SANtricityソフトウェアのドキュメント11.90

SANtricity 11.9

NetApp
December 16, 2024

目次

SANtricityソフトウェアのドキュメント11.90

リリースノート

SANtricity OS 11.90の新機能

次の表に、SANtricity System Manager 11.9の新機能を示します。

バージョン**11.90**の新機能

新機能	説明
新しいストレージシステムモデル– E4000	このリリースでは、E4000低コストストレージシステムが導入されています。E4000は、コントローラごとに12本と60本のドライブと1つのホストインターフェイスカード（HIC）をサポートします。初期リリースでは、サポートされるホストインターフェイスカードにはiSCSIとFibre Channelがあります。E4000ストレージシステムとその他のEシリーズストレージシステムは、Unified Managerで表示および管理できます。
Dynamic Disk Poolsの容量の拡張	プール内の個 々 のドライブの容量が23TBを超えるたびに、Dynamic Disk Pools（DDP）の容量が12PBに拡張されました。個 々 のドライブの容量が23TB未満の場合、DDPの容量は6PBになります。
デフォルトのメディアスキャン設定の拡張	デフォルトのメディアスキャン速度が120日に引き上げられました。
外部キー管理で秘密鍵を承認	秘密鍵と公開鍵のペアから外部で生成された証明書署名要求（CSR）ファイルを、System Managerからインポートできるようになりました。
Web Servicesでログインロックアウト機能を使用できるようになりました	REST APIでのみ設定可能で、組み込みWebサービスとプロキシWebサービスで新しいログインロックアウト設定を使用できるようになりました。

リリースノート

このサイトにはリリースノートがありません。ネットアップサポートサイトのクレデンシャルでログインするように求められます。

- "11.90リリースノート"
- "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"

はじめに

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を設定できます。

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

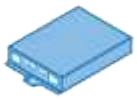
パフォーマンス

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する重要なイベントを管理者に通知します。アラートは E メール、 SNMP トラップ、 syslog を通じて送信できます。
 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 の略

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（E4000、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の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
ストレージアレイを管理しやすくするために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。

サポートされてい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	八九
Mozilla Firefox	8時80分
Safari	14
Microsoft Edge の場合	90

Unified Managerの場合は、Web Services Proxyをインストールしてブラウザから使用できるようにしておく必要があります。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および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の場合	2016年、2019年、2022 / 64ビット
Ubuntu	18.04、20.04/64ビット

System Managerのセットアップ

System Managerにアクセスします

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を設定できます。

作業を開始する前に

- 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。を参照してください "サポートされてい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、「+ https://<IPAddress>+`」というURLを入力します

   「 IPAddress 」は、ストレージアレイコントローラの 1 つのアドレスです。

設定されていないアレイでSystem Managerを初めて開くと、Set Administrator Password（管理者パスワードの設定）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、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、およびAutoSupport 。

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 "Upgrade Center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。

用語集

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	説明
アプリケーション	アプリケーションは、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、ホストにアクセス可能な 1 つ以上のボリュームを作成することができます。（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。ボリュームが複数のドライブで構成される場合でも、ホスト側では1つの論理コンポーネントとして認識され、
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ごとに容量と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、ホストにアクセス可能な1つ以上のボリュームを作成することができます。（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	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またはインスタンスを定義できます。一部のアプリケーションでは、特性が似たボリュームで構成されるようにワークロードが設定されます。これらのボリューム特性は、ワークロードがサポートするアプリケーションのタイプに基づいて最適化されます。たとえば、Microsoft SQL Serverアプリケーションをサポートするワークロードを作成し、そのワークロード用のボリュームを作成すると、Microsoft SQL Serverをサポートするようにボリューム特性が最適化されます。

よくある質問です

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？

ハードウェアの検証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、ストレージアレイに互換性のないシェルフが設置さ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。互換性の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。

ホストの設定は、セットアップの完了後に実行できます。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）が設定されていて、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。

アプリケーションによってボリュームを最適化することで、データストレージの処理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、読み取りと書き込みのキャッシュなどの特性が含まれます。また、アプリケーションごと、ワークロードごとに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。

ワークロードとは何ですか？

SQL ServerやExchangeなど、ネットワーク内の一部のアプリケーションについては、そのアプリケーション用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またはインスタンスを定義できます。一部のアプリケーションでは、特性が似たボリュームで構成されるようにワークロードが設定されます。これらのボリューム特性は、ワークロードがサポートするアプリケーションのタイプに基づいて最適化されます。たとえば、Microsoft SQL Serverアプリケーションをサポートするワークロードを作成し、そのワークロード用のボリュームを作成すると、Microsoft SQL Serverをサポートするようにボリューム特性が最適化されます。

ボリュームの作成時には、ワークロードの用途について回答 から質問するプロンプトが表示されます。たとえば、Microsoft Exchange用のボリュームを作成する場合は、必要なメールボックスの数、メールボックスに必要とされる平均容量、およびデータベースのコピーをいくつ作成するかについて設定します。この情報に基づいて最適なボリューム構成が作成されるため、必要に応じて編集することができます。

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と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、要件に最も適したストレージのタイプを特定します。

- できるだけ大きいプールではなく、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？
- 推奨される構成を使用するのではなく、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？

これらのいずれかの質問に対する「はい」と答えた場合は、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。

ホストの設定は、セットアップの完了後に実行できます。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）が設定されていて、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のセットアップを実行します

Unified Manager をインストールします

Unified ManagerはWeb Services Proxyに含まれています。Web Services Proxy 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/ 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"
2. "Web Services Proxy ファイルをダウンロードしてインストール"

Unified Managerにアクセスします

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 "サポートされてい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] ： //< サーバ > ： <port>/um+`

   この URL では、「 <server> 」は Web Services Proxy がインストールされているサーバの IP 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 が 8080 、 HTTPS が 8443 ）です。

   Unified Manager のログインページが開きます。

2. 初めてのログインの場合は、ユーザ名に「 admin 」と入力し、管理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 30 文字まで使用できます。

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

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を行うための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ており、ストレージアレイの状態と健常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（ **Area** ）	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	Performance領域では、時間の経過に伴うリソース使用量を比較したり、対比したりできます。応答時間（IOPS）、転送速度（MiB/秒）、使用中の処理能力（CPU）に関して、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、および割り当てられていないストレージ容量のグラフが表示されます。
ストレージ階層	ストレージ階層領域には、ストレージアレイで管理されるさまざまなハードウェアコンポーネントと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、その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。

インターフェイスの設定

メインインターフェイスから表示環境設定やその他の設定を変更できます。

設定	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。
セッションタイムアウト	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	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、次の項を参照してください。

- "管理者パスワード保護を設定します"
- "パスワードを変更します"

パフォーマンスデータを表示します

パフォーマンスの概要

Performance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がわかりますか？

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。

詳細はこちら。

- "パフォーマンス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は、ホームページおよびストレージページから確認できます。

詳細はこちら。

- "グラフィカルなパフォーマンスデータを表示します"
- "表形式のパフォーマンスデータを表示および保存する"
- "パフォーマンスデータを解釈する"

パフォーマンスグラフとガイドライン

パフォーマンスページには、いくつかの重要な領域でストレージアレイのパフォーマンスを評価できる、データのグラフと表が表示されます。

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する。
- 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ります	デフォルトは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（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ります	選択した期間によって異なります	無制限	はい。

パフォーマンスデータを表示する際のガイドライン

- パフォーマンスデータの収集は常にオンです。オフにするオプションはありません。
- ストレージアレイがサンプリング間隔で照会され、データが更新されます。
- グラフデータでは、期間を5分に設定すると10秒ごとのサンプリングで5分間の平均が算出されます。他のすべての期間は5分ごとに更新され、選択した期間の平均が算出されます。
- グラフィカル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のオブジェクトが変わると、選択した期間全体をカバーするデータポイントがオブジェクトに存在しない場合があります。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とボリュームセットが変わる場合があり、また、ドライブが追加、削除されたり、障害が発生したりする可能性もあります。

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	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「中央処理装置」用ではありません。 cpuは、ストレージアレイの使用中の処理容量の割合を示します。
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の形式でホストに容量として提示されます。 各ホストには独自のLUNアドレススペースがあります。したがって、同じLUNを複数のホストで使用して、異なるボリュームにアクセスできます。
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、ホストにアクセス可能な 1 つ以上のボリュームを作成することができます。（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	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。ボリュームが複数のドライブで構成される場合でも、ホスト側では1つの論理コンポーネントとして認識され、
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ごとに容量と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、ホストにアクセス可能な1つ以上のボリュームを作成することができます。（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またはインスタンスを定義できます。一部のアプリケーションでは、特性が似たボリュームで構成されるようにワークロードが設定されます。これらのボリューム特性は、ワークロードがサポートするアプリケーションのタイプに基づいて最適化されます。たとえば、Microsoft SQL Serverアプリケーションをサポートするワークロードを作成し、そのワークロード用のボリュームを作成すると、Microsoft SQL Serverをサポートするようにボリューム特性が最適化されます。
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を表示します

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データをグラフで表示できます。

このタスクについて

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では、3つのタブからそれぞれグラフを使用できます。

- 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（ **Options** ）

オブジェクトを表示するためのオプション	説明
ドロワーを展開してオブジェクトのリストを表示します。	_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（Filter）]ボックスに、ドロワー内のオブジェクトのみをリストするオブジェクトの名前または名前の一部を入力する。
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。
グラフの表示と非表示を切り替えます	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	説明
期間	表示する期間（5分、1時間、8時間、1日、7日）を選択します。 または30日）。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をロードする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閉じたりしないでください。また、ブラウザをリフレッシュしないでください。
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すると、前後の期間を表示できます。
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すると、期間を拡大表示できます。ズームバーを広げるほど、グラフの細かい部分が小さくなります。 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。
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を表示および保存する

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することができます。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を示す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して、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'performanceStatistics-yyyy-mm-dd_hh-mm-ss.csv'で、ファイルのエクスポート日時が含まれます。

パフォーマンスデータを解釈する

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、考慮すべき主な要素を示します。

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が複数のボリューム間で共有されている場合は、個々のボリュームに独自のボリュームグループを割り当てると、ドライブのシーケンシャルパフォーマンスが向上し、レイテンシが低減される可能性があります。 • 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。 • ドライブタイプと速度はレイテンシに影響します。ランダムI/Oの場合、ドライブの回転速度が速いほど、ディスク上の別の場所との間の移動にかかる時間は短くなります。 • ドライブ数が少なすぎると、キューに格納されるコマンドが多くなり、ドライブのコマンド処理時間が長くなるため、システムの一般的なレイテンシが増加します。 • I/Oが大きいと、データの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、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不均衡な場合は、ドライブが低速であ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、次のものがあります。 • 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になっているかどうか • 書き込みキャッシュが有効になっているかどうか • 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の数 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てください。 ボリュームのIOPS統計からは、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。実際に試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要求のサイズが小さいと転送速度は遅くなりますが、I/O速度は上がり、応答時間は短縮されます。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。

パフォーマンスデータ	パフォーマンス調整の関連事項
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使用率は高く、時間とともに増加していて、もう一方のコントローラは使用率が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。 ストレージアレイ間でCPUを監視する必要がある場合があります。CPU使用率が時間とともに増加し続け、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追加することで、許容されるパフォーマンスレベルで引き続きアプリケーションのニーズを満たすことができます。
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のドライブチャネルの残りのパフォーマンス容量を指します。この値は割合で表され、これらのオブジェクトで実現可能な最大パフォーマンスと現在のパフォーマンスレベルとのギャップを表しています。 • 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。

ストレージ階層を表示します

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る各種ハードウェアコンポーネントと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

次の表では、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	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。

コンポーネント	説明
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を収容します。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は、コントローラとドライブを収容します。ドライブシェルフは、入出力モジュール（ IOM ）とドライブを収容します。 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、データ用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。
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。

論理構成要素

ストレージアレイ内のドライブは、データに対して物理ストレージ容量を提供します。System Managerを使用して、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物理容量を割り当てます。これらのコンポーネントは、ストレージアレイ上のデータの設定、格納、メンテナンス、および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	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、ホストにアクセス可能な 1 つ以上のボリュームを作成することができます。（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ごとに容量と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、ホストにアクセス可能な1つ以上のボリュームを作成することができます。（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。

コンポーネント	説明
Logical Unit Number（LUN；論理ユニット番号）	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の形式でホストに容量として提示されます。 各ホストには独自のLUNアドレススペースがあります。したがって、同じLUNを複数のホストで使用して、異なるボリュームにアクセスできます。

インターフェイスの設定を管理します

パスワード保護を管理します

ストレージアレイには、不正なアクセスを防ぐためにパスワードを設定する必要があります。

パスワードを設定および変更する

System Managerを初めて起動したときは、管理者パスワードの設定を求めるプロンプトが表示されます。管理者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。初回起動時に管理者パスワードを設定するには、を参照してください "System Managerにアクセスします"。

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。この状態のストレージアレイは以降のパスワード入力を拒否します。パスワードを再度入力するには、ストレージアレイが「通常」状態にリセットされるまで10分間待つ必要があります。

adminパスワードに加えて、ストレージアレイには、1つ以上のロールがマッピングされた事前定義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 "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だけです。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 "パスワードを変更します"。

セッションタイムアウト後にパスワードを再入力します

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。ただし、操作を行わないまま30分が経過するとセッションはタイムアウトし、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、次回の設定処理や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したり、セッションタイムアウトを無効にしたりできます。を参照してください "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保護を削除します

パスワードで保護されたドライブを取り外す場合やパスワードで保護されたドライブ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、そのパスワードは使用できなくなります。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度取り付けます。

- 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、原因 がデータ損失などの深刻な損害を受ける可能性があります。このため、ストレージアレイには常に管理者パスワードを設定する必要があります。セキュリティを強化するには、英数字15文字以上の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します

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	価値
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を設定します

パフォーマンスグラフに表示されるデフォルト期間を変更できます。

このタスクについて

ホームページおよびパフォーマンスページに表示されるパフォーマンスグラフの初回表示は、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。

ログインバナーを設定します

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、注意と同意を求めるメッセージを含めることができます。

このタスクについて

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タグ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。

このタスクについて

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。

アレイに組み込まれているSecurity Assertion Markup Language（SAML）機能を使用してアクセス管理が設定されている場合は、ユーザのSSOセッションがその期限に達したときにセッションタイムアウトが発生する可能性があります。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できます。

   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。

通知を管理します

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。	説明
	最適
	最適でないか、障害が発生しています
	対応または修正が必要です
	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は、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失敗したアイコンが表示されます。
- [コンポーネント]ページで、ドライブとコントローラのグラフィックス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、リカバリ手順について説明しているハードウェアのドキュメントを参照し、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対処します

長時間実行されている処理を表示して実行するには、Operations in Progressページを使用します。

このタスクについて

[Operations in Progress]ページにリストされている各オペレーションについて、完了した割合と処理が完了するまでの推定時間が表示されます。場合によっては、処理を停止したり、処理の優先度を変更したりできます。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（Actions）]列のリンクを使用して、オペレーションの優先度を停止または変更します。

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

   ボリュームコピー処理を停止するか、優先度を変更できます。

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。

[Operations in Progress]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	完了しました	クリア
ボリュームコピー	実行中です	• 優先度を変更します • 停止します
ボリュームコピー	保留中です	クリア
ボリュームコピー	失敗しました	• クリア • 再コピー
ボリュームコピー	停止しました	• 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）	実行中です	_ なし _
ボリュームの削除（64TiBを超えるシックプールボリュームのみ）	実行中です	_ なし _
非同期ミラーグループの初期同期	実行中です	一時停止
非同期ミラーグループの初期同期	中断しました	再開

操作	処理のステータス	対処方法
同期ミラーリング	実行中です	一時停止
同期ミラーリング	中断しました	再開
Snapshotイメージのロールバック	実行中です	キャンセル
Snapshotイメージのロールバック	保留中です	キャンセル
Snapshotイメージのロールバック	一時停止中	• キャンセル • 再開
ドライブの退避	実行中です	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に容量を追加してください	実行中です	_ なし _
ボリュームのRAIDレベルを変更します	実行中です	_ なし _
プールの容量を削減します	実行中です	_ なし _
シンボリュームの再生	実行中です	_ なし _
プールボリュームのInstant Availability Format（IAF）処理の残り時間を確認します	実行中です	_ なし _
ボリュームグループのデータ冗長性をチェックします	実行中です	_ なし _
ボリュームグループのデフラグ	実行中です	_ なし _
ボリュームを初期化	実行中です	_ なし _
ボリュームの容量を拡張します	実行中です	_ なし _
ボリュームのセグメントサイズを変更します	実行中です	_ なし _
ドライブコピー	実行中です	_ なし _

操作	処理のステータス	対処方法
データ再構築	実行中です	_ なし _
コピーバック	実行中です	_ なし _
ドライブ消去	実行中です	_ なし _
リモートストレージのインポート	実行中です	• 優先度を変更します • 停止します
リモートストレージのインポート	停止しました	• 再開 • 切断します
リモートストレージのインポート	失敗しました	• 再開 • 切断します
リモートストレージのインポート	完了しました	切断します

Recovery Guruを使用して問題からリカバリします

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ている最初の問題を選択し、リカバリ手順 の手順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。表示された問題ごとに、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場合があります。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。概要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の複数の障害も1つの問題として表示されます。

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、ストレージアレイのアイコンは最終的に要注意から最適に変わります。一部の問題では、再構築などの処理の実行中に修正中の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。

   このファイルは'recovery-guru -yyyy-mm-dd-hh-mm-smm.html'という名前でブラウザのDownloadsフォルダに保存されます

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。

よくある質問です

サポートされているブラウザ

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	八九
Mozilla Firefox	8時80分
Safari	14
Microsoft Edge の場合	90

どのようなキーボードショートカットを使用できますか？

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。	タブをクリックする
前の項目に移動する。	Shift + Tabキーを押します
アイテムを選択します。	入力するコマンド
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—項目を切り替える	下矢印または上矢印

アクション	キーボードショートカット
拡張可能なテキスト—項目を展開または縮小します。	入力するコマンド

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
上または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。	ページアップしてください
次の月に移動する。	ページダウン
前の年に移動する。	Ctrl + Page Upキーを押します
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 +右矢印をクリックします
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。	入力するコマンド
日付ピッカーを閉じて日付を消去します。	Ctrl / Command + End

アクション	キーボードショートカット
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値との関係はどうなっていますか？

プールとボリュームグループの統計は、リザーブ容量用ボリュームを含むすべてのボリュームの集計によって計算されます。

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は、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と表示される場合は、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。オブジェクトのI/Oアクティビティが発生すると、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、特定のオブジェクトのデータポイント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がインポート中である。 • 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どのような情報が表示されますか？

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、論理ビュー、物理ビュー、アプリケーションとワークロードのビューの各タブに表示されます。

レイテンシとは、データの読み取りや書き込みが行われるとき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のグラフは何を示していますか。

CPUグラフには、各コントローラ（コントローラAおよびコントローラ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して使用されているCPU処理容量の割合が表示されます。外部I/Oが発生していないときでもCPU利用率がゼロにならないことがあります。これは、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ためです。グラフの特定のポイントにカーソルを合わせると、その時点における使用中の処理能力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機能に関連したものです。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、その時点におけるコントローラAとコントローラBの残りのIOPSおよびMiB/秒容量の割合が表示されます

表示環境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。

- 容量値を表示する際のデフォルトの単位については、を参照してください "容量値のデフォルトの単位を設定します"。
- パフォーマンスグラフを表示する際のデフォルト期間については、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を設定します"。

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の形式にすることができます。

プールとボリュームグループとは何ですか？

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、ホストにアクセス可能なボリュームを作成することができます。

詳細はこちら。

- "プールとボリュームグループの仕組み"

- "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します"

プールの作成方法

System Managerを使用すると、ストレージアレイの未割り当て容量を検出したときにプールを自動的に作成できます。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。

詳細はこちら。

- "プールの自動作成と手動作成"
- "プールを自動的に作成する"
- "プールを手動で作成する"
- "プールまたはボリュームグループに容量を追加します"

ボリュームグループの作成方法

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]

詳細はこちら。

- "ボリュームグループを作成します"
- "プールまたはボリュームグループに容量を追加します"

関連情報

プールとボリュームグループ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。

- "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仕組み

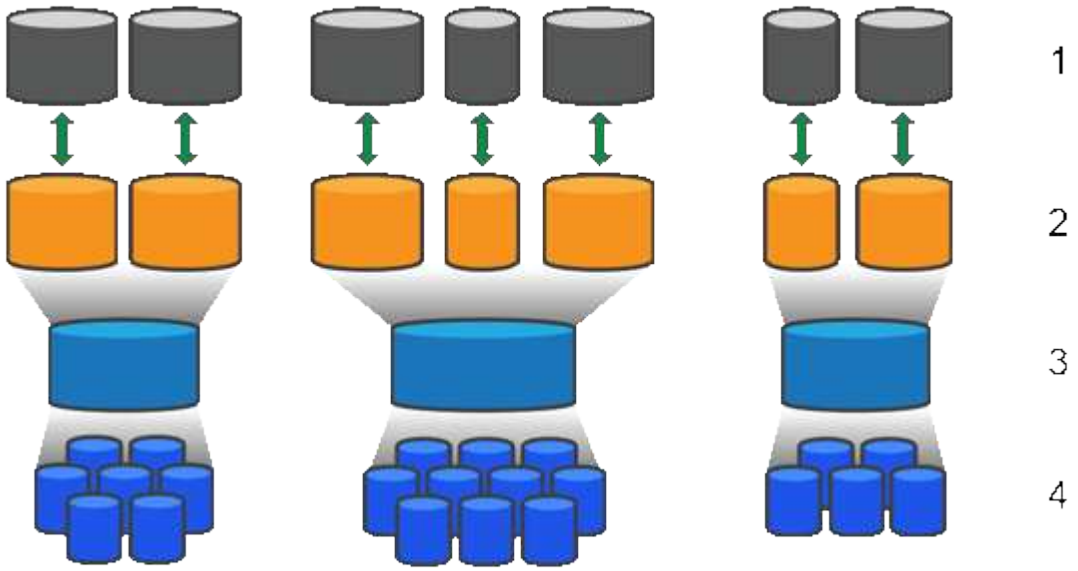
ストレージをプロビジョニングするには、ストレージアレイで使用するハードディスクドライブ（HDD）またはソリッドステートディスク（SSD）ドライブを含むプールまたはボリュームグループを作成します。

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

理可能な区分に分割します。これらの論理区分内に、データが格納される個々のボリュームまたはLUNがあります。次の図に、この概念を示します。



^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、まず次の処理を実行して使用可能なドライブ容量をさまざまなホストに提供します。

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

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

プール

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

プール機能はワンランク上のRAIDとして機能します。基盤となるRAIDアーキテクチャが仮想化されるため、リビルド、ドライブ拡張、ドライブ障害への対応といったタスクの処理に最適なパフォーマンスと柔軟性が提供されます。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。

ドライブが一致しません

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

ます。

障害ドライブの管理

プールの最小容量は11ドライブですが、1本のドライブ分の容量が、ドライブ障害時のスペア容量として予約されます。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、一定量の容量が緊急用に保持されます。この容量はSystem Manager内のドライブ数で表されますが、実際の実装はドライブのプール全体に分散されます。保持されるデフォルトの容量は、プール内のドライブの数に基づきます。

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

ボリュームグループ

ボリュームグループは、ストレージシステム内で容量をボリュームに割り当てる方法を定義します。ディスクドライブはRAIDグループにまとめられ、ボリュームは1つのRAIDグループ内の複数のドライブにまたがって実装されます。したがって、ボリュームグループの設定により、グループに含まれるドライブと、使用されているRAIDレベルが特定されます。

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

ドライブが一致しません

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

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

障害ドライブの管理

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

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

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利用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	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の形式でホストに容量として提示されます。 各ホストには独自のLUNアドレススペースがあります。したがって、同じLUNを複数のホストで使用して、異なるボリュームにアクセスできます。
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、ホストにアクセス可能な 1 つ以上のボリュームを作成することができます。（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）。
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。各ボリュームのSnapshotイメージが作成されますが、すべてのイメージが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あり、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ごとに容量と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、ホストにアクセス可能な1つ以上のボリュームを作成することができます。（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るさまざまなタイプの容量を示しています。

容量タイプ	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、ストレージアレイ内の容量のうち、プールまたはボリュームグループに割り当てられている容量です。この容量は、ボリュームの作成、およびコピーサービス処理とストレージオブジェクトのさまざまな容量ニーズ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。
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キャッシュ機能では、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します

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。どちらが適しているかは、主に、予想されるI/Oワークロードなどの主要なストレージ要件、パフォーマンス要件、データ保護要件によって決まります。

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

- ドライブのリビルド時間を短縮し、ストレージ管理を簡易化する必要がある場合、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が発生している場合。
- 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レベルは設定または変更できません。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

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

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

プール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	良好です
シーケンシャルワークロード	良好です	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）	良い：小さなブロックのランダムワークロードに最適	良い：大きな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）	より良い：通常はRAID 6よりも良い	Degraded：パフォーマンスが最大40%低下します
複数のドライブ障害が発生した場合	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	速い：オンザフライでプールに追加できます	遅い：Dynamic Capacity Expansion処理が必要です
シンボリュームがサポートされます	はい。	いいえ

使用	プール	ボリュームグループ
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	○：ホットスペアやRAID設定の構成は不要	×：ホットスペアを割り当てRAIDを設定する必要があります
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で論理的にグループ化されている一連のドライブであり、ホストがアクセス可能なボリュームを作成するために使用されます。

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レベルがサポートされています	いいえSystem Managerでは常にRAID 6を使用します。	はい。RAID 0、1、10、5、6を使用可能。
シンボリュームがサポートされています	はい。	いいえ
Full Disk Encryption（FDE）がサポートされる	はい。	はい。
Data Assurance（DA）がサポートされています	はい。	はい。
シェルフ損失の保護がサポートされます	はい。	はい。
ドロワー損失の保護がサポートされます	はい。	はい。
ドライブ速度混在のサポート	同じにすることを推奨しますが、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。	同じにすることを推奨しますが、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。
ドライブ容量混在がサポートされています	同じにすることを推奨しますが、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。	同じにすることを推奨しますが、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。

機能	プール	ボリュームグループ
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本必要RAID 1または10には2本（偶数）必要。RAID 5の最小数は3RAID 6の最小数は5
ドライブの最大数	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RAID 5、6～30ドライブの最大数
ボリュームの作成時に個々のドライブを選択できます	いいえ	はい。
ボリュームの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。
ボリュームの作成時にI/O特性を指定できます	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。
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一定の割合に達したときにアラートを設定できる。	いいえ
別のストレージアレイへの移行をサポート	いいえ最初にボリュームグループに移行する必要があります。	はい。
動的セグメントサイズ（DSS）	いいえ	はい。
RAIDレベルを変更できます	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

ドライブタイプ（HDD、SSD）の混在は、プールでもボリュームグループでも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。プールの作成時に物理ドライブを追加できます。

自動作成

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、プールの自動作成が開始されます。未割り当て容量が検出されると、System Managerは1つ以上のプールを作成するか、既存のプールに未割り当て容量を追加するか、またはその両方を実行するように求めます。

プールの自動作成は、次のいずれかの条件に該当する場合に実行されます。

- プールがストレージアレイに存在せず、新しいプールの作成に十分なドライブがない。
- 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、タイプ（HDDまたはSSD）が同じで容量が同等である必要があります。次のタスクを実行するように求められます。

- タイプが十分な数のドライブがある場合は、単一のプールを作成する。
- 未割り当て容量が異なるドライブタイプで構成されている場合は、複数のプールを作成する。
- ストレージアレイにすでにプールが定義されている場合は、既存のプールにドライブを追加し、同じタイプの新しいドライブをプールに追加する。
- タイプの異なる複数のドライブを追加した場合は、ドライブタイプが同じドライブを既存のプールに追加し、別のドライブタイプのドライブを使用して別のプールを作成する。

手動作成

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

- 新しいドライブが複数のプールに追加される可能性があります。
- 1つ以上の新しいプールの候補で、シェルフ損失の保護またはドロワー損失の保護を使用できる。
- 1つ以上の現在のプールの候補で、シェルフ損失の保護またはドロワー損失の保護のステータスを維持できない。

ストレージアレイ上に複数のアプリケーションがあり、同じドライブリソースにアクセスしないようにする場合に、プールを手動で作成することもできます。この場合、1つ以上のアプリケーション用に小規模なプールを手動で作成することを検討してください。データを分散するための多数のボリュームを含む大規模なプールにワークロードを割り当てるのではなく、1~2個のボリュームだけを割り当てることができます。特定のアプリケーションのワークロード専用の個別のプールを手動で作成すると、ストレージアレイの処理をより迅速に実行でき、競合が軽減されます。

ストレージを設定する

プールを自動的に作成する

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。

作業を開始する前に

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

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

このタスクについて

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ではドライブが自動的に検出され、ドライブタイプと現在の構成に基づいて、1つまたは複数のプールを作成するように求められます。
- プールが以前に定義されている場合、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メッセージがSystem Managerで自動的に表示されます。新しいドライブを既存のプールに追加すると、System Managerによって、追加した新しいドライブを含む新しい容量にデータが自動的に再配分されます。
- EF600またはEF300ストレージアレイを設定する場合は、各コントローラが最初の12個のスロットと直近の12個のスロットに同じ数のドライブにアクセスできることを確認します。この構成により、コントローラは両方のドライブ側PCIeバスをより効果的に使用できます。

プールの自動構成（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）が同じで容量が同等の十分な数のドライブがある場合は、単一のプールが作成されます。
   - 未割り当て容量が異なるドライブタイプで構成されている場合は、複数のプールが作成されます。
   - ストレージアレイにすでにプールが定義されている場合に、そのプールにドライブタイプが同じ新しいドライブを追加すると、既存のプールにドライブが追加されます。
   - ドライブタイプが同じドライブを既存のプールに追加し、別のドライブタイプのドライブを使用して別のプールを作成する。

