSSDを特定できます。稲妻アイコン（SSDが取り付けられていることを示す）が表示されているドライブベイを探します。

== ボリュームグループ

ボリュームグループ内のすべてのドライブのメディアタイプ（すべてのSSDまたはすべてのハードドライブ）が同じである必要があります。ボリュームグループでメディアタイプやインターフェイスタイプを混在させることはできません。

== キャッシュ

コントローラの書き込みキャッシュは常にSSDに対して有効になります。書き込みキャッシュによってパフォーマンスが向上し、SSDの寿命が延びます。

コントローラキャッシュに加えて、SSDキャッシュ機能を実装してシステム全体のパフォーマンスを向上させることができます。SSDキャッシュでは、データがボリュームからコピーされ、2つの内部RAIDボリューム（コントローラごとに1つ）に格納されます。

[[IDd8c4f1cb41ed0c173224712dd58b4c51]]
= ドライブ表示の制限
:allow-uri-read:

```
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
物理属性と論理属性のタイプが異なるドライブがストレージアレイに含まれている場合、[ハードウェア]ページのフィルタフィールドを使用して、ドライブの表示を制限したり特定のドライブを特定したりできます。

.タスクの内容
ドライブフィルタを使用すると、特定のセキュリティ属性（セキュリティ対応など）を備えた特定の論理的な場所（ボリュームグループ1など）にある特定のタイプの物理ドライブ（すべてのSASなど）のみに表示を制限できます。これらのフィルタは一緒に使用することも別 々
に使用することもできます

[NOTE]
====
すべてのドライブが同じ物理属性を共有している場合、*次のドライブを表示する*フィルタフィールドは表示されません。すべてのドライブが同じ論理属性を共有している場合'ストレージ・アレイ*フィルタ・フィールドの* Anywhereは表示されません

====
.手順
. 「 * ハードウェア * 」を選択します。
. 最初のフィルタフィールド（* Show drives that are
...*）で、ドロップダウン矢印をクリックして、使用可能なドライブタイプとセキュリティ属性を表示します。
+
ドライブタイプには次のものがあります。

+
** ドライブのメディアタイプ（SSD、HDD）
** ドライブインターフェイスタイプ
** ドライブの容量（最大から最小）
** セキュリティ属性には次のようなものがあります（ドライブ速度（最大から最小）。
** セキュリティ対応
** セキュリティ有効
** DA（Data Assurance）対応
** FIPS に準拠している
** FIPS準拠（FIPS 140-2）
** FIPS準拠（FIPS 140-3）
+
これらの属性のいずれかがすべてのドライブで同じ場合、ドロップダウンリストには表示されません。たとえば、ストレージアレイにSASインターフェイスと速度15000rpmのSSDドライブがすべて含まれていて、一部のSSDの容量が異なる場合、ドロップダウンリストには容量のみがフィルタリングの選択肢として表示されます。
```

+
フィールドからオプションを選択すると、フィルタ条件に一致しないドライブはグラフィックビューでグレー表示されます。

.
2番目のフィルタボックスで、ドロップダウン矢印をクリックしてドライブに使用できる論理的な場所を表示します。
+
[NOTE]
====
フィルタ条件をクリアする必要がある場合は、フィルタボックスの右端にある[*Clear*]を選択します。

====
+
論理的な場所は次のとおりです。

+
** プール
** ボリュームグループ
** ホットスペア
** SSD キャッシュ
** 未割り当て
+
フィールドからオプションを選択すると、フィルタ条件に一致しないドライブはグラフィックビューでグレー表示されます。

. 必要に応じて、フィルタフィールドの右端で「
*ロケーターライトを点灯」を選択し、表示されたドライブのロケーターライトを点灯できます。
+
この操作は、ストレージアレイ内のドライブの物理的な場所を特定するのに役立ちます。

[[ID112bf48acce8aefab17af0005bf96ab0]]
= ドライブのロケーターライトを点灯
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
[ハードウェア]ページでロケータライトを点灯して、ストレージアレイ内のドライブの物理的な場所を特定できます。

.タスクの内容
[ハードウェア]ページには、1本または複数のドライブが表示されます。

.手順
. 「 * ハードウェア * 」を選択します。
. 1つ以上のドライブを特定するには、次のいずれかを実行します。
+
** *シングルドライブ*--
シェルフの図から、アレイ内の物理的な場所に配置するドライブを探します。（図にコントローラが表示されている場合は、*[ドライブ]*タブをクリックします）。ドライブをクリックしてコンテキストメニューを表示し、*[ロケーターライトを点灯]*を選択します。
+
ドライブのロケーターライトが点灯します。ドライブを物理的に配置したら、ダイアログに戻り、*電源をオフにする*を選択します。

** *複数のドライブ*--フィルタフィールドで
'左側のドロップダウンリストから物理ドライブタイプを選択し'右側のドロップダウンリストから論理ドライブタイプを選択します条件に一致するドライブの数がフィールドの右端に表示されます。次に、*ロケーターライトを点灯*をクリックするか、コンテキストメニューから*フィルタリングされたすべてのドライブを検索*を選択します。ドライブを物理的に配置したら、ダイアログに戻り、*電源をオフにする*を選択します。

[[ID721c1a5a232cd55e5d43cd0a7d86425f]]
= ドライブのステータスと設定の表示
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
メディアタイプ、インターフェイスタイプ、容量など、ドライブのステータスと設定を確認できます。

.手順
. 「 * ハードウェア * 」を選択します。

. 図にコントローラが表示された場合は、*[ドライブ]*タブをクリックします。
+
図の表示が切り替わり、コントローラではなくドライブが表示されます。

. ステータスおよび設定を表示するドライブを選択します。
+
ドライブのコンテキストメニューが開きます。

. 「 * 表示設定 * 」を選択します。
+
[ドライブ設定]ダイアログボックスが開きます。

. すべての設定を表示するには、ダイアログボックスの右上にある*詳細設定を表示
*をクリックします。
+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 製品説明

a|
ステータス
a|
「最適」、「オフライン」、「重大でない障害」、および「失敗」が表示されます。最適ステータスは、目的の動作状態を示します。

a|
モード
a|
割り当て済み、未割り当て、ホットスペアスタンバイ、または使用中のホットスペアが表示されます。

a|
場所
a|
ドライブが配置されているシェルフとベイの番号が表示されます。

a|

割り当て先/保護対象/保護対象

a|
ドライブがプール、ボリューム グループ、または
SSDキャッシュに割り当てられている場合は「割り当て先」と表示されます。値は、プール名、ボリューム グループ名、SSDキャッシュ名のいずれかです。ドライブが「スタンバイ」モードのホットスペアに割り当てられている場合は「保護対象」と表示されます。そのホット スペアが
1つ以上のボリューム グループを保護できる場合は、ボリューム
グループ名が表示されます。ボリュームグループを保護できない場合は、0個のボリュームグループが表示されます。

ドライブが「使用中」モードのホット
スペアに割り当てられている場合は「保護」と表示されます。値は、影響を受けるボリューム
グループの名前です。

ドライブが未割り当ての場合、このフィールドは表示されません。

a|
メディアタイプ

a|
ドライブが使用する記録メディアのタイプが表示されます。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）のいずれかです。

a|
使用済み寿命の割合（SSDドライブが存在する場合にのみ表示）

a|
これまでにドライブに書き込まれたデータ量を理論上の合計書き込み制限値で割った値。

a|
インターフェイスタイプ

a|
ドライブが使用するインターフェイスのタイプ（SASなど）が表示されます。

a|
ドライブパスの冗長性

a|
ドライブとコントローラ間の接続が冗長であるかどうか（「はい」または「いいえ」）が表示されます。

a|
容量（GiB）
a|
ドライブの使用可能容量（設定済みの合計容量）が表示されます。

a|
速度（RPM）
a|
速度がRPM単位で表示されます（SSDの場合は表示されません）。

a|
現在のデータ速度
a|
ドライブとストレージアレイの間のデータ転送速度が表示されます。

a|
論理セクターサイズ（バイト）
a|
ドライブが使用する論理セクターサイズが表示されます。

a|
物理セクターサイズ（バイト）
a|
ドライブで使用される物理セクターサイズが表示されます。通常、ハードディスクドライブの物理セクターサイズは4096バイトです。

a|
ドライブファームウェアバージョン
a|
ドライブファームウェアのリビジョンレベルが表示されます。

a|
World-Wide Identifier
a|

ドライブの一意の16進数の識別子が表示されます。

a|
製品ID
a|
製造元によって割り当てられた製品IDが表示されます。

a|
シリアル番号
a|
ドライブのシリアル番号が表示されます。

a|
メーカー
a|
ドライブのベンダーが表示されます。

a|
製造日
a|
ドライブが作成された日付が表示されます。

NOTE: NVMeドライブでは使用できません。

a|
セキュリティ対応
a|
セキュリティ対応ドライブであるかどうか（「はい」または「いいえ」）が表示されます。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（レベル140-2または140-3）があります。これらのドライブでは、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。ドライブセキュリティ機能を使用したセキュリティの強化に使用できるため、これらのドライブはsecured_capable_とみなされます。これらのドライブを使用するボリュームグループやプールでドライブセキュリティ機能を有効にすると、ドライブはsecure-_enabled_になります。

a|
セキュリティ有効
a|
セキュリティ有効ドライブであるかどうか（「はい」または「いいえ」）が表示されます。セキュリティ有効ドライブは、ドライブセキュリティ機能で使用されます。ドライブセキュリティ機能を有効にし、かつsecure-_enabled_drivesにあるプールまたはボリュームグループにドライブセキュリティを適用すると、ドライブはsecure-_enabled_になります。読み取り/書き込みアクセスは、正しいセキュリティキーが設定されたコントローラからのみ実行できます。この追加のセキュリティ機能により、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。

a|
読み取り/書き込みアクセス
a|
ドライブが読み取り/書き込みアクセス可能かどうか（「はい」または「いいえ」）が表示されます。

a|
ドライブセキュリティキー識別子
a|
セキュリティ有効ドライブのセキュリティキーが表示されます。ドライブセキュリティは、 Full Disk Encryption （ FDE ）ドライブまたは連邦情報処理標準（ FIPS ）ドライブを使用してセキュリティを強化するストレージアレイの機能です。これらのドライブをドライブセキュリティ機能と組み合わせて使用すると、データにアクセスするためのセキュリティキーが必要になります。ドライブをアレイから物理的に取り外した場合、別のアレイに取り付けるまでドライブは動作しません。別のアレイに取り付けると、正しいセキュリティキーを指定するまでセキュリティロック状態になります。

a|
Data Assurance（DA）対応
a|
Data Assurance（DA ）機能が有効かどうか（「はい」または「いいえ」）が表示されます。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する機能です。Data Assuranceは、Fibre ChannelなどのDA対応I/Oインターフェイスを使用するホストで、プールまたはボリュームグループのレベルで有効にすることができます。

```
 a|
DULBE対応
 a|
Deallocated or Unwritten Logical Block Error（
DULBE）のオプションが有効かどうか（「はい」または「いいえ」）を示します。DULBEはNVMeドライブのオプションです。このオプションを使用すると、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。

|===
====
. [* 閉じる * ] をクリックします。




[[ID021e689a9f425003c5c364477599a968]]
= ドライブの論理的な交換
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
ドライブに障害が発生した場合や、何らかの理由でドライブを交換する場合は、障害が発生したドライブを未割り当てのドライブまたは完全に統合されたホットスペアと論理的に交換できます。

.タスクの内容
ドライブを論理的に交換すると、ドライブが割り当てられ、関連付けられたプールまたはボリュームグループの永続的なメンバーになります。

論理的交換オプションは、次のタイプのドライブを交換する場合に使用します。

* 障害ドライブ
* 不明なドライブ
* 寿命に近付いていることがRecovery Guruによって通知されたSSDドライブ
* ドライブ障害の兆候があることがRecovery Guruによって通知されたハードドライブ
* 割り当てドライブ（プール内ではなく、ボリュームグループ内のドライブでのみ使用可能）


.開始する前に
交換用ドライブには次の特性が必要です。

* 最適状態
* 未割り当て状態
* 交換するドライブと同じ属性（メディアタイプ、インターフェイスタイプなど）
* FDE機能が同じ（推奨、必須ではない）
```

* DA機能が同じ（推奨、必須ではない）

.手順
. 「 * ハードウェア * 」を選択します。
. 図にコントローラが表示された場合は、*[ドライブ]*タブをクリックします。
+
図の表示が切り替わり、コントローラではなくドライブが表示されます。

. 論理的に交換するドライブをクリックします。
+
ドライブのコンテキストメニューが表示されます。

. 論理的に置換*をクリックします。
. *オプション：*交換後にドライブを使用停止する
*チェックボックスをオンにして、元のドライブを交換後に使用停止にします。
+
このチェックボックスは、元の割り当て済みドライブが障害状態でも不明状態でもない場合にのみ有効になります。

. [交換用ドライブの選択*]テーブルで、使用する交換用ドライブを選択します。
+
この表には、交換対象のドライブと互換性があるドライブのみが表示されます。可能であれば、シェルフ損失の保護とドロワー損失の保護が維持されるドライブを選択します。

. [*置換*]をクリックします。
+
元のドライブが障害状態または不明な場合は、パリティ情報を使用して交換用ドライブにデータが再構築されます。この再構築は自動的に開始されます。ドライブの障害インジケータライトが消灯し、プールまたはボリュームグループ内のドライブのアクティビティインジケータライトが点滅し始めます。

+
元のドライブが障害状態でも不明状態でもない場合は、元のドライブのデータが交換用ドライブにコピーされます。このコピー処理は自動的に開始されます。コピー処理が完了すると、元のドライブは未割り当て状態、またはチェックボックスが選択されている場合は失敗状態に移行します。

[[IDe2286a182f8d04b9280807fc7b98b66e]]
= ドライブの手動による再構築
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ドライブの再構築は、通常、ドライブの交換後に自動的に開始されます。ドライブの再構築が自動的に開始されない場合は、再構築を手動で開始できます。

[NOTE]
====
この処理は、テクニカルサポートまたはRecovery
Guruから指示があった場合にのみ実行してください。

====
.手順
. 「 * ハードウェア * 」を選択します。
. 図にコントローラが表示された場合は、*[ドライブ]*タブをクリックします。
+
図の表示が切り替わり、コントローラではなくドライブが表示されます。

. 手動で再構築するドライブをクリックします。
+
ドライブのコンテキストメニューが表示されます。

. 「* Reconstruct *」を選択して、処理を実行することを確認します。

[[ID7d04207344de10045e53ea2210c6aac3]]
= ドライブの初期化（フォーマット）
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ストレージアレイ間で割り当てられたドライブを移動する場合は、新しいストレージアレイで使用する前にドライブを初期化（フォーマット）する必要があります。

.タスクの内容
初期化すると、以前の設定情報がドライブから削除され、ドライブが未割り当て状態に戻ります。作成したドライブは、新しいストレージアレイの新しいプールまたはボリュームグループに追加できるようになります。

単一のドライブを移動する場合は、ドライブの初期化処理を使用します。あるストレージアレイから別のストレージアレイにボリュームグループ全体を移動する場合は、ドライブを初期化する必要はありません。

[CAUTION]
====
データ損失の可能性--ドライブを初期化すると
'ドライブ上のすべてのデータが失われますこの処理は、テクニカルサポートから指示があった場合にのみ実行してください。

====
.手順
. 「 * ハードウェア * 」を選択します。
. 図にコントローラが表示された場合は、*[ドライブ]*タブをクリックします。
+
図の表示が切り替わり、コントローラではなくドライブが表示されます。

. 初期化するドライブをクリックします。
+
ドライブのコンテキストメニューが表示されます。

. [Initialize（初期化）]を選択し、処理を実行することを確認します。

[[IDfbbf41407e5b5f409f632ef9a272813c]]
= ドライブの使用停止
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
指示があった場合は、ドライブを手動で使用停止できます。

.タスクの内容
System Managerは、ストレージアレイ内のドライブを監視します。あるドライブが多数のエラーを生成していることを検出すると、近いうちにドライブ障害が発生する可能性があることがRecovery Guruから通知されます。この状況が発生し、交換用ドライブがある場合は、ドライブを使用停止して予防的措置を講じることができます。交換用ドライブがない場合は、ドライブが自動的に障害状態になるまで待つことができます。

[CAUTION]
====
データアクセスが失われる可能性-
この操作により、データの損失やデータの冗長性の喪失が発生する可能性があります。この処理は、テクニカルサポートまたはRecovery Guruから指示があった場合にのみ実行してください。

====
.手順
. 「 * ハードウェア * 」を選択します。
. 図にコントローラが表示された場合は、*[ドライブ]*タブをクリックします。
+
図の表示が切り替わり、コントローラではなくドライブが表示されます。

. 使用停止するドライブをクリックします。
+
ドライブのコンテキストメニューが表示されます。

. 「* Fail *」を選択します。
. Copy contents of drive before failing *チェックボックスを選択したままにします。
+
コピーオプションは、割り当て済みドライブおよびRAID
0以外のボリュームグループに対してのみ表示されます。

+
ドライブを使用停止する前に、ドライブの内容をコピーしてください。構成によっては、ドライブの内容を先にコピーしないと、関連付けられているプールまたはボリュームグループのすべてのデータまたはデータの冗長性が失われる可能性があります。

+
コピーオプションを使用すると、再構築よりも短時間でドライブをリカバリでき、コピー処理中に別のドライブで障害が発生した場合にボリューム障害が発生する可能性が低くなります。

. ドライブを使用停止することを確定します。
+
ドライブを使用停止したら、30秒以上待ってから取り外します。

[[ID7bfb4cf3f8edefa1525b128dd9aba673]]
= ドライブの消去
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
[消去]オプションを使用すると、未割り当てのドライブをシステムから取り外す準備をすることができます。この手順では、データが永久に削除され、データが再度読み取れないようにします。

.開始する前に
ドライブは未割り当て状態である必要があります。

.タスクの内容
[消去]オプションは、ドライブ上のすべてのデータを完全に削除する場合にのみ使用してください。セキュリティ有効ドライブの場合、[消去]オプションを使用すると暗号化データが消去され、セキュリティ属性がセキュリティ対応にリセットされます。

[NOTE]
====
消去機能は、一部の古いドライブモデルをサポートしていません。これらの古いモデルのいずれかを消去しようとすると、エラーメッセージが表示されます。

====
.手順
. 「 * ハードウェア * 」を選択します。
. 図にコントローラが表示された場合は、*[ドライブ]*タブをクリックします。
+
図の表示が切り替わり、コントローラではなくドライブが表示されます。

.
必要に応じて、フィルタフィールドを使用してシェルフ内の未割り当てのドライブをすべて表示できます。[Show drives that are ...*]ドロップダウンリストから、[*Unassigned *]を選択します。
+
シェルフビューには未割り当てのドライブのみが表示され、それ以外のドライブはすべてグレー表示になります。

.
ドライブのコンテキストメニューを開くには、消去するドライブをクリックします。（複数のドライブを選択する場合は、[ドライブを消去]ダイアログボックスで選択できます）。
+
[CAUTION]
====
データ損失の可能性--
消去操作は取り消せません。手順の実行中に正しいドライブを選択していることを確認してください。

====
. コンテキストメニューから*消去*を選択します。
+
[ドライブを消去]ダイアログボックスが開き、消去処理の対象となるすべてのドライブが表示されます。

. 必要に応じて、表から追加のドライブを選択します。
_all_drivesを選択することはできません。1つのドライブの選択が解除されたままになっていることを

. と入力して処理を確認し `erase`、*[消去]*をクリックします。
+
[CAUTION]
====
この処理を続行することを確認してください。次のダイアログで[はい（Yes）]をクリックすると、操作を中止できません。

====
. 推定完了時間（Estimated Completion Time）ダイアログボックスで、*はい*（*Yes）をクリックして消去操作を続行します。

.結果
消去処理には数分から数時間かかることがあります。ステータスは、ホーム[進行中の処理を表示]メニューで確認できます。消去処理が完了すると、ドライブは別のボリュームグループまたはディスクプール、または別のストレージアレイで使用できるようになります。

.終了後
ドライブを再度使用する場合は、最初に初期化する必要があります。これを行うには、ドライブのコンテキストメニューから* Initialize *（初期化）を選択します。

[[ID07c8004f664def26b0cb4a0fee43ce47]]
= ロックされたNVMe / FIPSドライブのロック解除またはリセット
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ロックされたNVMeまたはFIPSドライブをストレージアレイに挿入する場合は、ドライブに関連付けられたセキュリティキーファイルを追加することでドライブデータのロックを解除できます。セキュリティキーがない場合は、ドライブの物理セキュリティID（PSID）を入力してロックされた各ドライブでリセットを実行し、セキュリティ属性をリセットしてドライブデータを消去できます。

.開始する前に
* ロックを解除する場合は、セキュリティキーファイル（拡張子）が管理クライアント（System Managerへのアクセスに使用するブラウザを備えたシステム）にあることを確認します `.slk`。キーに関連付けられているパスフレーズも確認しておく必要があります。
* リセットする場合は、リセットする各ドライブのPSIDを確認する必要があります。PSIDを確認するには、ドライブを物理的に取り外し、ドライブのラベルに記載されているPSID（最大32文字）を確認してから、ドライブを再度取り付けます。

.タスクの内容
このタスクでは、セキュリティキーファイルをストレージアレイにインポートして、NVMeドライブまたはFIPSドライブのデータのロックを解除する方法について説明します。セキュリティキーを使用できない状況では、ロックされたドライブでリセットを実行する方法についても説明します。

[NOTE]
====
外部キー管理サーバを使用してドライブがロックされている場合は、System Managerでメニュー：設定（System）>セキュリティキー管理（Security key management）を選択して、外部キー管理を設定し、ドライブのロックを解除します。

====
ロック解除機能には、[ハードウェア]ページまたはメニューからアクセスできます。[設定][システム]>[セキュリティキー管理]。次のタスクでは、[ハードウェア]ページからの手順を説明します。

.手順
. 「 * ハードウェア * 」を選択します。
. 図にコントローラが表示された場合は、*[ドライブ]*タブをクリックします。
+
図の表示が切り替わり、コントローラではなくドライブが表示されます。

. ロックを解除またはリセットするNVMeドライブまたはFIPSドライブを選択します。
+
ドライブのコンテキストメニューが開きます。

. セキュリティー・キー・ファイルを適用するには、*ロック解除*を選択します。セキュリティー・キー・ファイルがない場合は、*リセット*を選択します。
+
これらのオプションは、ロックされたNVMeドライブまたはFIPSドライブを選択した場合にのみ表示されます。

+
[CAUTION]
====
リセット処理を実行すると、すべてのデータが消去されます。リセットは、セキュリティキーがない場合にのみ実行してください。ロックされたドライブをリセットすると、ドライブ上のすべてのデータが完全に削除され、ドライブのセキュリティ属性がセキュリティ対応（ただし有効ではない）にリセットされます。*この操作は元に戻せません。*

====
. 次のいずれかを実行します。
+
.. *ロック解除*：［*セキュアドライブのロック解除*］ダイアログボックスで、［*参照*］をクリックし、ロック解除するドライブに対応するセキュリティキーファイルを選択します。次に、パスフレーズを入力し、*ロック解除*をクリックします。
.. *リセット*：*ロックされたドライブのリセット*ダイアログボックスで、フィールドに

PSID文字列を入力し、と入力し `RESET`て確認します。[*リセット*]をクリックします。
+
ロック解除の場合、1回の処理ですべてのNVMeドライブまたはFIPSドライブのロックを解除できます。リセット処理では、リセットするドライブを個別に選択する必要があります。

.結果
これで、別のボリュームグループまたはディスクプール、または別のストレージアレイでドライブを使用できるようになります。

:leveloffset: -1

= ホットスペアの管理

:leveloffset: +1

[[IDff41d13b89b9db098efedfa3a75dbbac]]
= ホットスペアドライブの概要
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ホットスペアは、System ManagerのRAID 1、RAID 5、またはRAID 6のボリュームグループで、スタンバイドライブとして機能します。

問題なく動作するドライブですが、データは格納されていません。ボリュームグループ内のドライブに障害が発生すると、障害が発生したドライブのデータがホットスペアとして割り当てられたドライブに自動的に再構築されます。

ホットスペアは、特定のボリュームグループ専用ではありません。ホットスペアとドライブで次の属性が共有されていれば、ストレージアレイ内の障害が発生したドライブに使用できます。

* 容量が等しい（またはホットスペアの容量が大きい）
* 同じメディアタイプ（HDD、SSDなど）
* インターフェイスタイプが同じ（SASなど）

== ホットスペアの特定方法

ホットスペアは、初期セットアップウィザードまたは[ハードウェア]ページから割り当てることができます。ホットスペアが割り当てられているかどうかを確認するには、[ハードウェア]ページに移動して、ピンクで表示されているドライブベイを探します。

== ホットスペアの適用方法

ホットスペアのカバレッジは次のように機能します。

* RAID 1、RAID 5、またはRAID 6のボリュームグループのホットスペアとして未割り当てのドライブを予約します。
+
[NOTE]
====
データ保護の方法が異なるプールにはホットスペアを使用できません。プールでは、追加のドライブを予約する代わりに、プール内の各ドライブにスペア容量（_予約済み容量_）を予約します。プール内のドライブに障害が発生した場合、コントローラはそのスペア容量内にデータを再構築します。

====
* RAID 1、RAID 5、またはRAID 6のボリュームグループ内のドライブで障害が発生した場合、コントローラは冗長性データを使用して障害が発生したドライブのデータを自動的に再構築します。障害が発生したドライブの代わりにホットスペアが自動的に使用され、物理的に交換する必要はありません。
*
障害が発生したドライブを物理的に交換すると、ホットスペアドライブから交換したドライブへのコピーバック処理が実行されます。ホットスペアドライブをボリュームグループの永続的メンバーとして指定している場合は、コピーバック処理は必要ありません。
*
ボリュームグループのトレイ損失の保護およびドロワー損失の保護が可能かどうかは、ボリュームグループを構成するドライブの場所によって異なります。ドライブの障害とホットスペアドライブの場所が原因で、トレイ損失の保護とドロワー損失の保護が失われることがあります。トレイ損失の保護とドロワー損失の保護が影響を受けないようにするには、障害が発生したドライブを交換してコピーバックプロセスを開始する必要があります。
*
障害が発生したドライブの代わりにホットスペアドライブが自動的に使用されるため、障害が発生したドライブの交換中もストレージアレイボリュームはオンラインのままでアクセス可能です。

== ホットスペアドライブの容量に関する考慮事項

保護するドライブの合計容量以上の容量のドライブを選択してください。たとえば、容量が8GiBの18GiBドライブがある場合、9GiB以上のドライブをホットスペアとして使用できます。通常、ドライブの容量がストレージアレイ内の最大ドライブの容量以上でないかぎり、ドライブをホットスペアとして割り当てないでください。

[NOTE]
====
物理容量が同じホットスペアを使用できない場合、ドライブの「使用容量」がホットスペアドライブの容量と同じかそれよりも小さい場合は、容量が小さいドライブをホットスペアとして使用できます。

====

== メディアおよびインターフェイスタイプに関する考慮事項

ホットスペアとして使用するドライブは、保護対象のドライブと同じメディアタイプおよびインターフェイスタイプである必要があります。たとえば、HDDドライブをSSDドライブのホットスペアとして使用することはできません。

== セキュリティ対応ドライブに関する考慮事項

セキュリティ対応ドライブ（FDEやFIPSなど）は、セキュリティ機能の有無にかかわらず、ドライブのホットスペアとして使用できます。ただし、セキュリティ対応でないドライブは、セキュリティ機能を備えたドライブのホットスペアとして使用することはできません。

セキュリティ有効ドライブをホットスペアとして使用するよう選択すると、完全消去を実行してから続行するようにSystem Managerから求められます。完全消去では、ドライブのセキュリティ属性はセキュリティ有効ではなくセキュリティ対応にリセットされます。

[NOTE]
====
ドライブセキュリティ機能を有効にし、セキュリティ対応ドライブで構成されるプールまたはボリュームグループを作成すると、ドライブは_secure-enabled _になります。読み取り/書き込みアクセスは、正しいセキュリティキーが設定されたコントローラからのみ実行できます。この追加のセキュリティ機能により、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。

====

== 推奨されるホットスペアドライブの数

初期セットアップウィザードを使用してホットスペアを自動的に作成した場合、System Managerでは、特定のメディアタイプおよびインターフェイスタイプのドライブ30本ごとに1つの

ホットスペアが作成されます。それ以外の場合は、ストレージアレイ内のボリュームグループ間にホットスペアドライブを手動で作成できます。

[[IDab0e4f36a34370a6f7c47b99ac944ba1]]
= ホットスペアの割り当て
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
RAID 1、RAID 5、またはRAID 6のボリュームグループでは、ホットスペアを追加データ保護のスタンバイドライブとして割り当てることができます。これらのボリュームグループのいずれかでドライブに障害が発生すると、コントローラは障害が発生したドライブのデータをホットスペアに再構築します。

.開始する前に
* RAID 1、RAID 5、またはRAID 6のボリュームグループを作成する必要があります。（ホットスペアはプールには使用できません。プールでは、データ保護用に各ドライブ内のスペア容量を使用します）。
* 次の条件を満たすドライブが使用可能な必要があります。
+
** 未割り当てで最適ステータス
** ボリュームグループ内のドライブと同じメディアタイプ（SSDなど）。
** ボリュームグループ内のドライブと同じインターフェイスタイプ（SASなど）。
** ボリュームグループ内のドライブの使用容量以上の容量。

.タスクの内容
このタスクでは、[ハードウェア]ページからホットスペアを手動で割り当てる方法について説明します。推奨されるカバレッジは、ドライブセットごとに2つのホットスペアです。

[NOTE]
====
ホットスペアは初期セットアップウィザードから割り当てることもできます。ホットスペアがすでに割り当てられているかどうかは、[ハードウェア]ページでピンクで表示されるドライブベイで確認できます。

====
.手順
. 「 * ハードウェア * 」を選択します。
. 図にコントローラが表示された場合は、*[ドライブ]*タブをクリックします。

+
図の表示が切り替わり、コントローラではなくドライブが表示されます。

. ホットスペアとして使用する未割り当てのドライブ（グレーで表示）を選択します。
+
ドライブのコンテキストメニューが開きます。

. [ホットスペアの割り当て]を選択します。
+
セキュリティ有効なドライブの場合は、[ドライブの完全消去]ダイアログ
ボックスが開きます。セキュリティ有効ドライブをホットスペアとして使用するには、まず完全消去処理を実行してドライブのすべてのデータを削除し、セキュリティ属性をリセットする必要があります。

+
[CAUTION]
====
データ損失の可能性--
正しいドライブを選択していることを確認してください完全消去処理が完了すると、どのデータもリカバリできなくなります。

====
+
ドライブが*セキュア有効でない場合は、ホットスペアドライブの割り当ての確認ダイアログボックスが開きます。

. ダイアログボックスのテキストを確認し、処理を確定します。
+
[ハードウェア]ページには、ホットスペアになったドライブがピンクで表示されます。

.結果
RAID 1、RAID 5、またはRAID
6のボリュームグループ内のドライブで障害が発生した場合、コントローラは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にデータを自動的に再構築します。

[[ID1e62484a54ebebc0f8ca0a75984e46f1]]
= ホットスペアの割り当て解除
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ホットスペアを未割り当てのドライブに戻すことができます。

.開始する前に
ホットスペアのステータスが最適、スタンバイである必要があります。

.タスクの内容
障害が発生したドライブのテイクオーバー中のホットスペアの割り当てを解除することはできません。ホットスペアのステータスが「最適」でない場合は、ドライブの割り当てを解除する前に、Recovery Guruの手順に従って問題を解決してください。

.手順
. 「 * ハードウェア * 」を選択します。
. 図にコントローラが表示された場合は、*[ドライブ]*タブをクリックします。
+
図の表示が切り替わり、コントローラではなくドライブが表示されます。

. 割り当てを解除するホットスペアドライブ（ピンクで表示）を選択します。
+
ピンクのドライブベイに対角線が表示されている場合は、ホットスペアが使用中であり、割り当てを解除できません。

+
ドライブのコンテキストメニューが開きます。

. ドライブのドロップダウンリストから、*ホットスペアの割り当て解除*を選択します。
+
このホットスペアの削除の影響を受けるボリュームグループと、他のホットスペアがそれらを保護しているかどうかがダイアログボックスに表示されます。

. 割り当て解除処理を確認します。

.結果
ドライブが未割り当てに戻ります（グレーで表示）。

:leveloffset: -1

= シェルフに関するFAQ

:leveloffset: +1

[[ID180a383deffdec98a138b7ed8782cc0b]]

= シェルフ損失の保護とドロワー損失の保護とは何ですか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
シェルフ損失の保護とドロワー損失の保護は、1つのシェルフまたはドロワーに障害が発生した場合にデータアクセスを維持できるプールおよび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例としては、ドライブシェルフへの電力供給の停止や、両方のI/Oモジュール（IOM）の障害などがあります。

[NOTE]
====
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。この場合、ドライブシェルフにアクセスできなくなり、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。

====
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。

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

 a|
プール
 a|
プールには5台以上のシェルフのドライブが含まれ、各シェルフに同数のドライブが含まれている必要があります。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。
 a|
5

 a|

```
RAID 6
 a|
ボリュームグループに同じシェルフのドライブが3本以上含まれない。
 a|
3




 a|
RAID 3またはRAID 5
 a|
ボリュームグループ内のドライブがそれぞれ別 々 のシェルフに配置されている。
 a|
3




 a|
RAID 1
 a|
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。
 a|
2




 a|
RAID 0
 a|
シェルフ損失の保護は実現できない。
 a|
該当なし

|===


== ドロワー損失の保護

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のシェルフだけです。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。

[NOTE]
====
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。この場合、ドロワーへのアクセス（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）を失うと、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。

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

 a|
プール
 a|
プール候補にはすべてのドロワーのドライブが含まれ、各ドロワーに同じ数のドライブが必要です。

プールに少なくとも5つのドロワーのドライブが含まれており、各ドロワーに同じ数のドライブが含まれている必要があります。

60ドライブシェルフでは、プールに含まれるドライブが15、20、25、30、35、40、45、50、55、または60本の場合にドロワー損失の保護を実現できます。最初の作成後に、5の倍数の増分をプールに追加できます。
 a|
5

 a|
RAID 6
 a|
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。
 a|
3

 a|
RAID 3またはRAID 5
 a|
ボリュームグループ内のドライブがそれぞれ別々のドロワーに配置されている。
 a|
3

 a|

```
RAID 1
 a|
```
ミラーペアの各ドライブが別 々 のドロワーに配置されている必要があります。
```
 a|
2




 a|
RAID 0
 a|
```
ドロワー損失の保護は実現できない。
```
 a|
```
該当なし

```
|===



[[ID7532a99f03fecdc7317d06bee1797c7c]]
= バッテリ学習サイクルとは何ですか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
学習サイクルは、スマートバッテリーゲージを較正するための自動サイクルです。

学習サイクルは次のフェーズで構成されます。

* 制御バッテリの放電
* 休息期間
* 充電

バッテリは所定のしきい値まで放電されます。このフェーズでは、バッテリゲージが較正されます。

学習サイクルに必要なパラメータは次のとおりです。

* フル充電されたバッテリ
* 過熱していないバッテリ

デュプレックスコントローラシステムでは、学習サイクルが同時に実行されます。複数のバッテリ

または一連のバッテリセルからバックアップ電源が供給されているコントローラでは、学習サイクルが連続して実行されます。

学習サイクルは、一定の間隔で、同じ曜日の同じ時刻に自動的に開始されるようにスケジュールされます。サイクルの間隔は週単位で記述されます。

[NOTE]
====
学習サイクルの完了には数時間かかることがあります。

====

:leveloffset: -1

= コントローラに関するFAQ

:leveloffset: +1

[[ID689fbaf924dcf88d11a2be3c6e88ded7]]
= 自動ネゴシエーションとは何ですか。
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
自動ネゴシエーションは、ネットワークインターフェイスが独自の接続パラメータ（速度とデュプレックス）を別のネットワークインターフェイスと自動的に調整する機能です。

通常、管理ポートの設定には自動ネゴシエーションが推奨されますが、ネゴシエーションに失敗した場合、ネットワークインターフェイスの設定が一致しないと、ネットワークパフォーマンスに重大な影響を与える可能性があります。この状況が許容できない場合は、ネットワークインターフェイスを手動で正しい設定に設定する必要があります。自動ネゴシエーションは、コントローラのイーサネット管理ポートによって実行されます。自動ネゴシエーションは、iSCSIホストバスアダプタでは実行されません。

[NOTE]
====
自動ネゴシエーションが失敗すると、コントローラは最も低レベルの共通設定である半二重の10BASE-Tで接続を確立しようとします。

====

```
[[ID7989bc2f6d5a954989c7713361ee6013]]
= IPv6ステートレスアドレス自動設定とは何ですか。
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
ステートレス自動設定を使用すると、ホストはアドレスやその他の設定情報をサーバから取得しません。

IPv6のステートレス自動設定には、リンクローカルアドレス、マルチキャスト、およびNeighbor Discovery（ND）プロトコルがあります。IPv6では、基盤となるデータリンク層アドレスからアドレスのインターフェイスIDを生成できます。

ステートレス自動設定とステートフル自動設定は、相互に補完しあう機能です。たとえば、ホストはステートレス自動設定を使用して自身のアドレスを設定できますが、ステートフル自動設定を使用してその他の情報を取得できます。ステートフル自動設定を使用すると、ホストはサーバからアドレスやその他の設定情報を取得できます。インターネットプロトコルバージョン6（IPv6）では、ネットワーク上のすべてのIPアドレスを一度に再番号付けできる方法も定義されています。IPv6は、ネットワーク上のデバイスがサーバを必要とせずにIPアドレスやその他のパラメータを自動的に設定する方法を定義します。

ステートレス自動設定を使用する場合、デバイスは次の手順を実行します。

. *リンクローカルアドレスを生成*--デバイスは10ビットのリンクローカルアドレスを生成し、その後に54個のゼロと64ビットのインターフェイスIDを生成します。
. *リンクローカルアドレスの一意性をテスト*--生成されるリンクローカルアドレスがローカルネットワークでまだ使用されていないことをテストしますデバイスがNDプロトコルを使用して近接要求メッセージを送信します。これに応答して、ローカルネットワークはネイバーアドバタイズメントメッセージをリッスンします。これは、別のデバイスがすでにリンクローカルアドレスを使用していることを示します。その場合は、新しいリンクローカルアドレスを生成するか、自動設定が失敗し、別の方法を使用する必要があります。
. *リンクローカルアドレスの割り当て*--一意性テストに合格すると、デバイスは自身のIPインタフェースにリンクローカルアドレスを割り当てます。リンクローカルアドレスは、ローカルネットワーク上での通信には使用できますが、インターネット経由では使用できません。
. *ルータに連絡*--ノードは、設定の続行の詳細についてローカルルータへの接続を試みます。この連絡先は、ルータから定期的に送信されるルータアドバタイズメントメッセージをリスンするか、またはルータに次の処理についての情報を要求する特定のルータ要求メッセージを送信することによって実行されます。
. *ノードへの指示*--ルーターは自動設定の続行方法をノードに指示します。または、ルータは、グローバルインターネットアドレスの決定方法をホストに通知します。

. *グローバルアドレスを設定*--
ホストは、グローバルに一意なインターネットアドレスを自身に設定します。このアドレスは、通常、ルータによってホストに提供されるネットワークプレフィックスから形成されます。

[[IDf99a4dbabc4250c88e51b4047b7d412b]]
= DHCPと手動設定のどちらを選択しますか。
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ネットワーク設定のデフォルトの方法は、Dynamic Host Configuration Protocol（DHCP；動的ホスト構成プロトコル）です。ネットワークにDHCPサーバがない場合を除き、必ずこのオプションを使用してください。

[[ID982f839bf211aaca20d3319ff27126c4]]
= DHCPサーバとは何ですか。
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Dynamic Host Configuration Protocol（DHCP；動的ホスト構成プロトコル）は、インターネットプロトコル（IP）アドレスの割り当てタスクを自動化するプロトコルです。

TCP / IPネットワークに接続されている各デバイスには、一意のIPアドレスを割り当てる必要があります。これらのデバイスには、ストレージアレイ内のコントローラが含まれます。

DHCPを使用しない場合は、ネットワーク管理者がこれらのIPアドレスを手動で入力します。DHCPでは、クライアントがTCP/IP操作を開始する必要がある場合、クライアントはアドレス情報の要求をブロードキャストします。DHCPサーバは要求を受信し、リース期間と呼ばれる指定された時間だけ新しいアドレスを割り当て、そのアドレスをクライアントに送信します。DHCPを使用すると、デバイスはネットワークに接続するたびに異なるIPアドレスを持つことができます。一部のシステムでは、デバイスが接続されている間でもデバイスのIPアドレスが変更されることがあります。

```
[[ID62be771618cfdf8f454c9ba85bc6aff5]]
= DHCPサーバを設定するにはどうすればよいですか。
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
ストレージアレイのコントローラに静的インターネットプロトコル（IP）アドレスを使用するには、動的ホスト構成プロトコル（DHCP）サーバを設定する必要があります。

DHCPサーバが割り当てるIPアドレスは、一般に動的であり、リース期間が終了するため変更される可能性があります。サーバやルータなどの一部のデバイスでは、スタティックアドレスを使用する必要があります。ストレージアレイのコントローラにも静的IPアドレスが必要です。

静的アドレスの割り当て方法については、DHCPサーバのマニュアルを参照してください。

```
[[IDd95aab6e786a2de15de9a2654d31d44f]]
= コントローラのネットワーク設定を変更する必要があるのはなぜですか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
アウトオブバンド管理を使用する場合は、各コントローラのネットワーク設定（インターネットプロトコル（IP）アドレス、サブネットワークマスク（サブネットマスク）、ゲートウェイ）を設定する必要があります。

ネットワーク設定は、動的ホスト構成プロトコル（DHCP）サーバを使用して設定できます。DHCPサーバを使用しない場合は、ネットワーク設定を手動で入力する必要があります。

```
[[ID771af2c8388fe9c9dcb883cfe53cb1a4]]
= ネットワーク設定はどこで入手できますか。
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]
インターネットプロトコル（IP）アドレス、サブネットワークマスク（サブネットマスク）、およびゲートウェイの情報は、ネットワーク管理者から入手できます。

この情報は、コントローラでポートを設定する際に必要となります。

[[ID30df5211f4ac470e3b5e4cf0de77d34e]]
= ICMP PING応答とは何ですか。
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Internet Control Message Protocol（ICMP）は、TCP / IPスイートのプロトコルの1つです。

`ICMP echo request`および(`ICMP echo reply`メッセージは、一般にメッセージと呼ばれ`ping`ます。
`Ping`は、システム管理者がネットワークデバイス間の接続を手動でテストしたり、ネットワーク遅延やパケット損失をテストしたりするために使用するトラブルシューティングツールです。このコマンドは `ping`、をネットワーク上のデバイスに送信します。デバイスは(`ICMP echo reply` (`ICMP echo reply`、すべてのデバイスでを無効にして、権限のないユーザがデバイスを検出しにくくするようにする必要があります。企業のネットワークセキュリティポリシーでは、が `ICMP echo request`要求される場合があり `ping`ます）。

[[ID5b8204138e8859f978144c5040172709]]
= DHCPサーバからポート設定または
iSNSサーバを更新する必要があるのはどのような場合ですか。
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
サーバが変更またはアップグレードされ、現在のストレージアレイと使用するストレージアレイに関連するDHCP情報が変更された場合は、DHCPサーバを更新します。

具体的には、DHCPサーバが別のアドレスを割り当てることがわかったときに、DHCPサーバからポート設定またはiSNSサーバを更新します。

[NOTE]
====
ポート設定を更新すると、そのポートのすべてのiSCSI接続が停止します。

====

[[ID35a48631f78a316190c24a353f6460d1]]
= 管理ポートを設定したあとはどうすればよいですか。
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ストレージアレイのIPアドレスを変更した場合は、必要に応じてUnified Managerのグローバルアレイビューを更新します。

Unified Managerでグローバルアレイビューを更新するには、インターフェイスを開き、メニューから「Manage [Discover]」に移動します。

SANtricity Storage Managerをまだ使用している場合は、Enterprise Management Window（EMW）に移動し、IPアドレスを削除してから、新しいIPアドレスを再度追加する必要があります。

[[IDc2908cebac10f0a28878a11e1ca63115]]
= ストレージシステムが最適モードでないのはなぜですか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ストレージシステムが最適モードでないのは、Invalid System Configuration状態が原因です。この状態でも既存のボリュームへの通常のI/Oアクセスは完全にサポートされますが、System Managerでは一部の処理が禁止されます。

ストレージシステムは、次のいずれかの理由で無効なシステム構成に移行する可能性があります。

* サブモデルID（
SMID）コードが正しくないか、プレミアム機能の制限を超えている可能性があるため、コントローラの規定違反が発生しています。
* ドライブファームウェアのダウンロードなどの内部サービス処理を実行中です。
* コントローラがパリティエラーのしきい値を超えたためロックダウンされました。
* 一般的なロックダウン状態が発生しました。

:leveloffset: -1

= iSCSIに関するFAQ

:leveloffset: +1

[[ID63cef008c4bfff48ea28e1e422502aa1]]
= iSNSサーバを登録に使用するとどうなりますか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Internet Storage Name Service（iSNS）サーバの情報を使用する場合は、
iSNSサーバを照会してターゲット（コントローラ）から情報を取得するようにホスト（イニシエータ）を設定できます。

この登録により、コントローラのiSCSI Qualified Name（IQN）とポート情報が
iSNSサーバに提供され、イニシエータ（iSCSIホスト）とターゲット（コントローラ）間の照会が可能になります。

[[ID2561e3b2a51c5404761938390fe9a668]]
= iSCSIでは、どの登録方法が自動的にサポートされますか。
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
iSCSIの実装では、Internet Storage Name Service（iSNS）検出方式またはSend

Targetsコマンドの使用がサポートされます。

iSNS方式では、イニシエータ（iSCSIホスト）とターゲット（コントローラ）の間でiSNS検出を実行できます。ターゲットコントローラを登録して、コントローラのiSCSI修飾名（IQN）とポート情報をiSNSサーバに提供します。

iSNSを設定しない場合、iSCSIホストはiSCSI検出セッション中にSend Targetsコマンドを送信できます。これに対する応答として、コントローラからポート情報（ターゲットIQN、ポートIPアドレス、リスニングポート、ターゲットポートグループなど）が返されます。ホストイニシエータはiSNSサーバからターゲットIPを取得できるため、iSNSを使用する場合はこの検出方法は必要ありません。

[[IDe294db063b65d08900eba02154c9cfbe]]
= iSER over InfiniBand統計には何が表示されますか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
View iSER over InfiniBand Statisticsダイアログボックスには、ローカルターゲット（プロトコル）統計とiSER over InfiniBand（IB）インターフェイス統計が表示されます。すべての統計は読み取り専用であり、設定することはできません。

* *ローカルターゲット（プロトコル）統計*- iSER over InfiniBandターゲットの統計を提供し、ストレージメディアへのブロックレベルのアクセスが表示されます。
* * iSER over InfiniBandインターフェイス統計*- InfiniBandインターフェイス上のすべてのiSER over InfiniBandポートの統計が提供され、各スイッチポートに関連付けられているパフォーマンス統計とリンクエラー情報が含まれます。

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

[[ID522f47cf51f03f295fde7d2270dcdc4b]]
= iSER over InfiniBandを設定または診断するためにほかに必要な作業は何ですか？
:allow-uri-read:
:experimental:

```
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
次の表に、iSER over InfiniBandセッションの設定と管理に使用するSystem
Managerの機能を示します。

[NOTE]
====
iSER over InfiniBandを設定できるのは、ストレージアレイのコントローラにiSER over
InfiniBandホスト管理ポートが搭載されている場合のみです。

====
[cols="35h,~"]
|===
| アクション | 場所


 a|
iSER over InfiniBandポートの設定
 a|
. 「 * ハードウェア * 」を選択します。
. [コントローラとコンポーネント]*タブを選択します。
. コントローラを選択します。
. iSER over InfiniBandポートの設定*を選択します。


または

. メニューを選択します。[設定][システム]。
. 下にスクロールして* iSER over InfiniBand setting*を選択し、* iSER over
InfiniBandポートの設定*を選択します。




 a|
iSER over InfiniBandの統計の表示
 a|
. メニューを選択します。[設定][システム]。
. 下にスクロールして* iSER over InfiniBand settings *を表示し、* View iSER over
InfiniBand Statistics *を選択します。


|===
```

```
[[IDc843315ad701d69e6273e06657e2301b]]
= iSCSIを設定または診断するために他に必要な作業は何ですか？
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
iSCSIセッションは、非同期ミラー関係にあるホストまたはリモートストレージアレイとの間で実行できます。次の表に、iSCSIセッションの設定と管理に使用するSystem Managerの機能を示します。

[NOTE]
====
iSCSI設定は、ストレージアレイでiSCSIがサポートされている場合にのみ使用できます。

====


== iSCSIの設定

[cols="1a,1a"]
|===
| アクション | 場所


 a|
iSCSI設定を管理します。
 a|
. メニューを選択します。[設定][システム]。
. 下にスクロールして* iscsi settings *を表示し、すべての管理機能を表示します。




 a|
iSCSIポートの設定
 a|
. 「 * ハードウェア * 」を選択します。
. [コントローラとコンポーネント]*タブを選択します。
. コントローラを選択します。
. Configure iSCSI Port* （ iSCSI ポートの設定）を選択します。
```

 a|
ホストのCHAPシークレットを設定する
 a|
. メニューを選択します。[設定][システム]。
. 下にスクロールして「* iSCSI settings *」（* iSCSI設定*）に進み、「Configure Authentication *」（認証の設定*）を選択

または

. メニューから「 Storage [Hosts] 」を選択します。
. ホストメンバーを選択します。
. メニューの[表示/設定の編集][ホストポート]タブをクリックします。

|===

== iSCSIの診断

[cols="1a,1a"]
|===
| アクション | 場所

 a|
iSCSIセッションの表示または終了
 a|
. メニューを選択します。[設定][システム]。
. 下にスクロールして「* iSCSI settings *」（* iSCSI設定）に進み、「* View/End iSCSI Sessions *」（* iSCSIセッションの表示/終了）を選択し

または

. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
. 「* iSCSIセッションの表示/終了*」を選択します。

 a|
iSCSI統計の表示

```
 a|
. メニューを選択します。[設定][システム]。
. 下にスクロールして* iSCSI設定*を表示し、* iSCSI統計パッケージの表示*を選択します。


または

. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
. [View iSCSI Statistics Packages]を選択します。


|===



:leveloffset: -1


= NVMeに関するFAQ

:leveloffset: +1


[[ID3dba76a10bf61c0202333d848c45ad0a]]
= NVMe over Fabrics統計には何が表示されますか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
View NVMe over Fabrics Statisticsダイアログボックスには、NVMeサブシステムとRDMAインターフェイスの統計が表示されます。すべての統計は読み取り専用であり、設定することはできません。

* * nvmeサブシステム統計*- NVMeコントローラとそのキューの統計が表示されます。NVMeコントローラは、ストレージアレイ内のネームスペースとホストの間のアクセスパスを提供します。NVMeサブシステム統計では、接続障害、リセット、シャットダウンなどの項目を確認できます。これらの統計の詳細については、[表見出しの凡例を表示する*]をクリックしてください。
* * rdma Interface statistics *-- RDMAインターフェイス上のすべてのNVMe over Fabricsポートの統計を提供します。各スイッチポートに関連付けられているパフォーマンス統計とリンクエラー情報が含まれます。このタブは、NVMe over Fabricsポートが使用可能な場合にのみ表示されます。統計の詳細については、[表見出しの凡例を表示する*]をクリックしてください。
```

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

[[ID46a1701bd06e7f818f0fe7723a72e1c3]]
= NVMe over InfiniBandを設定または診断するためにほかに必要な作業は何ですか？
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
次の表に、NVMe over InfiniBandセッションの設定と管理に使用するSystem Managerの機能を示します。

[NOTE]
====
NVMe over InfiniBandを設定できるのは、ストレージアレイのコントローラにNVMe over InfiniBandポートが搭載されている場合のみです。

====
[cols="35h,~"]
|===
| アクション | 場所

a|
NVMe over InfiniBandポートの設定
a|
. 「 * ハードウェア * 」を選択します。
. [コントローラとコンポーネント]*タブを選択します。
. コントローラを選択します。
. Configure NVMe over InfiniBand ports] を選択します。

または

. メニューを選択します。[設定][システム]。
. 下にスクロールして* NVMe over InfiniBand settings *を表示し、* Configure NVMe over InfiniBand ports *を選択します。

```
 a|
NVMe over InfiniBandの統計の表示
 a|
. メニューを選択します。[設定][システム]。
. 下にスクロールして* NVMe over InfiniBand settings *を表示し、* View NVMe over
Fabrics Statistics *を選択します。


|===



[[ID429ca9aaeaf1767fdea5a769dce65d2c]]
= NVMe over RoCEを設定または診断するために他に必要な作業は何ですか？
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
NVMe over RoCEは、[ハードウェア]ページと[設定]ページで設定および管理できます。

[NOTE]
====
NVMe over RoCEを設定できるのは、ストレージアレイのコントローラにNVMe over
RoCEポートが搭載されている場合のみです。

====
[cols="35h,~"]
|===
| アクション | 場所


 a|
NVMe over RoCEポートの設定
 a|
. 「 * ハードウェア * 」を選択します。
. [コントローラとコンポーネント]*タブを選択します。
. コントローラを選択します。
. NVMe over RoCE ポートの設定 * を選択します。


または
```

. メニューを選択します。[設定][システム]。
. 下にスクロールして* NVMe over RoCE settings *（NVMe over RoCE設定*）に進み、* Configure NVMe over RoCE Ports *（NVMe over RoCEポートの設定*）を選択します。

 a|
NVMe over Fabrics統計の表示
 a|
. メニューを選択します。[設定][システム]。
. 下にスクロールして* NVMe over RoCE settings *を表示し、* View NVMe over Fabrics Statistics *を選択します。

|===

[[ID15fb2978c6ffddb0056d78964f7a0534]]
= 1つの物理ポートに2つのIPアドレスがあるのはなぜですか。
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
EF600ストレージアレイには、外付けと内蔵の2つのHICを搭載できます。

この構成では、外部HICが内部の補助HICに接続されます。外部HICからアクセス可能な各物理ポートには、内部HICの仮想ポートが関連付けられています。

最大200Gbのパフォーマンスを実現するには、物理ポートと仮想ポートの両方に一意のIPアドレスを割り当てて、ホストが各ポートへの接続を確立できるようにする必要があります。仮想ポートにIPアドレスを割り当てない場合、HICの実行速度は約半分になります。

[[ID4350a8d5cc4e6728f77513a34ee395e6]]
= 1つの物理ポートに2セットのパラメータがあるのはなぜですか。
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
EF600ストレージアレイには、外付けと内蔵の2つのHICを搭載できます。

この構成では、外部HICが内部の補助HICに接続されます。外部HICからアクセス可能な各物理ポートには、内部HICの仮想ポートが関連付けられています。

最大200Gbのパフォーマンスを実現するには、物理ポートと仮想ポートの両方にパラメータを割り当てて、ホストが各ポートへの接続を確立できるようにする必要があります。仮想ポートにパラメータを割り当てない場合、HICの実行速度は約半分になります。

:leveloffset: -1

= ドライブに関するFAQ

:leveloffset: +1

[[ID4c0108ba133451378b49c2c2e1275bdc]]
= ホットスペアドライブとは何ですか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-storage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ホットスペアは、RAID 1、RAID 5、またはRAID 6のボリュームグループで、スタンバイドライブとして機能します。問題なく動作するドライブですが、データは格納されていません。ボリュームグループ内のドライブに障害が発生すると、障害が発生したドライブのデータがホットスペアに自動的に再構築されます。

ストレージアレイ内のドライブで障害が発生した場合は、障害が発生したドライブの代わりにホットスペアドライブが自動的に使用されます。物理的に交換する必要はありません。ドライブに障害が発生したときにホットスペアドライブを使用できる場合、コントローラは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を再構築します。

ホットスペアドライブは、特定のボリュームグループ専用ではありません。ホットスペアドライブは、ストレージアレイ内で容量が同じかそれよりも小さい障害が発生したドライブに使用できます。ホットスペアドライブは、保護対象のドライブとメディアタイプ（HDDまたはSSD）が同じである必要があります。

[NOTE]
====
ホットスペアドライブはプールではサポートされません。プールでは、ホットスペアドライブの代わりに、プールを構成する各ドライブ内の予約済み容量を使用します。

```
====



[[IDf62a1d470f41e735caef8926366e6612]]
= 予約済み容量とは何ですか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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。予約済み容量方式は、再構築の所要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本のドライブではなくプール内の複数のドライブに分散されるため、1本のドライブの速度や可用性に制限されることはありません。



[[ID513e08f8c0467a14bafab148acc0e27d]]
= ドライブを論理的に交換するのはどのような場合ですか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
ドライブに障害が発生した場合や、何らかの理由でドライブを交換する場合、ストレージアレイに未割り当てのドライブがあれば、障害が発生したドライブを未割り当てのドライブに論理的に交換することができます。未割り当てのドライブがない場合は、代わりにドライブを物理的に交換できます。

元のドライブのデータは、交換用ドライブにコピーまたは再構築されます。



[[ID447316213146aa75f5fdb57a87cd5cfb]]
= 再構築中のドライブのステータスはどこで確認できますか？
```

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


[role="lead"]
```
ドライブの再構築ステータスは、[実行中の処理]ダッシュボードで確認できます。

ホームページの右上にある* View Operations in Progress *リンクをクリックします。

ドライブによっては、完全な再構築にかなりの時間がかかることがあります。ボリューム所有権が変更された場合は、迅速な再構築の代わりに完全な再構築が実行されることがあります。

```
:leveloffset: -1


:leveloffset: -1


= アラート

:leveloffset: +1


[[IDec2179a4bf3f5f9924cfb64177359328]]
= アラートの概要
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
System Managerでは、ストレージアレイのアラートをEメール、SNMPトラップ、およびsyslogメッセージで送信するように設定できます。



== アラートとは

_アラート_ストレージアレイで発生した重要なイベントについて管理者に通知します。イベントには、バッテリの障害、最適からオフラインへのコンポーネントの移動、コントローラの冗長性の問題などが含まれます。重大イベントはすべて「アラート対象」とみなされるほか、一部の警告イベ
```

ントと情報イベントも「アラート対象」とみなされます。

詳細：

```
* xref:{relative_path}how-alerts-work.html["アラートの仕組み"]
* xref:{relative_path}alerts-terminology.html["アラートの用語"]
```

== アラートの設定方法

アラートは、メッセージとして1つ以上のEメールアドレスに送信するか、SNMPサーバにSNMPトラップとして送信するか、syslogサーバにメッセージとして送信するように設定できます。アラート設定はメニューから選択できます。Settings [Alerts]

詳細：

```
* xref:{relative_path}configure-mail-server-and-recipients-for-
alerts.html["メールサーバとアラートの受信者の設定"]
* xref:{relative_path}configure-syslog-server-for-alerts.html["
アラート用のsyslogサーバの設定"]
* xref:{relative_path}configure-snmp-alerts.html["SNMPアラートの設定"]
```

== 関連情報

アラートに関連する概念の詳細については、以下を参照してください。

```
* xref:{relative_path}../sm-support/overview-event-
log.html["イベントログの概要"]
* xref:{relative_path}why-are-timestamps-inconsistent-between-the-array-
and-alerts.html["一貫性のないタイムスタンプ"]
```

= 概念

```
:leveloffset: +1

[[ID88e7104474fe095ed5c81feafaf702c0]]
= アラートの仕組み
:allow-uri-read:
```

```
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
アラートは、ストレージアレイで発生した重要なイベントについて管理者に通知します。Eメール、SNMPトラップ、syslogを使用してアラートを送信できます。

アラートプロセスは次のように機能します。

. 管理者がSystem Managerで、次のうち1つ以上のアラート方法を設定します。
+
** *電子メール*--電子メールアドレスにメッセージが送信されます。
** *snmp *-- SNMPトラップがSNMPサーバに送信されます。
** *syslog *--メッセージがsyslogサーバに送信される。


. ストレージアレイのイベントモニタが問題 を検出すると、その問題
に関する情報をイベントログに書き込みます（メニュー：サポート[イベントログ]から選択できます）。これには、バッテリの障害、最適からオフラインへのコンポーネントの状態の変化、コントローラの冗長性の問題などが含まれます。
.
イベントモニタがイベントが「アラート対象」であると判断すると、設定されているアラート方法（Eメール、SNMP、syslog）を使用して通知が送信されます。重大イベントはすべて「アラート対象」とみなされるほか、一部の警告イベントと情報イベントも「アラート対象」とみなされます。




== アラートの設定

アラートは、初期セットアップウィザード（Eメールアラートのみ）または[アラート]ページから設定できます。現在の設定を確認するには、メニューから「Settings [Alerts]」に移動します。

[アラート]タイルには、次のいずれかのアラート設定が表示されます。

* 未設定
* 設定：少なくとも
1つのアラート方法が設定されています。どのアラート方法が設定されているかを確認するには、カーソルでタイルをポイントします。




== アラート情報
```

アラートには次の種類の情報を含めることができます。

* ストレージアレイの名前。
* イベントログエントリに関連するイベントエラータイプ。
* イベントが発生した日時。
* イベントの簡単な説明。

[NOTE]
====
syslogアラートはRFC 5424のメッセージング標準に準拠します。

====

[[ID4dfd3ba925477fb9221b919d38d0a888]]
= アラートの用語
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ストレージアレイに関連するアラートの用語を次に示します。

[cols="25h,~"]
|===
| コンポーネント | 製品説明

a|
イベントモニタ
a|
イベントモニタはストレージアレイに常駐し、バックグラウンドタスクとして実行されます。イベントモニタは、ストレージアレイの異常を検出すると、問題に関する情報をイベントログに書き込みます。これには、バッテリの障害、最適からオフラインへのコンポーネントの状態の変化、コントローラの冗長性の問題などが含まれます。イベントモニタがイベントが「アラート対象」であると判断すると、設定されているアラート方法（Eメール、SNMP、syslog）を使用して通知が送信されます。重大イベントはすべて「アラート対象」とみなされるほか、一部の警告イベントと情報イベントも「アラート対象」とみなされます。

a|

メールサーバ
a|
メールサーバは、Eメールアラートの送受信に使用されます。サーバはSimple Mail Transfer Protocol（SMTP；簡易メール転送プロトコル）を使用します。

a|
SNMP
a|
簡易ネットワーク管理プロトコル（SNMP）は、IPネットワーク上のデバイス間で情報を管理および共有するために使用されるインターネット標準プロトコルです。

a|
SNMPトラップ
a|
SNMPトラップは、SNMPサーバに送信される通知です。トラップには、ストレージアレイの重大な問題に関する情報が含まれています。

a|
SNMPトラップの送信先
a|
SNMPトラップの送信先は、SNMPサービスを実行しているサーバのIPv4またはIPv6アドレスです。

a|
コミュニティ名
a|
コミュニティ名は、SNMP環境でネットワークサーバのパスワードのように機能する文字列です。

a|
MIBファイル
a|
管理情報ベース（MIB）ファイルは、ストレージアレイ内で監視および管理されるデータを定義します。SNMPサービスアプリケーションがインストールされたサーバにコピーしてコンパイルする必要があります。このMIBファイルは、サポートサイトのSystem Managerソフトウェアで入手できます。

```
 a|
MIB変数
 a|
管理情報ベース（MIB）変数は、SNMP
GetRequestsへの応答として、ストレージアレイ名、アレイの場所、担当者などの値を返すことができます。



 a|
syslog
 a|
syslogは、ネットワークデバイスがイベントメッセージをロギングサーバに送信するために使用するプロトコルです。



 a|
UDP
 a|
User Datagram Protocol（
UDP;ユーザデータグラムプロトコル）は、パケットヘッダーで送信元と宛先のポート番号を指定するトランスポートレイヤプロトコルです。

|===



:leveloffset: -1


= Eメールアラートの管理

:leveloffset: +1


[[ID1f6e20ecd5e889aaac8203f6c26c452a]]
= メールサーバとアラートの受信者の設定
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Eメールアラートを設定するには、メールサーバのアドレスとアラート受信者のEメールアドレスを
```

指定する必要があります。Eメールアドレスは20個まで指定できます。

.開始する前に
* メールサーバのアドレスを確認しておく必要があります。アドレスには、IPv4アドレス、IPv6アドレス、または完全修飾ドメイン名を使用できます。
+
[NOTE]
====
完全修飾ドメイン名を使用するには、両方のコントローラにDNSサーバを設定する必要があります。DNSサーバは[ハードウェア]ページで設定できます。

====
* アラート送信者として使用する
Eメールアドレスを確認しておく必要があります。これは、アラートメッセージの「送信元」フィールドに表示されるアドレスです。SMTPプロトコルでは送信者アドレスが必要です。ない場合はエラーになります。
* アラート受信者の
Eメールアドレスを確認しておく必要があります。受信者は、通常、ネットワーク管理者またはストレージ管理者のアドレスです。Eメールアドレスは20個まで入力できます。

.タスクの内容
このタスクでは、メールサーバを設定し、送信者と受信者のEメールアドレスを入力し、入力したすべてのEメールアドレスを[アラート]ページからテストする方法について説明します。

[NOTE]
====
Eメールアラートは初期セットアップウィザードで設定することもできます。

====
.手順
. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
. [*Email*]タブを選択します。
+
Eメールサーバがまだ設定されていない場合は、[Email]タブに[Configure Mail Server]と表示されます。

. ［*メールサーバーの設定*］を選択します。
+
メールサーバーの設定ダイアログボックスが開きます。

. メールサーバの情報を入力し、[保存]をクリックします。
+
** *メールサーバーアドレス*--メールサーバーの完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスを入力します。
+
[NOTE]

====
完全修飾ドメイン名を使用するには、両方のコントローラにDNSサーバを設定する必要があります。DNSサーバは[ハードウェア]ページで設定できます。

====
** *Email sender address *--
電子メールの送信者として使用する有効な電子メールアドレスを入力しますこのアドレスは、電子メールメッセージの[送信元]フィールドに表示されます。
** *Encryption*--メッセージを暗号化する場合は、暗号化タイプとして*SMTPS*
または*STARTTLS
*を選択し、暗号化されたメッセージのポート番号を選択します。それ以外の場合は、*なし*を選択します。
** *ユーザー名とパスワード*--
必要に応じて、送信側とメールサーバーで認証を行うためのユーザー名とパスワードを入力します。
** *電子メールに連絡先情報を含める*--
送信者の連絡先情報を警告メッセージに含めるには、このオプションを選択し、名前と電話番号を入力します。
+
[保存]をクリックすると、[アラート]ページの[電子メール]タブに電子メールアドレスが表示されます。

. [電子メールの追加]を選択します。
+
[電子メールの追加]ダイアログボックスが開きます。

. アラート受信者のEメールアドレスを1つ以上入力し、*追加*をクリックします。
+
EメールアドレスがAlerts（アラート）ページに表示されます。

. メールアドレスが有効であることを確認するには、「*すべてのメールをテスト*」をクリックして、テストメッセージを受信者に送信します。

.結果
Eメールアラートを設定すると、アラート対象のイベントが発生するたびに、イベントモニタから指定した受信者にEメールメッセージが送信されます。

[[ID63d9c40a96da66645bf42891a369ff37]]
= アラート用のEメールアドレスの編集
:allow-uri-read:
:experimental:
:icons: font

```
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Eメールアラートを受信する受信者のEメールアドレスを変更できます。

.開始する前に
編集する電子メールアドレスは、[Alerts]ページの[Email]タブで定義する必要があります。

.手順
. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
. [*Email*]タブを選択します。
. [*Email Address*]テーブルで、変更するアドレスを選択し、右端にある
*Edit*（鉛筆）アイコンをクリックします。
+
行が編集可能なフィールドになります。

. 新しいアドレスを入力し、*保存*（チェックマーク）アイコンをクリックします。
+
[NOTE]
====
変更をキャンセルする場合は、* Cancel *（X）アイコンを選択します。

====


.結果
[Alerts]ページの[Email]タブには、更新された電子メールアドレスが表示されます。



[[ID8d86be4772d89566487ff78cb379676e]]
= アラート用のEメールアドレスの追加
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Eメールアラートには受信者を20人まで追加できます。

.手順
. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
. [*Email*]タブを選択します。
```

. [電子メールの追加]を選択します。
+
[電子メールの追加]ダイアログボックスが開きます。

. 空のフィールドに、新しいEメールアドレスを入力します。複数のアドレスを追加する場合は、[別の電子メールを追加]を選択して別のフィールドを開きます。
. [追加]*をクリックします。

.結果
[Alerts]ページの[Email]タブに新しい電子メールアドレスが表示されます。

[[ID5720345595874402d317907d56730d0d]]
= アラート用のメールサーバまたはEメールアドレスの削除
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
以前に定義したメールサーバを削除してアラートがEメールアドレスに送信されないようにすることも、個 々 のEメールアドレスを削除することもできます。

.手順
. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
. [*Email*]タブを選択します。
. テーブルで、次のいずれかを実行します。
+
** メールサーバを削除してアラートが
Eメールアドレスに送信されないようにするには、メールサーバの行を選択します。
** E
メールアドレスを削除してこのアドレスにアラートが送信されないようにするには、削除するEメールアドレスの行を選択します。表の右上にある* Delete *ボタンを選択できるようになります。

. [削除（Delete）]をクリックし、操作を確定する。

[[ID874a3689fcb0d5a5db3d614866fedf5c]]
= アラート用のメールサーバの編集
:allow-uri-read:

```
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Eメールアラートに使用するメールサーバのアドレスやEメール送信者のアドレスを変更することができます。

.開始する前に
変更するメールサーバのアドレスを確認しておく必要があります。アドレスには、IPv4アドレス、IPv6アドレス、または完全修飾ドメイン名を使用できます。

[NOTE]
====
完全修飾ドメイン名を使用するには、両方のコントローラにDNSサーバを設定する必要があります。DNSサーバは[ハードウェア]ページで設定できます。

====
.手順
. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
. [*Email*]タブを選択します。
. ［*メールサーバーの設定*］を選択します。
+
メールサーバーの設定ダイアログボックスが開きます。

. メールサーバのアドレス、送信者情報、および連絡先情報を編集します。
+
** *メールサーバのアドレス*--メールサーバの完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスを編集します。
+
[NOTE]
====
完全修飾ドメイン名を使用するには、両方のコントローラにDNSサーバを設定する必要があります。DNSサーバは[ハードウェア]ページで設定できます。

====
** *電子メール送信者のアドレス*--
電子メールの送信者として使用される電子メールアドレスを編集しますこのアドレスは、電子メールメッセージの[送信元]フィールドに表示されます。
** *電子メールに連絡先情報を含める*--
送信者の連絡先情報を編集するには、このオプションを選択し、名前と電話番号を編集します。


. [ 保存（ Save ） ] をクリックします。
```

```
:leveloffset: -1


= SNMPアラートの管理

:leveloffset: +1


[[ID23eae046e0bf55ec6e34ba8ea6978357]]
= SNMPアラートの設定
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
簡易ネットワーク管理プロトコル（SNMP）アラートを設定するには、ストレージアレイのイベントモニタからSNMPトラップを送信できるサーバを少なくとも1つ指定する必要があります。この設定には、コミュニティ名またはユーザ名、およびサーバのIPアドレスが必要です。

.開始する前に
* ネットワークサーバに
SNMPサービスアプリケーションが設定されている必要があります。イベントモニタがトラップメッセージをそのアドレスに送信できるようにするには、このサーバのネットワークアドレス（IPv4またはIPv6アドレス）が必要です。複数のサーバを使用できます（最大10台のサーバを使用できます）。
* 管理情報ベース（MIB）ファイルは、
SNMPサービスアプリケーションを使用してサーバにコピーおよびコンパイルされています。このMIBファイルは、監視および管理されるデータを定義します。
+
MIBファイルがない場合は、NetAppサポートサイトから入手できます。

+
** に進みます
https://mysupport.netapp.com/site/global/dashboard["NetAppのサポート"^]。
** [*ダウンロード]タブをクリックし、[*ダウンロード]を選択します。
** EシリーズSANtricity OSコントローラソフトウェア*をクリックします。
** [最新リリースのダウンロード]を選択します。
** ログインします。
** 注意事項と使用許諾契約書に同意します。
** コントローラタイプの
MIBファイルが表示されるまで下にスクロールし、リンクをクリックしてファイルをダウンロードし
```

ます。

.タスクの内容
このタスクでは、トラップの送信先となるSNMPサーバを指定し、設定をテストする方法について説明します。

.手順
. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
. SNMP *タブを選択します。
+
初回セットアップ時に、[SNMP]タブに「コミュニティ/ユーザの設定」と表示されます。

. コミュニティ/ユーザーの設定*を選択します。
+
[SNMPバージョンの選択]ダイアログボックスが開きます。

. アラートのSNMPバージョンとして、* SNMPv2c *または* SNMPv3 *のいずれかを選択します。
+
選択した内容に応じて、[コミュニティの設定]ダイアログボックスまたは[SNMPv3ユーザの設定]ダイアログボックスが開きます。

. SNMPv2c（コミュニティ）またはSNMPv3（ユーザ）に対応する手順に従います。
+
** *SNMPv2c (communities)*--
コミュニティの設定ダイアログで、ネットワークサーバーのコミュニティストリングを1つ以上入力します。コミュニティ名は、既知の管理ステーションのセットを識別する文字列で、通常はネットワーク管理者によって作成されます。印刷可能なASCII文字のみで構成されます。コミュニティは最大256個追加できます。完了したら、*保存*をクリックします。
** *SNMPv3(Users)*-- SNMPv3ユーザーの設定ダイアログで、*Add*をクリックし、次の情報を入力します。
+
*** *ユーザー名*--ユーザーを識別するための名前を入力します最大31文字まで入力できます
*** *エンジンID *--メッセージの認証キーと暗号化キーを生成するために使用されるエンジンIDを選択します管理ドメイン上で一意である必要がありますほとんどの場合、*ローカル*を選択してください。標準以外の設定を使用している場合は、「*カスタム*」を選択します。別のフィールドが表示され、10～32文字の範囲で、正規のエンジンIDを16進数の文字列で入力する必要があります。
*** *認証資格情報*--
ユーザーの識別を保証する認証プロトコルを選択します次に、認証プロトコルを設定または変更するときに必要な認証パスワードを入力します。パスワードは8~128文字で指定する必要があります。
*** *プライバシー資格情報*--
メッセージの内容を暗号化するために使用するプライバシープロトコルを選択します次に、プライ

バシープロトコルを設定または変更するときに必要なプライバシーパスワードを入力します。パスワードは8~128文字で指定する必要があります。完了したら、[*追加]をクリックし、[*閉じる]をクリックします。

. [SNMP]タブが選択されている[Alerts]ページで、[Add Trap Destinations*]をクリックします。
+
トラップ送信先の追加ダイアログボックスが開きます。

.
1つ以上のトラップ送信先を入力し、関連付けられているコミュニティ名またはユーザ名を選択して、* Add *をクリックします。
+
** *Trap Destination*-- SNMPサービスを実行しているサーバーのIPv4またはIPv6アドレスを入力します
** *コミュニティ名またはユーザー名*--
ドロップダウンから、このトラップの送信先のコミュニティ名（SNMPv2c）またはユーザー名（SNMPv3）を選択します。（定義した名前が1つだけの場合は、このフィールドにすでに名前が表示されます）。
** *認証失敗トラップを送信*--コミュニティ名またはユーザ名が認識されないためにSNMP要求が拒否された場合にトラップの送信先にアラートを送信するには、このオプション（チェックボックス）を選択します。[Add（追加）]をクリックすると、[* Alerts]ページの[* SNMP]タブにトラップの送信先と関連する名前が表示されます。

. トラップが有効であることを確認するには、テーブルからトラップの送信先を選択し、*トラップの送信先のテスト*をクリックして、設定したアドレスにテストトラップを送信します。

.結果
アラート対象のイベントが発生すると、イベントモニタはSNMPトラップをサーバに送信します。

[[ID6e09564f3397ff76b6d7ea608eb1cd2e]]
= SNMPアラートのトラップ送信先の追加
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]

SNMPトラップを送信するサーバは最大10台まで追加できます。

.開始する前に
* 追加するネットワークサーバに
SNMPサービスアプリケーションが設定されている必要があります。イベントモニタがトラップメッセージをそのアドレスに送信できるようにするには、このサーバのネットワークアドレス（IPv4またはIPv6アドレス）が必要です。複数のサーバを使用できます（最大10台のサーバを使用できます）。
* 管理情報ベース（MIB）ファイルは、
SNMPサービスアプリケーションを使用してサーバにコピーおよびコンパイルされています。このMIBファイルは、監視および管理されるデータを定義します。
+
MIBファイルがない場合は、NetAppサポートサイトから入手できます。

+
** に進みます
https://mysupport.netapp.com/site/global/dashboard["NetAppのサポート"^]。
** [* Downloads（ダウンロード）]をクリックし、[* Downloads（ダウンロード）]を選択します。
** EシリーズSANtricity OSコントローラソフトウェア*をクリックします。
** [最新リリースのダウンロード]を選択します。
** ログインします。
** 注意事項と使用許諾契約書に同意します。
** コントローラタイプの
MIBファイルが表示されるまで下にスクロールし、リンクをクリックしてファイルをダウンロードします。

.手順
. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
. SNMP *タブを選択します。
+
現在定義されているトラップ送信先が表に表示されます。

. 「トラップのディスペションを追加」*を選択します。
+
トラップ送信先の追加ダイアログボックスが開きます。

.
1つ以上のトラップ送信先を入力し、関連付けられているコミュニティ名またはユーザ名を選択して、* Add *をクリックします。
+
** *Trap Destination*-- SNMPサービスを実行しているサーバーのIPv4または
IPv6アドレスを入力します
** *コミュニティ名またはユーザー名*--

ドロップダウンから、このトラップの送信先のコミュニティ名（SNMPv2c）またはユーザー名（SNMPv3）を選択します。（定義した名前が1つだけの場合は、このフィールドにすでに名前が表示されます）。
** *認証失敗トラップを送信*--コミュニティ名またはユーザ名が認識されないためにSNMP要求が拒否された場合にトラップの送信先にアラートを送信するには、このオプション（チェックボックス）を選択します。「*追加」をクリックすると、トラップの送信先と関連するコミュニティ名またはユーザ名が表に表示されます。

. トラップが有効であることを確認するには、テーブルからトラップの送信先を選択し、*トラップの送信先のテスト*をクリックして、設定したアドレスにテストトラップを送信します。

.結果
アラート対象のイベントが発生すると、イベントモニタはSNMPトラップをサーバに送信します。

[[ID60ea7604b913adbfbbe4691b98dd8bbf]]
= SNMP MIB変数の設定
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SNMPアラートの場合、必要に応じて、SNMPトラップに表示される管理情報ベース（MIB）変数を設定できます。これらの変数は、ストレージアレイ名、アレイの場所、および担当者を返すことができます。

.開始する前に
MIBファイルは、SNMPサービスアプリケーションがインストールされたサーバにコピーしてコンパイルする必要があります。

MIBファイルがない場合は、次の方法で入手できます。

* に進みます
https://mysupport.netapp.com/site/global/dashboard["NetAppのサポート"^]。
* [* Downloads（ダウンロード）]をクリックし、[* Downloads（ダウンロード）]を選択します。
* EシリーズSANtricity OSコントローラソフトウェア*をクリックします。
* [最新リリースのダウンロード]を選択します。
* ログインします。
* 注意事項と使用許諾契約書に同意します。
* コントローラタイプの

MIBファイルが表示されるまで下にスクロールし、リンクをクリックしてファイルをダウンロードします。

.タスクの内容
このタスクでは、SNMPトラップのMIB変数を定義する方法について説明します。これらの変数は、SNMP GetRequestsへの応答として次の値を返すことができます。

* `sysName`（ストレージアレイの名前）
* `sysLocation`（ストレージアレイの場所）
* `sysContact`（管理者の名前）

.手順
. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
. SNMP *タブを選択します。
. [Configure SNMP MIB Variables]を選択します。
+
SNMP MIB変数の設定ダイアログボックスが開きます。

. 次の値を1つ以上入力し、*保存*をクリックします。
+
** *Name*-- MIB変数の値 `sysName`。たとえば、ストレージアレイの名前を入力します。
** *Location*-- MIB変数の値
`sysLocation`。たとえば、ストレージアレイの場所を入力します。
** *Contact*-- MIB変数の値
`sysContact`。たとえば、ストレージアレイを担当する管理者を入力します。

.結果
これらの値は、ストレージアレイのアラートのSNMPトラップメッセージに表示されます。

[[ID515a538fdfd08a18f40c7f8ded2d79b4]]
= SNMPv2cトラップのコミュニティの編集
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SNMPv2cトラップのコミュニティ名を編集できます。

.開始する前に
コミュニティ名を作成する必要があります。

.手順
. メニューを選択します：[Alerts]を設定します。
. SNMP *タブを選択します。
+
トラップの送信先とコミュニティ名が表に表示されます。

. [コミュニティの設定]を選択します。
. 新しいコミュニティ名を入力し、* Save *
をクリックします。コミュニティ名には印刷可能なASCII文字のみを使用できます。

.結果
[アラート]ページの[SNMP]タブに、更新されたコミュニティ名が表示されます。

[[ID29efd2daa6bd4dafdcd7224b251e4a9c]]
= SNMPv3トラップのユーザ設定の編集
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SNMPv3トラップのユーザ定義を編集できます。

.開始する前に
SNMPv3トラップ用のユーザを作成する必要があります。

.手順
. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
. SNMP *タブを選択します。
+
トラップの送信先とユーザ名が表に表示されます。

. ユーザー定義を編集するには、テーブルでユーザーを選択し、*ユーザーの設定
*をクリックします。
. ダイアログで、*表示/設定の編集*をクリックします。
. 次の情報を編集します。
+
** *ユーザー名*--ユーザーを識別する名前を変更します最大31文字まで入力できます

** *エンジンID *--メッセージの認証キーと暗号化キーを生成するために使用されるエンジンIDを選択します管理ドメイン上で一意である必要がありますほとんどの場合、*ローカル*を選択してください。標準以外の設定を使用している場合は、「*カスタム*」を選択します。別のフィールドが表示され、10～32文字の範囲で、正規のエンジンIDを16進数の文字列で入力する必要があります。
** *認証資格情報*--
ユーザーの識別を保証する認証プロトコルを選択します次に、認証プロトコルを設定または変更するときに必要な認証パスワードを入力します。パスワードは8~128文字で指定する必要があります。
** *プライバシー資格情報*--
メッセージの内容を暗号化するために使用するプライバシープロトコルを選択します次に、プライバシープロトコルを設定または変更するときに必要なプライバシーパスワードを入力します。パスワードは8~128文字で指定する必要があります。

.結果
[アラート]ページの[SNMP]タブに、更新された設定が表示されます。

[[ID9f44e215f0b41391a7e48c1b0f4b19c5]]
= SNMPv2cトラップのコミュニティの追加
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SNMPv2cトラップには、最大256個のコミュニティ名を追加できます。

.手順
. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
. SNMP *タブを選択します。
+
トラップの送信先とコミュニティ名が表に表示されます。

. [コミュニティの設定]を選択します。
+
コミュニティの設定ダイアログボックスが開きます。

. [*別のコミュニティを追加*]を選択します。
. 新しいコミュニティ名を入力し、* Save *をクリックします。

.結果
[Alerts]ページの[SNMP]タブに新しいコミュニティ名が表示されます。

[[IDe5b8a9f83926f6d81dd327edaea92d5b]]
= SNMPv3トラップのユーザの追加
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SNMPv3トラップには最大256人のユーザを追加できます。

.手順
. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
. SNMP *タブを選択します。
+
トラップの送信先とユーザ名が表に表示されます。

. [ユーザーの設定]を選択します。
+
[SNMPv3ユーザの設定]ダイアログボックスが開きます。

. 「 * 追加」を選択します。
. 次の情報を入力し、*追加*をクリックします。
+
** *ユーザー名*--ユーザーを識別するための名前を入力します最大31文字まで入力できます
** *エンジンID *--メッセージの認証キーと暗号化キーを生成するために使用されるエンジンIDを選択します管理ドメイン上で一意である必要がありますほとんどの場合、*ローカル*を選択してください。標準以外の設定を使用している場合は、「*カスタム*」を選択します。別のフィールドが表示され、10～32文字の範囲で、正規のエンジンIDを16進数の文字列で入力する必要があります。
** *認証資格情報*--
ユーザーの識別を保証する認証プロトコルを選択します次に、認証プロトコルを設定または変更するときに必要な認証パスワードを入力します。パスワードは8~128文字で指定する必要があります。
** *プライバシー資格情報*--
メッセージの内容を暗号化するために使用するプライバシープロトコルを選択します次に、プライバシープロトコルを設定または変更するときに必要なプライバシーパスワードを入力します。パスワードは8~128文字で指定する必要があります。

[[IDb9f9635f4b9a35476ad5ea479ff02938]]
= SNMPv2cトラップのコミュニティを削除します。
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SNMPv2cトラップのコミュニティ名を削除できます。

.手順
. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
. SNMP *タブを選択します。
+
トラップの送信先とコミュニティ名は、[* Alerts]*ページに表示されます。

. [コミュニティの設定]を選択します。
+
コミュニティの設定ダイアログボックスが開きます。

. 削除するコミュニティ名を選択し、右端の*削除*（X）アイコンをクリックします。
+
このコミュニティ名にトラップ送信先が関連付けられている場合は、Confirm Remove Communityダイアログボックスに、影響を受けるトラップ送信先アドレスが表示されます。

. 操作を確定し、*削除*をクリックします。

.結果
コミュニティ名とそれに関連付けられているトラップ送信先は、[Alerts]ページから削除されます。

[[ID0e1be32d50101fb46cfe775cf370aaaf]]
= SNMPv3トラップのユーザの削除
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SNMPv3トラップのユーザを削除できます。

.手順
. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
. SNMP *タブを選択します。
+
トラップの送信先とユーザ名が[アラート]ページに表示されます。

. [ユーザーの設定]を選択します。
+
[SNMPv3ユーザの設定]ダイアログボックスが開きます。

. 削除するユーザー名を選択し、*削除*をクリックします。
. 操作を確定し、*削除*をクリックします。

.結果
ユーザ名と関連付けられているトラップ送信先が[アラート]ページから削除されます。

[[ID4225b7e9731d7f113710feab4d213046]]
= トラップ送信先の削除
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
トラップ送信先アドレスを削除して、ストレージアレイのイベントモニタからそのアドレスにSNMPトラップが送信されないようにすることができます。

.手順
. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
. SNMP *タブを選択します。
+
トラップ送信先のアドレスが表に表示されます。

. トラップの送信先を選択し、ページ右上の*削除*をクリックします。
. 操作を確定し、*削除*をクリックします。
+
宛先アドレスは[Alerts]ページに表示されなくなります。

.結果
削除したトラップ送信先にストレージアレイのイベントモニタからSNMPトラップが受信されなくなります。

:leveloffset: -1

= syslogアラートの管理

:leveloffset: +1

[[IDfa9dde2e61cb528699df5324254b3ec9]]
= アラート用のsyslogサーバの設定
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
syslogアラートを設定するには、syslogサーバのアドレスとUDPポートを入力する必要があります。最大5つのsyslogサーバを指定できます。

.開始する前に
*
syslogサーバのアドレスを確認しておく必要があります。このアドレスは、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスのいずれかで指定できます。
* syslogサーバのUDPポート番号を確認しておく必要があります。通常は514です。

.タスクの内容
このタスクでは、syslogサーバのアドレスとポートを入力し、入力したアドレスをテストする方法について説明します。

.手順
. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
. *Syslog *タブを選択します。
+
syslogサーバがまだ定義されていない場合は、[アラート]ページに「syslogサーバの追加」と表示されます。

. [Add Syslog Servers]をクリックします。
+
[Add Syslog Server]ダイアログボックスが開きます。

. 1つ以上のsyslogサーバ（最大5つ）の情報を入力し、* Add *をクリックします。
+
** *サーバーアドレス*--完全修飾ドメイン名、IPv4アドレス、または
IPv6アドレスを入力します。
** *UDPポート*-- syslogのUDPポートは通常514です。設定されている
syslogサーバが表に表示されます。

. サーバーアドレスにテストアラートを送信するには、*すべてのSyslogサーバーをテスト
*を選択します。

.結果
アラート対象のイベントが発生すると、イベントモニタからsyslogサーバにアラートが送信されます。監査ログのsyslog設定の詳細については、を参照してください
https://docs.netapp.com/us-en/e-series-santricity/sm-settings/configure-syslog-server-for-audit-logs.html["監査ログ用のsyslogサーバの設定"]。

NOTE: 複数のsyslogサーバが設定されている場合は、設定されているすべての
syslogサーバに監査ログが送信されます。

[[ID2890bd25b9a78caddb90c1179d7584d7]]
= アラート用のsyslogサーバの編集
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
syslogアラートの受信に使用するサーバアドレスを編集できます。

.手順
. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
. *Syslog *タブを選択します。
. 表からsyslogサーバのアドレスを選択し、右端の* Edit
*（鉛筆）アイコンをクリックします。
+

行が編集可能なフィールドになります。

. サーバーアドレスとUDPポート番号を編集し、*保存
*（チェックマーク）アイコンをクリックします。

.結果
更新されたサーバアドレスがテーブルに表示されます。

[[ID45c62186926f0c858d826460b50d321a]]
= アラート用のsyslogサーバの追加
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
syslogアラート用に最大5台のサーバを追加できます。

.開始する前に
*
syslogサーバのアドレスを確認しておく必要があります。このアドレスは、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスのいずれかで指定できます。
* syslogサーバのUDPポート番号を確認しておく必要があります。通常は514です。

.手順
. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
. *Syslog *タブを選択します。
. [Add Syslog Servers]を選択します。
+
[Add Syslog Server]ダイアログボックスが開きます。

. [Add another syslog server*]を選択します。
. syslogサーバの情報を入力し、*Add*をクリックします。
+
** *Syslogサーバ・アドレス*--完全修飾ドメイン名'IPv4アドレス'または
IPv6アドレスを入力します
** *UDPポート*-- syslogのUDPポートは通常514です。

+

NOTE: 最大5台のsyslogサーバを設定できます。

.結果
syslogサーバのアドレスが表に表示されます。

[[ID954ade6765a78a0a7684c65c989b2a3a]]
= アラート用のsyslogサーバの削除
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
syslogサーバを削除してアラートの受信を中止することができます。

.手順
. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
. *Syslog *タブを選択します。
. syslogサーバのアドレスを選択し、右上の「* Remove *」をクリックします。
+
Confirm Delete Syslog Serverダイアログボックスが開きます。

. 操作を確定し、*削除*をクリックします。

.結果
削除したサーバにイベントモニタからアラートが送信されなくなります。

:leveloffset: -1

= FAQ

:leveloffset: +1

[[ID615afaaef4abc0cade1324a19ffb06ea]]
= アラートが無効になっている場合
:allow-uri-read:

```
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
ストレージアレイで発生した重要なイベントに関する通知を管理者が受信できるようにするには、アラート方法を設定する必要があります。

SANtricity System Manager
で管理されるストレージアレイの場合は、アラートページからアラートを設定します。アラート通知は、Eメール、SNMPトラップ、またはsyslogメッセージを使用して送信できます。また、初期セットアップウィザードでEメールアラートを設定することもできます。



[[ID62ed0055ac4fa56c68ccbc7c4d0b8223]]
= SNMPまたはsyslogアラートを設定するにはどうすればよいですか？
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Eメールアラートに加えて、簡易ネットワーク管理プロトコル（SNMP）トラップまたはsyslogメッセージで送信されるようにアラートを設定できます。

SNMPまたはsyslogのアラートを設定するには、メニューの[アラート]に移動します。



[[IDd341ca6e3294370231c1215c5014f7da]]
= アレイとアラートでタイムスタンプが一致しないのはなぜですか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
ストレージアレイは、アラートの送信時に、アラートを受信するターゲットサーバまたはホストのタイムゾーンに合わせて修正しません。代わりに、ローカル時間（GMT）を使用してアラートの記録に使用されるタイムスタンプを作成します。そのため、ストレージアレイのタイムスタンプとアラートを受信するサーバまたはホストのタイムスタンプが一致しないことがあります。
```

ストレージアレイではアラートの送信時にタイムゾーンが修正されないため、アラートのタイムスタンプはGMT相対であり、タイムゾーンオフセットはゼロです。ローカルタイムゾーンに適したタイムスタンプを計算するには、GMTからの時間オフセットを決定し、タイムスタンプからその値を加算または減算する必要があります。

```
:leveloffset: -1


:leveloffset: -1


= アレイ設定

:leveloffset: +1


[[ID43b0859792cbfdf4d2c00e860581f0b8]]
= 設定の概要
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
System Managerでは、一部の一般的なアレイ設定やアドオン機能を設定できます。



== どのような設定を構成できますか？

アレイの設定は次のとおりです。

* xref:{relative_path}cache-settings-and-
performance.html["キャッシュの設定とパフォーマンス"]
* xref:{relative_path}automatic-load-balancing-
overview.html"["自動ロードバランシング"]
* xref:{relative_path}how-add-on-features-work.html["アドオン機能"]
* xref:{relative_path}overview-drive-security.html["ドライブセキュリティ"]




== 関連タスク
```

システム設定に関連するタスクの詳細については、以下を参照してください。

* xref:{relative_path}download-cli.html["コマンドラインインターフェイス（CLI）のダウンロード"]
* xref:{relative_path}create-internal-security-key.html["内部セキュリティキーの作成"]
* xref:{relative_path}create-external-security-key.html["外部セキュリティキーの作成"]
* xref:{relative_path}../sm-hardware/configure-iscsi-ports-hardware.html["iSCSIポートの設定"]
* xref:{relative_path}../sm-hardware/configure-nvme-over-infiniband-ports-hardware.html["NVMe over IBポートの設定"]
* xref:{relative_path}../sm-hardware/configure-nvme-over-roce-ports-hardware.html["NVMe over RoCEポートの設定"]

= 概念

:leveloffset: +1

[[IDa1b4bf2b0c7e98f62b18a102b878e937]]
= キャッシュの設定とパフォーマンス
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
キャッシュメモリは、ドライブメディアよりもアクセス時間が速い、コントローラ上の一時的な揮発性ストレージ領域です。

キャッシュを使用すると、全体的なI/Oパフォーマンスを次のように向上させることができます。

*
読み取り用にホストから要求されたデータは、以前の処理ですでにキャッシュに格納されている可能性があるため、ドライブにアクセスする必要はありません。
*
書き込みデータは最初にキャッシュに書き込まれるため、データがドライブに書き込まれるのを待つことなくアプリケーションが処理を続行できます。

デフォルトのキャッシュ設定はほとんどの環境の要件を満たしていますが、必要に応じて設定を変更できます。

== ストレージアレイキャッシュの設定

ストレージアレイ内のすべてのボリュームについて、[システム]ページで次の値を指定できます。

* *フラッシュの開始値*--
キャッシュフラッシュ（ディスクへの書き込み）をトリガーするキャッシュ内の書き込み前のデータの割合。指定した開始の割合の書き込み前のデータがキャッシュに格納されると、フラッシュがトリガーされます。デフォルトでは、キャッシュが80%フルに達すると、コントローラがキャッシュのフラッシュを開始します。
* *キャッシュブロックサイズ*--
キャッシュ管理の組織単位である各キャッシュブロックの最大サイズ。キャッシュブロックサイズはデフォルトで8KiBですが、4KiB、8KiB、16KiB、32KiBに設定できます。キャッシュブロックサイズは、アプリケーションの主なI/Oサイズに設定するのが理想的です。ファイルシステムやデータベースアプリケーションは一般に小さいサイズを使用しますが、大きいサイズは大規模なデータ転送やシーケンシャルI/Oを必要とするアプリケーションに適しています。

== ボリュームキャッシュの設定

ストレージアレイ内の個々のボリュームについて、Volumes（ボリューム）ページで次の値を指定できます（メニュー：Storage [Volumes]）。

* *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。
+
** *動的キャッシュ読み取りプリフェッチ*--動的キャッシュ読み取りプリフェッチにより
'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'追加のシーケンシャル・データ・ブロックをキャッシュにコピーすることができますこのキャッシュにより、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。ランダムアクセスでは、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。

* *書き込みキャッシュ*--書き込みキャッシュは
'まだドライブに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データは、ドライブに書き込まれるまで書き込みキャッシュに残ります。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。

+
[CAUTION]
====
データ損失の可能性--バッテリなしの書き込みキャッシュ
*オプションを有効にして保護用のユニバーサル電源装置を持たないと、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*バッテリなしの書き込みキャッシュ*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。

====
+
** *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設定により、バッテリがない、故障している、完全に放電されている、またはフル充電されていない場合でも書き込みキャッシュを続行できます。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。
** *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たときに発生しますそのため、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。

[[ID02a1844d0c4e37cbd75a2f9276d08219]]
= 自動ロードバランシングの概要
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
自動ロードバランシングでは、時間の経過に伴う負荷の変化に動的に対応し、ボリュームのコントローラ所有権が自動的に調整されて、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るため、I/Oリソースの管理が強化されます。

各コントローラのワークロードは継続的に監視され、ホストにインストールされたマルチパスドライバとの連携により、必要に応じて自動的に負荷を分散できます。コントローラ間でワークロードが自動的にリバランシングされるため、ストレージアレイの負荷の変化に合わせてボリュームのコントローラ所有権を手動で調整する負担が軽減されます。

自動ロードバランシングを有効にすると、次の機能が実行されます。

* コントローラのリソース使用率を自動的に監視してバランスを調整します。
*
ボリュームのコントローラ所有権が必要に応じて自動的に調整され、ホストとストレージアレイの間のI/O帯域幅が最適化されます。

== 自動ロードバランシングの有効化と無効化

自動ロードバランシングは、すべてのストレージアレイでデフォルトで有効になっています。

自動ロードバランシングは、次のような理由でストレージアレイで無効にすることができます。

*
特定のボリュームのコントローラ所有権を自動的に変更してワークロードを分散させたくない場合
*
高度に調整された環境で、コントローラ間の負荷分散が特定の要件を満たすように意図的に設定されている。

== 自動ロードバランシング機能をサポートするホストタイプ

自動ロードバランシングはストレージアレイレベルで有効になっていますが、ホストまたはホストクラスタに対して選択するホストタイプは機能の動作に直接影響します。

ストレージアレイのワークロードをコントローラ間で分散する場合、自動ロードバランシング機能は、両方のコントローラからアクセス可能で、自動ロードバランシング機能に対応したホストまたはホストクラスタにのみマッピングされたボリュームの移動を試みます。

これにより、ロードバランシングプロセスが原因でホストがボリュームにアクセスできなくなるのを防ぐことができます。ただし、自動ロードバランシングをサポートしていないホストにマッピングされたボリュームがあると、ストレージアレイのワークロードを分散できなくなります。自動ロードバランシングでワークロードを分散するには、マルチパスドライバがTPGSをサポートし、ホストタイプが次の表に含まれている必要があります。

[NOTE]
====
ホストクラスタが自動ロードバランシングに対応しているとみなされるには、そのグループ内のすべてのホストが自動ロードバランシングをサポートしている必要があります。

====
[cols="1a,1a"]
|===
| 自動ロードバランシングをサポートするホストタイプ | マルチパスドライバ

```
 a|
WindowsまたはWindowsクラスタ
 a|
MPIOとNetApp EシリーズDSM



 a|
Linux DM-MP（カーネル3.10以降）
 a|
DM-MPと `scsi_dh_alua`デバイスハンドラ



 a|
VMware
 a|
Native Multipathing Plugin（NMP）と `VMW_SATP_ALUA Storage Array
Type`プラグイン

|===
[NOTE]
====
一部の例外を除き、自動ロードバランシング機能が有効になっているかどうかに関係なく、自動ロードバランシングをサポートしないホストタイプは引き続き正常に動作します。例外の1つは、システムでフェイルオーバーが発生した場合、データパスが戻った時点で、マッピングされていないボリュームまたは割り当てられていないボリュームがストレージアレイによって所有権を持つコントローラに戻されます。自動ロードバランシング以外のホストにマッピングまたは割り当てられているボリュームは移動されません。

====
特定のマルチパスドライバ、OSレベル、およびコントローラドライブトレイのサポートに関する互換性情報については、を参照してください
https://mysupport.netapp.com/matrix["Interoperability Matrix Tool"^]。



== 自動ロードバランシング機能とOSの互換性の確認

新しいシステムをセットアップ（または既存のシステムを移行）する前に、自動ロードバランシング機能とOSの互換性を確認してください。

. にアクセスし https://mysupport.netapp.com/matrix["Interoperability Matrix Tool"^]てソリューションを検索し、サポートを確認します。
+
```

システムでRed Hat Enterprise Linux 6またはSUSE Linux Enterprise Server 11を実行している場合は、テクニカルサポートにお問い合わせください。

. を更新して設定し `/etc/multipath.conf file`ます。
. 該当するベンダーと製品に対してとの `detect_prio`両方がに設定されている `yes`ことを確認する `retain_attached_device_handler`か、デフォルト設定を使用します。

:leveloffset: -1

= アレイの設定

:leveloffset: +1

[[IDfa2b304ed13d110cc2c866a336c04678]]
= ストレージアレイ名の編集
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SANtricity System Managerのタイトルバーに表示されるストレージアレイ名を変更することができます。

.手順
. メニューを選択します。[設定][システム]。
. [*General]で[*Name:*]フィールドを探します。
+
ストレージアレイ名が定義されていない場合、このフィールドには「不明」と表示されます。

. ストレージアレイ名の横にある* Edit *（鉛筆）アイコンをクリックします。
+
フィールドが編集可能になります。

. 新しい名前を入力します。
+
名前には、アルファベット、数字、アンダースコア（_）、ダッシュ（-）、ハッシュ記号（#）を使用できます。スペースを含めることはできません。名前の最大文字数は30文字です。名前は一意である必要があります。

. [*保存*（Save *）]（チェックマーク）アイコンをクリックします。
+
[NOTE]
====
変更せずに編集可能なフィールドを閉じるには、*キャンセル*（X）アイコンをクリックします。

====

.結果
新しい名前がSANtricity System Managerのタイトルバーに表示されます。

[[IDdfc8ff3d41a6a1710f8bd1cb899b760c]]
= ストレージアレイのロケーターライトの点灯
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
キャビネット内のストレージアレイの物理的な場所を確認するには、ストレージアレイのロケータ（LED）ライトを点灯します。

.手順
. メニューを選択します。[設定][システム]。
. [*General]で、[*Turn on Storage Array Locator Lights]をクリックします。
+
ストレージアレイのロケーターライトを点灯ダイアログボックスが開き、対応するストレージアレイのロケーターライトが点灯します。

. ストレージアレイが物理的に配置されている場合は、ダイアログボックスに戻り、*電源オフ*を選択します。

.結果
ロケーターライトが消灯し、ダイアログボックスが閉じます。

[[IDd441232a4737e2a358e2086006df551c]]
= ストレージアレイのクロックの同期
:allow-uri-read:

```
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
ネットワークタイムプロトコル（NTP）が有効になっていない場合は、コントローラのクロックを手動で設定して、管理クライアント（System
Managerにアクセスするブラウザの実行に使用されるシステム）と同期されるようにすることができます。

.タスクの内容
同期により、イベントログ内のイベントタイムスタンプがホストログファイルに書き込まれたタイムスタンプと一致するようになります。同期プロセス中も、コントローラは引き続き使用可能で動作します。

[NOTE]
====
System Managerで
NTPが有効になっている場合は、このオプションを使用してクロックを同期しないでください。代わりに、NTPはSNTP（Simple Network Time
Protocol）を使用してクロックを外部ホストと自動的に同期します。

====
[NOTE]
====
同期後に、パフォーマンス統計が失われたり歪んだりしたり、スケジュールが影響を受けたり（ASUP、Snapshotなど）、ログデータのタイムスタンプが歪んだりすることがあります。NTPを使用すると、この問題を回避できます。

====
.手順
. メニューを選択します。[設定][システム]。
. [*General]で'[*ストレージ・アレイ・クロックの同期化*]をクリックします
+
[ストレージアレイクロックの同期]ダイアログボックスが開きます。コントローラと管理クライアントとして使用されているコンピュータの現在の日時が表示されます。

+
[NOTE]
====
シンプレックスストレージアレイの場合は、1台のコントローラのみが表示されます。

====
. ダイアログボックスに表示された時間が一致しない場合は、*同期化*をクリックします。
```

.結果
同期が成功すると、イベントのタイムスタンプはイベントログとホストログで同じになります。

[[ID0abcd6dc2e7d0366e97dd5aa72333e17]]
= ストレージアレイの構成の保存
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ストレージアレイの構成情報をスクリプトファイルに保存すると、追加のストレージアレイをセットアップする際に同じ構成を使用するための時間を節約できます。

.開始する前に
論理構成の設定を変更する処理がストレージアレイで行われていないことを確認してください。このような処理の例としては、ボリュームの作成または削除、コントローラファームウェアのダウンロード、ホットスペアドライブの割り当てまたは変更、ボリュームグループへの容量（ドライブ）の追加などがあります。

.タスクの内容
ストレージアレイの構成を保存すると、ストレージアレイの設定、ボリュームの構成、ホストの構成、またはストレージアレイに対するホストとボリュームの割り当てを含むコマンドラインインターフェイス（CLI）スクリプトが生成されます。生成されたこのCLIスクリプトを使用して、ハードウェア構成がまったく同じ別のストレージアレイに構成をレプリケートできます。

ただし、ディザスタリカバリにはこのCLIスクリプトを使用しないでください。システムをリストアするには、代わりに、手動で作成する構成データベースのバックアップファイルを使用するか、テクニカルサポートに問い合わせて最新のAutoSupportデータからこのデータを取得してください。

この操作では、次の設定は保存されません。

* バッテリーの寿命
* コントローラの時刻
* Nonvolatile Static Random Access Memory（
NVSRAM；不揮発性静的ランダムアクセスメモリ）の設定
* すべてのプレミアム機能
* ストレージアレイのパスワード
* ハードウェアコンポーネントの動作ステータスと状態
* ボリュームグループの動作ステータス（最適を除く）と状態
* ミラーリングやボリュームコピーなどのコピーサービス

[CAUTION]
====
アプリケーションエラーのリスク-
論理構成の設定を変更する処理をストレージアレイで実行中の場合は、このオプションを使用しないでください。このような処理の例としては、ボリュームの作成または削除、コントローラファームウェアのダウンロード、ホットスペアドライブの割り当てまたは変更、ボリュームグループへの容量（ドライブ）の追加などがあります。

====
.手順
. メニューを選択します。[設定][システム]。
. 「ストレージアレイ構成の保存」を選択します。
. 保存する構成の項目を選択します。
+
** ストレージアレイの設定
** ボリューム構成
** ホストの設定
** ホスト/ボリューム間の割り当て

+
[NOTE]
====
［*ホスト/ボリューム間の割り当て*］項目を選択した場合、［*ボリューム構成*］項目と［*ホスト構成*］項目もデフォルトで選択されます。「ホスト/ボリューム間の割り当て」は、「ボリューム構成」と「ホスト構成」も保存しないと保存できません。

====
. [保存（ Save ）] をクリックします。
+
ブラウザのDownloadsフォルダにという名前でファイルが保存されます `storage-array-configuration.cfg`。

.終了後
保存したストレージアレイの構成を別のストレージアレイにロードするには、SANtricityコマンドラインインターフェイス（SMcli）でオプションを指定して `-f`ファイルを適用し `.cfg`ます。

[NOTE]
====
Unified
Managerインターフェイスを使用して、ストレージアレイの構成を他のストレージアレイにロードすることもできます（選択メニュー：管理[設定のインポート]）。

====

[[ID062d144d8529c4b81d5eb377fc0ce15e]]
= ストレージアレイ構成のクリア
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ストレージアレイからすべてのプール、ボリュームグループ、ボリューム、ホスト定義、およびホスト割り当てを削除する場合は、構成のクリア処理を使用します。

.開始する前に
ストレージアレイ構成をクリアする前に、データをバックアップしてください。

.タスクの内容
ストレージアレイ構成のクリアには2つのオプションがあります。

* *ボリューム*--
通常、テスト用ストレージアレイを本番ストレージアレイとして再構成するために、ボリュームオプションを使用します。たとえば、テスト用にストレージアレイを構成し、テストが完了したらテスト構成を削除して、本番環境用にストレージアレイをセットアップすることができます。
* *ストレージ・アレイ*--通常'ストレージ・アレイを別の部門またはグループに移動するには'ストレージ・アレイ・オプションを使用しますたとえば、エンジニアリング部門でストレージアレイを使用していて、エンジニアリング部門が新しいストレージアレイを入手したために、現在のストレージアレイを再設定する管理部門に移動するとします。
+
[ストレージアレイ]オプションでは、いくつかの追加設定が削除されます。

[cols="1a,1a,1a"]
|===
| | ボリューム | ストレージアレイ

 a|
ARVMを非アクティブ化
 a|
X
 a|
X

a|
プールとボリュームグループを削除
a|
X
a|
X

a|
ボリュームを削除
a|
X
a|
X

a|
ホストとホストクラスタを削除
a|
X
a|
X

a|
ホスト割り当てを削除
a|
X
a|
X

a|
ストレージアレイ名を削除
a|
a|
X

a|

ストレージアレイのキャッシュ設定をデフォルトにリセット
 a|
 a|
X

|===
[CAUTION]
====
データ損失のリスク-
この処理を実行すると、ストレージアレイからすべてのデータが削除されます。（完全消去は実行されません）。この処理は開始後にキャンセルすることはできません。この処理は、テクニカルサポートから指示があった場合にのみ実行してください。

====
.手順
. メニューを選択します。[設定][システム]。
. 「ストレージアレイ構成のクリア」を選択します。
. ドロップダウンリストで、* Volume *または* Storage Array *のいずれかを選択します。
. *オプション：
*（データではなく）設定を保存する場合は、ダイアログボックス内のリンクを使用します。
. 処理を確定します。

.結果
* 現在の構成が削除され、ストレージアレイ上の既存のデータがすべて削除されます。
* すべてのドライブの割り当てが解除されます。

[[ID99434937861144417d2301384ece5cad5]]
= ストレージアレイのキャッシュ設定の変更
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ストレージアレイ内のすべてのボリュームについて、フラッシュとブロックサイズのキャッシュメモリ設定を調整できます。

.タスクの内容
キャッシュメモリはコントローラ上の一時的な揮発性ストレージの領域であり、ドライブメディアよりもアクセス時間が速くなります。キャッシュパフォーマンスを調整するには、次の設定を調整します。

[cols="25h,~"]
|===
| キャッシュ設定 | 製品説明

a|
デマンドキャッシュフラッシュの開始
a|
キャッシュに格納された書き込み前のデータが何パーセントに達したらキャッシュフラッシュ（ディスクへの書き込み）を開始するかを指定します。デフォルトでは、書き込み前のデータが容量の80%に達するとキャッシュフラッシュが開始されます。書き込み処理が中心の環境では、この割合を高くすると、新しい書き込み要求をディスクにアクセスせずにキャッシュで処理できるため便利です。I/Oが不規則でデータのバーストがある環境では、この割合を低くして、バーストとバーストの間に頻繁にキャッシュがフラッシュされるようにすると効果的です。ただし、開始パーセンテージが80%未満の場合は、パフォーマンスが低下する可能性があります。

a|
キャッシュブロックサイズ
a|
キャッシュブロックサイズは、各キャッシュブロックの最大サイズであり、キャッシュを管理する際の単位となります。デフォルトのブロックサイズは32KiBです。キャッシュブロックサイズは、4KiB、8KiB、16KiB、32KiBのいずれかです。使用するブロックサイズはアプリケーションによって異なり、ストレージのパフォーマンスに影響します。ファイルシステムやデータベースアプリケーションには、サイズを小さくすることをお勧めします。マルチメディアなどのシーケンシャルI/Oを生成するアプリケーションには、大きいサイズが適しています。

|===
.手順
. メニューを選択します。[設定][システム]。
. 下にスクロールして「その他の設定」を選択し、「キャッシュ設定の変更」をクリックします。
+
[キャッシュ設定の変更]ダイアログボックスが開きます。

. 次の値を調整します。
+
** *デマンド・キャッシュ・フラッシュを開始*--ご使用の環境で使用されるI/Oに適した割合を選択します80%未満の値を選択すると、パフォーマンスが低下することがあります。
** **キャッシュブロックサイズ--**アプリケーションに適したサイズを選択してください。

. [保存（ Save ）] をクリックします。

[[ID4496bceb7c61ee9339080277c79e9859]]
= 自動ロードバランシングの設定
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
自動ロードバランシング機能を使用すると、ホストからの受信I/Oトラフィックが動的に管理され、両方のコントローラに分散されます。この機能はデフォルトで有効になっていますが、System Managerから無効にすることもできます。

.タスクの内容
自動ロードバランシングを有効にすると、次の機能が実行されます。

* コントローラのリソース使用率を自動的に監視してバランスを調整します。
*
ボリュームのコントローラ所有権が必要に応じて自動的に調整され、ホストとストレージアレイの間のI/O帯域幅が最適化されます。

自動ロードバランシングは、次のような理由でストレージアレイで無効にすることができます。

*
特定のボリュームのコントローラ所有権を自動的に変更してワークロードを分散させたくない場合
*
高度に調整された環境で、コントローラ間の負荷分散が特定の要件を満たすように意図的に設定されている。

.手順
. メニューを選択します。[設定][システム]。
. 下にスクロールして「その他の設定」を選択し、「*自動ロードバランシングの有効化/無効化*」をクリックします。
+
この機能が現在有効か無効かを示すテキストがこのオプションの下に表示されます。

+
確認のダイアログボックスが開きます。

. 続行するには、[はい]をクリックして確定します。
+
このオプションを選択すると、機能の有効と無効を切り替えることができます。

```
+
[NOTE]
====
この機能を無効から有効に切り替えると、ホスト接続レポート機能も自動的に有効になります。

====




[[ID5c2115253f288a2a7a7fb901fc60b0a5]]
= 従来の管理インターフェイスの有効化または無効化
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
ストレージアレイと管理クライアントの間の通信方法である従来の管理インターフェイス（SYMbol）を有効または無効にすることができます。

.タスクの内容
デフォルトでは、従来の管理インターフェイスは有効になっています。無効にすると、ストレージアレイと管理クライアントはよりセキュアな通信方法（HTTPS経由のREST
API）を使用しますが、無効にすると特定のツールやタスクに影響する可能性があります。

[NOTE]
====
EF600ストレージシステムでは、この機能はデフォルトで無効になっています。

====
この設定は処理に次のように影響します。

* * on *（デフォルト）-- CLIや
OCIアダプタなどのその他のツールを使用してミラーリングを設定する場合に必要な設定です。
* *オフ*--
ストレージアレイと管理クライアント間の通信の機密性を強化し、外部ツールにアクセスするために必要な設定です。ディレクトリサーバ（LDAP）を設定する際に推奨される設定です。


.手順
. メニューを選択します。[設定][システム]。
. 下にスクロールして「その他の設定」を選択し、「
*管理インターフェイスの変更」をクリックします。
```

. ダイアログボックスで、*はい*をクリックして続行します。

:leveloffset: -1

= アドオン機能の設定

:leveloffset: +1

[[ID76a0a0dd584b2cfddc72ca7bb038fdda]]
= アドオン機能の仕組み
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アドオンはSystem Managerの標準構成には含まれていない機能であり、有効にするにはキーが必要になる場合があります。アドオン機能には、単一のプレミアム機能と、バンドルされた機能パックがあります。

次に、プレミアム機能または機能パックを有効にする手順の概要を示します。

. 次の情報を入手します。
+
**
シャーシのシリアル番号と機能有効識別子。機能をインストールするストレージアレイを識別します。これらの項目はSystem Managerで使用できます。
** Feature Activation Code。機能の購入時にサポートサイトから入手できます。

. ストレージプロバイダに問い合わせるか、Premium Feature Activationサイトにアクセスして機能キーを取得します。アクティブ化するシャーシのシリアル番号、イネーブルID、および機能コードを入力します。
. System Managerで、機能キーファイルを使用してプレミアム機能または機能パックを有効にします。

[[IDe06a785042682ab73f25d07582a16f61]]
= アドオン機能に関する用語

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


[role="lead"]
ストレージアレイに関連するアドオン機能の用語を次に示します。

[cols="25h,~"]
|===
| 期間 | 製品説明


 a|
機能有効識別子
 a|
機能有効識別子は、特定のストレージアレイを識別する一意の文字列です。この識別子により、プレミアム機能を取得した時点でそのストレージアレイのみに関連付けられるようになります。この文字列は、[システム]ページの[アドオン]に表示されます。



 a|
キノウキイフアイル
 a|
機能キーファイルは、プレミアム機能または機能パックのロックを解除して有効にするためのファイルです。



 a|
機能パック
 a|
機能パックは、ストレージアレイの属性を変更する（プロトコルをFibre ChannelからiSCSIに変更するなど）バンドルです。機能パックを有効にするには特別なキーが必要です。



 a|
プレミアム機能
 a|
プレミアム機能は追加オプションであり、有効にするにはキーが必要です。標準構成のSystem Managerには含まれていません。

|===
```

```
[[ID26962a220429ec65669fd5616bc932fa]]
= 機能キーファイルの取得
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
ストレージアレイでプレミアム機能または機能パックを有効にするには、まず機能キーファイルを取得する必要があります。キーは1つのストレージアレイにのみ関連付けられます。

.タスクの内容
このタスクでは、機能に必要な情報を収集し、機能キーファイルの要求を送信する方法について説明します。必要な情報は次のとおりです。

* シャーシのシリアル番号
* 機能有効識別子
* 機能のアクティブ化コード


.手順
. System Managerで、シャーシのシリアル番号を確認して記録します。このシリアル番号は、[サポートセンター]タイルの上にマウスを置くと表示されます。
. System Managerで、機能有効識別子を確認します。[設定]、[システム
]の順に移動し、下にスクロールして*アドオン*を表示します。機能有効識別子*を探します。機能有効識別子の番号を記録します。
.
機能を有効にするためのコードを見つけて記録します。機能パックの場合、このコードは変換の実行手順に記載されています。
+
NetAppの手順については、を参照して https://www.netapp.com/support-and-training/documentation/eseries-santricity/["NetApp
Eシリーズシステムのドキュメントセンター"^]ください。

+
プレミアム機能の場合は、サポートサイトから次の手順でアクティベーションコードにアクセスできます。

+
.. にログインし
https://mysupport.netapp.com/site/global/dashboard["NetAppのサポート"^]ます。
.. お使いの製品の「*ソフトウェアライセンス*」にアクセスします。
.. ストレージアレイシャーシのシリアル番号を入力し、* Go *をクリックします。
```

.. [*License Key*]列で、Feature Activation Codeを探します。
.. 必要な機能のFeature Activation Codeを記録します。

.
機能キーファイルをリクエストするには、シャーシのシリアル番号、有効識別子、機能のアクティブ化のコードを記載したEメールまたはテキストドキュメントをストレージサプライヤに送信してください。
+
に移動して必要な情報を入力し、機能パックまたは機能パックを入手することもできます http://partnerspfk.netapp.com["ネットアップライセンスのアクティブ化：ストレージアレイプレミアム機能のアクティブ化"^]。（このサイトの手順はプレミアム機能用であり、機能パック用ではありません）。

.終了後
機能キーファイルがある場合は、プレミアム機能または機能パックを有効にすることができます。

[[ID8cfbc75c4c91c9d14ac9d1bf093a32b7]]
= プレミアム機能を有効にする
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
プレミアム機能は追加オプションであり、有効にするにはキーが必要です。

.開始する前に
*
機能キーを入手しておきます。キーについては、必要に応じてテクニカルサポートにお問い合わせください。
* 管理クライアント（System
Managerにアクセスするためのブラウザを備えたシステム）上にキーファイルをロードしておきます。

.タスクの内容
このタスクでは、System
Managerを使用してプレミアム機能を有効にする方法について説明します。

[NOTE]

====
プレミアム機能を無効にする場合は(`disable storageArray) (featurePack | feature=featureAttributeList`、コマンドラインインターフェイス（CLI）でDisable Storage Array Featureコマンドを使用する必要があります。

====
.手順
. メニューを選択します。[設定][システム]。
. 「*アドオン*」で、「*プレミアム機能を有効にする*」を選択します。
+
[プレミアム機能の有効化]ダイアログボックスが開きます。

. [*Browse*](参照)をクリックし、キーファイルを選択します。
+
ファイル名がダイアログボックスに表示されます。

. [*Enable*] をクリックします。

[[ID4c80595fbbfc06c307c7123237359941]]
= 機能パックの有効化
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
機能パックは、ストレージアレイの属性を変更する（プロトコルをFibre ChannelからiSCSIに変更するなど）バンドルです。機能パックを有効にするには特別なキーが必要です。

.開始する前に
*
ストレージアレイの新しい属性の変換と準備について説明した適切な手順に従います。ホストプロトコルの変換手順については、コントローラモデルのハードウェアメンテナンスガイドを参照してください。
*
ストレージアレイがオフラインであるため、ホストやアプリケーションがアクセスしていません。
* すべてのデータがバックアップされます。
* 機能パックファイルを入手しておきます。
+
機能パックファイルは管理クライアント（System Managerにアクセスするためのブラウザを備えたシステム）上にロードされます。

[NOTE]
====
ダウンタイムのメンテナンス時間をスケジュールし、ホストとコントローラの間のI/O処理をすべて停止する必要があります。また、変換が完了するまではストレージアレイのデータにアクセスできないことに注意してください。

====
.タスクの内容
このタスクでは、System Managerを使用して機能パックを有効にする方法について説明します。完了したら、ストレージアレイを再起動する必要があります。

.手順
. メニューを選択します。[設定][システム]。
. [* アドオン *] で、 [* 機能パックの変更 *] を選択します。
. [*Browse*](参照)をクリックし、キーファイルを選択します。
+
ファイル名がダイアログボックスに表示されます。

. フィールドにと入力し `change`ます。
. [変更（ Change ）] をクリックします。
+
機能パックの移行が開始され、コントローラがリブートします。書き込み前のキャッシュデータが削除されるため、I/Oアクティビティが発生しません。両方のコントローラが自動的にリブートし、新しい機能パックが有効になります。リブートが完了すると、ストレージアレイは応答可能な状態に戻ります。

:leveloffset: -1

[[IDdd34a9417d13ee97ccea2218dc52eca3]]
= コマンドラインインターフェイス（CLI）のダウンロード
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
System Managerからコマンドラインインターフェイス（

CLI）パッケージをダウンロードできます。

CLIでは、テキストベースの方法でストレージアレイを設定および監視できます。HTTPS経由で通信し、外部にインストールされた管理ソフトウェアパッケージに含まれるCLIと同じ構文を使用します。CLIをダウンロードするためにキーは必要ありません。

.開始する前に
CLIコマンドを実行する管理システムに、Java Runtime Environment（JRE）バージョン8以降がインストールされている必要があります。

.手順
. メニューを選択します。[設定][システム]。
. [*アドオン*（* Add-ons *）]で、[*コマンドラインインターフェイス*（* Command Line Interface）]を選択
+
ZIPパッケージがブラウザにダウンロードされます。

. ストレージアレイに対してCLIコマンドを実行する管理システムに
ZIPファイルを保存し、ファイルを展開します。
+
DOS C:プロンプトなどのオペレーティングシステムのプロンプトから
CLIコマンドを実行できるようになりました。CLIコマンドリファレンスは、System Managerユーザインターフェイスの右上にあるヘルプメニューから入手できます。

= FAQ

:leveloffset: +1

[[ID5a657a23181c837cb92fcfe69017a308]]
= 自動ロードバランシングとは
:allow-uri-read:
:icons: font
:relative_path: ./sm-storage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
自動ロードバランシング機能は、I/Oを自動で分散し、ホストからの受信I/Oトラフィックを動的に管理して両方のコントローラに分散します。