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

5. [* 同意する *] をクリックします。

プールを手動で作成する

プールの自動構成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。

作業を開始する前に

- ドライブタイプ（HDDまたはSSD）が同じドライブが少なくとも11本必要です。
- シェルフ損失の保護を有効にするには、プールを構成するドライブが少なくとも6つのドライブシェルフに配置されていて、同じシェルフのドライブが3本以上含まれていないことが必要です。
- ドロワー損失の保護を有効にするには、プールを構成するドライブが少なくとも5つのドロワーに同じ数ずつ配置されている必要があります。
- EF600またはEF300ストレージアレイを設定する場合は、各コントローラが最初の12個のスロットと直近の12個のスロットに同じ数のドライブにアクセスできることを確認します。この構成により、コントローラは両方のドライブ側PCIeバスをより効果的に使用できます。現在のところ、System Managerでは、ボリュームグループの作成時に詳細設定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（プールの作成）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	プールの空き容量がGiB単位で表示されます。アプリケーションのストレージニーズに応じて、必要な容量の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、空き容量に含まれることはありません。
合計ドライブ数	プール候補に含まれるドライブの数が表示されます。 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めるブロックサイズ（セクターサイズ）が表示されます。値は次のとおりです。 • 512 — 512バイトのセクターサイズ。 • 4K — 4、096バイトのセクターサイズ。
セキュリティ対応	プール候補がセキュリティ対応ドライブだけで構成されているかどうかを示します。セキュリティ対応ドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。 • プールはドライブセキュリティを使用して保護できますが、この機能を使用するには、すべてのドライブがセキュリティ対応である必要があります。 • FDEのみのプールを作成する場合は、SecureCapable列で「* Yes-fde」を検索してください。FIPSのみのプールを作成する場合は、「はい- FIPS *」または「はい- FIPS（混在）」を探します。「Mixed」は140-2と140-3レベルのドライブが混在していることを示します。これらのレベルを組み合わせて使用する場合は、プールが下位レベルのセキュリティ（140〜2）で動作することに注意してください。 • セキュリティ対応かどうかがドライブによって異なるプールや、セキュリティレベルが異なるドライブが混在したプールを作成することもできます。プールにセキュリティ対応でないドライブが含まれている場合、プールをセキュリティ対応にすることはできません。
セキュリティを有効化	セキュリティ対応ドライブでドライブセキュリティ機能を有効にするオプションです。プールがセキュリティ対応で、セキュリティキーを作成している場合、チェックボックスを選択してセキュリティを有効にできます。 一度有効にしたドライブセキュリティは、プールを削除してドライブを消去しないかぎり解除できません。

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

ボリュームグループを作成します

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同じボリュームのコンテナです。

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

作業を開始する前に

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、RAID 1を使用している場合を除き、少なくとも3台のシェルフまたはドロワーに配置されたドライブを使用するボリュームグループを作成する必要があります。最小のシェルフ/ドロワーは2台です。
- EF600またはEF300ストレージアレイがある場合にボリュームグループを手動で作成するときは、各コントローラが最初の12個のスロットと残りの12個のスロットに同数のドライブにアクセスできることを確認します。この構成により、コントローラは両方のドライブ側PCIeバスをより効果的に使用できます。現在のところ、System Managerでは、ボリュームグループの作成時に詳細設定機能でドライブを選択できます。
- ボリュームグループの容量は、選択するRAIDレベルによって次のように異なります。
  - RAID 1を使用する場合は、ドライブを一度に2本ずつ追加してミラーペアを構成する必要があります。ミラーリングとストライピング（RAID 10またはRAID 1+0）は、ドライブを4本以上選択した場合に実装されます。
  - RAID 5を使用する場合は、少なくとも3本のドライブを追加してボリュームグループを作成する必要があります。
  - RAID 6を使用する場合は、少なくとも5本のドライブを追加してボリュームグループを作成する必要があります。

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（ボリュームグループの作成）ダイアログボックスが表示されます。
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だけが表示されます。
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だけが表示されます。
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ドライブを選択できます。未割り当ての特定のドライブを選択して必要な容量を確保することができます。ストレージアレイにメディアタイプやインターフェイスタイプが異なるドライブが含まれている場合、新しいボリュームグループの作成用に選択できるのは1つのドライブタイプの未設定の容量のみです。

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	使用可能な容量がGiB単位で表示されます。アプリケーションのストレージのニーズに応じて、必要な容量のボリュームグループ候補を選択します。
合計ドライブ数	このボリュームグループに含まれるドライブの数を示します。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めるブロックサイズ（セクターサイズ）が表示されます。値は次のとおりです。 • 512 — 512バイトのセクターサイズ。 • 4K — 4、096バイトのセクターサイズ。
セキュリティ対応	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と140-3レベルのドライブが混在していることを示します。これらのレベルを組み合わせて使用する場合、ボリュームグループのセキュリティレベルは低下（140 - 2）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です。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	このグループの候補で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、プールに作成されたボリュームで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。これにより、バックグラウンドの初期化プロセスを実行せずに、ボリュームをただちに使用できます。
シェルフ損失の保護	シェルフ損失の保護が使用可能かどうかを示します。シェルフ損失の保護が有効な場合、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が使用可能かどうかを示します。この保護は、使用しているドライブシェルフにドロワーが搭載されている場合にのみ提供されます。ドロワー損失の保護が有効な場合、ドライブシェルフの1台のドロワーとの通信が完全に失われた場合でも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作成できるブロックサイズが表示されます。 • 512n — 512バイトネイティブ。 • 512e — 512バイトエミュレーション。 • 4k — 4,096バイト

手動方式のドライブの特性

特性	使用
	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の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めるブロックサイズ（セクターサイズ）が表示されます。値は次のとおりです。 • 512 — 512バイトのセクターサイズ。 • 4K — 4、096バイトのセクターサイズ。
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と140-3レベルのドライブが混在していることを示します。これらのレベルを組み合わせて使用する場合、ボリュームグループのセキュリティレベルは低下（140 - 2）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	このグループの候補でData Assurance（DA）を使用できるかどうかを示します。Data Assurance（DA）は、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、プールに作成されたボリュームで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作成できるブロックサイズが表示されます。 • 512n — 512バイトネイティブ。 • 512e — 512バイトエミュレーション。 • 4k — 4,096バイト
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。これにより、バックグラウンドの初期化プロセスを実行せずに、ボリュームをただちに使用できます。

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

その結果、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。この空き容量は追加ボリュームの作成に使用できます。この処理の実行中もボリューム内のデータには引き続きアクセスできます。

作業を開始する前に

- ドライブのステータスが最適Iである必要があります。
- ドライブタイプ（HDDまたはSSD）が同じである必要があります。
- プールまたはボリュームグループのステータスが最適である必要があります。
- 1つのボリュームグループに含めることができるボリュームの最大数は256です。
- プールで使用できる最大ボリューム数は、ストレージシステムのモデルによって異なります。
  - 2、048ボリューム（EF600およびE5700シリーズ）
  - 1、024ボリューム（EF300）
  - 512（E4000および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いずれもセキュリティ対応ドライブの場合、セキュリティ対応ドライブの暗号化機能を引き続き使用するには、セキュリティ対応のドライブだけを追加します。

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

このタスクについて

プールに一度に追加できるドライブは最大60本です。ボリュームグループに一度に追加できるドライブは最大2本です。最大数を超えるドライブを追加する必要がある場合は、手順 を繰り返します。（プールにはストレージ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。拡張処理の実行後にリザーブ容量を増やすことを検討してください。

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

手順

1. 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。

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

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

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

4. [追加（ Add ）] をクリックします。

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

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

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

ストレージを管理します

ボリュームの冗長性をチェックします

テクニカルサポートから指示があった場合やRecovery Guruに記載されている場合は、プールまたはボリュームグループ内のボリュームの冗長性をチェックし、そのボリュー

ムのデータに整合性があるかどうかを確認できます。

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

作業を開始する前に

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

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

このタスクについて

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

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

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

手順

1. 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. チェックするボリュームを選択してから'check'と入力して'この操作を実行することを確認します
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表の一番上から順番にスキャンされます。各ボリュームがスキャンされるたびに、次の操作が実行されます。

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

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を削除します

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

作業を開始する前に

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

- ボリュームグループのドライブに永続的予約が設定されていないことを確認する必要があります。

手順

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

ボリュームグループの空き容量を統合します

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

作業を開始する前に

- ボリュームグループに少なくとも1つの空き容量領域が含まれている必要があります。
- ボリュームグループ内のすべてのボリュームがオンラインで、ステータスが最適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ことを確認してください。

このタスクについて

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

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

- ボリュームグループに対して空き容量領域が1つ以上検出されると、通知領域のホームページに「空き容量の統合」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、[Pools & Volume Groups]ページから[Consolidate Free Capacity]ダイアログボックスを起動することもできます。

空き容量領域についての詳細はこちらをご覧ください

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

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

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

手順

1. 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。

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

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

   System Managerが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、以降のストレージ設定タスク用に1つの連続したブロックに統合します。

完了後

[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をエクスポート/インポートする

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、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された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**キャッシュから容量を削除する

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

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

このタスクについて

容量を削除する際のガイドラインを次に示します。

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

パフォーマンスへの影響

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

セキュリティ対応ドライブへの影響について説明します

- セキュリティ対応でない最後のドライブを削除すると、プール内に残るのはすべてセキュリティ対応のドライブになります。この場合、プールのセキュリティを有効にするオプションが表示されます。
- Data Assurance（DA）対応でない最後のドライブを削除すると、プール内に残るのはすべてDA対応のドライブになります。

このプールに作成する新しいボリュームはすべてDA対応になります。既存のボリュームをDA対応にする場合は、ボリュームを削除してから再作成する必要があります。

手順

1. 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]

   Remove Capacityダイアログボックスが表示されます。

3. リストから1つ以上のドライブを選択します。

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

プールとグループの設定を変更します

プールの設定を変更します

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

このタスクについて

このタスクでは、プールの構成設定を変更する方法について説明します。

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

設定	説明
予約済み容量（EF600またはEF300の場合は「最適化容量」）	予約済み容量-ドライブ数を定義して、ドライブ障害に備えてプールに確保されている容量を特定できます。ドライブ障害が発生すると、予約済み容量を使用して再構築されたデータが格納されます。プールのデータ再構築プロセスでは、ボリュームグループで使用されるホットスペアドライブではなく、予約済み容量が使用されます。 ドライブ数はスピンボックスで調整します。指定したドライブ数に応じて、スピンボックスの横にプールの予約済み容量が表示されます。 予約済み容量については、次の点に注意してください。 • 予約済み容量はプールの合計空き容量から差し引かれるため、確保する容量がボリュームの作成に使用できる空き容量に影響します。予約済み容量に0を指定すると、プールのすべての空き容量がボリュームの作成に使用されます。 • 予約済み容量を減らすと、プールボリュームに使用できる容量が増えます。 追加の最適化容量（EF600およびEF300アレイのみ）-プールの作成時に、使用可能容量とパフォーマンスおよびドライブ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減らすことで最小レベルの最適化容量を確保するため、ボリュームの作成には使用できません。

4. [保存（ Save ）] をクリックします。

ボリュームグループの設定を変更します

名前やRAIDレベルなど、ボリュームグループの設定を編集できます。

作業を開始する前に

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

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

手順

1. 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（ボリュームグループ設定）ダイアログボックスが表示されます。

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

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。処理の実行中は、パフォーマンスが若干低下することがあります。

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

DULBE対応ドライブの場合は、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。これにより、バックグラウンドの初期化プロセスを実行せずに、ボリュームをただちに使用できます。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（マッピング解除）、SSDの寿命が延び、書き込みパフォーマンスが最大化されます。

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。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。ただし、事前に無効にしておく必要があります。

作業を開始する前に

- EF300またはEF600ストレージアレイが必要です。
- SSDボリュームグループまたはプールが必要です。このプールでは、すべてのドライブがNVMe Deallocated or Unwritten Logical Block Error（DULBE）エラーリカバリ機能をサポートしています。そうしないと、リソースプロビジョニングオプションを使用できません。

このタスクについて

既存のボリュームグループおよびプールでリソースの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、ブロックの割り当てが解除されます。このプロセスでは、UNMAP単位で一貫した割り当てを行うためにバックグラウンド処理が必要になることがあります。この処理では、スペースについて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で未使用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。既存データはそのまま維持されます。書き込みは、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上のブロックをマッピングまたはプロビジョニングします。

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します

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、新しく作成する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。この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。これにより、バックグラウンドの初期化プロセスを実行せずに、ボリュームをただちに使用できます。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（マッピング解除）、SSDの寿命が延び、書き込みパフォーマンスが最大化されます。

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。

作業を開始する前に

- EF300またはEF600ストレージアレイが必要です。
- SSDボリュームグループまたはプールが必要です。このプールでは、すべてのドライブがNVMe Deallocated or Unwritten Logical Block Error（DULBE）エラーリカバリ機能をサポートしています。

このタスクについて

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に影響します。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。

   この設定の概要 は、リソースプロビジョニングが現在有効か無効かを示します。

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を有効または無効にすると、新しく作成する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します

プールまたはボリュームグループのドライブセキュリティを有効にして、プールまたはボリュームグループに含まれているドライブ上のデータへの不正アクセスを防止できます。ドライブの読み取りおよび書き込みアクセスは、セキュリティキーが設定されたコントローラからのみ可能です。

作業を開始する前に

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

このタスクについて

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

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

手順

1. 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。

   [セキュリティの有効化の確認]ダイアログボックスが表示されます。

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キャッシュを管理する

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キャッシュとプライマリキャッシュ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経由で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、データはホスト読み取り後に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。ユーザがアクセスすることはできず、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つのボリュームも含まれます。

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では、低レイテンシのドライブにデータが配置されるため、以降そのデータに対して要求があった場合の応答速度が大幅に向上します。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加するほど、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するとシステム全体の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がリード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キャッシュで検出されない場合は、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

最もアクセスされるデータ（ホットスポット）をSSDキャッシュにコピーすると、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キャッシュに対して実行されるため、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キャッシュを実装する

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による転送の対象外となります。

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を次に示します。

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による転送の対象外となります。
- 現在、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キャッシュが有効になっているボリュームや無効になっているボリュームをインポートまたはエクスポートしても、キャッシュデータはインポートまたはエクスポートされません。
- 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キャッシュを作成する

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

作業を開始する前に

ストレージアレイにSSDドライブが含まれている必要があります。

このタスクについて

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内にあるため、ストレージアレイを使用するすべてのアプリケーションでキャッシュが共有されます。キャッシュするボリュームを選択すると、あとは動的に自動でキャッシングが実行されます。

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。
- SSDキャッシュはストレージアレイごとに1つだけサポートされます。
- 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で決まります。
- SSDキャッシュはSnapshotイメージではサポートされません。
- SSDキャッシュが有効になっているボリュームや無効になっているボリュームをインポートまたはエクスポートしても、キャッシュデータはインポートまたはエクスポートされません。
- コントローラのSSDキャッシュを使用するように割り当てられたボリュームは、自動ロードバランシングによる転送の対象外となります。
- 関連するボリュームがセキュリティ有効の場合は、セキュリティ有効のSSDキャッシュを作成してください。

手順

1. 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	使用可能な容量がGiB単位で表示されます。アプリケーションのストレージニーズに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で決まります。SSDキャッシュに最大容量を超える容量を割り当てた場合、超過した容量は使用できません。 SSDキャッシュの容量は、全体の割り当て容量にカウントされます。
合計ドライブ数	このSSDキャッシュで使用できるドライブの数を示します。必要なドライブ数のSSD候補を選択します。

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です。セキュリティ有効SSDキャッシュを作成する場合は、セキュリティの有効化チェックボックスをオンにします。 一度有効にした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。

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

6. [作成（ Create ）] をクリックします。

SSDキャッシュの設定を変更する

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

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

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

4. [保存（ Save ）] をクリックします。

SSDキャッシュの統計を表示します

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

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

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

手順

1. 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）]

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

フィールドの詳細

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

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。

リザーブ容量を管理します

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、以下のコピーサービスオブジェクトによって使用される、基盤となるストレージメカニズムです。

- Snapshotグループ
- 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
- ミラーペアボリューム

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、データがボリュームに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、リザーブ容量に関して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が自動的に失敗状態に移行することはありません。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処理は常にCheck Conditionを要求元ホストに返します。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を使用して再初期化されます。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。

容量アラート

コピーサービスオブジェクトには、容量の警告およびアラートのしきい値を設定可能で、リザーブ容量がフルの場合の応答も設定可能です。

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フルに近付くと、アラートが送信されます。デフォルトでは、このアラートはリザーブ容量ボリュームの使用率が75%に達したときに発行されます。ただし、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を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とは、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にコピーサービス処理のデータを保存しなくなったボリュームのことです。コピーサービスオブジェクトが削除されたときは、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。リザーブ容量ボリュームの削除に失敗しました。

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では、孤立したリザーブ容量ボリュームについて、ホームページの通知領域に「再利用未使用容量」というメッセージが表示されます。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。

リザーブ容量を増やします

ストレージオブジェクトに対する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ている容量であるリザーブ容量を増やすことができます。

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。一般には、ストレージオブジェクトのリザーブ容量がフルに近付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。

作業を開始する前に

- 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。

このタスクについて

次のストレージオブジェクトの場合、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見込まれる場合や、特定のコピーサービス処理のライフサイクルが非常に長くなる場合は、リザーブ容量の割合を高くします。

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が含まれているプールまたはボリュームグループに空き容量が存在せず、ストレージアレイに未割り当ての容量がある場合は、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上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。

リザーブ容量を削減します

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、整合性グループメンバーボリュームの各ストレージオブジェクトのリザーブ容量を削減します。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。

作業を開始する前に

- 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のボリュームでないことを確認する必要があります。
- ストレージオブジェクトがSnapshotボリュームの場合は、Snapshotボリュームの状態がDisabled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、関連付けられたSnapshotイメージが含まれていないことを確認する必要があります。

このタスクについて

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後の新しいリザーブ容量を表示します。
- Snapshotボリュームの容量を削減すると、System ManagerはSnapshotボリュームの状態を自動的に無効に移行します。無効の場合、Snapshotボリュームは現在Snapshotイメージに関連付けられておらず、したがってI/O処理用にホストに割り当てることはできません

Snapshotグループのリザーブ容量の設定を変更します

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	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。ユーザが設定できます。	Snapshotスケジュール
「はい」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
アラートの送信しきい値	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	説明
リザーブ容量がフルになったときの処理です	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
グループで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。シックボリュームの場合もシンボリュームの場合もあり、通常はホストに割り当てられています。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イメージ

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を変更します

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	説明
アラートの送信しきい値	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を変更します

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。

このタスクについて

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設定を適宜変更します。

フィールドの詳細

設定	説明
アラートの送信しきい値	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ときの処理です	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の設定を変更する

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設定を適宜変更します。

フィールドの詳細

設定	説明
アラートの送信しきい値	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**イメージをキャンセルします

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。同期処理が完了した時点でSnapshotイメージが作成されます。

このタスクについて

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個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グループを削除します

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、リザーブ容量が解放され、プールやボリュームグループで再利用できるようになります。

このタスクについて

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

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. 確認のため’delete]と入力します

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。

よくある質問です

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ごとに容量と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、ホストにアクセス可能な1つ以上のボリュームを作成することができます。（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）。

プールとは何ですか？

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、ホストにアクセス可能な 1 つ以上のボリュームを作成することができます。（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タイミングを判断する必要がなくなり、従来のようなディスクサイズの変更に伴うシステム停止もありません。プールの容量が不足してきたらシステムを停止せずにプールにドライブを追加することができ、ホストには透過的に容量が拡張されます。

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がプール全体に分散されるため、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再構築に使用できます。このアプローチでは専用のホットスペアドライブは使用されません。代わりに、予約済み（スペア）容量がプール全体で確保されます。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。その後、新しいドライブが選択されて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るため、ドライブ間のデータ分散は維持されます。

リザーブ容量とは何ですか？

リザーブ容量は物理的に割り当てられた容量で、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の格納に使用されます。

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パスしたドライブです。

FIPSのサポートが必要なボリュームには、FIPSドライブのみを使用します。ボリュームグループまたはプールにFIPSドライブとFDEドライブが混在している場合、すべてのドライブがFDEドライブとして扱われます。また、FIPSドライブのみを含むボリュームグループまたはプールでは、FDEドライブを追加したりスペアとして使用したりすることはできません。

冗長性チェックとは何ですか？

冗長性チェックでは、プールまたはボリュームグループ内のボリューム上のデータに整合性があるかどうかが判別されます。冗長性データは、プールまたはボリュームグループ内のいずれかのドライブで障害が発生した場合に、交換用ドライブに迅速に情報を再構築するために使用されます。

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

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

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

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、同じ一連のドライブに格納されるボリュームグループ内のデータとは異なり、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。

- プールの方がドライブ障害時のパフォーマンスの低下と再構築にかかる時間が少なくなります。
- 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RAIDレベルを指定する必要はありません。

プールを手動で設定するのはどのような場合ですか？

プールを手動で設定する理由を、次の例に示します。

- ストレージアレイ上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と同じドライブリソースの競合が発生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規模なプールを手動で作成することを検討してください。

  データを分散するための多数のボリュームを含む大規模なプールにワークロードを割り当てるのではなく、1~2個のボリュームだけを割り当てることができます。特定のアプリケーションのワークロード専用の個別のプールを手動で作成すると、ストレージアレイの処理をより迅速に実行でき、競合が軽減されます。

  プールを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を自動的に推奨でき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、プールにドライブを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、容量不足による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、アラート通知の設定を指定します。必要に応じて、デフォルトの設定をそのまま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は、予約済み容量を増やせないことがあります。

予約済み容量は、ドライブ障害に備えてプール内に確保されている容量（ドライブ数）です。プールが作成されると、プール内のドライブ数に応じて自動的にデフォルトの予約済み容量が確保されます。使用可能なすべての容量でボリュームを作成している場合は、ドライブを追加するかボリュームを削除してプールに容量を追加しないと、予約済み容量を増やすことはできません。

予約済み容量は* 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複数のドライブに分散されますが、予約するときはドライブ数で指定します。

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。

ドライブでサポートされているメディアタイプを教えてください。

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、既存のプールまたはボリュームグループに容量を追加できるドライブがすべて表示されるわけではありません。

ドライブを追加できない理由は次のとおりです。

- 未割り当てで、セキュリティ有効でないドライブを指定する必要があります。すでに別のプールやボリュームグループに含まれているドライブ、またはホットスペアとして設定されているドライブは使用できません。未割り当てだが、セキュリティ有効なドライブは、手動で消去すると使用可能になります。
- 最適な状態でないドライブは使用できません。
- 容量が小さすぎるドライブは使用できません。
- プールまたはボリュームグループ内でドライブのメディアタイプが一致している必要があります。次のものを混在させることはできません。
  - ソリッドステートディスク（SSD）搭載のハードディスクドライブ（HDD）
  - NVMeとSASドライブ
  - ボリュームブロックサイズが512バイトおよび4KiBのドライブ
- プールまたはボリュームグループに含まれているドライブがすべてセキュリティ対応の場合は、セキュリティ対応でないドライブは表示されません。

- プールまたはボリュームグループに含まれているドライブがすべて連邦情報処理標準（FIPS）ドライブの場合、非FIPSドライブは表示されません。
- プールまたはボリュームグループに含まれているドライブがすべてData Assurance（DA）対応で、プールまたはボリュームグループにDA有効ボリュームが1つ以上ある場合は、DA非対応のドライブは使用できないためプールまたはボリュームグループに追加できません。ただし、プールまたはボリュームグループにDA有効ボリュームがない場合は、DA非対応のドライブをプールまたはボリュームグループに追加できます。DA対応と非対応のドライブが混在している場合は、DA対応ボリュームを作成できないことに注意してください。

ストレージアレイの容量は、新しいドライブを追加するか、プールまたはボリュームグループを削除することで増やすことができます。

シェルフ/ドロワー損失の保護を維持するにはどうすればよいですか？

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

レベル	シェルフ/ドロワー損失の保護の基準	必要なシェルフ/ドロワーの最小数
プール	シェルフの場合、プールに同じシェルフのドライブが3本以上含まれない。 ドロワーの場合、プールに各ドロワーから同数のドライブが含まれている。	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すべて別々のシェルフまたはドロワーに配置されている。	3.
RAID 1	ミラーペア内のドライブがそれぞれ別のシェルフまたはドロワーに配置されている。	2.
RAID 0	シェルフ/ドロワー損失の保護は実現できない。	該当なし

プールまたはボリュームグループですでにドライブに障害が発生している場合は、シェルフ/ドロワー損失の保護は維持されません。この状況で、ドライブシェルフまたはドロワーへのアクセス、さらにその結果プールまたはボリュームグループ内の別のドライブへのアクセスを失うと、データが失われます。

プールとボリュームグループの最適なドライブ配置は何ですか？

プールおよびボリュームグループを作成するときは、ドライブの選択範囲を上下のドライブスロットに合わせて調整してください。

EF600およびEF300コントローラの場合、ドライブスロット0 11は1つのPCIブリッジに接続され、スロット12 23は別のPCIブリッジに接続されます。最適なパフォーマンスを確保するには、ドライブを選択した際に、上下のスロットから同数のドライブを選択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短い時間で帯域幅の上限に達しないようにすることができます。

アプリケーションに最適な**RAID**レベルはどれですか？

ボリュームグループのパフォーマンスを最大限に高めるには、適切なRAIDレベルを選択する必要があります。適切なRAIDレベルを特定するには、ボリュームグループにアクセスしているアプリケーションでの読み取りと書き込みの割合を把握します。これらの割合を取得するには、[パフォーマンス]ページを使用します。

RAIDレベルとアプリケーションパフォーマンス

RAIDには、_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レベルごとにパフォーマンス機能が異なります。読み取り比率が高いアプリケーションの場合、RAID 5ボリュームまたはRAID 6ボリュームを使用するとパフォーマンスが向上します。これは、RAID 5およびRAID 6構成の読み取りパフォーマンスが優れているためです。

読み取り比率が低い（書き込み中心の）アプリケーションの場合、RAID 5ボリュームまたはRAID 6ボリュームでは同様のパフォーマンスを実現できません。パフォーマンスの低下は、コントローラがデータと冗長性データをRAID 5ボリュームグループまたはRAID 6ボリュームグループのドライブに書き込む方法に起因します。

次の情報に基づいてRAIDレベルを選択します。

- RAID 0 *
- * 概要 *
  - 冗長性なし、ストライピングモード。
- 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データをストライピングします。
- データ保護機能
  - 高可用性が求められる場合、RAID 0は推奨されません。RAID 0は重要度の低いデータに適しています。
  - ボリュームグループ内の1本のドライブで障害が発生すると、関連付けられているすべてのボリュームで障害が発生し、すべてのデータが失われます。
- 必要なドライブ数
  - RAIDレベル0には少なくとも1本のドライブが必要です。
  - RAID 0ボリュームグループには30本を超えるドライブを含めることができます。
  - ストレージアレイのすべてのドライブを含むボリュームグループを作成できます。
- RAID 1またはRAID 10 *

- * 概要 *
  - ストライピング/ミラーモード。
- どのように機能するか
  - RAID 1では、ディスクミラーリングを使用して、2本のディスクに同時にデータが書き込まれます。
  - RAID 10は、ドライブストライピングを使用して、複数のミラーリングされたドライブペアにデータをストライピングします。
- データ保護機能
  - RAID 1とRAID 10は、ハイパフォーマンスと最高のデータ可用性を提供します。
  - RAID 1とRAID 10は、ドライブミラーリングを使用して、あるドライブから別のドライブにまったく同じコピーを作成します。
  - ドライブペアの一方のドライブで障害が発生した場合、ストレージアレイはデータやサービスを失うことなくもう一方のドライブに即座に切り替えることができます。
  - 単一ドライブ障害が発生すると、関連付けられているボリュームはデグレード状態になります。ミラードライブがデータへのアクセスを許可します。
  - ボリュームグループ内のドライブペアで障害が発生すると、関連付けられているすべてのボリュームで障害が発生し、データが失われる可能性があります。
- 必要なドライブ数
  - RAID 1には、ユーザデータ用に1本、ミラーデータ用に1本、合計2本以上のドライブが必要です。
  - 4本以上のドライブを選択すると、ボリュームグループ全体でRAID 10が自動的に設定されます。ユーザデータ用にドライブが2本、ミラーデータ用にドライブが2本です。
  - ボリュームグループのドライブ数は偶数でなければなりません。ドライブ数が偶数ではなく未割り当てのドライブが残っている場合は、「* Pools & Volume Groups」に移動してボリュームグループにドライブを追加し、処理を再試行します。
  - RAID 1とRAID 10のボリュームグループは、30本を超えるドライブで構成できます。ストレージアレイのすべてのドライブを含むボリュームグループを作成できます。
- RAID 5 *
- * 概要 *
  - 高I/Oモード。
- どのように機能するか
  - ユーザデータと冗長性情報（パリティ）が複数のドライブにストライピングされます。
  - 冗長性情報を格納するために、ドライブ1本分の容量が使用されます。
- データ保護機能
  - RAID 5ボリュームグループで1本のドライブに障害が発生すると、関連付けられているすべてのボリュームがデグレード状態になります。冗長な情報があるので、データには引き続きアクセスできます。
  - RAID 5ボリュームグループで複数のドライブに障害が発生すると、関連付けられているすべてのボリュームに障害が発生し、すべてのデータが失われます。
- 必要なドライブ数
  - ボリュームグループには最低3本のドライブが必要です。

- 通常、ボリュームグループのドライブ数は最大30本に制限されます。

- RAID 6 *
- * 概要 *
  - 高I/Oモード。
- どのように機能するか
  - ユーザデータと冗長性情報（デュアルパリティ）が複数のドライブにストライピングされます。
  - 冗長性情報を格納するために、ドライブ2本分の容量が使用されます。
- データ保護機能
  - RAID 6ボリュームグループで1本または2本のドライブに障害が発生すると、関連付けられているすべてのボリュームがデグレード状態になりますが、冗長性情報があるためデータには引き続きアクセスできます。
  - RAID 6ボリュームグループで3本以上のドライブに障害が発生すると、関連付けられているすべてのボリュームに障害が発生し、すべてのデータが失われます。
- 必要なドライブ数
  - ボリュームグループには最低5本のドライブが必要です。
  - 通常、ボリュームグループのドライブ数は最大30本に制限されます。

プールのRAIDレベルは変更できません。ユーザーインタフェースは'プールを自動的にRAID 6として構成します

RAIDレベルとデータ保護

RAID 1、RAID 5、およびRAID 6は、フォールトトレランス用に冗長性データをドライブメディアに書き込みます。冗長性データには、データのコピー（ミラー）、またはデータから導出されたエラー修正コードがあります。ドライブで障害が発生した場合は、冗長性データを使用して交換用ドライブに迅速に情報を再構築できます。

単一のボリュームグループ全体で単一のRAIDレベルを設定します。そのボリュームグループの冗長性データは、すべてボリュームグループ内に格納されます。ボリュームグループの容量は、メンバードライブのアグリゲート容量から冗長性データ用に確保された容量を引いた値です。冗長性を確保するために必要な容量は、使用するRAIDレベルによって異なります。

Data Assuranceとは何ですか？

Data Assurance（DA）はT10 Protection Information（PI）標準を実装しています。I/Oパスでデータが転送される際に発生する可能性のあるエラーをチェックして修正することで、データの整合性が向上します。

Data Assurance機能の一般的な用途として、コントローラとドライブ間のI/Oパスがチェックされます。DA機能はプールおよびボリュームグループのレベルで提供されます。

この機能を有効にすると、ボリューム内の各データブロックに巡回冗長検査（CRC）と呼ばれるエラーチェック用のコードが付加されます。データブロックが移動されると、ストレージアレイはこれらのCRCコードを使用して、転送中にエラーが発生したかどうかを判断します。破損している可能性があるデータはディスクに書き込まれず、ホストにも返されません。DA機能を使用する場合は、新しいボリュームを作成するとき

にDAに対応したプールまたはボリュームグループを選択します（プールとボリュームグループの候補の表で「DA」の横の「はい」を探します）。

これらのDA対応ボリュームは、必ずDAに対応したI/Oインターフェイスを使用しているホストに割り当ててください。DAに対応したI/Oインターフェイスには、ファイバチャネル、SAS、iSCSI over TCP/IP、NVMe/FC、NVMe/IB、 NVMe/RoCEとiSER over InfiniBand（iSCSI Extensions for RDMA/IB）：SRP over InfiniBandではDAはサポートされていません。

セキュリティ対応（ドライブセキュリティ）とは何ですか？

ドライブセキュリティは、セキュリティ有効ドライブをストレージアレイから取り外したときに、そのドライブ上のデータへの不正アクセスを防止する機能です。対応するドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。

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？

一般に、リザーブ容量がフルに近付いてい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処理の場合、リザーブ容量は通常ベースボリュームの40%です。非同期ミラーリング処理のリザーブ容量は、一般に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は、ストレージオブジェクトのリザーブ容量を削減できません。

- ストレージオブジェクトがミラーペアのボリュームである。
- 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つしかない。ストレージオブジェクトには、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になっているSnapshotボリュームである。
- ストレージオブジェクトに関連付けられているSnapshotイメージが含まれている。

リザーブ容量のボリュームは、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整合性グループの各メンバーボリュームには、参照先の整合性グループSnapshotイメージに影響を与えずに、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。リザーブ容量を使用すると、読み取り/書き込み用のメンバーボリュームに含まれているデータのコピーに、ホストアプリケーションが書き込みアクセスすることができます。

整合性グループのSnapshotイメージにホストから直接読み取りや書き込みを行うことはできません。Snapshotイメージには、ベースボリュームから取得されたデータのみが保存されます。

読み取り/書き込み用の整合性グループSnapshotボリュームの作成中に、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って、ホストアプリケーションは、整合性グループのSnapshotイメージに含まれているデータのコピーに書き込みアクセスすることができます。

SSDキャッシュのすべての統計情報を表示するにはどうすればよいですか？また、何が

SSDキャッシュについては、一般統計と詳細統計を表示できます。一般統計は詳細統計のサブセットです。

詳細統計は’すべてのSSD統計を.csvファイルにエクスポートした場合にのみ表示できます統計を確認および解釈する際には、複数の統計を組み合わせることで見えてくる情報もあることに注意してください。

一般統計

SSDキャッシュの統計を表示するには、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]公称統計はView SSD Cache Statistics（SSDキャッシュ統計の表示）ダイアログに表示されます。

次に、詳細統計のサブセットである、一般統計の一覧を示します。

一般統計	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	説明
キャッシュヒット率（%）	キャッシュヒット数を読み取りと書き込みの合計数で割った値。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%より高いことが必要です。この値が小さい場合は、次のような状況が考えられます。 • 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です。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、SSDキャッシュ容量を小さくしても同レベルのパフォーマンスが得られる可能性があります。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割合は、通常は100%より小さく、多くの場合はるかに小さくなります。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はサブブロックと呼ばれる小さい単位に分割され、それぞれ独立して使用されるため、この値は100%より小さくなります。この値が大きいほど一般には有効ですが、小さい数値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。これらの追加統計は一般統計とともに保存されますが、一般統計とは異なり、View SSD Cache Statistics（SSDキャッシュ統計の表示）ダイアログには表示されません。詳細統計は'.csvファイルに統計をエクスポートした後にのみ表示できます

「.csv」ファイルを表示するときに、詳細統計が一般統計の後にリストされていることに注目してください。

詳細統計	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。
完全ヒットブロック	キャッシュヒットのブロック数。この値は、SSDキャッシュから完全に読み込まれたブロックの数を示します。SSDキャッシュがパフォーマンスの向上に効果があるのは、フルキャッシュヒットである処理に対してのみです。

詳細統計	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キャッシュ内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、キャッシュされている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、キャッシュヒットに比べて、部分ヒットとミスの数が増えることが予想されます。
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、キャッシュヒットに比べて、部分ヒットとミスの数が増えることが予想されます。
ミス-ブロック	ミスしたブロックの数。
取り込み処理（ホスト読み取り）	ベースボリュームからSSDキャッシュへ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キャッシュへ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処理によってキャッシュが一杯にならないキャッシュ設定では、取り込み処理（ホスト書き込み）の数が0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。効果的なキャッシュでは、再利用の回数は、読み取り処理と書き込み処理の合計数よりも少なくする必要があります。リサイクル処理の回数が読み取りと書き込みの合計数に近づいている場合、SSDキャッシュがスラッシングしています。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	説明
使用可能なバイト数	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、空の場合と、ベースボリュームのデータが含まれている場合があります。
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。使用可能なバイト数、割り当て済みバイト数、およびユーザデータのバイト数を使用して、キャッシュ割り当ての割合とキャッシュ利用率の割合が計算されます。

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減らすことで最小レベルの最適化容量を確保するため、ボリュームの作成には使用できません。

プールの作成時に、パフォーマンス、ドライブの寿命、使用可能容量のバランスに基づいて、推奨される最適化容量が決定されます。プール設定ダイアログにある追加の最適化容量スライダを使用して、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。

追加の最適化容量スライダは、EF600およびEF300ストレージシステムに対してのみ使用できます。

ボリュームグループの最適化容量とは何ですか？

SSDドライブでは、その容量の一部が未割り当ての場合に寿命が長くなり、最大書き込みパフォーマンスが向上します。

ボリュームグループに関連付けられているドライブの未割り当て容量は、ボリュームグループの空き容量（ボリュームで使用されていない容量）と、使用可能容量のうちの最適化容量として確保された容量で構成されます。この最適化容量は使用可能容量を減らすことで最小レベルの最適化容量を確保するため、ボリュームの作成には使用できません。

ボリュームグループの作成時に、パフォーマンス、ドライブの寿命、使用可能容量のバランスに基づいて、推奨される最適化容量が決定されます。ボリュームグループ設定ダイアログの最適化容量のスライダを使用して、ボリュームグループの最適化容量を調整できます。スライダを動かすことで、使用可能容量を犠牲にしてパフォーマンスの向上とドライブ寿命の延長を図るか、またはパフォーマンスとドライブ寿命を犠牲にして使用可能容量を増やすことができます。

追加の最適化容量スライダは、EF600およびEF300ストレージシステムに対してのみ使用できます。

リソースプロビジョニング機能とは何ですか？

リソースプロビジョニングは、EF300およびEF600ストレージアレイで使用できる機能です。これにより、バックグラウンドの初期化プロセスを実行せずに、ボリュームをただちに使用できます。

リソースプロビジョニングボリュームは、SSDグループまたはプール内のシックボリュームです。ボリュームの作成時にはドライブ容量が割り当てられますが（ボリュームに割り当てられます）、ドライブブロックは割り当て解除されます（マッピング解除されます）。これに対し、従来のシックボリュームでは、Data Assurance保護情報のフィールドを初期化し、各RAIDストライプでデータとRAIDパリティの整合性を確保するために、すべてのドライブブロックがバックグラウンドボリューム初期化処理中にマッピングまたは割り当てられます。リソースプロビジョニングボリュームでは、時間制限付きのバックグラウンド初期化は実行されません。代わりに、各RAIDストライプは、ストライプ内のボリュームブロックへの最初の書き込み時に初期化されます。

リソースプロビジョニングボリュームはSSDボリュームグループおよびプールでのみサポートされます。グループまたはプール内のすべてのドライブでNVMeのDeallocated or Unwritten Logical Block Error（DULBE）エラーリカバリ機能がサポートされます。リソースでプロビジョニングされたボリュームを作成すると、そのボリュームに割り当てられていたすべてのドライブブロックが割り当て解除（マッピング解除）されます。また、ホストではNVMe Dataset Managementコマンドまたは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の消耗度が改善され、書き込みパフォーマンスが最大化されます。向上率はドライブのモデルと容量によって異なります。

リソースでプロビジョニングされるボリューム機能について、どのような点に注意する必要がありますか？

リソースプロビジョニングは、EF300およびEF600ストレージアレイで使用できる機能です。これにより、バックグラウンドの初期化プロセスを実行せずに、ボリュームをただちに使用できます。

リソースプロビジョニングボリュームは、SSDグループまたはプール内のシックボリュームです。ボリュームの作成時にはドライブ容量が割り当てられますが（ボリュームに割り当てられます）、ドライブブロックは割り当て解除されます（マッピング解除されます）。これに対し、従来のシックボリュームでは、Data Assurance保護情報のフィールドを初期化し、各RAIDストライプでデータとRAIDパリティの整合性を確保するために、すべてのドライブブロックがバックグラウンドボリューム初期化処理中にマッピングまたは割り当てられます。リソースプロビジョニングボリュームでは、時間制限付きのバックグラウンド初期化は実行されません。代わりに、各RAIDストライプは、ストライプ内のボリュームブロックへの最初の書き込み時に初期化されます。

リソースプロビジョニングボリュームはSSDボリュームグループおよびプールでのみサポートされます。グループまたはプール内のすべてのドライブでNVMeのDeallocated or Unwritten Logical Block Error（DULBE）エラーリカバリ機能がサポートされます。リソースでプロビジョニングされたボリュームを作成すると、そのボリュームに割り当てられていたすべてのドライブブロックが割り当て解除（マッピング解除）されます。また、ホストではNVMe Dataset Managementコマンドまたは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の消耗度が改善され、書き込みパフォーマンスが最大化されます。向上率はドライブのモデルと容量によって異なります。

DULBEがサポートされているシステムでは、リソースプロビジョニングがデフォルトで有効になっています。このデフォルト設定は、* 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際には、ワークロードを選択して特定のアプリケーション用のストレージアレイ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何ですか？

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。ボリュームが複数のドライブで構成される場合でも、ホスト側では1つの論理コンポーネントとして認識され、ボリュームを定義したら、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。

詳細はこちら。

- "ボリュームの仕組み"
- "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内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。

詳細はこちら。

- "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"
- "ボリュームを作成します"
- "ワークロードにボリュームを追加する"

関連情報

ボリュームに関連する概念の詳細：

- "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

ボリュームの仕組み

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。

ストレージアレイ上の使用可能なストレージ容量からボリュームを作成して、システムのリソースを簡単に編成して使用することができます。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、すばやく簡単にアクセスできるようにすることに似ています。

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

プール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、次に示す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の際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、無駄な容量の割り当てを回避し、ストレージの初期コストを削減できます。ただし、シックボリュームが作成されるとすべてのストレージが一度に割り当てられるため、完全なプロビジョニングのメリットとしてはレイテンシの低下が挙げられます。

> ⓘ 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、格納されるデータのタイプに基づいて独自の特性があります。たとえば、次のような特性があります。

- セグメントサイズ-セグメントは、あるドライブに格納されるデータの量（KiB）です。この量に達すると、ストライプ（RAIDグループ）内の次のドライブへと進みます。セグメントサイズは、ボリュームグループの容量と同じかそれよりも小さくなります。プールのセグメントサイズは固定で、変更することはできません。

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

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

- わかりやすい名前--ボリュームに任意の名前を付けることができますが、わかりやすい名前にすることをお勧めします。

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

ワークロードの仕組み

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

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

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

ワークロードのタイプ

アプリケーション固有とその他の2種類のワークロードを作成できます。

- アプリケーション固有。アプリケーション固有のワークロードを使用してボリュームを作成する場合、アプリケーションワークロードのI/Oとアプリケーションインスタンスからの他のトラフィックの競合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。I/Oタイプ、セグメントサイズ、コントローラ所有権、読み取り/書き込みキャッシュなどのボリューム特性が自動的に推奨され、次の

アプリケーションタイプ用に作成されるワークロードに合わせて最適化されます。

- Microsoft®SQL Server™
- 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）

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

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

アプリケーションとワークロードの表示

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

- ボリュームのタイルで「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定期的に収集することで、ベースラインとなる数値を設定して傾向を分析することができ、I/Oパフォーマンスに関する問題の調査に役立ちます。

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	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、ホストに報告される容量がレポート容量で、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が割り当て容量となります。

期間	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です。アプリケーションごとに、サポートするワークロードを1つ以上定義します。一部のアプリケーションについては、ストレージを最適化するボリューム構成が自動的に提示されます。ボリューム構成には、I/Oタイプ、セグメントサイズ、コントローラ所有権、読み取りと書き込みのキャッシュなどの特性が含まれます。
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の不均衡が解消されます。自動ロードバランシングはI/Oワークロードを自動的に分散する機能を提供し、ホストからの受信I/Oトラフィックは動的に管理されて両方のコントローラに分散されます。
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。このキャッシングにより、以降のデータ要求にキャッシュから対応できる可能性が高まります。動的キャッシュ読み取りプリフェッチは、シーケンシャルI/Oを使用するマルチメディアアプリケーションで重要ですデータがキャッシュにプリフェッチされる速度と量は、ホスト読み取りの速度と要求サイズに基づいて自動で調整されます。ランダムアクセスの場合、原因 データがキャッシュにプリフェッチされることはありません。この機能は、読み取りキャッシュが無効になっている場合は適用されません。 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以内に制限されます。たとえば、ボリュームグループに合計15GiBの空き容量があり、最も大きい空き容量領域が10GiBであるとすると、作成できるボリュームのサイズは最大10GiBです。 空き容量を統合すると、追加ボリュームを作成する際にボリュームグループ内の空き容量を最大限使用できるようになります。
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	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、RAID 1、RAID 3、RAID 5、またはRAID 6のボリュームグループに含まれるボリュームで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の形式でホストに容量として提示されます。 各ホストには独自のLUNアドレススペースがあります。したがって、同じLUNを複数のホストで使用して、異なるボリュームにアクセスできます。
メディアスキャン	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をスキャンします。
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、ストレージアレイでは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、ホストにアクセス可能な 1 つ以上のボリュームを作成することができます。（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、ストレージアレイ内の容量のうち、プールまたはボリュームグループに割り当てられている容量です。この容量は、ボリュームの作成、およびコピーサービス処理とストレージオブジェクトのさまざまな容量ニーズ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、ホストに報告される容量がレポート容量で、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が割り当て容量となります。

期間	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。セグメントサイズは、ボリュームグループの容量と同じかそれよりも小さくなります。プールのセグメントサイズは固定で、変更することはできません。
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。データフローを一定のサイズのブロック（「ブロックサイズ」）に分割し、このブロックを各ドライブに1つずつ順に書き込みます。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ごとに容量と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、ホストにアクセス可能な1つ以上のボリュームを作成することができます。（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またはインスタンスを定義できます。一部のアプリケーションでは、特性が似たボリュームで構成されるようにワークロードが設定されます。これらのボリューム特性は、ワークロードがサポートするアプリケーションのタイプに基づいて最適化されます。たとえば、Microsoft SQL Serverアプリケーションをサポートするワークロードを作成し、そのワークロード用のボリュームを作成すると、Microsoft SQL Serverをサポートするようにボリューム特性が最適化されます。
書き込みキャッシュ	書き込みキャッシュは、ドライブにまだ書き込まれていないホストからのデータを格納するバッファです。書き込みキャッシュ内のデータは、ドライブに書き込まれるまで保持されます。書き込みキャッシュにより、I/Oパフォーマンスを向上させることができます。

期間	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では、一方のコントローラのキャッシュメモリに書き込まれたデータがもう一方のコントローラのキャッシュメモリにも書き込まれます。そのため、一方のコントローラで障害が発生した場合、もう一方のコントローラで未処理の書き込み処理をすべて完了できます。書き込みキャッシュのミラーリングは、書き込みキャッシュが有効で、2台のコントローラが配置されている場合にのみ使用できます。ミラーリングありの書き込みキャッシュは、ボリュームの作成時にデフォルトで設定されます。
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では、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。

シンボリュームに固有の用語

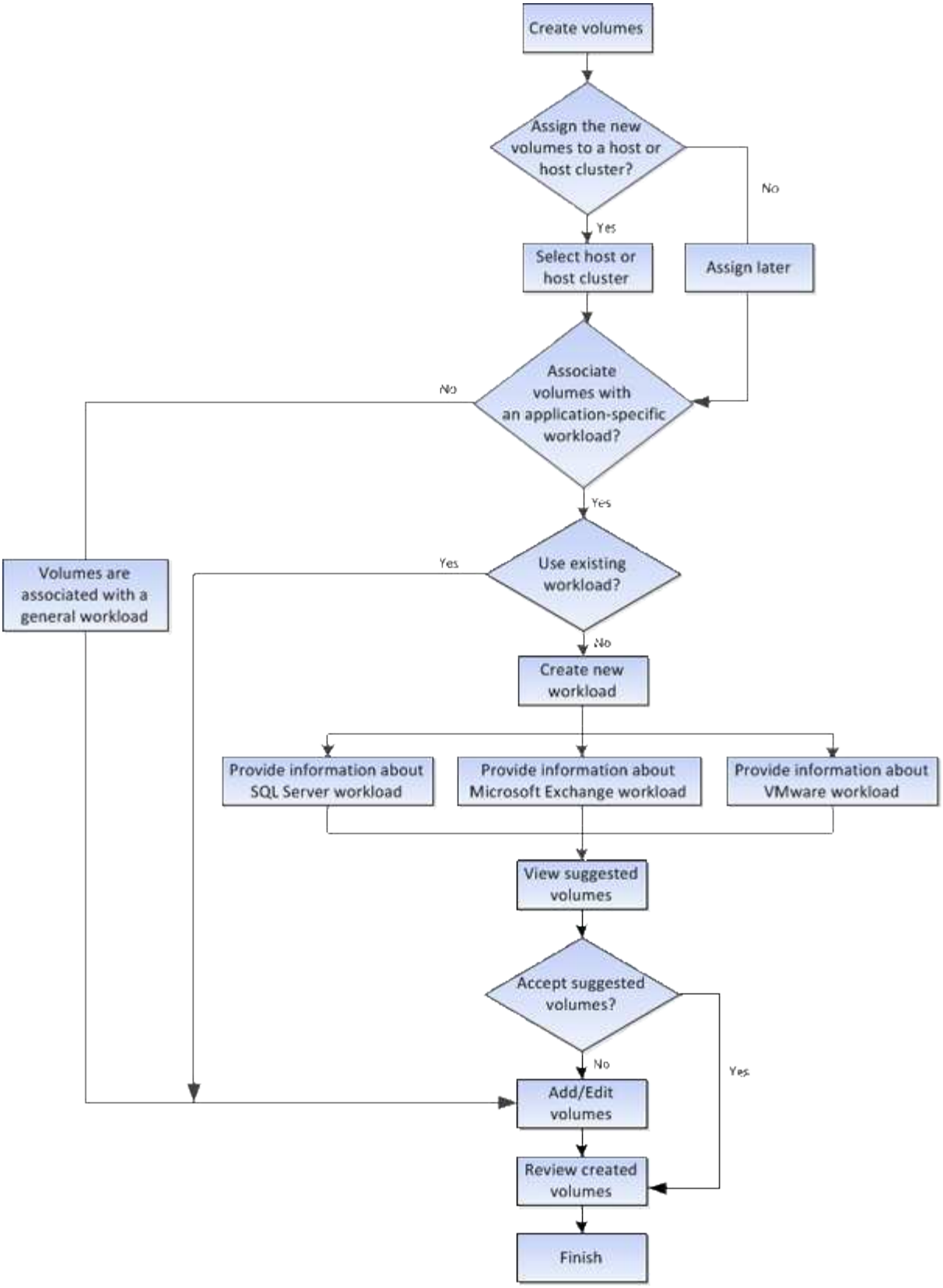
System Managerには、シンボリュームを作成するオプションはありません。シンボリュームを作成する場合は、コマンドラインインターフェイス（CLI）を使用します。

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。

期間	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、ボリューム内の各データブロックに巡回冗長検査（CRC）と呼ばれるエラーチェック用のコードが付加されます。データブロックが移動されると、ストレージアレイはこれらのCRCコードを使用して、転送中にエラーが発生したかどうかを判断します。破損している可能性があるデータはディスクに書き込まれず、ホストにも返されません。DA機能を使用する場合は、新しいボリュームを作成するときにDAに対応したプールまたはボリュームグループを選択します（プールとボリュームグループの候補の表で「DA」の横の「はい」を探します）。

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）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。ドライブごとに固有の暗号化キーがあり、このキーを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ドライブの両方を含めることができますが、暗号化機能を使用するためにはすべてのドライブがセキュリティ対応である必要があります。

ドライブセキュリティを実装する方法

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ドライブのみを含むボリュームグループまたはプールでは、FDEドライブを追加したりスペアとして使用したりすることはできません）。
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することができます。外部キー管理の場合、キー管理サーバとの間に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、コントローラによってセキュリティキーが適用され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ために、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ソリッドステートディスク（SSD）ドライブで構成されます。

個のボリューム

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キャッシュに対して実行されるため、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、データはホスト読み取り後に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。ユーザがアクセスすることはできず、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つのボリュームも含まれます。

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による転送の対象外となります。

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、再配置など、さまざまな処理を実行できます。 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

容量を拡張

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。また、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場合は、ソースボリュームとターゲットボリュームの2つの個別のボリュームのポイントインタイムコピーを同じストレージアレイに作成します。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。

初期化します

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、最初に作成されるときに自動的に初期化されます。ただし、一定の障害状況からリカバリするために、ボリュームを手動で初期化するようRecovery Guruから指示される場合があります。ボリュームを初期化しても、ボリュームのWWN、ホストの割り当て、割り当て済み容量、およびリザーブ容量の設定は保持されます。Data Assurance（DA）設定とセキュリティ設定も同じままです。

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に問題が発生した場合、マルチパスドライバがボリュームを優先コントローラ所有者から移動します。

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

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

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]

ボリューム所有権を変更します

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、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セカンダリボリュームの所有者も自動的に変更されます。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を変更すると、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転送されます。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。

ボリュームとボリュームの所有権をコピーします

ボリュームのコピー処理中は、同じコントローラがソースボリュームとターゲットボリュームの両方を所有している必要があります。ボリュームの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自動的にソースボリュームの優先コントローラに転送されます。ボリュームのコピーが完了または停止すると、ターゲットボリュームの所有権は元の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、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）。

キャッシュ設定を変更します

キャッシュメモリは、ドライブメディアよりも速くアクセスできる、コントローラ上の一時的な揮発性ストレージ（RAM）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が以前の処理からすでにキャッシュに格納されている可能性があるため、ドライブへのアクセスが不要になります。
- 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。書き込みキャッシュ内のデータは、ドライブに書き込まれるまで保持されます。書き込みキャッシュにより、I/Oパフォーマンスを向上させることができます。

- 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ングにより、以降のデータ要求にキャッシュから対応できる可能性が高まります。動的キャッシュ読み取りプリフェッチは、シーケンシャルI/Oを使用するマルチメディアアプリケーションで重要ですデータがキャッシュにプリフェッチされる速度と量は、ホスト読み取りの速度と要求サイズに基づいて自動で調整されます。ランダムアクセスの場合、原因 データがキャッシュにプリフェッチされることはありません。この機能は、読み取りキャッシュが無効になっている場合は適用されません。

  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。このスキャンにより、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ても、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、データが失われることはありません。

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

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。そのボリュームで冗長性チェックも有効になっている場合、ボリュームに冗長性情報があるかぎり、ボリューム内の冗長性情報とデータの整合性がチェックされます。メディアスキャンでの冗長性チェックは、ボリュームの作成時にデフォルトで有効になります。

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

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

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

容量を使用したボリュームの作成と拡張

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

- 未割り当て容量からボリュームを作成する場合は、プールまたはボリュームグループとボリュームを同時に作成できます。
- 空き容量からボリュームを作成する場合は、既存のプールまたはボリュームグループに追加のボリュームを作成します。

ボリュームの容量を拡張したら、それに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のどちらかを作成できます。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済みの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るスペースは、ホストに報告されるスペースと同じです。

  通常は、シックボリュームのレポート容量を、ボリュームが拡張すると予想される最大容量に設定します。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、割り当てられているためです。

- シンボリュームの場合、ホストに報告される容量がレポート容量で、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が割り当て容量となります。

  レポート容量は、ストレージアレイ上の割り当て容量よりも大きくなる場合があります。現在使用可能な資産に関係なく、シンボリュームの拡張に合わせ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であり、最大容量はプールまたはボリュームグループ内のドライブの数と容量で決まります。

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

- 小数点以下3桁まで指定できます（例：65.375GiB）。
- ボリュームグループで使用可能な最大値以下の容量を指定してください。

  ボリュームを作成する場合は、セグメントサイズの動的（DSS）変更のための追加容量が事前に割り当てられます。DSS変更は、ボリュームのセグメントサイズを変更できるソフトウェアの機能です。

- 一部のホストオペレーティングシステムでは、2TiBを超えるボリュームがサポートされます（最大レポート容量はホストオペレーティングシステムで決定されます）。実際には、一部のホストオペレーティングシステムでサポートされるのは最大128TiBのボリュームです。詳細については、ホストオペレーティングシステムのドキュメントを参照してください。

シンボリュームの容量制限

レポート容量が多く、割り当て容量が比較的少な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や効率性に効果的です。シンボリュームを使用すると、アプリケーションの実行を中断することなく、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拡張できるため、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ています。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
報告済み	32MiB	256TiB です
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により、シンボリュームの自動拡張をレポート容量までに制限できます。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。スペース不足の場合は、シンボリュームについてだけでなく、プールの容量を必要とす

る他の処理（SnapshotイメージやSnapshotボリュームなど）について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し、容量不足が発生するのを回避できます。

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。

- シンボリュームで自動的に拡張可能な割り当て容量を制限する制限を定義します。
- シンボリュームが最大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	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を見越して、大容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上で事前に割り当てられたボリューム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、スペースが使用されず、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てしまわないように注意してください。スペースが不足すると、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。 • シンボリュームの作成には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は割り当てられず、必要に応じてあとから提供されます。 • シンボリュームのサイズは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、つまり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できます）。 • シンプロビジョニングブロックのスペース再生（UNMAP）では、ホストからSCSI UNMAPコマンドを実行し、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改善され、リソースがより効率的に使用されます。

シンボリュームの制限事項

シンボリュームでは、次の例外を除いて、シックボリュームと同じ処理がすべてサポートされます。

- シンボリュームのセグメントサイズは変更できません。

- シンボリュームでは読み取り前冗長性チェックを有効にできません。
- シンボリュームはコピーボリューム処理のターゲットボリュームとして使用できません。
- シンボリュームの割り当て容量の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だけで変更できます。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

あらゆる種類のアプリケーションのワークロードを作成できます。

このタスクについて

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

手順

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

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

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。

完了後

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。

ボリュームを作成します

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

このタスクについて

ほとんどのアプリケーションタイプでは、ユーザが定義した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る手順 です。

手順1：ボリュームのホストを選択します

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

作業を開始する前に

- 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で DA をサポートしていないホスト接続が使用されている場合、関連付けられているホストからは DA 対応ボリュームのデータにアクセスできません。

このタスクについて

ボリュームを割り当てる際は、次のガイドラインに注意してください。

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

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

手順

1. 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. ボリュームを割り当てるホストまたはホストクラスタをドロップダウンリストから選択するか、ホストまたはホストクラスタをあとで割り当てるように選択します。
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続行するには、* Next *をクリックしてに進みます [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ない場合は、「Other application」を選択します。

このタスクについて

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。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。
- _"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ていない場合は、「Other」エントリのいずれかを選択します。
     - 作成するワークロードの名前を入力します。
2. 「 * 次へ * 」をクリックします。
3. ワークロードがサポート対象のアプリケーションタイプに関連付けられている場合は、要求された情報を入力します。それ以外の場合は、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」のアプリケーションのいずれかを選択した場合は、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。

作業を開始する前に

- プールまたはボリュームグループに十分な空き容量が必要です。
- 1つのボリュームグループに含めることができるボリュームの最大数は256です。
- プールで使用できる最大ボリューム数は、ストレージシステムのモデルによって異なります。
  - 2、048ボリューム（EF600およびE5700シリーズ）
  - 1、024ボリューム（EF300）
  - 512（E4000および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を選択しています

DA対応ボリュームを作成する場合は、DAに対応したプールまたはボリュームグループを選択します（プールとボリュームグループの候補テーブルで「DA」の横にある「* Yes」を探します）。

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、エラーがある場合には検出されて修正されます。

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

- セキュリティ有効ボリュームを作成するには、ストレージアレイのセキュリティキーを作成する必要があります。

セキュリティ対応のプールまたはボリュームグループを選択しています

セキュリティ有効ボリュームを作成する場合は、セキュリティ対応のプールまたはボリュームグループを選択します（プールとボリュームグループの候補テーブルで、「セキュリティ対応」の横にある「はい」*を探します）。

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

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

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

このタスクについて

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。対象となる各プールおよびボリュームグループについて、使用可能なドライブの数と合計空き容量が表示されます。

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

手順

1. 他のワークロード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	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単位（ MiB 、 GiB 、または TiB ）を定義します。シックボリュームの場合、最小容量は1MiBであり、最大容量はプールまたはボリュームグループに含まれるドライブの数と容量で決まります。 コピーサービス（Snapshotイメージ、Snapshotボリューム、ボリュームコピー、およびリモートミラー）用のストレージ容量も必要であることに注意してください。そのため、 標準ボリュームにすべての容量を割り当てないでください。 プールの容量は、ドライブの種類に応じて4GiBまたは8GiB単位で割り当てられます。4GiBまたは8GiBの倍数でない容量を割り当てた場合、その容量は使用できません。全容量を使用できるようにするため、4GiB単位または8GiB単位で容量を指定してください。使用不可容量が存在する場合、その容量を使用するにはボリュームの容量を増やすしかありません。
ボリュームのブロックサイズ（EF300およびEF600のみ）	ボリュームに対して作成できるブロックサイズが表示されます。 • 512 — 512バイト • 4k — 4,096バイト