自動ロードバランシング機能を使用すると、負荷の変化に動的に対応してボリュームのコントローラ所有権が自動的に調整されるため、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、I/Oリソースの管理が強化されます。

各コントローラのワークロードは継続的に監視され、ホストにインストールされたマルチパスドライバとの連携により、必要に応じて自動的に負荷を分散できます。コントローラ間でワークロードが自動的にリバランシングされるため、ストレージアレイの負荷の変化に合わせてボリュームのコントローラ所有権を手動で調整する負担が軽減されます。

自動ロードバランシングを有効にすると、次の機能が実行されます。

* コントローラのリソース使用率を自動的に監視してバランスを調整します。
*
ボリュームのコントローラ所有権が必要に応じて自動的に調整され、ホストとストレージアレイの間のI/O帯域幅が最適化されます。

[NOTE]
====
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転送の対象になりません。

====

[[IDeb9055e44843a0fb7e3a44b1bfd100fb]]
= コントローラキャッシュとは何ですか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
コントローラキャッシュは、コントローラとホスト間、およびコントローラとディスク間の2種類のI/O（入出力）処理を合理化する物理メモリスペースです。

読み取りおよび書き込みのデータ転送では、ホストとコントローラは高速な接続を介して通信します。ただし、ディスクは比較的低速なデバイスであるため、コントローラのバックエンドからディスクへの通信は低速です。

コントローラキャッシュがデータを受信すると、コントローラはデータを保持していることをホストアプリケーションに確認応答します。これにより、ホストアプリケーションはI/Oがディスクに書き込まれるのを待つ必要がなくなります。代わりに、アプリケーションは処理を続行できます。また、キャッシュされたデータにサーバアプリケーションから簡単にアクセスできるため、データにアクセスするためにディスクを読み取る必要がありません。

コントローラキャッシュは、ストレージアレイの全体的なパフォーマンスにいくつかの点で影響します。

*
キャッシュはバッファとして機能するため、ホストとディスクのデータ転送を同期する必要がありません。
*
ホストからの読み取りまたは書き込み処理のデータは、以前の処理でキャッシュに格納されている場合があるため、ディスクにアクセスする必要はありません。
*
書き込みキャッシュを使用している場合、ホストは以前の書き込み処理がディスクに書き込まれる前に後続の書き込みコマンドを送信できます。
*
キャッシュプリフェッチを有効にすると、シーケンシャルリードアクセスが最適化されます。読み取り処理ではデータがディスクから読み取られるのではなく、キャッシュ内のデータが使用される可能性が高くなります。

[CAUTION]
====
データ損失の可能性--バッテリなしの書き込みキャッシュ
*オプションを有効にして保護用のユニバーサル電源装置を持たないと、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*バッテリなしの書き込みキャッシュ*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。

====

[[ID4056553f366e783423db5eec361064e2]]
= キャッシュフラッシュとは何ですか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
キャッシュ内の書き込み前のデータの量が一定のレベルに達すると、コントローラはキャッシュされたデータを定期的にドライブに書き込みます。この書き込みプロセスは「フラッシュ」と呼ばれます。

コントローラは、デマンドベースと経過時間ベースの2つのアルゴリズムを使用してキャッシュをフラッシュします。キャッシュされたデータの量がキャッシュフラッシュしきい値を下回るまで、コントローラはデマンドベースのアルゴリズムを使用します。デフォルトでは、キャッシュの80%が使用中になるとフラッシュが開始されます。

System
Managerでは、「デマンド・キャッシュ・フラッシュの開始」しきい値を、環境で使用されるI/O

のタイプに最も適した値に設定できます。書き込み操作が主な環境では'新しい書き込み要求をディスクに移動せずにキャッシュで処理できる可能性を高めるために'デマンド・キャッシュ・フラッシュの開始パーセントを高く設定する必要があります割合を高く設定すると、キャッシュフラッシュの回数が制限され、キャッシュに残っているデータが増えるため、キャッシュヒット率が高くなります。

I/Oが不安定な（データバーストが発生する）環境では、キャッシュフラッシュを低くすることで、データバースト間でキャッシュが頻繁にフラッシュされるようにすることができます。さまざまな負荷を処理する多様なI/O環境や、負荷のタイプが不明な環境では、このしきい値を中間の50%に設定します。80%未満に設定した場合、ホスト読み取りに必要なデータがキャッシュにないためにパフォーマンスが低下する可能性があります。割合を低くすると、キャッシュレベルを維持するために必要なディスク書き込みの数も増加し、システムオーバーヘッドが増加します。

経過時間ベースのアルゴリズムでは、書き込みデータがディスクにフラッシュされるまでのキャッシュでの保持期間を指定します。キャッシュフラッシュしきい値に達するまで、経過時間ベースのアルゴリズムが使用されます。デフォルトは10秒ですが、この期間は非アクティブな期間にのみカウントされます。System
Managerではフラッシュのタイミングを変更できません。代わりに、コマンドラインインターフェイス（CLI）で* Set Storage Array *コマンドを使用する必要があります。

[CAUTION]
====
データ損失の可能性--バッテリなしの書き込みキャッシュ
*オプションを有効にして保護用のユニバーサル電源装置を持たないと、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*バッテリなしの書き込みキャッシュ*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。

====

[[ID15d2c344494a5cb1d4f499503738d0ea]]
= キャッシュブロックサイズとは何ですか。
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ストレージアレイのコントローラはキャッシュを複数の「ブロック」に編成します。ブロックは、サイズが8、16、32KiBのメモリチャンクです。ストレージシステム上のすべてのボリュームは同じキャッシュスペースを共有するため、ボリュームで使用できるキャッシュブロックサイズは1つだけです。

使用するブロックサイズはアプリケーションによって異なり、ストレージのパフォーマンスに影響する可能性があります。System Managerのデフォルトのブロックサイズは32KiBですが、8KiB

、16KiB、または32KiBに設定できます。ファイルシステムやデータベースアプリケーションには、サイズを小さくすることをお勧めします。大規模なデータ転送、シーケンシャルI/O、または高帯域幅を必要とするアプリケーション（マルチメディアなど）には、サイズを大きくすることをお勧めします。

[[IDcd44e78b2b2e8b4a9991fa38a06294f1]]
= ストレージアレイのクロックを同期する必要があるのはどのような場合ですか。
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
System Managerに表示されるタイムスタンプが管理クライアント（ブラウザからSystem Managerにアクセスしているコンピュータ）に表示されるタイムスタンプと一致していない場合は、ストレージアレイのコントローラクロックを手動で同期する必要があります。このタスクを実行する必要があるのは、System Managerで
NTP（ネットワークタイムプロトコル）が有効になっていない場合だけです。

[NOTE]
====
クロックを手動で同期する代わりに、NTPサーバを使用することを強く推奨します。NTPは、SNTP（Simple Network Time Protocol）を使用して自動的にクロックを外部サーバと同期します。

====
同期ステータスは、[システム]ページからアクセスできる[ストレージアレイクロックの同期]ダイアログボックスで確認できます。ダイアログボックスに表示される時刻が一致しない場合は、同期を実行します。このダイアログボックスを定期的に表示して、コントローラクロックの時刻表示がずれて同期されていないかどうかを確認できます。

:leveloffset: -1

:leveloffset: -1

= ドライブセキュリティ

:leveloffset: +1

[[IDe9af8a7ffb44e917da0476641e72d783]]

= ドライブセキュリティの概要
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
[セキュリティキー管理]ページで、ドライブセキュリティとキー管理を設定できます。

== ドライブセキュリティとは

_Drive Security_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。FDEドライブまたはFIPSドライブをアレイから物理的に取り外した場合は、別のアレイに取り付けるまで動作できません。別のアレイに取り付けると、正しいセキュリティキーを指定するまでドライブはセキュリティロック状態になります。a_security key_は、ストレージアレイ内のこれらのタイプのドライブおよびコントローラで共有される文字列です。

詳細：

* xref:{relative_path}how-the-drive-security-feature-works.html["ドライブセキュリティ機能の仕組み"]
* xref:{relative_path}how-security-key-management-works.html["セキュリティキー管理の仕組み"]
* xref:{relative_path}drive-security-terminology.html["ドライブセキュリティの用語"]

== キー管理の設定方法

ドライブセキュリティを実装するには、アレイにFDEドライブまたはFIPSドライブを取り付ける必要があります。これらのドライブのキー管理を設定するには、メニューから次のいずれかを選択します。Settings [System > Security key management]コントローラの永続的メモリから内部キーを作成するか、キー管理サーバから外部キーを作成できます。最後に、ボリューム設定で[セキュリティ対応]を選択して、プールおよび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ます。

詳細：

```
* xref:{relative_path}create-internal-security-
key.html["内部セキュリティキーの作成"]
* xref:{relative_path}create-external-security-
key.html["外部セキュリティキーの作成"]
* xref:{relative_path}../sm-storage/create-pool-
manually.html["プールの手動作成"]
* xref:{relative_path}../sm-storage/create-volume-
group.html["ボリュームグループの作成"]
```

== ドライブのロックを解除する方法を教えてください。

キー管理を設定したあとにセキュリティ有効ドライブをストレージアレイ間で移動した場合、ドライブ上の暗号化データにアクセスできるようにするには、セキュリティキーを新しいストレージアレイに再割り当てする必要があります。

詳細：

```
* xref:{relative_path}unlock-drives-using-an-internal-security-
key.html["内部キー管理の使用時のドライブのロック解除"]
* xref:{relative_path}unlock-drives-using-an-external-security-
key.html["外部キー管理の使用時のドライブのロック解除"]
```

== 関連情報

キー管理に関連するタスクの詳細については、以下を参照してください。

```
* xref:{relative_path}use-ca-signed-certificates-for-authentication-with-
a-key-management-server.html["キー管理サーバでの認証にCA署名証明書を使用する"]
* xref:{relative_path}back-up-security-key.html["
セキュリティキーのバックアップ"]
```

= 概念

```
:leveloffset: +1

[[ID6696c09e2abbca1e22f58cf4f2acde3f]]
```

= ドライブセキュリティ機能の仕組み
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ドライブセキュリティは、 Full Disk Encryption （ FDE ）ドライブまたは連邦情報処理標準（ FIPS ）ドライブを使用してセキュリティを強化するストレージアレイの機能です。

これらのドライブをドライブセキュリティ機能と組み合わせて使用すると、データにアクセスするためのセキュリティキーが必要になります。ドライブをアレイから物理的に取り外した場合、別のアレイに取り付けるまでドライブは動作しません。別のアレイに取り付けると、正しいセキュリティキーを指定するまでセキュリティロック状態になります。

== ドライブセキュリティの実装方法

ドライブセキュリティを実装するには、次の手順を実行します。

. ストレージアレイにセキュリティ対応のFDEドライブまたはFIPSドライブを取り付けます（FIPSのサポートが必要なドライブには、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のみのボリュームグループまたはプールで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）。
. セキュリティキーを作成します。セキュリティキーは、読み取り/書き込みアクセス用にコントローラとドライブで共有される文字列です。コントローラの永続的メモリから内部キーを作成するか、キー管理サーバから外部キーを作成できます。外部キー管理の場合は、キー管理サーバとの間で認証を確立する必要があります。
. プールおよびボリュームグループに対してドライブ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を作成します（受験者テーブルの「Secure Capable *」列で「* Yes」を検索してください）。
** 新しいボリュームを作成するときにプールまたはボリュームグループを選択します（Pool and volume group Candidatesテーブルで、「* SecureCapable *」の横の「* Yes」*を探します）。

== ドライブレベルでのドライブセキュリティの動作

セキュリティ対応ドライブであるFDEまたはFIPSでは、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。この暗号化と復号化は、パフォーマンスやユーザのワークフローには影響しません。各ドライブには固有の暗号化キーがあり、ドライブから転送することはできません。

ドライブセキュリティ機能は、セキュリティ対応ドライブを使用して保護を強化します。これらのドライブのボリュームグループまたはプールをドライブセキュリティの対象として選択すると、ドライブはセキュリティキーを探してからデータへのアクセスを許可します。プールおよびボリュームグループのドライブセキュリティはいつでも有効にでき、ドライブ上の既存データには影響しません。ただし、ドライブセキュリティを無効にするには、ドライブ上のすべてのデータを消去する必要があります。

== ストレージアレイレベルでのドライブセキュリティの動作

ドライブセキュリティ機能を使用する場合、セキュリティ有効ドライブとストレージアレイのコントローラで共有されるセキュリティキーを作成します。ドライブの電源をオフにしてオンにするたびに、コントローラがセキュリティキーを適用するまでセキュリティ有効ドライブはセキュリティロック状態になります。

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して別のストレージアレイに取り付けると、ドライブはセキュリティロック状態になります。再配置したドライブでは、データに再びアクセスできるようにする前にセキュリティキーが検索されます。データのロックを解除するには、ソースストレージアレイからセキュリティキーを適用します。ロック解除プロセスが正常に完了すると、再配置したドライブでターゲットストレージアレイにすでに格納されているセキュリティキーが使用されるため、インポートしたセキュリティキーファイルは不要になります。

[NOTE]
====
内部でキーを管理する場合、実際の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。人間が判読できる形式ではなく、ユーザがアクセスすることもできません。

====

== ボリュームレベルでのドライブセキュリティの動作

セキュリティ対応ドライブからプールまたはボリュームグループを作成する場合、そのプールまたはボリュームグループに対してドライブセキュリティを有効にすることもできます。ドライブセキュリティを有効にすると、ドライブとそれに関連付けられているボリュームグループおよびプールがsecure-_enabled_になります。

セキュリティ有効のボリュームグループおよびプールを作成する際は、次のガイドラインに注意してください。

*
ボリュームグループとプールはセキュリティ対応ドライブだけで構成されている必要があります。（FIPSのサポートが必要なドライブには、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のみのボリュームグループまたはプールで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）。
* ボリュームグループとプールの状態が最適1である必要があります。

[[ID27f08bf521afd4c052082bbcabba1e08]]
= セキュリティキー管理の仕組み
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ドライブセキュリティ機能を実装する場合、セキュリティ有効ドライブ（FIPSまたはFDE）にはデータアクセス用のセキュリティキーが必要です。セキュリティキーは、ストレージアレイ内のこれらのタイプのドライブとコントローラで共有される文字列です。

ドライブの電源をオフにしてオンにするたびに、コントローラがセキュリティキーを適用するまでセキュリティ有効ドライブはセキュリティロック状態になります。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、ドライブのデータはロックされます。ドライブを別のストレージアレイに取り付け直すと、データへのアクセスを再開する前にセキュリティキーが検索されます。データのロックを解除するには、元のセキュリティキーを適用する必要があります。

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

内部キーは、コントローラの永続的メモリ上のアクセス不能な場所に保持され、「非表示」になります。内部キー管理を実装するには、次の手順を実行します。

. 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。
.
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お問い合わせください。
.
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た文字列で、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します。内部キーを作成するには、メニューに移動します。[システム]、[セキュリティキー管理]、[内部キーの作成]の順に選択します。

セキュリティキーは、コントローラのアクセスできない非表示の場所に格納されます。その後、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および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。外部キー管理を実装するには、次の手順を実行します。

. 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。
.
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お問い合わせください。
.
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、キー管理サーバがストレージアレイのKMIP要求を信頼できるように、ストレージアレイのコントローラを検証します。
+
.. 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。
.. 次に、キー管理サーバによって信頼されているCAから署名済みクライアント証明書を要求します。（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）。
.. クライアント証明書ファイルが作成されたら、そのファイルをSystem Managerにアクセスするホストにコピーします。

. キー管理サーバから証明書ファイルを取得し、そのファイルをSystem Managerにアクセスするホストにコピーします。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に、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。外部キーを作成するには、メニューに移動します。[設定]、[システム]、[セキュリティキー管理]、[外部キーの作成]の順に選択します。

入力したクレデンシャルを使用して、システムがキー管理サーバに接続されます。その後、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およびプールでセキュリティを有効にしたりできます。

[[ID9e0e978d53468aaab66e98106f289d1b]]
= ドライブセキュリティの用語
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ストレージアレイに関連するドライブセキュリティの用語を次に示します。

[cols="25h,~"]
|===
| 期間 | 製品説明

a|
ドライブセキュリティ機能
a|
ドライブセキュリティは、 Full Disk Encryption （ FDE ）ドライブまたは連邦情報処理標準（ FIPS ）ドライブを使用してセキュリティを強化するストレージアレイの機能です。これらのドライブをドライブセキュリティ機能と組み合わせて使用すると、データにアクセスするためのセキュリティキーが必要になります。ドライブをアレイから物理的に取り外した場合、別のアレイに取り付けるまでドライブは動作しません。別のアレイに取り付けると、正しいセキュリティキーを指定するまでセキュリティロック状態になります。

a|
FDEトライフ
a|
Full Disk Encryption （ FDE）ドライブは、ハードウェアレベルでディスクドライブの暗号化を実行します。ハードドライブには、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ASICチップが搭載されています。

a|
FIPSトライフ
a|

FIPSドライブは、連邦情報処理標準（FIPS）140-2レベル2
に準拠しています。基本的な概念はFDEドライブと同じですが、米国政府の基準に従って強力な暗号化アルゴリズムと暗号化方式を実装しています。FIPSドライブにはFDEドライブよりも高度なセキュリティ基準が採用されています。

a|
管理クライアント
a|
System
Managerにアクセスするためのブラウザを含むローカルシステム（コンピュータやタブレットなど）。

a|
パスフレーズ
a|
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します。ドライブの移行またはヘッドの交換によってバックアップされたセキュリティキーをインポートする場合は、セキュリティキーの暗号化に使用したパスフレーズを指定する必要があります。パスフレーズは8~32文字で指定できます。

[NOTE]
====
ドライブセキュリティのパスフレーズは、ストレージアレイの管理者パスワードとは別のものです。

====

a|
セキュリティ対応ドライブ
a|
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。これらのドライブでは、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。ドライブセキュリティ機能を使用したセキュリティの強化に使用できるため、これらのドライブはsecured_capable_とみなされます。これらのドライブを使用するボリュームグループやプールでドライブセキュリティ機能を有効にすると、ドライブはsecure-_enabled_になります。

a|
セキュリティ有効ドライブ
a|
セキュリティ有効ドライブは、ドライブセキュリティ機能で使用されます。ドライブセキュリティ

機能を有効にし、かつsecured_caped_drivesのプールまたはボリュームグループにドライブセキュリティを適用すると、ドライブはsecure__enable__になります。読み取り/書き込みアクセスは、正しいセキュリティキーが設定されたコントローラからのみ実行できます。この追加のセキュリティ機能により、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。

 a|
セキュリティキー
 a|
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。ドライブの電源をオフにしてオンにするたびに、コントローラがセキュリティキーを適用するまでセキュリティ有効ドライブはセキュリティロック状態になります。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、ドライブのデータはロックされます。ドライブを別のストレージアレイに取り付け直すと、データへのアクセスを再開する前にセキュリティキーが検索されます。データのロックを解除するには、元のセキュリティキーを適用する必要があります。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。

* 内部キー管理--セキュリティキーをコントローラの永続的メモリに作成して保持します。
* 外部キー管理--セキュリティキーを外部キー管理サーバに作成して保管します。

 a|
セキュリティキー識別子
 a|
セキュリティキー識別子は、キーの作成時にセキュリティキーに関連付けられる文字列です。識別子は、コントローラとセキュリティ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。

|===

:leveloffset: -1

= セキュリティキーの設定

:leveloffset: +1

[[IDaabf19bdc60f64546cb767a5189ed02f]]
= 内部セキュリティキーの作成
:allow-uri-read:
:experimental:
:icons: font

```
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
ドライブセキュリティ機能を使用するには、ストレージアレイのコントローラとセキュリティ対応ドライブで共有される内部セキュリティキーを作成します。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。

.開始する前に
*
ストレージアレイにセキュリティ対応ドライブが搭載されている必要があります。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。
*
ドライブセキュリティ機能が有効になっている必要があります。そうしないと、このタスクの実行中に[セキュリティキーを作成できません]ダイアログボックスが開きます。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お問い合わせください。

```
[NOTE]
====
```
ストレージアレイにFDEドライブとFIPSドライブの両方が搭載されている場合は、すべてのドライブで同じセキュリティキーが共有されます。

```
====
```
.タスクの内容
このタスクでは、内部セキュリティキーに関連付ける識別子とパスフレーズを定義します。

```
[NOTE]
====
```
ドライブセキュリティのパスフレーズは、ストレージアレイの管理者パスワードとは別のものです。

```
====
```
.手順
. メニューを選択します。[設定][システム]。
. セキュリティキー管理*で、*内部キーの作成*を選択します。
+
まだセキュリティキーを生成していない場合は、セキュリティキーの作成ダイアログボックスが開きます。

. 次のフィールドに情報を入力します。
+
** *セキュリティキー識別子を定義*--デフォルト値
(コントローラファームウェアによって生成されたストレージアレイ名とタイムスタンプ)をそのまま使用するか'独自の値を入力することができます入力できる文字数は最大189文字です。使用でき

るのは英数字のみで、スペース、句読点、記号は使用できません。
+
[NOTE]
====
入力した文字列の前後に追加の文字が自動的に生成されて付加されます。文字が追加されることで識別子が一意であることが保証されます。

====
** *パスフレーズを定義/パスフレーズを再入力*--パスフレーズを入力して確認します値は8~32文字で、次の文字をそれぞれ含める必要があります。
+
*** 大文字のアルファベット（
1文字以上）。パスフレーズでは大文字と小文字が区別されることに注意してください。
*** 数字（1文字以上）。
*** !、*、@などの英数字以外の文字（1文字以上）。

+
[CAUTION]
====
後で使用するために、必ず入力を記録しておいてください。セキュリティ有効ドライブをストレージアレイから移動する必要がある場合は、ドライブデータのロックを解除するために識別子とパスフレーズが必要です。

====
. [作成（ Create ）] をクリックします。
+
セキュリティキーは、コントローラのアクセスできない場所に格納されています。実際のキーと一緒に、ブラウザからダウンロードされる暗号化されたキーファイルがあります。

+
[NOTE]
====
ダウンロードしたファイルのパスは、ブラウザのデフォルトのダウンロード先によって異なる場合があります。

====
. キー識別子、パスフレーズ、ダウンロードしたキーファイルの場所を記録し、*閉じる*をクリックします。

.結果
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およびプールでセキュリティを有効にしたりできます。

[NOTE]
====
ドライブの電源をオフにして再度オンにすると、すべてのセキュリティ有効ドライブがセキュリティロック状態に変わります。この状態のデータには、ドライブの初期化時にコントローラが正しいセキュリティキーを適用するまでアクセスできません。第三者がロックされたドライブを物理的に取り外して別のシステムに取り付けた場合でも、データへの不正アクセスを防止することができます。

====
.終了後
セキュリティキーを検証して、キーファイルが破損していないことを確認する必要があります。

[[ID64c90ac59237b2e46710a757c378f2cc]]
= 外部セキュリティキーの作成
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
キー管理サーバでドライブセキュリティ機能を使用するには、キー管理サーバとストレージアレイのセキュリティ対応ドライブで共有される外部キーを作成する必要があります。

.開始する前に
*
アレイにセキュリティ対応ドライブが搭載されている必要があります。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。
+
[NOTE]
====
ストレージアレイにFDEドライブとFIPSドライブの両方が搭載されている場合は、すべてのドライブで同じセキュリティキーが共有されます。

====
*
ドライブセキュリティ機能が有効になっている必要があります。そうしないと、このタスクの実行中に[セキュリティキーを作成できません]ダイアログボックスが開きます。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お問い合わせください。
*
ストレージアレイのコントローラ用の署名済みクライアント証明書ファイルがあり、そのファイルをSystem
Managerにアクセスするホストにコピーしておきます。クライアント証明書はストレージアレイのコントローラを検証し、キー管理サーバがKey Management Interoperability Protocol

（KMIP）要求を信頼できるようにします。
* キー管理サーバから証明書ファイルを取得し、そのファイルをSystem Managerにアクセスするホストにコピーする必要があります。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に、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。
+
[NOTE]
====
サーバ証明書の詳細については、キー管理サーバのドキュメントを参照してください。

====

.タスクの内容
このタスクでは、キー管理サーバのIPアドレスと使用するポート番号を定義し、外部キー管理に使用する証明書をロードします。

.手順
. メニューを選択します。[設定][システム]。
. セキュリティキー管理*で、*外部キーの作成*を選択します。
+
[NOTE]
====
現在内部キー管理が設定されている場合は、外部キー管理に切り替えるかどうかを確認するダイアログボックスが開きます。

====
+
[外部セキュリティキーの作成]ダイアログボックスが開きます。

. [*キーサーバへの接続*]で、次のフィールドに情報を入力します。
+
** *キー管理サーバのアドレス*-キー管理に使用するサーバの完全修飾ドメイン名またはIPアドレス（IPv4またはIPv6）を入力します。
** *キー管理ポート番号*--
KMIP通信に使用するポート番号を入力しますキー管理サーバの通信に使用される最も一般的なポート番号は5696です。
+
*オプション：*バックアップ・キー・サーバを構成する場合は、*キー・サーバの追加*をクリックし、そのサーバの情報を入力します。プライマリキーサーバに到達できない場合は、2番目のキーサーバが使用されます。各キーサーバが同じキーデータベースにアクセスできることを確認します。アクセスできないと、アレイはエラーを投稿し、バックアップサーバを使用できません。

+

NOTE: 一度に使用されるキーサーバは
1つだけです。ストレージアレイがプライマリキーサーバに到達できない場合、アレイはバックアッ

プキーサーバに接続します。両方のサーバ間でパリティを維持する必要があることに注意してください。そうしないと、エラーが発生する可能性があります。

** *クライアント証明書の選択*--最初の*参照
*ボタンをクリックして、ストレージアレイのコントローラの証明書ファイルを選択します。
** *キー管理サーバのサーバ証明書を選択*-- 2番目の*参照
*ボタンをクリックして、キー管理サーバの証明書ファイルを選択します。キー管理サーバのルート証明書、中間証明書、またはサーバ証明書を選択できます。

. 「 * 次へ * 」をクリックします。
. 「*キーの作成/バックアップ
*」では、セキュリティ上の理由からバックアップ・キーを作成できます。
+
**
（推奨）バックアップキーを作成する場合は、チェックボックスを選択したまま、パスフレーズを入力して確認します。値は8~32文字で、次の文字をそれぞれ含める必要があります。
+
*** 大文字のアルファベット（
1文字以上）。パスフレーズでは大文字と小文字が区別されることに注意してください。
*** 数字（1文字以上）。
*** !、*、@などの英数字以外の文字（1文字以上）。

+
[CAUTION]
====
後で使用するために、必ず入力を記録しておいてください。セキュリティ有効ドライブをストレージアレイから移動する必要がある場合は、ドライブデータのロックを解除するためにパスフレーズが必要です。

====
+
** バックアップキーを作成しない場合は、チェックボックスを選択解除します。
+
[CAUTION]
====
外部キーサーバへのアクセスが失われ、バックアップキーがないと、ドライブを別のストレージアレイに移行するとドライブ上のデータにアクセスできなくなることに注意してください。このオプションは、System Managerでバックアップキーを作成する唯一の方法です。

====

. [完了] をクリックします。

+
入力したクレデンシャルを使用して、システムがキー管理サーバに接続されます。その後、セキュリティキーのコピーがローカルシステムに格納されます。

+
[NOTE]
====
ダウンロードしたファイルのパスは、ブラウザのデフォルトのダウンロード先によって異なる場合があります。

====
. パスフレーズとダウンロードしたキーファイルの場所を記録し、*閉じる*をクリックします。
+
ページには、次のメッセージと外部キー管理用のリンクが表示されます。

+
`Current key management method: External`

. 「* Test Communication
*」を選択して、ストレージアレイとキー管理サーバの間の接続をテストします。
+
テスト結果がダイアログボックスに表示されます。

.結果
外部キー管理を有効にすると、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およびプールでセキュリティを有効にしたりできます。

[NOTE]
====
ドライブの電源をオフにして再度オンにすると、すべてのセキュリティ有効ドライブがセキュリティロック状態に変わります。この状態のデータには、ドライブの初期化時にコントローラが正しいセキュリティキーを適用するまでアクセスできません。第三者がロックされたドライブを物理的に取り外して別のシステムに取り付けた場合でも、データへの不正アクセスを防止することができます。

====
.終了後
セキュリティキーを検証して、キーファイルが破損していないことを確認する必要があります。

:leveloffset: -1

= セキュリティキーを管理します。

```
:leveloffset: +1


[[ID27eca6de5ac56aa5e6641999807ef9ac]]
= セキュリティキーの変更
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
セキュリティキーはいつでも新しいキーに置き換えることができます。社内でセキュリティ侵害の可能性があり、権限のない担当者がドライブデータにアクセスできないようにする場合は、セキュリティキーの変更が必要になることがあります。

.手順
. メニューを選択します。[設定][システム]。
. セキュリティキー管理*で、*キーの変更*を選択します。
+
[セキュリティキーの変更]ダイアログボックスが開きます。

. 次のフィールドに情報を入力します。
+
** *セキュリティキー識別子を定義する*--(内部セキュリティキーのみ
)デフォルトの値（コントローラ ファームウェアで生成されたストレージ
アレイ名とタイムスタンプ）をそのまま使用するか、独自の値を入力します。入力できる文字数は最大189文字です。使用できるのは英数字のみで、スペース、句読点、記号は使用できません。
+
[NOTE]
====
入力した文字列の前後に追加の文字が自動的に生成されて付加されます。文字が追加されることで識別子が一意であることが保証されます。

====
** *パスフレーズを定義/パスフレーズを再入力*--
これらの各フィールドにパスフレーズを入力します値は8~32文字で、次の文字をそれぞれ含める必要があります。
+
*** 大文字のアルファベット（
1文字以上）。パスフレーズでは大文字と小文字が区別されることに注意してください。
*** 数字（1文字以上）。
*** !、*、@などの英数字以外の文字（1文字以上）。
```

.
外部セキュリティキーの場合、新しいセキュリティキーの作成時に古いセキュリティキーを削除するには、ダイアログの下部にある[Delete current security key...]チェックボックスを選択します。
+
[CAUTION]
====
後で使用するためにエントリを記録しておいてください--
セキュリティ有効ドライブをストレージアレイから移動する必要がある場合、ドライブデータのロックを解除するために識別子とパスフレーズを知っておく必要があります。

====
. [変更（ Change ）] をクリックします。
+
前のキーは新しいセキュリティキーで上書きされ、無効になります。

+
[NOTE]
====
ダウンロードしたファイルのパスは、ブラウザのデフォルトのダウンロード先によって異なる場合があります。

====
. キー識別子、パスフレーズ、ダウンロードしたキーファイルの場所を記録し、*閉じる*をクリックします。

.終了後
セキュリティキーを検証して、キーファイルが破損していないことを確認する必要があります。

[[ID85a59902774ff7d49b5a5403af71ad54]]
= 外部キー管理から内部キー管理への切り替え
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ドライブセキュリティの管理方法を外部キーサーバからストレージアレイで使用される内部方式に変更できます。以前に外部キー管理用に定義したセキュリティキーが、内部キー管理に使用されます。

.タスクの内容
このタスクでは、外部キー管理を無効にし、新しいバックアップコピーをローカルホストにダウンロードします。既存のキーは引き続きドライブセキュリティに使用されますが、ストレージアレイで内部的に管理されます。

.手順
. メニューを選択します。[設定][システム]。
. [*セキュリティキー管理*]で、[*外部キー管理を無効にする*]を選択します。
+
[外部キー管理の無効化]ダイアログボックスが開きます。

. 「*パスフレーズを定義/パスフレーズを再入力
*」で、キーのバックアップに使用するパスフレーズを入力して確認します。値は8~32文字で、次の文字をそれぞれ含める必要があります。
+
** 大文字のアルファベット（
1文字以上）。パスフレーズでは大文字と小文字が区別されることに注意してください。
** 数字（1文字以上）。
** !、*、@などの英数字以外の文字（1文字以上）。

+
[CAUTION]
====
_後で使用するために、必ずエントリを記録しておいてください。セキュリティ有効ドライブをストレージアレイから移動する必要がある場合は、ドライブデータのロックを解除するために識別子とパスフレーズが必要です。

====
. [*Disable*] をクリックします。
+
バックアップキーがローカルホストにダウンロードされます。

. キー識別子、パスフレーズ、ダウンロードしたキーファイルの場所を記録し、*閉じる
*をクリックします。

.結果
ドライブセキュリティがストレージアレイを使用して内部的に管理されるようになりました。

.終了後
セキュリティキーを検証して、キーファイルが破損していないことを確認する必要があります。

[[ID0b38120b58712058cc7672b908450cfd]]
= キー管理サーバ設定の編集

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


[role="lead"]
外部キー管理を設定している場合は、キー管理サーバの設定をいつでも表示および編集できます。

.手順
. メニューを選択します。[設定][システム]。
. セキュリティキー管理*で、*キー管理サーバ設定の表示/編集*を選択します。
. 次のフィールドの情報を編集します。
+
** *キー管理サーバのアドレス*-キー管理に使用するサーバの完全修飾ドメイン名または
IPアドレス（IPv4またはIPv6）を入力します。
** *キー管理ポート番号*-- Key Management Interoperability Protocol (KMIP
)通信に使用するポート番号を入力します
+
*オプション：* Add Key Server*をクリックすると、別のキーサーバを含めることができます。



. [ 保存（ Save ） ] をクリックします。




[[ID74b26ed0dc7803ab03b05e8fe2e378f9]]
= セキュリティキーのバックアップ
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
セキュリティキーを作成または変更したら、元のキーファイルが破損した場合に備えて、キーファイルのバックアップコピーを作成できます。

.タスクの内容
このタスクでは、以前に作成したセキュリティキーをバックアップする方法について説明します。この手順では、バックアップ用の新しいパスフレーズを作成します。このパスフレーズは、元のキーの作成時または最後の変更時に使用されたパスフレーズと一致する必要はありません。このパスフレーズは、作成するバックアップにのみ適用されます。
```

.手順
. メニューを選択します。[設定][システム]。
. セキュリティキー管理*で、*バックアップキー*を選択します。
+
[セキュリティキーのバックアップ]ダイアログボックスが開きます。

. [*パスフレーズを定義/パスフレーズを再入力
*]フィールドに、このバックアップのパスフレーズを入力して確認します。
+
値は8~32文字で、次の文字をそれぞれ含める必要があります。

+
** 大文字（1文字以上）
** 数字（1文字以上）
** 英数字以外の文字（！、*、@など）（1文字以上）

+
[CAUTION]
====
後で使用するためには、必ず入力を記録してください。このセキュリティキーのバックアップにアクセスするには、パスフレーズが必要です。

====
. [バックアップ]をクリックします。
+
セキュリティキーのバックアップがローカルホストにダウンロードされ、[*Confirm/Record Security Key Backup*]ダイアログボックスが開きます。

+
[NOTE]
====
ダウンロードしたセキュリティキーファイルのパスは、ブラウザのデフォルトのダウンロード先によって異なる場合があります。

====
. パスフレーズを安全な場所に記録し、*閉じる*をクリックします。

.終了後
バックアップセキュリティキーを検証する必要があります。

[[IDa26583abe9a7da924b1e5e75b8f2fa21]]
= セキュリティキーの検証

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


[role="lead"]
セキュリティキーを検証して、セキュリティキーが破損していないこと、およびパスフレーズが正しいことを確認できます。

.タスクの内容
このタスクでは、以前に作成したセキュリティキーを検証する方法について説明します。これは、キーファイルが破損していないこと、およびパスフレーズが正しいことを確認するための重要な手順です。これにより、セキュリティ有効ドライブをストレージアレイ間で移動するときに、あとでドライブデータにアクセスできるようになります。

.手順
. メニューを選択します。[設定][システム]。
. ［*セキュリティキー管理*］で、［*キーの検証*］を選択します。
+
[セキュリティキーの検証]ダイアログボックスが開きます。

. [参照]*をクリックし、キーファイル（など）を選択します `drivesecurity.slk`。
. 選択したキーに関連付けられているパスフレーズを入力します。
+
有効なキーファイルとパスフレーズを選択すると、*検証*ボタンが使用可能になります。

. [*Validate]をクリックします。
+
検証の結果がダイアログボックスに表示されます。

. 結果に「セキュリティキーの検証に成功しました」と表示された場合は、*閉じる*をクリックします。エラーメッセージが表示された場合は、ダイアログボックスに表示される推奨される手順に従います。




[[IDdb78f8f68240dd98f26e2513fe7a9faa]]
= 内部キー管理の使用時のドライブのロック解除
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]
内部キー管理を設定したあとにセキュリティ有効ドライブをストレージアレイ間で移動した場合、ドライブ上の暗号化されたデータにアクセスできるようにするには、セキュリティキーを新しいストレージアレイに再割り当てする必要があります。

.開始する前に
*
ソースアレイ（ドライブを取り外すアレイ）で、ボリュームグループをエクスポートし、ドライブを取り外しておきます。ターゲットアレイにドライブを取り付け直しておきます。
+

NOTE: エクスポート/インポート機能はSystem Managerユーザインターフェイスではサポートされていません。ボリュームグループを別のストレージアレイにエクスポート/インポートするには、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。

+
ボリュームグループの移行の詳細な手順については、を参照してhttps://kb.netapp.com/["NetAppナレッジベース"^]ください。System Managerで管理している新しいアレイや従来型システムのアレイについては、該当する手順に従ってください。

*
ドライブセキュリティ機能が有効になっている必要があります。そうしないと、このタスクの実行中に[セキュリティキーを作成できません]ダイアログボックスが開きます。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お問い合わせください。
*
ロックを解除するドライブに関連付けられているセキュリティキーを確認しておく必要があります。
* セキュリティキーファイルは管理クライアント（System Managerへのアクセスに使用するブラウザを備えたシステム）にあります。別のシステムで管理されているストレージアレイにドライブを移動する場合は、その管理クライアントにセキュリティキーファイルを移動する必要があります。

.タスクの内容
内部キー管理を使用する場合、セキュリティキーはストレージアレイにローカルに格納されます。セキュリティキーは、読み取り/書き込みアクセス用にコントローラとドライブで共有される文字列です。ドライブをアレイから物理的に取り外して別のドライブに取り付けた場合、正しいセキュリティキーを指定するまでドライブは動作しません。

[NOTE]
====
コントローラの永続的メモリから内部キーを作成するか、キー管理サーバから外部キーを作成できます。ここでは、_INTERNAL _KEY管理を使用する場合のデータのロック解除について説明します。外部キー管理を使用した場合は、を参照してくださいlink:unlock-drives-using-an-external-security-

key.html["外部キー管理の使用時のドライブのロック解除"]。コントローラのアップグレードを実行し、すべてのコントローラを最新のハードウェアに交換する場合は、のEシリーズおよびSANtricityドキュメントセンターに記載されている手順に従う必要があります。link:https://docs.netapp.com/us-en/e-series/upgrade-controllers/upgrade-unlock-drives-task.html["ドライブのロック解除"]

====
セキュリティ有効ドライブを別のアレイに取り付けると、そのアレイでドライブが検出され、「要対応」状態となって「セキュリティ キーが必要です」というステータスが表示されます。ドライブデータのロックを解除するには、セキュリティ キー ファイルを選択し、キーのパスフレーズを入力します（このパスフレーズはストレージアレイの管理者パスワードとは異なります）。

新しいストレージアレイに取り付けられている他のセキュリティ有効ドライブでは、インポートするセキュリティキーとは異なるセキュリティキーが使用される場合があります。インポートプロセスでは、取り付けようとしているドライブのデータのロックを解除するためにのみ古いセキュリティキーが使用されます。ロック解除プロセスが完了すると、新しく取り付けたドライブのキーがターゲットストレージアレイのセキュリティキーに変更されます。

.手順
. メニューを選択します。[設定][システム]。
. セキュリティキー管理*で、*セキュアドライブのロック解除*を選択します。
+
[セキュアドライブのロック解除]ダイアログボックスが開きます。セキュリティキーを必要とするドライブが表に表示されます。

.
*オプション：ドライブ番号にカーソルを合わせると、ドライブの場所（シェルフ番号とベイ番号）が表示されます。
. [*参照
]をクリックし、ロックを解除するドライブに対応するセキュリティキーファイルを選択します。
+
選択したキーファイルがダイアログボックスに表示されます。

. このキーファイルに関連付けられているパスフレーズを入力します。
+
入力した文字はマスクされます。

. [ロック解除]をクリックします。
+
ロック解除処理が成功すると、ダイアログボックスに「The associated secure drives have been unlocked」と表示されます。

.結果
すべてのドライブがロックされてロックが解除されると、ストレージアレイ内の各コントローラがリブートされます。ただし、ターゲットストレージアレイ内にロック解除されたドライブがすでに

ある場合、コントローラはリブートされません。

.終了後
デスティネーションアレイ（新しくドライブを取り付けたアレイ）で、ボリュームグループをインポートできるようになりました。

NOTE: エクスポート/インポート機能はSystem Managerユーザインターフェイスではサポートされていません。ボリュームグループを別のストレージアレイにエクスポート/インポートするには、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。

ボリュームグループの移行の詳細な手順については、を参照して https://kb.netapp.com/["NetAppナレッジベース"^]ください。

[[ID3ab1694f459e67b540cfa543c772fe3e]]
= 外部キー管理の使用時のドライブのロック解除
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
外部キー管理を設定したあとにセキュリティ有効ドライブをストレージアレイ間で移動した場合、ドライブ上の暗号化されたデータにアクセスできるようにするには、セキュリティキーを新しいストレージアレイに再割り当てする必要があります。

.開始する前に
*
ソースアレイ（ドライブを取り外すアレイ）で、ボリュームグループをエクスポートし、ドライブを取り外しておきます。ターゲットアレイにドライブを取り付け直しておきます。
+

NOTE: エクスポート/インポート機能はSystem Managerユーザインターフェイスではサポートされていません。ボリュームグループを別のストレージアレイにエクスポート/インポートするには、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。

+
ボリュームグループの移行の詳細な手順については、を参照して https://kb.netapp.com/["NetAppナレッジベース"^]ください。System Managerで管理している新しいアレイや従来型システムのアレイについては、該当する手順に従ってください。

*
ドライブセキュリティ機能が有効になっている必要があります。そうしないと、このタスクの実行中に[セキュリティキーを作成できません]ダイアログボックスが開きます。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お問い合わせください。
* キー管理サーバのIPアドレスとポート番号を確認しておく必要があります。
*
ストレージアレイのコントローラ用の署名済みクライアント証明書ファイルがあり、そのファイルをSystem
Managerにアクセスするホストにコピーしておきます。クライアント証明書はストレージアレイのコントローラを検証し、キー管理サーバがKey Management Interoperability Protocol（KMIP）要求を信頼できるようにします。
* キー管理サーバから証明書ファイルを取得し、そのファイルをSystem
Managerにアクセスするホストにコピーする必要があります。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に、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。

[NOTE]
====
サーバ証明書の詳細については、キー管理サーバのドキュメントを参照してください。

====
.タスクの内容
外部キー管理を使用する場合、セキュリティキーは外部のサーバに格納され、セキュリティキーを保護するように設計されています。セキュリティキーは、読み取り/書き込みアクセス用にコントローラとドライブで共有される文字列です。ドライブをアレイから物理的に取り外して別のドライブに取り付けた場合、正しいセキュリティキーを指定するまでドライブは動作しません。

[NOTE]
====
コントローラの永続的メモリから内部キーを作成するか、キー管理サーバから外部キーを作成できます。ここでは、_external_key管理を使用する場合のデータのロック解除について説明します。内部キー管理を使用した場合は、を参照してくださいlink:unlock-drives-using-an-internal-security-key.html["内部キー管理の使用時のドライブのロック解除
"]。コントローラのアップグレードを実行し、すべてのコントローラを最新のハードウェアに交換する場合は、のEシリーズおよびSANtricityドキュメントセンターに記載されている手順に従う必要があります。link:https://docs.netapp.com/us-en/e-series/upgrade-controllers/upgrade-unlock-drives-task.html["ドライブのロック解除"]

====
セキュリティ有効ドライブを別のアレイに取り付けると、そのアレイでドライブが検出され、「要対応」状態となって「セキュリティ キーが必要です」というステータスが表示されます。ドライブデータのロックを解除するには、セキュリティ キー ファイルをインポートし、キーのパスフレーズを入力します（このパスフレーズはストレージアレイの管理者パスワードとは異なります）。その際に、外部キー管理サーバを使用するようにストレージ
アレイを設定すると、セキュリティ

キーにアクセスできるようになります。ストレージアレイに接続してセキュリティキーを取得するためには、サーバの連絡先情報を指定する必要があります。

新しいストレージアレイに取り付けられている他のセキュリティ有効ドライブでは、インポートするセキュリティキーとは異なるセキュリティキーが使用される場合があります。インポートプロセスでは、取り付けようとしているドライブのデータのロックを解除するためにのみ古いセキュリティキーが使用されます。ロック解除プロセスが完了すると、新しく取り付けたドライブのキーがターゲットストレージアレイのセキュリティキーに変更されます。

.手順
. メニューを選択します。[設定][システム]。
. セキュリティキー管理*で、*外部キーの作成*を選択します。
. 必要な接続情報と証明書をウィザードに入力します。
. ［*通信のテスト*］をクリックして、外部キー管理サーバへのアクセスを確認します。
. [セキュアドライブのロック解除]を選択します。
+
[セキュアドライブのロック解除]ダイアログボックスが開きます。セキュリティキーを必要とするドライブが表に表示されます。

.
*オプション：ドライブ番号にカーソルを合わせると、ドライブの場所（シェルフ番号とベイ番号）が表示されます。
. [*参照
]をクリックし、ロックを解除するドライブに対応するセキュリティキーファイルを選択します。
+
選択したキーファイルがダイアログボックスに表示されます。

. このキーファイルに関連付けられているパスフレーズを入力します。
+
入力した文字はマスクされます。

. [ロック解除]をクリックします。
+
ロック解除処理が成功すると、ダイアログボックスに「The associated secure drives have been unlocked」と表示されます。

.結果
すべてのドライブがロックされてロックが解除されると、ストレージアレイ内の各コントローラがリブートされます。ただし、ターゲットストレージアレイ内にロック解除されたドライブがすでにある場合、コントローラはリブートされません。

.終了後
デスティネーションアレイ（新しくドライブを取り付けたアレイ）で、ボリュームグループをインポートできるようになりました。

NOTE: エクスポート/インポート機能はSystem Managerユーザインターフェイスではサポートされていません。ボリュームグループを別のストレージアレイにエクスポート/インポートするには、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。

ボリュームグループの移行の詳細な手順については、を参照して https://kb.netapp.com/["NetAppナレッジベース"^]ください。

:leveloffset: -1

= FAQ

:leveloffset: +1

[[IDdc3ca43f38b84b45a2cde2bf148c5765]]
= 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？
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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で共有されます。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

内部キーは、コントローラの永続的メモリ上のアクセス不能な場所に保持され、「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、次の作業を実行する必要があります。

. 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。

.
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お問い合わせください。

その後、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た文字列で、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します。完了すると、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。その後、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および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、次の作業を実行する必要があります。

. 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。
.
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お問い合わせください。
.
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、キー管理サーバがストレージアレイのKMIP要求を信頼できるように、ストレージアレイのコントローラを検証します。
+
.. 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。
.. 次に、キー管理サーバによって信頼されているCAから署名済み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）。
.. クライアント証明書ファイルが作成されたら、そのファイルをSystem Managerにアクセスするホストにコピーします。

. キー管理サーバから証明書ファイルを取得し、そのファイルをSystem Managerにアクセスするホストにコピーします。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に、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。完了すると、入力したクレデンシャルでキ

ー管理サーバに接続されます。その後、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およびプールでセキュリティを有効にしたりできます。

[[ID261e6d8ae7ea8b64919c2cc96a59b74e]]
= パスフレーズを定義する必要があるのはなぜですか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
パスフレーズは、ローカル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度取り付けられた場合、そのドライブの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。

[[ID2a17c61e9af9109e007b06a7936cd7c8]]
= セキュリティキー情報を記録することが重要なのはなぜですか。
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
セキュリティキー情報を紛失し、バックアップがない場合、セキュリティ有効ドライブの再配置時やコントローラのアップグレード時にデータが失われる可能性があります。ドライブ上のデータのロックを解除するには、セキュリティキーが必要です。

セキュリティキー識別子、関連付けられているパスフレーズ、およびセキュリティキーファイルが保存されているローカルホスト上の場所を必ず記録してください。

[[ID7da306bd1a914d613cba42dd73f5ea0b]]
= セキュリティキーをバックアップするときは、どのような点に注意する必要がありますか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
バックアップがない状態で元のセキュリティキーが破損した場合、ドライブ上のデータをストレージアレイ間で移行すると、ドライブ上のデータにアクセスできなくなります。

セキュリティキーをバックアップする前に、次のガイドラインに注意してください。

* 元のキーファイルのセキュリティキー識別子とパスフレーズを確認しておきます。
+
[NOTE]
====
識別子を使用するのは内部キーのみです。識別子を作成すると、追加の文字が自動的に生成され、識別子文字列の両端に追加されます。文字が追加されることで識別子が一意であることが保証されます。

====
*
バックアップ用の新しいパスフレーズを作成します。このパスフレーズは、元のキーの作成時または最後の変更時に使用されたパスフレーズと一致する必要はありません。このパスフレーズは、作成するバックアップにのみ適用されます。
+
[NOTE]
====
ドライブセキュリティのパスフレーズをストレージアレイの管理者パスワードと混同しないでください。ドライブセキュリティのパスフレーズは、セキュリティキーのバックアップを保護します。管理者パスワードは、ストレージアレイ全体を不正アクセスから保護します。

====
*
バックアップセキュリティキーファイルが管理クライアントにダウンロードされます。ダウンロードしたファイルのパスは、ブラウザのデフォルトのダウンロード先によって異なる場合があります。セキュリティキー情報が格納されている場所を必ず記録しておいてください。

[[ID7dcf31e6a01b96e57662da80097a2ccb]]
= セキュアドライブのロックを解除するときは、どのような点に注意する必要がありますか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
セキュリティ有効ドライブのデータのロックを解除するには、ドライブのセキュリティキーをインポートする必要があります。

セキュリティ有効ドライブのロックを解除する際は、次のガイドラインに注意してください。

*
ストレージアレイにすでにセキュリティキーが設定されている必要があります。移行したドライブのキーがターゲットストレージアレイに変更されます。
*
移行するドライブについて、セキュリティキー識別子とセキュリティキーファイルに対応するパスフレーズを確認しておく必要があります。
* セキュリティキーファイルが管理クライアント（System Managerへのアクセスに使用するブラウザを備えたシステム）にある必要があります。
* ロックされたNVMeドライブをリセットする場合は、ドライブのセキュリティIDを入力する必要があります。セキュリティIDを確認するには、ドライブを取り外す必要があります。ドライブのラベルに記載されたPSID（最大32文字）を確認してください。処理を開始する前に、ドライブが再取り付けされていることを確認してください。

[[IDdead65ecb419fdb0874179f57842893c]]
= 読み取り/書き込みアクセスとは何ですか？
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
[ドライブ設定]ウィンドウには、ドライブセキュリティ属性に関する情報が表示されます。「読み取り/書き込みアクセス」は、ドライブのデータがロックされているかどうかを表示する属性の1つです。

ドライブセキュリティ属性を表示するには、[ハードウェア]ページに移動します。ドライブを選択し、*設定の表示*をクリックして、*詳細設定を表示*をクリックします。ドライブのロックが解除されている場合、ページの下部にある「読み取り/書き込みアクセス可能」属性の値は「*はい」です。読み取り/書き込みアクセス可能属性の値は*いいえ、ドライブがロックされている場合は無効なセキュリティキー*です。セキュリティキーをインポートすることで、セキュアドライブのロックを解除できます（メニュー：[設定][システム]>[セキュアドライブのロック解除]に進みます）。

[[IDa2e2942479bb04029eea0dca310b9859]]
= セキュリティキーを検証するときは、どのような点に注意する必要がありますか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
セキュリティキーを作成したら、キーファイルを検証して破損していないことを確認する必要があります。

検証に失敗した場合は、次の手順を実行します。

*
セキュリティキー識別子がコントローラ上の識別子と一致しない場合は、正しいセキュリティキーファイルを探して検証をやり直してください。
*
コントローラが検証用のセキュリティキーを復号化できない場合は、パスフレーズが正しく入力されていない可能性があります。パスフレーズを再確認し、必要に応じて再入力してから、もう一度検証を実行してください。エラーメッセージが再び表示される場合は、キーファイルのバックアップ（存在する場合）を選択して検証を再試行してください。
*
それでもセキュリティキーを検証できない場合は、元のファイルが破損している可能性があります。キーの新しいバックアップを作成し、そのコピーを検証してください。

[[IDc3264c177de77f51c081486b0e280d02]]
= 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。
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

:leveloffset: -1

:leveloffset: -1

```
= アクセス管理

:leveloffset: +1


[[ID841fe30cad2c09a65e27318877791b39]]
= アクセス管理の概要
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
アクセス管理は、System Managerでユーザ認証を確立する手段の1つです。



== どのような認証方式を使用できますか。

認証方式には、ロールベースアクセス制御（RBAC）、ディレクトリサービス、およびSecurity Assertion Markup Language（SAML）があります。

* *RBAC/ローカルユーザーロール*--ストレージアレイに適用される
RBAC機能を使用して認証を管理しますローカルユーザロールには、事前定義されたユーザプロファイルと、特定のアクセス権限を持つロールが含まれます。
* *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)を介して認証を管理します
* *saml *-- SAML 2.0を使用して、アイデンティティプロバイダ（IdP）を介して認証を管理します。


詳細：

* xref:{relative_path}how-access-management-works.html["アクセス管理の仕組み"]
* xref:{relative_path}access-management-terminology.html["アクセス管理の用語"]
* xref:{relative_path}permissions-for-mapped-roles.html["マッピングされたロールの権限"]
* xref:{relative_path}access-management-with-local-user-roles.html["ローカルユーザロール"]
* xref:{relative_path}access-management-with-directory-services.html["ディレクトリサービス"]
* xref:{relative_path}access-management-with-saml.html["SAML"]
```

== 認証を設定するにはどうすればよいですか。

ストレージアレイは、ローカルユーザロールを使用するように事前に設定されています。これはRBAC機能の実装です。別の方法を設定する場合は、[設定][アクセス管理]メニューに移動します。

詳細：

* xref:{relative_path}add-directory-server.html["LDAPディレクトリサーバを追加する"]
* xref:{relative_path}configure-saml.html["SAMLの設定"]

== 関連情報

アクセス管理に関連するタスクの詳細については、以下を参照してください。

* xref:{relative_path}change-passwords.html["パスワードの変更"]
* xref:{relative_path}view-audit-log-activity.html["監査ログアクティビティの表示"]
* xref:{relative_path}configure-syslog-server-for-audit-logs.html["監査ログ用のsyslogサーバの設定"]

= 概念

:leveloffset: +1

[[ID31490731f84fdec14233c19f683f3ba9]]
= アクセス管理の仕組み
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセス管理は、System Managerでユーザ認証を確立する手段の1つです。

設定とユーザ認証は次のように機能します。

. Security Adminの権限を含むユーザプロファイルでSystem Managerにログインします。
+
[NOTE]
====
初回ログイン時は、ユーザ名が `admin`自動的に表示され、変更することはできません。
`admin`ユーザには、システム内のすべての機能へのフルアクセス権が付与されます。

====
.
ユーザインターフェイスでアクセス管理に移動します。ストレージアレイはローカルユーザロールを使用するように事前に設定されています。これはロールベースアクセス制御（RBAC）機能の実装です。
. 管理者は、次の認証方式を1つ以上設定します。
+
** *ローカルユーザーの役割*--ストレージアレイに適用されるRBAC機能を使用して認証を管理しますローカルユーザロールには、事前定義されたユーザプロファイルと、特定のアクセス権限を持つロールが含まれます。管理者は、これらのローカルユーザロールを単一の認証方式として使用することも、ディレクトリサービスと組み合わせて使用することもできます。ユーザのパスワードを設定する以外、設定は必要ありません。
** *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)を介して認証を管理します管理者がLDAPサーバに接続し、ストレージアレイに組み込まれているローカルユーザロールにLDAPユーザをマッピングします。
** *saml *-- Security Assertion Markup Language（SAML）2.0を使用してアイデンティティプロバイダ（IdP）を介して認証を管理します。管理者がIdPシステムとストレージアレイの間の通信を確立し、ストレージアレイに組み込まれているローカルユーザロールにIdPユーザをマッピングします。

. ユーザにSystem Managerのログインクレデンシャルを渡します。
. ユーザが自身のクレデンシャルを入力してシステムにログインします。
+
[NOTE]
====
認証がSAMLとシングルサインオン（SSO）で管理されている場合は、System Managerのログインダイアログが省略されることがあります。

====
+
ログイン中、システムは次のバックグラウンドタスクを実行します。

+
** ユーザアカウントに対してユーザ名とパスワードを認証します。
** 割り当てられたロールに基づいてユーザの権限を決定します。
** ユーザインターフェイスのタスクにユーザがアクセスできるようにします。
** インターフェイスの右上にユーザ名が表示されます。

== System Managerで実行できるタスク

タスクへのアクセス権は、ユーザに割り当てられている次のロールによって異なります。

* * Storage admin *--
ストレージ・オブジェクト（ボリュームやディスク・プールなど）への読み取り/書き込みのフル・アクセス。セキュリティ構成へのアクセスはありません。
* * Security admin *--
アクセス管理、証明書管理、監査ログ管理のセキュリティ構成へのアクセス、および従来の管理インターフェイス（SYMbol）のオン/オフの切り替え機能。
* * Support admin *--ストレージアレイのすべてのハードウェアリソース、障害データ、MELイベント、およびコントローラファームウェアアップグレードへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
* *Monitor *--
すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

使用できないタスクは、ユーザインターフェイスではグレー表示されるか、非表示になります。たとえば、Monitorロールを持つユーザは、ボリュームに関するすべての情報を表示できますが、そのボリュームを変更するための機能にはアクセスできません。[サービスのコピー*（Copy Services *）]や[ワークロードに追加（Add to Workload *）]などの機能のタブはぼかし表示され、[設定の表示/編集（View / Edit Settings）]のみが使用できます。

== Unified ManagerとStorage Managerの制限事項

ストレージアレイにSAMLが設定されている場合、ユーザはそのアレイのストレージをUnified Managerや従来のStorage Managerインターフェイスから検出または管理することはできません。

ローカルユーザロールとディレクトリサービスが設定されている場合、次のいずれかの機能を実行する前にクレデンシャルを入力する必要があります。

* ストレージアレイの名前変更
* コントローラファームウェアのアップグレード
* ストレージアレイの構成のロード
* スクリプトの実行
* 未使用のセッションがタイムアウトしたときにアクティブな処理を実行しようとしています

```
[[IDf6d3adcd89758a029f6daef93cc78e4e]]
= アクセス管理の用語
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
ストレージアレイに関連するアクセス管理の用語を次に示します。

[cols="25h,~"]
|===
| 期間 | 製品説明


 a|
アクセストークン
 a|
アクセストークンは、ユーザ名とパスワードの代わりにREST
APIまたはコマンドラインインターフェイス（CLI）での認証に使用されます。トークンは特定のユーザ（LDAPユーザを含む）に関連付けられ、一連の権限と有効期限が含まれます。



 a|
Active Directory
 a|
Active Directory（AD）は、Windowsドメインネットワーク用にLDAPを使用する
Microsoftのディレクトリサービスです。



 a|
バインド
 a|
バインド操作は、ディレクトリサーバに対してクライアントを認証するために使用されます。通常はアカウントとパスワードのクレデンシャルが必要ですが、匿名のバインド処理が可能なサーバもあります。



 a|
```

カリフォルニア州
a|
認証局（CA）は、インターネットセキュリティのためにデジタル証明書と呼ばれる電子ドキュメントを発行する信頼されたエンティティです。証明書でWebサイトの所有者を識別することにより、クライアントとサーバの間のセキュアな接続が確立されます。

a|
証明書
a|
証明書はセキュリティ上の目的でサイトの所有者を識別するもので、攻撃者による偽装を防止します。証明書には、サイトの所有者に関する情報と、この情報を証明（署名）する信頼されたエンティティのIDが含まれています。

a|
IdP
a|
アイデンティティプロバイダ（IdP）は、ユーザにクレデンシャルを要求して認証されたユーザかどうかを確認するために使用される外部のシステムです。多要素認証を提供し、Active Directoryなどの任意のユーザデータベースを使用するようにIdPを設定できます。IdPの保守はセキュリティチームが行います。

a|
LDAP
a|
Lightweight Directory Access Protocol（
LDAP）は、分散されたディレクトリ情報サービスにアクセスして管理するためのアプリケーションプロトコルです。このプロトコルを使用すると、さまざまなアプリケーションやサービスをLDAPサーバに接続してユーザを検証できます。

a|
RBAC
a|
ロールベースアクセス制御（RBAC）は、個 々
のユーザのロールに基づいてコンピュータリソースまたはネットワークリソースへのアクセスを制御する方法です。ストレージアレイにはRBACが適用され、事前定義されたロールが含まれます。

a|

SAML
 a|
Security Assertion Markup Language（SAML）は、
2つのエンティティ間の認証と許可に使用されるXMLベースの標準規格です。SAMLでは多要素認証が可能で、ユーザはIDを証明するために2つ以上の項目（パスワードやフィンガープリントなど）を指定する必要があります。ストレージアレイに組み込まれているSAML機能は、アイデンティティのアサーション、認証、および許可に関してSAML2.0に準拠しています。

 a|
SP
 a|
サービスプロバイダ（SP）は、ユーザの認証とアクセスを制御するシステムです。アクセス管理にSAMLが設定されている場合、ストレージアレイはアイデンティティプロバイダに認証を要求するサービスプロバイダとして機能します。

 a|
SSO
 a|
シングルサインオン（SSO）は、1組のログインクレデンシャルで複数のアプリケーションにアクセスできるようにする認証サービスです。

|===

[[ID7fc0beb805ed8b916bc9a10727c01e46]]
= マッピングされたロールの権限
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ストレージアレイに適用されたロールベースアクセス制御（RBAC）機能には、1つ以上のロールがマッピングされた事前定義されたユーザプロファイルが含まれています。各ロールには、System Managerのタスクにアクセスするための権限が含まれています。