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

フィールド	説明
ダ	• 「 DA 」の横には、プールまたはボリュームグループのドライブで Data Assurance （ DA ）がサポートされている場合にのみ「 Yes 」と表示されます。 DA を使用すると、ストレージシステム全体のデータの整合性が向上します。DA を使用すると、データがコントローラ経由でドライブに転送される際にストレージアレイがエラーの有無をチェックできます。新しいボリュームに DA を使用すると、すべてのエラーが検出されます。
リソースのプロビジョニング（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。これにより、バックグラウンドの初期化プロセスを実行せずに、ボリュームをただちに使用できます。

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

フィールドの詳細

フィールド	説明
ボリューム名	ボリュームには、作成時に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単位（ MiB 、 GiB 、または TiB ）を定義します。シックボリュームの場合、最小容量は1MiBであり、最大容量はプールまたはボリュームグループに含まれるドライブの数と容量で決まります。 コピーサービス（Snapshotイメージ、Snapshotボリューム、ボリュームコピー、およびリモートミラー）用のストレージ容量も必要であることに注意してください。そのため、 標準ボリュームにすべての容量を割り当てないでください。 プールの容量は、ドライブの種類に応じて4GiBまたは8GiB単位で割り当てられます。4GiBまたは8GiBの倍数でない容量を割り当てた場合、その容量は使用できません。全容量を使用できるようにするため、4GiB単位または8GiB単位で容量を指定してください。使用不可容量が存在する場合、その容量を使用するにはボリュームの容量を増やすしかありません。
ボリュームタイプ	アプリケーション固有のワークロード用に作成されたボリュームのタイプを示します。
ボリュームのブロックサイズ（EF300およびEF600のみ）	ボリュームに対して作成できるブロックサイズが表示されます。 • 512 — 512バイト • 4k — 4,096バイト

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

フィールド	説明
セキュリティ対応	*「Secure Capable」の横には、プールまたはボリュームグループ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ドライブの両方を含めることができますが、暗号化機能を使用するためにはすべてのドライブがセキュリティ対応である必要があります。
ダ	• 「 DA 」の横には、プールまたはボリュームグループのドライブで Data Assurance （ DA ）がサポートされている場合にのみ「 Yes 」と表示されます。 DA を使用すると、ストレージシステム全体のデータの整合性が向上します。DA を使用すると、データがコントローラ経由でドライブに転送される際にストレージアレイがエラーの有無をチェックできます。新しいボリュームに DA を使用すると、すべてのエラーが検出されます。
リソースのプロビジョニング（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。これにより、バックグラウンドの初期化プロセスを実行せずに、ボリュームをただちに使用できます。

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

完了後

- 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のオペレーティングシステムに対して必要な変更を行います。
- オペレーティングシステム固有のユーティリティ（サードパーティベンダーから入手可能）を実行してから、SMcliコマンドを実行します。 `-identifyDevices` ボリューム名をホストストレージアレイ名に関連付けるには、次の手順を実行します。

  SMcliは、SANtricityシステムマネージャから直接使用できます。このダウンロード可能バージョンのSMcliは、E4000、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。

ワークロードにボリュームを追加する

ワークロードに現在関連付けられていないボリュームについて、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することができます。

このタスクについて

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

手順

1. 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。そのワークロードに関連付けられているアプリケーションタイプが、追加するボリュームに割り当てられます。

   - 新しいワークロードにボリュームを追加--アプリケーションタイプの新しいワークロードを定義して新しいワークロードにボリュームを追加するには、このオプションを選択します。
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（ボリュームの選択）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。

ボリュームを管理します

ボリュームの容量を拡張します

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

作業を開始する前に

- ボリュームの関連付けられたプールまたはボリュームグループに十分な空き容量が必要です。
- ボリュームが最適状態で、変更中の状態ではありません。
- シンボリュームのレポート容量が最大値の256TiBに達していない必要があります。
- ボリュームでホットスペアドライブが使用されていない必要があります。（ボリュームグループ内のボリュームにのみ適用されます）。

ボリューム容量は一度に最大128TiBまで拡張できます。

このタスクについて

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で今後必要になる容量を考慮してください。Snapshotイメージ、Snapshotボリューム、またはリモートミラーを十分に作成できる空き容量があることを確認してください。

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

手順

1. 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内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 ）、またはテビバイト（ TiB ）のいずれかで表示するように容量の値を変更で

きます。

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。

完了後

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

ボリュームを初期化

ボリュームは、最初に作成されるときに自動的に初期化されます。ただし、一定の障害状況からリカバリするために、ボリュームを手動で初期化するようRecovery Guruから指示される場合があります。このオプションを使用する場合は、必ずテクニカルサポートの指示に従ってください。初期化するボリュームは1つ以上選択できます。

作業を開始する前に

- すべてのI/O処理を停止しておきます。
- 初期化するボリューム上のデバイスまたはファイルシステムをすべてアンマウントしておく必要があります。
- ボリュームは最適ステータスであり、ボリューム上で変更処理が実行されていません。

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の指示があった場合を除き、この処理は実行しないでください。この手順 を開始する前に、テクニカルサポートにお問い合わせください。

このタスクについて

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

次のタイプのボリュームは初期化できません：

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

このトピックは、プールまたはボリュームグループから作成された標準のボリュームのみに該当します。

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

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がクリアされます。これにより、書き込み前のブロックはゼロで埋められているかのように読み取られます（ボリュームは完全に空のように表示されます）。

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。

ボリュームを再配置する

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

作業を開始する前に

- 再配置するボリュームが使用中でない必要があります。使用中の場合はI/Oエラーが発生します。
- 再配置するボリュームを使用しているすべてのホストにマルチパスドライバがインストールされている必要があります。インストールされていない場合はI/Oエラーが発生します。

  ホストにマルチパスドライバがインストールされていないボリュームを再配置する場合は、再配置処理の実行中に_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。

このタスクについて

ほとんどのホストマルチパスドライバは、優先コントローラ所有者へのパスで各ボリュームへのアクセスを試みます。ただし、この優先パスが使用できなくなると、ホストのマルチパスドライバは代替パスにフェイルオーバーします。このフェイルオーバー原因 によって、ボリューム所有権が代替コントローラに変更される可能性があります。フェイルオーバーの原因となった状況を解決すると、一部のホストではボリュームの所有権が優先コントローラ所有者に自動的に戻りますが、場合によっては手動でのボリュームの再配置が必要になります。

手順

1. 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を変更する

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

作業を開始する前に

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

このタスクについて

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

手順

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

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。ボリュームへのI/Oが、このI/Oパス経由で転送されるようになります。
- マルチパスドライバが新しいパスを認識するように再設定されるまで、ボリュームで新しいI/Oパスが使用されない場合があります。この処理にかかる時間は通常5分未満です。

ボリュームを削除します

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。

作業を開始する前に

削除するボリュームで、次の点を確認します。

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

このタスクについて

次のいずれかの条件に該当する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になった場合を除き、セグメントサイズの変更などの変更処理を実行中です。
- ボリュームにいずれかのタイプの永続的予約が設定されている。
- ボリュームがボリュームコピー処理のソースボリュームまたはターゲットボリュームで、処理のステータスが「保留」、「実行中」、または「失敗」である。

ボリュームを削除すると、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。

   ボリュームの削除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の制限を変更します

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の場合、シンボリュームが自動的に拡張できる割り当て容量を制限する制限を変更できます。

また、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により、シンボリュームの自動拡張をレポート容量までに制限できます。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が消費するスペースを考慮してください。

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。

   [境界を変更（Change Limit）]ダイアログボックスが表示され選択したシンボリュームの割り当て容量の上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. 必要に応じて、割り当て容量の制限と警告しきい値を変更します。

   フィールドの詳細

設定	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できなくなる容量のしきい値。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。
アラートの送信しきい値 （警告しきい値）	シンボリュームが割り当て容量の上限に近付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オンにします。アラートは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。

設定を管理します

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

作業を開始する前に

変更するボリュームのステータスは「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（ボリューム設定）ダイアログボックスが表示されます。選択したボリュームの設定がこのダイアログボックスに表示されます。

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

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

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

設定	説明
キャッシュ	キャッシュ設定が表示されます。この設定を変更すると、ボリュームの全体的なI/Oパフォーマンスを向上させることができます。
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の読み取り時間が速くなるため、アプリケーションパフォーマンスが向上します。読み取りキャッシュはストレージアレイ内にあるため、ストレージアレイを使用するすべてのアプリケーションでキャッシュが共有されます。キャッシュするボリュームを選択すると、あとは動的に自動でキャッシングが実行されます。

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。

完了後

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。

ワークロードの設定を変更する

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

読み取りキャッシュと書き込みキャッシュの設定を変更して、ボリュームの全体的なI/O

パフォーマンスを調整することができます。

このタスクについて

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

- [キャッシュ設定の変更]ダイアログボックスを開いた後、選択したキャッシュプロパティの横にアイコンが表示されることがあります。このアイコンは、コントローラがキャッシュ処理を一時的に停止したことを示しています。

  この処理は、新しいバッテリを充電しているとき、コントローラが削除されたとき、またはコントローラによってキャッシュサイズの不一致が検出された場合に発生します。この状況が解消されると、ダイアログボックスで選択したキャッシュプロパティがアクティブになります。選択したキャッシュプロパティがアクティブにならない場合は、テクニカルサポートにお問い合わせください。

- キャッシュ設定は、単一のボリュームまたはストレージアレイ上の複数のボリュームに対して変更できます。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に対して同時にキャッシュ設定を変更することができます。

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

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	説明
読み取りキャッシュ	読み取りキャッシュは、ドライブから読み取られたデータを格納するバッファです。読み取り処理の対象となるデータが以前の処理ですでにキャッシュに格納されていれば、ドライブにアクセスする必要はありません。読み取りキャッシュのデータは、フラッシュされるまで保持されます。
書き込みキャッシュ	書き込みキャッシュは、ドライブにまだ書き込まれていないホストからのデータを格納するバッファです。書き込みキャッシュ内のデータは、ドライブに書き込まれるまで保持されます。書き込みキャッシュにより、I/Oパフォーマンスを向上させることができます。 キャッシュは、ボリュームに対して*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。アドバンストキャッシュ設定は、シックボリュームに対してのみ使用できます。

フィールドの詳細

キャッシュ設定	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。このキャッシングにより、以降のデータ要求にキャッシュから対応できる可能性が高まります。動的キャッシュ読み取りプリフェッチは、シーケンシャルI/Oを使用するマルチメディアアプリケーションで重要ですデータがキャッシュにプリフェッチされる速度と量は、ホスト読み取りの速度と要求サイズに基づいて自動で調整されます。ランダムアクセスの場合、原因 データがキャッシュにプリフェッチされることはありません。この機能は、読み取りキャッシュが無効になっている場合は適用されません。 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では、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では、一方のコントローラのキャッシュメモリに書き込まれたデータがもう一方のコントローラのキャッシュメモリにも書き込まれます。そのため、一方のコントローラで障害が発生した場合、もう一方のコントローラで未処理の書き込み処理をすべて完了できます。書き込みキャッシュのミラーリングは、書き込みキャッシュが有効で、2台のコントローラが配置されている場合にのみ使用できます。ミラーリングありの書き込みキャッシュは、ボリュームの作成時にデフォルトで設定されます。 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を変更します

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

作業を開始する前に

次の点を理解しておきます

- メディアスキャンは、スキャンする容量とスキャン期間に基づいて一定の速度で継続的に実行されます。優先度の高いバックグラウンドタスク（再構築など）によってバックグラウンドスキャンが一時的に中断されることはありますが、その場合も同じ速度で再開されます。
- ボリュームは、ストレージアレイとそのボリュームでメディアスキャンオプションが有効になっている場合にのみスキャンされます。そのボリュームで冗長性チェックも有効になっている場合、ボリュームに冗長性情報があるかぎり、ボリューム内の冗長性情報とデータの整合性がチェックされます。メディアスキャンでの冗長性チェックは、ボリュームの作成時にデフォルトで有効になります。
- スキャン中に回復不能なメディアエラーが発生した場合、可能であれば、冗長性情報を使用してデータが修復されます。

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

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

デフォルトのメディアスキャン期間は120日に設定されています。

このタスクについて

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

次の操作を実行できます。

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

手順

1. 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]。

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

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。

コピーサービスを使用する

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の2つのボリュームを同じストレージアレイ上に作成して、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。

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じになるように、ソースボリュームからターゲットボリュームに1バイトずつデータがコピーされます。

データをコピーすることでアクセスを向上

ボリュームのストレージ要件が変わった場合、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ことが可能です。

- 大容量ドライブにデータを移動
- データ転送速度が速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を加える。
- シンボリュームをシックボリュームに変更する。

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。

シンボリュームをシックボリュームに変更する

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。

データをバックアップする

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の別のボリュームにコピーすることで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をソースボリュームのバックアップとして使用して、システムテストを実施したり、テープドライブなどの別のデバイスにバックアップしたりできます。

Snapshotボリュームのデータをベースボリュームにリストアします

ベースボリュームのデータを関連付けられたSnapshotボリュームのデータから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ボリューム上に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。

ボリュームコピー処理のタイプ

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って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て、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。これは、手順 が完了するまでターゲットボリューム上のデータが整合性のない状態になるためです。

オフラインおよびオンラインのボリュームコピー処理について以下で説明します。

オフラインのボリュームコピー処理です

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間の関係です。オフラインコピーは、ソースボリュームからデータを読み取り、そのデータを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を一時停止するのは、時間の経過による不整合がターゲットボリュームで発生しないようにするためです。

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場合、オフラインコピーに参加しているソースボリュームは読み取り専用の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が完了したあとで許可されます。 • 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ために、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は、ソースボリュームに対する読み取り要求の問題 処理がストレージアレイコントローラから拒否されて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のドライバは、読み取り要求の問題 処理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。この状況により、ソースボリュームが書き込み禁止であることを示すエラーメッセージが表示される場合があります。 • この問題 が実行されないようにするために、ボリュームコピー処理のステータスが実行中のときは、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関係は、Snapshotボリュームとターゲットボリューム間の関係です。ソースボリュームがオンラインになっていて、データの書き込みに使用できる場合は、ボリュームコピー処理を開始できます。そのためには、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します。

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Snapshotイメージ間のコピー関係を作成します。Snapshotイメージをソースボリュームとして使用すると、ストレージアレイでは、コピーの実行中も引き続きソースボリュームへの書き込みを行うことができます。

オンラインコピー処理中は、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も呼ばれます。このボリュームには、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を使用する必要があります。 • ターゲットボリュームには、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を使用できます。ターゲットボリュームに、シンボリュームやSnapshotグループ内のベースボリュームを使用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すると、シンボリュームから同じストレージアレイにある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	• コピー元として使用するSnapshot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、Snapshotは無効になり、ベースボリュームのパフォーマンスが元に戻ります。Snapshot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	• Snapshot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。 • Snapshot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Snapshotごとに、そのSnapshot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、Snapshotイメージの管理にのみ使用されます。

オンラインコピー処理に関する重要なポイント	
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管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そのデータブロック内の元のデータのコピーが格納されるため、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Snapshotの作成時刻以降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。

ボリュームをコピーする

ボリュームのデータを同じストレージアレイ内の別のボリュームにコピーすることで、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。

作業を開始する前に

- 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過去にボリュームコピー処理で使用したことがある場合、そのデータが不要になったか、またはデータをバックアップしたことになります。

このタスクについて

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。ボリュームコピーが開始されると、ソースボリュームのデータがターゲットボリュームに丸ごとコピーされます。

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のボリュームです。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にはソースボリュームと同じかそれ以上の容量が必要です。ただし、RAIDレベルは同じである必要はありません。

オンラインコピーとオフラインコピーについて

オンラインコピー

オンラインコピーは、ストレージアレイ内のボリュームのポイントインタイムコピーを作成します。コピーの実行中も、そのボリュームへの書き込みを継続できます。そのためには、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します。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

オフラインコピーは、ソースボリュームからデータを読み取り、そのデータを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を一時停止するのは、時間の経過による不整合がターゲットボリュームで発生しないようにするためです。オフラインボリュームコピーの関係は、ソースボリュームとターゲットボリューム間の関係です。

ボリュームコピー処理はターゲットボリュームのデータを上書きし、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します。

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. データをコピーす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、ターゲットボリュームとして使用できるすべてのボリュームが表示されます。

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。

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

コピー優先度を最低速度に設定すると、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。コピー優先度が最高のレートに設定されている場合は、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。

   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の完了後、ターゲットボリュームはホストに対して自動的に読み取り専用になります。

完了後

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して実行します

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	説明
停止します	ステータスが実行中、保留、または失敗である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されると、マッピングされた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上のデータはソースボリューム上のデータと一致しなくなります。
優先度を変更します	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までの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上の既存のデータが上書きされます。この操作は、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失敗します。
クリア	ステータスが実行中、保留、または失敗である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。確認ダイアログはありません。

よくある質問です

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。ボリュームが複数のドライブで構成される場合でも、ホスト側では1つの論理コンポーネントとして認識され、

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にもかかわらず、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以内に制限されます。たとえば、ボリュームグループに合計15GiBの空き容量があり、最も大きい空き容量領域が10GiBであるとすると、作成できるボリュームのサイズは最大10GiBです。

ボリュームグループ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と、追加ボリュームを作成する際にボリュームグループ内の空き容量を最大限使用できるようになります。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に対して空き容量領域が1つ以上検出されると、通知領域のホームページに「空き容量の統合」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。

最も大きい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）を使用します。

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

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

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

- 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）

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

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

ボリュームがワークロードに関連付けられていないのはなぜですか？

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

選択したワークロードを削除できないのはなぜですか？

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

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

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

アプリケーションとは、SQL ServerやExchangeなどのソフトウェアです。アプリケーションごとに、サポートするワークロードを1つ以上定義します。

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り、ワークロードとストレージアレイコンポーネントとの連携方法が決まります。

ユーザが指定したワークロード情報に基づいて、System Managerは適切なボリュームを作成し、システム上に現在存在する使用可能なプールまたはボリュームグループに配置します。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。

拡張後の容量を認識させるにはどうすればよいですか？

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

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

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

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

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。

以下は、プールまたはボリュームグループを使用できない理由です。

- プールまたはボリュームグループのData Assurance（DA）機能が一致しない。
- 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る。

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該当し、プールには該当しません。

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際には、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、一般に小さなセグメントサイズが適しています。アプリケーションがラージシーケンシャルリードとラージシーケンシャルライト（スループット）を使用する場合は、一般に大きなセグメントサイズが適しています。

アプリケーションがスモールランダムリード/ライトとラージシーケンシャルリード/ライトのどちらを使用するかに関係なく、セグメントサイズが標準的なデータブロックのチャンクサイズより大きい場合、ストレージアレイのパフォーマンスが向上します。これはドライブがより簡単かつ高速にデータにアクセスできるようにするためであり、ストレージアレイのパフォーマンス向上にとって重要です。

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

スループットを重視する環境では、標準的なデータチャンクサイズ（I/Oサイズ）をデータ用ドライブの総数で割った値にセグメントサイズを設定します。こうすることで、データが単一のストライプとしてボリュームグループの複数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。コントローラ間で総I/O数をできるだけ均等に分散する必要があります。

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なデータブロックを頻繁に読み書きする場合、両者の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るようになります。

ホストの割り当てをあとで実行する場合に選択します。

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

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

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

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

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

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

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

- 一部のオペレーティングシステムと仮想マシン（現時点ではVMwareなど）は512バイトのブロックサイズを必要とし、4KiBをサポートしないため、ボリュームを作成する前にホストの要件を確認してください。通常、最適なパフォーマンスを実現するには、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。
- プールまたはボリュームグループ用に選択したドライブのタイプによって、サポートされるボリュームブ

ロックサイズも次のように決まります。

- 512バイトブロックに書き込むドライブを使用してボリュームグループを作成する場合、作成できるのは512バイトブロックのボリュームのみです。
- 4KiBブロックに書き込むドライブを使用してボリュームグループを作成する場合は、512バイトまたは4KiBブロックでボリュームを作成します。

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

ホストとホストクラスタ

ホストとホストクラスタの概要

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

ホストおよびホストクラスタとは何ですか？

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。

詳細はこちら。

- "ホストの用語"
- "アクセスボリューム"
- "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。複数のホストが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。

詳細はこちら。

- "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"
- "ホストを手動で作成する"
- "ホストクラスタを作成する"
- "ホストにボリュームを割り当てます"

関連情報

ホストに関連するタスクの詳細を確認してください。

- "自動ロードバランシングを設定する"
- "ホスト接続レポートの設定"
- "デフォルトのホストタイプを変更"

概念

ホストの用語

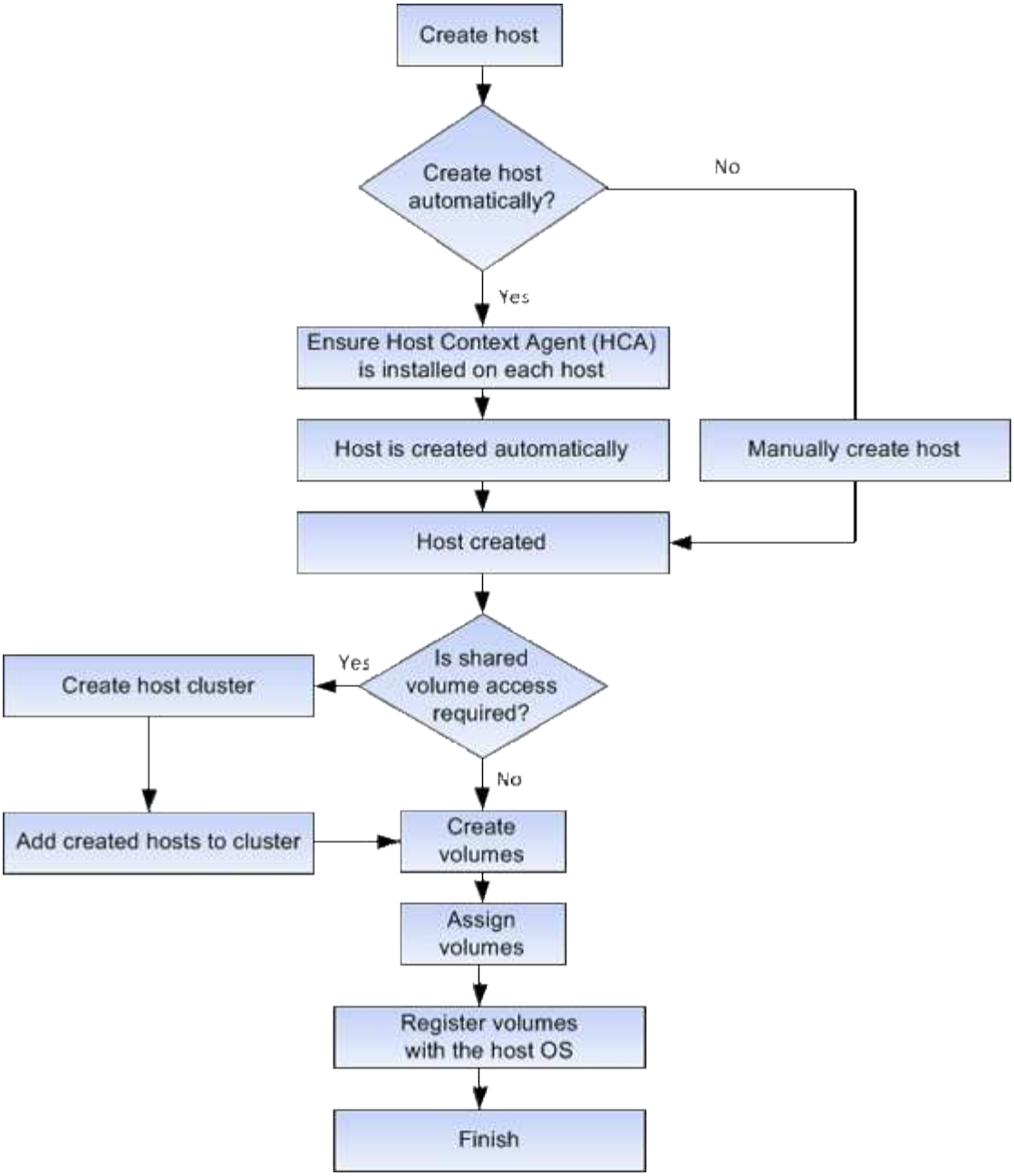
ストレージアレイに関連するホストの用語を次に示します。

コンポーネント	定義（ **Definition** ）
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。
ホストポートの識別子	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）のホストポート識別子は、1~233文字にする必要があります。iSCSIホスト・ポート識別子は'標準的なIQN形式（例：iqn.xxx.com.xxx:8b3ad`）で表示されます • Fibre ChannelやSerial Attached SCSI（SAS）などの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られた形式で表示されます（例：「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（ **Definition** ）
ホストオペレーティングシステムのタイプ	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の形式でホストに容量として提示されます。 各ホストには独自のLUNアドレススペースがあります。したがって、同じLUNを複数のホストで使用して、異なるボリュームにアクセスできます。

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

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、または手動で入力して関連付けます。ホストの作成後、ボリュームへのアクセスを共有する場合は、ボリュームをホストに割り当てたり、ホストクラスタに追加したりできます。

ホスト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へ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。

ボリュームを作成するときにホストまたはホストクラスタを選択するか、あとからボリュームをホストまたはホストクラスタに割り当てることができます。ホストクラスタはホストのグループです。ホストクラスタを作成すると、同じボリュームを複数のホストに簡単に割り当てることができます。

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

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

ボリュームの作成時に、論理ユニット番号（LUN）が自動的に割り当てられます。LUNは、I/O処理中のホストとコントローラの間の「アドレス」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。

アクセスボリューム

アクセスボリュームは、ストレージアレイ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）で管理する場合にのみ可能です。

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

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、および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、各ホストに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、ホストの最初の接続時にストレージアレイで使用されます。ボリュームがアクセスされたときに、ストレージアレイ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。

接続されたホストを基準に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。一般に、デフォルトのホストタイプは、ストレージアレイにホストを接続する前、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ホストのオペレーティングシステムがすべて同じ場合は（同機種ホスト環境）、オペレーティングシステムに一致するホストタイプに変更します。
- 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。

- ほとんどの接続ホスト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。

ホストアクセスを設定

ホストを手動で作成する

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

このタスクについて

ホストを作成する際は、次のガイドラインに注意してください。

- ホストに関連付けられたホストポート識別子を定義する必要があります。
- ホストに割り当てられたシステム名と同じ名前を指定してください。
- 選択した名前がすでに使用されている場合、この処理は失敗します。

- 名前は 30 文字以内にする必要があります。

手順

1. 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。

   Create Host （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	説明
名前	新しいホストの名前を入力します。
ホストオペレーティングシステムのタイプ	新しいホストで実行しているオペレーティングシステムをドロップダウンリストから選択します。
ホストインターフェイスタイプ	（オプション）ストレージアレイで複数のタイプのホストインターフェイスがサポートされている場合、使用するホストインターフェイスタイプを選択します。
ホストポート	次のいずれかを実行します。 • * I/O インターフェイス * を選択します 通常は、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することができます。 • * 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をいくつでも選択することができます。各識別子は、［* ホストポート *］フィールドに表示されます。必要に応じて、横の * X * を選択して識別子を削除することもできます。

設定	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されたものと同じ CHAP シークレットを入力します。相互 CHAP 認証（ホストが自身をストレージアレイに対して検証し、ストレージアレイが自身をホストに対して検証できるようにする双方向認証）を使用する場合は、ストレージアレイの初期セットアップまたは設定変更時に CHAP シークレットも設定する必要があります。 • ホストの認証が不要な場合は、このフィールドを空白のままにします。 現在のところ、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

ホストの作成が完了すると、ホストに設定されている各ホストポートのデフォルト名（ユーザラベル）が作成されます。

デフォルトのエイリアスは<`Hostname_Port Number``>です。たとえば、「ホスト IPT 」用に作成される最初のポートのデフォルトのエイリアスは、 ipt_1 です。

ホストクラスタを作成する

同じボリュームへのI/Oアクセスを必要とするホストが複数ある場合は、ホストクラスタを作成します。

このタスクについて

ホストクラスタを作成する際は、次のガイドラインに注意してください。

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

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

- 選択した名前がすでに使用されている場合、この処理は失敗します。

- 名前は 30 文字以内にする必要があります。

手順

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

4. [作成（ Create ）] をクリックします。

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

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

結果

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

ホストにボリュームを割り当てます

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

このタスクについて

ホストにボリュームを割り当てる際は、次のガイドラインに注意してください。

- ボリュームは一度に 1 つのホストまたはホストクラスタにのみ割り当てることができます。
- 割り当てられたボリュームは、ストレージアレイのコントローラ間で共有されます。
- あるホストまたはホストクラスタからボリュームへのアクセスに、同じ論理ユニット番号（LUN）を複数回使用することはできません。一意のLUNを使用する必要があります。

- 新しいボリュームグループでは、すべてのボリュームが作成されて初期化されるまでホストに割り当てると、ボリュームの初期化時間が短縮されます。ボリュームグループに関連付けられているボリュームをマッピングすると、_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。
- ホストポート識別子がホストに対して定義されていない。
- すべてのボリューム割り当てが定義されている。

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

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

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、テーブルヘッダーにあるチェックボックスを選択してすべてのボリュームを選択します。
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 番号が受信されます。ホストはこの LUN 番号を使用してボリュームにアクセスします。
- ホストに関連付けられているボリュームの一覧にユーザが指定したボリューム名が表示されます。該当する場合、ホストに関連付けられているボリュームの一覧には、工場出荷時に設定されたアクセスボリュームも表示されます。

ホストとクラスタを管理

デフォルトのホストタイプを変更

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て、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します。一般に、デフォルトのホストタイプは、ストレージアレイにホストを接続する前、または追加のホストを接続するときに変更します。

このタスクについて

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ホストのオペレーティングシステムがすべて同じ場合は（同機種ホスト環境）、オペレーティングシステムに一致するホストタイプに変更します。
- 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。

- ほとんどの接続ホスト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の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を解除する

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そのボリュームの割り当てを解除します。

このタスクについて

ボリュームの割り当てを解除する際は、次のガイドラインに注意してください。

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

手順

1. 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、テーブルヘッダーにあるチェックボックスを選択してすべてのボリュームを選択します。
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、ボリュームは引き続きホストオペレーティングシステムで認識されます。

ホストまたはホストクラスタを削除

ホストまたはホストクラスタを削除することができます。

このタスクについて

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

- ボリュームの割り当てはすべて削除され、関連付けられたボリュームを新しい割り当てに使用できるようになります。
- ホストが属するホストクラスタに固有の割り当てがある場合、ホストクラスタへの影響はありません。ただし、ホストが属するホストクラスタに他の割り当てがない場合は、ホストクラスタとそれに関連付けられている他のすべてのホストまたはホストポート識別子にデフォルトの割り当てが継承されます。
- ホストに関連付けられていたホストポート識別子の定義は削除されます。

手順

1. 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も削除します。
- 割り当てられているボリュームへのアクセスを削除します。
- 関連付けられているボリュームの割り当てを解除します。
- ホストに関連付けられているホストポート識別子の関連付けを解除します。

ホストクラスタを削除すると、システムは次の処理を実行します。

- ホストクラスタとそれに関連付けられているホスト（存在する場合）を削除します。
- 割り当てられているボリュームへのアクセスを削除します。
- 関連付けられているボリュームの割り当てを解除します。
- ホストに関連付けられているホストポート識別子の関連付けを解除します。

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済みのホスト間の接続をストレージアレイで常時監視して、接続が中断された場合に通知されるようにすることができます。この機能はデフォルトで有効になっています。

このタスクについて

ホスト接続の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がシステムによって監視されなくなります。

また、コントローラのリソース利用率を監視してバランスを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。
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。

設定を管理します

ホストの設定を変更します

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

手順

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

5. [保存（ Save ）] をクリックします。

ホストクラスタの設定を変更します

ホストクラスタの名前を変更したり、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開き、ホストクラスタの現在の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	説明
名前	ユーザが指定したホストクラスタの名前を指定できます。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を変更する

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。

このタスクについて

ホストポート識別子を変更する際は、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。ポート情報は、ホストバスアダプタ（HBA）ユーティリティを使用して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場合は、ホストポートを新しいホストに移動（関連付ける）する必要があります。
- 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開き、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	説明
ホストポート	次のいずれかのオプションを選択できます。 • *追加-- Addを使用して'新しいホストポート識別子をホストに関連付けますホストポート識別子名の長さは、ホストインターフェイスのテクノロジによって決まります。Fibre ChannelとInfiniBandのホストポート識別子名は、16文字にする必要があります。iSCSI のホストポート識別子名は最大 223 文字です。ポートは一意である必要があります。すでに設定されているポート番号は使用できません。 • *Delete *-- Deleteを使用して、ホストポート識別子を削除(関連付けを解除)します。Deleteオプションを使用しても、ホストポートは物理的には削除されません。このオプションを選択すると、ホストポートとホストの間の関連付けが削除されます。ホストバスアダプタまたは iSCSI イニシエータを削除しないかぎり、ホストポートは引き続きコントローラで認識されます。 ホストポート識別子を削除すると、そのホストとの関連付けが解除されます。また、ホストはホストに割り当てられているボリュームにこのホストポート識別子経由でアクセスできなくなります。
ラベル	ポートラベル名を変更するには、* Edit *アイコン（鉛筆）をクリックします。ポートラベル名は一意である必要があります。すでに設定されているラベル名は使用できません。
CHAPシークレット	iSCSIホストにのみ表示されます。イニシエータ（iSCSIホスト）のCHAPシークレットを設定または変更できます。 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。

よくある質問です

ホストおよびホストクラスタとは何ですか？

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。ホストを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ができます。または、ホストをホストクラスタの一部として指定し、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？

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

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

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

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

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

リストに表示されるホストタイプは次のとおりです。

ホストオペレーティングシステムのタイプ	オペレーティングシステム（**OS**）とマルチパスドライバ
Linux DM-MP（カーネル3.10以降）	Device Mapper Multipathのフェイルオーバー解決策 と3.10以降のカーネルを使用するLinuxオペレーティングシステムをサポートします。
VMware ESXi	VMwareに組み込みのストレージアレイタイプポリシーモジュールであるSATP_ALUAを使用してNative Multipathing Plug-in（NMP）アーキテクチャを実行するVMware ESXiオペレーティングシステムをサポートします。
Windows（クラスタまたは非クラスタ）	ATTOマルチパスドライバを実行しないWindowsクラスタ構成または非クラスタ構成をサポートします。
ATTOクラスタ（すべてのオペレーティングシステム）	ATTO Technology、Inc.のマルチパスドライバを使用するすべてのクラスタ構成をサポートします。
Linux（Veritas DMP）	Veritas DMPマルチパス解決策 を使用するLinuxオペレーティングシステムをサポートします。
Linux（ATTO）	ATTO Technology、Inc.のマルチパスドライバを使用するLinuxオペレーティングシステムをサポートします。
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のタイプ	オペレーティングシステム（**OS**）とマルチパスドライバ
Windows（ATTO）	ATTO Technology、Inc.のマルチパスドライバを使用するWindowsオペレーティングシステムをサポートします。
FlexArray （ALUA）	マルチパスにALUAを使用するNetApp FlexArray システムをサポートします。
IBM SVCの場合	IBM SAN Volume Controller構成をサポートします。
工場出荷時のデフォルト	ストレージアレイの初回起動用です。ホストオペレーティングシステムのタイプが工場出荷時のデフォルトに設定されている場合は、接続先ホストで実行されているホストオペレーティングシステムとマルチパスドライバに合わせて変更します。
Linux DM-MP（カーネル3.9以前）	Device Mapper Multipathのフェイルオーバー解決策 と3.9以前のカーネルを使用するLinuxオペレーティングシステムをサポートします。
Windowsクラスタ（廃止）	ホストオペレーティングシステムのタイプがこの値に設定されている場合は、代わりにWindows（クラスタまたは非クラスタ）の設定を使用します。

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と各HBAホストポートには、それぞれ一意のWorld Wide Identifier（WWID）が割り当てられています。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にはどうすればよいですか？

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

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

作成するホストに適したホストポート識別子を選択してください。誤ったホストポート識別子を関連付けると、別のホストからこのデータへの原因 の意図しないアクセスが発生する可能性があります。

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ホスト上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の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をホストの作成処理または設定の表示/編集オプションのどちらかとして使用します。

CHAP相互認証を使用する場合は、ストレージアレイのターゲットCHAPシークレットを［設定］ページで定義し、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す。ストレージアレイにログインしたホストポート識別子が関連付けられていない場合、そのポートはデフォルトクラスタに割り当てられているボリュームにアクセスできます。関連付けられていないホストポート識別子は、特定のホストに論理的に関連付けられておらず、ホストに物理的に搭載されてストレージアレイにログインしているホストポートです。

> ホストがストレージアレイ内の特定のボリュームにアクセスできるようにする場合は、デフォルトクラスタを使用する_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。その後、ボリュームを個々のホストまたはホストクラスタに割り当てます。

デフォルトクラスタは、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際には、コマンドラインインターフェイス（CLI）を使用する必要があります。ただし、ボリュームを少なくとも1つデフォルトクラスタに割り当てると、このエンティティを管理できるユーザインターフェイスに表示されます（デフォルトクラスタ）。

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たホスト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。

ケーブルに緩み、損傷、脱落が生じた場合や、ホストに問題が生じた場合は、接続の中断が発生す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。

また、コントローラのリソース使用量を監視してバランスを調整する自動ロードバランシングも無効になります。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。

Snapshot

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またはテストに使用できます。

Snapshotイメージとは何ですか？

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、直接読み取ったり書き込んだりすることはできません。

詳細はこちら。

- "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ボリューム"

Snapshot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することができます。この手順 は次のメニューから使用できます。Storage [Snapshots]。

詳細はこちら。

- "Snapshotの要件とガイドライン"
- "Snapshotイメージとボリュームを作成するためのワークフロー"
- "Snapshotイメージを作成"
- "Snapshotイメージのスケジュールを設定"
- "Snapshot整合性グループを作成します"
- "Snapshotボリュームを作成します"

Snapshotからデータをロールバックするにはどうすればよいですか？

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]。

詳細はこちら。

- "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を開始する"
- "整合性グループメンバーのSnapshotイメージのロールバックを開始します"

関連情報

Snapshotに関連するタスクの詳細を確認できます。

- "Snapshotボリュームのリザーブ容量を変更します"
- "Snapshotグループのリザーブ容量を変更します"

概念

Snapshotストレージの仕組み

Snapshot機能は、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

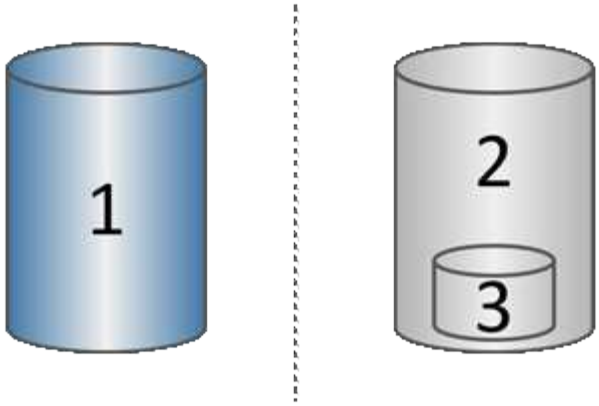
Snapshotイメージは、特定の時点でキャプチャされた、ボリュームの内容の論理的な読み取り専用コピーです。Snapshotを使用して、データ損失からデータを保護できます。

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により、実際のボリューム自体は変更せずに、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た時点では、Snapshotイメージは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に対して最初の書き込みが行われると、新しいデータをベースボリュームに書き込む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、ベースボリューム上で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保存されます。一般に、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。

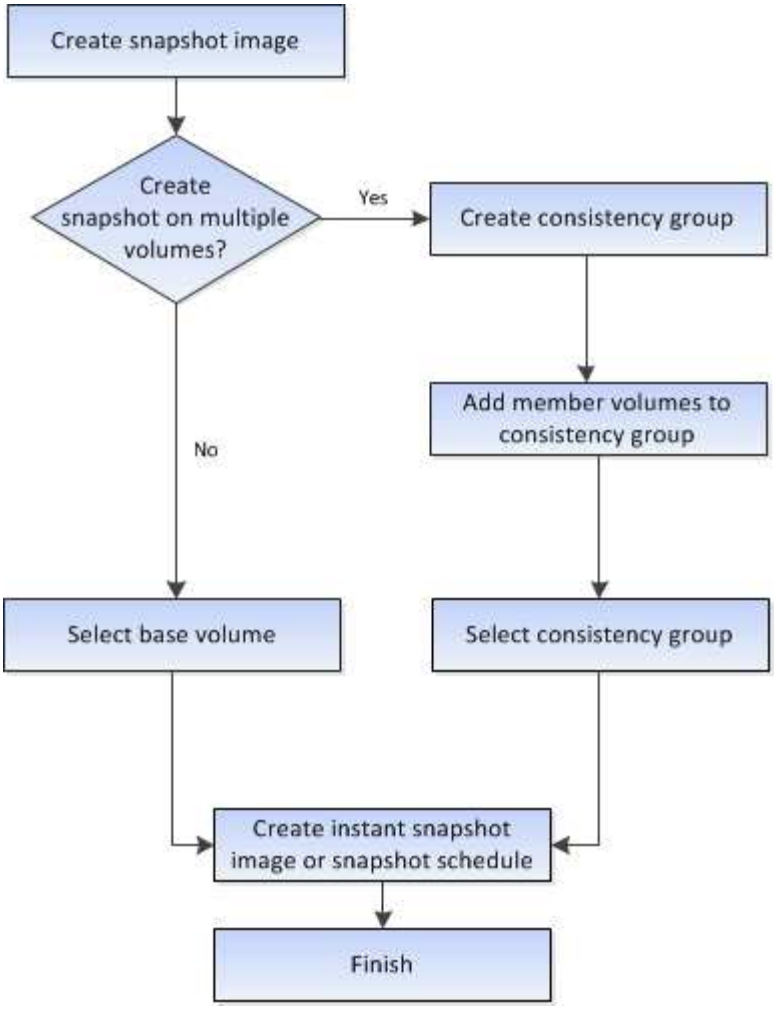
期間	説明
Snapshot機能	Snapshot機能は、ボリュームのイメージの作成と管理に使用されます。
Snapshotイメージ	Snapshot イメージは、ボリュームのデータを特定の時点でキャプチャした論理コピーです。リストアポイントと同様に、 Snapshot イメージを使用して既知の正常なデータセットにロールバックできます。ホストはSnapshotイメージにアクセスできますが、直接読み取ったり書き込んだりすることはできません。
ベースボリューム	ベースボリュームは、Snapshotイメージの作成元のボリュームです。シックボリュームの場合もシンボリュームの場合もあり、通常はホストに割り当てられています。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	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あり、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。各ボリュームのSnapshotイメージが作成されますが、すべてのイメージが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。

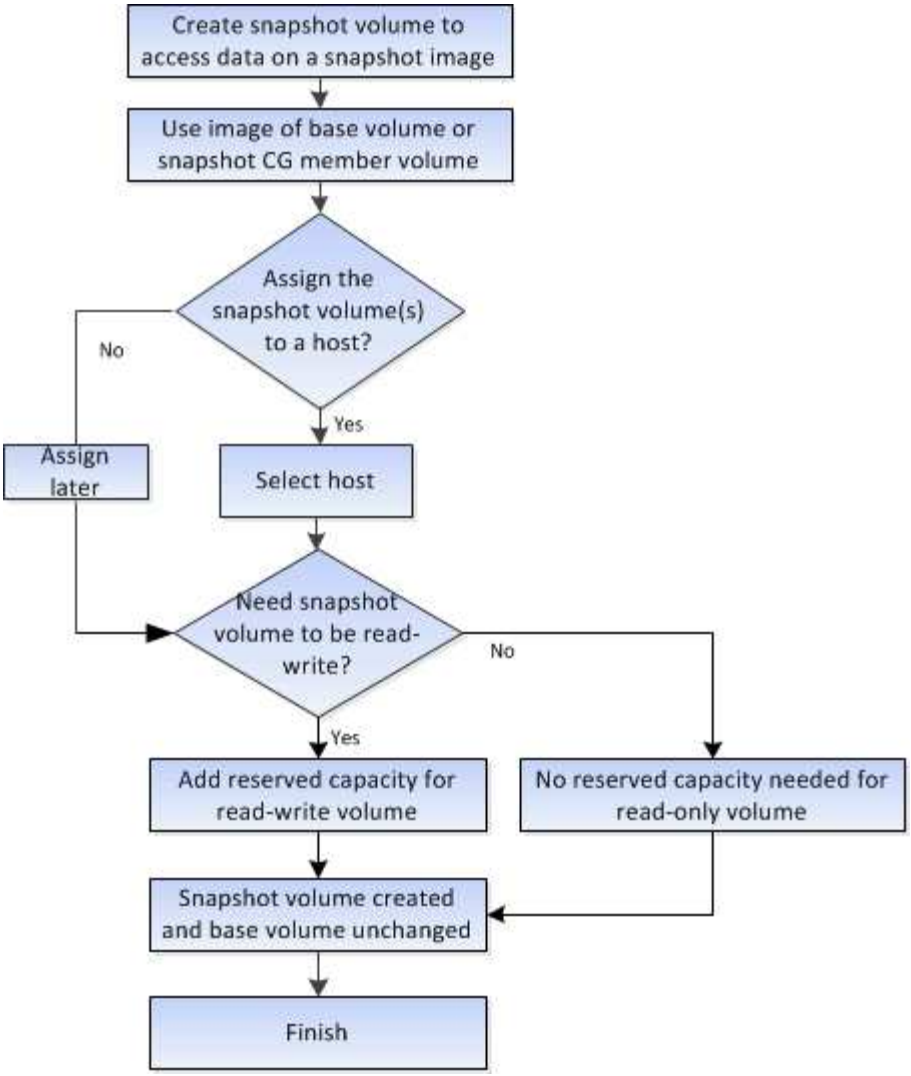
Snapshotイメージと**Snapshot**ボリュームを作成するためのワークフロー

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

Snapshotを作成して使用する場合は、次の要件および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グループにのみ関連付けられます。
- Snapshotグループは、関連オブジェクトに対して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場合や電源がオフの場合は作成されません。
- 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ボリュームは、同じSnapshotイメージまたは別のSnapshotイメージに再関連付けできます。

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つ含まれています。
- 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）とセキュリティの設定は、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。
- 障害のあるベースボリュームからSnapshotボリュームを作成することはできません。
- 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のみに関連付けられます。
- 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用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場合。
- ベースボリュームで同期処理を実行中の場合。同期処理が完了した時点でSnapshotイメージの作成が完了します。

Snapshotイメージの最大数

- あるボリュームが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用のSnapshot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、次の操作は実行できません。
  - ロールバックに使用されているSnapshotイメージを削除する。
  - ロールバック処理の対象であるベースボリュームの新しいSnapshotイメージの作成
  - 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の進行中は、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が変更された
- ベースボリュームがボリュームコピーの対象である場合は、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内の使用済み容量に読み取り不能なセクターが含まれている場合、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

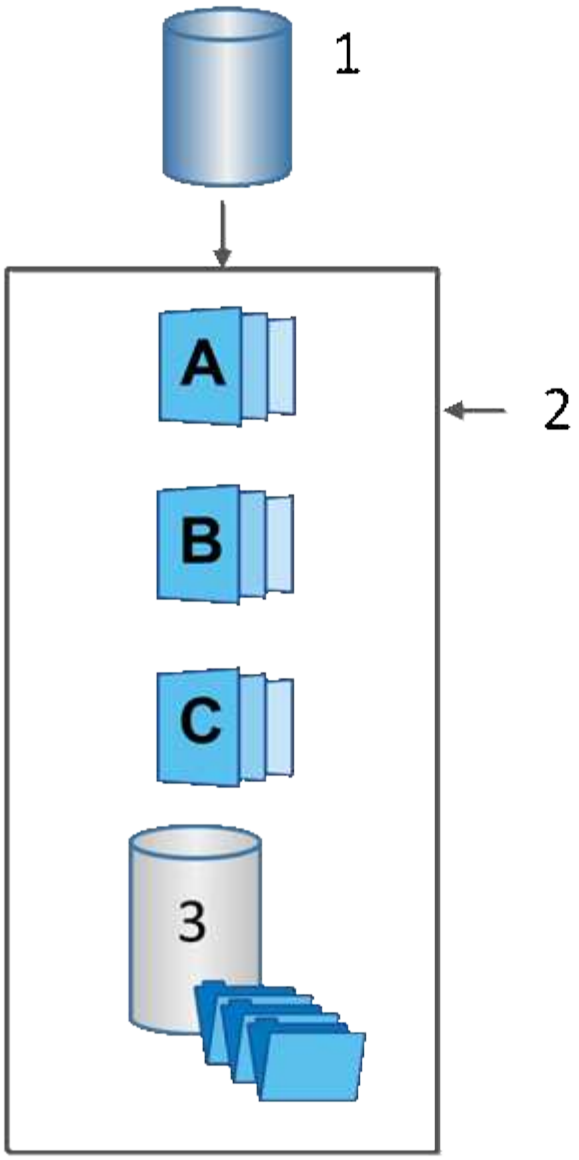
Snapshot機能は、ベースボリューム、リザーブ容量、およびSnapshotグループを使用します。

ベースボリューム

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。シックボリュームまたはシンボリュームをベースボリュームとして使用できます。ベースボリュームはプールまたはボリュームグループに配置できます。

ベースボリュームのSnapshotを作成するために、インスタントイメージをいつでも作成できます。また、Snapshotの定期的なスケジュールを定義することでプロセスを自動化することもできます。

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、リザーブ容量はプールまたはボリュームグループに配置できます。ベースボリュームがプールに含まれている場合、リザーブ容量は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、次の条件を満たす場合は、リザーブ容量の作成を求められることがあります。

- Snapshotグループがまだないベースボリュームの Snapshotを作成するたびに、System Managerはスナップショットグループを自動的に作成します。この操作では、以降のSnapshotイメージの格納に使用する

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たびに、System ManagerはSnapshotグループを自動的に作成します。

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有効にします。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グループの制限値を超えるため、Snapshotグループの設定と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

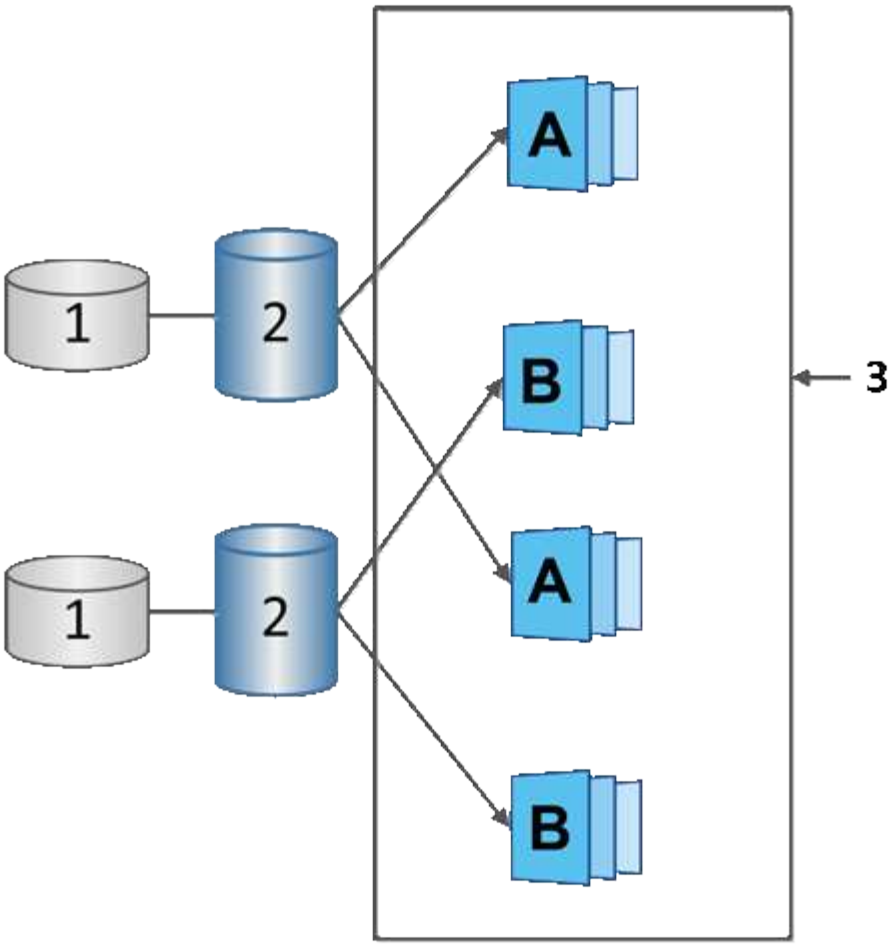
Snapshotスケジュール

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たあとは、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

Snapshot整合性グループは、複数のボリュームで同時にSnapshotイメージが作成されるようにする場合に作成します。Snapshotイメージの操作は、Snapshot整合性グループに対してまとめて実行されます。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整合グループは、あるボリュームにログを格納するデータベースアプリケーションや別のボリュームにあるデータベースファイルなど、複数のボリュームにまたがるアプリケーションに最適です。

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。ボリュームを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リザーブ容量を自動的に作成します。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。



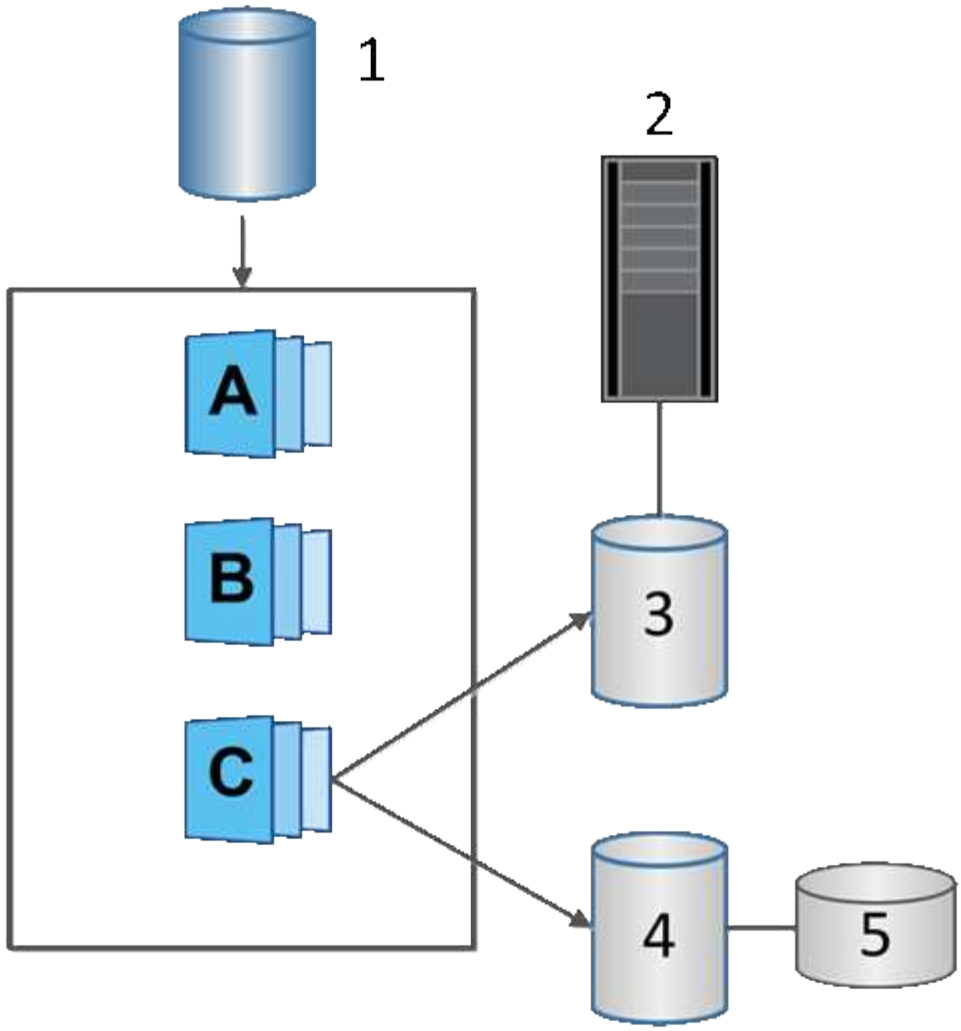
1リザーブ容量；2メンバーボリューム；3^整合グループSnapshotイメージ

Snapshotボリューム

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。

読み取り専用のSnapshotボリュームを作成する場合、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。

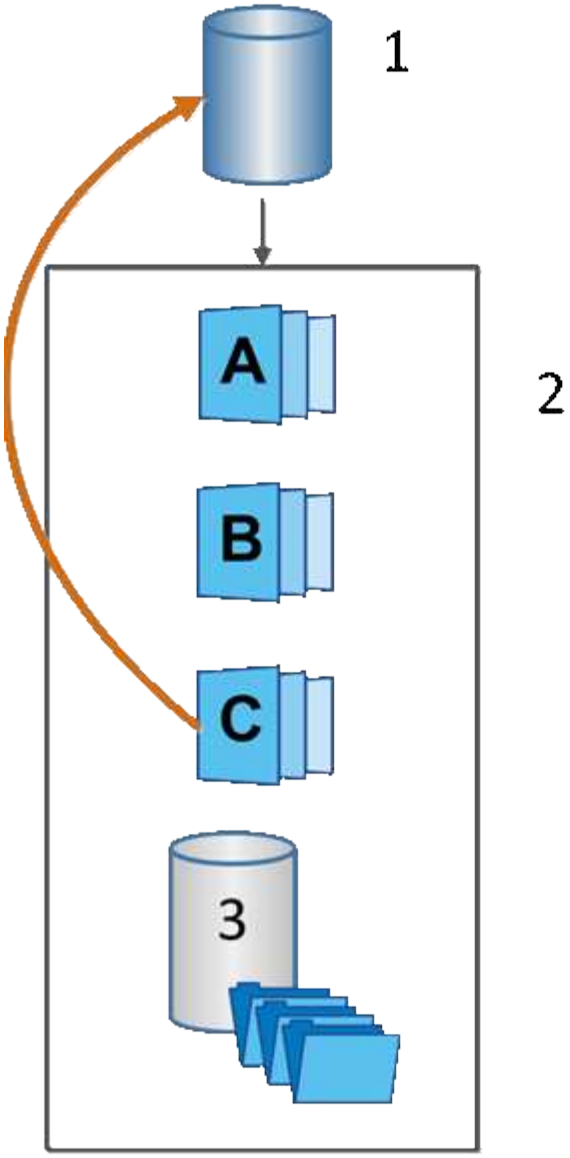
ロールバックでは、次のいずれかのソースからSnapshotイメージを選択できます。

- * 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、グループ内のすべてのSnapshotイメージがSnapshot機能によって保持されます。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できます。

ロールバックが起動すると、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、リストア対象となる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可能であり、以前に書き込まれたすべてのデータをただちに使用できるため、リザーブ容量ボリュームにはロールバック処理中のすべての変更を格納できるだけの十分な容量が必要です。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およびSnapshotオブジェクトを作成します

Snapshotイメージを作成する

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することができます。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

作業を開始する前に

- 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I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）の設定は、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整合性グループの以前のSnapshotイメージが作成されている場合は、インスタントSnapshotがすぐに作成されます。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	説明
• Snapshotイメージの設定*	Snapshotイメージの上限
指定した制限に達したときにSnapshotイメージを自動的に削除する場合は、このチェックボックスをオンのままにします。制限はスピンボックスを使用して変更できます。このチェックボックスの選択を解除すると、Snapshotイメージが32個作成された時点で作成が停止します。	リザーブ容量の設定
アラートの送信しきい値	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ときの処理です	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。新しいイメージは、タイムスタンプと関連付けられたベースボリュームまたはSnapshot整合性グループ別に表示されます。
- 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場合。
  - ベースボリュームで同期処理を実行中の場合。同期処理が完了した時点で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を設定

Snapshotスケジュールを作成して、ベースボリュームに関する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、任意の時刻に日次、週次、または月単位のスケジュールで作成できます。