ユーザプロファイルとマッピングされたロールには、どちらかのSystem Managerのユーザインターフェイスで設定（Access Management >ローカルユーザロール）のメニューからアクセスできます。

各ロールは、次のタスクへのアクセスをユーザに提供します。

* * Storage admin *--
ストレージ・オブジェクト（ボリュームやディスク・プールなど）への読み取り/書き込みのフル・アクセス。セキュリティ構成へのアクセスはありません。
* * Security admin *--
アクセス管理、証明書管理、監査ログ管理のセキュリティ構成へのアクセス、および従来の管理インターフェイス（SYMbol）のオン/オフの切り替え機能。
* * Support admin *--ストレージアレイのすべてのハードウェアリソース、障害データ、MELイベント、およびコントローラファームウェアアップグレードへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
* *Monitor *--
すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

ユーザに特定のタスクに対する権限がない場合、そのタスクはグレー表示されるか、ユーザインターフェイスに表示されません。

[[ID7bc2be627dd5635182336b3c646fe2de]]
= ローカルユーザロールを使用したアクセス管理
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
管理者は、ストレージアレイに組み込みのロールベースアクセス制御（RBAC）機能をアクセス管理に使用できます。これらの機能は、「ローカルユーザロール」と呼ばれます。

== 設定ワークフロー

ローカルユーザロールはストレージアレイに対して事前に設定されています。認証にローカルユーザロールを使用するには、管理者は次の操作を実行します。

. Security Adminの権限を含むユーザプロファイルでSystem Managerにログインします。
+
[NOTE]
====
 `admin`ユーザには、システム内のすべての機能へのフルアクセス権が付与されます。

====

.
管理者がユーザプロファイルを確認します。ユーザプロファイルは事前に定義されており、変更できません。
. 必要に応じて、管理者は各ユーザプロファイルに新しいパスワードを割り当てます。
. ユーザは各自に割り当てられたクレデンシャルでシステムにログインします。

== 管理

認証にローカルユーザロールのみを使用する場合、管理者は次の管理タスクを実行できます。

* パスワードを変更します。
* パスワードの最小文字数を設定する。
* ユーザがパスワードなしでログインできるようにします。

[[ID28aaa0fc2207142e2f48c93760429dc8]]
= ディレクトリサービスを使用したアクセス管理
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
管理者は、Lightweight Directory Access Protocol（LDAP）サーバとディレクトリサービス（MicrosoftのActive Directoryなど）をアクセス管理に使用できます。

== 設定ワークフロー

ネットワークでLDAPサーバとディレクトリサービスが使用されている場合、設定は次のように機能します。

. Security Adminの権限を含むユーザプロファイルでSystem Managerにログインします。
+
[NOTE]
====
 `admin`ユーザには、システム内のすべての機能へのフルアクセス権が付与されます。

====

. LDAPサーバの設定を入力します。設定には、ドメイン名、
URL、バインドアカウント情報が含まれます。
. LDAPサーバでセキュアなプロトコル（LDAPS）を使用している場合は、
LDAPサーバとストレージアレイの間の認証に使用する認証局（CA）証明書チェーンをアップロードします。
.
サーバ接続が確立されると、ユーザグループをストレージアレイのロールにマッピングします。これらのロールは事前定義されており、変更することはできません。
. LDAPサーバとストレージアレイの間の接続をテストします。
. ユーザは、自分に割り当てられたLDAP
/ディレクトリサービスのクレデンシャルを使用してシステムにログインします。

== 管理

認証にディレクトリサービスを使用する場合、管理者は次の管理タスクを実行できます。

* ディレクトリサーバを追加します。
* ディレクトリサーバの設定を編集します。
* LDAPユーザをローカルユーザロールにマッピングします。
* ディレクトリサーバを削除します。

[[IDbcbd59f1335c1277d00ae15c78409fb6]]
= SAMLを使用したアクセス管理
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
管理者は、アレイに組み込みのSecurity Assertion Markup Language（SAML）
2.0の機能をアクセス管理に使用できます。

== 設定ワークフロー

SAMLの設定は次のように機能します。

. Security Adminの権限を含むユーザプロファイルでSystem Managerにログインします。
+

[NOTE]
====
この `admin`ユーザには、System Managerのすべての機能に対するフルアクセスが付与されます。

====
. 管理者は、[アクセス管理]の下の[*SAML *]タブに移動します。
. アイデンティティプロバイダ（IdP）との通信を設定します。
IdPは、ユーザにクレデンシャルを要求して認証されたユーザかどうかを確認するための外部システムです。ストレージアレイとの通信を設定するには、IdPシステムからIdPメタデータファイルをダウンロードし、System Managerを使用してそのファイルをストレージアレイにアップロードします。
. サービスプロバイダとIdPの間に信頼関係を確立します。サービスプロバイダはユーザ権限を制御します。このケースでは、ストレージアレイ内のコントローラがサービスプロバイダの役割を果たします。通信を設定するには、System Managerを使用して、各コントローラのサービスプロバイダメタデータファイルをエクスポートします。次に、IdPシステムからそれらのメタデータファイルをIdPにインポートします。
+
[NOTE]
====
また、認証時に名前IDを返す機能がIdPでサポートされていることを確認しておく必要があります。

====
. ストレージアレイのロールをIdPで定義されているユーザ属性にマッピングします。これを行うには、管理者はSystem Managerを使用してマッピングを作成します。
. IdP URLへのSSOログインをテストします。このテストでは、ストレージアレイとIdPが通信できることを確認します。
+
[CAUTION]
====
SAMLを有効にすると、ユーザインターフェイスで無効にしたり、IdP設定を編集したりすることはできなくなります。SAMLの設定を無効にしたり編集したりする必要がある場合は、テクニカルサポートにお問い合わせください。

====
. System Managerから、ストレージアレイのSAMLを有効にします。
. ユーザが自身のSSOクレデンシャルを使用してシステムにログインします。

== 管理

認証にSAMLを使用している場合、管理者は次の管理タスクを実行できます。

* 新しいロールマッピングを変更または作成する
* サービスプロバイダファイルのエクスポート

== アクセス制限

SAMLが有効になっている場合、ユーザはUnified Managerや従来のStorage Managerインターフェイスからそのアレイのストレージを検出または管理できません。

また、次のクライアントはストレージアレイのサービスとリソースにアクセスできません。

* Enterprise Management Window（EMW）
* コマンドラインインターフェイス（CLI）
* ソフトウェア開発キット（SDK）クライアント
* インバンドクライアント
* HTTPベーシック認証REST APIクライアント
* 標準のREST APIエンドポイントを使用したログイン

[[IDc48973a687e53085712b0b3c6e7c0a87]]
= アクセストオクン
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセストークンは、ユーザ名とパスワードを公開することなく、REST APIまたはコマンドラインインターフェイス（CLI）を使用した認証方法を提供します。トークンは特定のユーザ（LDAPユーザを含む）に関連付けられ、一連の権限と有効期限が含まれます。

== SAMLおよびJSON Webトークンアクセス

デフォルトでは、SAMLが有効になっているシステムでは、従来のコマンドラインツールへのアクセスは許可されません。MFAワークフローでは認証のためにアイデンティティプロバイダサーバへのリダイレクトが必要になるため、REST APIとCLIは実質的に動作しなくなります。そのため、System Managerでトークンを生成する必要があります。このトークンでは、MFAを使用してユーザを認証する必要があります。

NOTE: Webトークンを使用するために
SAMLを有効にする必要はありませんが、最高レベルのセキュリティを確保するためにSAMLを推奨します。

== トークンノサクセイトシヨウノワクフロ

. System Managerでトークンを作成し、有効期限を確認します。
.
トークンテキストをクリップボードにコピーするかファイルにダウンロードし、トークンテキストを安全な場所に保存します。
. トークンは次のように使用します。
+
** * REST API *：REST API要求でトークンを使用するには、要求に
HTTPヘッダーを追加します。例：
`Authorization: Bearer _<access-token-value>_`
** * Secure CLI *：
CLIでトークンを使用するには、コマンドラインでトークン値を追加するか、トークン値を含むファイルへのパスを使用します。例：
+
*** コマンドラインのトークン値： `-t _access-token-value_`
*** トークン値を含むファイルへのパス： `-T _access-token-file_`

詳細：

* xref:{relative_path}access-management-tokens-
create.html["アクセストークンの作成"]
* xref:{relative_path}access-management-tokens-
edit.html["アクセストークンの編集"]
* xref:{relative_path}access-management-tokens-
revoke.html["アクセストークンの取り消し"]

:leveloffset: -1

= ローカルユーザロールを使用する

```
:leveloffset: +1


[[IDb9ddc745232dbe9aab6acd321a56e84c]]
= ローカルユーザロールの表示
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
[ローカルユーザーの役割]タブでは、ユーザープロファイルとデフォルトの役割のマッピングを表示できます。これらのマッピングは、ストレージアレイに適用されるロールベースアクセス制御（RBAC）の一部です。

.開始する前に
Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。

.タスクの内容
ユーザプロファイルとマッピングは変更できません。変更できるのはパスワードのみです。

.手順
. メニューを選択します。Settings [Access Management]。
. [ローカルユーザー役割*（Local User Roles *）]タブを選択します。
+
ユーザプロファイルが表に表示されます。

+
** * Root admin *(admin)--
システム内のすべての機能にアクセスできるスーパー管理者。このユーザプロファイルにはすべてのロールが含まれています。
** * Storage admin *（storage）--
すべてのストレージプロビジョニングを担当する管理者。このユーザプロファイルには、Storage Admin、Support Admin、Monitorの各ロールが含まれています。
** * Security admin *（security）--
アクセス管理、証明書管理、セキュリティ有効ドライブ機能など、セキュリティ構成を担当するユーザー。このユーザプロファイルには、Security Adminと
Monitorの各ロールが含まれています。
** * Support admin*(support)--ハードウェアリソース'障害データ
'ファームウェアのアップグレードを担当するユーザーこのユーザプロファイルには、Support AdminとMonitorの各ロールが含まれています。
** *Monitor*(モニタ)--
```

システムへの読み取り専用アクセス権を持つユーザ。このユーザプロファイルにはMonitorロールのみが含まれています。

[[IDf1f50e301935e0f7bf8cb99ad1fe2209]]
= パスワードの変更
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセス管理で各ユーザプロファイルのユーザパスワードを変更できます。

.開始する前に
* Root Adminの権限が割り当てられたローカル管理者としてログインする必要があります。
* ローカル管理者のパスワードを確認しておく必要があります。

.タスクの内容
パスワードを選択する際は、次のガイドラインに注意してください。

* 新しいローカルユーザパスワードは、最小パスワードの現在の設定（[設定の表示/編集]）以上にする必要があります。
* パスワードは大文字と小文字が区別されます。
*
パスワードの末尾のスペースは削除されません。パスワードにスペースが含まれている場合は、スペースを含めるように注意してください。
* セキュリティを強化するために、
15文字以上の英数字を使用し、パスワードを頻繁に変更してください。

[NOTE]
====
System Managerでパスワードを変更すると、コマンドラインインターフェイス（CLI）のパスワードも変更されます。また、パスワードを変更すると、ユーザーのアクティブなセッションが終了します。

====
.手順
. メニューを選択します。Settings [Access Management]。

. [ローカルユーザー役割* （Local User Roles *）]タブを選択します。
. 表からユーザを選択します。
+
[パスワードの変更]ボタンが使用可能になります。

. [パスワードの変更 *] を選択します。
+
[パスワードの変更]ダイアログボックスが開きます。

.
ローカルユーザパスワードの最小文字数が設定されていない場合は、選択したユーザがストレージアレイにアクセスする際にパスワードの入力を必須にするチェックボックスをオンにして、選択したユーザの新しいパスワードを入力できます。
. ローカル管理者パスワードを入力し、* Change *をクリックします。

.結果
ユーザが現在ログインしている場合、パスワードを変更するとユーザのアクティブなセッションが終了します。

[[IDe7e3eb83f5eb0174bc0ec86ad9ac151f]]
= ローカルユーザのパスワード設定の変更
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ストレージアレイ上のすべての新規または更新されるローカルユーザパスワードに必要な最小文字数を設定できます。また、ローカルユーザにパスワードを入力せずにストレージアレイへのアクセスを許可することもできます。

.開始する前に
Root Adminの権限が割り当てられたローカル管理者としてログインする必要があります。

.タスクの内容
ローカルユーザパスワードの最小文字数を設定する際は、次のガイドラインに注意してください。

* 設定を変更しても、既存のローカルユーザパスワードには影響しません。
* ローカルユーザパスワードの最小文字数は0~30文字に設定する必要があります。
* 新しいローカルユーザパスワードは、現在の最小文字数の設定以上にする必要があります。
*
ローカルユーザがパスワードを入力せずにストレージアレイにアクセスできるようにする場合は、

パスワードの最小文字数を設定しないでください。

.手順
. メニューを選択します。Settings [Access Management]。
. [ローカルユーザー役割*（Local User Roles *）]タブを選択します。
. 「*表示/設定の編集*」ボタンを選択します。
+
[ローカルユーザーパスワードの設定]ダイアログボックスが開きます。

. 次のいずれかを実行します。
+
**
ローカルユーザがパスワードを入力せずにストレージアレイにアクセスできるようにするには、「すべてのローカルユーザパスワードを少なくとも必要とする」チェックボックスをオフにします。
**
すべてのローカルユーザパスワードに対してパスワードの最小文字数を設定するには、[Require all local user passwords to be at least]チェックボックスをオンにし、スピンボックスですべてのローカルユーザパスワードの最小文字数を設定します。
+
新しいローカルユーザパスワードは現在の設定以上にする必要があります。

. [保存（ Save ）] をクリックします。

:leveloffset: -1

= ディレクトリサービスを使用する

:leveloffset: +1

[[ID9337daab21b60f3632defcffa630bdd6]]
= LDAPディレクトリサーバを追加する
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセス管理用の認証を設定するには、ストレージアレイとLDAPサーバの間の通信を確立し、LDAPユーザグループをアレイの事前定義されたロールにマッピングします。

.開始する前に
* Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
* ユーザグループがディレクトリサービスに定義されている必要があります。
* LDAPサーバのクレデンシャルを確認しておく必要があります。ドメイン名とサーバのURLのほか、必要に応じてバインドアカウントのユーザ名とパスワードも指定できます。
* セキュアなプロトコルを使用するLDAPSサーバの場合は、LDAPサーバの証明書チェーンをローカルマシンにインストールする必要があります。

.タスクの内容
ディレクトリサーバの追加は、2つの手順で行います。最初にドメイン名とURLを入力します。サーバでセキュアなプロトコルを使用している場合は、認証用のCA証明書もアップロードする必要があります（標準の署名機関によって署名されている場合）。バインドアカウントのクレデンシャルがある場合は、ユーザアカウント名とパスワードも入力できます。次に、LDAPサーバのユーザグループをストレージアレイの事前定義されたロールにマッピングします。

[NOTE]
====
LDAPサーバを追加すると、従来の管理インターフェイスが無効になります。従来の管理インターフェイス（SYMbol）は、ストレージアレイと管理クライアントの間の通信方法です。無効にすると、ストレージアレイと管理クライアントはよりセキュアな通信方法（HTTPS経由のREST API）を使用します。

====
.手順
. メニューを選択します。Settings [Access Management]。
. [ディレクトリサービス]タブで、[*ディレクトリサーバーの追加*]を選択します。
+
[ディレクトリサーバーの追加]ダイアログボックスが開きます。

. [Server Settings]タブで、LDAPサーバのクレデンシャルを入力します。
+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 製品説明

 a|

構成設定

a|
ドメイン
a|
LDAPサーバのドメイン名を入力します。ドメインを複数入力する場合は、カンマで区切って入力します。ドメイン名は、ログイン（_username_@_domain_）で、認証するディレクトリサーバを指定するために使用されます。

a|
サーバURL
a|
LDAPサーバにアクセスするためのURLをの形式で入力し `ldap[s]://*host*:*port*`ます。

a|
証明書のアップロード（オプション）
a|

NOTE: このフィールドは、上記の[Server URL]フィールドで
LDAPSプロトコルが指定されている場合にのみ表示されます。

[*Browse*]をクリックして、アップロードするCA証明書を選択します。これは、LDAPサーバの認証に使用される信頼された証明書または証明書チェーンです。

a|
バインドアカウント（オプション）
a|
LDAPサーバに対する検索クエリおよびグループ内の検索に使用する読み取り専用ユーザアカウントを入力します。アカウント名はLDAPタイプの形式で入力します。たとえば、バインドユーザの名前が「bindacct」の場合は、「CN=bindacct、CN=Users、DC=cpoc、DC=local」のように入力します。

a|
バインドパスワード（オプション）
a|

NOTE: このフィールドは、上記のバインドアカウントを入力すると表示されます。

バインドアカウントのパスワードを入力します。

a|
追加する前にサーバ接続をテストする
a|
入力したLDAPサーバの設定でストレージアレイが通信できるようにするには、このチェックボックスをオンにします。このテストは、ダイアログボックスの下部にある*追加*（* Add *）をクリックした後に実行されます。このチェックボックスを選択してテストに失敗した場合、設定は追加されません。設定を追加するには、エラーを解決するか、チェックボックスを選択解除してテストをスキップする必要があります。

a|
権限の設定

a|
検索ベースDN
a|
ユーザを検索するLDAPコンテキストを入力します。通常はの形式で入力します `CN=Users, DC=cpoc, DC=local`。

a|
ユーザ名属性
a|
認証用のユーザIDにバインドされた属性を入力します。例： `sAMAccountName`。

a|
グループ属性
a|
グループとロールのマッピングに使用される、ユーザの一連のグループ属性を入力します。例： `memberOf, managedObjects`。

|===
====
. [**ロールマッピング**]タブをクリックします。
. 事前定義されたロールにLDAPグループを割り当てます。
1つのグループに複数のロールを割り当てることができます。

+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 製品説明

a|
マッピング

a|
グループDN
a|
マッピングするLDAPユーザグループの識別名（DN）を指定します。正規表現がサポートされています。(`\`正規表現パターンに含まれていない特殊な正規表現文字は、バックスラッシュでエスケープする必要があります。\.[]{}()<>*+-=!?^$|

a|
役割
a|
フィールド内をクリックし、グループDNにマッピングするストレージアレイのロールを1つ選択します。このグループに含めるロールをそれぞれ個別に選択する必要があります。MonitorロールはSANtricity System Managerにログインするため必要なロールであり、他のロールと一緒に指定する必要があります。各ロールの権限は次のとおりです。

** * Storage admin *--
ストレージ・オブジェクト（ボリュームやディスク・プールなど）への読み取り/書き込みのフル・アクセス。セキュリティ構成へのアクセスはありません。
** * Security admin *--
アクセス管理、証明書管理、監査ログ管理のセキュリティ構成へのアクセス、および従来の管理インターフェイス（SYMbol）のオン/オフの切り替え機能。
** * Support admin *--
ストレージアレイのすべてのハードウェアリソース、障害データ、MELイベント、およびコントローラファームウェアアップグレードへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
** *Monitor *--
すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

```
|===
====
+
[NOTE]
====
Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールがないユーザの場合、System Managerは正常に動作しません。

====
. 必要に応じて、*別のマッピングを追加
*をクリックして、グループとロールのマッピングをさらに入力します。
. マッピングが終了したら、*追加*をクリックします。
+
システムによって検証が実行され、ストレージアレイとLDAPサーバが通信できるかどうかが確認されます。エラーメッセージが表示された場合は、ダイアログボックスで入力したクレデンシャルを確認し、必要に応じて情報を再入力します。




[[IDdd50c337b5e7a9fb4898dffeb1962a80]]
= ディレクトリサーバの設定とロールマッピングの編集
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
アクセス管理でディレクトリサーバをすでに設定している場合は、その設定をいつでも変更できます。設定には、サーバ接続情報とグループとロールのマッピングが含まれます。

.開始する前に
* Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
* ディレクトリサーバを定義する必要があります。


.手順
. メニューを選択します。Settings [Access Management]。
. [*ディレクトリサービス*]タブを選択します。
. 複数のサーバが定義されている場合は、編集するサーバを表から選択します。
. 「*表示/設定の編集*」を選択します。
+
```

[ディレクトリサーバーの設定]ダイアログボックスが開きます。

. [サーバーの設定]タブで、目的の設定を変更します。
+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 製品説明

a|
構成設定

a|
ドメイン
a|
LDAPサーバのドメイン名。ドメインを複数入力する場合は、カンマで区切って入力します。ドメイン名は、ログイン（_username_@_domain_）で、認証するディレクトリサーバを指定するために使用されます。

a|
サーバURL
a|
LDAPサーバにアクセスするためのURL（の形式） `ldap[s]://host:port`。

a|
バインドアカウント（オプション）
a|
LDAPサーバに対する検索クエリおよびグループ内の検索に使用する読み取り専用ユーザアカウント。

a|
バインドパスワード（オプション）
a|
バインドアカウントのパスワード。（このフィールドは、バインドアカウントを入力すると表示されます）。

a|
保存する前にサーバ接続をテストする
a|
ストレージアレイがLDAPサーバと通信できるかどうかを確認します。このテストは、ダイアログボックスの下部にある*保存*（* Save
*）をクリックすると実行されます。このチェックボックスを選択してテストに失敗した場合、設定は変更されません。設定を編集するには、エラーを解決するか、チェックボックスを選択解除してテストをスキップする必要があります。

a|
権限の設定

a|
検索ベースDN
a|
ユーザを検索するLDAPコンテキスト。通常はの形式です。 `CN=Users, DC=cpoc, DC=local`

a|
ユーザ名属性
a|
認証用のユーザIDにバインドされた属性。例： `sAMAccountName`。

a|
グループ属性
a|
ユーザのグループ属性のリスト。グループとロールのマッピングに使用されます。例：
`memberOf, managedObjects`。

|===
====
. [Role Mapping]タブで、目的のマッピングを変更します。
+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===

| 設定 | 製品説明

a|
マッピング

a|
グループDN
a|
マッピングするLDAPユーザグループのドメイン名。正規表現がサポートされています。(`\`正規表現パターンに含まれていない特殊な正規表現文字は、バックスラッシュでエスケープする必要があります。\.[]{}()<>*+-=!?^$|

a|
役割
a|
グループDNにマッピングするストレージアレイのロール。このグループに含めるロールをそれぞれ個別に選択する必要があります。Monitorロールは SANtricity System Managerにログインするため必要なロールであり、他のロールと一緒に指定する必要があります。ストレージアレイのロールには次のものがあります。

** * Storage admin *--
ストレージ・オブジェクト（ボリュームやディスク・プールなど）への読み取り/書き込みのフル・アクセス。セキュリティ構成へのアクセスはありません。
** * Security admin *--
アクセス管理、証明書管理、監査ログ管理のセキュリティ構成へのアクセス、および従来の管理インターフェイス（SYMbol）のオン/オフの切り替え機能。
** * Support admin *--
ストレージアレイのすべてのハードウェアリソース、障害データ、MELイベント、およびコントローラファームウェアアップグレードへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
** *Monitor *--
すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

|===
====
+
[NOTE]
====
Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールがないユーザの場合、System Managerは正常に動作しません。

====
. 必要に応じて、*別のマッピングを追加
*をクリックして、グループとロールのマッピングをさらに入力します。
. [保存（ Save ）] をクリックします。

.結果
このタスクを完了すると、アクティブなユーザセッションはすべて終了します。現在のユーザーセッションのみが保持されます。

[[ID4986dd3d0c6f2994446133f6c93e29f6]]
= ディレクトリサーバの削除
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ディレクトリサーバとストレージアレイの間の接続を切断するには、[アクセス管理]ページでサーバ情報を削除します。このタスクは、新しいサーバを設定したあとに古いサーバを削除する場合に実行できます。

.開始する前に
Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。

.タスクの内容
このタスクを完了すると、アクティブなユーザセッションはすべて終了します。現在のユーザーセッションのみが保持されます。

.手順
. メニューを選択します。Settings [Access Management]。
. [*ディレクトリサービス*]タブを選択します。
. リストから、削除するディレクトリサーバを選択します。
. [削除（ Remove ）] をクリックします。
+
[ディレクトリサーバーの削除]ダイアログボックスが開きます。

. フィールドにと入力し `remove`、*[削除]*をクリックします。
+
ディレクトリサーバの構成設定、権限設定、およびロールのマッピングが削除されます。ユーザは

、このサーバのクレデンシャルを使用してログインできなくなります。

:leveloffset: -1

= SAMLを使用

:leveloffset: +1

[[ID4cb871b0456e1ab04556b9400fceacab]]
= SAMLの設定
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセス管理用の認証を設定するには、ストレージアレイに組み込みのSecurity Assertion Markup Language（
SAML）機能を使用できます。この設定により、アイデンティティプロバイダとストレージプロバイダの間の接続が確立されます。

.開始する前に
* Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
* ストレージアレイの各コントローラの
IPアドレスまたはドメイン名を確認しておく必要があります。
* IdP管理者がIdPシステムの設定を完了している必要があります。
* IdP管理者が、認証時に名前IDを返す機能が
IdPでサポートされていることを確認しておく必要があります。
* IdPサーバとコントローラのクロックを同期しておきます（
NTPサーバを使用するかコントローラのクロックの設定を調整します）。
* IdPのメタデータファイルをIdPシステムからダウンロードし、System
Managerへのアクセスに使用するローカルシステムで使用できるようにしておきます。

.タスクの内容
アイデンティティプロバイダ（IdP）は、ユーザにクレデンシャルを要求して認証されたユーザかどうかを確認するために使用される外部のシステムです。多要素認証を提供し、Active

Directoryなどの任意のユーザデータベースを使用するようにIdPを設定できます。IdPの保守はセキュリティチームが行います。サービスプロバイダ（SP）は、ユーザの認証とアクセスを制御するシステムです。アクセス管理にSAMLが設定されている場合、ストレージアレイはアイデンティティプロバイダに認証を要求するサービスプロバイダとして機能します。IdPとストレージアレイの間の接続を確立するには、この2つのエンティティ間でメタデータファイルを共有します。次に、IdPのユーザエンティティをストレージアレイのロールにマッピングします。最後に、接続とSSOログインをテストしたうえでSAMLを有効にします。

[NOTE]
====
* SAMLとディレクトリサービス
*。認証方式としてディレクトリサービスを使用するように設定されている状況でSAMLを有効にした場合、System ManagerではSAMLがディレクトリサービスよりも優先されます。
SAMLをあとで無効にすると、ディレクトリサービスの設定は以前の設定に戻ります。

====
[CAUTION]
====
*編集と無効化。*SAMLを有効にすると、ユーザインターフェイスで無効にしたり、IdP設定を編集したりすることはできなくなります。SAMLの設定を無効にしたり編集したりする必要がある場合は、テクニカルサポートにお問い合わせください。

====
SAML認証の設定は複数の手順で構成されます。

== 手順1：IdPのメタデータファイルをアップロードする

ストレージアレイにIdPの接続情報を提供するには、System Managerに
IdPのメタデータをインポートします。このメタデータは、IdPシステムが認証要求を正しいURLにリダイレクトし、受信した応答を検証するために必要です。コントローラが2台ある場合でも、アップロードするメタデータファイルはストレージアレイに対して1つだけです。

.手順
. メニューを選択します。Settings [Access Management]。
. SAML *タブを選択します。
+
設定手順の概要が表示されます。

. アイデンティティプロバイダ（IdP）ファイルのインポート*リンクをクリックします。
+
[Import Identity Provider File]ダイアログボックスが開きます。

. Browse *をクリックして、ローカルシステムにコピーした
IdPメタデータファイルを選択してアップロードします。
+

ファイルを選択すると、IdPのエンティティIDが表示されます。

. [* インポート *] をクリックします。

== 手順2：サービスプロバイダのファイルをエクスポートする

IdPとストレージアレイの間の信頼関係を確立するには、サービスプロバイダのメタデータをIdPにインポートします。このメタデータは、IdPがコントローラとの間の信頼関係を確立し、許可要求を処理するために必要になります。このファイルには、IdPがサービスプロバイダと通信できるように、コントローラのドメイン名やIPアドレスなどの情報が含まれています。

.手順
. [サービスプロバイダファイルのエクスポート*]リンクをクリックします。
+
[サービスプロバイダファイルのエクスポート]ダイアログボックスが開きます。

. コントローラのIPアドレスまたはDNS名を[*コントローラA *]フィールドに入力し、[*エクスポート]をクリックしてメタデータファイルをローカルシステムに保存します。ストレージアレイにコントローラが2台ある場合は、2台目のコントローラの* Controller B *フィールドでこの手順を繰り返します。
+
「*Export」をクリックすると、サービスプロバイダのメタデータがローカルシステムにダウンロードされます。ファイルが保存されている場所をメモします。

. ローカルシステムで、エクスポートしたサービスプロバイダメタデータファイルを探します。
+
コントローラごとにXML形式のファイルが1つあります。

.
IdPサーバから、サービスプロバイダのメタデータファイルをインポートして信頼関係を確立します。ファイルを直接インポートすることも、ファイルからコントローラの情報を手動で入力することもできます。

== 手順3：ロールをマッピングする

System Managerに対する許可とアクセスをユーザに提供するには、IdPユーザ属性とグループメンバーシップをストレージアレイの事前定義されたロールにマッピングする必要があります。

.開始する前に

* IdP管理者が、
IdPシステムでユーザ属性とグループメンバーシップを設定しておく必要があります。
* IdPのメタデータファイルをSystem Managerにインポートしておきます。
* 各コントローラのサービスプロバイダメタデータファイルを
IdPシステムにインポートして信頼関係を確立します。

.手順
. マッピングSystem Manager *の役割のリンクをクリックします。
+
ロールマッピング(Role Mapping)ダイアログボックスが開きます

. IdPユーザの属性とグループを事前定義されたロールに割り当てます。
1つのグループに複数のロールを割り当てることができます。
+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 製品説明

a|
マッピング

a|
ユーザ属性
a|
マッピングするSAMLグループの属性（「member of」など）を指定します。

a|
属性値
a|
マッピングするグループの属性値を指定します。正規表現がサポートされています。(`\`正規表現パターンに含まれていない特殊な正規表現文字は、バックスラッシュでエスケープする必要があります。\.[]{}()<>*+-=!?^$|

a|
役割
a|

フィールド内をクリックし、属性にマッピングするストレージアレイのロールを1つ選択します。含めるロールをそれぞれ個別に選択する必要があります。Monitorロールは System Managerにログインするため必要なロールであり、他のロールと一緒に指定する必要があります。少なくとも1つのグループにはSecurity Adminロールも必要です。

各ロールの権限は次のとおりです。

** * Storage admin *--
ストレージ・オブジェクト（ボリュームやディスク・プールなど）への読み取り/書き込みのフル・アクセス。セキュリティ構成へのアクセスはありません。
** * Security admin *--
アクセス管理、証明書管理、監査ログ管理のセキュリティ構成へのアクセス、および従来の管理インターフェイス（SYMbol）のオン/オフの切り替え機能。
** * Support admin *--
ストレージアレイのすべてのハードウェアリソース、障害データ、MELイベント、およびコントローラファームウェアアップグレードへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
** *Monitor *--
すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

|===
====
+
[NOTE]
====
Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールがないユーザの場合、System Managerは正常に動作しません。

====
. 必要に応じて、*別のマッピングを追加
*をクリックして、グループとロールのマッピングをさらに入力します。
+
[NOTE]
====
ロールのマッピングは、SAMLを有効にしたあとに変更できます。

====
. マッピングが終了したら、*保存*をクリックします。

== 手順4：SSOログインをテストする

IdPシステムとストレージアレイが通信できることを確認するために、必要に応じてSSOログインを

テストできます。このテストは、SAMLを有効にする最後の手順でも実行します。

.開始する前に
* IdPのメタデータファイルをSystem Managerにインポートしておきます。
* 各コントローラのサービスプロバイダメタデータファイルを
IdPシステムにインポートして信頼関係を確立します。

.手順
. [Test SSO Login*]リンクを選択します。
+
SSOクレデンシャルを入力するためのダイアログボックスが開きます。

. Security Adminと
Monitorの両方の権限を持つユーザのログインクレデンシャルを入力します。
+
ログインのテスト中は、ダイアログボックスが開きます。

. テストに成功したことを示すメッセージを確認します。テストに成功した場合は、
SAMLを有効にする次の手順に進みます。
+
テストが正常に完了しなかった場合は、エラーメッセージと詳細情報が表示されます。次の点を確認してください。

+
** ユーザがSecurity AdminとMonitorの権限を持つグループに属していること。
** アップロードしたIdPサーバのメタデータが正しいこと。
** SPメタデータファイル内のコントローラアドレスが正しい。

== 手順5：SAMLを有効にする

最後に、ユーザ認証用のSAMLの設定を完了します。このプロセスでは、SSOログインのテストも求められます。SSOログインのテストプロセスについては、前の手順で説明しています。

.開始する前に
* IdPのメタデータファイルをSystem Managerにインポートしておきます。
* 各コントローラのサービスプロバイダメタデータファイルを
IdPシステムにインポートして信頼関係を確立します。
* 少なくともMonitorロールとSecurity Adminロールを1つずつマッピングしておきます。

[CAUTION]

====
*編集と無効化。*SAMLを有効にすると、ユーザインターフェイスで無効にしたり、IdP設定を編集したりすることはできなくなります。SAMLの設定を無効にしたり編集したりする必要がある場合は、テクニカルサポートにお問い合わせください。

====
.手順
. [* SAML *]タブで、[* SAMLを有効にする]リンクを選択します。
+
[SAMLの有効化の確認]ダイアログボックスが開きます。

. と入力し `enable`、*[有効化]*をクリックします。
. SSOログインテスト用のユーザクレデンシャルを入力します。

.結果
SAMLが有効になると、アクティブなセッションはすべて終了され、SAMLを使用したユーザの認証が開始されます。

[[ID94d156f20cf89c556ac5ccd05dbe1ba5]]
= SAMLロールマッピングの変更
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセス管理用にSAMLを設定している場合は、IdPグループとストレージアレイの事前定義されたロールの間のロールマッピングを変更できます。

.開始する前に
* Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
* IdP管理者が、
IdPシステムでユーザ属性とグループメンバーシップを設定しておく必要があります。
* SAMLを設定して有効にします。

.手順
. メニューを選択します。Settings [Access Management]。
. SAML *タブを選択します。
. [*役割のマッピング*]を選択します。

+
ロールマッピング(Role Mapping)ダイアログボックスが開きます

. IdPユーザの属性とグループを事前定義されたロールに割り当てます。
1つのグループに複数のロールを割り当てることができます。
+
[CAUTION]
====
SAMLが有効になっているときは権限を削除しないように注意してください。削除すると、System Managerにアクセスできなくなります。

====
+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 製品説明

a|
マッピング

a|
ユーザ属性
a|
マッピングするSAMLグループの属性（「member of」など）を指定します。

a|
属性値
a|
マッピングするグループの属性値を指定します。

a|
役割
a|
フィールド内をクリックし、属性にマッピングするストレージアレイのロールを1つ選択します。このグループに含めるロールをそれぞれ個別に選択する必要があります。Monitorロールは System Managerにログインするため必要なロールであり、他のロールと一緒に指定する必要があります。
少なくとも1つのグループにSecurity

Adminロールを割り当てる必要があります。各ロールの権限は次のとおりです。

** * Storage admin *--
ストレージ・オブジェクト（ボリュームやディスク・プールなど）への読み取り/書き込みのフル・アクセス。セキュリティ構成へのアクセスはありません。
** * Security admin *--
アクセス管理、証明書管理、監査ログ管理のセキュリティ構成へのアクセス、および従来の管理インターフェイス（SYMbol）のオン/オフの切り替え機能。
** * Support admin *--
ストレージアレイのすべてのハードウェアリソース、障害データ、MELイベント、およびコントローラファームウェアアップグレードへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
** *Monitor *--
すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

|===
====
+

NOTE: Monitorロールは、管理者を含むすべてのユーザに必要です。
Monitorロールがないユーザの場合、System Managerは正常に動作しません。

. 必要に応じて、* Add another mapping
*をクリックして、グループとロールのマッピングをさらに入力します。
. [保存（ Save ）] をクリックします。

.結果
このタスクを完了すると、アクティブなユーザセッションはすべて終了します。現在のユーザーセッションのみが保持されます。

[[ID7973c749dc104e972ea098e0b36c3d63]]
= SAMLサービスプロバイダファイルのエクスポート
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
必要に応じて、ストレージアレイのサービスプロバイダメタデータをエクスポートし、ファイルをアイデンティティプロバイダ（IdP）システムに再インポートできます。

.開始する前に
* Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
* SAMLを設定して有効にします。

.タスクの内容
このタスクでは、コントローラからメタデータ（コントローラごとに1ファイル）をエクスポートします。このメタデータは、IdPがコントローラとの間の信頼関係を確立し、認証要求を処理するために必要になります。このファイルには、コントローラのドメイン名やIPアドレスなど、IdPで要求の送信に使用できる情報が含まれています。

.手順
. メニューを選択します。Settings [Access Management]。
. SAML *タブを選択します。
. 「*書き出し*」を選択します。
+
[サービスプロバイダファイルのエクスポート]ダイアログボックスが開きます。

. 各コントローラについて、* Export（エクスポート）
*をクリックしてメタデータファイルをローカルシステムに保存します。
+
[NOTE]
====
各コントローラのドメイン名フィールドは読み取り専用です。

====
+
ファイルが保存されている場所をメモします。

. ローカルシステムで、エクスポートしたサービスプロバイダメタデータファイルを探します。
+
コントローラごとにXML形式のファイルが1つあります。

.
IdPサーバから、サービスプロバイダのメタデータファイルをインポートします。ファイルを直接インポートすることも、ファイルからコントローラ情報を手動で入力することもできます。
. [* 閉じる *] をクリックします。

:leveloffset: -1

= アクセストークンの使用

:leveloffset: +1

[[ID53084b3fb417ecaaac276eabf4e5e6a3]]
= アクセストークンの作成
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ユーザ名とパスワードの代わりにREST APIまたはコマンドラインインターフェイス（CLI）で認証するアクセストークンを作成できます。

NOTE: トークンにはパスワードがないため、慎重に管理する必要があります。

.手順
. メニューを選択します。Settings [Access Management]。
. [* Access Tokens *] タブを選択します。
. [アクセストークン設定の表示/編集]を選択します。ダイアログボックスで、*アクセストークンを有効にする*チェックボックスが選択されていることを確認します。[保存（Save）]をクリックして、ダイアログボックスを閉じます。
. [アクセストークンの作成*]を選択します。
. ダイアログボックスで、トークンの有効期間を選択します。
+

NOTE: トークンの有効期限が切れると、ユーザーの認証は失敗します。

. [* 作成 .*] をクリックします
. ダイアログボックスで、次のいずれかを選択します。
+
** *コピー*をクリックしてトークンテキストをクリップボードに保存します。
** *ダウンロード*：トークンテキストをファイルに保存します。
+

NOTE:
トークンテキストは必ず保存してください。これは、ダイアログを閉じる前にテキストを表示する唯一の機会です。

. [* 閉じる *] をクリックします。

. トークンは次のように使用します。
+
** * REST API *：REST API要求でトークンを使用するには、要求に
HTTPヘッダーを追加します。例：
`Authorization: Bearer _<access-token-value>_`
** * Secure CLI *：
CLIでトークンを使用するには、コマンドラインでトークン値を追加するか、トークン値を含むファイルへのパスを使用します。例：
+
*** コマンドラインのトークン値： `-t _access-token-value_`
*** トークン値を含むファイルへのパス： `-T _access-token-file_`
+

NOTE: ユーザ名、パスワード、またはトークンが指定されていない場合、
CLIはコマンドラインでアクセストークン値の入力をユーザに要求します。

[[ID23166c40463b85d8497e1b820c432429]]
= アクセストークン設定の編集
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
有効期限や新しいトークンを作成する機能など、アクセストークンの設定を編集できます。

.手順
. メニューを選択します。Settings [Access Management]。
. [* Access Tokens *] タブを選択します。
. [アクセストークン設定の表示/編集]を選択します。
. ダイアログボックスでは、次のいずれかまたは両方のタスクを実行できます。
+
** トークンの作成を有効または無効にします。
** 既存のトークンの有効期限を変更します。
+

NOTE: [*アクセストークンを有効にする

*]設定をオフにすると、トークンの作成とトークン認証の両方が無効になります。後でこの設定を再度有効にすると、期限切れになっていないトークンを再利用できます。既存のトークンをすべて完全に無効にする場合は、を参照してくださいlink:access-management-tokens-revoke.html["アクセストークンの取り消し"]。

. [保存（ Save ）] をクリックします。

[[IDe1a2be0ef8d820a1c1893cc0f4c676cd]]
= アクセストークンの取り消し
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
トークンが侵害されたと判断した場合、またはアクセストークンの署名と検証に使用する暗号キーに対して手動でキーローテーションを実行する場合は、すべてのアクセストークンを取り消すことができます。

この操作では、トークンに署名するために使用されるキーが再生成されます。キーをリセットすると、_ALL_Issuedトークンがただちに無効になります。ストレージアレイはトークンを追跡しないため、個 々 のトークンを取り消すことはできません。

.手順
. メニューを選択します。Settings [Access Management]。
. ［* Access Tokens *］タブを選択します。
. 「* Revoke all Access Tokens（すべてのアクセストークンを無効にする
. ダイアログボックスで、*はい*をクリックします。

すべてのトークンを取り消した後、新しいトークンを作成してすぐに使用できます。

:leveloffset: -1

= syslogの管理

:leveloffset: +1

```
[[ID0652c690636b62a0f2448a2a777b3c1a]]
= 監査ログアクティビティの表示
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Security
Admin権限を持つユーザは、監査ログを表示することで、ユーザ操作、認証エラー、無効なログイン試行、およびユーザセッションの期間を監視できます。

.開始する前に
Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。

.手順
. メニューを選択します。Settings [Access Management]。
. [**監査ログ**]タブを選択します。
+
監査ログアクティビティが表形式で表示され、次の列の情報が表示されます。

+
** *日付/時刻*--ストレージアレイがイベントを検出した日時（GMT）のタイムスタンプ
** *ユーザー名*--
イベントに関連付けられたユーザー名。ストレージアレイに対する認証されていない操作については、ユーザ名として「N/A」と表示されます。認証されていないアクションは、内部プロキシまたはその他のメカニズムによってトリガーされる可能性があります。
** *ステータスコード*--操作のHTTPステータスコード(200、400など
)およびイベントに関連する説明テキスト。
** *URLアクセス*--完全なURL (ホストを含む)とクエリ文字列。
** *クライアントIPアドレス*--イベントに関連付けられたクライアントのIPアドレス。
** *Source*--イベントに関連付けられたロギングソース。System Manager、CLI、
Webサービス、またはサポートシェルがあります。
** *概要 *--イベントに関する追加情報 （該当する場合）。


. イベントを表示および管理するには、[Audit Log]ページの選択項目を使用します。
+
.選択の詳細
[%collapsible]
====
```

```
[cols="25h,~"]
|===
| 選択 | 製品説明


 a|
イベントを表示する期間を選択...
 a|
表示されるイベントを日付範囲（過去24時間、過去7日間、過去30日間、またはカスタムの日付範囲）で制限します。




 a|
フィルタ
 a|
表示されるイベントをフィールドに入力した文字で限定します。単語を完全に一致させるには引用符（""）を使用します。1つ以上の単語を返すにはと入力します。
`OR`単語を省略するにはダッシュ（--）を入力します。




 a|
更新する
 a|
最新のイベントにページを更新するには、「*更新*」を選択します。




 a|
設定の表示/編集
 a|
［*表示/設定の編集*］を選択すると、ログに記録するフルログポリシーとアクションのレベルを指定できるダイアログボックスが開きます。




 a|
イベントの削除
 a|
「*削除*」を選択すると、ページから古いイベントを削除できるダイアログボックスが開きます。




 a|
列の表示/非表示
 a|
```

[列の表示/非表示（Show/Hide * Column）]アイコンをクリックしimage:../media/sam-1140-ss-access-
columns.gif[""]て、テーブルに表示する追加の列を選択します。追加の列は次のとおりです。

** *メソッド*-- HTTPメソッド(POST、GET、削除など)。
** *CLIコマンド実行*-- Secure CLI要求に対して実行されるCLIコマンド(文法)。
** *CLI戻りステータス*--
CLIステータスコードまたはクライアントからの入力ファイルの要求。
** *SYMBOL手順 *--実行されたSYMBOL手順 。
** *SSH Event Type *-- Secure Shell (SSH)イベントのタイプ(
ログイン、ログアウト、login_failなど)
** *SSHセッションPID *-- SSHセッションのプロセスID番号。
** *SSHセッション期間*--ユーザーがログインした秒数
** *認証タイプ*--ローカルユーザー、LDAP、
SAML、およびアクセストークンを含むことができます。
** *認証ID *--認証されたセッションのID。

a|
列フィルタの切り替え
a|
[切り替え]アイコンをクリックするimage:../media/sam-1140-ss-access-
toggle.gif[""]と、各列のフィルタリングフィールドが開きます。表示されるイベントを制限するには、列フィールドに文字を入力します。フィルタリングフィールドを閉じるには、アイコンをもう一度クリックします。

a|
変更を元に戻す
a|
[元に戻す（Undo）]アイコンをクリックしimage:../media/sam-1140-ss-access-
undo.gif[""]て、テーブルをデフォルトの構成に戻します。

a|
エクスポート
a|
[*Export*]をクリックして、テーブルデータをカンマ区切り値（CSV）ファイルに保存します。

|===
====

```
[[ID8fc4f9f02466b51a3552b8964737bb3e]]
= 監査ログポリシーの定義
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
上書きポリシーや監査ログに記録するイベントのタイプを変更することができます。

.開始する前に
Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。

.タスクの内容
このタスクでは、古いイベントを上書きするポリシーやイベントタイプを記録するポリシーなど、監査ログ設定を変更する方法について説明します。

.手順
. メニューを選択します。Settings [Access Management]。
. [*監査ログ*]タブを選択します。
. 「*表示/設定の編集*」を選択します。
+
[監査ログの設定]ダイアログボックスが開きます。

. 上書きポリシーや記録するイベントのタイプを変更します。
+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 製品説明


 a|
上書きポリシー
 a|
最大容量に達したときに古いイベントを上書きするポリシーを決定します。

** *監査ログがいっぱいになったらイベントを古いものから上書きする*-監査ログが50、000レコードに達したときに古いイベントを上書きします。
```

** *監査ログのイベントを手動で削除する必要があります*-
イベントが自動的に削除されないように指定します。設定した割合に達した場合、しきい値の警告が表示されます。イベントは手動で削除する必要があります。
+

NOTE: 上書きポリシーを無効にした場合、監査ログのエントリが上限に達すると、Security Adminの権限がないユーザによるSystem Managerへのアクセスは拒否されます。Security Adminの権限がないユーザにシステムアクセスをリストアするには、Security Adminロールに割り当てられたユーザが古いイベントレコードを削除する必要があります。

+

NOTE: 上書きポリシーは、監査ログをsyslogサーバにアーカイブするように設定されている場合は適用されません。

a|
ログに記録するアクションのレベル
a|
ログに記録するイベントのタイプを指定します。

** *変更イベントのみを記録する*--
ユーザーの操作によってシステムに変更が発生するイベントのみを記録します
** *すべての変更イベントと読み取り専用イベントを記録する*--
情報の読み取りまたはダウンロードを伴うユーザー操作を含むすべてのイベントを記録します

|===
====
. [保存（ Save ）] をクリックします。

[[ID70fdcb9c38c195889c63b3d3dead1829]]
= 監査ログからのイベントの削除
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]

監査ログの古いイベントをクリアすることができます。これにより、イベントの検索が容易になります。削除時に古いイベントをCSV（カンマ区切り値）ファイルに保存することもできます。

.開始する前に
Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。

.手順
. メニューを選択します。Settings [Access Management]。
. [*監査ログ*]タブを選択します。
. 「 * 削除」を選択します。
+
Delete Audit Logダイアログボックスが開きます。

. 削除する古いイベントの数を選択または入力します。
. 削除したイベントを
CSVファイルにエクスポートする場合は、チェックボックスを選択したままにします（推奨）。次の手順で*削除*をクリックすると、ファイル名と場所の入力を求められます。イベントをCSVファイルに保存しない場合は、チェックボックスをクリックして選択を解除します。
. [削除（ Delete ）] をクリックします。
+
確認のダイアログボックスが開きます。

. フィールドにと入力し `delete`、*[削除]*をクリックします。
+
最も古いイベントが[Audit Log]ページから削除されます。

[[ID77a8980fe75f4e1f60428e118a3c0a20]]
= 監査ログ用のsyslogサーバの設定
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
監査ログを外部syslogサーバにアーカイブする場合は、そのサーバとストレージアレイの間の通信を設定できます。接続が確立されると、監査ログはsyslogサーバに自動的に保存されます。

.開始する前に
* Security

Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
*
syslogサーバのアドレス、プロトコル、およびポート番号を確認しておく必要があります。サーバアドレスには、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスを使用できます。
* サーバでセキュアなプロトコル（
TLSなど）を使用している場合は、ローカルシステムに認証局（CA）証明書がある必要があります。CA証明書はWebサイトの所有者を識別し、サーバとクライアントの間のセキュアな接続を確立します。

.手順
. メニューを選択します。Settings [Access Management]。
. 監査ログタブで、*Configure Syslog Servers *を選択します。
+
Configure Syslog Serversダイアログボックスが開きます。

. [追加]*をクリックします。
+
[Add Syslog Server]ダイアログボックスが開きます。

. サーバーの情報を入力し、*追加*をクリックします。
+
** *サーバーアドレス*--完全修飾ドメイン名、IPv4アドレス、または
IPv6アドレスを入力します。
** *Protocol*--ドロップダウンリストからプロトコル(TLS、UDP、TCPなど)を選択します。
** *証明書のアップロード（オプション）*-- TLSプロトコルを選択して署名済み
CA証明書をまだアップロードしていない場合は、[*参照]をクリックして証明書ファイルをアップロードします。監査ログは、信頼された証明書がないとsyslogサーバにアーカイブされません。
+
[NOTE]
====
あとで証明書が無効になると、TLSハンドシェイクは失敗します。その結果、監査ログにエラーメッセージが記録され、syslogサーバにメッセージが送信されなくなります。この問題
を解決するには、syslogサーバで証明書を修正してから、メニューの[設定]、[監査ログ]、[syslogサーバの設定]、[すべてテスト]の順に選択します。

====
** *ポート*-- syslogレシーバーのポート番号を入力します。[Add *]
をクリックすると、[Configure Syslog Servers]
ダイアログボックスが開き、設定したsyslogサーバがページに表示されます。

. ストレージアレイとのサーバ接続をテストするには、「*すべてテスト」を選択します。

.結果

設定が完了すると、以降すべての監査ログがsyslogサーバに送信されるようになります。以前のログは転送されません。アラートのsyslog設定の詳細については、を参照してください
https://docs.netapp.com/us-en/e-series-santricity/sm-settings/configure-syslog-server-for-alerts.html["アラート用のsyslogサーバの設定"]。

 NOTE: If multiple syslog servers are configured, all configured syslog servers will receive an audit log.

[[ID477992bec987056b3817fd1a143d9a93]]
= 監査ログレコードのsyslogサーバ設定の編集
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
監査ログのアーカイブに使用するsyslogサーバの設定を変更できます。また、サーバ用の新しい認証局（CA）証明書をアップロードすることもできます。

.開始する前に
* Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
* syslogサーバのアドレス、プロトコル、およびポート番号を確認しておく必要があります。サーバアドレスには、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスを使用できます。
* 新しいCA証明書をアップロードする場合は、ローカルシステムに証明書がある必要があります。

.手順
. メニューを選択します。Settings [Access Management]。
. 監査ログタブで、*Configure Syslog Servers *を選択します。
+
設定されているsyslogサーバがページに表示されます。

. サーバ情報を編集するには、サーバ名の右側にある* Edit *（鉛筆）アイコンを選択し、次のフィールドで必要な変更を行います。
+
** *サーバーアドレス*--完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスを入力します。
** *Protocol*--ドロップダウンリストからプロトコル(TLS、UDP、TCPなど)を選択します。
** *ポート*-- syslogレシーバーのポート番号を入力します。

. （UDPまたはTCPから）プロトコルをセキュアTLSプロトコルに変更した場合は、[*Import Trusted Certificate*]をクリックしてCA証明書をアップロードします。
. ストレージアレイとの新しい接続をテストするには、「*すべてテスト」を選択します。

.結果
設定が完了すると、以降すべての監査ログがsyslogサーバに送信されるようになります。以前のログは転送されません。

:leveloffset: -1

= FAQ

:leveloffset: +1

[[ID61f1109525a99e5ac423a3e92dbacd72]]
= ログインできないのはなぜですか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
System Managerにログインする際にエラーが表示される場合は、次の問題がないか確認してください。

System Managerのログインエラーは、次のいずれかが原因の可能性があります。

* 入力したユーザ名またはパスワードが正しくありません。
* Privilegesが不十分です。
*
ディレクトリサーバ（設定されている場合）が使用できない可能性があります。その場合は、ローカルユーザロールでログインしてみてください。
* ログインに何度も失敗したため、ロックアウトモードがトリガーされました。
10分待ってから再ログインしてください。
*
ロックアウト状態がトリガーされ、監査ログがいっぱいになっている可能性があります。アクセス管理に移動し、監査ログから古いイベントを削除します。
* SAML認証が有効になりました。ブラウザの表示を更新してログインします。

ミラーリングタスクでリモートストレージアレイにログインエラーが発生する原因は次のいずれかです。

* 入力したパスワードが正しくありません。
* ログインに何度も失敗したため、ロックアウトモードがトリガーされました。
10分待ってから再度ログインしてください。
*
コントローラで使用されているクライアント接続の最大数に達しました。複数のユーザまたはクライアントがないかどうかを確認します。

[[ID695f7c993fb8a7ed7a9fcd7c75ae716f]]
= ディレクトリサーバを追加するときは、どのような点に注意する必要がありますか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセス管理でディレクトリサーバを追加する前に、次の要件を満たしていることを確認してください。

* ユーザグループがディレクトリサービスに定義されている必要があります。
* LDAPサーバのクレデンシャルを確認しておく必要があります。ドメイン名とサーバのURLのほか、必要に応じてバインドアカウントのユーザ名とパスワードも指定できます。
* セキュアなプロトコルを使用するLDAPSサーバの場合は、LDAPサーバの証明書チェーンをローカルマシンにインストールする必要があります。

[[ID052de8d046eb266938038252e436827e]]
=
ストレージアレイのロールにマッピングするときは、どのような点に注意する必要がありますか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
グループをロールにマッピングする前に、次のガイドラインを確認してください。

ストレージアレイに組み込まれているロールベースアクセス制御（RBAC）機能には、次のロールが

あります。

* * Storage admin *--
ストレージ・オブジェクト（ボリュームやディスク・プールなど）への読み取り/書き込みのフル・アクセス。セキュリティ構成へのアクセスはありません。
* * Security admin *--
アクセス管理、証明書管理、監査ログ管理のセキュリティ構成へのアクセス、および従来の管理インターフェイス（SYMbol）のオン/オフの切り替え機能。
* * Support admin *--ストレージアレイのすべてのハードウェアリソース、障害データ、MELイベント、およびコントローラファームウェアアップグレードへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
* *Monitor *--
すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

== 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を使用する場合は、次の点を確認してください。

* 管理者がディレクトリサービスでユーザーグループを定義しました。
*
LDAPユーザグループのグループドメイン名を確認しておきます。正規表現がサポートされています。（`\`正規表現パターンに含まれていない特殊な正規表現文字は、バックスラッシュでエスケープする必要があります）。
+
[listing]

\.[]{}()<>*+-=!?^$|
----
* Monitorロールは、管理者を含むすべてのユーザに必要です。
Monitorロールがないユーザの場合、System Managerは正常に動作しません。

== SAML

ストレージアレイに組み込みのSecurity Assertion Markup Language（SAML）機能を使用する場合は、次の点を確認してください。

* アイデンティティプロバイダ（IdP）管理者が、IdPシステムでユーザ属性とグループメンバーシップを設定しておく必要があります。
* グループメンバーシップ名を確認しておきます。

*
マッピングするグループの属性値がわかっている必要があります。正規表現がサポートされています。(`\`正規表現パターンに含まれていない特殊な正規表現文字は、バックスラッシュでエスケープする必要があります）。
+
[listing]

\.[]{}()<>*+-=!?^$|
----
* Monitorロールは、管理者を含むすべてのユーザに必要です。
Monitorロールがないユーザの場合、System Managerは正常に動作しません。

[[ID4de5cafa05eb6ab899f3ec00f2e5286f]]
= この変更の影響を受ける外部管理ツールはどれですか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
管理インターフェイスを切り替える、認証方式にSAMLを使用する、などの特定の変更をSystem Managerで行うと、一部の外部ツールや機能が使用できなくなることがあります。

== 管理インターフェイス

SANtricity SMI-S ProviderやOnCommand Insight （
OCI）などの従来の管理インターフェイス（SYMbol）と直接通信するツールは、レガシー管理インターフェイスの設定が有効になっていないかぎり機能しません。また、この設定が無効になっている場合、従来のCLIコマンドを使用したりミラーリング処理を実行したりすることはできません。

詳細については、テクニカルサポートにお問い合わせください。

== SAML認証

SAMLが有効な場合、次のクライアントはストレージアレイのサービスとリソースにアクセスできません。

* Enterprise Management Window（EMW）
* コマンドラインインターフェイス（CLI）

* ソフトウェア開発キット（SDK）クライアント
* インバンドクライアント
* HTTPベーシック認証REST APIクライアント
* 標準のREST APIエンドポイントを使用したログイン

詳細については、テクニカルサポートにお問い合わせください。

[[IDfcf8d7da37fc03f02025f01cea2a4e8f]]
= SAMLを設定して有効にするときは、どのような点に注意する必要がありますか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
認証のためにSecurity Assertion Markup Language（
SAML）の機能を設定して有効にする前に、次の要件を満たしていることを確認し、SAMLの制限事項を理解しておきます。

== 要件

開始する前に、次のことを確認してください。

* ネットワークにアイデンティティプロバイダ（IdP）を設定しておきます。
IdPは、ユーザにクレデンシャルを要求して認証されたユーザかどうかを確認するための外部システムです。IdPの保守はセキュリティチームが行います。
* IdP管理者が、IdPシステムでユーザ属性とユーザグループを設定しておきます。
* IdP管理者が、認証時に名前IDを返す機能が
IdPでサポートされていることを確認しておく必要があります。
* IdPサーバとコントローラのクロックを同期しておきます（
NTPサーバを使用するかコントローラのクロックの設定を調整します）。
* IdPのメタデータファイルをIdPシステムからダウンロードし、System
Managerへのアクセスに使用するローカルシステムで使用できるようにしておきます。
* ストレージアレイ内の各コントローラのIPアドレスまたはドメイン名を確認しておきます。

== 制限事項

上記の要件に加えて、次の制限事項を理解していることを確認してください。

* SAMLを有効にすると、ユーザインターフェイスで無効にしたり、
IdP設定を編集したりすることはできなくなります。SAMLの設定を無効にしたり編集したりする必要がある場合は、テクニカルサポートにお問い合わせください。最後の設定手順でSAMLを有効にする前に、SSOログインをテストすることを推奨します。（SAMLを有効にする前にSSOログインのテストも実行されます）。
* あとで
SAMLを無効にすると、以前の設定（ローカルユーザロールまたはディレクトリサービス）が自動的にリストアされます。
* 現在ユーザ認証用にディレクトリサービスが設定されている場合は、
SAMLによって上書きされます。
*
SAMLが設定されている場合、次のクライアントはストレージアレイリソースにアクセスできません。
+
** Enterprise Management Window（EMW）
** コマンドラインインターフェイス（CLI）
** ソフトウェア開発キット（SDK）クライアント
** インバンドクライアント
** HTTPベーシック認証REST APIクライアント
** 標準のREST APIエンドポイントを使用したログイン

[[ID9b9a6f99dcd453c58181cb95404dd425]]
= 監査ログにはどのような種類のイベントが記録されますか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
監査ログには、変更イベント、または変更イベントと読み取り専用イベントの両方を記録できます。

ポリシー設定に応じて、次のタイプのイベントが表示されます。

* *変更イベント*--ストレージのプロビジョニングなど、システムへの変更を含む、System Manager内からのユーザーアクション。
* *変更イベントおよび読み取り専用イベント*--
システムへの変更を伴うユーザー操作、およびボリューム割り当ての表示やダウンロードなどの情報を含むイベント。

[[ID47ddf415f9ac99218e348075f9fbc465]]
= syslogサーバを設定するときは、どのような点に注意する必要がありますか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
監査ログを外部syslogサーバにアーカイブできます。

syslogサーバを設定する際は、次のガイドラインに注意してください。

*
サーバのアドレス、プロトコル、ポート番号を確認しておきます。サーバアドレスには、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスを使用できます。
* サーバでセキュアなプロトコル（
TLSなど）を使用している場合は、ローカルシステムに認証局（CA）証明書がある必要があります。CA証明書はWebサイトの所有者を識別し、サーバとクライアントの間のセキュアな接続を確立します。
* 設定が完了すると、以降すべての監査ログが
syslogサーバに送信されるようになります。以前のログは転送されません。
* 上書きポリシーの設定（*View/Edit Settings*から入手可能）は、ログが
syslogサーバ設定でどのように管理されるかに影響しません。
* 監査ログは、RFC 5424のメッセージ形式に従います。

[[ID918a4b0f1ca339906df88c383a60ea93]]
= syslogサーバが監査ログを受信しなくなりました。どうすればいいですか？
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
syslogサーバにTLSプロトコルを設定している場合、何らかの理由で証明書が無効になるとサーバはメッセージを受信できなくなります。無効な証明書に関するエラーメッセージが監査ログに記録されます。

この問題を解決するには、まずsyslogサーバの証明書を修正する必要があります。有効な証明書チ

ェーンが確立されたら、メニューに移動します。Settings [Audit Log]> Configure Syslog Servers > Test All]。

:leveloffset: -1

:leveloffset: -1

= 証明書

:leveloffset: +1

[[IDf313eaf4e20c4ea33b5d8575f081db64]]
= 証明書の概要
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
System Managerを使用して、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

_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し、インターネット上のセキュアな通信を実現するデジタルファイルです。証明書には2種類あります。A_Signed certificate_is validated by a Certificate Authority（CA；認証局）とa_self-signed certificate_is validated by the entity of the entity instead of a third party。

詳細：

* xref:{relative_path}how-certificates-work-sam.html["証明書の仕組み"]
* xref:{relative_path}certificate-terminology.html["証明書の用語"]

== 署名済み証明書を設定する方法を教えてください。

最初にSystem Managerから署名要求を生成し、そのファイルをCAに送信します。
CAから証明書ファイルが返されたら、System Managerを使用してインポートします。

詳細：

* xref:{relative_path}use-ca-signed-certificates-for-controllers.html["コントローラのCA署名証明書の使用"]
* xref:{relative_path}use-ca-signed-certificates-for-authentication-with-a-key-management-server.html["キー管理サーバでの認証にCA署名証明書を使用する"]

== 関連情報

証明書に関するタスクの詳細については、以下を参照してください。

* xref:{relative_path}view-imported-certificates.html["インポートした証明書情報の表示"]
* xref:{relative_path}enable-certificate-revocation-checking.html["証明書失効チェックを有効にする"]

= 概念

:leveloffset: +1

[[ID16fe36a0bcd9366dcf0b93354ef3f5a2]]
= 証明書の仕組み
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

証明書を使用すると、Web通信が、指定されたサーバとクライアントの間でのみ、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が保証されます。System Managerを使用すると、ホスト管理システムのブラウザ（クライアントとして機能）とストレージシステムのコントローラ（サーバとして機能）の間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、誰かが所有者のIDを検証し、自分のデバイスが信頼できると判断したことを意味します。ストレージアレイには、自動生成された自己署名証明書が各コントローラに付属しています。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の間のよりセキュアな接続を確立することもできます。

[NOTE]
====
CA署名証明書はセキュリティ保護に優れていますが（中間者攻撃を防止するなど）、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、自己署名証明書は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（通常はサーバまたはWebサイト）の所有者に関する詳細、証明書の発行日と有効期限、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ます。

ブラウザを開いてWebアドレスを入力すると、証明書の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、南京錠のアイコンとhttpsの指定が含まれます。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、申請プロセス中にユーザー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、CAからホスト管理システムにロードするデジタルファイルが送信されます。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、必要なルート証明書は1つだけです。
* *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されて送信されることも保証されます。ただし、自己署名証明書はCA署名証明書と同じ信頼チェーンを使用しません。

自己署名証明書はブラウザでは「信頼されている」ものではありません。自己署名証明書のみが含まれている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。

== キー管理サーバに使用される証明書

ドライブセキュリティ機能を備えた外部キー管理サーバを使用している場合は、そのサーバとコントローラの間の認証用の証明書も管理できます。

[[ID888e64819e42cd8b5836275cc7ad8a44]]
= 証明書の用語
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
証明書管理に関連する用語を次に示します。

[cols="25h,~"]
|===
| 期間 | 製品説明

a|
カリフォルニア州
a|
認証局（CA）は、インターネットセキュリティのためにデジタル証明書と呼ばれる電子ドキュメントを発行する信頼されたエンティティです。証明書でWebサイトの所有者を識別することにより、クライアントとサーバの間のセキュアな接続が確立されます。

a|
CSR
a|
証明書署名要求（CSR）は、申請者から認証局（CA）に送信されるメッセージです。CSRは、CAが証明書を発行するために必要な情報を検証します。

a|
証明書
a|
証明書はセキュリティ上の目的でサイトの所有者を識別するもので、攻撃者による偽装を防止します。証明書には、サイトの所有者に関する情報と、この情報を証明（署名）する信頼されたエンティティのIDが含まれています。

a|
証明書チェーン
a|
証明書にセキュリティレイヤを追加するファイルの階層。通常、チェーンには階層の最上位にある1つのルート証明書、1つ以上の中間証明書、およびエンティティを識別するサーバ証明書が含まれます。

a|
クライアント証明書
a|
セキュリティキー管理のために、クライアント証明書はストレージアレイのコントローラを検証し、キー管理サーバがコントローラのIPアドレスを信頼できるようにします。

a|
中間証明書
a|
証明書チェーンのルートから1つ以上の中間証明書が分岐します。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。

a|
キー管理サーバ証明書
a|

セキュリティキー管理のために、キー管理サーバ証明書はサーバを検証し、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にします。

a|
キーストア
a|
キーストアはホスト管理システム上のリポジトリであり、秘密鍵とそれに対応する公開鍵および証明書が格納されています。これらのキーと証明書によって、コントローラなどの独自のエンティティが識別されます。

a|
OCSPサーバ
a|
Online Certificate Status Protocol（OCSP）サーバは、スケジュールされた有効期限の前に認証局（CA）が証明書を失効させたかどうかを確認し、証明書が失効している場合はユーザがサーバにアクセスできないようにします。

a|
ルート証明書
a|
ルート証明書は、証明書チェーンの階層の最上位にあります。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、必要なルート証明書は1つだけです。

a|
署名済み証明書
a|
認証局（CA）によって検証される証明書。このデータファイルには秘密鍵が含まれており、HTTPS接続を介してサーバとクライアントの間でデータが暗号化された形式で送信されるようにします。また、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。署名済み証明書は信頼チェーンを使用するため、本番環境で最もよく使用されます。「CA署名証明書」または「管理証明書」とも呼ばれます。

a|
自己署名証明書
a|
自己署名証明書は、エンティティの所有者によって検証されます。このデータファイルには秘密鍵

が含まれており、HTTPS接続を介してサーバとクライアントの間でデータが暗号化された形式で送信されるようにします。また、文字と数字で構成されるデジタル署名も含まれています。自己署名証明書はCA署名証明書と同じ信頼チェーンを使用しないため、テスト環境で最もよく使用されます。「事前にインストールされている」証明書とも呼ばれます。

 a|
サーバ証明書
 a|
サーバ証明書は、証明書チェーンの最下位にあります。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します。ストレージシステムの各コントローラには、個別のサーバ証明書が必要です。

|===

:leveloffset: -1

= 証明書を使用する

:leveloffset: +1

[[IDfd7edb853ca9e103da249426b55155d9]]
= コントローラのCA署名証明書の使用
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
コントローラとSystem Managerへのアクセスに使用されるブラウザとの間のセキュアな通信を確立するために、CA署名証明書を取得できます。

.開始する前に
* Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書機能は表示されません。
* 各コントローラのIPアドレスまたはDNS名を確認しておく必要があります。

.タスクの内容
CA署名証明書の使用は、3つの手順で構成されます。

== 手順1：コントローラのCSRを作成します

最初に、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）ファイルを生成する必要があります。

.タスクの内容
このタスクでは、System ManagerからCSRファイルを生成する方法について説明します。
CSRは、組織に関する情報、およびコントローラのIPアドレスまたはDNS名を提供します。このタスクでは、ストレージアレイにコントローラが1つある場合は1つ、コントローラが2つある場合は2つのCSRファイルが生成されます。

[NOTE]
====
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
. メニューから[設定][証明書]を選択します。
. [Array Management]タブで、[*Complete CSR*]を選択します。
+
[NOTE]
====
2台目のコントローラの自己署名証明書を受け入れるよう求めるダイアログボックスが表示された場合は、*自己署名証明書を受け入れる*をクリックして続行します。

====
. 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.などのサフィックスを含めます。
** *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*--ストレージアレイ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）*-ストレージアレイ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）。

+
[CAUTION]
====
一部のフィールドには、コントローラのIPアドレスなどの適切な情報があらかじめ入力されています。事前入力された値は、明らかな間違いでないかぎり変更しないでください。たとえば、CSRをまだ作成していない場合、コントローラのIPアドレスは「localhost」に設定されます。

この場合は、「localhost」をコントローラのDNS名またはIPアドレスに変更する必要があります。

====
. ストレージアレイ内のコントローラAに関する次の情報を確認または入力します。
+
** *コントローラAの共通名*--コントローラAのIPアドレスまたは
DNS名がデフォルトで表示されます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System Managerにアクセスする際に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。
DNS名の1文字目をワイルドカードにすることはできません。
** *コントローラAの代替IPアドレス*--共通名がIPアドレスの場合は、コントローラA
の追加のIPアドレスまたはエイリアスをオプションで入力できます。複数のエントリを入力する場合は、カンマで区切って指定します。
** *コントローラAの代替DNS名*--共通名がDNS名の場合は、コントローラAの追加の
DNS名を入力します。複数のエントリを入力する場合は、カンマで区切って指定します。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1文字目をワイルドカードにすることはできません。ストレージアレイにコントローラが1台しかない場合は、「完了」ボタンを使用できます。
+
ストレージアレイにコントローラが2台ある場合は、* Next *ボタンを使用できます。

+
[NOTE]
====
CSR要求を最初に作成するときは、[この手順をスキップ]リンクをクリックしないでください。このリンクは、エラーリカバリの状況で提供されます。CSR要求が一方のコントローラで失敗し、もう一方のコントローラで失敗することがあります。このリンクを使用すると、コントローラAでCSRがすでに定義されている場合はその作成をスキップし、コントローラBでCSRを再作成する次の手順に進むことができます

====
. コントローラが1台しかない場合は、[完了]をクリックします。コントローラが2
台ある場合は、[次へ]をクリックしてコントローラBの情報を入力し（上記と同じ）、[完了]をクリックします。
+
シングルコントローラの場合は、1つのCSRファイルがローカルシステムにダウンロードされます。デュアルコントローラの場合は、2つのCSRファイルがダウンロードされます。ダウンロードのフォルダの場所は、ブラウザによって異なります。

. にアクセスします。

== 手順2：CSRファイルを送信する

証明書署名要求（CSR）ファイルを作成したら、ファイルを認証局（CA）に送信します。Eシリーズシステムでは、署名済み証明書のPEM形式（Base64 ASCIIエンコード）が必要です。PEM、.crt、.cer、または.keyのファイルタイプが含まれます。

.手順
. ダウンロードしたCSRファイルの場所を確認します。
. 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。
+
[CAUTION]
====
* CSRファイルをCAに送信した後は、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、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。

====
. CAから署名済み証明書が返されたら、に進みます<<手順
3：コントローラの署名済み証明書をインポートする>>。

== 手順3：コントローラの署名済み証明書をインポートする

認証局（CA）から署名済み証明書を受け取ったら、コントローラのファイルをインポートします。

.開始する前に
* 署名済み証明書ファイルをCA
から受け取っておきます。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（
.p7bファイルなど）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、コントローラを識別するサーバ証明書）に展開する必要があります。Windowsユーティリティを使用してファイルを展開でき `certmgr`ます(右クリックしてメニューを選択します:すべてのタスク[エクスポート])。Base-64エンコードを推奨します。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。
* System Managerにアクセスするホストシステムに証明書ファイルをコピーしておきます。

.手順
. 選択メニュー：設定[証明書]
. Array Management（アレイ管理）タブで、* Import（インポート）*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開きます。

. 「
*参照」ボタンをクリックして、最初にルート証明書と中間証明書ファイルを選択してから、コントローラの各サーバ証明書を選択します。ルートファイルと中間ファイルは両方のコントローラで同じです。サーバ証明書のみコントローラごとに一意です。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。

. [* インポート *] をクリックします。
+
ファイルがアップロードされて検証されます。

.結果
セッションは自動的に終了します。証明書を有効にするには、再度ログインする必要があります。再度ログインすると、新しいCA署名証明書がセッションに使用されます。

[[IDac8256bd23db92eca9b092765281324b]]
= 管理証明書のリセット
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
コントローラの証明書をCA署名証明書から工場出荷時の自己署名証明書に戻すことができます。

.開始する前に
* Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書機能は表示されません。
* CA署名証明書を事前にインポートしておく必要があります。

.タスクの内容
リセット機能は、現在のCA署名証明書ファイルを各コントローラから削除します。その後、コントローラ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
. メニューから[設定][証明書]を選択します。

. Array Management（アレイ管理）タブで、* Reset（リセット）*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。

. フィールドにと入力し `reset`、*[リセット]*をクリックします。
+
ブラウザの更新後、ブラウザによって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、そのサイトがHTTP Strict Transport Securityを使用していると報告されることがあります。この状態は、自己署名証明書に切り替えたときに発生します。宛先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、ブラウザから閲覧データをクリアする必要があります。

.結果
コントローラで自己署名証明書が使用されるようになります。その結果、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るプロンプトが表示されます。

[[ID2d2ac55121493969a386e80869614296]]
= インポートした証明書情報の表示
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
[証明書]ページでは、証明書のタイプ、発行元機関、およびストレージアレイの証明書の有効な日付範囲を確認できます。

.開始する前に
Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書機能は表示されません。

.手順
. メニューから[設定][証明書]を選択します。
. いずれかのタブを選択して、証明書に関する情報を表示します。
+
[cols="25h,~"]
|===
| タブ | 製品説明

a|
アレイ管理
a|
ルートファイル、中間ファイル、サーバファイルなど、各コントローラ用にインポートしたCA署名証明書に関する情報が表示されます。

a|
信頼性
a|
コントローラ用にインポートしたその他すべてのタイプの証明書に関する情報が表示されます。[Show certificates that are ...]の下のフィルタフィールドを使用して、ユーザがインストールした証明書または事前にインストールされた証明書を表示します。

** *ユーザーがインストールした証明書*--
ユーザーがストレージアレイにアップロードした証明書。これには、コントローラがサーバーではなくクライアントとして機能する場合に信頼された証明書、LDAPS証明書、アイデンティティフェデレーション証明書が含まれます。
** *プリインストール*--ストレージアレイに含まれている自己署名証明書。

a|
キー管理
a|
外部キー管理サーバ用にインポートしたCA署名証明書に関する情報が表示されます。

|===

[[IDd5dd67894c020c3e8a3eb96f706fba34]]
= クライアントとして機能するコントローラの証明書のインポート
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ネットワークサーバの信頼チェーンを検証できないためにコントローラが接続を拒否した場合は、[信頼済み]タブから証明書をインポートして、コントローラ（クライアントとして機能）がそのサー

バからの通信を受け入れることができます。

.開始する前に
* Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書機能は表示されません。
* 証明書ファイルがローカルシステムにインストールされている必要があります。

.タスクの内容
別のサーバ（LDAPサーバやTLSを使用するsyslogサーバなど）からコントローラへの接続を許可する場合は、[信頼済み]タブから証明書をインポートする必要があります。

.手順
. メニューから[設定][証明書]を選択します。
. [信頼済み]タブで、[*インポート*]を選択します。
+
信頼された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開きます。

. Browse（参照）*をクリックして、コントローラの証明書ファイルを選択します。
+
ダイアログボックスにファイル名が表示されます。

. [* 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。

[[IDce6c033a122d364772afa9141d3bf40b]]
= 証明書失効チェックを有効にする
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
失効した証明書の自動チェックを有効にして、Online Certificate Status Protocol（OCSP）サーバがユーザによるセキュアでない接続をブロックするようにすることができます。

.開始する前に
* Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書機

能は表示されません。
* 両方のコントローラにDNSサーバが設定されている必要があります。これにより、OCSPサーバの完全修飾ドメイン名が使用できるようになります。このタスクは[ハードウェア]ページから実行できます。
* 独自のOCSPサーバを指定する場合は、そのサーバのURLを確認しておく必要があります。

.タスクの内容
自動失効チェックは、CAが発行した証明書に問題がある場合や、秘密鍵が漏えいした場合に役立ちます。

このタスクでは、OCSPサーバを設定するか、証明書ファイルに指定されているサーバを使用することができます。OCSPサーバは、スケジュールされた有効期限よりも前にCAによって失効された証明書がないかを判断し、証明書が失効している場合は、ユーザによるサイトへのアクセスをブロックします。

.手順
. メニューから[設定][証明書]を選択します。
. [*Trusted*]タブを選択します。
+
[NOTE]
====
また、*Key Management*タブから失効チェックを有効にすることもできます。

====
. [一般的でないタスク]をクリックし、ドロップダウンメニューから[
失効チェックを有効にする*]を選択します。
. 「*失効チェックを有効にする
*」を選択して、チェックボックスにチェックマークが表示され、ダイアログボックスに追加のフィールドが表示されるようにします。
. [* OCSPレスポンダのアドレス*]フィールドに、OCSPレスポンダサーバの
URLをオプションで入力できます。アドレスを入力しない場合は、証明書ファイルで指定されているOCSPサーバのURLが使用されます。
. [アドレスのテスト*]をクリックして、指定した
URLへの接続をシステムがオープンできることを確認します。
. [保存（ Save ）] をクリックします。

.結果
証明書が失効しているサーバにストレージアレイが接続しようとすると、接続は拒否され、イベントがログに記録されます。

[[ID2a494f948b52aeb9c7390f4d1a2138b6]]
= 信頼できる証明書の削除
:allow-uri-read:

```
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
以前にインポートしたユーザがインストールした証明書を[信頼済み]タブから削除できます。

.開始する前に
* Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書機能は表示されません。
*
信頼された証明書を新しいバージョンに更新する場合は、古い証明書を削除する前に更新された証明書をインポートする必要があります。


[CAUTION]
====
コントローラと別のサーバ（LDAPサーバなど）の認証に使用していた証明書を、交換用の証明書をインポートする前に削除すると、システムにアクセスできなくなることがあります。

====
.タスクの内容
このタスクでは、ユーザがインストールした証明書を削除する方法について説明します。あらかじめインストールされている自己署名証明書を削除することはできません。

.手順
. メニューから[設定][証明書]を選択します。
. [*Trusted*]タブを選択します。
+
この表には、ストレージアレイの信頼された証明書が表示されます。

. 削除する証明書を表から選択します。
. [メニュー]、[一般的ではないタスク]、[削除]の順にクリック
+
[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。

. フィールドにと入力し `delete`、*[削除]*をクリックします。




[[ID636653372ec1469477017e39e11b47a9]]
= キー管理サーバでの認証にCA署名証明書を使用する
:allow-uri-read:
```

```
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
キー管理サーバとストレージアレイコントローラの間のセキュアな通信を実現するには、適切な証明書セットを設定する必要があります。

.開始する前に
Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書機能は表示されません。

.タスクの内容
コントローラとキー管理サーバ間の認証は、2つの手順で行います。

== 手順1：キー管理サーバを使用した認証用にCSRを作成および送信します

最初に証明書署名要求（CSR）ファイルを生成し、そのCSRを使用して、キー管理サーバが信頼する認証局（CA）から署名済みのクライアント証明書を要求する必要があります。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してダウンロードすることもできます。クライアント証明書はストレージアレイのコントローラを検証し、キー管理サーバがKey Management Interoperability Protocol（KMIP）要求を信頼できるようにします。

.手順
. メニューから[設定][証明書]を選択します。
. [キー管理]タブで、[*Complete CSR*]を選択します。
. 次の情報を入力します。
+
** *共通名*--証明書ファイルに表示されるストレージアレイ名など、このCSRを識別する名前。
** *組織*--会社または組織の正式名称。Inc.やCorp.などのサフィックスを含めます。
** *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*--組織の所在地である市区町村。
** *都道府県(オプション)*--組織の所在地である都道府県。
** *国のISOコード*--組織の所在地である米国などの2桁のISO（国際標準化機構）コード。

. [* ダウンロード] をクリックします。
+
CSRファイルがローカルシステムに保存されます。

. キー管理サーバによって信頼されているCAから署名済みクライアント証明書を要求します。
. クライアント証明書がある場合は、に進みます<<手順

2：キー管理サーバの証明書をインポートする>>。

== 手順2：キー管理サーバの証明書をインポートする

次の手順では、ストレージアレイとキー管理サーバの間の認証用の証明書をインポートします。証明書には2種類あります。クライアント証明書はストレージアレイのコントローラを検証し、キー管理サーバ証明書はサーバを検証します。コントローラのクライアント証明書ファイルとキー管理サーバのサーバ証明書ファイルの両方をロードする必要があります。

.開始する前に
* 署名済みのクライアント証明書ファイル（を参照<<手順1
：キー管理サーバを使用した認証用にCSRを作成および送信します>>）を用意し、そのファイルをSystem
Managerにアクセスするホストにコピーしておきます。クライアント証明書はストレージアレイのコントローラを検証し、キー管理サーバがKey Management Interoperability Protocol（KMIP）要求を信頼できるようにします。
* キー管理サーバから証明書ファイルを取得し、そのファイルをSystem
Managerにアクセスするホストにコピーする必要があります。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に、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。
+
[NOTE]
====
サーバ証明書の詳細については、キー管理サーバのドキュメントを参照してください。

====

.手順
. メニューから[設定][証明書]を選択します。
. [キー管理]タブで、[*インポート*]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開きます。

. Select client certificate *の横にある* Browse
*ボタンをクリックして、ストレージアレイのコントローラ用のクライアント証明書ファイルを選択します。
+
ダイアログボックスにファイル名が表示されます。

. キー管理サーバのサーバ証明書の選択*の横にある*参照
*ボタンをクリックして、キー管理サーバのサーバ証明書ファイルを選択します。キー管理サーバのルート証明書、中間証明書、またはサーバ証明書を選択できます。
+

ダイアログボックスにファイル名が表示されます。

. [* インポート *] をクリックします。
+
ファイルがアップロードされて検証されます。

[[ID235cc735987bda06c33602e6db62160a]]
= キー管理サーバ証明書のエクスポート
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
キー管理サーバの証明書をローカルマシンに保存できます。

.開始する前に
* Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書機能は表示されません。
* 証明書をインポートしておく必要があります。

.手順
. メニューから[設定][証明書]を選択します。
. [*キー管理*（Key Management *）]タブを選択します。
. 表からエクスポートする証明書を選択し、* Export *（エクスポート）をクリックします。
+
保存(Save)ダイアログボックスが開きます

. ファイル名を入力し、*保存*をクリックします。

:leveloffset: -1

= FAQ

:leveloffset: +1

[[ID43c235ede86b8a28cdd776f7a5671d6e]]
= [他のコントローラにアクセスできません]ダイアログボックスが表示されるのはなぜですか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
CA証明書に関連する特定の処理（証明書のインポートなど）を実行すると、2台目のコントローラの自己署名証明書を受け入れるよう求めるダイアログボックスが表示されることがあります。

2台のコントローラを搭載したストレージアレイ（デュプレックス構成）では、SANtricity System Managerが
2台目のコントローラと通信できない場合、または処理の特定の段階でブラウザが証明書を受け入れられない場合に、このダイアログボックスが表示されることがあります。

このダイアログボックスが表示された場合は、[*自己署名証明書を承認する*]をクリックして続行します。パスワードの入力を求めるダイアログボックスが表示された場合は、System Managerへのアクセスに使用する管理者パスワードを入力します。

このダイアログボックスが再度表示され、証明書タスクを完了できない場合は、次のいずれかの手順を実行してください。

* 別のブラウザを使用してこのコントローラにアクセスし、証明書を受け入れて続行します。
* System Managerを使用して
2台目のコントローラにアクセスし、自己署名証明書を受け入れてから、1台目のコントローラに戻って続行します。

[[IDe6b02353eaa480c65b964b58c966271e]]
= 外部キー管理用にSystem Managerにアップロードする必要がある証明書を確認するにはどうすればよいですか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
外部キー管理では、ストレージアレイとキー管理サーバの間の認証用に2種類の証明書をインポートして、2つのエンティティが相互に信頼できるようにします。

クライアント証明書はストレージアレイのコントローラを検証し、キー管理サーバがKey Management Interoperability Protocol（KMIP）要求を信頼できるようにします。クライアント証明書を取得するには、System Managerを使用してストレージアレイのCSRを作成します。その後、CSRをキー管理サーバにアップロードし、そこからクライアント証明書を生成できます。クライアント証明書を入手したら、System Managerにアクセスす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に、キー管理サーバを検証します。キー管理サーバからサーバ証明書ファイルを取得し、そのファイルをSystem Managerにアクセスするホストにコピーします。

[[ID816a21ef9ba07d6aec10dab14faaebc8]]
= 証明書失効チェックについて、どのような点に注意する必要がありますか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
System Managerでは、証明書失効リスト（CRL）をアップロードする代わりに、Online Certificate Status Protocol（OCSP）サーバを使用して失効した証明書をチェックできます。

失効した証明書は信頼しないようにしてください。証明書が失効する理由はいくつかあります。たとえば、認証局（CA）から証明書が適切に発行されていない、秘密鍵が不正に使用された、特定されたエンティティがポリシーの要件を満たしていない、などの場合です。

System ManagerでOCSPサーバへの接続を確立すると、ストレージアレイは、AutoSupportサーバ、外部キー管理サーバ（EKMS）、Lightweight Directory Access Protocol over SSL（LDAPS）サーバ、またはsyslogサーバに接続するたびに失効チェックを実行します。ストレージアレイは、これらのサーバの証明書の検証を試行して、証明書が失効していないことを確認します。その後、サーバはその証明書に対して「good」、「revoked」、または「unknown」の値を返します。証明書が失効している場合や、アレイがOCSPサーバにアクセスできない場合は、接続が拒否されます。

[NOTE]
====
System ManagerまたはコマンドラインインターフェイスCLIで指定したOCSPレスポンダアドレスは、証明書ファイル内のOCSPアドレスよりも優先されます。

====

```
[[IDba715cd9a0ad965dc4f7c7bdc100f9fc]]
= 失効チェックはどのような種類のサーバで有効になりますか。
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
ストレージアレイは、AutoSupportサーバ、外部キー管理サーバ（EKMS）、Lightweight Directory Access Protocol over SSL（LDAPS）サーバ、または syslogサーバに接続するたびに失効チェックを実行します。



:leveloffset: -1


:leveloffset: -1


= サポート

:leveloffset: +1


[[IDac8da01cdef0789d6f510ec14e8b7641]]
= サポートの概要
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
[Support]ページでは、テクニカルサポートのリソースにアクセスできます。



== どのようなサポートタスクを利用できますか。

[Support]では、テクニカルサポートの連絡先の表示、診断の実行、AutoSupportの設定、イベントログの表示、ソフトウェアのアップグレードを実行できます。

詳細：
```

```
* xref:{relative_path}autosupport-feature-
overview.html["AutoSupport機能の概要"]
* xref:{relative_path}overview-event-log.html["イベントログの概要"]
* xref:{relative_path}overview-upgrade-
center.html["アップグレードセンターの概要"]
```

== テクニカルサポートへの連絡方法を教えてください。

メインページで、[メニュー]、[サポートセンター]、[サポートリソース]タブの順にクリックします。テクニカルサポートの連絡先情報は、インターフェイスの右上に表示されます。

= 情報と診断の表示

```
:leveloffset: +1
```

```
[[ID21dc532686bb102dda0fd5b726643d44]]
```
= ストレージアレイプロファイルの表示
```
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```
ストレージアレイプロファイルには、ストレージアレイのすべてのコンポーネントとプロパティの説明が表示されます。

.タスクの内容
ストレージアレイプロファイルは、リカバリ時の補助として、またはストレージアレイの現在の構成の概要として使用できます。ストレージアレイプロファイルのコピーを管理クライアントに保存したり、ストレージアレイプロファイルのハードコピーをストレージアレイとともに保管したりできます。構成を変更する場合は、ストレージアレイプロファイルの新しいコピーを作成します。

.手順
. メニューを選択します。Support [サポートセンター]>[サポートリソース]タブ。
. 下にスクロールして「 Launch detailed storage array information 」 * と進み、「 * Storage Array Profile 」を選択します。
+
レポートが画面に表示されます。

+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| セクション | 製品説明

a|
ストレージアレイ
a|
ストレージアレイに対して設定可能なすべてのオプションとシステムの静的オプションが表示されます。これらのオプションには、コントローラ、ドライブシェルフ、ドライブ、ディスクプール、ボリュームグループ、ボリューム、ホットスペアドライブの数、許可されるドライブシェルフ、ドライブ、ソリッドステートディスク（SSD）、ボリュームの最大数、Snapshotグループ、Snapshotイメージ、Snapshotボリューム、整合性グループの数、機能に関する情報、ファームウェアバージョンに関する情報、シャーシのシリアル番号に関する情報、AutoSupportステータスとAutoSupportスキャンスケジュール情報、自動サポートデータ収集とスケジュールの設定（WWID）、ストレージID）が含まれます。

a|
ストレージ
a|
ストレージアレイ内のすべてのストレージデバイスのリストが表示されます。ストレージアレイの構成によっては、[Storage]セクションに次のサブセクションが表示される場合があります。

** *ディスク・プール*--
ストレージ・アレイ内のすべてのディスク・プールのリストを表示します
** *ボリュームグループ*--
ストレージアレイ内のすべてのボリュームグループのリストを表示しますボリュームと空き容量は作成順に表示されます。
** * Volumes *--
ストレージアレイ内のすべてのボリュームのリストを表示します表示される情報には、ボリューム名、ボリュームステータス、容量、RAIDレベル、ボリュームグループまたはディスクプール、ドライブタイプ、およびその他の詳細があります。
** *見つからないボリューム*--
ストレージアレイ内で現在ステータスが不明なすべてのボリュームのリストを表示します表示される情報には、見つからない各ボリュームのWorld Wide Identifier（WWID）があります。

a|
コピーサービス

a|
ストレージアレイに使用されているすべてのコピーサービスのリストが表示されます。ストレージアレイの構成によっては、[Copy Services]セクションに次のサブセクションが表示される場合があります。

** *ボリュームコピー*--
ストレージアレイ内のすべてのコピーペアのリストを表示します表示される情報には、コピーの数、コピーペア名、ステータス、開始タイムスタンプ、およびその他の詳細があります。
** *スナップショット・グループ*--
ストレージ・アレイ内のすべてのスナップショット・グループのリストを表示します
** *スナップショット・イメージ*--
ストレージ・アレイ内のすべてのスナップショットのリストを表示します
** *スナップショット・ボリューム*--
ストレージ・アレイ内のすべてのスナップショット・ボリュームのリストを表示します
** *コンシステンシ・グループ*--
ストレージ・アレイ内のすべてのコンシステンシ・グループのリストを表示します
** *メンバーボリューム*--
ストレージアレイ内のすべてのコンシステンシグループメンバーボリュームのリストを表示します
** *ミラーグループ*--すべてのミラーボリュームのリストを表示します
** *リザーブ容量*-
ストレージアレイ内のすべてのリザーブ容量ボリュームのリストが表示されます

a|
ホストの割り当て
a|
ストレージアレイ内のホスト割り当てのリストが表示されます。表示される情報には、ボリューム名、論理ユニット番号（LUN）、コントローラID、ホスト名またはホストクラスタ名、およびボリュームステータスがあります。トポロジ定義とホストタイプ定義などの追加情報が表示されます。

a|
ハードウェア
a|
ストレージアレイ内のすべてのハードウェアのリストが表示されます。ストレージアレイの構成によっては、[ハードウェア]セクションに次のサブセクションが表示される場合があります。

** *コントローラ*--
ストレージアレイ内のすべてのコントローラのリストを表示しますコントローラの場所'ステータス'構成が含まれますまた、ドライブチャネル情報、ホストチャネル情報、イーサネットポート情報も含まれます。
** *ドライブ*--ストレージアレイ内のすべてのドライブのリストを表示しますシェルフID、ドロワーID、スロットIDの順にドライブが表示されます。表示される情報には、シェルフID、ドロワーID、スロットID、ステータス、物理容量、メディアタイプ、インターフェイスタイプ、現

在のデータ速度、製品ID、および各ドライブのファームウェアバージョンがあります。[ドライブ]セクションには、ドライブチャネル情報、ホットスペアの対象情報、および消耗度情報（SSDドライブの場合のみ）も表示されます。消耗度情報には、使用済み寿命の割合が含まれます。これは、これまでにSSDドライブに書き込まれたデータ量を、ドライブの理論上の合計書き込み制限で割った値です。
** *ドライブチャネル*--
ストレージアレイ内のすべてのドライブチャネルの情報を表示します表示される情報には、チャネルステータス、リンクステータス（該当する場合）、ドライブ数、および累積エラー数があります。
** * shelves *--
ストレージアレイ内のすべてのシェルフの情報を表示します。表示される情報には、ドライブタイプとシェルフの各コンポーネントのステータス情報があります。シェルフコンポーネントには、バッテリパック、Small Form-factor Pluggable（SFP）トランシーバ、電源/ファンキャニスター、入出力モジュール（IOM）キャニスターなどがあります。ストレージアレイでセキュリティキーが使用されている場合は、[ハードウェア]セクションにセキュリティキー識別子も表示されます。

 a|
特徴
 a|
インストールされている機能パックのリストと、ホストまたはホストクラスタあたりのSnapshotグループ、Snapshot（レガシー）、ボリュームの最大許容数が表示されます。[機能]セクションの情報には、ドライブセキュリティ（ストレージアレイでセキュリティが有効になっているか無効になっているか）も含まれます。

|===
====
. ストレージアレイプロファイルを検索するには、検索キーワードを*検索*テキストボックスに入力し、*検索*をクリックします。
+
一致するすべての用語が強調表示されます。すべての結果を一度に 1 つずつスクロールするには、* 検索 * をクリックします。

. ストレージアレイプロファイルを保存するには、* Save *をクリックします。
+
ブラウザのDownloadsフォルダにという名前でファイルが保存されます `storage-array-profile.txt`。

[[ID3e5712879506db49a9a2c55cd78b001e]]
= ソフトウェアとファームウェアのインベントリの表示

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


[role="lead"]
ソフトウェアとファームウェアのインベントリには、ストレージアレイ内の各コンポーネントのファームウェアバージョンがリストされます。

.タスクの内容
ストレージアレイは、コントローラ、ドライブ、ドロワー、入出力モジュール（IOM）などの多数のコンポーネントで構成されます。これらの各コンポーネントにはファームウェアが含まれています。ファームウェアの一部のバージョンは、他のバージョンのファームウェアに依存します。ストレージアレイ内のすべてのファームウェアバージョンに関する情報を取得するには、ソフトウェアとファームウェアのインベントリを表示します。テクニカルサポートは、ソフトウェアとファームウェアのインベントリを分析して、ファームウェアの不一致を検出できます。

.手順
. メニューを選択します。Support [サポートセンター]>[サポートリソース]タブ。
. 下にスクロールして「Launch detailed storage array information」*と進み、「*Software and Firmware Inventory」を選択します。
+
Software and Firmware Inventoryレポートが画面に表示されます。

. ソフトウェアとファームウェアのインベントリを保存するには、*保存*をクリックします。
+
ブラウザのDownloadsフォルダにファイル名が付けられて保存され `firmware-inventory.txt`ます。

. テクニカルサポートの指示に従って、ファイルをテクニカルサポートに送信します。




:leveloffset: -1


= 診断データの収集

:leveloffset: +1


[[IDec8235287141bba83228c67b8d1b6afa]]
= 手動でのサポートデータの収集
:allow-uri-read:
```

```
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
ストレージアレイに関するさまざまな種類のインベントリ、ステータス、およびパフォーマンスデータを1つのファイルに収集できます。テクニカルサポートは、このファイルをトラブルシューティングや詳細な分析に使用できます。

.タスクの内容

AutoSupport 機能が有効になっている場合は、* AutoSupport タブに移動し、 AutoSupport ディスパッチを送信*を選択して、このデータを収集することもできます。

収集処理は一度に1つだけ実行できます。別の処理を開始しようとすると、エラーメッセージが表示されます。

この処理は、テクニカルサポートから指示があった場合にのみ実行してください。

手順

1. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
2. 「サポートデータの収集」を選択します。
3. [**Collect**](収集) をクリックします

   ブラウザのDownloadsフォルダにという名前でファイルが保存されます `support-data.7z`。シェルフにドロワーが搭載されている場合、そのシェルフの診断データはという別の圧縮ファイルにアーカイブされます `tray-component-state-capture.7z`。

4. テクニカルサポートの指示に従って、ファイルをテクニカルサポートに送信します。

構成データの収集

ボリュームグループとディスクプールのすべてのデータを含むRAID構成データをコントローラから保存できます。その後、データのリストアについてテクニカルサポートにお問い合わせください。

タスクの内容

このタスクでは、RAID構成データベースの現在の状態を保存する方法について説明します。このデータは、コントローラのRPAメモリ位置から取得されます。

構成データの収集機能では、のCLIコマンドと同じ情報が保存されます `save storageArray dbmDatabase`。

このタスクは、Recovery Guruの処理またはテクニカルサポートから指示があった場合にのみ実行してください。

手順

1. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
2. [構成データの収集 *] を選択します。
3. ダイアログボックスで、* Collect *をクリックします。

   ファイルが `configurationData-<arrayName>-<dateTime>.7z`ブラウザのDownloadsフォルダに保存されます。

4. ファイルの送信とシステムへのデータのロードの詳細については、テクニカルサポートにお問い合わせください。

リカバリサポートファイルの取得

テクニカルサポートは、リカバリサポートファイルを使用して問題のトラブルシューティングを行うことができます。これらのファイルはSystem Managerで自動的に保存されます。

開始する前に

テクニカルサポートから、トラブルシューティング用に追加のファイルを送信するように依頼されました。

タスクの内容

リカバリサポートファイルには、次のタイプのファイルが含まれます。

- サポートデータファイル
- AutoSupportの歴史
- AutoSupportログ
- SAS / RLS診断ファイル
- リカバリプロファイルデータ
- データベースキャプチャファイル

手順

1. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
2. リカバリサポートファイルの取得*を選択します。

   ダイアログボックスに、ストレージアレイで収集されたすべてのリカバリサポートファイルが表示されます。特定のファイルを検索するには、任意の列を並べ替えるか、*フィルター*ボックスに文字を入力します。

3. ファイルを選択し、*ダウンロード*をクリックします。

   ブラウザのDownloadsフォルダにファイルが保存されます。

4. 追加のファイルを保存する必要がある場合は、前の手順を繰り返します。
5. [* 閉じる *] をクリックします。
6. テクニカルサポートの指示に従って、ファイルをテクニカルサポートに送信します。

トレースバッファの取得

コントローラからトレースバッファを取得し、分析用にファイルをテクニカルサポートに送信できます。

タスクの内容

ファームウェアはトレースバッファを使用して、デバッグに役立つ可能性のある処理（特に例外条件）を記録します。トレースバッファを取得する際、ストレージアレイの処理を中断することなく、パフォーマンスへの影響を最小限に抑えることができます。

この処理は、テクニカルサポートから指示があった場合にのみ実行してください。

手順

1. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
2. [トレースバッファの取得*]を選択します。
3. トレースバッファを取得する各コントローラの横にあるチェックボックスを選択します。

   一方または両方のコントローラを選択することができます。チェックボックスの右側にあるコントローラステータスメッセージが[Failed]または[Disabled]の場合、このチェックボックスは無効になります。

4. 「 * はい * 」をクリックします。

   ブラウザのDownloadsフォルダにファイル名が付けられて保存され `trace-buffers.7z`ます。

5. テクニカルサポートの指示に従って、ファイルをテクニカルサポートに送信します。

I/Oパス統計の収集

I/Oパス統計のファイルを保存して、分析用にテクニカルサポートに送信できます。

タスクの内容

テクニカルサポートは、I/Oパス統計を使用してパフォーマンスの問題を診断します。アプリケーションのパフォーマンスの問題は、メモリ利用率、CPU利用率、ネットワーク遅延、I/O遅延などの問題が原因で発生することがあります。I/Oパス統計はサポートデータの収集時に自動的に収集されますが、手動で収集することもできます。また、AutoSupportを有効にしている場合は、I/Oパス統計が自動的に収集されてテクニカルサポートに送信されます。

I/Oパス統計の収集を確定すると、I/Oパス統計のカウンタはリセットされます。あとで処理をキャンセルした場合でも、カウンタはリセットされます。カウンタは、コントローラのリセット（リブート）時にもリセットされます。

この処理は、テクニカルサポートから指示があった場合にのみ実行してください。

手順

1. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
2. [**Collect I/O Path Statistics**]を選択します。
3. と入力して処理を確定し `collect`、*[収集]*をクリックします。

ブラウザのDownloadsフォルダにファイル名が付けられて保存され `io-path-statistics.7z`ます。

4. テクニカルサポートの指示に従って、ファイルをテクニカルサポートに送信します。

ヘルスイメージの取得

コントローラのヘルスイメージを確認できます。ヘルスイメージは、コントローラのプロセッサメモリの生データダンプです。テクニカルサポートは、コントローラの問題を診断するために使用できます。

タスクの内容

ファームウェアが特定のエラーを検出すると、自動的にヘルスイメージが生成されます。ヘルスイメージが生成されると、エラーが発生したコントローラがリブートし、イベントがイベントログに記録されます。

AutoSupportを有効にしている場合は、ヘルスイメージがテクニカルサポートに自動的に送信されます。AutoSupportを有効にしていない場合は、ヘルスイメージを取得して分析用に送信する手順について、テクニカルサポートにお問い合わせください。

この処理は、テクニカルサポートから指示があった場合にのみ実行してください。

手順

1. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
2. [ヘルスイメージの取得]を選択します。

   ファイルをダウンロードする前に、詳細セクションでヘルスイメージのサイズを確認できます。

3. [**Collect**](収集) をクリックします

   ブラウザのDownloadsフォルダにという名前でファイルが保存されます `health-image.7z`。

4. テクニカルサポートの指示に従って、ファイルをテクニカルサポートに送信します。

リカバリ操作の実行

読み取り不能セクターのログの表示

読み取り不能セクターのログを保存し、分析用にファイルをテクニカルサポートに送信できます。

タスクの内容

読み取り不能セクターのログには、リカバリ不能なメディアエラーが報告されたドライブが原因で発生した読み取り不能セクターの詳細なレコードが含まれます。読み取り不能セクターは、通常のI/Oおよび変更処理（再構築など）の実行中に検出されます。読み取り不能セクターがストレージアレイで検出されると、ストレージアレイに対する要注意アラートが表示されます。Recovery Guruでは、注意すべき読み取り不能セクターの状態を識別します。読み取り不能セクターに格納されているデータはリカバリできないため、失われたとみなされます。

読み取り不能セクターのログには、最大1、000個の読み取り不能セクターを格納できます。読み取り不能セクターのログのエントリ数が1、000に達すると、次の条件が適用されます。

- 再構築中に読み取り不能セクターが新しく検出された場合は、再構築が失敗し、エントリがログに記録されません。
- I/O中に読み取り不能セクターが新しく検出された場合は、I/Oが失敗し、エントリがログに記録されません。

これらのアクションには、オーバーフロー前に成功していたRAID 5書き込みとRAID 6書き込みが含まれます。

データが失われる可能性--読み取り不能セクターからのリカバリは複雑な手順 であり、さまざまな方法を使用する可能性があります。この処理は、テクニカルサポートから指示があった場合にのみ実行してください。

手順

1. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
2. 読み取り不能セクターの表示/消去*を選択します。
3. 読み取り不能セクターのログを保存するには、次の手順に従います。

   a. テーブルの最初の列で、読み取り不能セクターのログを保存するボリュームを個別に選択する（各ボリュームの横にあるチェックボックスをオンにする）か、テーブルのヘッダーにあるチェックボックスをオンにしてすべてのボリュームを選択できます。

      特定のボリュームを検索するには、任意の列をソートしたり、* Filter *ボックスに文字を入力したりできます。

   b. [保存（ Save ）] をクリックします。

   ブラウザのDownloadsフォルダにという名前でファイルが保存されます `unreadable-sectors.txt`。

4. テクニカルサポートから読み取り不能セクターのログを消去するように指示された場合は、次の手順を実行します。

   a. テーブルの最初の列で、読み取り不能セクターのログを消去するボリュームを個別に選択する（各ボリュームの横にあるチェックボックスをオンにする）か、テーブルのヘッダーにあるチェックボックスをオンにしてすべてのボリュームを選択できます。

   b. [* Clear*](クリア)をクリックし'操作を実行することを確認します

ドライブポートの再有効化

誤配線状態からリカバリするための修正措置が実施されたことをコントローラに示すことができます。

手順

1. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
2. ドライブポートを再度有効にする*を選択し、処理を確定します。

   このオプションは、ストレージアレイに無効なドライブポートがある場合にのみ表示されます。

   誤配線が検出されたときに無効になったSASポートが、コントローラによって再有効化されます。

ストレージアレイ構成をリストアしたら、リカバリモードのクリア処理を使用してストレージアレイでのI/Oを再開し、通常の動作に戻します。

開始する前に

- ストレージアレイを以前の構成に戻す場合は、リカバリモードをクリアする前にバックアップから設定をリストアする必要があります。
- リストアが正常に完了したことを確認するには、検証チェックを実行するか、テクニカルサポートに確認する必要があります。リストアが正常に完了したことを確認したら、リカバリモードをクリアできます。

タスクの内容

ストレージアレイには、論理構成（プール、ボリュームグループ、ボリュームなど）が記録された構成データベースが格納されています。ストレージアレイ構成を意図的にクリアした場合、または構成データベースが破損した場合、ストレージアレイはリカバリモードになります。リカバリモードではI/Oが停止し、構成データベースがフリーズされるため、次のいずれかの処理を実行できます。

- コントローラのフラッシュデバイスに保存されている自動バックアップから設定を復元します。この処理を実行するには、テクニカルサポートにお問い合わせください。
- 前回の構成データベース保存処理から構成をリストアします。構成データベースの保存処理は、コマンドラインインターフェイス（CLI）を使用して実行します。
- ストレージアレイを最初から再構成します。

ストレージアレイ構成をリストアまたは再定義し、すべて問題がないことを確認したら、リカバリモードを手動でクリアする必要があります。

> リカバリモードのクリア処理は開始後にキャンセルすることはできません。リカバリモードのクリアには時間がかかることがあります。この処理は、テクニカルサポートから指示があった場合にのみ実行してください。

手順

1. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
2. リカバリモードのクリア*を選択し、この処理を実行することを確認します。

   このオプションは、ストレージアレイがリカバリモードの場合にのみ表示されます。

AutoSupportの管理

AutoSupport機能の概要

AutoSupport機能は、ストレージアレイの健常性を監視し、テクニカルサポートに自動ディスパッチを送信します。

テクニカルサポートは、AutoSupportデータをリアクティブに使用してお客様の問題の診断と解決を迅速化し、潜在的な問題をプロアクティブに検出して回避します。

AutoSupportデータには、ストレージアレイの構成、ステータス、パフォーマンス、およびシステムイベントに関する情報が含まれます。AutoSupport データにユーザデータが含まれることはありません。ディスパッチ

はすぐに送信することも、スケジュールに従って送信することもできます（日次および週次）。

主なメリット

AutoSupport機能の主なメリットは次のとおりです。

- ケースの解決時間の短縮
- 高度な監視でインシデント管理を迅速化
- スケジュールに基づく自動レポート、および重大イベントに関する自動レポート
- 選択したコンポーネント（ドライブなど）のハードウェア交換要求を自動化
- 問題が発生した場合は、お客様の邪魔にならない方法で通知し、テクニカルサポートが修正措置を講じるための情報を提供します。
- ディスパッチを監視して構成に関する既知の問題を検出するAutoSupport分析ツール

個々の**AutoSupport**機能

AutoSupport 機能は、個別に有効にする3つの機能で構成されています。

- *Basic AutoSupport *--ストレージ・アレイが自動的にデータを収集してテクニカル・サポートに送信することを可能にします
- * AutoSupport OnDemand*--問題 のトラブルシューティングに必要なときに、テクニカルサポートが以前のAutoSupport ディスパッチの再送信を要求できるようにします。転送はすべて、AutoSupportサーバではなくストレージアレイから開始されます。ストレージアレイはAutoSupportサーバに定期的にコンタクトし、保留中の再送信要求がないかどうかをチェックし、適切に応答します。
- リモート診断--問題 のトラブルシューティングに必要な場合に、テクニカルサポートが最新のAutoSupport ディスパッチをリクエストできるようにします。転送はすべて、AutoSupportサーバではなくストレージアレイから開始されます。ストレージアレイはAutoSupportサーバに定期的にコンタクトし、保留中の新しい要求がないかどうかをチェックし、適切に応答します。

AutoSupportとサポートデータの収集の違い

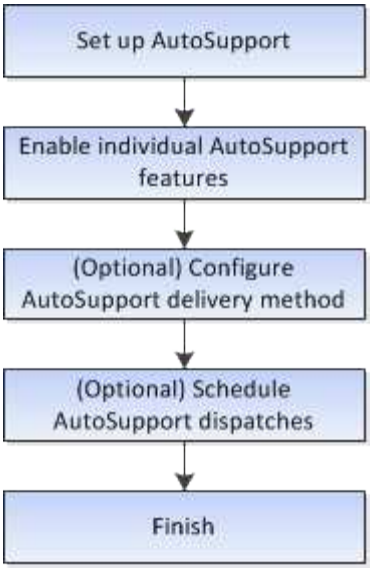
ストレージアレイでは、次の2つの方法でサポートデータを収集できます。

- * AutoSupport 機能*--データが自動的に収集されます。
- サポートデータの収集オプション--データを収集して手動で送信する必要があります。

データが自動的に収集されて送信されるため、AutoSupport機能の方が簡単です。AutoSupportデータをプロアクティブに使用して、問題を未然に防止できます。AutoSupport機能を使用すると、テクニカルサポートがデータにアクセスできるため、トラブルシューティングにかかる時間が短縮されます。このような理由から、AutoSupport機能を使用することを推奨します。

AutoSupport機能のワークフロー

System Managerでは、次の手順でAutoSupport機能を設定します。



AutoSupport機能の有効化または無効化

AutoSupport機能およびAutoSupportの個 々 の機能は、初期セットアップ時に有効にすることも、あとから有効または無効にすることもできます。

開始する前に

AutoSupport OnDemandまたはRemote Diagnosticsを有効にする場合は、AutoSupport の配信方法をHTTPSに設定する必要があります。

タスクの内容

AutoSupport機能はいつでも無効にできますが、有効のままにしておくことを強く推奨します。AutoSupport機能を有効にすると、ストレージアレイに問題が発生した場合に、迅速に原因を特定して解決できます。

AutoSupport 機能は、個別に有効にする3つの機能で構成されています。

- *Basic AutoSupport *--ストレージ・アレイが自動的にデータを収集してテクニカル・サポートに送信することを可能にします
- * AutoSupport OnDemand*--問題 のトラブルシューティングに必要なときに、テクニカルサポートが以前のAutoSupport ディスパッチの再送信を要求できるようにします。転送はすべて、AutoSupportサーバではなくストレージアレイから開始されます。ストレージアレイはAutoSupportサーバに定期的にコンタクトし、保留中の再送信要求がないかどうかをチェックし、適切に応答します。
- リモート診断--問題 のトラブルシューティングに必要な場合に、テクニカルサポートが最新のAutoSupport ディスパッチをリクエストできるようにします。転送はすべて、AutoSupportサーバではなくストレージアレイから開始されます。ストレージアレイはAutoSupportサーバに定期的にコンタクトし、保留中の新しい要求がないかどうかをチェックし、適切に応答します。

手順

1. メニューを選択AutoSupport します。[Support Center]>[Support]（サポートセンター）タブ。
2. AutoSupport 機能の有効化/無効化*を選択します。
3. 有効にするAutoSupport機能の横にあるチェックボックスをオンにします。

   ダイアログボックス内の項目のインデントによって示されるように、フィーチャーは相互に依存します。

たとえば、Remote Diagnosticsを有効にするには、まずAutoSupport OnDemandを有効にする必要があります。

4. [保存（ Save ）] をクリックします。

   AutoSupportを無効にすると、ホームページに通知が表示されます。[無視]をクリックすると、通知を閉じることができます。

AutoSupportの配信方法の設定

AutoSupport機能では、テクニカルサポートにディスパッチを配信するために、HTTPS、HTTP、SMTPの各プロトコルがサポートされています。

開始する前に

- AutoSupport機能を有効にする必要があります。有効になっているかどうかは、AutoSupportページで確認できます。
- ネットワークにDNSサーバをインストールし、設定する必要があります。DNSサーバのアドレスがSystem Managerで設定されている必要があります（このタスクは[ハードウェア]ページから実行できます）。

タスクの内容

各プロトコルを確認します。

- * HTTPS *-- HTTPSを使用して、テクニカルサポートの宛先サーバーに直接接続できます。AutoSupport OnDemandまたはRemote Diagnosticsを有効にする場合は、AutoSupport の配信方法をHTTPSに設定する必要があります。
- * HTTP *-- HTTPを使用して、テクニカルサポートの宛先サーバーに直接接続できます。
- **Email**-- AutoSupport ディスパッチの配信方法として電子メールサーバーを使用できます

- HTTPS / HTTPとEメールの配信方法*の違い。SMTPを使用するEメール配信方法とHTTPSおよびHTTP配信方法の間には、重要な違いがいくつかあります。まず、Eメールではディスパッチのサイズが5MBに制限されるため、ASUPデータ収集の一部はディスパッチされません。次に、AutoSupport OnDemand機能は、HTTPPおよびHTTPSメソッドでのみ使用できます。

手順

1. メニューを選択AutoSupport します。[Support Center]>[Support]（サポートセンター）タブ。
2. AutoSupport 配信方法の設定 * を選択します。

   ディスパッチの配信方法を示すダイアログボックスが表示されます。

3. 目的の配信方法を選択し、その配信方法のパラメータを選択します。次のいずれかを実行します。
   - [HTTPS]または[HTTP]を選択した場合は、次のいずれかの配信パラメータを選択します。
     - * direct*--このデリバリパラメータはデフォルトで選択されています。このオプションを選択すると、HTTPSまたはHTTPプロトコルを使用してテクニカルサポートのデスティネーションシステムに直接接続できます。
     - プロキシ・サーバ経由--このオプションを選択すると’テクニカル・サポート・システムとの接続を

確立するために必要なHTTPプロキシ・サーバの詳細を指定できますホストアドレスとポート番号を指定する必要があります。ただし、ホスト認証の詳細（ユーザ名とパスワード）を入力する必要があるのは、必要な場合だけです。

- プロキシ自動設定（**PAC**）スクリプト経由-- Proxy Auto-Configuration（PAC）スクリプトファイルの場所を指定します。PACファイルを使用すると、テクニカルサポートのデスティネーションシステムとの接続を確立するために適切なプロキシサーバが自動的に選択されます。

◦ [Email]を選択した場合は、次の情報を入力します。

- メールサーバのアドレス（完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレス）。
- AutoSupportディスパッチEメールの[差出人]フィールドに表示されるEメールアドレス。
- オプション。設定テストを実行する場合：AutoSupport システムがテストディスパッチを受信したときに確認が送信されるEメールアドレス。
- メッセージを暗号化する場合は、暗号化タイプとして*SMTPS*または*STARTTLS *を選択し、暗号化されたメッセージのポート番号を選択します。それ以外の場合は、*なし*を選択します。
- 必要に応じて、送信元およびメールサーバとの認証に使用するユーザ名とパスワードを入力します。

4. これらのASUPディスパッチの配信をファイアウォールでブロックしている場合は、次のURLをホワイトリストに追加します。 `https://support.netapp.com/put/AsupPut/`
5. Test Configuration *をクリックして、指定された配信パラメータを使用してテクニカルサポートサーバーへの接続をテストします。AutoSupport On-Demand機能を有効にした場合は、AutoSupport OnDemandディスパッチの配信のための接続もシステムでテストされます。

   設定テストに失敗した場合は、設定を確認し、もう一度テストを実行してください。テストが引き続き失敗する場合は、テクニカルサポートにお問い合わせください。

6. [保存（ Save ）] をクリックします。

AutoSupportディスパッチのスケジュール設定

System Managerでは、AutoSupportディスパッチのデフォルトのスケジュールが自動的に作成されます。必要に応じて、独自のスケジュールを指定できます。

開始する前に

AutoSupport機能を有効にする必要があります。有効になっているかどうかは、AutoSupportページで確認できます。

タスクの内容

- 毎日の時刻--毎日のディスパッチが収集され、指定した期間内に毎日送信されます。System Managerは、範囲内のランダムな時間を選択します。時間はすべて協定世界時（UTC）です。これはストレージアレイの現地時間とは異なる場合があります。ストレージアレイのローカル時間をUTCに変換する必要があります。
- 週次日--週次ディスパッチが収集され、週に1回送信されます。System Managerでは、指定した日にちからランダムな日にちが選択されます。週次ディスパッチの実行を許可しない曜日の選択を解除します。System Managerでは、許可した日にちからランダムな日にちが選択されます。
- 週次時間--週次ディスパッチが収集され、指定した期間に週に1回送信されます。System Managerは、範囲内のランダムな時間を選択します。時間はすべて協定世界時（UTC）です。これはストレージアレイの現地時間とは異なる場合があります。ストレージアレイのローカル時間をUTCに変換する必要があります。

手順

1. メニューを選択AutoSupport します。[Support Center]>[Support]（サポートセンター）タブ。
2. 「* AutoSupport ディスパッチのスケジュール設定*」を選択します。

   AutoSupport ディスパッチのスケジュール設定ウィザードが表示されます。
3. ウィザードの手順に従います。

AutoSupportディスパッチの送信

System Managerでは、スケジュールされたディスパッチを待たずにAutoSupportディスパッチをテクニカルサポートに送信できます。

開始する前に

AutoSupport機能を有効にする必要があります。有効になっているかどうかは、AutoSupportページで確認できます。

タスクの内容

この処理では、サポートデータが収集されてテクニカルサポートに自動的に送信され、問題のトラブルシューティングが可能になります。

手順

1. メニューを選択AutoSupport します。[Support Center]>[Support]（サポートセンター）タブ。
2. 「AutoSupport ディスパッチを送信」を選択します。

   [Send AutoSupport Dispatch]ダイアログボックスが表示されます。
3. 「*送信」を選択して操作を確定します。

AutoSupportステータスの表示

AutoSupportページには、AutoSupport機能と個 々 のAutoSupport機能が現在有効になっているかどうかが表示されます。

手順

1. メニューを選択AutoSupport します。[Support Center]>[Support]（サポートセンター）タブ。
2. タブのすぐ下にあるページの右側を見て、基本的なAutoSupport機能が有効になっているかどうかを確認します。
3. 疑問符にカーソルを合わせると、個 々 のAutoSupport機能が有効になっているかどうかが表示されます。

AutoSupportログの表示

AutoSupportログには、ステータス、ディスパッチ履歴、およびAutoSupportディスパッチの配信中に発生したエラーに関する情報が記録されます。

タスクの内容

複数のログファイルが存在する可能性があります。現在のログファイルが200KBに達するとアーカイブされ、

新しいログファイルが作成されます。アーカイブされたログファイルの名前はです `ASUPMessages.n`。_n_には1～9の整数を指定します。複数のログファイルが存在する場合は、最新のログと前のログのどちらを表示するかを選択できます。

- *current log *--キャプチャされた最新のイベントのリストを表示します
- アーカイブログ--以前のイベントのリストを表示します

手順

1. メニューを選択AutoSupport します。[Support Center]>[Support]（サポートセンター）タブ。
2. 「* AutoSupport ログを表示*」を選択します。

   ダイアログボックスが表示され、現在のAutoSupportログが一覧表示されます。

3. 以前のAutoSupport ログを表示するには、[アーカイブ済み]ラジオ・ボタンを選択し、[* AutoSupport ログの選択*]ドロップダウン・リストからログを選択します。

   [Archived]オプションは、ストレージアレイにアーカイブログが存在する場合にのみ表示されます。

   選択したAutoSupportログがダイアログボックスに表示されます。

4. オプション： AutoSupport ログを検索するには、*検索*ボックスにキーワードを入力し、*検索*をクリックします。

   再度*検索*をクリックして、用語のその他の出現箇所を検索します。

AutoSupportメンテナンス時間の有効化

エラーイベント発生時に自動でチケットが作成されないようにするには、AutoSupportメンテナンス期間を有効にします。通常運用モードでは、問題が発生した場合、ストレージアレイはAutoSupportを使用してサポートケースをオープンします。

手順

1. メニューを選択AutoSupport します。[Support Center]>[Support]（サポートセンター）タブ。
2. AutoSupport メンテナンス期間を有効にする*を選択します。
3. メンテナンス時間の要求が処理されたことの確認を受け取るEメールアドレスを入力します。

   設定に応じて、最大5つのEメールアドレスを入力できます。複数のアドレスを追加する場合は、[別の電子メールを追加]を選択して別のフィールドを開きます。

4. メンテナンス時間を有効にする期間（時間）を指定します。

   サポートされる期間は最大で72時間です。

5. 「 * はい * 」をクリックします。

   エラーイベント発生時のAutoSupport自動チケット作成は、指定された期間の間、一時的に抑制されます。

終了後

メンテナンス時間は、ストレージアレイからの要求がAutoSupportサーバで処理されるまで開始されません。ストレージアレイのメンテナンス作業を実行する前に、確認のEメールが届いていることを確認してください。

AutoSupportメンテナンス時間の無効化

エラーイベント発生時に自動でチケットが作成されるようにするには、AutoSupportメンテナンス期間を無効にしてください。AutoSupportのメンテナンス時間を無効にすると、問題が発生した場合、ストレージアレイはAutoSupportを使用してサポートケースをオープンします。

手順

1. メニューを選択AutoSupport します。[Support Center]>[Support]（サポートセンター）タブ。
2. [* AutoSupport メンテナンス期間を無効にする*]を選択します。
3. メンテナンス時間無効化の要求が処理されたことの確認を受け取るEメールアドレスを入力します。

   設定に応じて、最大5つのEメールアドレスを入力できます。複数のアドレスを追加する場合は、[別の電子メールを追加]を選択して別のフィールドを開きます。

4. 「 * はい * 」をクリックします。

   エラーイベント発生時のAutoSupport自動チケット作成が有効になっています。

終了後

メンテナンス時間は、ストレージアレイからの要求がAutoSupportサーバで処理されるまで終了しません。確認のEメールが送信されるまで待ってから、次に進んでください。

イベントの表示

イベントログの概要

イベントログには、ストレージアレイで発生したイベントの履歴レコードが記録されます。これは、テクニカルサポートが障害につながるイベントのトラブルシューティングに役立ちます。

イベントログは、Recovery Guruでストレージアレイイベントを追跡するための補助的な診断ツールとして使用できます。ストレージアレイのコンポーネント障害からのリカバリを試みるときは、必ず最初にRecovery Guruを参照してください。