作業を開始する前に

ベースボリュームが最適lである必要があります。

このタスクについて

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	説明
基本設定	日を選択します
Snapshotイメージの個々の曜日を選択します。	開始時刻
日次Snapshotの新しい開始時間をドロップダウンリストから選択します（30分単位で選択可能）。開始時間のデフォルトは現在時刻の30分前です。	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 *
曜日/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	日次Snapshotの新しい開始時間をドロップダウンリストから選択します（30分単位で選択可能）。開始時間のデフォルトは現在時刻の30分前です。
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。複数選択する場合は、Snapshotイメージを作成する間隔も選択してください。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。
Snapshotイメージを今すぐ作成？	スケジュール設定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。

フィールド	説明
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。

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	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…
指定した制限に達したときにSnapshotイメージを自動的に削除する場合は、このチェックボックスをオンのままにします。制限はスピンボックスを使用して変更できます。このチェックボックスの選択を解除すると、Snapshotイメージが32個作成された時点で作成が停止します。	リザーブ容量の設定
アラートの送信しきい値	スピンボックスを使用して、スケジュール用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。 スケジュール用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ときの処理です	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整合性グループを作成します

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。

このグループでは、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保つことができます。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。ボリュームをSnapshot整合性グループに追加すると、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。

このタスクについて

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る手順 です。

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すべての操作は、選択したすべてのメンバーボリュームに対して一様に実行されます。

作業を開始する前に

メンバーボリュームが最適lである必要があります。

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」をクリックして、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。

このタスクについて

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整合性グループの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のリザーブ容量を割り当てる推奨されるオプションであり、デフォルトの設定でリザーブ容量を割り当てます。

   - 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」をクリックして、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。

このタスクについて

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	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…
指定した制限に達したときにSnapshotイメージを自動的に削除する場合は、このチェックボックスをオンのままにします。制限はスピンボックスを使用して変更できます。このチェックボックスの選択を解除すると、Snapshotイメージが32個作成された時点で作成が停止します。	リザーブ容量の設定
アラートの送信しきい値	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ときの処理です	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ボリュームを作成します

Snapshotボリュームを作成して、ボリュームまたはSnapshot整合性グループのSnapshotイメージにホストからアクセスできるようにします。Snapshotボリュームは

読み取り専用または読み取り/書き込みに指定できます。

このタスクについて

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ます。ボリュームが読み取り/書き込みの場合は、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に対する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。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。
- 読み取り/書き込みのSnapshotボリュームは、Snapshotイメージに格納されたデータ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う以降の変更を、参照元のSnapshotイメージに影響を及ぼさずに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る手順 です。

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イメージを選択した場合は、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イメージに対してを選択した場合は、Review Members（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. に進みます 手順2：Snapshotボリュームをホストに割り当てる。

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、ホストまたはホストクラスタにSnapshotボリュームへのアクセスが許可されます。必要に応じて、ホストをあとから割り当てることもできます。

作業を開始する前に

- 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が定義されている必要があります。
- DA対応ボリュームを作成する前に、使用するホスト接続で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で DA をサポートしていないホスト接続が使用されている場合、関連付けられているホストからは DA 対応ボリュームのデータにアクセスできません。

このタスクについて

ボリュームを割り当てる際は、次のガイドラインに注意してください。

- ホストのオペレーティングシステムによって、ホストがアクセスできるボリュームの数に制限がある場合があります。
- 割り当てることができるホストまたはホストクラスタは、ストレージアレイのSnapshotボリュームごとに1つです。
- 割り当てられたボリュームは、ストレージアレイのコントローラ間で共有されます。
- あるホストまたはホストクラスタからSnapshotボリュームへのアクセスに、同じ論理ユニット番号（LUN）を複数回使用することはできません。一意のLUNを使用する必要があります。

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

手順

1. [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。に進みます 手順3：Snapshotボリューム用の容量をリザーブする。
   - 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。に進みます 手順4：Snapshotボリュームの設定を編集する。

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。

このタスクについて

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ボリュームのリザーブ容量を割り当てます。

   ボリューム候補表には、指定したリザーブ容量に対応する候補だけが表示されます。

   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。

     デフォルト設定を使用してSnapshotボリュームの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」をクリックして、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。

このタスクについて

読み取り専用のパフォーマンスを向上させるために、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SSDドライブのセットで構成されます。

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	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キャッシュを有効にする
SSDで読み取り専用の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
アラートの送信しきい値	*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。

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スケジュールを管理します

Snapshotスケジュールの設定を変更します

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。

このタスクについて

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	説明
曜日/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、日次Snapshotの新しい開始時間を選択します。選択肢は30分単位で表示されます。開始時間のデフォルトは現在時刻の30分前です。
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。 複数選択する場合は、リストアポイントの間隔も選択します。複数のリストアポイントを作成する場合は、リザーブ容量が十分にあることを確認してください。
開始日 終了日 終了日がありません	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の節約が必要な場合は、Snapshotイメージのスケジュールされた収集を一時的に停止できます。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。

このタスクについて

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スケジュールを削除します

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。

このタスクについて

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イメージの収集を再開す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イメージを管理します

Snapshotイメージの設定を表示します

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。

このタスクについて

Snapshotイメージの関連オブジェクトには、その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、関連付けられている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イメージの設定を表示します。

ベースボリュームのSnapshotイメージのロールバックを開始する

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することができます。

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。

作業を開始する前に

- 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確保されています。
- 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。

このタスクについて

ロールバックの開始手順によって、ベースボリュームの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。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後の新しいベースボリュームにすぐにアクセスできますが、ロールバックを実行中のベースボリュームに読み取り/書き込みアクセスすることはできません。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ためには、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い場合や、ストレージアレイに未割り当て容量がない場合は、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上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。

完了後

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。処理が再び失敗する場合は、Recovery Guru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整合性グループのメンバーボリュームの**Snapshot**イメージのロールバックを開始します

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。

作業を開始する前に

- 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確保されています。
- 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。

このタスクについて

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後の新しいボリュームにすぐにアクセスできますが、ロールバックを実行中のメンバーボリュームに読み取り/書き込みアクセスすることはできません。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ためには、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る手順 です。

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。に進みます [手順2：容量を確認する]。
   - 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。に進みます [手順3：優先度を編集する]。

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、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い場合や、ストレージアレイに未割り当て容量がない場合は、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上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」をクリックして、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。

このタスクについて

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考慮せずロールバック処理専用とな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た内容を使用してSnapshot整合性グループ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。

完了後

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。処理が再び失敗する場合は、Recovery Guru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を再開します

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をキャンセルします

実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）、（リソースの開始を待機している保留キューで）保留中のロールバック、またはエラーが原因で一時停止されたロールバックをキャンセルできます。

このタスクについて

実行中のロールバック処理をキャンセルすると、ベースボリュームが使用できない状態に戻り、「失敗」と表示されます。そのため、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、含まれているデータの整合性が確保されない、またはデータが維持されない場合があります

完了後

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、ロールバックのキャンセル処理で使用されたのと同じ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イメージを削除します

Snapshotイメージを削除すると、SnapshotグループまたはSnapshot整合性グループから最も古いSnapshotイメージがクリーンアップされます。

このタスクについて

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を削除すると、削除したSnapshotイメージに関連付けられていたメンバーボリュームの状態が停止になります。

Snapshot整合性グループを管理します

Snapshot整合性グループにメンバーボリュームを追加します

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、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。

作業を開始する前に

- 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が、許容される最大ボリューム数（設定で定義）を下回っている必要があります。
- 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が、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。

このタスクについて

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どちらかに配置できます。

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。

   Reserve Capacityステップが表示されます。ボリューム候補表には、指定したリザーブ容量に対応する候補だけが表示されます。

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のリザーブ容量を割り当てる推奨されるオプションであり、デフォルトの設定でリザーブ容量を割り当てます。

   - 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メンバーボリュームを削除します

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。

このタスクについて

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、System Managerは、そのメンバーボリュームに関連付けられているSnapshotオブジェクトを自動的に削除します。

手順

1. メニューを選択します。Storage [Snapshots]。
2. スナップショット・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（+）をクリックして展開します。
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。
- こ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を変更します

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 Consistency Group Setting（スナップショット整合グループ設定）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	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
指定した制限に達したときにSnapshotイメージを自動的に削除する場合は、このチェックボックスをオンのままにします。制限はスピンボックスを使用して変更できます。このチェックボックスの選択を解除すると、Snapshotイメージが32個作成された時点で作成が停止します。	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確認できます。

5. [保存（ Save ）] をクリックします。

Snapshot整合性グループを削除します

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。

作業を開始する前に

すべてのメンバーボリュームのイメージについて、バックアップやテストに使用する必要がなくなったことを確認します。

このタスクについて

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すべてのSnapshotイメージまたはスケジュールが削除されます。

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ボリュームを管理します

Snapshotボリュームを読み取り/書き込みモードに変換します

必要に応じて、読み取り専用のSnapshotボリュームや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することができます。

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割り当てられます。この容量は、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う以降の変更を、参照元のSnapshotイメージに影響を及ぼさずに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 Volumesテーブルが表示され、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。ボリューム候補表には、指定したリザーブ容量に対応する候補だけが表示されます。

4. 読み取り/書き込みの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	説明
リザーブ容量の設定	アラートの送信しきい値

Snapshotボリュームのボリューム設定を変更します

SnapshotボリュームまたはSnapshot整合性グループのSnapshotボリュームの設定では、Snapshotボリュームの名前を変更したり、SSDキャッシュを有効または無効にしたり、ホスト、ホストクラスタ、または論理ユニット番号（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適宜表示または編集します。

フィールドの詳細

設定	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、直接読み取ったり書き込んだりすることはできません。
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。シックボリュームの場合もシンボリュームの場合もあり、通常はホストに割り当てられています。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グループを確認できます。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ボリュームをコピーします

SnapshotボリュームやSnapshot整合性グループのSnapshotボリュームについて、ボリュームコピープロセスを実行することができます。

このタスクについて

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ボリュームはオンラインのままコピープロセス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 Volumesテーブルが表示され、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ボリュームを再作成します

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、新規作成よりも短時間で完了します。

作業を開始する前に

- Snapshotボリュームが最適または無効のいずれかの状態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。

このタスクについて

メンバーであるSnapshotボリュームを個別に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は、その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 Volumesテーブルが表示され、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、そこから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Snapshotボリュームの再作成する場合は、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。

- 関連づけられているスナップショット・リポジトリ・ボリューム上のすべての書き込みデータを削除します
- SnapshotボリュームまたはSnapshot整合性グループのSnapshotボリュームのパラメータは、以前無効にしたボリュームのパラメータから変更しません。
- 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ボリュームを無効にします

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。

このタスクについて

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ボリュームを（読み取り/書き込み用に）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ておきたい。
- 読み取り/書き込みの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/書き込み用の場合、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は、そのボリュームで無効化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。

   System Manager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. 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と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ボリュームを削除します

Snapshotボリューム、またはSnapshot整合性グループのSnapshotボリュームは、バックアップやソフトウェアアプリケーションのテストに必要なくなったときは削除することができます。

また'読み取り/書き込みのスナップショット・ボリュームに関連づけられているスナップショット・リザーブ容量ボリュームを削除するか'スナップショット・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保持するかを指定することもできます

このタスクについて

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ボリュームは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。

   System Manager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. 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。

よくある質問です

ボリューム、ホスト、またはホストクラスタが一部表示されないのはなぜですか？

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

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

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

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

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イメージが使用するストレージスペースは最小限です。

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た時点では、Snapshotイメージは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ブロックに対して最初の書き込み要求が行われると、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のはなぜですか？

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であるSnapshot整合性グループを選択し、次のいずれかまたは複数の方法で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整合性グループの定期的なSnapshotイメージを自動的にキャプチャするスケジュールを作成できます。
- 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るため、特定の時点の既知の正常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、偶発的なデータの削除や破損からの保護が提供されます。

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イメージを格納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どちらかに配置できます。

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？

Snapshot整合性グループは、複数のボリュームで同時にSnapshotイメージが作成されるようにする場合に作成します。

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ために、Snapshot整合性グループのSnapshotイメージを作成する。
- 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ために、Snapshot整合性グループのスケジュールを作成する。
- 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ボリュームを作成する。
- 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、**Snapshot**ボリュームに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あり、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や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、リザーブ容量が使用され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、1つの関連する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、次の条件を満たす場合は、リザーブ容量の作成を求められることがあります。

- Snapshotグループがまだないベースボリュームのスナップショットを作成するたびに、System ManagerはSnapshotグループを自動的に作成します。これにより、ベースボリュームのリザーブ容量が作成され、後続の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たびに、System ManagerはSnapshotグループを自動的に作成します。

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、無効にするのではなく、ボリュームを削除してください。

無効状態とは何ですか？

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ボリュームでは、読み取り/書き込みアクティビティは中断されています。

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、スケジュールに基づいた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、あとでスケジュールされたSnapshotを再開できます。

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のデータレプリケーション用に、コントローラレベル、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何ですか？

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ったときに送信されます。

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ます。そのため、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に応えるための手段として最適であり、一般的には、定期的なプロセスをはるかに少ないネットワーク負荷で実施できます。

詳細はこちら。

- "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を実行するには、Unified Managerインターフェイスを使用する必要があります。設定が完了すると、System Managerでミラーペアと整合グループを管理できるようになります。

詳細はこちら。

- "非同期ミラーリングを使用するための要件"
- "ボリュームを非同期でミラーリングするためのワークフロー"
- "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を確認できます。

- "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"
- "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、遠距離にあるストレージアレイ間の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何ですか？

_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。ストレージアレイコントローラがミラーリング処理を管理します。この処理は、ホストマシンとソフトウェアアプリケーションに対して透過的に行われます。

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確保に最適です。

詳細はこちら。

- "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を実行するには、Unified Managerインターフェイスを使用する必要があります。設定が完了したら、System Managerでミラーペアを管理できます。

詳細はこちら。

- "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ときは、どのような点に注意する必要がありますか"
- "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、データボリュームをオンデマンドで、またはスケジュールに基づいてコピーします。これにより、データの破損や損失が原因で発生するダウンタイムを回避または最小限に抑えることができます。

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ったときに送信されます。

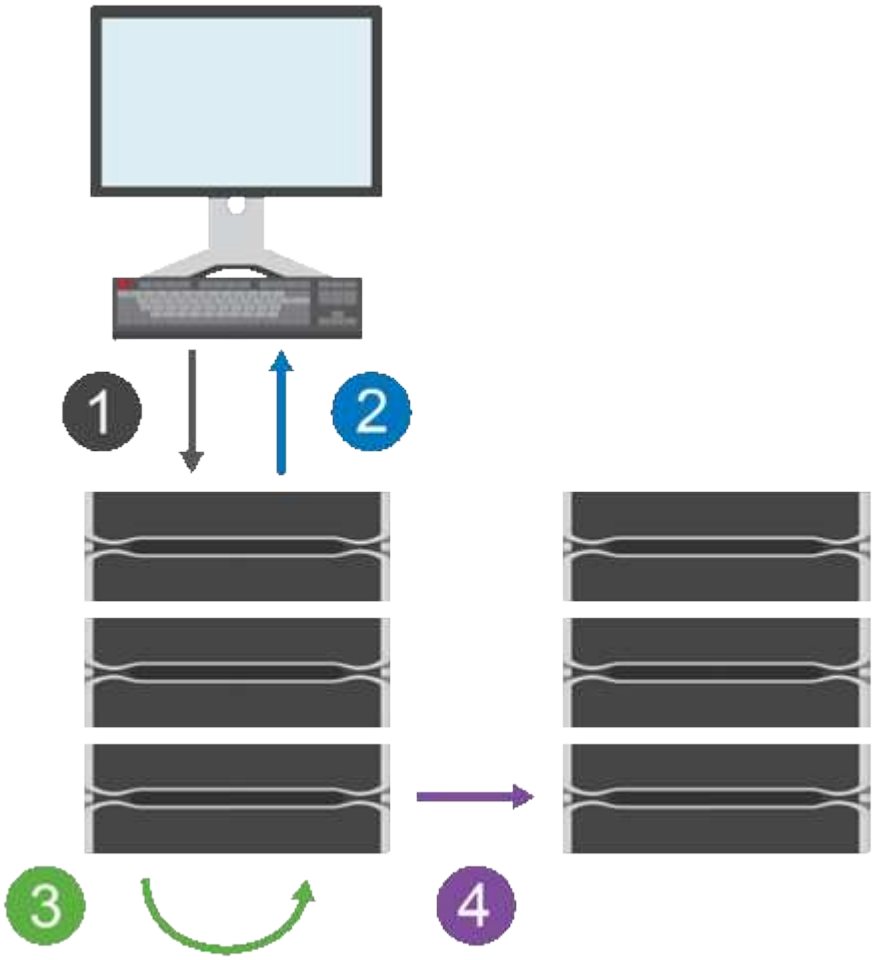
このタイプのミラーリングはノンストップオペレーションの要求に応えるための手段として最適であり、一般的には、バックアップやアーカイブなどの定期的なプロセスをはるかに少ないネットワーク負荷で実施できます。非同期ミラーリングを使用する理由は次のとおりです。

- 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ったときに送信されます。

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. 最初にプライマリボリュームのストレージアレイで書き込み処理が実行されます。
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上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には関連付けられていないため、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の最小バージョンは7.84でなければなりません（それぞれ異なるバージョンのOS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の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、1つの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というミラーペアで構成されます。

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問題
- セカンダリボリュームの障害
- ミラーペアの同期が手動で一時停止されている。
- 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。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。

設定と管理

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	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。書き込み処理はまずプライマリボリュームに対して実行され、その後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	ロール変更とは、セカンダリボリュームにプライマリロールを、セカンダリボリュームにプライマリロールを割り当てる処理です。
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	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。また、通信が中断されて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ときにも実行されます。通信リンクが再確立されると、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。

ボリュームを非同期で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、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、手動同期とスケジュールされた同期のどちらを実行するかを指定します。
   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のみ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、システムでは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 の略

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各コントローラにイーサネット管理ポートが設定されていて、各コントローラが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（それぞれ異なるバージョンのOS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対してFCとiSCSIの両方の接続が確立されている場合は、そのグループでどちらを使用するかを選択することができます。あるチャネルタイプから別のチャネルタイプへのフェイ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のI/Oポートを使用して、プライマリ側からセカンダリ側にミラーデータが送信されます。

- * 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。このポートでは、ミラーリング処理の対象となるコントローラからのI/O要求のみが許可されます。

  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のI/Oポートを使用して、プライマリ側からセカンダリ側にミラーデータが送信されます。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の機能であるため、iSCSI接続（TCP / IPベースの接続）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には、プライマリボリュームと同等以上のサイズが必要です。
- ボリュームに設定できるミラー関係は1つだけです。
- ボリューム候補は、同じ データ セキュリティ 機能を共有している必要があります。
  - 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	説明
同期（初期）	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行状況。 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）	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行状況。

ステータス	説明
システムが中断しました	ミラー整合性グループレベルで、すべてのミラーペアに関して、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失敗状態です。
ユーザが中断しました	ミラー整合性グループレベルで、すべてのミラーペアに関して、データの同期がユーザによって一時停止された状態。 この状態は、ローカルストレージアレイ上の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際に発生する可能性があるホストアプリケーションへのパフォーマンスへの影響を軽減するのに役立ちます。
一時停止中	リモートストレージアレイにアクセスする際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ています。
孤立	孤立したミラーペアボリュームは、ミラー整合性グループの一方（プライマリまたはセカンダリ）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/実行中です	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。 ロールの（プライマリロールまたはセカンダリロールへの）反転変更は、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影響します。 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。 ロールの競合は、通信の問題が解決した時点で発生します。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際には、強制昇格は許可されません。

ミラーペアのステータス

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	説明
同期中です	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行状況。 同期には、初期同期と定期的同期の2種類があります。初期同期の進行状況は、[実行時間の長いオペレーション（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は同期されています。これは、ストレージアレイ間の接続に問題がなく、各ボリュームが想定される動作状態であることを示します。
不完全です	System Managerでサポートされていないストレージアレイ上でミラーペアの作成手順が開始され、セカンダリ上でミラーペアが完成していないため、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が追加されたときに完了します。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成します。
失敗しました	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に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、ミラー整合性グループの一方（プライマリまたはセカンダリ）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。
停止しました	ミラー整合性グループがシステムによる一時停止状態のため、ミラーペアは停止状態です。

ボリューム所有権

ミラーペア内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、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セカンダリボリュームの所有者も自動的に変更されます。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に所有されているプライマリボリュームの所有コントローラをコントローラ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で、セカンダリボリュームの所有コントローラがコントローラ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。

コントローラがリセットされます

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別の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リモート書き込みが行われる前に、コントローラのリセットまたは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、コントローラはミラーペアの完全な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で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た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。そのため、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。ロール変更では、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、または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できます。

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たホストはボリュームへの書き込みアクセスができなくなります。
- 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するホストはボリュームに書き込めるようになります。
- 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ミラー整合性グループ内のメンバーボリュームの昇格またはプライマリミラー整合性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 グループ：

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、そのミラー整合性グループ内の新しく昇格されたメンバー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。

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が許可されるのは、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ていて、一貫したリカバリポイントがある場合のみです。

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ある。
- （フルリザーブ容量エラーなどが原因で）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。
- 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ない。
- 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に障害が発生している。

ミラーグループのロールの競合

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状態を回避して、後続のリカバリ手順を行わないようにするには、ストレージアレイ間の接続が回復するまで待ってから強制的にロールを変更してください。

ロール変更を実行中です

ミラーリング構成内の2つのストレージアレイの接続が切断されて、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、 その後、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。

概念を同期します

同期ミラーリングの仕組み

同期ミラーリングでは、データボリュームをリアルタイムでレプリケートして、継続的な可用性を確保します。

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しておくことにより、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、どの時点においてもコピーは本番環境のデータと同一です。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。

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確保に最適です。

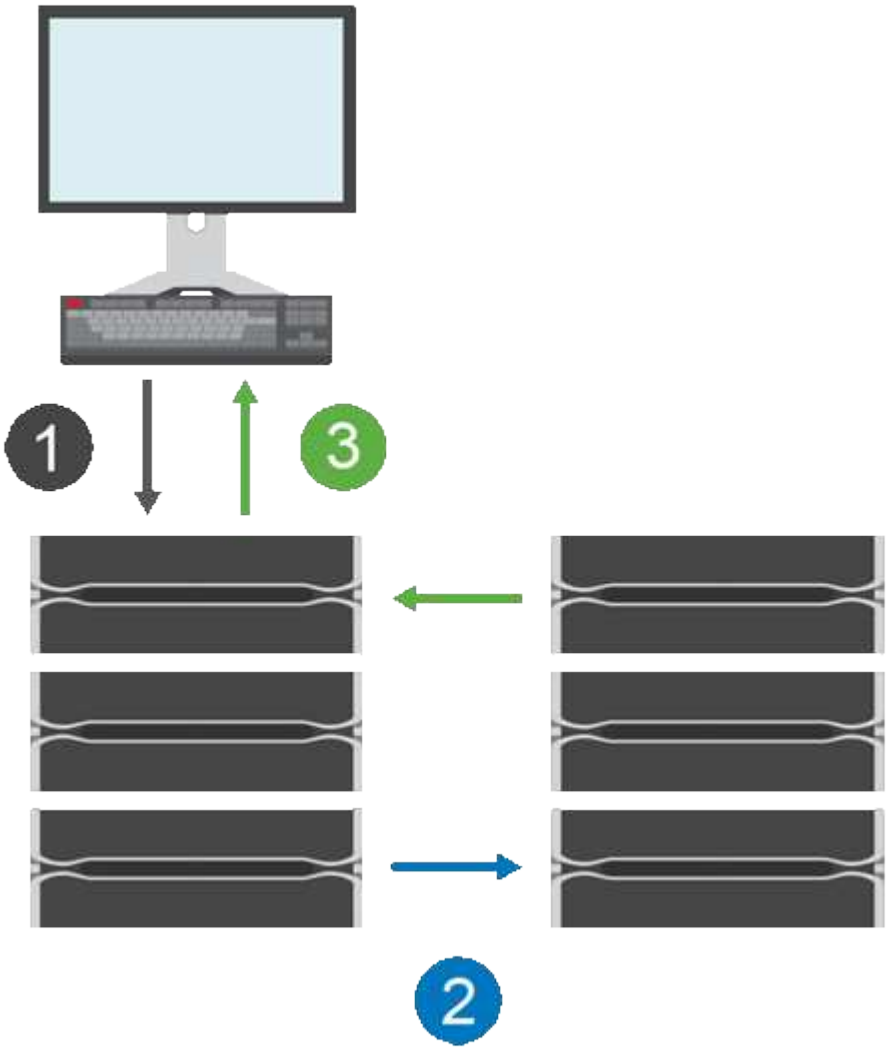
同期ミラー関係

同期ミラー関係は、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。同期ミラーリングは以下のように実行されます。



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。

同期されていないデータ

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問題
- セカンダリボリュームの障害
- ミラーペアの同期が手動で一時停止されている

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	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、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ないことを意味します。RPOがゼロより大きい場合は、セカンダリボリュームのデータがプライマリボリュームよりも古いことを示します。
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	ロール変更とは、セカンダリボリュームにプライマリロールを、セカンダリボリュームにプライマリロールを割り当てる処理です。
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。また、通信が中断されて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ときにも実行されます。通信リンクが再確立されると、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、通常の動作を行って同期を維持しようとします。新しいブロックと変更されたブロックのみ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に行われるため、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を確保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 の略

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各コントローラにイーサネット管理ポートが設定されていて、各コントローラが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（それぞれ異なるバージョンのOS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には、プライマリボリュームと同等以上のサイズが必要です。
- 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、作成済みの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、ミラーペアに含まれるボリュームのコンポーネントステータスとは無関係です。

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

同期ミラーペアは、次のいずれかのステータスになります。

- 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機能しており、各ボリュームが想定される動作状態になっています。

- 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のブロックだけ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。ローカルホストは引き続きプライマリボリュームへの書き込みを行うことができますが、リモートでの書き込みは行われません。次に示すような別の条件によって、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くなる場合があります。

  - セカンダリボリュームにアクセスできない。
  - 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。
  - 新しいWorld Wide Identifier（WWID）を使用してセカンダリボリュームを更新できない。

- 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ると、セカン

ダリボリュームへの接続は試行されなくなります。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

ミラーペア内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、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セカンダリボリュームの所有者も自動的に変更されます。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に所有されているプライマリボリュームの所有コントローラをコントローラ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で、セカンダリボリュームの所有コントローラがコントローラ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。

コントローラがリセットされます

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別の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リモート書き込みが行われる前に、コントローラのリセットまたは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、コントローラはミラーペアの完全な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で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た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。そのため、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。ロール変更では、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、または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。

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、そのミラーペア内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たホストはボリュームへの書き込みアクセスができなくなります。
- 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するホストはボリュームに書き込めるようになります。
- 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、ミラーペア内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して通信の問題が解決すると、「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、ミラーペア内のボリュームの強制昇格が許可されません。

- ミラーペア内のいずれかのボリュームが初期同期中である。
- 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に障害が発生している。

ロール変更を実行中です

ミラーリング構成内の2つのストレージアレイの接続が切断されて、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ると、 その後、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。

システムでは、変更ログを転送し、再同期を実行し、ミラーペアを通常の動作状態に戻して、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をテストする

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間の通信に関する潜在的な問題を診断できます。

作業を開始する前に

テスト対象のミラー整合性グループが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に存在する必要があります。

このタスクについて

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て、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メンバーボリュームと一致するかどうかも検証します。
- * 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。

   [通信のテスト]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た情報を確認します。

通信テストのステータス	説明
正常。エラーはありません	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）	ネットワークまたは接続に問題がないかどうかを確認してから、もう一度テストを実行してください。
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。
ポートの接続エラーです	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ことが原因である可能性があります。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正常、パス、失敗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で、ミラー整合性グループ間の通信が復旧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を中断または再開します

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。

このタスクについて

グループでの同期を中断および再開すると、ホストアプリケーションのパフォーマンスへの影響を軽減できます。このパフォーマンスへの影響は、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間に発生する可能性があります。

ミラー整合性グループとそのミラーペアは、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になります。

手順

1. メニューを選択します。Storage [非同期ミラーリング]。
2. [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テーブルが表示され、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たときに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のミラー整合性グループがデータの初回同期時や非同期ミラーリング処理中のデータの再同期時に使用する、同期設定と警告しきい値を変更できます。

このタスクについて

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適用されます。

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テーブルが表示され、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	説明
ミラーペアを同期する方法を選択…	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を手動で再同期します

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。

   Mirror Consistency Groupテーブルが表示され、ストレージアレイに関連付けられた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へ、変更されたデータが更新されます。

ミラー整合性グループ間で同期されていないデータ量を表示します

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が非同期ステータスの場合は、ミラーリングアクティビティが実行されません。

このタスクについて

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や、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。

   Mirror Consistency Groupテーブルが表示され、ストレージアレイに関連付けられた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**アドレスを更新します

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。

作業を開始する前に

iSCSI接続を使用して非同期ミラーリングを行うために、ローカルストレージアレイとリモートストレージア

レイの両方を設定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。

   Mirror Consistency Groupテーブルには、ストレージアレイに関連付けられた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をプライマリまたはセカンダリに変更します

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することができます。

このタスクについて

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。

   Mirror Consistency Groupテーブルが表示され、ストレージアレイに関連付けられた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の表に、ロール変更中のミラー整合性グループの横にステータス「pending」または「in-progress」が表示されます。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が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、または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を削除します

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で不要になったミラー整合性グループを削除することができます。

作業を開始する前に

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。

   Mirror Consistency Groupテーブルが表示され、ストレージアレイに関連付けられた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、続い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。

完了後

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た場合、リモートストレージアレイからはミラー整合性グループが削除されずに残ってしまうことがあります。この場合は、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

非同期ミラー関係を削除します

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。

このタスクについて

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またはリモートストレージアレイ）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。

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上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なミラーリング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返します。
- 非同期ミラーペアを削除することで、非同期ミラーリングタイルを更新します。

リザーブ容量を増やします

ストレージオブジェクトに対する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ている容量であるリザーブ容量を増やすことができます。

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。一般には、ストレージオブジェクトのリザーブ容量がフルに近付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。

作業を開始する前に

- 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。

このタスクについて

次のストレージオブジェクトの場合、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見込まれる場合や、特定のコピーサービス処理のライフサイクルが非常に長くなる場合は、リザーブ容量の割合を高くします。