イベントのカテゴリ

イベントログ内のイベントは、さまざまなステータスで分類されます。処理が必要なイベントのステータスは次のとおりです。

- 重大
- 警告

情報提供のイベントで、すぐに対処する必要がないイベントは次のとおりです。

- 情報

重大イベント

重大イベントは、ストレージアレイに問題があることを示します。重大イベントをすぐに解決すると、データアクセスの中断を回避できる可能性があります。

重大イベントが発生すると、イベントログに記録されます。すべての重大イベントは、SNMP管理コンソールまたはアラート通知を受信するように設定したEメール受信者に送信されます。イベントが発生した時点でシェルフIDが不明な場合、シェルフIDは「Shelf unknown」と記載されます。

重大イベントを受け取った場合は、Recovery Guruの手順で重大イベントの詳細な説明を参照してください。Recovery Guruの手順を実行して重大イベントを修正します。特定の重大イベントを修正するには、テクニカルサポートへの連絡が必要になる場合があります。

イベントログを使用したイベントの表示

ストレージアレイで発生したイベントの履歴レコードを提供するイベントログを表示できます。

手順

1. メニューを選択します。サポート[イベントログ]。

   [Event Log]ページが表示されます。

ページの詳細

項目	製品説明
[すべて表示]フィールド	すべてのイベントを表示するか、重大イベントと警告イベントのみを表示するかを切り替えます。
フィルタフィールド	イベントをフィルタします。特定のコンポーネントやイベントなどに関連するイベントのみを表示する場合に便利です。
[列の選択]アイコン	表示する他の列を選択できます。その他の列には、イベントに関する追加情報が表示されます。
チェックボックス	保存するイベントを選択できます。テーブルヘッダーのチェックボックスをオンにすると、すべてのイベントが選択されます。
[日付/時刻]列	コントローラクロックに応じたイベントの日時スタンプ。 イベントログでは、最初にシーケンス番号に基づいてイベントがソートされます。通常、このシーケンスは日付と時刻に対応します。ただし、ストレージアレイ内の2つのコントローラクロックは同期されていない可能性があります。この場合、イベントログには、表示されているイベントと日時に一部の不整合が記録されることがあります。
[優先度]列	優先度の値は次のとおりです。 • クリティカル--ストレージアレイに問題がありますただし、すぐに対処すると、データへのアクセスが失われないようにすることができます。重大イベントはアラート通知に使用されます。すべての重大イベントは、ネットワーク管理クライアント（SNMPトラップ経由）または設定したEメール受信者に送信されます。 • 警告--ストレージアレイのパフォーマンスと機能を低下させて別のエラーから回復するエラーが発生しました • 情報--ストレージアレイに関連する重要でない情報。
[コンポーネントタイプ]列	イベントの影響を受けるコンポーネント。コンポーネントには、ドライブやコントローラなどのハードウェアや、コントローラファームウェアなどのソフトウェアがあります。
[コンポーネントの場所]列	ストレージアレイ内のコンポーネントの物理的な場所。
[説明]列	イベントの説明。 例-- `Drive write failure - retries exhausted`

項目	製品説明
[シーケンス番号]列	ストレージアレイの特定のログエントリを一意に識別する64ビットの番号。この数は、新しいイベントログエントリごとに1ずつ増加します。この情報を表示するには、列の選択*アイコンをクリックします。
[イベントタイプ]列	ログに記録される各イベントタイプを識別する4桁の番号。この情報を表示するには、列の選択*アイコンをクリックします。
[イベント固有のコード]列	この情報はテクニカルサポートが使用します。この情報を表示するには、列の選択*アイコンをクリックします。
[イベントカテゴリ]列	• 障害：ドライブ障害やバッテリ障害など’ストレージアレイのコンポーネントに障害が発生した • 状態の変更–状態が変更されたストレージアレイの要素。たとえば、ボリュームが最適ステータスに移行した場合や、コントローラがオフラインステータスに移行した場合などです。 • **Internal** ：ユーザの操作を必要としない内部コントローラ操作。たとえば、コントローラが一日の開始を完了した場合など。 • コマンド–ホットスペアが割り当てられているなど、ストレージアレイに対して発行されたコマンド。 • エラー–ストレージアレイでエラー状態が検出されました。たとえば、コントローラがキャッシュを同期およびパージできない、ストレージアレイで冗長性エラーが検出されたなどです。 • 一般–他のカテゴリには適していないイベント。この情報を表示するには'[列の選択]アイコンをクリックします
[ログ元]列	イベントを記録したコントローラの名前。この情報を表示するには'[列の選択]アイコンをクリックします

2. ストレージアレイから新しいイベントを取得するには'[更新]をクリックします

   イベントがログに記録され、[イベントログ]ページに表示されるまでに数分かかる場合があります。

3. イベントログをファイルに保存するには、次の手順を実行します。
   a. 保存する各イベントの横にあるチェックボックスをオンにします。
   b. [保存（ Save ）] をクリックします。

      ブラウザのDownloadsフォルダにという名前でファイルが保存されます `major-event-log-timestamp.log`。

4. イベントログからイベントをクリアするには、次の手順に従います。

   イベントログには約8、000件のイベントが格納されてから、1つのイベントが新しいイベントに置き換えられます。イベントを保持する場合は、保存してイベントログからクリアできます。

a. まず、イベントログを保存します。

b. [すべてクリア]をクリックし、操作を実行することを確認します。

アップグレードの管理

アップグレードセンターの概要

アップグレードセンターを使用して、最新のソフトウェアとファームウェアをダウンロードし、コントローラとドライブをアップグレードします。

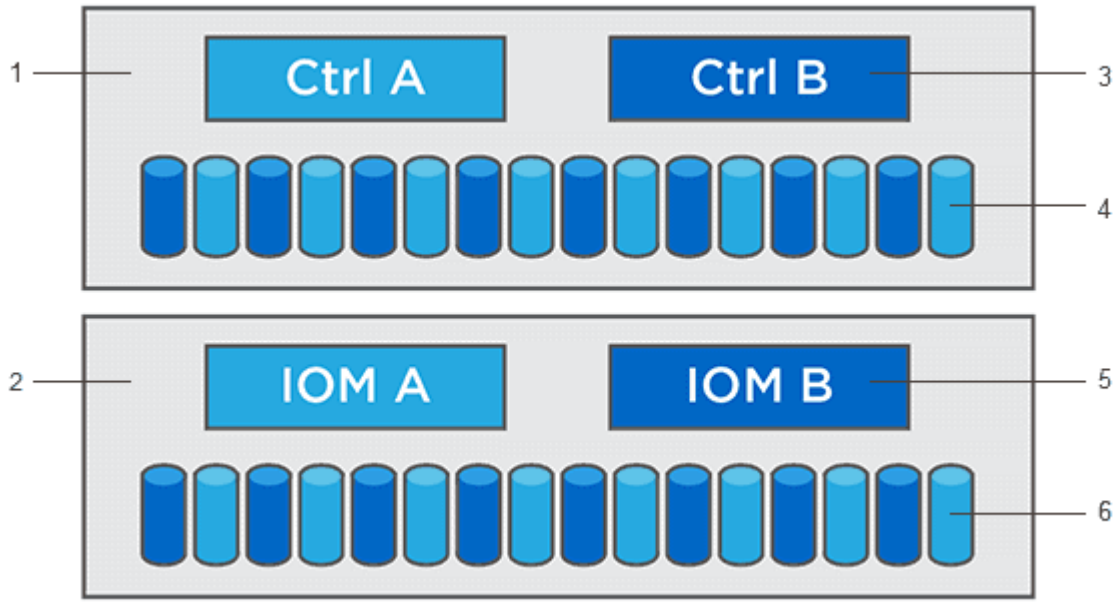
コントローラのアップグレードの概要

ストレージアレイのソフトウェアとファームウェア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できます。

OSコントローラのアップグレードに含まれるコンポーネント

ストレージアレイのコンポーネントには、ときどきアップグレードが必要になるソフトウェアやハードウェアが含まれています。

- 管理ソフトウェア-- System Managerはストレージ・アレイを管理するソフトウェアです
- * コントローラファームウェア *— コントローラファームウェアは、ホストとボリューム間の I/O を管理します。
- * コントローラ NVSRAM *— コントローラ NVSRAM は、コントローラのデフォルト設定を指定するコントローラファイルです。
- * IOM ファームウェア * - I/O モジュール（ IOM ）ファームウェアは、コントローラとドライブシェルフの間の接続を管理します。また、コンポーネントのステータスも監視します。
- * スーパーバイザー・ソフトウェア *— スーパーバイザー・ソフトウェアは、ソフトウェアが実行されるコントローラ上の仮想マシンです。



[1]コントローラシェルフ；[2]ドライブシェルフ；3^ソフトウェア、コントローラファームウェア、コントローラNVSRAM、 スーパーバイザーソフトウェア、[4]Driveファームウェア、[5]IOMファームウェア、[6]Driveファームウェア

現在のソフトウェアとファームウェアのバージョンは、[ソフトウェアとファームウェアのインベントリ]ダイアログボックスで確認できます。[Upgrade Center] メニューに移動し、 [* Software and Firmware Inventory] のリンクをクリックします。

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できるように、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場合があります。該当するかどうかを確認するには、を参照してください "NetApp Interoperability Matrix Toolで確認できます"。

I/Oを停止するタイミング

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の処理を続行できます。アップグレードでは、コントローラAがすべてのボリュームをコントローラBにフェイルオーバーしてアップグレードされ、ボリュームとコントローラBのすべてのボリュームがテイクバックされてから、コントローラBがアップグレードされます。

アップグレード前の健全性チェック

アップグレード前の健常性チェックは、アップグレードプロセスの一環として実行されます。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かどうかがチェックされます。アップグレードを実行できない状況は次のとおりです。

- 割り当て済みドライブで障害が発生
- ホットスペアを使用中です
- ボリュームグループに不備がある
- 同時に実行できない処理
- ボリュームが見つからない
- コントローラのステータスが最適でない
- イベントログイベントの数が多すぎる
- 構成データベースの検証エラー
- 古いバージョンのDACstoreを搭載したドライブ

アップグレード前の健常性チェックは、アップグレードとは別に実行することもできます。

ドライブのアップグレードの概要

ドライブファームウェアは、ドライブの下位レベルの動作特性を制御します。新しい機能の追加、パフォーマンスの向上、不具合の修正を目的として、ドライブのメーカーからドライブファームウェアの更新が定期的にリリースされます。

ドライブファームウェアのオンラインアップグレードとオフラインアップグレード

ドライブファームウェアのアップグレード方法には、オンラインとオフラインの2種類があります。

オンライン

オンラインアップグレードでは、ドライブが一度に1つずつ順番にアップグレードされます。ストレージアレイはアップグレードの実行中もI/Oの処理を継続します。I/Oを停止する必要はありません。オンラインアップグレードが可能なドライブの場合は、自動的にオンライン方式が使用されます。

オンラインアップグレードを実行できるドライブは次のとおりです。

- 最適な状態のプール内のドライブ
- 最適な冗長性が確保されたボリュームグループ内のドライブ（RAID 1、RAID 5、およびRAID 6）
- 未割り当てのドライブ
- スタンバイのホットスペアドライブ

ドライブファームウェアのオンラインアップグレードには数時間かかることがあり、ストレージアレイでボリューム障害が発生する可能性があります。ボリューム障害は、次の場合に発生する可能性があります。

- RAID 1またはRAID 5のボリュームグループで、ボリュームグループ内の別のドライブのアップグレード中に1本のドライブで障害が発生した場合。
- RAID 6のプールまたはボリュームグループで、プールまたはボリュームグループ内の別のドライブのアップグレード中に2本のドライブで障害が発生した場合。

オフライン（並行処理）

オフラインアップグレードでは、ドライブタイプが同じすべてのドライブが同時にアップグレードされます。この方法では、選択したドライブに関連付けられているボリュームへのI/Oアクティビティを停止する必要があります。複数のドライブを同時に並行してアップグレードできるため、全体的なダウンタイムは大幅に短縮されます。オフラインアップグレードしか実行できないドライブの場合は、自動的にオフライン方式が使用されます。

次のドライブではオフライン方式を使用する必要があります。

- 非冗長ボリュームグループ内のドライブ（RAID 0）
- 最適な状態でないプールまたはボリュームグループ内のドライブ
- SSDキャッシュ内のドライブ

互換性

各ドライブファームウェアファイルには、ファームウェアが実行されるドライブタイプに関する情報が含まれています。指定したファームウェアファイルは互換性があるドライブにのみダウンロードできます。アップグレードプロセスの実行中に、 System Manager で自動的に互換性がチェックされます。

コントローラのソフトウェアとファームウェアのアップグレード

ストレージアレイのソフトウェア、および必要に応じてIOMファームウェアと不揮発性静的ランダムアクセスメモリ（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することができます。

開始する前に

- IOMファームウェアをアップグレードするかどうかを決めます。

  通常は、すべてのコンポーネントを同時にアップグレードする必要があります。ただし、 IOM ファームウェアを SANtricity OS ソフトウェアアップグレードの一部としてアップグレードしない場合や、テクニカルサポートから IOM ファームウェアをダウングレードするよう依頼された場合は（ファームウェアのダウングレード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）、アップグレードを中止することもできます。

- コントローラNVSRAMファイルをアップグレードするかどうかを決めます。

  通常は、すべてのコンポーネントを同時にアップグレードする必要があります。ただし、コントローラのNVSRAMファイルにパッチを適用している場合や、ファイルがカスタムバージョンであり、上書きしたくない場合は、アップグレードしないこともできます。

- OSのアップグレードを今すぐアクティブ化するかあとでアクティブ化するかを決めておきます。

  あとでアクティブ化する理由は次のとおりです。

  - 時間帯--ソフトウェアとファーム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

- セキュリティ保護されていないドライブまたは内部で保護されたドライブから切り替えて、ドライブセキュリティに外部キー管理サーバ（KMS）を使用するかどうかを確認します。
- ストレージアレイでロールベースアクセス制御を使用するかどうかを確認しておきます。

タスクの内容

OSソフトウェアファイルのみをアップグレードするか、コントローラNVSRAMファイルのみをアップグレードするか、両方のファイルをアップグレードするかを選択できます。

この処理は、テクニカルサポートから指示があった場合にのみ実行してください。

- 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。ストレージアレイへの電源を維持します。

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インストール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. メニューを選択します。Support [Upgrade Center]を選択します。
3. 新しいファイルをサポートサイトから管理クライアントにダウンロードします。

   a. ネットアップサポートをクリックして、サポートWebサイトを起動します。

   b. サポートWebサイトで、* Downloads （ダウンロード）タブをクリックし、 Downloads *（ダウンロード）を選択します。

   c. EシリーズSANtricity OSコントローラソフトウェア*を選択します。

d. 残りの手順に従います。

バージョン8.42以降では、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。

4. この時点でIOMファームウェアをアップグレードしない場合は、* IOMの自動同期を中断*をクリックします。

   ストレージアレイにコントローラが1台しかない場合、IOMファームウェアはアップグレードされません。

5. SANtricity OSソフトウェアアップグレードで、*アップグレードの開始*をクリックします。

   [Upgrade SANtricity OS Software]ダイアログボックスが表示されます。

6. アップグレードプロセスを開始するファイルを1つ以上選択します。

   a. SANtricity OSソフトウェアファイルを選択するには、「*参照」をクリックし、サポートWebサイトからダウンロードしたOSソフトウェアファイルを選択します。

   b. 参照 * をクリックし、サポートサイトからダウンロードした NVSRAM ファイルに移動して、コントローラ NVSRAM ファイルを選択します。コントローラNVSRAMファイルの名前は、のようになります。 `N2800-830000-000.dlp`

      次のアクションが実行されます。

      - デフォルトでは、現在のストレージアレイ構成と互換性のあるファイルのみが表示されます。
      - アップグレードするファイルを選択すると、ファイルの名前とサイズが表示されます。

7. *オプション：*アップグレードするSANtricity OSソフトウェアファイルを選択した場合、*ファイルを今すぐ転送するが、アップグレードしない（後でアップグレードをアクティブ化する）*チェックボックスをオンにして、ファイルをコントローラに転送することができます。

8. [* スタート *] をクリックし、操作を確定します。

   アップグレード前の健常性チェックの実行中は処理をキャンセルできますが、転送中またはアクティブ化中はキャンセルできません。

9. *オプション：*アップグレードされた内容のリストを表示するには、*ログの保存*をクリックします。

   ブラウザのDownloadsフォルダにという名前でファイルが保存されます `drive_upgrade_log-timestamp.txt`。

終了後

- ハードウェアページにすべてのコンポーネントが表示されていることを確認します。
- [Software and Firmware Inventory] ダイアログボックスをチェックして、新しいソフトウェアとファームウェアのバージョンを確認します（ [Menu] ： [Upgrade Center] を選択し、 [* Software and Firmware Inventory] のリンクをクリックします）。
- コントローラNVSRAMをアップグレードした場合、既存のNVSRAMに適用したカスタム設定はアクティブ化のプロセスで失われます。アクティブ化のプロセスが完了したら、NVSRAMにカスタム設定を再度適用する必要があります。

アップグレードファイルはすぐにアクティブ化することも、都合の良いタイミングでアクティブ化することもできます。

タスクの内容

アクティブ化せずにファイルをダウンロードして転送できます。あとでアクティブ化する理由は次のとおりです。

- 時間帯--ソフトウェアとファーム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

ソフトウェアまたはファームウェアの転送は完了していてもアクティブ化されていない場合は、System Managerのホームページの通知領域とアップグレードセンターのページに通知が表示されます。

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. メニューを選択します。Support [Upgrade Center]を選択します。
2. SANtricity OS Controller Software upgrade（OSコントローラソフトウェアのアップグレード）というラベルの付いた領域で、* Activate（アクティブ化）*をクリックし、操作を実行することを確認します。

   アップグレード前の健常性チェックの段階で処理をキャンセルすることはできますが、アクティブ化の実行中はキャンセルできません。

   アップグレード前の健常性チェックが開始されます。アップグレード前の健常性チェックに合格すると、アップグレードプロセスはファイルのアクティブ化に進みます。アップグレード前の健常性チェックに失敗した場合は、Recovery Guruを使用するかテクニカルサポートに連絡して問題を解決してください。一部の種類の条件では、*アップグレードを許可*チェックボックスを選択してエラーが発生しても、テクニカルサポートからアップグレードを続行するようにアドバイスされる場合があります。

   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するコンポーネントによって異なります。

3. *オプション：*アップグレードされた内容のリストを表示するには、*ログの保存*をクリックします。

   ブラウザのDownloadsフォルダにという名前でファイルが保存されます `drive_upgrade_log-timestamp.txt`。

終了後

- ハードウェアページにすべてのコンポーネントが表示されていることを確認します。
- [Software and Firmware Inventory] ダイアログボックスをチェックして、新しいソフトウェアとファームウェアのバージョンを確認します（ [Menu] ： [Upgrade Center] を選択し、 [* Software and Firmware Inventory] のリンクをクリックします）。
- コントローラNVSRAMをアップグレードした場合、既存のNVSRAMに適用したカスタム設定はアクティブ化のプロセスで失われます。アクティブ化のプロセスが完了したら、NVSRAMにカスタム設定を再度適

用する必要があります。

ドライブファームウェアのアップグレード

ドライブファームウェア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することができます。

開始する前に

- ディスクツーディスクバックアップ、（計画的なファームウェアアップグレードの影響を受けないボリュームグループへの）ボリュームコピー、またはリモートミラーを使用してデータをバックアップしておきます。
- ストレージアレイのステータスが「最適」である。
- すべてのドライブのステータスが「最適」である。
- ストレージアレイで設定の変更が実行されていません。
- ドライブのオフラインアップグレードのみが可能な場合は、ドライブに関連付けられているすべてのボリュームへのI/Oアクティビティが停止します。

手順

1. メニューを選択します。Support [Upgrade Center]を選択します。
2. サポートサイトから管理クライアントに新しいファイルをダウンロードします。
   a. Drive Firmware upgrade（ドライブファームウェアのアップグレード）で、**NetApp Support**（ネットアップサポート）をクリック
   b. ネットアップサポートWebサイトで、「* Downloads *」タブをクリックします。
   c. 「* Disk Drive & Firmware Matrix *」を選択します。
   d. 残りの手順に従います。
3. ドライブファームウェアのアップグレードで、*アップグレードの開始*をクリックします。

   ダイアログボックスが表示され、使用中のドライブファームウェアファイルが表示されます。
4. サポートサイトからダウンロードしたファイルを展開（解凍）します。
5. [* Browse] をクリックし、サポートサイトからダウンロードした新しいドライブファームウェアファイルを選択します。

   ドライブファームウェアファイルのファイル名は、のようになり `D_HUC101212CSS600_30602291_MS01_2800_0002`、拡張子はに `.dlp`なります。

   一度に1つずつ、最大4つのドライブファームウェアファイルを選択できます。同じドライブに互換性があるドライブファームウェアファイルが複数ある場合は、ファイル競合エラーが発生します。アップグレードに使用するドライブファームウェアファイルを決定し、もう一方のファイルを削除します。
6. 「 * 次へ * 」をクリックします。

   ドライブの選択*（* Select Drives *）ダイアログボックスが表示され、選択したファイルでアップグレードできるドライブがリストされます。

   互換性があるドライブのみが表示されます。

ドライブに対して選択したファームウェアが、推奨されるファームウェア情報領域に表示されます。ファームウェアを変更する必要がある場合は、［* 戻る ］をクリックして前のダイアログに戻ります。

7. 実行するアップグレードのタイプを選択します。
   - * オンライン（デフォルト） * - ストレージ・アレイが I/O を処理している間に ' ファームウェア・ダウンロードをサポートできるドライブを表示しますこのアップグレード方式を選択した場合、これらのドライブを使用している関連ボリュームへのI/Oを停止する必要はありません。これらのドライブは、ストレージアレイがドライブへのI/Oを処理している間に一度に1つずつアップグレードされます。
   - * オフライン（並行処理） * — ドライブを使用するすべてのボリュームですべての I/O アクティビティが停止されている間に ' ファームウェアのダウンロードのみをサポートできるドライブを表示しますこのアップグレード方式を選択した場合は、アップグレード対象のドライブを使用するすべてのボリュームでI/Oアクティビティをすべて停止する必要があります。冗長性のないドライブはオフライン処理として処理する必要があります。これには、SSDキャッシュ、RAID 0ボリュームグループ、またはデグレード状態のプールやボリュームグループに関連付けられているドライブが含まれます。通常、オフライン（並行）アップグレードはオンライン（デフォルト）アップグレードよりも高速です。
8. テーブルの最初の列で、アップグレードするドライブを選択します。
9. [* スタート *] をクリックし、操作を確定します。

   アップグレードを停止する必要がある場合は、 * 停止 * をクリックします。実行中のファームウェアのダウンロードは完了します。開始されていないファームウェアのダウンロードはキャンセルされます。

   > ドライブファームウェアのアップグレードを停止すると、データが失われたり、ドライブを使用できなくなったりする可能性があります。

10. *オプション：*アップグレードされた内容のリストを表示するには、*ログの保存*をクリックします。

    ブラウザのDownloadsフォルダにという名前でファイルが保存されます `drive_upgrade_log-timestamp.txt`。

11. 手順のアップグレード中に次のいずれかのエラーが発生した場合は、推奨される対処方法を実行してください。

エラーと推奨される対処方法

ファームウェアのダウンロードエラー	対処方法
割り当て済みドライブで障害が発生	障害の原因の1つとして、ドライブに適切な署名がないことが考えられます。該当するドライブが認証済みドライブであることを確認します。詳細については、テクニカルサポートにお問い合わせください。 ドライブを交換する場合は、交換用ドライブの容量が障害が発生したドライブと同じかそれよりも大きいことを確認してください。 障害が発生したドライブの交換は、ストレージアレイでI/Oを受信中に実行できます。
ストレエシアレイノカクニン	• 各コントローラにIPアドレスが割り当てられていることを確認します。 • コントローラに接続されているすべてのケーブルが破損していないことを確認します。 • すべてのケーブルがしっかりと接続されていることを確認します。
統合ホットスペアドライブ	ファームウェアをアップグレードする前に、このエラーを修正する必要があります。System Managerを起動し、Recovery Guruを使用して問題を解決します。
ボリュームグループに不備がある	1つ以上のボリュームグループまたはディスクプールが不完全な場合は、ファームウェアをアップグレードする前にこのエラーを修正する必要があります。System Managerを起動し、Recovery Guruを使用して問題を解決します。
いずれかのボリュームグループで排他的な処理\（バックグラウンドメディア/パリティスキャン\を除く）を実行中	同時に実行できない処理が1つ以上実行中の場合は、その処理が完了してからファームウェアをアップグレードする必要があります。System Managerを使用して処理の進捗状況を監視します。
ボリュームが見つからない	ファームウェアをアップグレードする前に、ボリュームが見つからない状態を修正する必要があります。System Managerを起動し、Recovery Guruを使用して問題を解決します。
いずれかのコントローラが最適以外の状態です	いずれかのストレージアレイコントローラで対応が必要です。ファームウェアをアップグレードする前に、この状態を修正する必要があります。System Managerを起動し、Recovery Guruを使用して問題を解決します。

ファームウェアのダウンロードエラー	対処方法
コントローラオブジェクトグラフ間でストレージパーティション情報が一致しません	コントローラ上のデータの検証中にエラーが発生しました。この問題を解決するには、テクニカルサポートにお問い合わせください。
SPM Verify Database Controllerチェックが失敗する	コントローラでストレージパーティションのマッピングデータベースエラーが発生しました。この問題を解決するには、テクニカルサポートにお問い合わせください。
構成データベースの検証\（ストレージアレイのコントローラバージョンでサポートされている場合\）	コントローラで構成データベースのエラーが発生しました。この問題を解決するには、テクニカルサポートにお問い合わせください。
MEL関連チェック	この問題を解決するには、テクニカルサポートにお問い合わせください。
過去7日間に10件を超えるDDE情報イベントまたは重大MELイベントが報告されました	この問題を解決するには、テクニカルサポートにお問い合わせください。
過去7日間に2つ以上のPage 2C重大MELイベントが報告されました	この問題を解決するには、テクニカルサポートにお問い合わせください。
過去7日間に、ドライブチャネルのデグレード重大MELイベントが2つ以上報告されました	この問題を解決するには、テクニカルサポートにお問い合わせください。
過去7日間に4件を超える重要なMELエントリ	この問題を解決するには、テクニカルサポートにお問い合わせください。

終了後

これでドライブファームウェアのアップグレードは完了です。通常の運用を再開することができます。

考えられるソフトウェアとファームウェアのアップグレードエラーを確認する

エラーは、コントローラソフトウェアのアップグレード中またはドライブファームウェアのアップグレード中に発生する可能性があります。

ファームウェアのダウンロードエラーです	製品説明	推奨される対処方法
割り当て済みドライブで障害が発生	ストレージアレイに割り当てられているドライブをアップグレードできませんでした。	障害の原因の1つとして、ドライブに適切な署名がないことが考えられます。該当するドライブが認証済みドライブであることを確認します。詳細については、テクニカルサポートにお問い合わせください。 ドライブを交換する場合は、交換用ドライブの容量が障害が発生したドライブと同じかそれよりも大きいことを確認してください。 障害が発生したドライブの交換は、ストレージアレイでI/Oを受信中に実行できます。
統合ホットスペアドライブ	ホットスペアとしてマークされたドライブがボリュームグループに使用されている場合は、ファームウェアのアップグレードプロセスが失敗します。	ファームウェアをアップグレードする前に、このエラーを修正する必要があります。System Managerを起動し、Recovery Guruを使用して問題を解決します。
ボリュームグループに不備がある	ボリュームグループに含まれるドライブがバイパスされた、削除された、または応答しない場合、そのドライブは不完全なボリュームグループとみなされます。ボリュームグループが不完全な場合、ファームウェアのアップグレードは実行できません。	1つ以上のボリュームグループまたはディスクプールが不完全な場合は、ファームウェアをアップグレードする前にこのエラーを修正する必要があります。System Managerを起動し、Recovery Guruを使用して問題を解決します。
いずれかのボリュームグループで実行中の排他的な処理（バックグラウンドメディア/パリティスキャンを除く）	ボリュームで排他的な処理を実行中の場合は、ファームウェアをアップグレードできません。	同時に実行できない処理が1つ以上実行中の場合は、その処理が完了してからファームウェアをアップグレードする必要があります。System Managerを使用して処理の進捗状況を監視します。
ボリュームが見つからない	いずれかのボリュームが見つからない場合は、ファームウェアをアップグレードできません。	ファームウェアをアップグレードする前に、ボリュームが見つからない状態を修正する必要があります。System Managerを起動し、Recovery Guruを使用して問題を解決します。
いずれかのコントローラが最適以外の状態です	いずれかのコントローラの状態が最適以外の場合は、ファームウェアをアップグレードできません。	いずれかのストレージアレイコントローラで対応が必要です。ファームウェアをアップグレードする前に、この状態を修正する必要があります。System Managerを起動し、Recovery Guruを使用して問題を解決します。

ファームウェアのダウンロードエラーです	製品説明	推奨される対処方法
SPM Verify Database Controllerチェックが失敗する	ストレージパーティションマッピングデータベースが破損しているため、ファームウェアをアップグレードできません。	コントローラでストレージパーティションのマッピングデータベースエラーが発生しました。この問題を解決するには、テクニカルサポートにお問い合わせください。
構成データベースの検証（ストレージアレイのコントローラバージョンでサポートされている場合）	構成データベースが破損しているため、ファームウェアをアップグレードできません。	コントローラで構成データベースのエラーが発生しました。この問題を解決するには、テクニカルサポートにお問い合わせください。
MEL関連チェック	イベントログにエラーが含まれているため、ファームウェアをアップグレードできません。	この問題を解決するには、テクニカルサポートにお問い合わせください。
過去7日間に10件を超えるDDE情報イベントまたは重大MELイベントが報告されました	10個を超えるDDE情報または重大MELイベントが過去7日以内に報告されたため、ファームウェアをアップグレードできません。	この問題を解決するには、テクニカルサポートにお問い合わせください。
過去7日間に2つ以上のPage 2C重大MELイベントが報告されました	2個を超えるページ2C重大MELイベントが過去7日以内に報告されたため、ファームウェアをアップグレードできません。	この問題を解決するには、テクニカルサポートにお問い合わせください。
過去7日間に、ドライブチャネルのデグレード重大MELイベントが2つ以上報告されました	2つを超えるデグレードドライブチャネルの重大MELイベントが過去7日間に報告されたため、ファームウェアをアップグレードできません。	この問題を解決するには、テクニカルサポートにお問い合わせください。
過去7日間に4件を超える重要なMELエントリ	4個を超える重大イベントログエントリが過去7日間に報告されたため、ファームウェアをアップグレードできません。	この問題を解決するには、テクニカルサポートにお問い合わせください。
有効な管理IPアドレスが必要です。	この処理を実行するには、有効なコントローラIPアドレスが必要です。	この問題を解決するには、テクニカルサポートにお問い合わせください。
コマンドでは、各コントローラのアクティブな管理IPアドレスを指定する必要があります。	この処理には、ストレージアレイに関連付けられている各コントローラのコントローラIPアドレスが必要です。	この問題を解決するには、テクニカルサポートにお問い合わせください。

ファームウェアのダウンロードエラーです	製品説明	推奨される対処方法
未処理のダウンロードファイルタイプが返されました。	指定したダウンロードファイルはサポートされていません。	この問題を解決するには、テクニカルサポートにお問い合わせください。
ファームウェアダウンロードのアップロード手順中にエラーが発生しました。	コントローラが要求を処理できないため、ファームウェアのダウンロードに失敗しました。ストレージアレイが最適な状態であることを確認してから、処理を再試行してください。	ストレージアレイが最適な状態であることを確認したあとにこのエラーが再び発生する場合は、テクニカルサポートに連絡して問題を解決してください。
ファームウェアのアクティブ化手順中にエラーが発生しました。	コントローラが要求を処理できないため、ファームウェアのアクティブ化に失敗しました。ストレージアレイが最適な状態であることを確認してから、処理を再試行してください。	ストレージアレイが最適な状態であることを確認したあとにこのエラーが再び発生する場合は、テクニカルサポートに連絡して問題を解決してください。
コントローラ｛0｝のリブートを待機中にタイムアウトしました。	リブート後に管理ソフトウェアがコントローラ{0}に再接続できません。ストレージアレイへの動作中の接続パスがあることを確認し、正常に完了しなかった場合は処理を再試行してください。	ストレージアレイが最適な状態であることを確認したあとにこのエラーが再び発生する場合は、テクニカルサポートに連絡して問題を解決してください。

System ManagerのRecovery Guruを使用して、上記の一部の状態を修正できます。ただし、一部の状況については、テクニカルサポートへの連絡が必要になる場合があります。最新のコントローラファームウェアのダウンロードに関する情報は、ストレージアレイから入手できます。この情報は、ファームウェアのアップグレードとダウンロードを妨げているエラー状態をテクニカルサポートが把握するのに役立ちます。

FAQ

どのようなデータを収集しますか？

AutoSupport機能と手動のサポートデータ収集機能を使用すると、テクニカルサポートによるリモートでのトラブルシューティングや問題分析のためにカスタマーサポートバンドルにデータを収集できます。

カスタマーサポートバンドルでは、ストレージアレイに関するすべてのタイプの情報が1つの圧縮ファイルに収集されます。収集される情報には、物理構成、論理構成、バージョン情報、イベント、ログファイル、パフォーマンスデータが含まれます。この情報は、テクニカルサポートがストレージアレイの問題を解決するためにのみ使用されます。

読み取り不能セクターのデータには何が表示されますか？

ストレージアレイのドライブで検出された読み取り不能セクターに関する詳細なデータを表示できます。

読み取り不能セクターのログでは、最後に検出された読み取り不能セクターが最初に表示されます。ログに

は、読み取り不能セクターを含むボリュームに関する次の情報が記録されます。フィールドはソート可能です。

フィールド	製品説明
影響を受けるボリューム	ボリュームのラベルが表示されます。見つからないボリュームに読み取り不能セクターが含まれている場合は、見つからないボリュームのWorld Wide Identifierが表示されます。
論理ユニット番号（LUN）	ボリュームのLUNが表示されます。ボリュームにLUNがない場合は、「NA」と表示されます。
割り当て先	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が表示されます。ホスト、ホストクラスタ、またはデフォルトクラスタからボリュームにアクセスできない場合は、「NA」と表示されます。

読み取り不能セクターに関するその他の情報を表示するには、ボリュームの横にあるプラス記号（+）をクリックします。

フィールド	製品説明
日付/時刻	読み取り不能セクターが検出された日付と時刻が表示されます。
ボリュームの論理ブロックアドレス	ボリュームの論理ブロックアドレス（LBA）が表示されます。
ドライブの場所	ドライブシェルフ、ドロワー（ドライブシェルフにドロワーが搭載されている場合）、およびベイの場所が表示されます。
ドライブの論理ブロックアドレス	ドライブのLBAが表示されます。
障害タイプ	次のいずれかの障害タイプが表示されます。 • * Physical *--物理的なメディアエラー。 • 論理--ストライプ内のどこかで読み取りエラーが発生し'データが読み取り不能になっていますたとえば、ボリューム内の他の場所のメディアエラーが原因の読み取り不能セクターなどです。 • 不整合--整合性のない冗長性データ。 • * Data Assurance *-- Data Assuranceエラー。

ヘルスイメージとは

ヘルスイメージは、コントローラのプロセッサメモリの生データダンプです。テクニカルサポートは、コントローラの問題を診断するために使用できます。

ファームウェアが特定のエラーを検出すると、自動的にヘルスイメージが生成されます。トラブルシューティ

ングのシナリオによっては、テクニカルサポートから、ヘルスイメージファイルを取得して送信するように要求されることがあります。

AutoSupportの機能について教えてください。

AutoSupport 機能は、個別に有効にする3つの機能で構成されています。

- *Basic AutoSupport *--ストレージ・アレイが自動的にデータを収集してテクニカル・サポートに送信することを可能にします
- * AutoSupport OnDemand*--問題 のトラブルシューティングに必要なときに、テクニカルサポートが以前のAutoSupport ディスパッチの再送信を要求できるようにします。転送はすべて、AutoSupportサーバではなくストレージアレイから開始されます。ストレージアレイはAutoSupportサーバに定期的にコンタクトし、保留中の再送信要求がないかどうかをチェックし、適切に応答します。
- リモート診断--問題 のトラブルシューティングに必要な場合に、テクニカルサポートが最新のAutoSupport ディスパッチをリクエストできるようにします。転送はすべて、AutoSupportサーバではなくストレージアレイから開始されます。ストレージアレイはAutoSupportサーバに定期的にコンタクトし、保留中の新しい要求がないかどうかをチェックし、適切に応答します。

AutoSupport機能を使用して収集されるデータの種類を教えてください。

AutoSupport機能には、イベントディスパッチ、スケジュールディスパッチ、オンデマンドおよびリモート診断ディスパッチの3つの標準ディスパッチタイプが含まれています。

AutoSupport データにユーザデータが含まれることはありません。

- イベントディスパッチ

  テクニカルサポートへのプロアクティブな通知が必要なシステムでイベントが発生すると、AutoSupport機能によってイベントトリガー型ディスパッチが自動的に送信されます。

  - 管理対象のストレージアレイでサポートイベントが発生したときに送信されます。
  - イベント発生時にストレージアレイで発生していた状況の包括的なスナップショットが含まれます。
- スケジュールディスパッチ

  AutoSupport機能は、定期的に複数のディスパッチを自動的に送信します。

  - 日次ディスパッチ--ユーザーが設定可能な時間間隔内に毎日1回送信されます最新のシステムイベントログとパフォーマンスデータが含まれます。
  - 週次ディスパッチ--ユーザーが設定可能な時間間隔と日の間に毎週1回送信されます構成とシステムの状態の情報が含まれます。
- * AutoSupport OnDemandおよびRemote Diagnosticsディスパッチ*
  - * AutoSupport OnDemand*--問題 のトラブルシューティングに必要なときに、テクニカルサポートが以前のAutoSupport ディスパッチの再送信を要求できるようにします。転送はすべて、AutoSupportサーバではなくストレージアレイから開始されます。ストレージアレイはAutoSupportサーバに定期的にコンタクトし、保留中の再送信要求がないかどうかをチェックし、適切に応答します。
  - リモート診断--問題 のトラブルシューティングに必要な場合に、テクニカルサポートが最新のAutoSupport ディスパッチをリクエストできるようにします。転送はすべて、AutoSupportサーバではなくストレージアレイから開始されます。ストレージアレイはAutoSupportサーバに定期的にコンタ

クトし、保留中の新しい要求がないかどうかをチェックし、適切に応答します。

AutoSupport機能の配信方法を設定するにはどうすればよいですか。

AutoSupport機能は、テクニカルサポートへのAutoSupportディスパッチの配信用に、HTTPS、HTTP、SMTPの各プロトコルをサポートしています。

開始する前に

- AutoSupport機能を有効にする必要があります。有効になっているかどうかは、AutoSupportページで確認できます。
- ネットワークにDNSサーバをインストールし、設定する必要があります。DNSサーバのアドレスがSystem Managerで設定されている必要があります（このタスクは[ハードウェア]ページから実行できます）。

タスクの内容

各プロトコルを確認します。

- * HTTPS *-- HTTPSを使用して、テクニカルサポートの宛先サーバーに直接接続できます。AutoSupport OnDemandまたはRemote Diagnosticsを有効にする場合は、AutoSupport の配信方法をHTTPSに設定する必要があります。
- * HTTP *-- HTTPを使用して、テクニカルサポートの宛先サーバーに直接接続できます。
- **Email**-- AutoSupport ディスパッチの配信方法として電子メールサーバーを使用できます

- HTTPS / HTTPとEメールの配信方法*の違い。SMTPを使用するEメール配信方法とHTTPSおよびHTTP配信方法の間には、重要な違いがいくつかあります。まず、Eメールではディスパッチのサイズが5MBに制限されるため、ASUPデータ収集の一部はディスパッチされません。次に、AutoSupport OnDemand機能は、HTTPPおよびHTTPSメソッドでのみ使用できます。

手順

1. メニューを選択AutoSupport します。[Support Center]>[Support]（サポートセンター）タブ。
2. AutoSupport 配信方法の設定 * を選択します。

   ディスパッチの配信方法を示すダイアログボックスが表示されます。

3. 目的の配信方法を選択し、その配信方法のパラメータを選択します。次のいずれかを実行します。
   - [HTTPS]または[HTTP]を選択した場合は、次のいずれかの配信パラメータを選択します。
     - * direct*--このデリバリパラメータはデフォルトで選択されています。このオプションを選択すると、HTTPSまたはHTTPプロトコルを使用してテクニカルサポートのデスティネーションシステムに直接接続できます。
     - プロキシ・サーバ経由--このオプションを選択すると'テクニカル・サポート・システムとの接続を確立するために必要なHTTPプロキシ・サーバの詳細を指定できますホストアドレスとポート番号を指定する必要があります。ただし、ホスト認証の詳細（ユーザ名とパスワード）を入力する必要があるのは、必要な場合だけです。
     - プロキシ自動設定（**PAC**）スクリプト経由-- Proxy Auto-Configuration（PAC）スクリプトファイルの場所を指定します。PACファイルを使用すると、テクニカルサポートのデスティネーションシステムとの接続を確立するために適切なプロキシサーバが自動的に選択されます。

- [Email]を選択した場合は、次の情報を入力します。
  - メールサーバのアドレス（完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレス）。
  - AutoSupportディスパッチEメールの[差出人]フィールドに表示されるEメールアドレス。
  - *オプション。設定テストを実行する場合。*AutoSupportシステムがテストディスパッチを受信したときに確認を送信するEメールアドレス。
  - メッセージを暗号化する場合は、暗号化タイプとして*SMTPS*または*STARTTLS *を選択し、暗号化されたメッセージのポート番号を選択します。それ以外の場合は、*なし*を選択します。
  - 必要に応じて、送信元およびメールサーバとの認証に使用するユーザ名とパスワードを入力します。

4. Test Configuration *をクリックして、指定された配信パラメータを使用してテクニカルサポートサーバーへの接続をテストします。AutoSupport On-Demand機能を有効にした場合は、AutoSupport OnDemandディスパッチの配信のための接続もシステムでテストされます。

   設定テストに失敗した場合は、設定を確認し、もう一度テストを実行してください。テストが引き続き失敗する場合は、テクニカルサポートにお問い合わせください。

5. [保存（ Save ）] をクリックします。

構成データとは

[Collect Configuration Data]を選択すると、RAID構成データベースの現在の状態が保存されます。

RAID構成データベースには、コントローラ上のボリュームグループおよびディスクプールのすべてのデータが含まれています。構成データの収集機能では、のCLIコマンドと同じ情報が保存されます `save storageArray dbmDatabase`。

SANtricity OSソフトウェアをアップグレードするときは、どのような点に注意する必要がありますか？

コントローラのソフトウェアとファームウェアをアップグレードする前に、次の項目を確認しておきます。

- ドキュメントとファイルを読み、 `readme.txt`アップグレードを実行することを決定しておきます。
- IOMファームウェアをアップグレードするかどうかを決めます。

  通常は、すべてのコンポーネントを同時にアップグレードする必要があります。ただし、SANtricity OSコントローラソフトウェアのアップグレードの一環としてIOMファームウェアをアップグレードしない場合や、テクニカルサポートからIOMファームウェアのダウングレードを指示された場合（ファームウェアをダウングレードす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）は、IOMファームウェアをアップグレードしないこともできます。

- コントローラNVSRAMファイルをアップグレードするかどうかを決めます。

  通常は、すべてのコンポーネントを同時にアップグレードする必要があります。ただし、コントローラのNVSRAMファイルにパッチを適用している場合や、ファイルがカスタムバージョンであり、上書きしたくない場合は、アップグレードしないこともできます。

- 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--ソフトウェアとファーム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

SANtricity OSコントローラソフトウェアのアップグレードに含まれるコンポーネントは次のとおりです。

- 管理ソフトウェア-- System Managerはストレージ・アレイを管理するソフトウェアです
- * コントローラファームウェア * — コントローラファームウェアは、ホストとボリューム間の I/O を管理します。
- * コントローラ NVSRAM * — コントローラ NVSRAM は、コントローラのデフォルト設定を指定するコントローラファイルです。
- * IOM ファームウェア * - I/O モジュール（ IOM ）ファームウェアは、コントローラとドライブシェルフの間の接続を管理します。また、コンポーネントのステータスも監視します。
- * スーパーバイザー・ソフトウェア * — スーパーバイザー・ソフトウェアは、ソフトウェアが実行されるコントローラ上の仮想マシンです。

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できるように、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場合があります。

該当するかどうかを確認するには、を参照してください "NetApp Interoperability Matrix Tool"。

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インストール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。

アップグレードの実行中はストレージアレイに変更を加えないでください。

IOMの自動同期を一時停止するときは、どのような点に注意する必要がありますか？

IOMの自動同期を一時停止すると、SANtricity OSコントローラソフトウェアの次回アップグレード時にIOMファームウェアがアップグレードされなくなります。

通常、コントローラソフトウェアとIOMファームウェアはバンドルとしてアップグレードされます。エンクロージャに保持するIOMファームウェアの特別なビルドがある場合は、IOMの自動同期を中断できます。そうしないと、コントローラソフトウェアの次回アップグレード時にコントローラソフトウェアにバンドルされているIOMファームウェアにリバートされます。

ファームウェアのアップグレードに時間がかかるのはなぜですか？

ファームウェアアップグレードの進行状況は、システムの全体的な負荷によって異なります。

ドライブファームウェアのオンラインアップグレード中に高速再構築プロセス中にボリューム転送が実行され

ると、転送されたボリュームで完全な再構築が開始されます。この処理にはかなりの時間がかかることがあります。完全な再構築に実際にかかる時間は、再構築処理中に発生するI/Oアクティビティの量、ボリュームグループ内のドライブ数、リビルドの優先度の設定、ドライブのパフォーマンスなど、いくつかの要因によって異なります。

ドライブファームウェアをアップグレードするときは、どのような点に注意する必要がありますか？

ドライブファームウェアをアップグレードする前に、次の項目に注意してください。

- 予防措置として、ディスクツーディスクバックアップ、（計画的なファームウェアアップグレードの影響を受けないボリュームグループへの）ボリュームコピー、またはリモートミラーを使用してデータをバックアップします。
- 新しいファームウェアが正常に機能することを確認するために、少数のドライブのみをアップグレードして動作をテストすることもできます。新しいファームウェアが正常に機能している場合は、残りのドライブをアップグレードします。
- 障害が発生したドライブがある場合は、ファームウェアのアップグレードを開始する前に修正してください。
- ドライブのオフラインアップグレードが可能な場合は、ドライブに関連付けられているすべてのボリュームへのI/Oアクティビティを停止します。I/Oアクティビティを停止すると、当該ボリュームに関連する設定処理は実行されません。
- ドライブファームウェアのアップグレード中にドライブを取り外さないでください。
- ドライブファームウェアのアップグレード中は、ストレージアレイの設定を変更しないでください。

実行するアップグレードの種類を選択する方法を教えてください。

ドライブで実行するアップグレードのタイプは、プールまたはボリュームグループの状態に応じて選択します。

- * オンライン *

  プールまたはボリュームグループで冗長性がサポートされていて最適な場合は、オンライン方式を使用してドライブファームウェアをアップグレードできます。オンライン方式では、ドライブを使用している関連付けられたボリュームにストレージアレイがI/Oを処理している間に、ファームウェアがダウンロードされます。ドライブを使用している関連付けられたボリュームへのI/Oを停止する必要はありません。ドライブは、ドライブに関連付けられているボリュームに対して一度に1つずつアップグレードされます。プールまたはボリュームグループに割り当てられていないドライブのファームウェアは、オンライン方式またはオフライン方式で更新できます。オンライン方式を使用してドライブファームウェアをアップグレードすると、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。

- * オフライン *

  プールまたはボリュームグループで冗長性がサポートされていない場合（RAID 0）、またはデグレード状態の場合は、オフライン方式を使用してドライブファームウェアをアップグレードする必要があります。オフライン方式では、すべてのI/Oアクティビティが停止している間にファームウェアのみがアップグレードされ、ドライブを使用している関連付けられたボリュームにアップグレードされます。ドライブを使用している関連付けられたボリュームへのI/Oをすべて停止する必要があります。プールまたはボリュームグループに割り当てられていないドライブのファームウェアは、オンライン方式でもオフライン方式でも更新できます。

Unified Manager 6による複数のアレイの管理

メインインターフェイス

Unified Managerインターフェイスの概要

Unified ManagerはWebベースのインターフェイスであり、1つのビューで複数のストレージアレイを管理することができます。

メインページ

Unified Managerにログインすると、メインページが開き、* Manage-All *が表示されます。このページでは、ネットワーク内で検出されたストレージアレイのリストをスクロールしてステータスを表示し、単一のアレイまたはアレイのグループに対して処理を実行できます。

ナビゲーションサイドバー

Unified Managerの機能には、ナビゲーションサイドバーからアクセスできます。

面積	製品説明
管理	ネットワーク内のストレージアレイを検出し、アレイのSANtricity System Managerを起動し、1つのアレイから複数のアレイに設定をインポートし、アレイグループを管理します。設定のインポートやアレイグループの作成などの処理を実行するには、アレイ名の横にあるチェックボックスをオンにします。各行の最後にある省略記号は、アレイ名の変更など、単一のアレイに対する操作のインラインメニューを提供します。
運用	アレイ間での設定のインポートなど、バッチ処理の進捗状況を表示します。 ストレージアレイのステータスが最適でない場合は、一部の処理を実行できません。
証明書管理	ブラウザとクライアントの間で認証する証明書を管理します。
アクセス管理	Unified Managerインターフェイスのユーザ認証を確立します。
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。

インターフェイスの設定とヘルプ

インターフェイスの右上にあるヘルプやその他のドキュメントにアクセスできます。ログイン名の横にあるドロップダウンから管理オプションにアクセスすることもできます。

ユーザログインとパスワード

システムにログインしている現在のユーザがインターフェイスの右上に表示されます。

ユーザとパスワードの詳細については、次を参照してください。

- "管理者パスワード保護の設定"
- "管理者パスワードの変更"
- "ローカルユーザプロファイルのパスワードの変更"

サポートされるブラウザ

Unified Manager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。

ブラウザ	最小バージョン
Google Chrome	89
Mozilla Firefox	80
Safari	14
Microsoft Edge	90

Web Services Proxyがインストールされていて、ブラウザで使用できる必要があります。

管理者パスワード保護の設定

Unified Managerには、不正なアクセスを防ぐために管理者パスワードを設定する必要があります。

管理者パスワードとユーザプロファイル

Unified Managerの初回起動時に、管理者パスワードを設定するように求められます。adminパスワードを持つユーザなら誰でも、ストレージアレイの設定を変更できます。

Unified Managerインターフェイスには、管理パスワードに加えて、1つ以上のロールがマッピングされた設定済みのユーザプロファイルが含まれています。詳細については、を参照してください "アクセス管理の仕組み"。

ユーザとマッピングは変更できません。変更できるのはパスワードのみです。パスワードの変更については、次を参照してください。

- "管理者パスワードの変更"
- "ローカルユーザプロファイルのパスワードの変更"

セツシヨンタイムアウト

1つの管理セッションでパスワードの入力を求められるのは1回のみです。デフォルトでは操作がない状態が30分続くとセッションがタイムアウトし、パスワードをもう一度入力する必要があります。セッション中に別の管理クライアントから同じソフトウェアにアクセスしている別のユーザがパスワードを変更した場合は、次回の設定処理や表示処理でパスワードの入力を求められます。

セキュリティ上の理由から、パスワードの入力を試行できるのは5回までとなっており、この回数を超えると、ソフトウェアは「ロックアウト」状態になります。この状態では、ソフトウェアは以降のパスワード試行を拒否します。パスワードを再度入力するには、10分待ってから「通常」の状態にリセットする必要があります。

セッションタイムアウトを調整したり、セッションタイムアウトを完全に無効にしたりできます。詳細については、を参照してください "セッションタイムアウトの管理"。

管理者パスワードの変更

Unified Managerへのアクセスに使用する管理者パスワードを変更できます。

開始する前に

- Root Adminの権限が割り当てられたローカル管理者としてログインする必要があります。
- 現在の管理者パスワードを確認しておく必要があります。

タスクの内容

パスワードを選択する際は、次のガイドラインに注意してください。

- パスワードは大文字と小文字が区別されます。
- パスワードの末尾のスペースは削除されません。パスワードにスペースが含まれている場合は、スペースを含めるように注意してください。
- セキュリティを強化するために、15文字以上の英数字を使用し、パスワードを頻繁に変更してください。

手順

1. メニューを選択します。Settings [Access Management]。
2. [ローカルユーザー役割*（Local User Roles *）]タブを選択します。
3. 表から* admin *ユーザを選択します。

   [パスワードの変更]ボタンが使用可能になります。

4. [パスワードの変更 *] を選択します。

   [パスワードの変更]ダイアログボックスが開きます。

5. ローカルユーザパスワードの最小文字数が設定されていない場合は、システムにアクセスする際にユーザにパスワードの入力を求めるチェックボックスを選択します。
6. 2つのフィールドに新しいパスワードを入力します。
7. この操作を確認するためにローカル管理者パスワードを入力し、*変更*をクリックします。

セッションタイムアウトの管理

非アクティブな状態が一定の時間続いたユーザセッションは切断されるように、Unified Managerでタイムアウトを設定できます。

タスクの内容

デフォルトでは、Unified Managerのセッションタイムアウトは30分です。この時間を調整したり、セッションタイムアウトを無効にしたりすることができます。

> アレイに組み込まれたSecurity Assertion Markup Language（SAML）機能を使用してアクセス管理を設定している場合、ユーザのSSOセッションが最大数に達したときにセッションタイムアウトが発生することがあります。これは、System Managerのセッションタイムアウトより前に発生することがあります。

手順

1. メニューバーで、ユーザログイン名の横にあるドロップダウン矢印を選択します。
2. 「セッションタイムアウトを有効/無効にする」を選択します。

   セッションタイムアウトの有効化/無効化ダイアログボックスが開きます。
3. スピナーコントロールを使用して、時間を分単位で増減します。

   設定できる最小タイムアウトは15分です。

   > セッションタイムアウトを無効にするには、*時間の長さを設定*チェックボックスをオフにします。
4. [保存（ Save ）] をクリックします。

ストレージアレイ

検出の概要

ストレージリソースを管理するには、まずネットワーク内のストレージアレイを検出する必要があります。

アレイの検出方法

[追加/検出]ページを使用して、組織のネットワークから管理するストレージアレイを検索して追加します。複数のアレイを検出することも、単一のアレイを検出することもできます。そのためには、ネットワークIPアドレスを入力すると、Unified Managerはその範囲内の各IPアドレスへの接続を個別に試行します。

詳細：

- "アレイの検出に関する考慮事項"
- "複数のストレージアレイの検出"
- "単一のアレイの検出"

アレイの管理方法

アレイを検出したら、* Manage-All *ページに移動します。このページでは、ネットワーク内で検出されたストレージアレイのリストをスクロールしてステータスを表示し、単一のアレイまたはアレイのグループに対して処理を実行できます。

単一のアレイを管理する場合は、アレイを選択してSystem Managerを開くことができます。

詳細：

- "System Managerへのアクセスに関する考慮事項"
- "個 々 のストレージアレイの管理"
- "ストレージアレイのステータスの表示"

概念

アレイの検出に関する考慮事項

Unified Managerでストレージリソースを表示および管理するには、組織のネットワークで管理するストレージアレイを検出する必要があります。複数のアレイを検出することも、単一のアレイを検出することもできます。

複数のストレージアレイの検出

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Unified Managerで個別に試行されます。到達したストレージアレイが検出ページに表示され、管理ドメインに追加されることがあります。

単一のストレージアレイの検出

単一のアレイを検出する場合は、ストレージアレイ内のいずれかのコントローラのIPアドレスを1つ入力すると、個 々 のストレージアレイが追加されます。

> Unified Managerは、あるコントローラに割り当てられている1つのIPアドレスまたは範囲内のIPアドレスのみを検出して表示します。代替のコントローラまたはそれらのコントローラに割り当てられているIPアドレスがあっても、この1つのIPアドレスまたはIPアドレス範囲に含まれていなければ、Unified Managerでは検出または表示されません。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て[管理]ビューに表示されます。

ユーザクレデンシャル

検出プロセスでは、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。

Webサービスの証明書

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Unified Managerで確認されます。Unified Managerでは、ブラウザで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

  Unified Managerで検出されたアレイについては、認証局が発行する信頼された証明書が追加で必要となる場合があります。

  これらの証明書をインポートするには、* Import *ボタンを使用します。このアレイに前に接続したことがある場合は、一方または両方のコントローラの証明書が期限切れになっているか、失効しているか、証明書チェーンにルート証明書または中間証明書がない可能性があります。ストレージアレイの管理を開始する前に、期限切れまたは失効した証明書を差し替えるか、不足しているルート証明書または中間証明書を追加する必要があります。

- 自己署名証明書

  自己署名証明書を使用することもできます。署名済みの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、Unified Managerにエラー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で自己署名証明書を承認することができます。自己署名証明書が信頼済みとしてマークされ、Unified Managerにストレージアレイが追加されます。

  ストレージアレイへの接続を信頼しない場合は、Unified Managerにストレージアレイを追加する前に* 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。

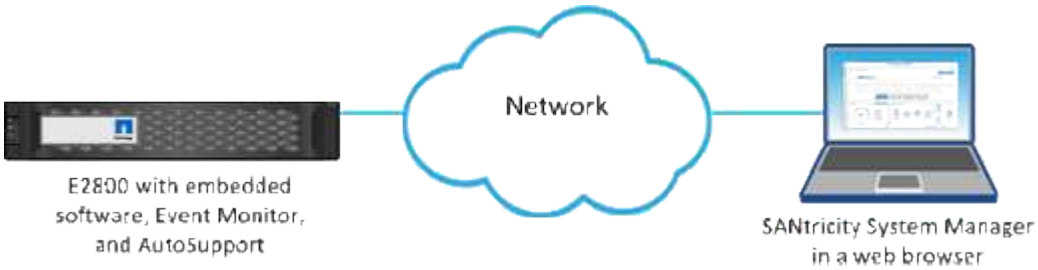
System Managerへのアクセスに関する考慮事項

ストレージアレイを設定および管理する場合は、1つ以上のストレージアレイを選択し、[起動]オプションを使用してSystem Managerを開きます。

System Managerはコントローラに組み込まれたアプリケーションで、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。これには、アレイベースのすべての関数が含まれます。

System Managerにアクセスするには、以下を準備しておく必要があります。

- 次のいずれかのアレイモデルを参照してください。"E シリーズハードウェアの概要"
- Webブラウザを使用したネットワーク管理クライアントへのアウトオブバンド接続。



アレイの検出

複数のストレージアレイの検出

複数のアレイを検出すると、管理サーバが配置されているサブネット全体ですべてのストレージアレイが検出され、検出されたアレイが管理ドメインに自動的に追加されます。

開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。
- 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。
- 信頼されていない証明書を解決するには、認証局（CA）の信頼された証明書ファイルが必要です。証明書ファイルがローカルシステムにある必要があります。

アレイの検出は複数の手順で構成されます。

手順**1**：ネットワークアドレスを入力します

ローカルサブネットワーク全体を検索するには、ネットワークアドレス範囲を入力します。到達したストレージアレイが検出ページに表示され、管理ドメインに追加されることがあります。

何らかの理由で検出操作を停止する必要がある場合は、*検出の停止*をクリックします。

手順

1. [管理] ページで、 [* 追加 / 検出 *] を選択します。

   [Add/Discover]ダイアログボックスが表示されます。

2. [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する]ラジオボタンを選択します。
3. 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、*検出の開始*をクリックします。

   検出プロセスが開始されます。この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。ストレージアレイが検出されると、検出ページの表にデータが表示されます。

   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おり、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. 検出されたストレージアレイのリストを確認します。
5. 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、[次へ]をクリックします。

   管理ドメインに追加する各アレイについて、Unified Managerでクレデンシャルのチェックが実行されます。そのアレイに関連付けられている自己署名証明書や信頼されていない証明書の解決が必要になる場合があります。

6. 「 * 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**2**：検出時に自己署名証明書を解決する

検出プロセスでは、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。

手順

1. 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、ウィザードの次のカードに進みます。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Unified Manager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Unified Managerに追加してください。

2. 「 * 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**：検出時に信頼されていない証明書を解決する

信頼されていない証明書は、ストレージアレイからUnified Manager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を確認できない場合に発生します。アレイの検出プロセスで信頼されていない証明書を解決するには、信頼できるサードパーティが発行した認証局（CA）証明書（CA署名証明書）をインポートします。

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最近追加した。
- 一方または両方の証明書の期限が切れている。
- 一方または両方の証明書が失効している。
- 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. 信頼されていない証明書を解決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て、[インポート]ボタンを選択します。

   信頼された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開きます。

2. Browse（参照）*をクリックして、ストレージアレイの証明書ファイルを選択します。

   ダイアログボックスにファイル名が表示されます。

3. [* インポート *] をクリックします。

   ファイルがアップロードされて検証されます。

   信頼されていない証明書の問題が未解決のストレージアレイはUnified Managerに追加されません。

4. 「 * 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**4**：パスワードを入力する

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. Unified Managerに追加する各ストレージアレイのパスワードを入力します。
2. *オプション：*ストレージアレイをグループに関連付けます。ドロップダウンリストから、選択したストレージアレイを関連付ける目的のグループを選択します。

3. [完了] をクリックします。

終了後

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。

指定したストレージアレイへのUnified Managerの接続には数分かかることがあります。

単一のアレイの検出

単一のストレージアレイを手動で検出して組織のネットワークに追加するには、[単一のストレージアレイの追加/検出]オプションを使用します。

開始する前に

- 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。

手順

1. [管理] ページで、 [* 追加 / 検出 *] を選択します。

   [Add/Discover]ダイアログボックスが表示されます。

2. [Discover a single storage array]オプションボタンを選択します。
3. ストレージアレイ内のいずれかのコントローラのIPアドレスを入力し、*検出の開始*をクリックします。