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が含まれているプールまたはボリュームグループに空き容量が存在せず、ストレージアレイに未割り当ての容量がある場合は、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上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の設定を変更する

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設定を適宜変更します。

フィールドの詳細

設定	説明
アラートの送信しきい値	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を作成します

System Managerで管理できない従来の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を使用してそのアレイにセカンダリボリュームを作成できます。

このタスクについて

System Managerで管理可能な別のインターフェイスや新しいアレイを使用する従来型アレイ間で、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. 次のいずれかのオプションボタンを選択して、ミラーペア作成手順を自動と手動のどちら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。デフォルト設定を使用してセカンダリボリューム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。

◦ 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。

- デフォルトの設定を使用します。

  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%であり、通常はこの容量で十分です。

- データストレージの非同期ミラーリング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

  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。

  - ミラーペアを長期にわたって維持する場合。
  - 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が作成され、ミラーペアのリモート側にリザーブ容量が割り当てられます。
- 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の間で初期同期を開始します。
- 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、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。この転送によって、初期同期を完了するために転送する必要があるデータの量が削減されます。
- 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。

同期ミラーペアを管理します

同期ミラーリングの通信をテストします

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の通信に関する潜在的な問題を診断できます。

このタスクについて

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上にあ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、表示された修正措置を実行します。

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で、ミラーペア間の通信が復旧するまでテストが続行されます。

ミラーペアの同期を中断して再開します

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。

このタスクについて

ミラーペアを手動で中断した場合、そのペアは手動で再開するまで同期されません。

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ログに記録します。
- 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ロールを変更します

同期ミラーリング対象のミラーペアに含まれる2つのボリューム間でロールを交換することができます。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

場合に必要となることがあります。

このタスクについて

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、またはセカンダリボリュームをプライマリロールに昇格することができます。プライマリボリュームにアクセスしているホストには、そのボリュームへの読み取り/書き込みアクセスが許可されます。プライマリボリュームがセカンダリボリュームになった場合、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その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を変更します。選択した内容に応じて、System Managerはミラーペアのセカンダリボリュームのロールをプライマリに昇格するか、またはプライマリボリュームのロールをセカンダリに降格します。

ミラーペアの同期の設定を変更する

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。

このタスクについて

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。

同期速度について

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上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。このオプションを選択すると、最適なタイミングでデータをリカバリできます。
   - 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。

同期ミラー関係を削除する

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。

このタスクについて

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（ローカルまたはリモート）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上とリモートストレージアレイ上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なミラーリング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返します。
- 同期ミラーリングタイルを更新し、同期ミラーペアを削除します。

ミラーリングを非アクティブ化する

非同期ミラーリングを非アクティブ化する

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。

作業を開始する前に

- 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てください。
- 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。

このタスクについて

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アクティビティ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ホストチャネルが、ホストの読み取り要求や書き込み要求を受け入れるようになります。
- このストレージアレイのいずれのボリュームも、ミラー関係の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使用することはできません。

同期ミラーリングを非アクティブ化する

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）のホストポート4を通常の用途に戻すことができます。

作業を開始する前に

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たことを確認してください。

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で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や書き込み要求を受け入れるようになります。
- 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です

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が同期ミラーリング機能と本質的に違う点は、非同期ミラーリングは特定の時点におけるソース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する点です。

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上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。セカンダリボリュームは、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、どの時点においても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とローカルストレージアレイは完全には同期されません。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。

ミラーリング機能間の比較：

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対してリザーブ容量ボリュームが1個必要です。
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をサポートします。	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のサポートされる距離は事実上無制限です。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 レイテンシおよび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）以内とする必要があります。

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、以下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を満たしていることも確認してください。

- 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各コントローラにイーサネット管理ポートが設定されていて、各コントローラが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（それぞれ異なるバージョンのOS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際は、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各コントローラにイーサネット管理ポートが設定されていて、各コントローラが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（それぞれ異なるバージョンのOS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、ミラーペアのリザーブ容量がフルに近付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、一般に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。

- ミラーペアを長期にわたって維持する場合。
- 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、次のいずれかの操作を実行します。

- 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のリザーブ容量は、一般に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どのような場合ですか？

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複数のボリュームがある場合は、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、推奨される候補の一覧が更新されます。選択内容に基づいて最適な候補が表示されます。

表に「該当なし」と表示される場合、どのような理由が考えられますか？

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きに、その非同期ミラーペアに使用でき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。

以下は、プールまたはボリュームグループを使用できない理由です。

- 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ない。
- 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る。

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ない。
- 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アドレスが変わったために、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です。

iSCSI接続と非同期ミラーリング関係を確立する際、ローカルおよびリモート両方のストレージアレイは、リモートストレージアレイのIPアドレスを非同期ミラーリング構成に保存します。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が同期ミラーリング機能と本質的に違う点は、非同期ミラーリングは特定の時点におけるソース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する点です。

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上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。セカンダリボリュームは、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、どの時点においても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とローカルストレージアレイは完全には同期されません。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。

ミラーリング機能間の比較：

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対してリザーブ容量ボリュームが1個必要です。
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。

非同期ミラーリング	同期ミラーリング
• 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をサポートします。	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のサポートされる距離は事実上無制限です。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 レイテンシおよび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）以内とする必要があります。

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。

- ボリュームが、Snapshotボリュームやシンボリュームなどの標準以外のボリュームである。
- 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。

- ボリュームが、Snapshotボリュームやシンボリュームなどの標準以外のボリュームである。
- 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際は、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各コントローラにイーサネット管理ポートが設定されていて、各コントローラが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（それぞれ異なるバージョンのOS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、同期アクティビティに割り当てられる処理時間をシステムパフォーマンスと比較して決定します。

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

優先度は次のとおりです。

- 最低
- 低
- 中
- 高
- 最高

最低ではシステムパフォーマンスが優先されますが、再同期化に時間がかかります。最高では再同期化が優先されますが、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、各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	最高の優先度であれば、約8倍の時間を要します。
低	最高の優先度であれば、約6回。
中	最高の優先度であれば、約3倍から半分。
高	優先度が最高の場合は、約2倍です。

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を使用している場合は、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、最小限のダウンタイムで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。

詳細はこちら。

- "リモートストレージの仕組み"
- "Remote Storageの用語"
- "Remote Storageの要件"
- "Remote Storageのボリューム要件"

この機能を使用してデータをインポートする方法

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（データインポートのソース）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。

詳細はこちら。

- "リモートストレージをインポートします"
- "データの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、最小限のダウンタイムで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

次のワークフローに従って、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、EシリーズおよびSANtricity ドキュメントセンターのユーザガイドで説明しています "Remote Storage Volumes の概要"で、を参照してください "Remote Storageテクニカルレポート"。

> SANtricityリモートストレージボリュームは、現在E4000システムではサポートされていません。

ローカルのEシリーズストレージシステム：

1. 各コントローラがリモートストレージシステムにiSCSI接続されていることを確認します。この接続により、ローカルのEシリーズシステムは、リモートシステム上でホストとして設定できるiSCSIイニシエータとして機能します。
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と同じかそれよりも大きく、同じブロックサイズでマッピングされていないことを確認してください。を参照してください "ボリュームを作成します"。
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。IQNはあとで、リモートストレージシステムでローカルEシリーズシステムをホストとして設定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Eシリーズシステムをリモートシステム上のホストとして設定します。適切なホストタイプを次のように設定します。
   - 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 "ホストとホストクラスタの概要"。ホストタイプとして「Factory Default」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. 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て、ソースボリュームの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修飾名（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

次のワークフローを使用して、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します。

1. System Managerのインターフェイスで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（データインポートのソース）をEシリーズシステム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. View Operations（操作の表示）ダイアログまたはOperations in Progress（進行中の操作）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解除するか、将来のインポート用に接続を維持します。

Remote Storage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	説明
IQN	iSCSI Qualified Name（IQN）。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。ホストにアクセス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	データが最初に存在するストレージシステム。リモートストレージシステムには、Eシリーズモデルを使用することも、別のベンダーのシステムを使用することもできます。
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格納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、「ボリューム」と呼ばれます。
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ための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と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。

サポートされているプロトコル

サポートされるプロトコルは次のとおりです。

- iSCSI
- IPv4

Eシリーズのサポート情報と設定情報の最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

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必要です。

- 2 台（デュプレックスモード）
- 1 つ以上の iSCSI 接続を介して両方の E シリーズコントローラがリモートストレージシステムと通信するための iSCSI 接続

- SANtricity OS 11.71 以降
- サブモデル ID （ SMID ）で有効化されたリモートストレージ機能

リモートシステムには、 E シリーズストレージシステムと別のベンダーのシステムを使用できます。次のものを含める必要があります

- 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 が存在しないようにします。
- インポートを開始する前に、 E シリーズシステム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が無効になっている必要があります。
- リモートストレージボリュームを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 はサポートされていません。
- 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 / インポートペアにあ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。

Remote Storageのボリューム要件

インポートに使用するボリュームは、サイズ、ステータス、およびその他の条件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ボリューム

インポートのソースボリュームを「リモートストレージボリューム」と呼びます。 このボリュームは次の条件を満たしている必要があります。

- 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によってリモートストレージボリュームがバックグラウンドで作成されます。そのため、リモートストレージボリュームは System Manager では管理できず、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、 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が、次の例外があります。

- 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や 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 設定を変更できません。
- ホストはインポート処理専用に予約されているため、どのホストにもマッピングできません。

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。ただし、 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、次の組み合わせによって一意に識別されます。

- リモートストレージのオブジェクト 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の候補

ターゲットボリュームが、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と同じかそれ以上の容量が必要です。
- リモートストレージボリュームと同じブロックサイズが必要です。
- 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関係を確立することはできません。
- 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。
- インポートを開始する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。

System Manager は、リモートストレージのインポートウィザードの一環として、これらの要件を自動的にチェックします。デスティネーションボリュームを選択する際には、すべての要件を満たすボリュームだけが表示されます。

リモートストレージを管理します

リモートストレージをインポートします

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。

作業を開始する前に

- 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できるように設定されている必要があります。

ハードウェアの構成については、EシリーズおよびSANtricity のドキュメントセンターで入手できる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 "ハードウェアを設定する"で、を参照してください "Remote Storageテクニカルレポート"。

- 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。を参照してください "ボリュームを作成します"。ターゲットボリュームが、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。
  - には、リモートストレージデバイスと同じかそれ以上の容量が必要です。
  - の状態が「最適」で、利用可能です。

要件の一覧については、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。

このタスクについて

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の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	説明
名前	System Managerインターフェイスで識別するリモートストレージデバイス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。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. E シリーズストレージシステムのターゲットボリュームを表から選択します。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。「 continue 」と入力し、「 * Continue * 」をクリックして、次のダイアログボックスで操作を確認します。

   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、 E シリーズシステムに接続されているホストにはその容量は報告されません。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。

   ダイアログで設定を確定すると、 [レビュー（ 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、ターゲット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。ホストがこのプロセス中に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. リモートストレージパネルの View Operations （操作の表示）ダイアログで、操作の進行状況を表示します。

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、ストレージシステムと関連するボリュームの両方の I/O 負荷の量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がリモートストレージデバイスの複製になります。

完了後

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。関係が切断されると、ローカルボリューム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。

リモートストレージの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ると、進行状況を表示して対処することができます。

このタスクについて

インポート処理ごとに、処理の進捗状況ダイアログに完了率と推定残り時間が表示されます。処理には、インポートの優先順位の変更、処理の停止と再開、および処理と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。

   [処理を実行中（Operations in Progress）]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、任意のリモートストレージ構成の接続設定を編集、追加、または削除できます。

このタスクについて

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。中断を避けるため、インポートが実行されていないときにのみ接続プロパティを変更してください。

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. リストから、変更するリモートストレージオブジェクトを選択します。
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の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「削除」と入力して操作を確認し、「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を削除する

インポートの完了後、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する必要がなくなった場合は、リモートストレージオブジェクトを削除できます。

作業を開始する前に

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てください。

このタスクについて

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. 「 re move 」と入力し、「 * Remove 」をクリックして操作を確認します。

   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。

よくある質問です

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ポートを設定"
- "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、ストレージシステムは未使用のリモートボリュームを自動的に検出し、削除するように求めます。

場合によっては、作成プロセス中に未使用のリモートボリュームが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際、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、以下の条件を満たしている必要があります。

- リモートボリュームと同等以上の容量。
- リモートボリュームと同じブロックサイズ。
- 現在のステータスが最適であること。

次の条件を満たすボリューム候補はリストから除外されます。

- 次のいずれかの関係：ボリュームコピー、Snapshot、またはミラーリング。
- 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）へのマッピング。
- 読み取りフラッシュキャッシュが有効です。

インポートで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、リモートボリュームがデータのソース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。この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。

設定

リモートストレージのインポートを作成する前に、次の操作を実行し、以下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と同じかそれよりも大きく、かつソースボリュームと同じブロックサイズでマッピングされていないことを確認します。を参照してください "ボリュームを作成します"。
- 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上のホストとして設定します。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。
- 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て、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対する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修飾名（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、ローカルの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。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、インポートの作成後に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

以下に、インポートプロセスの概要を示します。

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。手順の詳細については、を参照してください "リモートストレージをインポートします"。

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。インポート処理にかかる時間は、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設定、ストレージシステムとその関連ボリュームのI/O負荷の量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がソースボリュームと同じになります。

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、ローカル宛先のパフォーマンスは通常に戻り、リモート接続による影響を受けなくなります。

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 が存在しないようにします。
- インポートを開始する前に、 E シリーズシステム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が無効になっている必要があります。
- リモートストレージボリュームを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 はサポートされていません。
- 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 / インポートペアにあ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。

どのコンポーネントを管理できますか？

コンポーネントのステータスを確認し、次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これには、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。

詳細はこちら。

- "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

ストレージアレイの物理コンポーネントをグラフィカルに表示するハードウェアページに移動します。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。

詳細はこちら。

- "シェルフコンポーネントのステータスと設定を表示します"
- "コントローラの設定を表示します"
- "ドライブのステータスと設定を表示します"

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およびドロワー損失の保護が有効です"

概念

ハードウェアの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の図が表示されます。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、ストレージアレイ用のハードウェア（コントローラ、電源/ファンキャニスター、ドライブ）が搭載され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ID番号が割り当てられます。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場所を確認しやすいように、シェルフのロケーターライトをオンにします。
- 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。
- シェルフビューを上下に移動して、ストレージアレイ内の物理的なレイアウトと一致させます。

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あり、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ています。

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）。
- ネットワークタイムプロトコル（NTP）サーバおよびドメインネームシステム（DNS）サーバを設定する。
- 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外のユーザがコントローラ上で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します。

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）を搭載できます。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。

- シェルフ内でドライブの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オンにします。
- 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	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、データ用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、ドライブシェルフをコントローラシェルフまたはその他のドライブシェルフに接続するSASポートが搭載されています。
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、シェルフに搭載されるアセンブリです。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を収容します。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は、コントローラとドライブを収容します。ドライブシェルフは、入出力モジュール（ IOM ）とドライブを収容します。
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	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	動的ホスト構成プロトコル（DHCP）は、インターネットプロトコル（IP）ネットワークでIPアドレスなどのネットワーク設定パラメータを動的に配布するために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保持し、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が完全に冗長化されます。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では、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つのデバイスが双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で通信できます（一方のデバイスがメッセージを送信し、他方のデバイスが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のことをベースボードホストポートと呼び、HIC に搭載されたホストポートのことを HIC ポートと呼びます。
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	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；最大転送単位）は、ネットワークで送信可能な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。
シンプレックス構成です	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構成になります。
VLAN	仮想ローカルエリアネットワーク（VLAN）は、同じデバイス（スイッチやルータなど）でサポートされる他のネットワークと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	説明
ダ	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に対応した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。これらのドライブにドライブセキュリティ機能を使用すると、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は動作しなくなり、取り付けた時点で正しいセキュリティキーが提供されるまでは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、ドライブシェルフをコントローラシェルフまたはその他のドライブシェルフに接続するSASポートが搭載されています。
DULBE	Deallocated or Unwritten Logical Block Error（DULBE）はNVMeドライブのオプションです。このオプションにより、EF300またはEF600ストレージアレイでリソースプロビジョニングボリュームをサポートできます。
FDEドライブ	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。ハードドライブに搭載されたASICチップにより、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。
FIPSドライブ	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で障害が発生すると、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。
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。以前の論理デバイスインターフェイスに比べ、I/Oオーバーヘッドが少なく、パフォーマンスも向上しています。

コンポーネント	説明
（ 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。読み取りおよび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しか実行できません。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 の場合	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	説明
CHAP	チャレンジハンドシェイク認証プロトコル（CHAP）方式では、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_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	動的ホスト構成プロトコル（DHCP）は、インターネットプロトコル（IP）ネットワークでIPアドレスなどのネットワーク設定パラメータを動的に配布するために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、構成が可能なプロトコルです。
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；最大転送単位）は、ネットワークで送信可能なパケットまたはフレームの最大サイズです。

期間	説明
RDMA	Remote Direct Memory Access（RDMA）は、ネットワークコンピュータ同士が、それぞれ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でデータを交換できるテクノロジです。
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	説明
InfiniBandの略	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、ストレージアレイでは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の一意の識別子です。1~255の値を設定できます。SCSIの論理ユニット番号（LUN）に相当します。
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	非揮発性メモリ（NVM）は、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。
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。以前の論理デバイスインターフェイスに比べ、I/Oオーバーヘッドが少なく、パフォーマンスも向上しています。
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の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キューです	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です。
RDMA	Remote Direct Memory Access（RDMA）を使用すると、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実現できます。
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	説明
SSD の場合	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を表示します

[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およびフィルタリング機能があります。

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	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を使用すると、ページに表示するドライブの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、個別に使用することもでき 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	説明
ステータスアイコンの詳細を表示します	ステータスインジケータには、可用性の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、関連コマンドのリスト、およびプロパティと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。上部のアイコンを選択して、各コンポーネントのステータスとプロパティを確認することもできます。コントローラ、IOM（ESM）、電源装置、ファン、温度、 バッテリ、SFP。
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できます。

構成部品のステータスを表示または非表示にします

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. ポップオーバーのステータスの説明を表示または非表示にするには、次の手順を実行
   - 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。

正面図と背面図を切り替えます

ハードウェアページでは、シェルフの前面ビューと背面ビューのどちらかを確認できます。

このタスクについて

背面ビューには、コントローラ/ IOMおよび電源/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します

ハードウェアの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に合わせて変更できます。

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します

ハードウェアのページに表示される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**を変更します

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。

このタスクについて

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、別の番号に変更することもできます。

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を表示します

ハードウェアページには、電源装置、ファン、バッテリなど、シェルフコンポーネントのステータスと設定が表示されます。

このタスクについて

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、次の表に示す一部のタブが表示されない場合があります。

タブをクリックする	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。

タブをクリックする	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構成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。 このステータスは、IOMアイコンを選択して確認することもできます をクリックします。
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。 電源装置アイコンを選択して、このステータスを確認することもできます をクリックします。
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。 ファンアイコンを選択して、このステータスを確認することもできます をクリックします。
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。 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 をクリックします。
電池	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。 このステータスは、バッテリアイコンを選択して確認することもできます をクリックします。

タブをクリックする	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。 このステータスは、SFPアイコンを選択して確認することもできます をクリックします。

3. [* 閉じる *] をクリックします。

バッテリ学習サイクルを更新します

学習サイクルは、スマートバッテリゲージを調整する自動サイクルです。このサイクルは、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す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。

このタスクについて

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。

コントローラを管理する

コントローラの状態

コントローラには、オンライン、オフライン、およびサービスモードの3種類の状態があります。

オンライン状態です

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。これは、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。

オフライン状態です

オフライン状態は、通常、コントローラが2台あるストレージアレイでコントローラの交換を準備するときに使用します。コントローラがオフライン状態になるのは、明示的なコマンドを問題 に設定した場合、またはコントローラで障害が発生した場合です。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台ある場合のみです。

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。

- そのコントローラをI/Oに使用できません
- そのコントローラを使用して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は無効になり、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なります。

サービスモード

サービスモードは、通常はテクニカルサポートのみが使用するモードです。コントローラを診断できるように、ストレージアレイのすべてのボリュームを1台のコントローラに移動します。コントローラのサービスモードへの切り替えは手動で行う必要があり、サービスの処理が完了したら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ときは次の状況になります。

- そのコントローラを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を介して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は無効になり、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なります。

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。ただし、別の方法で管理ポートのIPアドレスを設定し、そのあとにSystem Managerを使用して管理ポートで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（LANから切断された状態）の場合、システムは設定を静的と報告してIPアドレスとして0.0.0.0を表示するか（以前のリリース）、DHCPが有効と報告してIPアドレスを表示しないか（新しいリリース）のどちらかです。ネットワークポートが「リンク稼働」状態（LANに接続されている状態）になると、DHCP経由でIPアドレスの取得が試行されます。

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、これには最大3分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は、次の点に

- コントローラのポート2は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。
- E4000、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システムマネージャを使用します。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すると失われます。コントローラのネットワークポートがDHCPを使用するように設定されている場合、ケーブルの差し込み、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の試行に失敗した場合は、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。

管理ポートを設定します

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。

このタスクについて

この手順 では、ポート1を選択し、速度とポートの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	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。リストには、速度と二重モードの有効な組み合わせのみが表示されます。
IPv4 を有効にする / IPv6 を有効にする	一方または両方のオプションを選択して、 IPv4 ネットワークと IPv6 ネットワークのサポートを有効にします。

   [**IPv4**を有効にする]を選択すると、[次へ*]をクリックした後に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 と IPv6 、またはその両方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	説明
DHCP サーバから自動的に設定を取得します	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。
静的な設定を手動で指定します	このオプションを選択した場合は、コントローラのIPアドレスを入力します。（必要に応じて、住所をカットアンドペーストして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も指定します。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 アドレスも指定します。 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サーバアドレスを設定する

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クロックを更新できるようになります。

作業を開始する前に

- 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つ以上入力した場合は、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。

このタスクについて

NTPを設定すると、ストレージアレイがSimple Network Time Protocol（SNTP）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るようになります。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、設定しておくことで、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（NTPサーバーの設定）*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その他の選択項目が表示されます。

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NTPサーバアドレスを自動的に取得*--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。（これらの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。
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サーバアドレスを設定する

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されます。ストレージアレイの管理ポートは、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。

作業を開始する前に

- 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アドレスでもIPv6アドレスでもかまいません。

このタスクについて

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サーバで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、かつ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がありません。この場合、DNS / NTPサーバのアドレスはストレージアレイによってすでに自動的に検出されているはずです。ただし、次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. 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。（これらの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アドレスでもIPv6アドレスでもかまいません。
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。

コントローラの設定を表示します

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、コントローラに関する情報を確認できます。

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. タブを選択して、プロパティ設定間を移動します。

   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

タブをクリックする	説明
ベース（ Base ）	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、不揮発性静的ランダムアクセスメモリ（NVSRAM）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喪失した場合にデータをキャッシュに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、取り外し、不明、書き込み禁止、 または互換性なし。
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、Fibre ChannelやiSCSIなど、コントローラとホストの間の接続です。 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）内のいずれかです。「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の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	コントローラへのアクセスに使用されるホスト名、リモートログインが有効になっているかどうかなど、管理ポートの詳細が表示されます。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保持し、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外のユーザがコントローラ上で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、SSHキーやSSHパスワードの入力をユーザに求めることで、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表示されます。

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。

   この設定では、リモートログインに次の3つの許可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できます。
   - * SSHキーまたはパスワード*。このオプションについては、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。#で始まる行と空白行は無視されます。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では、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セッションがすべて終了し、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します

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によって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要求を受け取った時点で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します

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。

作業を開始する前に

- ストレージアレイに2台のコントローラが必要です。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、またはボリュームを使用しているすべてのホストにマルチパスドライバがインストールされていることを確認してください。

このタスクについて

```
[CAUTION]
====
Recovery
Guruまたはテクニカルサポートの指示があった場合を除き、コントローラをオフラインに切り替えないでください。

====
.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。



[[IDbb7ad4cf64399103d1a8cbc3695e111f]]
= コントローラをサービスモードにします
: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。

.作業を開始する前に
* ストレージアレイに
2台のコントローラが必要です。サービスモード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、またはボリュームを使用しているすべてのホストにマルチパスドライバがインストールされていることを確認してください。

[NOTE]
====
コントローラをサービスモードに切り替えると、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の指示があった場合を除き、コントローラをサービスモードに切り替えないでください。

====
.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。

. [サービスモードに切り替え]を選択し、操作を確定します。

[[IDb9d5d36a32e1fd8e36c68986a88f6a9a]]
= コントローラをリセット（リブート）します
: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。

.作業を開始する前に
* ストレージアレイに
2台のコントローラが必要です。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、またはボリュームを使用しているすべてのホストにマルチパスドライバがインストールされていることを確認してください。

.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。

. 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

[[ID2142840280de998f9e43c7b7cafc1617]]
= iSCSIポートを設定
: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でiSCSIポートを設定できます。

.作業を開始する前に
* 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の設定および機能は、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。

====
+
Configure iSCSI Ports （ 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,~"]
|===
| ポートの設定 | 説明

 a|
設定された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）
 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;前方誤り訂正）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）

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モードは、25Gbpsポート速度をサポートしていません。

a|
IPv4 を有効にする / IPv6 を有効にする

a|
一方または両方のオプションを選択して、 IPv4 ネットワークと IPv6 ネットワークのサポートを有効にします。

NOTE: ポートへのアクセスを無効にする場合は、両方のチェックボックスを選択解除します。

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 ；最大伝送ユニット）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 ；最大転送単位）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 応答を有効にします

a|
Internet Control Message Protocol （ ICMP ）を有効にする場合は、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。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。

|===
====
+
[*IPv4 を有効にする *] を選択した場合は、 [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 と IPv6
、またはその両方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,~"]
|===
| ポートの設定 | 説明

a|
自動的に設定を取得します
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|
静的な設定を手動で指定します
a|
このオプションを選択した場合は、フィールドに静的アドレスを入力します。（必要に応じて、住所をカットアンドペーストして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も指定します。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 アドレスも指定します。

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 を入力する場合は、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
（ローカルエリアネットワーク）および仮想 LAN
から物理的に分離された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場合は、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。

共有 LAN
環境（イーサネットなど）では、多数のステーションがネットワークアクセスで競合する可能性があります。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、再試行するまで待機します。スイッチイーサネットでは、 1
つのステーションだけがスイッチポートに接続されるため、このプロセスは最小限に抑えられます。

|===
====
. [完了] をクリックします。

[[IDe442cf8ca107b37a89812c7ac4e8615e]]
= iSCSI認証を設定
: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。

.作業を開始する前に
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iSCS

I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、手動で入力する必要はありません。

.このタスクについて
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できるようにし、さらに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、二次的な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（認証の設定）ダイアログボックスが表示され、現在設定されている方式が示されます。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。

. 双方向認証について、任意の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。

[[ID9813e3279e6c252d82adc3ac27a17577]]
= iSCSI検出設定を有効にします
: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設定できます。

.作業を開始する前に
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ています。

.このタスクについて
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ります。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、住所をカットアンドペーストしてフィールドに貼り付けることもできます）。 フィールドに、IPv4アドレスまたはIPv6アドレスを入力します。両方を設定した場合は、IPv4がデフォルトです。また、TCPリスニングポートを入力します（デフォルトの3205を使用するか、49152~65535の値を入力）。

. 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、セキュリティが向上します。

. [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。この処理には最大5分かかることがあります。

[[ID889233afe25ac6aa4835a13332bf119b]]
= iSCSI統計パッケージを表示します
: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。

.このタスクについて
System Managerには、次のタイプの
iSCSI統計が表示されます。統計はすべて読み取り専用で、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ている一意のアドレスです。MACアドレスは、サブネットワーク内のデスティネーションへのデータパケットの配信に役立ちます。
* *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、ネットワークホスト上のアプリケーションが相互に接続を作成し、パケットでデータを交換できます。IPは、パケット交換インターネットワークを介して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、識別や機能のために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。

```
[[ID1148f9e5cd9811341298711135 20c7e7]]
= iSCSI セッションを表示します
: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確立できます。

.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。

. *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 | 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、ISIDとTPGTで構成されます。



 a|
イニシエータセッション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|
イニシエータの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。1~4を接続の最大数として指定できます。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|
イニシエータのエイリアス
a|
イニシエータに関連付けられているラベル。

a|
ターゲットの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（バイト単位）。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|
接続の終了または接続のリセット後に接続を試行するまでの最小秒数。0~3600をデフォルトの待機時間の値として指定できます。デフォルトは* 2 *です。

a|
デフォルトの保持時間です
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。0~3600をデフォルトの保持時間として指定できます。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。1~16を未処理の「準備が完了した転送」の最大値として指定できます。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ペイロードデータユニット（PDU）で受信できる最大データ量。

 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'iscsi-session-connections.txt'というファイル名でファイルが保存されます

[[IDbd46fb0a1e94ab9d139f5b9b73e90200]]
= iSCSIセッションを終了します
: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確立できます。

.このタスクについて
iSCSIセッションを終了する理由としては、次のようなものが考えられます。

* *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。認証方法を「なし」にしたため、iSCSIイニシエータがログオンし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。

[[IDe489614dd41c40020a94acdc45005cb3]]
= iSER over InfiniBandポートを設定します
: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。

.作業を開始する前に
* 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。

+
Configure iSER over InfiniBand ports（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。

[[IDf767c93680b93ae8664f09fa284db09a]]
= iSER over InfiniBandの統計を表示します
: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。

.このタスクについて
System Managerには、次のタイプのiSER over InfiniBand統計が表示されます。統計はすべて読み取り専用で、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

[[IDa3f97e09e4519160a18e421d6142cd97]]
= 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インターフェイスのエンドツーエンドがホストからストレージへ拡張され、コマンドセットが標準化、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示されます。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 Qualified Nameは常にサブシステムによって割り当てられ、変更はできません。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。

== ネームスペースおよびネームスペース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

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を表すSCSI I_T
Nexusと同様に、ホスト接続プロセスで作成される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コントローラを関連付けることができるのは単一のホストのみですが、NVMeコントローラは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。

[[ID7dbecbd0e80a107479943c6fdf9cbac9]]
= NVMe over InfiniBandポートを設定する
: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でNVMeポートを設定できます。

.作業を開始する前に
* 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。
+
Configure NVMe over InfiniBand Ports（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。これらの設定により、ホストは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。