   指定したストレージアレイへのUnified Managerの接続には数分かかることがあります。

   指定したIPアドレスでコントローラに接続できない場合、「ストレージアレイにアクセスできません」というメッセージが表示されます。

4. プロンプトが表示されたら、自己署名証明書を解決します。

   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。ストレージアレイのデジタル証明書が見つからない場合は、認識された認証局（CA）によって署名されていない証明書を解決するためにセキュリティ例外を追加するように求められます。

5. 信頼されていない証明書があれば解決します。

   信頼されていない証明書は、ストレージアレイからUnified Manager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を確認できない場合に発生します。信頼されていない証明書を解決するには、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。

6. 「 * 次へ * 」をクリックします。
7. *オプション：*検出されたストレージアレイをグループに関連付けます。ドロップダウンリストから、ストレージアレイを関連付ける目的のグループを選択します。

   デフォルトでは「All」グループが選択されています。

8. 管理ドメインに追加するストレージアレイの管理者パスワードを入力し、* OK *をクリックします。

終了後

ストレージアレイがUnified Managerに追加され、指定した場合は選択したグループにも追加されます。

サポートデータの自動収集が有効になっている場合は、追加したストレージアレイのサポートデータが自動的に収集されます。

アレイの管理

ストレージアレイのステータスの表示

Unified Managerには、検出された各ストレージアレイのステータスが表示されます。

[* Manage-All*]ページに移動します。このページでは、Web Services Proxyとそのストレージアレイの間の接続のステータスを確認できます。

ステータスインジケータについては、次の表で説明します。

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、パスワードは有効です。
無効なパスワード	無効なストレージアレイパスワードが指定されました。
信頼されない証明書	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。
要注意	ストレージアレイにユーザによる修正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	ストレージアレイに一度も接続されていません。この状況は、Web Services Proxy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Web Services Proxyの起動後に一度も接続されていない場合に発生します。
オフライン	Web Services Proxyは以前にストレージアレイに接続していましたが、現在はすべての接続が失われています。

個 々 のストレージアレイの管理

[起動]オプションを使用すると、管理処理を実行する場合に1つ以上のストレージアレイに対してブラウザベースのSystem Managerを開くことができます。

手順

1. [管理]ページで、管理するストレージアレイを1つ以上選択します。
2. [* 起動 *] をクリックします。

   新しいウィンドウが開き、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。

ストレージアレイのパスワードの変更

Unified Managerでストレージアレイを表示したりアクセスしたりするために使用するパスワードを更新できます。

開始する前に

- Storage Adminの権限を含むユーザプロファイルでログインする必要があります。
- ストレージアレイの現在のパスワード（System Managerで設定されているパスワード）を確認しておく必要があります。

タスクの内容

このタスクでは、Unified Managerから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ために、Unified Managerでも変更が必要になった場合などに行います。

手順

1. 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。

SANtricity Unified Managerからのストレージアレイの削除

Unified Managerで管理する必要がなくなったストレージアレイは、削除することができます。

タスクの内容

削除したストレージアレイにはアクセスできません。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ることで、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、ストレージアレイやそのデータには影響しません。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）]ページを選択します。
2. 削除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「Uncommon Tasks（一般的でないタスク）」を選択します。

   ストレージアレイがSANtricity Unified Managerのすべてのビューから削除されます。

設定のインポート

設定のインポートの概要

設定のインポート機能を使用すると、1つのアレイから複数のアレイに設定をインポートするバッチ処理を実行できます。この機能により、ネットワーク内で複数のアレイを構成する必要がある場合に時間を節約できます。

どのような設定をインポートできますか？

アラート方法、AutoSupport設定、ディレクトリサービス設定、ストレージ設定（ボリュームグループやプールなど）、およびシステム設定（自動ロードバランシングなど）をインポートできます。

詳細：

- "設定のインポートの仕組み"
- "ストレージ構成のレプリケートに関する要件"

バッチインポートの実行方法を教えてください。

ソースとして使用するストレージアレイで、System Managerを開き、必要な設定を行います。そのあと、Unified Managerの[管理]ページに移動し、1つ以上のアレイに設定をインポートします。

詳細：

- "アラート設定のインポート"
- "AutoSupport設定のインポート"
- "ディレクトリサービス設定のインポート"
- "ストレージ構成のインポート"
- "システム設定のインポート"

概念

設定のインポートの仕組み

Unified Managerを使用して、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設定をインポートできます。設定のインポート機能は、ネットワーク内に複数のアレイを構成する必要がある場合に時間を節約するバッチ処理です。

インポートできる設定

複数のアレイに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ためのアラート方法。
- * 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。
- 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以外の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
- 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）

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. Unified Managerの* Manage *ページに移動して、設定をインポートします。
4. [* Operations]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、要件と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。
- 拡張シェルフは、同じドライブタイプの同じスロットに搭載する必要があります（ドライブが構成で使用されている場合は、未使用ドライブの場所は関係ありません）。

コントローラ

- コントローラのタイプはソースアレイとターゲットアレイで異なる場合があり（E2800からE5700にインポートする場合など）、RBODエンクロージャのタイプは同じである必要があります。
- HIC（ホストのDA機能を含む）が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。
- 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ません。

ステータス

- ターゲットアレイのステータスが最適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、ソースアレイとターゲットアレイでドライブ容量が異なる場合があります。（ターゲットアレイには、より新しい大容量のドライブが搭載されている場合がありますが、こ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構成されません）。
- ソースアレイのディスクプールボリュームが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ません。
- シンボリュームはインポートプロセスに含まれません。

バッチインポートの使用

アラート設定のインポート

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。

開始する前に

- 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で設定します（メニュー：Settings [Alerts]）。
- 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]）。

タスクの内容

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。インポートされ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。
- **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、[設定のインポート*]をクリックします。

   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ボックスで、電子メールアラート、* SNMPアラート*、または* Syslogアラート*のいずれかを選択し、*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]ダイアログボックスで、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. [Select Targets]ダイアログボックスで、新しい設定を適用するアレイを1つ以上選択します。

   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、Unified Managerが通信できないアレイ（オフラインのアレイ、証明書、パスワード、ネットワークに問題があるアレイなど）は、このダイアログボックスに表示されません。

5. [完了] をクリックします。

   [Operations]ページにインポート処理の結果が表示されます。処理に失敗した場合は、その行をクリックすると詳細が表示されます。

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した。

AutoSupport設定のインポート

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。

開始する前に

- AutoSupport は、ソースとして使用するストレージアレイ（メニュー：サポート[サポートセンター]）に対してSystem Manager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]）。

タスクの内容

インポートされる設定には、個別の機能（Basic AutoSupport、AutoSupport OnDemand、および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が含まれます。

手順

1. [管理]ページで、[設定のインポート*]をクリックします。

   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ボックスで、「* 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]ダイアログボックスで、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. [Select Targets]ダイアログボックスで、新しい設定を適用するアレイを1つ以上選択します。

   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、Unified Managerが通信できないアレイ（オフラインのアレイ、証明書、パスワード、ネットワークに問題があるアレイなど）は、このダイアログボックスに表示されません。

5. [完了] をクリックします。

[Operations]ページにインポート処理の結果が表示されます。処理に失敗した場合は、その行をクリックすると詳細が表示されます。

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なります。

ディレクトリサービス設定のインポート

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。

開始する前に

- 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で設定されます（メニュー：設定[アクセス管理]）。
- 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]）。

タスクの内容

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のマッピングが含まれます。

手順

1. [管理]ページで、[設定のインポート*]をクリックします。

   設定のインポートウィザードが開きます。

2. [設定の選択]ダイアログボックスで、[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]ダイアログボックスで、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. [Select Targets]ダイアログボックスで、新しい設定を適用するアレイを1つ以上選択します。

   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、Unified Managerが通信できないアレイ（オフラインのアレイ、証明書、パスワード、ネットワークに問題があるアレイなど）は、このダイアログボックスに表示されません。

5. [完了] をクリックします。

   [Operations]ページにインポート処理の結果が表示されます。処理に失敗した場合は、その行をクリックすると詳細が表示されます。

結果

ターゲットストレージアレイにソースアレイと同じディレクトリサービスが設定されます。

システム設定のインポート

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。

開始する前に

- 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]）。

タスクの内容

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、[設定のインポート*]をクリックします。

   設定のインポートウィザードが開きます。

2. [設定の選択]ダイアログボックスで、[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]ダイアログボックスで、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. [Select Targets]ダイアログボックスで、新しい設定を適用するアレイを1つ以上選択します。

   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、Unified Managerが通信できないアレイ（オフラインのアレイ、証明書、パスワード、ネットワークに問題があるアレイなど）は、このダイアログボックスに表示されません。

5. [完了] をクリックします。

   [Operations]ページにインポート処理の結果が表示されます。処理に失敗した場合は、その行をクリックすると詳細が表示されます。

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なります。

ストレージ構成のインポート

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。

開始する前に

- 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SANtricity 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]）。
- 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。
  - 拡張シェルフには、同じドライブタイプの同じスロットが搭載されている必要があります。
  - RBODエンクロージャタイプは同一である必要があります。
  - 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の容量よりも大きい。
- 次の制限事項に注意してください。
  - 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ません。
  - シンボリュームはインポートプロセスに含まれません。

タスクの内容

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、[設定のインポート*]をクリックします。

   設定のインポートウィザードが開きます。

2. [設定の選択]ダイアログボックスで、[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]ダイアログボックスで、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. [Select Targets]ダイアログボックスで、新しい設定を適用するアレイを1つ以上選択します。

   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、Unified Managerが通信できないアレイ（オフラインのアレイ、証明書、パスワード、ネットワークに問題があるアレイなど）は、このダイアログボックスに表示されません。

5. [完了] をクリックします。

   [Operations]ページにインポート処理の結果が表示されます。処理に失敗した場合は、その行をクリックすると詳細が表示されます。

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。

FAQ

どのような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、ソースストレージアレイがSystem Managerで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実行時に、一部のストレージアレイがターゲットの選択ダイアログボックスに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です。
- システムがそのアレイと通信できない（アレイに証明書、パスワード、ネットワークの問題があるなど）。

アレイクルウフ

グループの概要

[グループの管理]ページでは、管理しやすいように一連のストレージアレイグループを作成できます。

アレイグループとは

一連のストレージアレイをグループ化して、物理インフラと仮想インフラを管理できます。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を簡単に実行できます。

グループには次の2種類があります。

- 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。[すべて]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。

グループを設定するにはどうすればよいですか。

[Manage Groups]ページでは、グループを作成し、そのグループにアレイを追加できます。

詳細：

- "ストレージアレイグループの設定"

ストレージアレイグループの設定

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。

グループの設定は、2つの手順で構成されます。

手順**1**：グループを作成する

最初にグループを作成します。ストレージグループは、ボリュームを構成するストレージを提供するドライブを定義します。

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。

手順**2**：ストレージアレイをグループに追加する

1つ以上のストレージアレイをユーザが作成したグループに追加できます。

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] をクリックします。 *

グループからのストレージアレイの削除

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から管理する必要がなくなった場合は、グループから削除できます。

タスクの内容

グループからストレージアレイを削除しても、ストレージアレイやそのデータには影響しません。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誤ってグループから削除した場合は、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の削除

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できます。

タスクの内容

この処理で削除されるのは、ストレージアレイグループのみです。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、[すべて管理]ビューまたは関連付けられているその他のグループから引き続きアクセスできます。

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。

ストレージアレイグループの名前変更

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

タスクの内容

これらのガイドラインに注意してください。

- 名前に使用できる文字は、アルファベット、数字、アンダースコア（_）、ハイフン（-）、シャープ（#）です。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。
- わかりやすく覚えやすい一意のわかりやすい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. *名前変更.*をクリックします

アップグレード

アップグレードセンターの概要

アップグレードセンターでは、複数のストレージアレイのSANtricity OSソフトウェアとNVSRAMのアップグレードを管理できます。

アップグレードの仕組み

最新のOSソフトウェアをダウンロードしてから、1つ以上のアレイをアップグレードします。

アップグレードワークフロー

次の手順では、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ソフトウェアファイルをサポートサイトからダウンロードします（サポートページのUnified Managerからリンクできます）。管理ホストシステム（ブラウザでUnified Manager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. Unified Managerで、SANtricity OSソフトウェアファイルとNVSRAMファイルをリポジトリ（Webサービスプロキシサーバのファイルが格納されている領域）にロードします。ファイルは、メニューから追加できます。[Upgrade SANtricity OS Software]または[Upgrade Center]>[Manage Software Repository]から選択します。
3. ファイルがリポジトリにロードされたら、アップグレードで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（メニュー：アップグレードセンター[Upgrade SANtricity OS software]）から、SANtricity 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に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. その後、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、後でアクティブ化するためにファイルをステージングすることもできます。アップグレードプロセスを実行すると、Unified Managerで次の処理が実行されます。
   a. 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を妨げる可能性のある状況がないかどうかが確認されます。いずれかのアレイが健全性チェックで不合格になった場合は、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合格しなかった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。
   b. アップグレードファイルを各コントローラに転送します。
   c. コントローラが一度に1台ずつリブートされ、新しいSANtricity OSソフトウェアがアクティブ化されます。アクティブ化では、既存のSANtricity 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。

即時アップグレードまたは段階的アップグレード

アップグレードはただちにアクティブ化することも、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。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。I/O負荷とキャッシュサイズによっては、コントローラのアップグレードが完了するまでに通常15~25分かかることがあります。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

ステージング済みソフトウェアをアクティブにするには、メニューサポート[Upgrade Center]に移動し、SANtricity OSコントローラソフトウェアのアップグレードというラベルの付いた領域で[Activate （有効化）]をクリックします。

健全性チェック

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、開始する前に別途実行することもできます（メニュー：Upgrade Center [Pre-Upgrade Health Check]に移動）。

健全性チェックでは、ストレージシステム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かどうかがチェックされます。アップグレードを実行できない状況は次のとおりです。

- 割り当て済みドライブで障害が発生
- ホットスペアを使用中です
- ボリュームグループに不備がある
- 同時に実行できない処理
- ボリュームが見つからない
- コントローラのステータスが最適でない
- イベントログイベントの数が多すぎる
- 構成データベースの検証エラー
- 古いバージョンのDACstoreを搭載したドライブ

アップグレードするときは、どのような点に注意する必要がありますか？

複数のストレージアレイをアップグレードする前に、計画の一環として重要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、Unified Manager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ソフトウェアの列に表示されます。各行の SANtricity 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できるように、ホストのマルチパス/フェイルオーバードライバまたはHBAドライバのアップグレードも必要になる場合があります。

互換性については、を参照して "NetAppのInteroperability Matrix"ください。手順については、使用しているオペレーティングシステムに対応したエクスプレスガイドを参照してください。エクスプレスガイドはから入手でき "E シリーズおよび SANtricity に関するドキュメント"ます。

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の処理を続行できます。アップグレード中に、次のプロセスが実行されます。

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が自身のLUNとコントローラBのすべてのLUNをテイクバックします。
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。

ソフトウェアとファームウェアのアップグレード

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、開始前に個別に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かどう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。

   [アップグレード前の健全性チェック]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一覧が表示されます。

2. 必要に応じて、ストレージシステムをリストでフィルタまたはソートして、現在最適状態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は、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、その他のタスクを実行したりできます。

> いずれかのアレイが健全性チェックで不合格になった場合は、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合格しなかった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のアップグレード

1つ以上のストレージアレイを最新のソフトウェアとNVSRAMで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

デフォルト設定を指定するコントローラファイルです。

開始する前に

- 最新のSANtricity OSファイルは、SANtricity Webサービスプロキシとの Unified Managerが実行されているホストシステムにあります。
- ソフトウェアアップグレードを今すぐアクティブ化するかあとでアクティブ化するかを決めておきます。

  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

システムを11.80.x以降にアップグレードするには、SANtricity OS 11.70.5が実行されている必要があります。

タスクの内容

```
[NOTE]
====
データ損失またはストレージアレイの破損のリスク-
アップグレードの実行中はストレージアレイを変更しないでください。ストレージアレイへの電源を維持します。

====
.手順
. ストレージアレイにコントローラが
1台しかない場合、またはマルチパスドライバを使用していない場合は、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。
. 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。
. メニューからアップグレードセンター [Upgrade SANtricity OS Software]
を選択します。
+
[Upgrade SANtricity OS software]ページが表示されます。

. 最新のSANtricity OSソフトウェアパッケージを
NetAppサポートサイトからローカルマシンにダウンロードします。
+
.. [ 新しいファイルをソフトウェアリポジトリに追加する *] をクリックします。
.. 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。
.. [Download Latest Release] リンクをクリックします。
.. 以降の手順に従って、 SANtricity 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。

+
[NOTE]
====
バージョン8.42以降では、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。

====
. 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。
+
.. [Select a SANtricity OS software file*]
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。

+
[NOTE]
====
ソフトウェアリポジトリには、Web Services
Proxy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。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。

====
.. 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。

. [互換性があるストレージアレイ]の表で、選択した
OSソフトウェアファイルと互換性が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。
+
** [互換性があるストレージアレイ]の表では、[管理
]ビューで選択したストレージアレイのうち、選択したファームウェアファイルと互換性があるストレージアレイがデフォルトで選択されます。
** 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。

. *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、後でアクティブ化*チェックボックスをオンにします。
. [スタート] ボタンをクリックします。
. 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、アップグレード対象として選択したアレイの OS ソフトウェアの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 [Upgrade Center] [Activate Staged OS Software] 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、リブートが開始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。

+
**
アップグレード前の健常性チェックは、アップグレードプロセスの一環として実行されます。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かどうかがチェックされます。
** ストレージアレイの健全性チェックに失敗すると、アップグレードは停止します。省略符号 (...) をクリックして * ログを保存 * を選択すると、エラーを確認できます。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できます。

. *オプション：*アップグレードが完了したら、省略記号（...）をクリックし、*ログの保存*を選択すると、特定のストレージ・アレイのアップグレード内容のリストが表示されます。
+
ブラウザのDownloadsフォルダにという名前でファイルが保存されます `upgrade_log-<date>.json`。

[[IDefb87482c18d4dd8872d3ee8c930e648]]
= ステージング済みOSソフトウェアのアクティブ化

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


[role="lead"]
```
ソフトウェアファイルはすぐにアクティブ化することも、都合の良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ことを前提としています。

.タスクの内容
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


```
[NOTE]
====
```
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
. メインビューで、* Manage *（管理）を選択します。必要に応じて、ページ上部の[ステータス]列をクリックしてソートし、ステータスが「OSアップグレード（アクティブ化待ち）」のすべてのストレージアレイを表示します。
. 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 OS 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、アクティブ化を続行できるかどうかがチェックされます。
** ストレージアレイの健全性チェックに失敗すると、アクティブ化は停止します。省略符号 (...) をクリックして * ログを保存 *
を選択すると、エラーを確認できます。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するコンポーネントによって異なります。

. *オプション：*アクティブ化が完了すると、省略記号（
...）をクリックし、「ログを保存」を選択することにより、特定のストレージアレイに対してアクティブ化された内容のリストが表示されます。
+
ブラウザのDownloadsフォルダにという名前でファイルが保存されます `activate_log-<date>.json`。

[[IDd0a8d664558c459907fb3f27eaa5cc8e]]
= ソフトウェアリポジトリの管理
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ソフトウェアリポジトリには、Web Services
Proxy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。

使用するファイルが表示されない場合は、ソフトウェアリポジトリの管理オプションを使用して、Webサービスプロキシと Unified Managerが実行されているホストシステムに1
つ以上のSANtricity 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SANtricity
OSファイルを削除することもできます。

.開始する前に
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。

.手順
. メインビューから* Manage *を選択し、メニューからUpgrade Center [Manage Software Repository]を選択します。
+
[Manage Software Repository]ダイアログボックスが表示されます。

. 次のいずれかを実行します。

+
[cols="25h,~"]
|===
| オプション | これをしなさい…

a|
インポート
a|
.. [*インポート.*]をクリックします
.. [*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、のようになり `N2800-830000-000.dlp`ます。

.. 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。

a|
削除
a|
.. 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。
.. [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。[Delete]を選択すると、ファイルがソフトウェアリポジトリから削除されます。

[[ID3b3d15cb8170528e2259d79a6688de07]]
= ステージング済みOSソフトウェアのクリア
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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
. メインビューから* Manage *を選択し、メニュー：Upgrade Center（アップグレードセンター）[Clear Staged OS Software]（ステージング済みOSソフトウェアのクリア）を選択します。
+
[ステージング済みOSソフトウェアのクリア]ダイアログボックスが開き、保留中のソフトウェアまたはNVSRAMがあるストレージシステムが検出されたすべてのリストが表示されます。

.
必要に応じて、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表示できるように、リストでストレージシステムをフィルタまたはソートします。
. 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。
. [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。

:leveloffset: -1

:leveloffset: -1

= ミラーリング

:leveloffset: +1

[[IDc932de422716fe626d2320cd4c5ff61c]]
= ミラーリングの概要
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ミラーリング機能を使用して、ローカルストレージアレイとリモートストレージアレイの間でデータを非同期または同期的にレプリケートします。

[NOTE]
====

同期ミラーリングは、EF600またはEF300ストレージシステムでは使用できません。

====

== ミラーリングとは

SANtricityアプリケーションには、非同期と同期の2種類のミラーリングがあります。非同期ミラーリングでは、データボリュームがオンデマンドまたはスケジュールに基づいてコピーされるため、データの破損や損失が原因で発生するダウンタイムを最小限または回避できます。同期ミラーリングでは、データボリュームがリアルタイムでレプリケートされるため、継続的な可用性が確保されます。

詳細：

* xref:{relative_path}mirroring-overview.html["ミラーリングの仕組み"]
* xref:{relative_path}mirroring-terminology.html["ミラーリングに関する用語"]

== ミラーリングの設定方法

Unified Managerで非同期ミラーリングまたは同期ミラーリングを設定し、System Managerを使用して同期を管理します。

詳細：

* xref:{relative_path}mirroring-configuration-workflow.html["ミラーリングの設定ワークフロー"]
* xref:{relative_path}requirements-for-using-mirroring.html["ミラーリングを使用するための要件"]
* xref:{relative_path}create-asynchronous-mirrored-pair-um.html["非同期ミラーペアの作成"]
* xref:{relative_path}create-synchronous-mirrored-pair-um.html["同期ミラーペアの作成"]

= 概念

:leveloffset: +1

[[ID6f5565d1479440cab9089cf06f8597c5]]
= ミラーリングの仕組み

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


[role="lead"]
Unified ManagerにはSANtricity
ミラーリング機能の設定オプションが用意されており、管理者は2つのストレージアレイ間でデータをレプリケートしてデータを保護できます。

[NOTE]
====
同期ミラーリングは、EF600またはEF300ストレージシステムでは使用できません。

====


== ミラーリングのタイプ

SANtricityアプリケーションには、非同期と同期の2種類のミラーリングがあります。

非同期ミラーリングでは、データボリュームがオンデマンドまたはスケジュールに基づいてコピーされるため、データの破損や損失が原因で発生するダウンタイムを最小限または回避できます。非同期ミラーリングでは、特定の時点におけるプライマリボリュームの状態がキャプチャされ、前回のイメージキャプチャ以降に変更されたデータだけがコピーされます。プライマリサイトはただちに更新でき、セカンダリサイトは帯域幅の許す限り更新できます。情報はキャッシュされ、あとでネットワークリソースが利用可能になると送信されます。このタイプのミラーリングは、バックアップやアーカイブなどの定期的なプロセスに最適です。

同期ミラーリングでは、データボリュームがリアルタイムでレプリケートされるため、継続的な可用性が確保されます。目的は、2つのストレージアレイのいずれかで災害が発生した場合に重要なデータのコピーを確保しておくことで、データ損失ゼロの目標復旧時点（RPO）を達成することです。プライマリボリュームに書き込みが行われるたびにセカンダリボリュームにも書き込みが行われるため、コピーは常に本番環境のデータと同じです。プライマリボリュームで行われた変更でセカンダリボリュームが更新されるまで、ホストは書き込みが成功したことを示す確認応答を受信しません。このタイプのミラーリングは、ディザスタリカバリなどのビジネス継続性の目的に最適です。



== ミラーリングのタイプの違い

次の表に、2種類のミラーリングの主な違いを示します。

[cols="1a,1a,1a"]
|===
| 属性 | 非同期 | 同期
```

a|
レプリケーション方法
a|
ポイントインタイム--
ミラーリングはオンデマンドで、またはユーザー定義のスケジュールに従って自動的に実行されます。
a|
continuous --ミラーリングは自動的に継続的に実行され
'ホストの書き込みごとにデータがコピーされます

a|
距離
a|
アレイ間の長距離をサポートします。通常、距離はネットワークとチャネル拡張テクノロジーの機能によってのみ制限されます。
a|
アレイ間の距離は短くしてください。レイテンシとアプリケーションパフォーマンスの要件を満たすために、通常はローカルストレージアレイから約10km（6.2マイル）以内の距離にする必要があります。

a|
通信方法
a|
標準のIPまたはFibre Channelネットワーク。
a|
Fibre Channelネットワークのみ。

a|
ボリュームタイプ
a|
標準またはシン。
a|
標準のみ。

|===

[[IDe4b35b813de58f9ea45fb16c13ba0198]]
= ミラーリングの設定ワークフロー

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


[role="lead"]
Unified Managerで非同期ミラーリングまたは同期ミラーリングを設定し、System
Managerを使用して同期を管理します。



== 非同期ミラーリングのワークフロー

非同期ミラーリングのワークフローは次のとおりです。

. Unified Managerで初期設定を実行します。
+
.. データ転送元としてローカルストレージアレイを選択します。
..
ミラー整合性グループを作成または選択します。ミラー整合性グループは、ローカルアレイ上のプライマリボリュームとリモートアレイ上のセカンダリボリュームのコンテナです。プライマリボリュームとセカンダリ ボリュームは「ミラーペア」と呼ばれます。ミラー整合性グループを初めて作成する場合は、実行する同期方法（手動またはスケジュール）を指定します。
..
ローカルストレージアレイからプライマリボリュームを選択し、リザーブ容量を確認します。リザーブ容量は、コピー処理に使用される物理割り当て容量です。
..
転送先としてリモートストレージアレイを選択し、セカンダリボリュームを選択して、リザーブ容量を確認します。
..
プライマリボリュームからセカンダリボリュームへの初回のデータ転送を開始します。ボリュームサイズによっては、この初回転送に数時間かかることがあります。



. 初期同期の進捗状況を確認します。
+
.. Unified Managerで、ローカルアレイのSystem Managerを起動します。
.. System
Managerで、ミラーリング処理のステータスを確認します。ミラーリングが完了すると、ミラーペアのステータスは「最適」になります。



. 必要に応じて、System
Managerで後続のデータ転送のスケジュールを再設定したり、手動で実行したりできます。新しいブロックと変更されたブロックだけがプライマリボリュームからセカンダリボリュームに転送され
```

ます。
+
[NOTE]
====
非同期レプリケーションは定期的に行われるため、変更されたブロックを統合してネットワーク帯域幅を節約できます。書き込みスループットと書き込みレイテンシへの影響は最小限に抑えられます。

====

== 同期ミラーリングのワークフロー

同期ミラーリングのワークフローは次のとおりです。

. Unified Managerで初期設定を実行します。
+
.. データ転送元としてローカルストレージアレイを選択します。
.. ローカルストレージアレイからプライマリボリュームを選択します。
.. データ転送先としてリモートストレージアレイを選択し、セカンダリボリュームを選択します。
.. 同期と再同期の優先度を選択します。
..
プライマリボリュームからセカンダリボリュームへの初回のデータ転送を開始します。ボリュームサイズによっては、この初回転送に数時間かかることがあります。

. 初期同期の進捗状況を確認します。
+
.. Unified Managerで、ローカルアレイのSystem Managerを起動します。
.. System Managerで、ミラーリング処理のステータスを確認します。ミラーリングが完了すると、ミラーペアのステータスは「最適」になります。2つのアレイは、通常の処理を通じて同期状態が維持されます。新しいブロックと変更されたブロックだけがプライマリボリュームからセカンダリボリュームに転送されます。

. 必要に応じて、System Managerで同期設定を変更できます。
+
[NOTE]
====
同期レプリケーションは継続的であるため、2つのサイト間のレプリケーションリンクで十分な帯域幅機能を提供する必要があります。

====

```
[[ID3dc652f6e4954eda1853e1bb06d4b1af]]
= ミラーリングに関する用語
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
ストレージアレイに関連するミラーリングの用語を次に示します。

```
[cols="25h,~"]
|===
| 期間 | 製品説明


 a|
```
ローカルストレージアレイ
```
 a|
```
ローカルストレージアレイは、操作の対象となるストレージアレイです。

```
 a|
```
ミラー整合性グループ
```
 a|
```
ミラー整合性グループは、1つ以上のミラーペアのコンテナです。非同期ミラーリング処理では、ミラー整合性グループを作成する必要があります。グループ内のすべてのミラーペアが同時に再同期されるため、整合性のあるリカバリポイントが維持されます。

同期ミラーリングではミラー整合性グループを使用しません。

```
 a|
```
ミラーペア
```
 a|
```
ミラーペアは、プライマリボリュームとセカンダリボリュームの2つのボリュームで構成されます。

非同期ミラーリングでは、ミラーペアは常にミラー整合性グループに属します。書き込み処理は最初にプライマリボリュームに対して実行され、次にセカンダリボリュームにレプリケートされます。ミラー整合性グループ内の各ミラーペアでは、同じ同期設定が共有されます。

a|
プライマリボリューム
a|
ミラーペアのプライマリボリュームは、ミラーリングするソースボリュームです。

a|
リモートストレージアレイ
a|
通常、リモートストレージアレイはセカンダリサイトとして指定され、セカンダリサイトにはミラーリング構成のデータのレプリカが格納されます。

a|
リザーブ容量
a|
リザーブ容量は、コピーサービス処理やストレージオブジェクトに使用される物理割り当て容量です。ホストから直接読み取ることはできません。

ミラーリングの動作状態を維持するために必要な情報をコントローラが永続的に保存できるようにするには、これらのボリュームが必要です。これらのボリュームには、差分ログや`copy-on-write`データなどの情報が格納されます。

a|
セカンダリボリューム
a|
ミラーペアのセカンダリボリュームは、通常はセカンダリサイトに配置され、データのレプリカが格納されます。

a|
同期
a|
同期は、ローカルストレージアレイとリモートストレージアレイの間の初期同期で実行されます。同期は、通信の中断後にプライマリボリュームとセカンダリボリュームが同期されていない状態になった場合にも実行されます。通信リンクの動作が再開されると、レプリケートされていないデータがセカンダリボリュームのストレージアレイに同期されます。

|===

```
[[ID559d2c73943347841fb3331625453072]]
= ミラーリングを使用するための要件
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
ミラーリングを設定する場合は、次の要件に注意してください。



== Unified Manager

* Web Services Proxyサービスが実行されている必要があります。
* Unified ManagerがHTTPS接続経由でローカルホストで実行されている必要があります。
* Unified Managerにストレージアレイの有効なSSL
証明書が表示されている必要があります。Unified Managerのメニューから「Certificate Management」に移動し、自己署名証明書を受け入れるか、独自のセキュリティ証明書をインストールできます。




== ストレージアレイ

[NOTE]
====
同期ミラーリングはEF600またはEF300ストレージアレイでは使用できません。

====
* 2つのストレージアレイが必要です。
* 各ストレージアレイに2台のコントローラが必要です。
* Unified Managerで2つのストレージアレイが検出されている必要があります。
*
プライマリアレイとセカンダリアレイの両方の各コントローラにイーサネット管理ポートが設定され、ネットワークに接続されている必要があります。
* ストレージアレイに必要なファームウェアの最小バージョンは7.84です（それぞれ異なるOSバージョンを実行できます）。
* ローカルとリモートのストレージアレイのパスワードを確認しておく必要があります。
*
ミラーリングするプライマリボリューム以上のセカンダリボリュームを作成するには、リモートストレージアレイに十分な空き容量が必要です。
* 非同期ミラーリングはFibre Channel（FC）または
iSCSIホストポートを搭載したコントローラでサポートされますが、同期ミラーリングはFCホスト
```

ポートを搭載したコントローラでのみサポートされます。

== 接続要件

FCインターフェイスでのミラーリング（非同期または同期）には次の要件が適用されます。

* ストレージアレイの各コントローラでは、最も番号が大きい
FCホストポートがミラーリング処理の専用ポートとして使用されます。
* ベースのFCポートとホストインターフェイスカード（HIC）の
FCポートの両方があるコントローラでは、HICの最も番号が大きいポートが使用されます。専用ポートにログオンしたホストはログアウトされ、ホストログイン要求は許可されません。このポートでのI/O要求は、ミラーリング処理の対象となるコントローラからのみ許可されます。
*
専用のミラーリングポートは、ディレクトリサービスとネームサービスのインターフェイスをサポートするFCファブリック環境に接続されている必要があります。特に、FC-
ALおよびポイントツーポイントはミラー関係が確立されたコントローラ間の接続オプションとしてサポートされないことに注意してください。

iSCSIインターフェイスでのミラーリング（非同期のみ）には次の要件が適用されます。

* FCとは異なり、iSCSIでは専用のポートを必要としません。
iSCSI環境で非同期ミラーリングを使用する場合、ストレージアレイのどのフロントエンドiSCSIポートも非同期ミラーリング専用にする必要はありません。これらのポートは、非同期ミラーリングのトラフィックとホスト/アレイ間のI/O接続で共有されます。
* コントローラはリモートストレージシステムのリストを管理しており、
iSCSIイニシエータはこのリストを使用してセッションの確立を試みます。iSCSI接続の確立に成功した最初のポートは、そのリモートストレージアレイとの以降のすべての通信に使用されます。通信に失敗すると、使用可能なすべてのポートを使用して新しいセッションの確立が試行されます。
*
iSCSIポートは、アレイレベルでポート単位で設定します。設定メッセージおよびデータ転送用のコントローラ間通信では、次の設定を含むグローバル設定が使用されます。
+
** VLAN：ローカルシステムとリモートシステムが通信するためには、両方のシステムで
VLAN設定が同じである必要があります
** iSCSIリスニングポート
** ジャンボフレーム
** イーサネットの優先順位

[NOTE]

====
コントローラ間のiSCSI通信には、管理イーサネットポートではなくホスト接続ポートを使用する必要があります。

====

== ミラーボリュームの候補

* ミラーペアのプライマリボリュームとセカンダリボリュームでは、RAIDレベル、キャッシングパラメータ、およびセグメントサイズが異なる場合があります。
+

NOTE: EF600およびEF300コントローラでは、非同期ミラーペアのプライマリボリュームとセカンダリボリュームのプロトコル、トレイレベル、セグメントサイズ、セキュリティタイプ、およびRAIDレベルが同じである必要があります。対応していない非同期ミラーペアは、使用可能なボリュームのリストに表示されません。

* セカンダリボリュームは、プライマリボリュームと同じサイズ以上である必要があります。
* ボリュームに設定できるミラー関係は1つだけです。
*
同期ミラーペアの場合、プライマリボリュームとセカンダリボリュームは標準ボリュームである必要があります。シンボリュームやSnapshotボリュームは使用できません。
*
同期ミラーリングの場合、特定のストレージアレイでサポートされるボリュームの数に制限があります。ストレージアレイに設定されているボリュームの数がサポートされている制限よりも少ないことを確認してください。同期ミラーリングがアクティブな場合は、作成された2つのリザーブ容量ボリュームがボリュームの制限に含まれます。
*
非同期ミラーリングの場合、プライマリボリュームとセカンダリボリュームのドライブセキュリティ機能が同じである必要があります。
+
** プライマリボリュームがFIPSに対応している場合、セカンダリボリュームはFIPSに対応している必要があります。
** プライマリボリュームがFDEに対応している場合、セカンダリボリュームはFDEに対応している必要があります。
**
プライマリボリュームでドライブセキュリティを使用していない場合、セカンダリボリュームでドライブセキュリティを使用していない必要があります。

== リザーブ容量

非同期ミラーリングの場合：

*
コントローラのリセットおよびその他の一時的な中断からリカバリするための書き込み情報をログに記録するには、ミラーペアのプライマリボリュームとセカンダリボリュームにリザーブ容量ボリュームが必要です。
*
ミラーペアのプライマリボリュームとセカンダリボリュームには追加のリザーブ容量が必要であるため、ミラー関係にある両方のストレージアレイに空き容量が確保されていることを確認してください。

同期ミラーリングの場合：

*
コントローラのリセットおよびその他の一時的な中断からリカバリするための書き込み情報をログに記録するには、プライマリボリュームとセカンダリボリュームにリザーブ容量が必要です。
*
同期ミラーリングがアクティブ化されると、リザーブ容量ボリュームが自動的に作成されます。ミラーペアのプライマリボリュームとセカンダリボリュームにはリザーブ容量が必要であるため、同期ミラー関係にある両方のストレージアレイに十分な空き容量が確保されていることを確認してください。

== ドライブセキュリティ機能

*
セキュリティ対応ドライブを使用する場合、プライマリボリュームとセカンダリボリュームのセキュリティ設定に互換性がある必要があります。この制限は強制的には適用されないため、自分で確認する必要があります。
*
セキュリティ対応ドライブを使用する場合、プライマリボリュームとセカンダリボリュームで同じタイプのドライブを使用する必要があります。この制限は強制的には適用されないため、自分で確認する必要があります。
* Data Assurance（DA）を使用する場合、プライマリボリュームとセカンダリボリュームでDA設定を同じにする必要があります。

:leveloffset: -1

= ミラーリングの設定

```
:leveloffset: +1


[[ID59f302dac40f9e20583e9a54b2bf5276]]
= 非同期ミラーペアの作成
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
非同期ミラーリングを設定するには、ローカルアレイのプライマリボリュームとリモートアレイのセカンダリボリュームを含むミラーペアを作成します。

.開始する前に
ミラーペアを作成する前に、Unified Managerに関する次の要件を満たしている必要があります。

* Web Services Proxyサービスが実行されている必要があります。
* Unified ManagerがHTTPS接続経由でローカルホストで実行されている必要があります。
* Unified Managerにストレージアレイの有効なSSL証明書が表示されている必要があります。Unified Managerのメニューから「Certificate Management」に移動し、自己署名証明書を受け入れるか、独自のセキュリティ証明書をインストールできます。


また、ストレージアレイおよびボリュームに関する次の要件も満たしている必要があります。

* 各ストレージアレイに2台のコントローラが必要です。
* Unified Managerで2つのストレージアレイが検出されている必要があります。
*
プライマリアレイとセカンダリアレイの両方の各コントローラにイーサネット管理ポートが設定され、ネットワークに接続されている必要があります。
* ストレージアレイに必要なファームウェアの最小バージョンは7.84です（それぞれ異なるOSバージョンを実行できます）。
* ローカルとリモートのストレージアレイのパスワードを確認しておく必要があります。
*
ミラーリングするプライマリボリューム以上のセカンダリボリュームを作成するには、リモートストレージアレイに十分な空き容量が必要です。
* ローカルとリモートのストレージアレイをFibre Channelファブリックまたは iSCSIインターフェイスを介して接続します。
*
非同期ミラー関係で使用するプライマリボリュームとセカンダリボリュームの両方を作成しておきます。
* セカンダリボリュームは、プライマリボリュームと同じサイズ以上である必要があります。
```

.タスクの内容
非同期ミラーペアを作成するプロセスは複数の手順で構成されます。

== 手順1：ミラー整合性グループを作成または選択する

この手順では、新しいミラー整合性グループを作成するか、既存のミラー整合性グループを選択します。ミラー整合性グループは、プライマリボリュームとセカンダリボリューム（ミラーペア）のコンテナであり、グループ内のすべてのペアに必要な再同期方法（手動または自動）を指定します。

.手順
. [* Manage *（管理）]ページで、ソースに使用するローカルストレージアレイを選択します。
. メニューを選択します。アクション[非同期ミラーペアの作成]。
+
非同期ミラーペアの作成ウィザードが開きます。

. 既存のミラー整合性グループを選択するか、新規に作成します。
+
既存のグループを選択するには、「*既存のミラー整合グループ*」が選択されていることを確認してから、表からグループを選択してください。整合グループには複数のミラーペアを含めることができます。

+
新しいグループを作成するには、次の手順を実行します。

+
.. 新しいミラー整合性グループを選択*し、*次へ*をクリックします。
..
2つのストレージアレイ間でミラーリングするボリューム上のデータに最も近い一意の名前を入力します。名前に使用できる文字は、アルファベット、数字、アンダースコア（_）、ダッシュ（-）、ハッシュ記号（#）だけです。最大文字数は30文字で、スペースは使用できません。
..
ローカルストレージアレイとの間でミラー関係を確立するリモートストレージアレイを選択します。
+
[NOTE]
====
リモートストレージアレイがパスワードで保護されている場合は、パスワードの入力を求められます。

====
.. ミラーペアの同期を手動で行うか自動で行うかを選択します。
+

*** *手動*-
このオプションは、グループ内のすべてのミラーペアの同期を手動で開始する場合に選択します。再同期をあとで実行する場合は、プライマリストレージアレイのSystem Managerを起動して、メニューから「Storage [Asynchronous Mirroring]」に移動し、「Mirror Consistency Groups *」タブでグループを選択して、メニューから「More [Manually resynchronize]」を選択する必要があります。
*** *自動*--前回の更新の開始から次の更新の開始までの間隔を*分*、*時間*、または*日*で選択します。たとえば、同期間隔が30分に設定され、同期プロセスが午後4時に開始される場合、次のプロセスは午後4時30分に開始されます。

. . 必要なアラート設定を選択します。
+
***
手動同期の場合は、アラートを受信するときのしきい値（残りの容量の割合によって定義）を指定します。
*** 自動同期では、3つのアラート方法を設定できます。
1つは、特定の時間内に同期が完了していない場合、リモートアレイのリカバリポイントデータが特定の制限時間を超えた場合、もう1つはリザーブ容量が特定のしきい値（残りの容量の割合で定義）に近づいている場合です。

. [次へ]*を選択し、に進みます<<手順2：プライマリボリュームを選択する>>。
+
新しいミラー整合性グループを定義した場合は、Unified Managerによって、最初にローカルストレージアレイに、続いてリモートストレージアレイにミラー整合性グループが作成されます。各アレイのSystem Managerを起動すると、ミラー整合性グループを表示および管理できます。

+
[NOTE]
====
Unified Managerによるミラー整合性グループの作成がローカルストレージアレイで成功したあと、リモートストレージアレイで失敗した場合は、ローカルストレージアレイからミラー整合性グループが自動的に削除されます。Unified Managerによるミラー整合性グループの削除でエラーが発生した場合は、手動で削除する必要があります。

====

== 手順2：プライマリボリュームを選択する

この手順では、ミラー関係で使用するプライマリボリュームを選択し、リザーブ容量を割り当てます。ローカルストレージアレイのプライマリボリュームを選択すると、そのミラーペアに対応するすべてのボリュームのリストが表示されます。使用できないボリュームはリストに表示されません。

ローカルストレージアレイのミラー整合性グループに追加したボリュームには、ミラー関係のプライマリロールが割り当てられます。

.手順
. 対応するボリュームのリストからプライマリボリュームとして使用するボリュームを選択し、*Next *をクリックしてリザーブ容量を割り当てます。
. 対応する候補のリストから、プライマリボリュームのリザーブ容量を選択します。
+
次のガイドラインに注意してください。

+
** リザーブ容量のデフォルト設定はベースボリュームの容量の20%で、通常はこの容量で十分です。割合を変更する場合は、[*候補の更新*]をクリックします。
** 必要な容量は、プライマリボリュームに対するI/O書き込みの頻度とサイズ、およびその容量を維持する必要がある期間によって異なります。
** 一般に、次のいずれかまたは両方に該当する場合は、リザーブ容量を大きくします。
+
*** ミラーペアを長期間保持する場合。
*** 大量のI/Oアクティビティにより、プライマリボリュームのデータブロックの大部分で変更が発生する場合。プライマリボリュームに対する一般的なI/Oアクティビティを判断するには、過去のパフォーマンスデータやその他のオペレーティングシステムユーティリティを使用します。

. [次へ]*を選択し、に進みます<<手順3：セカンダリボリュームを選択する>>。

== 手順3：セカンダリボリュームを選択する

この手順では、ミラー関係で使用するセカンダリボリュームを選択し、リザーブ容量を割り当てます。リモートストレージアレイのセカンダリボリュームを選択すると、そのミラーペアに対応するすべてのボリュームのリストが表示されます。使用できないボリュームはリストに表示されません。

リモートストレージアレイのミラー整合性グループに追加したボリュームには、ミラー関係のセカンダリロールが割り当てられます。

.手順
.
対応するボリュームのリストから、ミラーペアのセカンダリボリュームとして使用するボリュームを選択し、* Next *をクリックしてリザーブ容量を割り当てます。
. 対応する候補のリストから、セカンダリボリュームのリザーブ容量を選択します。
+
次のガイドラインに注意してください。

+
** リザーブ容量のデフォルト設定はベースボリュームの容量の20%で、通常はこの容量で十分です。割合を変更する場合は、[*候補の更新*]をクリックします。
** 必要な容量は、プライマリボリュームに対するI/O書き込みの頻度とサイズ、およびその容量を維持する必要がある期間によって異なります。
** 一般に、次のいずれかまたは両方に該当する場合は、リザーブ容量を大きくします。
+
*** ミラーペアを長期間保持する場合。
*** 大量のI/Oアクティビティにより、プライマリボリュームのデータブロックの大部分で変更が発生する場合。プライマリボリュームに対する一般的なI/Oアクティビティを判断するには、過去のパフォーマンスデータやその他のオペレーティングシステムユーティリティを使用します。

. 「* Finish *」を選択して、非同期ミラーリングのシーケンスを完了します。

.結果
Unified Managerは次の処理を実行します。

* ローカルストレージアレイとリモートストレージアレイの間の初期同期を開始します。
*
ローカルストレージアレイとリモートストレージアレイにミラーペア用のリザーブ容量を作成します。

NOTE:
ミラーリングしているボリュームがシンボリュームの場合、初期同期では、プロビジョニングされたブロック（レポート容量ではなく割り当て容量）のみがセカンダリボリュームに転送されます。これにより、初期同期を完了するために転送する必要のあるデータ量が削減されます。

[[ID80ef80528b56691e77df8a49457c771e]]
= 同期ミラーペアの作成
:allow-uri-read:

```
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
同期ミラーリングを設定するには、ローカルアレイのプライマリボリュームとリモートアレイのセカンダリボリュームを含むミラーペアを作成します。

[NOTE]
====
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。

====
.開始する前に
ミラーペアを作成する前に、Unified
Managerに関する次の要件を満たしている必要があります。

* Web Services Proxyサービスが実行されている必要があります。
* Unified ManagerがHTTPS接続経由でローカルホストで実行されている必要があります。
* Unified Managerにストレージアレイの有効なSSL
証明書が表示されている必要があります。Unified Managerのメニューから「Certificate
Management」に移動し、自己署名証明書を受け入れるか、独自のセキュリティ証明書をインストールできます。


また、ストレージアレイおよびボリュームに関する次の要件も満たしている必要があります。

* ミラーリングに使用する2つのストレージアレイがUnified
Managerで検出されている必要があります。
* 各ストレージアレイに2台のコントローラが必要です。
*
プライマリアレイとセカンダリアレイの両方の各コントローラにイーサネット管理ポートが設定され、ネットワークに接続されている必要があります。
* ストレージアレイに必要なファームウェアの最小バージョンは7.84です（それぞれ異なる
OSバージョンを実行できます）。
* ローカルとリモートのストレージアレイのパスワードを確認しておく必要があります。
* ローカルとリモートのストレージアレイをFibre Channelファブリックを介して接続します。
*
同期ミラー関係で使用するプライマリボリュームとセカンダリボリュームの両方を作成しておきます。
* プライマリボリュームは標準ボリュームである必要があります。シンボリュームや
Snapshotボリュームを使用することはできません。
* セカンダリボリュームは標準ボリュームである必要があります。シンボリュームや
Snapshotボリュームを使用することはできません。
*
```

セカンダリボリュームには、プライマリボリュームと同じサイズ以上のサイズを指定する必要があります。

.タスクの内容
同期ミラーペアを作成するプロセスは複数の手順で構成されます。

== 手順1：プライマリボリュームを選択する

この手順では、同期ミラー関係で使用するプライマリボリュームを選択します。ローカルストレージアレイのプライマリボリュームを選択すると、そのミラーペアに対応するすべてのボリュームのリストが表示されます。使用できないボリュームはリストに表示されません。選択するボリュームには、ミラー関係のプライマリロールが割り当てられます。

.手順
. [* Manage *（管理）]ページで、ソースに使用するローカルストレージアレイを選択します。
. メニューを選択します。アクション[同期ミラーペアの作成]。
+
同期ミラーペアの作成ウィザードが開きます。

.
対応するボリュームのリストから、ミラーのプライマリボリュームとして使用するボリュームを選択します。
. [次へ]*を選択し、に進みます<<手順2：セカンダリボリュームを選択する>>。

== 手順2：セカンダリボリュームを選択する

この手順では、ミラー関係で使用するセカンダリボリュームを選択します。リモートストレージアレイのセカンダリボリュームを選択すると、そのミラーペアに対応するすべてのボリュームのリストが表示されます。使用できないボリュームはリストに表示されません。選択するボリュームには、ミラー関係のセカンダリロールが割り当てられます。

.手順
.
ローカルストレージアレイとの間でミラー関係を確立するリモートストレージアレイを選択します。
+
[NOTE]
====
リモートストレージアレイがパスワードで保護されている場合は、パスワードの入力を求められます。

====

+
**
ストレージアレイは、それぞれのストレージアレイ名で表示されます。ストレージアレイに名前を付けていない場合は、「unnamed」と表示されます。
** 使用するストレージアレイがリストにない場合は、Unified Managerでそのストレージアレイが検出されていることを確認してください。

.
対応するボリュームのリストから、ミラーのセカンダリボリュームとして使用するボリュームを選択します。
+
[NOTE]
====
選択したセカンダリボリュームの容量がプライマリボリュームよりも大きい場合、使用可能な容量はプライマリボリュームのサイズまでに制限されます。

====
. [次へ]*をクリックし、に進みます<<手順3：同期設定を選択します>>。

== 手順3：同期設定を選択します

このステップでは、通信中断後のデータの同期方法を決定する設定を選択します。通信が中断した場合に、プライマリボリュームの所有コントローラがセカンダリボリュームとの間でデータを再同期する優先度を設定できます。また、再同期ポリシーとして、手動または自動のどちらかを選択する必要があります。

.手順
. スライダバーを使用して同期優先度を設定します。
+
同期優先度は、I/O要求の処理と比較して、初期同期および通信中断後の再同期処理を完了するためにどの程度のシステムリソースが使用されるかを決定するものです。

+
このダイアログで設定した優先度は、プライマリボリュームとセカンダリボリュームの両方に適用されます。プライマリボリュームの速度は、あとからSystem Managerでメニューを選択して変更できます。Storage [Synchronous Mirroring > More > Edit Settings]を選択します。

+
同期優先度は5段階で設定できます。

+
** 最低

** 低
** 中
** 高
** 最高
+
同期優先度を最低に設定すると、I/Oアクティビティが優先され、再同期処理にかかる時間が長くなります。同期優先度が最高に設定されている場合は再同期処理が優先されますが、ストレージアレイのI/Oアクティビティに影響する可能性があります。

. リモートストレージアレイのミラーペアの再同期を手動で行うか自動で行うかを選択します。
+
** *手動*（推奨オプション）-
ミラーペアとの通信が回復したあとに同期を手動で再開する場合に選択します。このオプションは、データをリカバリするための最良の機会を提供します。
** *自動*--ミラーペアとの通信が回復した後、再同期を自動的に開始する場合に選択します。
+
同期を手動で再開するには、System Managerでメニューから「Storage [Synchronous Mirroring]（ストレージ同期ミラーリング）を選択し、テーブルでミラーペアを強調表示して、「* More *」（詳細*）で「Resume *」（続行）を選択します。

. 完了*をクリックして、同期ミラーリングを完了します。

.結果
ミラーリングがアクティブ化されると、システムは次の処理を実行します。

* ローカルストレージアレイとリモートストレージアレイの間の初期同期を開始します。
* 同期優先度と再同期ポリシーを設定します。
* コントローラのHICで最も大きい番号のポートをデータ送信のミラーリング用に予約します。
+
このポートで受信したI/O要求は、ミラーペアに含まれるセカンダリボリュームのリモートの優先コントローラ所有者からのみ承認されます。（プライマリボリュームでの予約が許可されます）。

* コントローラごとに1つずつ、リザーブ容量用ボリュームを
2つ作成します。これは、コントローラのリセットおよびその他の一時的な中断からリカバリするための書き込み情報のロギングに使用されます。
+
各ボリュームの容量は128MiBです。ただし、ボリュームがプールに配置されている場合は、ボリュームごとに4GiBが予約されます。

.終了後

System Managerに移動して、メニューHome（View Operations in Progress）を選択し、同期ミラーリング処理の進捗状況を表示します。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。

:leveloffset: -1

= FAQ

:leveloffset: +1

[[ID7a1bfd48e6c5cd10360a88ed2b1f8f52]]
= ミラー整合性グループを作成するときは、どのような点に注意する必要がありますか？
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ミラー整合性グループを作成する際は、次のガイドラインに従ってください。

Unified Managerに関する次の要件を満たしている必要があります。

* Web Services Proxyサービスが実行されている必要があります。
* Unified ManagerがHTTPS接続経由でローカルホストで実行されている必要があります。
* Unified Managerにストレージアレイの有効なSSL
証明書が表示されている必要があります。Unified Managerのメニューから「Certificate Management」に移動し、自己署名証明書を受け入れるか、独自のセキュリティ証明書をインストールできます。

また、ストレージアレイに関する次の要件も満たしている必要があります。

* Unified Managerで2つのストレージアレイが検出されている必要があります。
* 各ストレージアレイに2台のコントローラが必要です。
*
プライマリアレイとセカンダリアレイの両方の各コントローラにイーサネット管理ポートが設定され、ネットワークに接続されている必要があります。
* ストレージアレイに必要なファームウェアの最小バージョンは7.84です（それぞれ異なるOSバージョンを実行できます）。
* ローカルとリモートのストレージアレイのパスワードを確認しておく必要があります。
* ローカルとリモートのストレージアレイをFibre Channelファブリックまたは

iSCSIインターフェイスを介して接続します。

[NOTE]
====
同期ミラーリングは、EF600またはEF300ストレージシステムでは使用できません。

====

[[ID687588a2f2ca0d8a597af23f26ab43db]]
= ミラーペアを作成するときは、どのような点に注意する必要がありますか？
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ミラーペアを作成する前に、次のガイドラインに従ってください。

* 2つのストレージアレイが必要です。
* 各ストレージアレイに2台のコントローラが必要です。
* Unified Managerで2つのストレージアレイが検出されている必要があります。
*
プライマリアレイとセカンダリアレイの両方の各コントローラにイーサネット管理ポートが設定され、ネットワークに接続されている必要があります。
* ストレージアレイに必要なファームウェアの最小バージョンは7.84です（それぞれ異なるOSバージョンを実行できます）。
* ローカルとリモートのストレージアレイのパスワードを確認しておく必要があります。
*
ミラーリングするプライマリボリューム以上のセカンダリボリュームを作成するには、リモートストレージアレイに十分な空き容量が必要です。
* 非同期ミラーリングはFibre Channel（FC）またはiSCSIホストポートを搭載したコントローラでサポートされますが、同期ミラーリングはFCホストポートを搭載したコントローラでのみサポートされます。

[NOTE]
====
同期ミラーリングは、EF600またはEF300ストレージシステムでは使用できません。

====

[[ID5e9f58868117fdc0ef115fce3373ebf1]]
= この割合を変更するのはなぜですか？
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
非同期ミラーリング処理用のリザーブ容量は、通常はベースボリュームの20%です。通常はこの容量で十分です。

必要な容量は、ベースボリュームに対するI/O書き込みの頻度とサイズ、およびストレージオブジェクトのコピーサービス処理を使用する期間によって異なります。一般に、次のいずれかまたは両方に該当する場合は、リザーブ容量の割合を大きくします。

* 特定のストレージオブジェクトのコピーサービス処理の期間が非常に長い場合。
* 大量の
I/Oアクティビティにより、ベースボリュームのデータブロックの大部分で変更が発生する場合。ベースボリュームに対する一般的なI/Oアクティビティを判断するには、過去のパフォーマンスデータやその他のオペレーティングシステムユーティリティを使用します。

[[IDbacb5d2b12dcccef833506702e37012b]]
= リザーブ容量の候補が複数表示されるのはなぜですか？
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
プールまたはボリュームグループ内にストレージオブジェクトに対して選択した容量の割合を満たすボリュームが複数ある場合は、複数の候補が表示されます。

ベースボリューム上でコピーサービス処理用にリザーブする物理ドライブスペースの割合を変更すると、推奨される候補のリストを更新できます。選択に基づいて最適な候補が表示されます。

[[IDe35ac4de892d3511be68b24dfaddbc5b]]
= ボリュームが一部表示されないのはなぜですか？
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/

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

[role="lead"]
ミラーペアのプライマリボリュームを選択すると、対応するすべてのボリュームのリストが表示されます。

使用できないボリュームはリストに表示されません。次のいずれかの理由で、ボリュームが対象外になっている可能性があります。

* 最適状態でない。
* すでにミラー関係に参加している。
*
同期ミラーリングの場合、ミラーペアのプライマリボリュームとセカンダリボリュームは標準ボリュームである必要があります。シンボリュームやSnapshotボリュームは使用できません。
* 非同期ミラーリングの場合、シンボリュームで自動拡張が有効になっている必要があります。

NOTE: EF600および
EF300コントローラでは、非同期ミラーペアのプライマリボリュームとセカンダリボリュームのプロトコル、トレイレベル、セグメントサイズ、セキュリティタイプ、およびRAIDレベルが同じである必要があります。対応していない非同期ミラーペアは、使用可能なボリュームのリストに表示されません。

[[IDb9f6c295a2b86f467ce0b3bde2e716a4]]
= リモートストレージアレイのボリュームが一部表示されないのはなぜですか？
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
リモートストレージアレイ上のセカンダリボリュームを選択すると、そのミラーペアに対応するすべてのボリュームのリストが表示されます。

使用できないボリュームはリストに表示されません。次のいずれかの理由でボリュームを使用できない可能性があります。

* 標準以外のボリューム（Snapshotボリュームなど）である。
* 最適状態でない。
* すでにミラー関係に参加している。
*
非同期ミラーリングの場合、シンボリューム属性がプライマリボリュームとセカンダリボリュームで一致しません。

* Data Assurance（DA）を使用する場合、プライマリボリュームとセカンダリボリュームでDA設定を同じにする必要があります。
+
** プライマリボリュームでDAを有効にする場合、セカンダリボリュームでもDAを有効にする必要があります。
** プライマリボリュームでDAを有効にしない場合、セカンダリボリュームでもDAを無効にする必要があります。

*
非同期ミラーリングの場合、プライマリボリュームとセカンダリボリュームのドライブセキュリティ機能が同じである必要があります。
+
** プライマリボリュームがFIPSに対応している場合、セカンダリボリュームはFIPSに対応している必要があります。
** プライマリボリュームがFDEに対応している場合、セカンダリボリュームはFDEに対応している必要があります。
**
プライマリボリュームでドライブセキュリティを使用していない場合、セカンダリボリュームでドライブセキュリティを使用していない必要があります。

[[IDa07e3666b91c442c4b67556b1689d529]]
= 同期優先度は同期速度にどのような影響を与えますか？
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
同期優先度は、システムパフォーマンスに対する同期アクティビティに割り当てる処理時間を定義します。

プライマリボリュームのコントローラ所有者はこの処理をバックグラウンドで実行します。同時にコントローラ所有者は、プライマリボリュームへのローカルのI/O書き込みと、対応するセカンダリボリュームへのリモートの書き込みを処理します。再同期には、I/Oアクティビティに使用されるはずのコントローラの処理リソースが使用されるため、再同期がホストアプリケーションのパフォーマンスに影響する可能性があります。

同期優先度に応じた所要時間や、同期優先度がシステムパフォーマンスに与える影響を特定する際には、次のガイドラインに注意してください。

次のプライオリティレートを使用できます。

* 最低
* 低
* 中
* 高
* 最高

優先度が最低の場合はシステムパフォーマンスがサポートされますが、再同期にかかる時間は長くなります。最も優先度が高い場合は再同期がサポートされますが、システムパフォーマンスが低下する可能性があります。

これらのガイドラインは、優先度の大まかな違いを示しています。

```
[cols="45h,~"]
|===
| 完全同期の優先度 | 最高の同期速度と比較した経過時間


 a|
最低
 a|
最高プライオリティレートの約8倍の長さになります。



 a|
低
 a|
最高プライオリティレートの約6倍の長さになります。



 a|
中
 a|
最高プライオリティレートの約3.5倍の長さになります。



 a|
高
 a|
最高プライオリティレートの約2倍の時間がかかります。

|===
```

同期の所要時間には、ボリュームサイズとホストのI/O速度が影響します。

[[ID13dd9eaf9744477367df9821945bdcde]]
= 手動同期ポリシーの使用が推奨されるのはなぜですか。
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
手動再同期が推奨されるのは、データがリカバリされる可能性が最も高い方法で再同期プロセスを管理できるためです。

自動再同期ポリシーを使用していて、再同期中に通信が中断する問題が発生した場合は、セカンダリボリューム上のデータが一時的に破損する可能性があります。再同期が完了すると、データは修正されます。

:leveloffset: -1

:leveloffset: -1

= 証明書

:leveloffset: +1

[[IDe29cbc73b9e466f44f98e4736bf805e2]]
= 証明書の概要
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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

_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し、インターネット上のセキュアな通信を実現するデジタルファイルです。証明書には2種類あります。A_Signed certificate_is validated by a Certificate Authority（CA；認証局）とa_self-signed certificate_is validated by the entity of the entity instead of a third party。

詳細：

* xref:{relative_path}how-certificates-work-unified.html["証明書の仕組み"]
* xref:{relative_path}certificate-terminology-unified.html["証明書の用語"]

== 証明書を設定する方法を教えてください。

[証明書管理]では、Unified Managerをホストする管理ステーションの証明書を設定できます。また、アレイのコントローラの証明書をインポートすることもできます。

詳細：

* xref:{relative_path}use-ca-signed-certificate-um.html["管理システム用のCA署名証明書の使用"]
* xref:{relative_path}import-array-certificates-unified.html["アレイの証明書のインポート"]

= 概念

:leveloffset: +1

[[ID28dc866e9f79dc56fa8eccaf910d9be5]]
= 証明書の仕組み
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

== 署名済み証明書

証明書を使用すると、Web通信が、指定されたサーバとクライアントの間でのみ、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が保証されます。Unified Manager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、誰かが所有者のIDを検証し、自分のデバイスが信頼できると判断したことを意味します。ストレージアレイには、自動生成された自己署名証明書が各コントローラに付属しています。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の間のよりセキュアな接続を確立することもできます。

[NOTE]
====
CA署名証明書はセキュリティ保護に優れていますが（中間者攻撃を防止するなど）、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、自己署名証明書は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（通常はサーバまたはWebサイト）の所有者に関する詳細、証明書の発行日と有効期限、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ます。

ブラウザを開いてWebアドレスを入力すると、証明書の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、南京錠のアイコンとhttpsの指定が含まれます。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、申請プロセス中にユーザー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、CAからホスト管理システムにロードするデジタルファイルが送信されます。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、必要なルート証明書は1つだけです。
* *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されて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「信頼されている」ものではありません。自己署名証明書のみが含まれている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。

== Unified Managerの証明書

Unified Managerインターフェイスは、ホストシステムにWeb Services Proxyとともにインストールされます。ブラウザを開いてUnified Managerに接続しようとすると、ホストが信頼できるソースであるかどうかを確認するためにデジタル証明書がチェックされます。ブラウザでサーバの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。または、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。

== コントローラの証明書

Unified Manager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、Web Services Proxyサーバ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。

[[ID3270e5aa501d1f4b528b472e8ebc5a7b]]

```
= 証明書の用語
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
証明書管理に関連する用語を次に示します。

[cols="25h,~"]
|===
| 期間 | 製品説明


 a|
カリフォルニア州
 a|
認証局（CA）は、インターネットセキュリティのためにデジタル証明書と呼ばれる電子ドキュメントを発行する信頼されたエンティティです。証明書でWebサイトの所有者を識別することにより、クライアントとサーバの間のセキュアな接続が確立されます。



 a|
CSR
 a|
証明書署名要求（CSR）は、申請者から認証局（CA）に送信されるメッセージです。CSRは、CAが証明書を発行するために必要な情報を検証します。



 a|
証明書
 a|
証明書はセキュリティ上の目的でサイトの所有者を識別するもので、攻撃者による偽装を防止します。証明書には、サイトの所有者に関する情報と、この情報を証明（署名）する信頼されたエンティティのIDが含まれています。



 a|
証明書チェーン
 a|
証明書にセキュリティレイヤを追加するファイルの階層。通常、チェーンには階層の最上位にある1つのルート証明書、1つ以上の中間証明書、およびエンティティを識別するサーバ証明書が含まれます。
```

a|
中間証明書
a|
証明書チェーンのルートから1つ以上の中間証明書が分岐します。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。

a|
キーストア
a|
キーストアはホスト管理システム上のリポジトリであり、秘密鍵とそれに対応する公開鍵および証明書が格納されています。これらのキーと証明書によって、コントローラなどの独自のエンティティが識別されます。

a|
ルート証明書
a|
ルート証明書は、証明書チェーンの階層の最上位にあります。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、必要なルート証明書は1つだけです。

a|
署名済み証明書
a|
認証局（CA）によって検証される証明書。このデータファイルには秘密鍵が含まれており、HTTPS接続を介してサーバとクライアントの間でデータが暗号化された形式で送信されるようにします。また、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。署名済み証明書は信頼チェーンを使用するため、本番環境で最もよく使用されます。「CA署名証明書」または「管理証明書」とも呼ばれます。

a|
自己署名証明書
a|
自己署名証明書は、エンティティの所有者によって検証されます。このデータファイルには秘密鍵が含まれており、HTTPS接続を介してサーバとクライアントの間でデータが暗号化された形式で送信されるようにします。また、文字と数字で構成されるデジタル署名も含まれています。自己署名証明書はCA署名証明書と同じ信頼チェーンを使用しないため、テスト環境で最もよく使用されます

。「事前にインストールされている」証明書とも呼ばれます。

a|
サーバ証明書
a|
サーバ証明書は、証明書チェーンの最下位にあります。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します。ストレージシステムの各コントローラには、個別のサーバ証明書が必要です。

a|
信頼ストア
a|
信頼ストアは、CAなどの信頼できるサードパーティの証明書を格納するリポジトリです。

|===

:leveloffset: -1

[[ID99583ab724c14dc43db7714457d7c99e]]
= 管理システム用のCA署名証明書の使用
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Unified Managerをホストす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。

.開始する前に
Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書機能は表示されません。

.タスクの内容
CA署名証明書の使用は、3つの手順で構成されます。

== 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）ファイルを生成して、組織とWeb Services ProxyとUnified Managerがインストールされているホストシステムを特定する必要があります。

[NOTE]
====
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
. [証明書管理]を選択します。
. [管理]タブで、[* CSR全体*]を選択します。
. 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.などのサフィックスを含めます。
** *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）。

. Web Services Proxyがインストール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*-- Webサービスプロキシがインストール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Unified Managerにアクセスする際に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://.は含めないでください。DNS名の1文字目をワイルドカードに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1文字目をワイルドカードにすることはできません。

. ホスト情報が正しいことを確認します。そうでない場合、CAから返された証明書はインポートしようとしたときに失敗します。
. [完了] をクリックします。
. にアクセスします。

== 手順2：CSRファイルを送信する

証明書署名要求（CSR）ファイルを作成したら、そのファイルを認証局（CA）に送信して、Unified ManagerとWeb Services
Proxyをホストするシステムの署名済み管理証明書を受け取ります。

NOTE: 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
. ダウンロードしたCSRファイルの場所を確認します。
+
ダウンロードのフォルダの場所は、ブラウザによって異なります。

. 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。
+
[CAUTION]
====
* CSRファイルをCAに送信した後は、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、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。

====
. CAから署名済み証明書が返されたら、に進みます<<手順3：管理証明書をインポートする>>。

== 手順3：管理証明書をインポートする

認証局（CA）から署名済み証明書を受け取ったら、Web Services ProxyとUnified
Managerインターフェイス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。

.開始する前に
* CAから署名済み証明書を受け取っておきます。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（
.p7bファイルなど）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ユーティリティを使用してファイルを展開でき `certmgr`ます

(右クリックしてメニューを選択します:すべてのタスク[エクスポート])。Base-64エンコードを推奨します。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。
* Web Services Proxyを実行しているホストシステムに証明書ファイルをコピーしておきます。

.手順
. [証明書管理]を選択します。
. [管理（Management）]タブで、[*インポート（* Import）]を選択する
+
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開きます。

.
[*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。

. [* 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。証明書の情報が[証明書管理]ページに表示されます。

[[IDbe7f3d496c294050813ba8eee3a051eb]]
= 管理証明書のリセット
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

.開始する前に
Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書機能は表示されません。

.タスクの内容
このタスクでは、Web Services ProxyとUnified

Managerがインストールされ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使用されるようになります。

.手順
. [設定]>[証明書]*を選択します。
. [アレイ管理]*タブを選択し、*[リセット]*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。

. フィールドにと入力し `reset`、*[リセット]*をクリックします。
+
ブラウザの更新後、ブラウザによって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、そのサイトがHTTP Strict Transport Securityを使用していると報告されることがあります。この状態は、自己署名証明書に切り替えたときに発生します。宛先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、ブラウザから閲覧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。その結果、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るプロンプトが表示されます。

= アレイ証明書を使用する

```
:leveloffset: +1
```

```
[[ID90666f44e3f607b214642991502447c4]]
```
= アレイの証明書のインポート
```
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```
必要に応じて、Unified Managerをホストするシステムで認証できるように、ストレージアレイの証明書をインポートできます。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。

.開始する前に
* Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書機

能は表示されません。
* 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
. [証明書管理]を選択します。
. [*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。

. 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。
+
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。

. 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。

[[IDc14d26ffe172f0d915dbd6779354ede0]]
= 信頼できる証明書の削除
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

.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。

[CAUTION]
====
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を共有す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ることに注意してください。

====
.手順

. [証明書管理]を選択します。
. [*Trusted*]タブを選択します。
. 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。
+
[NOTE]
====
* Delete *機能は、プリ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。

. 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。

[[ID117723ccbfa1572e010cf99339779133]]
= 信頼されない証明書の解決
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
信頼されていない証明書は、ストレージアレイからUnified Manager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を確認できない場合に発生します。

[証明書]ページで信頼されていない証明書を解決するには、ストレージアレイの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が発行した認証局（CA）証明書をインポートします。

.開始する前に
* Security Adminの権限を含むユーザプロファイルでログインする必要があります。
* CA署名証明書をインポートする場合は、次の手順を実行します。
+
** 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にあることを確認します。

.タスクの内容
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最近追加した。
* 一方または両方の証明書の期限が切れている。
* 一方または両方の証明書が失効している。
* 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
. [証明書管理]を選択します。
. [*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。

. 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。
+
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。

. 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。

:leveloffset: -1

= 証明書の管理

:leveloffset: +1

[[ID0fdd731be7081d42c47858621bdddf69]]
= 証明書の表示
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
証明書の概要情報を表示できます。これには、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）が含まれます。

.開始する前に
Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書機能は表示されません。

.手順
. [証明書管理]を選択します。
. 次のいずれかのタブを選択します。
+
** *管理*--
Webサービスプロキシをホストす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。この証明書によって、Unified Managerへのセキュアなアクセスが許可されます
** * Trusted *-- Unified Managerがストレージアレイや
LDAPサーバなどのその他のリモートサーバ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。

. 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。

[[ID7dbb82f215de9b3802dbc5eba3836c5b]]
= 証明書のエクスポート
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

.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
. [証明書管理]を選択します。
. 次のいずれかのタブを選択します。

+
** *管理*--
Webサービスプロキシをホストす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。この証明書によって、Unified Managerへのセキュアなアクセスが許可されます
** * Trusted *-- Unified Managerがストレージアレイや
LDAPサーバなどのその他のリモートサーバ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。

. 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。
. [* Export*]をクリックし、証明書ファイルを保存します。
. 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。

:leveloffset: -1

:leveloffset: -1

= アクセス管理

:leveloffset: +1

[[ID46f4c3f8232650bcf75967b7ba0cde67]]
= アクセス管理の概要
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセス管理は、Unified Managerでユーザ認証を設定する方法の1つです。

== どのような認証方式を使用できますか。

次の認証方式を使用できます。

* *ローカルユーザーの役割*--
RBAC（役割ベースのアクセス制御）機能を使用して認証を管理しますローカルユーザロールには、

事前定義されたユーザプロファイルと、特定のアクセス権限を持つロールが含まれます。
* *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)を介して認証を管理します
* *saml *-- SAML 2.0を使用して、アイデンティティプロバイダ（IdP）を介して認証を管理します。

詳細：

* xref:{relative_path}how-access-management-works-unified.html["アクセス管理の仕組み"]
* xref:{relative_path}access-management-terminology-unified.html["アクセス管理の用語"]
* xref:{relative_path}permissions-for-mapped-roles-unified.html["マッピングされたロールの権限"]
* xref:{relative_path}access-management-with-saml.html["SAML"]

== アクセス管理を設定するにはどうすればよいですか？

SANtricityソフトウェアは、ローカルユーザロールを使用するように事前に設定されています。LDAPを使用する場合は、[アクセス管理]ページで設定できます。

詳細：

* xref:{relative_path}access-management-with-local-user-roles-unified.html["ローカルユーザロールを使用したアクセス管理"]
* xref:{relative_path}access-management-with-directory-services-unified.html["ディレクトリサービスを使用したアクセス管理"]
* xref:{relative_path}configure-saml.html["SAMLの設定"]

= 概念

:leveloffset: +1

[[IDcbda7abe8496c1ca55b8217c142bff92]]
= アクセス管理の仕組み
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/

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


[role="lead"]
アクセス管理を使用してUnified Managerでユーザ認証を確立します。



== 設定ワークフロー

アクセス管理の設定は次のように機能します。

. Security Adminの権限を含むユーザプロファイルでUnified Managerにログインします。
+
[NOTE]
====
初回ログイン時は、ユーザ名が `admin`自動的に表示され、変更することはできません。
`admin`ユーザには、システム内のすべての機能へのフルアクセス権が付与されます。初回ログイン時にパスワードを設定する必要があります。

====
.
ユーザインターフェイスでアクセス管理に移動します。事前に設定されているローカルユーザロールが表示されます。これらのロールは、RBAC（ロールベースアクセス制御）機能の実装です。
. 管理者は、次の認証方式を1つ以上設定します。
+
** *ローカルユーザーの役割*--
RBAC機能を使用して認証を管理しますローカルユーザロールには、事前定義されたユーザと、特定のアクセス権限を持つロールが含まれます。管理者は、これらのローカルユーザロールを単一の認証方式として使用することも、ディレクトリサービスと組み合わせて使用することもできます。ユーザのパスワードを設定する以外、設定は必要ありません。
** *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)を介して認証を管理します管理者がLDAPサーバに接続し、LDAPユーザをローカルユーザロールにマッピングします。
** *saml *-- Security Assertion Markup Language（SAML）2.0を使用してアイデンティティプロバイダ（IdP）を介して認証を管理します。管理者がIdPシステムとストレージアレイの間の通信を確立し、ストレージアレイに組み込まれているローカルユーザロールにIdPユーザをマッピングします。



. Unified Managerのログインクレデンシャルをユーザに割り当てます。
.
ユーザが自身のクレデンシャルを入力してシステムにログインします。ログイン中、システムは次のバックグラウンドタスクを実行します。
+
** ユーザアカウントに対してユーザ名とパスワードを認証します。
```

** 割り当てられたロールに基づいてユーザの権限を決定します。
** ユーザインターフェイスの機能にユーザがアクセスできるようにします。
** 上部のバナーにユーザ名が表示されます。

== Unified Managerで使用できる機能

機能にアクセスできるかどうかは、ユーザに割り当てられたロールによって異なります。ロールには次のようなものがあります。

* * Storage admin *--アレイ上のストレージ・オブジェクトへの読み取り/書き込みのフル・アクセスを提供しますが'セキュリティ構成へのアクセスはありません
* * Security admin *--アクセス管理と証明書管理のセキュリティ設定へのアクセス。
* * Support admin *--ストレージアレイ上のすべてのハードウェアリソース、障害データ、およびMELイベントへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
* *Monitor *--すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

使用できない機能は淡色表示されるか、ユーザインターフェイスに表示されません。

[[IDef8b908c7a6ff4692fe527b9fbc719f8]]
= アクセス管理の用語
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Unified Managerに関連するアクセス管理の用語を次に示します。

[cols="25h,~"]
|===
| 期間 | 製品説明

a|
Active Directory

a|
Active Directory（AD）は、Windowsドメインネットワーク用にLDAPを使用するMicrosoftのディレクトリサービスです。

a|
バインド
a|
バインド操作は、ディレクトリサーバに対してクライアントを認証するために使用されます。通常はアカウントとパスワードのクレデンシャルが必要ですが、匿名のバインド処理が可能なサーバもあります。

a|
カリフォルニア州
a|
認証局（CA）は、インターネットセキュリティのためにデジタル証明書と呼ばれる電子ドキュメントを発行する信頼されたエンティティです。証明書でWebサイトの所有者を識別することにより、クライアントとサーバの間のセキュアな接続が確立されます。

a|
証明書
a|
証明書はセキュリティ上の目的でサイトの所有者を識別するもので、攻撃者による偽装を防止します。証明書には、サイトの所有者に関する情報と、この情報を証明（署名）する信頼されたエンティティのIDが含まれています。

a|
LDAP
a|
Lightweight Directory Access Protocol（LDAP）は、分散されたディレクトリ情報サービスにアクセスして管理するためのアプリケーションプロトコルです。このプロトコルを使用すると、さまざまなアプリケーションやサービスをLDAPサーバに接続してユーザを検証できます。

a|
RBAC
a|
ロールベースアクセス制御（RBAC）は、個 々

のユーザのロールに基づいてコンピュータリソースまたはネットワークリソースへのアクセスを制御する方法です。Unified Managerには事前定義されたロールがあります

 a|
SAML
 a|
Security Assertion Markup Language（SAML）は、
2つのエンティティ間の認証と許可に使用されるXMLベースの標準規格です。SAMLでは多要素認証が可能で、ユーザはIDを証明するために2つ以上の項目（パスワードやフィンガープリントなど）を指定する必要があります。ストレージアレイに組み込まれているSAML機能は、アイデンティティのアサーション、認証、および許可に関してSAML2.0に準拠しています。

 a|
SSO
 a|
シングルサインオン（SSO）は、1組のログインクレデンシャルで複数のアプリケーションにアクセスできるようにする認証サービスです。

 a|
Web Services Proxy
 a|
Web Services Proxyは標準の
HTTPSメカニズムを介したアクセスを提供し、管理者がストレージアレイの管理サービスを設定できるようにします。このプロキシは、WindowsホストまたはLinuxホストにインストールできます。Unified Managerインターフェイスは Web Services Proxyで使用できます。

|===

[[ID102c42f1301a0fc7a001a0020f69878a]]
= マッピングされたロールの権限
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ロールベースアクセス制御（RBAC）機能には、1つ以上のロールがマッピングされた事前定義されたユーザが含まれます。各ロールには、Unified

Managerのタスクにアクセスするための権限が含まれています。

各ロールは、次のタスクへのアクセスをユーザに提供します。

* * Storage admin *--アレイ上のストレージ・オブジェクトへの読み取り
/書き込みのフル・アクセスを提供しますが'セキュリティ構成へのアクセスはありません
* * Security admin *--アクセス管理と証明書管理のセキュリティ設定へのアクセス。
* * Support admin *--
ストレージアレイ上のすべてのハードウェアリソース、障害データ、およびMELイベントへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
* *Monitor *--
すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

ユーザに特定の機能に対する権限がない場合、その機能は選択できないか、ユーザインターフェイスに表示されません。

[[ID39f8a00218d9f8f6b80d44539ee903a6]]
= ローカルユーザロールを使用したアクセス管理
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
管理者は、Unified Managerで適用されるロールベースアクセス制御（
RBAC）機能を使用できます。これらの機能は、「ローカルユーザロール」と呼ばれます。

== 設定ワークフロー

ローカルユーザロールはシステムで事前に設定されています。認証にローカルユーザロールを使用するには、管理者は次の操作を実行します。

. Security Adminの権限を含むユーザプロファイルでUnified Managerにログインします。
+
[NOTE]
====
 `admin`ユーザには、システム内のすべての機能へのフルアクセス権が付与されます。

====
.

管理者がユーザプロファイルを確認します。ユーザプロファイルは事前に定義されており、変更できません。
. 必要に応じて、管理者は各ユーザプロファイルに新しいパスワードを割り当てます。
. ユーザは各自に割り当てられたクレデンシャルでシステムにログインします。

== 管理

認証にローカルユーザロールのみを使用する場合、管理者は次の管理タスクを実行できます。

* パスワードを変更します。
* パスワードの最小文字数を設定する。
* ユーザがパスワードなしでログインできるようにします。

[[ID47461a1a3c5b5b30ca32c7606eff5fbc]]
= ディレクトリサービスを使用したアクセス管理
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
管理者は、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）を使用できます。

== 設定ワークフロー

ネットワークでLDAPサーバとディレクトリサービスが使用されている場合、設定は次のように機能します。

. Security Adminの権限を含むユーザプロファイルでUnified Managerにログインします。
+
[NOTE]
====
 `admin`ユーザには、システム内のすべての機能へのフルアクセス権が付与されます。

====
. LDAPサーバの設定を入力します。設定には、ドメイン名、

URL、バインドアカウント情報が含まれます。
. LDAPサーバでセキュアなプロトコル（LDAPS）を使用している場合は、LDAPサーバとWeb Services Proxyがインストールされているホストシステムの間の認証に使用する認証局（CA）証明書チェーンをアップロードします。
.
サーバ接続が確立されると、管理者はユーザグループをローカルユーザロールにマッピングします。これらのロールは事前定義されており、変更することはできません。
. LDAPサーバとWeb Services Proxyの間の接続をテストします。
. ユーザは、自分に割り当てられたLDAP/ディレクトリサービスのクレデンシャルを使用してシステムにログインします。

== 管理

認証にディレクトリサービスを使用する場合、管理者は次の管理タスクを実行できます。

* ディレクトリサーバを追加します。
* ディレクトリサーバの設定を編集します。
* LDAPユーザをローカルユーザロールにマッピングします。
* ディレクトリサーバを削除します。
* パスワードを変更します。
* パスワードの最小文字数を設定する。
* ユーザがパスワードなしでログインできるようにします。

[[ID3a69d138577698d76e34434d82eda6e3]]
= SAMLを使用したアクセス管理
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
管理者は、アレイに組み込みのSecurity Assertion Markup Language（SAML）2.0の機能をアクセス管理に使用できます。

== 設定ワークフロー

SAMLの設定は次のように機能します。

. Security Adminの権限を含むユーザプロファイルでUnified Managerにログインします。
+
[NOTE]
====
この `admin`ユーザには、System
Managerのすべての機能に対するフルアクセスが付与されます。

====
. 管理者は、[アクセス管理]の下の[*SAML *]タブに移動します。
. アイデンティティプロバイダ（IdP）との通信を設定します。
IdPは、ユーザにクレデンシャルを要求して認証されたユーザかどうかを確認するための外部システムです。ストレージアレイとの通信を設定するには、IdPシステムからIdPメタデータファイルをダウンロードし、Unified
Managerを使用してそのファイルをストレージアレイにアップロードします。
. サービスプロバイダと
IdPの間に信頼関係を確立します。サービスプロバイダはユーザ権限を制御します。このケースでは、ストレージアレイ内のコントローラがサービスプロバイダの役割を果たします。通信を設定するために、管理者はUnified
Managerを使用してコントローラのサービスプロバイダメタデータファイルをエクスポートします。次に、IdPシステムからメタデータファイルをIdPにインポートします。
+
[NOTE]
====
また、認証時に名前IDを返す機能がIdPでサポートされていることを確認しておく必要があります。

====
. ストレージアレイのロールを
IdPで定義されているユーザ属性にマッピングします。そのためには、管理者はUnified
Managerを使用してマッピングを作成します。
. IdP URLへのSSOログインをテストします。このテストでは、ストレージアレイと
IdPが通信できることを確認します。
+
[CAUTION]
====
SAMLを有効にすると、ユーザインターフェイスで無効にしたり、IdP設定を編集したりすることはできなくなります。SAMLの設定を無効にしたり編集したりする必要がある場合は、テクニカルサポートにお問い合わせください。

====
. Unified Managerで、ストレージアレイのSAMLを有効にします。
. ユーザが自身のSSOクレデンシャルを使用してシステムにログインします。

== 管理

認証にSAMLを使用している場合、管理者は次の管理タスクを実行できます。

* 新しいロールマッピングを変更または作成する
* サービスプロバイダファイルのエクスポート

== アクセス制限

SAMLが有効な場合、ユーザは従来のStorage Managerインターフェイスからそのアレイのストレージを検出または管理できません。

また、次のクライアントはストレージアレイのサービスとリソースにアクセスできません。

* Enterprise Management Window（EMW）
* コマンドラインインターフェイス（CLI）
* ソフトウェア開発キット（SDK）クライアント
* インバンドクライアント
* HTTPベーシック認証REST APIクライアント
* 標準のREST APIエンドポイントを使用したログイン

:leveloffset: -1

= ローカルユーザロールを使用する

:leveloffset: +1

[[IDaba8ea594b7aaa19d6dba13bd01e3d63]]
= ローカルユーザロールの表示
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
[ローカルユーザーの役割]タブでは、ユーザーとデフォルトの役割とのマッピングを表示できます。これらのマッピングは、Unified Managerの Webサービスプロキシで適用されるロールベースアクセス制御（RBAC）の一部です。

.開始する前に
Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。

.タスクの内容
ユーザとマッピングは変更できません。変更できるのはパスワードのみです。

.手順
. アクセス管理*を選択します。
. [ローカルユーザー役割*（Local User Roles *）]タブを選択します。
+
表にユーザが表示されます。

+
** *admin*--
システム内のすべての機能にアクセスできるスーパー管理者。このユーザにはすべてのロールが含まれます。
** * storage *--
すべてのストレージ・プロビジョニングを担当する管理者。このユーザには、Storage Admin、Support Admin、Monitorのロールが含まれています。
** * security *--
アクセス管理や証明書管理など、セキュリティ設定を担当するユーザー。このユーザには、Security AdminとMonitorのロールが含まれています。
** * support *--
ハードウェアリソース、障害データ、ファームウェアアップグレードを担当するユーザー。このユーザには、Support AdminとMonitorのロールが含まれています。
** *monitor *--
システムへの読み取り専用アクセス権を持つユーザー。このユーザにはMonitorロールのみが含まれています。
** * rw *（読み取り/書き込み）-このユーザには、Storage Admin、Support Admin、Monitorのロールが含まれています。
** * ro *（読み取り専用）--このユーザーには、Monitorロールのみが含まれています。

[[IDdb7e0c5300b1947829c549e1cc159465]]
= ローカルユーザプロファイルのパスワードの変更
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセス管理で各ユーザのユーザパスワードを変更できます。

.開始する前に
* Root Adminの権限が割り当てられたローカル管理者としてログインする必要があります。
* ローカル管理者のパスワードを確認しておく必要があります。

.タスクの内容
パスワードを選択する際は、次のガイドラインに注意してください。

* 新しいローカルユーザパスワードは、最小パスワードの現在の設定（[設定の表示/編集]）以上にする必要があります。
* パスワードは大文字と小文字が区別されます。
*
パスワードの末尾のスペースは削除されません。パスワードにスペースが含まれている場合は、スペースを含めるように注意してください。
* セキュリティを強化するために、
15文字以上の英数字を使用し、パスワードを頻繁に変更してください。

.手順
. アクセス管理*を選択します。
. [ローカルユーザー役割*（Local User Roles *）]タブを選択します。
. 表からユーザを選択します。
+
[パスワードの変更]ボタンが使用可能になります。

. [パスワードの変更 *] を選択します。
+
[パスワードの変更]ダイアログボックスが開きます。

.
ローカルユーザパスワードの最小文字数が設定されていない場合は、システムにアクセスする際にユーザにパスワードの入力を求めるチェックボックスを選択できます。
. 選択したユーザの新しいパスワードを2つのフィールドに入力します。
. この操作を確認するためにローカル管理者パスワードを入力し、*変更*をクリックします。

.結果
ユーザが現在ログインしている場合、パスワードを変更するとユーザのアクティブなセッションが終了します。

[[ID1efabd95bf91ec53cc8587946402cdc7]]
= ローカルユーザのパスワード設定の変更

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


[role="lead"]
```
すべての新規または更新されるローカルユーザパスワードに必要な最小文字数を設定できます。また、ローカルユーザがパスワードを入力せずにシステムにアクセスできるようにすることもできます。

.開始する前に
Root Adminの権限が割り当てられたローカル管理者としてログインする必要があります。

.タスクの内容
ローカルユーザパスワードの最小文字数を設定する際は、次のガイドラインに注意してください。

* 設定を変更しても、既存のローカルユーザパスワードには影響しません。
* ローカルユーザパスワードの最小文字数は0~30文字に設定する必要があります。
* 新しいローカルユーザパスワードは、現在の最小文字数の設定以上にする必要があります。
*
ローカルユーザがパスワードを入力せずにシステムにアクセスできるようにする場合は、パスワードの最小文字数を設定しないでください。

.手順
. アクセス管理*を選択します。
. [ローカルユーザー役割*（Local User Roles *）]タブを選択します。
. 「*表示/設定の編集*」を選択します。
+
[ローカルユーザーパスワードの設定]ダイアログボックスが開きます。

. 次のいずれかを実行します。
+
** ローカルユーザがパスワードを入力せずにsystem_に
アクセスできるようにするには、「すべてのローカルユーザパスワードを最低必要とする」チェックボックスをオフにします。
**
すべてのローカルユーザパスワードに対してパスワードの最小文字数を設定するには、[Require all local user passwords to be at least]チェックボックスをオンにし、スピンボックスですべてのローカルユーザパスワードの最小文字数を設定します。
+
新しいローカルユーザパスワードは現在の設定以上にする必要があります。

. [保存（ Save ）] をクリックします。

:leveloffset: -1

= ディレクトリサービスを使用する

:leveloffset: +1

[[ID7ba621ca443d028fbcb7d7d968347a18]]
= ディレクトリサーバの追加
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセス管理用の認証を設定するには、LDAPサーバとUnified Managerの
Webサービスプロキシを実行するホストの間の通信を確立します。次に、LDAPユーザグループをローカルユーザロールにマッピングします。

.開始する前に
* Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
* ユーザグループがディレクトリサービスに定義されている必要があります。
* LDAPサーバのクレデンシャルを確認しておく必要があります。ドメイン名とサーバの
URLのほか、必要に応じてバインドアカウントのユーザ名とパスワードも指定できます。
* セキュアなプロトコルを使用するLDAPSサーバの場合は、
LDAPサーバの証明書チェーンをローカルマシンにインストールする必要があります。

.タスクの内容
ディレクトリサーバの追加は、2つの手順で行います。最初にドメイン名とURLを入力します。サーバでセキュアなプロトコルを使用している場合は、認証用のCA証明書もアップロードする必要があります（標準の署名機関によって署名されている場合）。バインドアカウントのクレデンシャルがある場合は、ユーザアカウント名とパスワードも入力できます。次に、LDAPサーバのユーザグループをローカルユーザロールにマッピングします。

.手順
. アクセス管理*を選択します。
. [*ディレクトリサービス*]タブで、[*ディレクトリサーバーの追加*]を選択します。

+
[ディレクトリサーバーの追加]ダイアログボックスが開きます。

. [*サーバー設定*]タブで、LDAPサーバーの資格情報を入力します。
+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 製品説明

 a|
構成設定

 a|
ドメイン
 a|
LDAPサーバのドメイン名を入力します。ドメインを複数入力する場合は、カンマで区切って入力します。ドメイン名は、ログイン（_username_@_domain_）で、認証するディレクトリサーバを指定するために使用されます。

 a|
サーバURL
 a|
LDAPサーバにアクセスするためのURLをの形式で入力し `ldap[s]://*host*:*port*`ます。

 a|
証明書のアップロード（オプション）
 a|

NOTE: このフィールドは、上記の[Server URL]フィールドで
LDAPSプロトコルが指定されている場合にのみ表示されます。

[*Browse*]をクリックして、アップロードするCA証明書を選択します。これは、LDAPサーバの認証に使用される信頼された証明書または証明書チェーンです。

 a|

バインドアカウント（オプション）

a|
LDAPサーバに対する検索クエリおよびグループ内の検索に使用する読み取り専用ユーザアカウントを入力します。アカウント名はLDAPタイプの形式で入力します。たとえば、バインドユーザの名前が「bindacct」の場合は、などの値を入力します `CN=bindacct,CN=Users,DC=cpoc,DC=local`。

a|
バインドパスワード（オプション）

a|
NOTE: このフィールドは、バインドアカウントを入力すると表示されます。

バインドアカウントのパスワードを入力します。

a|
追加する前にサーバ接続をテストする

a|
入力したLDAPサーバの設定でシステムと通信できるかどうかを確認するには、このチェックボックスを選択します。このテストは、ダイアログボックスの下部にある*追加*（* Add *）をクリックした後に実行されます。

このチェックボックスを選択してテストに失敗した場合、設定は追加されません。設定を追加するには、エラーを解決するか、チェックボックスを選択解除してテストをスキップする必要があります。

a|
権限の設定

a|
検索ベースDN

a|
ユーザを検索するLDAPコンテキストを入力します。通常はの形式で入力します `CN=Users, DC=cpoc, DC=local`。

a|
ユーザ名属性

a|
認証用のユーザIDにバインドされた属性を入力します。例： `sAMAccountName`。

a|
グループ属性
a|
グループとロールのマッピングに使用される、ユーザの一連のグループ属性を入力します。例：
`memberOf, managedObjects`。

|===
====
. [*役割マッピング*（Role Mapping *）]タブをクリックします。
. 事前定義されたロールにLDAPグループを割り当てます。
1つのグループに複数のロールを割り当てることができます。
+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 製品説明

a|
マッピング

a|
グループDN
a|
マッピングするLDAPユーザグループの識別名（DN）を指定します。正規表現がサポートされています。正規表現パターンに含まれていない場合は、これらの特殊な正規表現文字をバックスラッシュ（\）でエスケープする必要があります。\.[]{}()<>*+-=!?^$|

a|
役割
a|
フィールド内をクリックし、グループDNにマッピングするローカルユーザロールを1つ選択します。このグループに含めるロールをそれぞれ個別に選択する必要があります。MonitorロールはSANtricity Unified
Managerにログインするため必要なロールであり、他のロールと一緒に指定する必要があります。各ロールの権限は次のとおりです。

** * Storage admin *--アレイ上のストレージ・オブジェクトへの読み取り
/書き込みのフル・アクセスを提供しますが'セキュリティ構成へのアクセスはありません
** * Security admin *--アクセス管理と証明書管理のセキュリティ設定へのアクセス。
** * Support admin *--
ストレージアレイ上のすべてのハードウェアリソース、障害データ、およびMELイベントへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
** *Monitor *--
すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

|===
====
+

NOTE: Monitorロールは、管理者を含むすべてのユーザに必要です。

. 必要に応じて、*別のマッピングを追加
*をクリックして、グループとロールのマッピングをさらに入力します。
. マッピングが終了したら、*追加*をクリックします。
+
システムによって検証が実行され、ストレージアレイとLDAPサーバが通信できるかどうかが確認されます。エラーメッセージが表示された場合は、ダイアログボックスで入力したクレデンシャルを確認し、必要に応じて情報を再入力します。

[[IDd7c67b0aefccde036cb52ab2e204a10b]]
= ディレクトリサーバの設定とロールマッピングの編集
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセス管理でディレクトリサーバをすでに設定している場合は、その設定をいつでも変更できます。設定には、サーバ接続情報とグループとロールのマッピングが含まれます。

.開始する前に
* Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
* ディレクトリサーバを定義する必要があります。

.手順
. アクセス管理*を選択します。
. [*ディレクトリサービス*]タブを選択します。
. 複数のサーバが定義されている場合は、編集するサーバを表から選択します。
. 「*表示/設定の編集*」を選択します。
+
[ディレクトリサーバーの設定]ダイアログボックスが開きます。

. サーバー設定*タブで、必要な設定を変更します。
+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 製品説明

a|
構成設定

a|
ドメイン
a|
LDAPサーバのドメイン名。ドメインを複数入力する場合は、カンマで区切って入力します。ドメイン名は、ログイン（_username_@_domain_）で、認証するディレクトリサーバを指定するために使用されます。

a|
サーバURL
a|
LDAPサーバにアクセスするためのURL（の形式） `ldap[s]://host:port`。

a|
バインドアカウント（オプション）
a|
LDAPサーバに対する検索クエリおよびグループ内の検索に使用する読み取り専用ユーザアカウント。

a|
バインドパスワード（オプション）
a|
バインドアカウントのパスワード。（このフィールドは、バインドアカウントを入力すると表示されます）。

a|
保存する前にサーバ接続をテストする
a|
システムがLDAPサーバ設定と通信できることを確認します。[保存（Save）]をクリックすると、テストが実行されます。このチェックボックスを選択してテストに失敗した場合、設定は変更されません。設定を編集するには、エラーを解決するか、チェックボックスを選択解除してテストをスキップする必要があります。

a|
権限の設定

a|
検索ベースDN
a|
ユーザを検索するLDAPコンテキスト。通常はの形式です。 `CN=Users, DC=cpoc, DC=local`

a|
ユーザ名属性
a|
認証用のユーザIDにバインドされた属性。例：
`sAMAccountName`。

a|
グループ属性
a|
ユーザのグループ属性のリスト。グループとロールのマッピングに使用されます。例：
`memberOf, managedObjects`。

|===

```
====
. [*役割マッピング*]タブで、目的のマッピングを変更します。
+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 製品説明


 a|
*マッピング*



 a|
グループDN
 a|
マッピングするLDAPユーザグループのドメイン名。正規表現がサポートされています。これらの特殊正規表現文字が正規表現パターンに含まれていない場合は、バックスラッシュ（\）でエスケープする必要があります。

\.[]{}()<>*+-=！？^$|



 a|
役割
 a|
グループDNにマッピングするロール。このグループに含めるロールをそれぞれ個別に選択する必要があります。Monitorロールは SANtricity Unified Managerにログインするため必要なロールであり、他のロールと一緒に指定する必要があります。ロールには次のものがあります。

** * Storage admin *--アレイ上のストレージ・オブジェクトへの読み取り/書き込みのフル・アクセスを提供しますが'セキュリティ構成へのアクセスはありません
** * Security admin *--アクセス管理と証明書管理のセキュリティ設定へのアクセス。
** * Support admin *--
ストレージアレイ上のすべてのハードウェアリソース、障害データ、およびMELイベントへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
** *Monitor *--
すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。


|===
```

====
+

NOTE: Monitorロールは、管理者を含むすべてのユーザに必要です。

. 必要に応じて、*別のマッピングを追加
*をクリックして、グループとロールのマッピングをさらに入力します。
. [保存（ Save ）] をクリックします。

.結果
このタスクを完了すると、アクティブなユーザセッションはすべて終了します。現在のユーザーセッションのみが保持されます。

[[IDc0251ddc7acce1772ef25e00c4000cd5]]
= ディレクトリサーバの削除
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ディレクトリサーバとWebサービスプロキシの間の接続を解除するには、[アクセス管理]ページでサーバ情報を削除します。このタスクは、新しいサーバを設定したあとに古いサーバを削除する場合に実行できます。

.開始する前に
Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。

.タスクの内容
このタスクを完了すると、アクティブなユーザセッションはすべて終了します。現在のユーザーセッションのみが保持されます。

.手順
. アクセス管理*を選択します。
. [*ディレクトリサービス*]タブを選択します。
. リストから、削除するディレクトリサーバを選択します。
. [削除（ Remove ）] をクリックします。
+
[ディレクトリサーバーの削除]ダイアログボックスが開きます。

. フィールドにと入力し `remove`、*[削除]*をクリックします。

+
ディレクトリサーバの構成設定、権限設定、およびロールのマッピングが削除されます。ユーザは、このサーバのクレデンシャルを使用してログインできなくなります。

:leveloffset: -1

= SAMLを使用

:leveloffset: +1

[[ID7897fae080fffbd7bf18e12d5d5af22e]]
= SAMLの設定
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセス管理用の認証を設定するには、ストレージアレイに組み込みのSecurity Assertion Markup Language（
SAML）機能を使用できます。この設定により、アイデンティティプロバイダとストレージプロバイダの間の接続が確立されます。

.開始する前に
* Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
* ストレージアレイのコントローラの
IPアドレスまたはドメイン名を確認しておく必要があります。
* IdP管理者がIdPシステムの設定を完了している必要があります。
* IdP管理者が、認証時に名前IDを返す機能が
IdPでサポートされていることを確認しておく必要があります。
* IdPサーバとコントローラのクロックが同期されていることを確認しておきます（
NTPサーバを使用するかコントローラのクロックの設定を調整します）。
* IdPのメタデータファイルをIdPシステムからダウンロードし、Unified
Managerへのアクセスに使用するローカルシステムで使用できるようにしておきます。

.タスクの内容

アイデンティティプロバイダ（IdP）は、ユーザにクレデンシャルを要求して認証されたユーザかどうかを確認するために使用される外部のシステムです。多要素認証を提供し、Active Directoryなどの任意のユーザデータベースを使用するようにIdPを設定できます。IdPの保守はセキュリティチームが行います。サービスプロバイダ（SP）は、ユーザの認証とアクセスを制御するシステムです。アクセス管理にSAMLが設定されている場合、ストレージアレイはアイデンティティプロバイダに認証を要求するサービスプロバイダとして機能します。IdPとストレージアレイの間の接続を確立するには、この2つのエンティティ間でメタデータファイルを共有します。次に、IdPのユーザエンティティをストレージアレイのロールにマッピングします。最後に、接続とSSOログインをテストしたうえでSAMLを有効にします。

[NOTE]
====
* SAMLとディレクトリサービス*
。認証方式としてディレクトリサービスを設定している場合にSAMLを有効にすると、Unified ManagerではSAMLがディレクトリサービスよりも優先されます。SAMLをあとで無効にすると、ディレクトリサービスの設定は以前の設定に戻ります。

====
[CAUTION]
====
*編集と無効化。*SAMLを有効にすると、ユーザインターフェイスで無効にしたり、IdP設定を編集したりすることはできなくなります。SAMLの設定を無効にしたり編集したりする必要がある場合は、テクニカルサポートにお問い合わせください。

====
SAML認証の設定は複数の手順で構成されます。

== 手順1：IdPのメタデータファイルをアップロードする

ストレージアレイにIdPの接続情報を提供するには、Unified ManagerにIdPメタデータをインポートします。このメタデータは、IdPシステムが認証要求を正しいURLにリダイレクトし、受信した応答を検証するために必要です。

.手順
. メニューを選択します。Settings [Access Management]。
. SAML *タブを選択します。
+
設定手順の概要が表示されます。

. アイデンティティプロバイダ（IdP）ファイルのインポート*リンクをクリックします。
+
[Import Identity Provider File]ダイアログボックスが開きます。

. Browse *をクリックして、ローカルシステムにコピーしたIdPメタデータファイルを選択してアップロードします。

+
ファイルを選択すると、IdPのエンティティIDが表示されます。

. [* インポート *] をクリックします。

== 手順2：サービスプロバイダのファイルをエクスポートする

IdPとストレージアレイの間の信頼関係を確立するには、サービスプロバイダのメタデータをIdPにインポートします。このメタデータは、IdPがコントローラとの信頼関係を確立し、許可要求を処理するために必要です。このファイルには、IdPがサービスプロバイダと通信できるように、コントローラのドメイン名やIPアドレスなどの情報が含まれています。

.手順
. [サービスプロバイダファイルのエクスポート*]リンクをクリックします。
+
[サービスプロバイダファイルのエクスポート]ダイアログボックスが開きます。

. コントローラのIPアドレスまたはDNS名を[*コントローラA *]フィールドに入力し、[*エクスポート]をクリックしてメタデータファイルをローカルシステムに保存します。
+
「*Export」をクリックすると、サービスプロバイダのメタデータがローカルシステムにダウンロードされます。ファイルが保存されている場所をメモします。

. ローカルシステムで、エクスポートしたXML形式のサービスプロバイダメタデータファイルを探します。
.
IdPサーバから、サービスプロバイダのメタデータファイルをインポートして信頼関係を確立します。ファイルを直接インポートすることも、ファイルからコントローラ情報を手動で入力することもできます。

== 手順3：ロールをマッピングする

Unified Managerへのアクセスをユーザに許可するには、IdPユーザの属性とグループメンバーシップをストレージアレイの事前定義されたロールにマッピングする必要があります。

.開始する前に
* IdP管理者が、IdPシステムでユーザ属性とグループメンバーシップを設定しておく必要があります。
* IdPのメタデータファイルをUnified Managerにインポートします。

* コントローラのサービスプロバイダメタデータファイルが、信頼関係のIdPシステムにインポートされている。

.手順
. 「mapping Unified Manager * roles」のリンクをクリックします。
+
ロールマッピング(Role Mapping)ダイアログボックスが開きます

. IdPユーザの属性とグループを事前定義されたロールに割り当てます。1つのグループに複数のロールを割り当てることができます。
+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 製品説明

a|
マッピング

a|
ユーザ属性
a|
マッピングするSAMLグループの属性（「member of」など）を指定します。

a|
属性値
a|
マッピングするグループの属性値を指定します。正規表現がサポートされています。(`\`正規表現パターンに含まれていない特殊な正規表現文字は、バックスラッシュでエスケープする必要があります。\.[]{}()<>*+-=!?^$|

a|
役割
a|
フィールド内をクリックし、属性にマッピングするストレージアレイのロールを1つ選択します。含めるロールをそれぞれ個別に選択する必要があります。Monitorロールは Unified Managerにログインするために必要な他のロールと一緒に指定する必要があります。少なくとも1つ

のグループにはSecurity Adminロールも必要です。

各ロールの権限は次のとおりです。

** * Storage admin *--
ストレージ・オブジェクト（ボリュームやディスク・プールなど）への読み取り/書き込みのフル・アクセス。セキュリティ構成へのアクセスはありません。
** * Security admin *--
アクセス管理、証明書管理、監査ログ管理のセキュリティ構成へのアクセス、および従来の管理インターフェイス（SYMbol）のオン/オフの切り替え機能。
** * Support admin *--
ストレージアレイのすべてのハードウェアリソース、障害データ、MELイベント、およびコントローラファームウェアアップグレードへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
** *Monitor *--
すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

|===
====
+
[NOTE]
====
Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールが割り当てられていないユーザのUnified Managerは正しく動作しません。

====
. 必要に応じて、*別のマッピングを追加
*をクリックして、グループとロールのマッピングをさらに入力します。
+
[NOTE]
====
ロールのマッピングは、SAMLを有効にしたあとに変更できます。

====
. マッピングが終了したら、*保存*をクリックします。

== 手順4：SSOログインをテストする

IdPシステムとストレージアレイが通信できることを確認するために、必要に応じてSSOログインをテストできます。このテストは、SAMLを有効にする最後の手順でも実行します。

.開始する前に

* IdPのメタデータファイルをUnified Managerにインポートします。
* コントローラのサービスプロバイダメタデータファイルが、信頼関係の
IdPシステムにインポートされている。

.手順
. [Test SSO Login*]リンクを選択します。
+
SSOクレデンシャルを入力するためのダイアログボックスが開きます。

. Security Adminと
Monitorの両方の権限を持つユーザのログインクレデンシャルを入力します。
+
ログインのテスト中は、ダイアログボックスが開きます。

. テストに成功したことを示すメッセージを確認します。テストに成功した場合は、
SAMLを有効にする次の手順に進みます。
+
テストが正常に完了しなかった場合は、エラーメッセージと詳細情報が表示されます。次の点を確認してください。

+
** ユーザがSecurity AdminとMonitorの権限を持つグループに属していること。
** アップロードしたIdPサーバのメタデータが正しいこと。
** SPメタデータファイル内のコントローラアドレスが正しい。

== 手順5：SAMLを有効にする

最後に、ユーザ認証用のSAMLの設定を完了します。このプロセスでは、SSOログインのテストも求められます。SSOログインのテストプロセスについては、前の手順で説明しています。

.開始する前に
* IdPのメタデータファイルをUnified Managerにインポートします。
* コントローラのサービスプロバイダメタデータファイルが、信頼関係の
IdPシステムにインポートされている。
* 少なくともMonitorロールとSecurity Adminロールを1つずつマッピングしておきます。

[CAUTION]
====
*編集と無効化。*SAMLを有効にすると、ユーザインターフェイスで無効にしたり、IdP設定を編集したりすることはできなくなります。SAMLの設定を無効にしたり編集したりする必要がある場合は

、テクニカルサポートにお問い合わせください。

====
.手順
. [* SAML *]タブで、[* SAMLを有効にする]リンクを選択します。
+
[SAMLの有効化の確認]ダイアログボックスが開きます。

. と入力し `enable`、*[有効化]*をクリックします。
. SSOログインテスト用のユーザクレデンシャルを入力します。

.結果
SAMLが有効になると、アクティブなセッションはすべて終了され、SAMLを使用したユーザの認証が開始されます。

[[ID0e0949e46c0e798eb608a7c8751faf7a]]
= SAMLロールマッピングの変更
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセス管理用にSAMLを設定している場合は、IdPグループとストレージアレイの事前定義されたロールの間のロールマッピングを変更できます。

.開始する前に
* Security
Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
* IdP管理者が、
IdPシステムでユーザ属性とグループメンバーシップを設定しておく必要があります。
* SAMLを設定して有効にします。

.手順
. メニューを選択します。Settings [Access Management]。
. SAML *タブを選択します。
. [*役割のマッピング*]を選択します。
+
ロールマッピング(Role Mapping)ダイアログボックスが開きます

. IdPユーザの属性とグループを事前定義されたロールに割り当てます。
1つのグループに複数のロールを割り当てることができます。
+
[CAUTION]
====
SAMLが有効になっている間は権限を削除しないように注意してください。削除すると、Unified Managerにアクセスできなくなります。

====
+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 製品説明

 a|
マッピング

 a|
ユーザ属性
 a|
マッピングするSAMLグループの属性（「member of」など）を指定します。

 a|
属性値
 a|
マッピングするグループの属性値を指定します。

 a|
役割
 a|
フィールド内をクリックし、属性にマッピングするストレージアレイのロールを1つ選択します。このグループに含めるロールをそれぞれ個別に選択する必要があります。Monitorロールは Unified Managerにログインするために必要な他のロールと一緒に指定する必要があります。少なくとも1つのグループに Security
Adminロールを割り当てる必要があります。各ロールの権限は次のとおりです。

** * Storage admin *--

ストレージ・オブジェクト（ボリュームやディスク・プールなど）への読み取り/書き込みのフル・アクセス。セキュリティ構成へのアクセスはありません。
** * Security admin *--
アクセス管理、証明書管理、監査ログ管理のセキュリティ構成へのアクセス、および従来の管理インターフェイス（SYMbol）のオン/オフの切り替え機能。
** * Support admin *--
ストレージアレイのすべてのハードウェアリソース、障害データ、MELイベント、およびコントローラファームウェアアップグレードへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
** *Monitor *--
すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

|===
====
+

NOTE: Monitorロールは、管理者を含むすべてのユーザに必要です。
Monitorロールが割り当てられていないユーザのUnified Managerは正しく動作しません。

. 必要に応じて、* Add another mapping
*をクリックして、グループとロールのマッピングをさらに入力します。
. [保存（ Save ）] をクリックします。

.結果
このタスクを完了すると、アクティブなユーザセッションはすべて終了します。現在のユーザーセッションのみが保持されます。

[[ID07b6aaf334cfa34916b0ae417667d0a5]]
= SAMLサービスプロバイダファイルのエクスポート
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
必要に応じて、ストレージアレイのサービスプロバイダメタデータをエクスポートし、そのファイルをアイデンティティプロバイダ（IdP）システムに再インポートできます。

.開始する前に
* Security

Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
* SAMLを設定して有効にします。

.タスクの内容
このタスクでは、コントローラからメタデータをエクスポートします。このメタデータは、IdPがコントローラとの信頼関係を確立し、認証要求を処理するために必要です。このファイルには、コントローラのドメイン名やIPアドレスなど、IdPで要求の送信に使用できる情報が含まれています。

.手順
. メニューを選択します。Settings [Access Management]。
. SAML *タブを選択します。
. 「*書き出し*」を選択します。
+
[サービスプロバイダファイルのエクスポート]ダイアログボックスが開きます。

. [エクスポート]*をクリックして、メタデータファイルをローカルシステムに保存します。
+
[NOTE]
====
ドメイン名フィールドは読み取り専用です。

====
+
ファイルが保存されている場所をメモします。

. ローカルシステムで、エクスポートした
XML形式のサービスプロバイダメタデータファイルを探します。
.
IdPサーバから、サービスプロバイダのメタデータファイルをインポートします。ファイルを直接インポートすることも、コントローラ情報を手動で入力することもできます。
. [* 閉じる *] をクリックします。

:leveloffset: -1

= FAQ

:leveloffset: +1

[[IDd570e40b61a2ad52272750f67f0e2592]]
= ログインできないのはなぜですか？

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


[role="lead"]
ログイン時にエラーが表示された場合は、次の原因を確認してください。

ログインエラーは、次のいずれかの理由で発生する可能性があります。

* 入力したユーザ名またはパスワードが正しくありません。
* Privilegesが不十分です。
* ログインに何度も失敗したため、ロックアウトモードがトリガーされました。
10分待ってから再ログインしてください。
* SAML認証が有効になりました。ブラウザの表示を更新してログインします。




[[IDdc7cc639c10528d2246aeaf1b536248e]]
= ディレクトリサーバを追加するときは、どのような点に注意する必要がありますか？
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
アクセス管理でディレクトリサーバを追加する前に、一定の要件を満たす必要があります。

* ユーザグループがディレクトリサービスに定義されている必要があります。
* LDAPサーバのクレデンシャルを確認しておく必要があります。ドメイン名とサーバの
URLのほか、必要に応じてバインドアカウントのユーザ名とパスワードも指定できます。
* セキュアなプロトコルを使用するLDAPSサーバの場合は、
LDAPサーバの証明書チェーンをローカルマシンにインストールする必要があります。




[[IDecf017413500378c8f73b7a374a78ef8]]
=
ストレージアレイのロールにマッピングするときは、どのような点に注意する必要がありますか？
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]
グループをロールにマッピングする前に、ガイドラインを確認してください。

RBAC（ロールベースアクセス制御）機能には次のロールがあります。

* * Storage admin *--アレイ上のストレージ・オブジェクトへの読み取り
/書き込みのフル・アクセスを提供しますが'セキュリティ構成へのアクセスはありません
* * Security admin *--アクセス管理と証明書管理のセキュリティ設定へのアクセス。
* * Support admin *--
ストレージアレイ上のすべてのハードウェアリソース、障害データ、およびMELイベントへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
* *Monitor *--
すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

[NOTE]
====
Monitorロールは、管理者を含むすべてのユーザに必要です。

====
LDAP（Lightweight Directory Access
Protocol）サーバとディレクトリサービスを使用する場合は、次の点を確認してください。

* 管理者がディレクトリサービスでユーザーグループを定義しました。
* LDAPユーザグループのグループドメイン名を確認しておきます。

== SAML

ストレージアレイに組み込みのSecurity Assertion Markup Language（
SAML）機能を使用する場合は、次の点を確認してください。

* アイデンティティプロバイダ（IdP）管理者が、
IdPシステムでユーザ属性とグループメンバーシップを設定しておく必要があります。
* グループメンバーシップ名を確認しておきます。
*
マッピングするグループの属性値がわかっている必要があります。正規表現がサポートされています。（`\`正規表現パターンに含まれていない特殊な正規表現文字は、バックスラッシュでエスケープする必要があります）。
+
[listing]

```
\.[]{}()<>*+-=!?^$|
----
* Monitorロールは、管理者を含むすべてのユーザに必要です。
Monitorロールが割り当てられていないユーザのUnified Managerは正しく動作しません。




[[ID2fd71270ddc31aef2686b5ec0df545af]]
= SAMLを設定して有効にするときは、どのような点に注意する必要がありますか？
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
認証のためにSecurity Assertion Markup Language（
SAML）の機能を設定して有効にする前に、次の要件を満たしていることを確認し、SAMLの制限事項を理解しておきます。



== 要件

開始する前に、次のことを確認してください。

* ネットワークにアイデンティティプロバイダ（IdP）を設定しておきます。
IdPは、ユーザにクレデンシャルを要求して認証されたユーザかどうかを確認するための外部システムです。IdPの保守はセキュリティチームが行います。
* IdP管理者が、IdPシステムでユーザ属性とユーザグループを設定しておきます。
* IdP管理者が、認証時に名前IDを返す機能が
IdPでサポートされていることを確認しておく必要があります。
* IdPサーバとコントローラのクロックが同期されていることを確認しておきます（
NTPサーバを使用するかコントローラのクロックの設定を調整します）。
* IdPのメタデータファイルをIdPシステムからダウンロードし、Unified
Managerへのアクセスに使用するローカルシステムで使用できるようにしておきます。
* ストレージアレイのコントローラのIPアドレスまたはドメイン名を確認しておきます。



== 制限事項

上記の要件に加えて、次の制限事項を理解していることを確認してください。

* SAMLを有効にすると、ユーザインターフェイスで無効にしたり、
```

IdP設定を編集したりすることはできなくなります。SAMLの設定を無効にしたり編集したりする必要がある場合は、テクニカルサポートにお問い合わせください。最後の設定手順でSAMLを有効にする前に、SSOログインをテストすることを推奨します。（SAMLを有効にする前にSSOログインのテストも実行されます）。
* あとで
SAMLを無効にすると、以前の設定（ローカルユーザロールまたはディレクトリサービス）が自動的にリストアされます。
* 現在ユーザ認証用にディレクトリサービスが設定されている場合は、
SAMLによって上書きされます。
*
SAMLが設定されている場合、次のクライアントはストレージアレイリソースにアクセスできません。
+
** Enterprise Management Window（EMW）
** コマンドラインインターフェイス（CLI）
** ソフトウェア開発キット（SDK）クライアント
** インバンドクライアント
** HTTPベーシック認証REST APIクライアント
** 標準のREST APIエンドポイントを使用したログイン

[[IDb42ad0bece338ecf63c01d6aa8106d6b]]
= ローカルユーザとは何ですか？
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ローカルユーザはシステムに事前に定義されており、特定の権限が含まれています。

ローカルユーザは次のとおりです。

* *admin*--
システム内のすべての機能にアクセスできるスーパー管理者。このユーザにはすべてのロールが含まれます。初回ログイン時にパスワードを設定する必要があります。
* * storage *--
すべてのストレージ・プロビジョニングを担当する管理者。このユーザには、Storage Admin、Support Admin、
Monitorのロールが含まれています。このアカウントは、パスワードが設定されるまで無効になります。
* * security *--

アクセス管理や証明書管理など、セキュリティ設定を担当するユーザー。このユーザには、Security Adminと
Monitorのロールが含まれています。このアカウントは、パスワードが設定されるまで無効になります。
* * support *--
ハードウェアリソース、障害データ、ファームウェアアップグレードを担当するユーザー。このユーザには、Support Adminと
Monitorのロールが含まれています。このアカウントは、パスワードが設定されるまで無効になります。
* *monitor *--システムへの読み取り専用アクセス権を持つユーザー。このユーザには
Monitorロールのみが含まれています。このアカウントは、パスワードが設定されるまで無効になります。
* * rw *（読み取り/書き込み）-このユーザには、Storage Admin、Support Admin
、Monitorのロールが含まれています。このアカウントは、パスワードが設定されるまで無効になります。
* * ro *（読み取り専用）--このユーザーには、
Monitorロールのみが含まれています。このアカウントは、パスワードが設定されるまで無効になります。

:leveloffset: -1

:leveloffset: -1

:leveloffset: -1

[[IDa18016aaa42e453f74523b9f06606ef6]]
= 以前のバージョン
:allow-uri-read:

[role="lead"]
E シリーズハードウェアおよび SANtricity
ソフトウェアの以前のバージョンのドキュメントにアクセスするには、以下のリンクを参照してください。リンクをクリックすると、別のドキュメントサイトにアクセスできます。

== 以前のリリースのハードウェアマニュアル

* https://library.netapp.com/ecm/ecm_download_file/ECMLP2484026["E2712 、 E2724 、 E5612 、 E5624 コントローラドライブトレイ、 DE1600 、 DE5600

拡張ドライブトレイを搭載"^]
* https://library.netapp.com/ecm/ecm_download_file/ECMLP2484072["E2760 と E5660 コントローラドライブトレイと DE6600 拡張ドライブトレイを設置します"^]
* https://library.netapp.com/ecm/ecm_download_file/ECMLP2484108["EF560 フラッシュアレイと DE5600 フラッシュ拡張トレイを設置"^]
*
https://mysupport.netapp.com/info/web/ECMP11392380.html["古いシステムをインストールします"^]
*
https://mysupport.netapp.com/info/web/ECMP11751516.html["古いシステムを維持します"^]
* https://mysupport.netapp.com/ecm/ecm_download_file/ECMP1394872["E2600 および E2700 に 2 台目のコントローラを追加します"^]
*
https://library.netapp.com/ecm/ecm_download_file/ECMLP2353447["ホストプロトコルを変更または追加する"^]
* https://mysupport.netapp.com/ecm/ecm_download_file/ECMP1656638["AC 電源から DC 電源に変換します"^]

== 以前のリリースのソフトウェアドキュメント

=== SANtricityリリース11.7

* https://docs.netapp.com/us-en/e-series-santricity-117/index.html["System Managerのヘルプ"^]
* https://docs.netapp.com/us-en/e-series-santricity-117/index.html["Unified Managerのヘルプ"^]

=== SANtricityリリース11.6

* https://docs.netapp.com/us-en/e-series-santricity-116/index.html["System Managerのヘルプ"^]
* https://docs.netapp.com/us-en/e-series-santricity-116/index.html["Unified Managerのヘルプ"^]

=== SANtricityリリース11.5

```
* https://docs.netapp.com/us-en/e-series-santricity-115/index.html["System
Managerのヘルプ"^]



=== SANtricityリリース11.4

* https://mysupport.netapp.com/ecm/ecm_get_file/ECMLP2862590["AMW（E2700
、E5600 / EF560）のヘルプ"^]
* https://mysupport.netapp.com/ecm/ecm_get_file/ECMLP2862588["EMW（E2700
、E5600 / EF560）のヘルプ"^]



[[ID72c10d033504016a19249c3a53d3cb98]]
= 法的通知
:hardbreaks:
:allow-uri-read:
:icons: font
:linkattrs:
:relative_path: ./
:imagesdir: {root_path}{relative_path}./media/


[role="lead lead"]
法的通知では、著作権に関する声明、商標、特許などにアクセスできます。



== 著作権

link:https://www.netapp.com/company/legal/copyright/["https://www.netapp.c
om/company/legal/copyright/"^]



== 商標

NetApp、NetAppのロゴ、およびNetAppの商標ページに記載されているマークは、NetApp、Inc.
の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。

link:https://www.netapp.com/company/legal/trademarks/["https://www.netapp.
com/company/legal/trademarks/"^]
```

== 特許

NetAppが所有する特許の最新リストは、次のサイトで参照できます。

link:https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf["https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf"^]

== プライバシーポリシー

link:https://www.netapp.com/company/legal/privacy-policy/["https://www.netapp.com/company/legal/privacy-policy/"^]

== オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

https://library.netapp.com/ecm/ecm_download_file/ECMLP2885978["E シリーズ / EF シリーズ SANtricity OS に関する通知です"]

:leveloffset: -1

<<<
著作権に関する情報

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、link:http://www.netapp.com/TM[http://www.netapp.com/TM^]に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。