[[ID833c62e75f0d4208e2547930222d2319]]
= NVMe over RoCEポートを設定します
: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）用の接続が含まれている場合は、ハードウェアページでNVMeポートを設定できます。

.作業を開始する前に
* 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。
+
Configure NVMe over RoCE Ports（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,~"]
|===
| ポートの設定 | 説明

a|
イーサネットポート速度の設定
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|
一方または両方のオプションを選択して、 IPv4 ネットワークと IPv6
ネットワークのサポートを有効にします。

NOTE: ポートへのアクセスを無効にする場合は、両方のチェックボックスを選択解除します。

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
；最大伝送ユニット）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 ；最大転送単位）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 *] を選択した場合は、 [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 と IPv6 、またはその両方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,~"]
|===
| ポートの設定 | 説明

 a|
自動的に設定を取得します
 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|
静的な設定を手動で指定します
 a|
このオプションを選択した場合は、フィールドに静的アドレスを入力します。（必要に応じて、住所をカットアンドペーストして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も指定します。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 アドレスも指定します。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。これらの設定により、ホストは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。

[[IDaee3d5914d17bea9b8635ee3e88fb898]]
= NVMe over Fabricsの統計を表示します
: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。

.このタスクについて
System Managerには、次のタイプのNVMe over Fabrics統計が表示されます。統計はすべて読み取り専用で、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

= ドライブを管理します

:leveloffset: +1

[[ID92b1c9991979e20ad3d14bdbdb76346e]]
= 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、ドライブのさまざまな状態が報告されます。

== アクセスの状態

[cols="25h,~"]
|===
| 状態 | 定義（ Definition ）

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かのポートで通信できません。

a|
互換性なし
a|
次のいずれかの状況に該当します。

* ストレージアレイでの使用が認定されていないドライブです。
* ドライブのセクターサイズが異なります。
*
ドライブの設定データが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で使用できません。

a|
削除されました
a|
ドライブがストレージアレイから取り外されています。

a|
あり
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|
応答しません
 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,~"]
|===
| 状態 | 定義（ Definition ）


 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す。




 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ありません。

|===


== 可用性の状態
```

```
[cols="25h,~"]
|===
| 状態 | 定義（ Definition ）


 a|
失敗しました
 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|
オフラインです
 a|
ドライブをデータの格納に使用できません。通常は、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を実行中であることが原因です。



 a|
最適
 a|
ドライブは正常に動作しています。

|===



[[ID8849422aaf2080816e8cb07dbebbf417]]
= 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の利点

ハードドライブに比べてSSDを使用する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
* IOPS（1秒あたりのI/O処理数）が高い
* 少ない可動部品で高い信頼性を実現
* 消費電力の削減
* 熱の発生を抑え、冷却コストを削減します

== SSDの識別

ハードウェアページでは、前面シェルフビューでSSDを特定できます。稲妻アイコンが表示されているドライブベイを探します。このアイコンはSSDが取り付けられていることを示します。

== 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の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することで、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、データは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。

```
[[IDaad4487ef60a726d2cf17bd5d4484440]]
= ドライブ表示を制限します
: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。

.このタスクについて
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）で、特定の論理的場所（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）のみに絞って表示することができます。これらのフィルタは、一緒に使用することも、個別に使用することもでき

[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）
** ドライブの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に準拠（FIPS 140-2）
** FIPSに準拠（FIPS 140-2）
+
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含まれているすべてのSSDドライブが、SASインターフェイスを備えた速度15000RPMのSSDドライブで、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。

+
フィールドで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、グラフィカル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、ドライブの使用可能な論理的場所を表示します。
+
[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。

====
+
論理的な場所には次のものがあり

+
** 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
+
フィールドで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、グラフィカル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でドライブの場所を特定する際に役立ちます。

[[ID219fb428ea2cf67777d023cb8764ec76]]
= ドライブのロケーターライトを点灯します
: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は、ロケーター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確認できます。

.このタスクについて
単一のドライブまたは複数のドライブは、Hardware（ハードウェア）ページに表示されています。

.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。

```
[[IDb648f04679aa28dd0206266d732adc9a]]
= ドライブのステータスと設定を表示します
: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、容量などのドライブのステータスと設定を表示できま

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。
+
Drive Settings（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 | 説明

a|
ステータス
a|
最適、オフライン、重大でない障害、失敗のいずれかが表示されます。「最適」ステータスは、必要な稼働状態を示します。

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、ホットスペア使用中のいずれかが表示されます。

a|
場所
a|
ドライブが配置されているシェルフおよび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、このフィールドには「割り当て先」と表示されます。
指定できる値は、プール名、ボリュームグループ名、またはSSDキャッシュ名です。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、このフィールドには「保護対象」と表示されます。
1つ以上のボリュームグループをホットスペアで保護できる場合は、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、このフィールドには「保護」と表示されます。 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|
ドライブが使用してい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間のデータ転送率が表示されます。

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|
ドライブが使用す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のバージョン
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|
ワールドワイド識別子
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|
メーカー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|
製造元
a|
ドライブのベンダーが表示されます。

a|
製造日
a|
ドライブがビルド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。読み取りおよび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しか実行できません。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|
読み取り/書き込みアクセス可能な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。

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。これらのドライブにドライブセキュリティ機能を使用すると、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は動作しなくなり、取り付けた時点で正しいセキュリティキーが提供されるまでは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に対応した
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。このオプションにより、EF300またはEF600ストレージアレイでリソースプロビジョニングボリュームをサポートできます。

|===
====
. [* 閉じる *] をクリックします。

[[IDfd3bdb76f3040471aa448007c6c3a9a9]]
= ドライブを論理的に交換します
: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。

.このタスクについて
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、関連付けられている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。

次のタイプのドライブを交換するには、論理的交換オプションを使用します。

* 障害ドライブ
* 不明なドライブです
* 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
*
割り当てられたドライブ（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）

.作業を開始する前に
交換用ドライブには次の特性が必要です。

* 最適状態です
* 未割り当て状態
* 交換するドライブと属性（メディアタイプ、インターフェイスタイプなど）が同じ
* 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およびドロワー損失の保護が維持されるドライブを選択してください。

. [*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、データはパリティ情報を使用して交換用ドライブで再構築されます。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を開始します。

+
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を選択した場合は失敗状態に移行します。

[[ID18072c095f444401463ae749b4c1c5b4]]
= ドライブを手動で再構築

```
: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、ドライブの交換後に通常は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。




[[ID21322033ff88b952dae68396094bdee3]]
= ドライブを初期化（フォーマット）します
: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、新しいストレージアレイで使用するには、そのドライブを初期化（フォーマット）する必要があります。

.このタスクについて
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。その後、新しいストレージアレイ内の新しいプールまたはボリュームグループにドライブを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。ストレージアレイ間で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。

[[ID492fe6b191aebd007a71714f8b2316fc]]
= ドライブを使用停止にする
: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、ドライブを手動で使用停止できます。

.このタスクについて
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、割り当てられたドライブおよびRAID 0以外のボリュームグループにのみ表示されます。

+
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、ドライブの内容を最初にコピーしないと、関連付けられているプールまたはボリュームグループ上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るため、コピー処理中に別のドライブで障害が発生した場合のボリューム障害の可能性を低減できます。

. 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、60秒以上待ってから取り外します。

[[IDf1983c4f4cc6214d86841ea4f6db66d3]]
= ドライブを消去します
: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して、未割り当てのドライブをシステムから取り外す準備を行うことができます。この手順 はデータを完全に削除し、データを二度と読み取れないようにします。

.作業を開始する前に
ドライブは未割り当て状態である必要があります。

.このタスクについて
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、[消去]オプションを使用します。セキュリティ有効ドライブの場合、消去オプションは暗号化の消去を実行し、ドライブのセキュリティ属性をセキュリティ対応にリセットします。

[NOTE]
====
消去機能では、一部の古いドライブモデルはサポートされていません。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、ドライブの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
で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。
+
ドライブの消去ダイアログボックスが開き、消去処理に使用でき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
. 「erase」と入力して操作を確定し、「* Erase *」をクリックします。
+
[CAUTION]
====
この処理を続行しますか？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
消去処理には数分または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、その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、あるいは別のストレージアレイで使用できるようになります。

.完了後
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。

[[ID639e78ee5d6993db65551f2bc6b57400]]
= ロックされたNVMeドライブまたはFIPSドライブのロックを解除またはリセットします
: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ドライブまたはFIPSドライブをストレージアレイに挿入する場合、ドライブに関連付けられている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、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。

.作業を開始する前に
* ロックを解除する場合は、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）にセキュリティキーファイル（拡張子は「.slk」）があることを確認します。キーに関連付けられているパスフレーズも必要です。
* 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た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。

.このタスクについて
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。セキュリティキーがない状況では、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、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が、有効になりません。*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をリセット*]ダイアログボックスのフィールドにPSID文字列を入力し、「reset」と入力して確定します。[*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。リセットの場合は、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、あるい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

= ホットスペアを管理します

:leveloffset: +1

[[ID030b0c423750697cb3cc1bb39f4ce300]]
= 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で障害が発生すると、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ている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。ストレージアレイ内で障害が発生したどのドライブにも使用できますが、ホットスペアとドライブで次の属性が共有されている必要があります。

* 容量（またはホットスペアの方が大きい）

* メディアタイプ（HDD、SSDなど）が同じ
* インターフェイスタイプ（SASなど）

== ホットスペアの識別方法

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で、ピンクで示されたドライブベイを探します。

== ホットスペアの適用方法

ホットスペアの適用範囲は次のとおりです。

* 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ため、ホットスペアはプールには使用できません。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に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からホットスペアに自動的に切り替わります。物理的にドライブを交換する必要はありません。
*
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と、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不要です。
*
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によっては、トレイ損失の保護とドロワー損失の保護が失われる場合があります。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からホットスペアドライブに自動的に切り替わるため、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があるドライブを選択します。たとえば、8GiBの容量が設定されている18GiBドライブがある場合は、9GiB以上のドライブをホットスペアとして使用できます。通常は、ストレージアレイ内で最大のドライブの容量以上の容量がないドライブは、ホットスペアとして割り当てないでください。

[NOTE]
====
同じ物理容量のホットスペアがない場合は、ドライブの「使用済み容量」がホットスペアドライブの容量以下であれば、容量の少な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関係なく、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、セキュリティ機能のあるドライブのホットスペアとしては使用できません。

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。読み取りおよび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しか実行できません。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。ホットスペアドライブがない場合は、ストレージアレイのボリュームグループ間に手動でホットスペアドライブを作成できます。

[[IDde69ee20c0fbadf4bcd91eec88c1b717]]
= ホットスペアを割り当てます
: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、データ保護を強化するために、ホットスペアを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、障害が発生したドライブのデータがホットスペアに再構築されます。

.作業を開始する前に
* 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済み容量以上の容量。

.このタスクについて
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。推奨される適用範囲は、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のピンクの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。
+
ドライブがセキュリティ有効の場合、Secure Erase
Drive？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、最初にSecure
Erase処理を実行してすべてのデータを削除し、その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Secure
Erase操作の完了後は、データを回復できません。

====
+
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内のテキストを確認し、処理を確定します。
+
ドライブはハードウェアページにピンク色で表示され、ホットスペアになったことが示されます。

.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に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へデータを自動的に再構築します。

[[ID4d600c11fe57abf9308de7c51bfc8d52]]
= ホットスペアの割り当てを解除します
: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。

.作業を開始する前に
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。

.このタスクについて
障害が発生したドライブの役割を現在引き継いでいる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な状態でない場合は、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修正してください。

.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（ピンク色で表示）を選択します。
+
ピンク色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、割り当てを解除することはできません。

+
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による影響を受けるボリュームグループ、および他のホットスペアがそのボリュームグループ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です

:leveloffset: +1

[[IDee7c4fc8e30f849cfef8ece262203f60]]
= シェルフ損失の保護およびドロワー損失の保護とは何ですか？
: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、シェルフまたはドロワーで単一障害が発生した場合にデータアクセスを維持するためのプールとボリュームグループの属性です。

== シェルフ損失の保護

シェルフは、ドライブまたはドライブとコントローラを格納するエンクロージャです。シェルフ損失の保護が有効な場合、1台のドライブシェルフとの通信が完全に失われた場合でもプールまたはボリュームグループ内のボリューム上のデータへのアクセスが保証されます。通信が完全に失われるケースには、ドライブシェルフの電源喪失や、両方のI/Oモジュール（IOM）の障害などがあります。

[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。この状況で、ドライブシェルフへのアクセス、さらにその結果プールまたはボリュームグループ内の別のドライブへのアクセスを失うと、データが失われます。

====
シェルフ損失の保護の条件は、次の表で説明するように、保護の手法によって異なります。

[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|
プールには少なくとも5つのシェルフのドライブが含まれている必要があり、各シェルフで同じ数のドライブが必要です。シェルフ損失の保護は大容量シェルフには適用されません。大容量シェルフがあるシステムの場合は、ドロワー損失の保護を参照してください。
 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すべて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シェルフのみです。ドロワー損失の保護が有効な場合、1つのドロワーとの通信が完全に失われた場合でもプールまたはボリュームグループ内のボリューム上のデータへのアクセスが保証されます。通信が完全に失われるケースには、ドロワーの電源喪失や、ドロワー内のコンポーネント障害などがあります。

[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。この状況でドロワーにアクセスできなくなると（その結果プールまたはボリュームグループ内の別のドライブにアクセスできなくなると）、データが失われます。

====
ドロワー損失の保護の条件は、次の表で説明するように、保護の手法によって異なります。

[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を含める必要があり、各ドロワーに同じ数のドライブが必要です。

プールには少なくとも5つのドロワーのドライブが含まれている必要があり、各ドロワーに同じ数のドライブが必要です。

60ドライブのシェルフでは、プールに含まれる15、20、25、30、35でドロワー損失の保護を実現できます。 40、45、50、55、または60ドライブ。初回作成後に、
5の倍数でプールに追加できます。
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すべて別々のドロワーに配置されている。
a|
3.

```
 a|
RAID 1
 a|
ミラーペアのドライブがそれぞれ別のドロワーに配置されている。
 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

|===



[[ID2051c28361f9349ba99e9466649e8295]]
= 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、スマートバッテリゲージを調整する自動サイクルです。

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


バッテリは事前に設定したしきい値まで放電されます。このフェーズでは、バッテリゲージが調整されます。

学習サイクルを実行するには、次のパラメータが必要です。

* 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のバックアップ電源を備えたコントローラの場合は、学習サイクルがシーケンシャルに実行されます。

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設定されます。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

[[IDbcca065e16f8796c787c69d55d540c98]]
= 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、自身の接続パラメータ（速度とデュプレックスモード）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、管理ポートを設定する際には自動ネゴシエーションが推奨されますが、ネゴシエーションが失敗してネットワークインターフェイスの設定が一致しなくなった場合、ネットワークパフォーマンスが大幅に低下することがあります。この状況が許容されない場合は、ネットワークインターフェイスを手動で正しく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。

====

```
[[IDd9e1835a0645a3b87329b954798996b7]]
= 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、近接探索（ND）プロトコルなどの機能があります。IPv6では、アドレスのインターフェイスIDが基盤のデータリンクレイヤアドレスから生成されます。

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、その他の情報はステートフル自動設定を使用して取得します。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。IPv6は、ネットワーク上のすべてのIPアドレスを一度に再割り当てする方法も定義します。IPv6では、ネットワーク上のデバイスがIPアドレスやその他のパラメータをサーバなしで自動的に設定する方法を定義しています。

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スンします。このメッセージは、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必要があるか、自動設定が失敗して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、インターネット上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。具体的には、ルータから定期的に送信されるルータ通知メッセージをリスンするか、または次に必要な作業についてルータに問い合わせるルータ要求メッセージをルータに送信します。
. *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指示します。

. *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、ルータから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。

[[IDac9a75e58e81b22470ebf95b9528fcc8]]
= 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。

[[ID2499ed81aba290dcc12adbcac670d99b]]
= 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"]
動的ホスト構成プロトコル（DHCP）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も含まれます。

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を使用する場合は、クライアントがTCP / IP処理を開始する必要があるときにアドレス情報の要求を送信します。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て、アドレスをクライアントに送信します。DHCPを使用すると、ネットワークに接続するたびにデバイスのIPアドレスが変わる可能性があります。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アドレスが変わる場合があります。

```
[[ID14cd0d3015d61aeb96b49a066a8f29db]]
= 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、有効期限が切れるリース期間があるため変更
できます。サーバやルータなどの一部のデバイスは、静的アドレスを使用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サーバのドキュメントを参照してください。



[[ID175e0c0d4c72e22af52d5818c76f2e69]]
= 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（IPアドレス、サブ
ネットワークマスク、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。



[[IDa3f9f2210b91503ac2ba598478fe0cb9]]
= 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。

[[ID5a7bb31d3a12d903b6f86b18b349997a]]
= 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エコー要求」および「ICMPエコー応答」メッセージは、一般的に「ping」メッセージと呼ばれます。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するために使用するトラブルシューティング・ツールであり'ネットワーク遅延やパケット損失をテストするためにも使用されますpingコマンドは'ICMPエコー要求をネットワーク上のデバイスに送信し'デバイスはただちにICMPエコー応答で応答します企業のネットワークセキュリティポリシーでは、許可されていない人が検出しにくいように、すべてのデバイスで「ping」（「ICMPエコー応答」）を無効にする必要がある場合があります。

[[ID48f9d47d2e22c0069513ca46f2140e30]]
= 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いつですか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
DHCPサーバは、サーバを変更またはアップグレードしたとき、および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情報が変更されたときに更新します。

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、そのポート上のすべてのiSCSI接続が停止します。

```
====



[[IDa5a0d5a59e1a59813a9f9495f85f3052]]
= 管理ポートを設定したあとに何をすればよいですか？
: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、Unified
Managerでグローバルアレイビューを更新できます。

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「Ma
nage [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。



[[ID32cb8a63ee645c9842bd3aa257625311]]
= 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"]
最適モードでないストレージシステムは、システム設定が無効であることが原因です。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がInvalid System
Configurationに移行する理由には、次のいずれかが考えられます。

* コントローラが準拠していません。間違ったサブモデルID（
SMID）コードを持っているか、プレミアム機能の制限を超えている可能性があります。
* 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が実行中です。
```

* 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状態になりました。
* 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

[[ID4d2ee333edf5799c9993b95ed7df75e5]]
= 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。

[[ID15fb8d0ea103ed7d4fe025d8047e0b25]]
= 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コマンドを送信します。これに応答して、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。iSNSを使用する場合は、ホストイニシエータがiSNSサーバからターゲットIPを取得できるため、この検出方式は必要ありません。

[[ID998d9490ff862016df4709aae8ca93e4]]
= 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。統計はすべて読み取り専用で、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。

[[ID371332630d55343361b1d878897a73f6]]
= 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ポートを設定します
 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の統計を表示します
 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* iSER over InfiniBand settings *を表示し、* View iSER over InfiniBand Statistics *を選択します。

|===

[[IDd3016ce1768a7dc7f02a069633781d19]]

```
= iSCSI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-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確立できます。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を設定できるのは、ストレージアレイでiSCSIがサポートされている場合のみです。

====


== iSCSIを設定

[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ポートを設定
 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 *」（* 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を診断する

[cols="1a,1a"]
|===
| アクション | 場所


 a|
iSCSIセッションを表示または終了します
 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 *」（* 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統計を表示します
 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です

:leveloffset: +1

[[IDd41391ba446c6e01b76bbb77160329e2]]
= 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。統計はすべて読み取り専用で、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。

```
[[ID0511dce7963aa29c97feb550fdd64a18]]
= 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ポートを設定する
 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の統計を表示します
 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* NVMe over InfiniBand settings *を表示し、* View NVMe over Fabrics Statistics *を選択します。

|===

[[ID6f0f4d27f526b56c3d69d7f19c455377]]
= NVMe over RoCE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"]
NVMe over RoCEの設定と管理は、ハードウェアと設定のページで実行できます。

[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ポートを設定します
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の統計を表示します
 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* NVMe over RoCE settings *を表示し、* View NVMe over Fabrics Statistics *を選択します。

|===

[[ID7167eee00ab7d7a3916c00a541474887]]
= 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、外部HICと内部HICが2つ搭載されています。

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。

[[ID28542add2b9ba9e1614f70b8abdd52c2]]
= 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、外部HICと内部HICが2つ搭載されています。

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

[[ID5d817dfd08edcb32ce102ca8213ebc78]]
= 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で障害が発生すると、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。

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

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。容量が同じかそれよりも小さいストレージアレイ内で障害が発生したどのドライブにも、ホットスペアドライブを使用できます。ホットスペアドライブのメディアタイプ（HDDまたはSSD）は、保護対象のドライブと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。

====

```
[[IDd55af4479c6f9f1ebf3c5b6d38cc1101]]
= 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。予約済み容量を使用する方式は、再構築の時間を短縮できるため、ホットスペアドライブよりも優れています。予約済み容量は、ホットスペアドライブの場合は1本のドライブに確保されるのではなく、プール内の複数のドライブに分散されるため、特定のドライブの速度や可用性に制限されません。



[[ID4483bc5486d2f09d9a0af5d0cb6cd483]]
= 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、ドライブを物理的に交換します。

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。



[[ID775abb92f42907a591474dcb1c7bb278]]
= 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、処理実行中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

[[IDe212b993ef3e02196b086eeb2e2b0bb0]]
= 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、syslogメッセージで送信するように設定できます。

== アラートとは何ですか？

_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状態の変化、コントローラの冗長性の問題などがあります。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。

詳細はこちら。

* 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"]

== アラートを設定するにはどうすればよいですか？

アラートは、1つ以上のEメールアドレスにメッセージとして送信されるように設定することも、SNMPサーバへのSNMPトラップとして送信されるように設定することも、syslogサーバへのメッセージとして送信されるように設定することもできます。アラート設定はメニューから選択できます。Settings [Alerts]

詳細はこちら。

* 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を設定"]
* xref:{relative_path}configure-syslog-server-for-alerts.html["アラート用のsyslogサーバを設定します"]
* xref:{relative_path}configure-snmp-alerts.html["SNMPアラートを設定する"]

== 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["タイムスタンプが一致していません"]

= 概念

:leveloffset: +1

[[IDd70aea1a66d0ad5a4eef2ade13a36a38]]
= 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。アラートは E メール、 SNMP トラップ、 syslog を通じて送信できます。

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。
.
イベントが「アラート対象」であると判断した場合、イベントモニタは設定されているアラート方法（Eメール、SNMP、syslog）を使用して通知を送信します。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、アラートの設定が表示されます。次のいずれかになります。

* 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。
* イベントの短い概要 。

[NOTE]
====
syslogアラートは、RFC 5424のメッセージング標準に準拠しています。

====

[[IDa997b475381b89b31caf5979e5ac1c77]]
= 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 | 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。ストレージアレイで異常を検出すると、その問題に関する情報をイベントログに書き込みます。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。イベントが「アラート対象」であると判断した場合、イベントモニタは設定されているアラート方法（Eメール、SNMP、syslog）を使用して通知を送信します。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要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環境内のネットワークサーバのパスワードのような役割を果たす文字列です。

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てい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）は、パケットヘッダーで送信元と送信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

[[IDb9f7c6321be856ae1ef5b78d6e0a9459]]
= メールサーバとアラートの受信者を設定
: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。

.作業を開始する前に
* 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から設定できます。

====
* 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。通常、受信者には、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を指定します。Eメールアドレスは20個まで入力できます。

.このタスクについて
このタスクでは、メールサーバの設定方法、送信者と受信者のEメールアドレスの入力方法、および[Alerts]ページから入力したすべてのEメールアドレスのテスト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から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、［Eメール］タブに［メールサーバの設定］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から設定できます。

====
** *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。

[[ID6d372477cec2b8f0ad4f0e7aa95f24ee]]
= 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け取る受信者のEメールアドレスを変更することができます。

.作業を開始する前に
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。

[[ID3fad30486d5709859cb8b27999cd558b]]
= アラート用のEメールアドレスを追加する
: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名まで追加できます。

.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（ Add ）] 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。

[[ID1aec943c4757f100f33aa4da854b7f44]]
= アラート用のメールサーバまたはEメールアドレスを削除します
: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ができます。また、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。
. 表から、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アラートがそのアドレスに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。

[[ID5b10be59bbdced9db7f58494c7272c26]]
= アラート用のメールサーバを編集します
: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メールの送信元のアドレスを変更することができます。

.作業を開始する前に
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から設定できます。

====
.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から設定できます。

====
** *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


[[ID4eb8cf6642627a961a484eff326a1666]]
= SNMPアラートを設定する
: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。

.作業を開始する前に
* 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。イベントモニタからトラップメッセージを送信するためには、このサーバのネットワークアドレス（IPv4アドレスまたは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）。
* 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管理情報ベース（
MIB）ファイルをコピーしてコンパイルしておきます。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、ネットアップ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["ネットアップサポート"^]。
** [*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。
** 注意事項および使用許諾契約に同意します。
** 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。
```

.このタスクについて
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。
+
初めて設定するときは、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。
+
Select SNMP version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ユーザー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）の適切な手順に従います。
+
** *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、既知の一連の管理ステーションを識別する文字列で、通常はネットワーク管理者が作成します。印刷可能なASCII文字だけで構成されます。コミュニティは最大で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、認証プロトコルの設定時または変更時に必要となる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。（定義したのが1つだけの場合は、このフィールドには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たびに、イベントモニタからサーバにSNMPトラップが送信されます。

[[ID352b2979cc0c44dce234cdb66355b7d3]]
= SNMPアラートのトラップ送信先を追加します
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SNMPトラップの送信に使用するサーバは最大10台まで追加できます。

.作業を開始する前に
* 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。イベントモニタからトラップメッセージを送信するためには、このサーバのネットワークアドレス（IPv4アドレスまたは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）。
* 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管理情報ベース（MIB）ファイルをコピーしてコンパイルしておきます。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、ネットアップ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["ネットアップサポート"^]。
** [* 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。
** 注意事項および使用許諾契約に同意します。
** 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。（定義したのが1つだけの場合は、このフィールドには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たびに、イベントモニタからサーバにSNMPトラップが送信されます。

[[ID485250eb150886771d97777b8ffdb7b2]]
= SNMP MIB変数を設定します
: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。これらの変数で、ストレージアレイの名前、場所、および担当者を返すことができます。

.作業を開始する前に
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MIBファイルをコピーしてコンパイルしておく必要があります。

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["ネットアップサポート"^]。
* [* 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。
* 注意事項および使用許諾契約に同意します。
* 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。

.このタスクについて
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に対する応答で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sysName`の値。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sysLocation(システムロケーション
)の値。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
sysContact'の値。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。

[[ID100bae1ca7666450d28301e691a0ae5f]]
= SNMPv2cトラップのコミュニティを編集します
: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編集できます。

.作業を開始する前に
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
Alerts（アラート）ページのSNMP（SNMP）タブには、アップデートされたコミュニティ名が表示されます。

[[IDd752169e2dd3c8362d1e88345a9d9057]]
= SNMPv3トラップのユーザ設定を編集します
: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。

.作業を開始する前に
SNMPv3トラップ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、認証プロトコルの設定時または変更時に必要となる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
Alerts（アラート）ページのSNMP（SNMP）タブに、更新された設定が表示されます。

[[ID4bd0188094c83a57286a80d87209a282]]
= SNMPv2cトラップのコミュニティを追加します
: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。

[[ID8250e99edcbdc7bf937706cdd9c94b80]]
= SNMPv3トラップのユーザを追加します
: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。
+
[Configure SNMPv3 Users]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、認証プロトコルの設定時または変更時に必要となる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。

```
[[ID9f3eec2fa591429ad5259ebe9e42d6dc]]
= 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。



[[ID5db80c1edf2ec5a56098417470922721]]
= SNMPv3トラップのユーザを削除します
: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[Alerts]ページに表示されます。

. [ユーザーの設定]を選択します。
+
[Configure SNMPv3 Users]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
ユーザ名とそれに関連付けられているトラップ送信先が[Alerts]ページから削除されます。

[[ID9ffe35c8a101ba1eb46554820af7bf04]]
= トラップ送信先を削除します
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
トラップ送信先の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トラップが届かなくなります。

:leveloffset: -1

= syslogアラートの管理

:leveloffset: +1

[[ID7339b666552c762be262415111393778]]
= アラート用のsyslogサーバを設定します
: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台のsyslogサーバを指定できます。

.作業を開始する前に
*
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。

.このタスクについて
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、[Alerts]ページに[Add Syslog Servers]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たびに、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サーバを設定します"]。

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。

[[IDe240f6a517fc7c66235bac48a0673484]]
= アラート用のsyslogサーバを編集します
: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表に表示されます。

[[ID6ece71cc48cf9154a550ef6a69fb1ee0]]
= アラート用のsyslogサーバを追加します
: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。

.作業を開始する前に
*
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。

[[IDf9ceaa6c8ad9e8bce1f19e1a35d46d46]]
= アラート用のsyslogサーバを削除します
: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届かなくなります。

:leveloffset: -1

= よくある質問です

:leveloffset: +1

[[ID418c708409e7b237ea498b9faf1c6620]]
= 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する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メッセージを介して送信できます。また、初期セットアップウィザードからEメールアラートを設定することもできます。

[[IDed59d5ef25e19d5c6f0ff48992e89750]]
= SNMPまたはsyslogの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、アラートが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。

[[ID79b9b96b974182f6e917996df5832f1d]]
= アレイとアラートでタイムスタンプが異なるのはなぜですか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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を行いません。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。

ストレージアレイはアラートの送信時にタイムゾーンを修正しないため、アラートのタイムスタンプはGMTであり、タイムゾーンオフセットはゼロです。タイムスタンプをローカルのタイムゾーンに換算するには、GMTからのオフセットを特定し、タイムスタンプにその値を加算するか減算します。

```
:leveloffset: -1


:leveloffset: -1


= アレイ設定

:leveloffset: +1


[[IDa152d84568ecbfd808e6e0a56e2e00fe]]
= 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：

* 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を作成します"]
* xref:{relative_path}create-external-security-
key.html["外部セキュリティキーを作成します"]
* xref:{relative_path}../sm-hardware/configure-iscsi-ports-
hardware.html["iSCSIポートを設定"]
* xref:{relative_path}../sm-hardware/configure-nvme-over-infiniband-ports-
hardware.html["NVMe over IBポートを設定"]
* xref:{relative_path}../sm-hardware/configure-nvme-over-roce-ports-
hardware.html["NVMe over RoCEポートを設定します"]




= 概念

:leveloffset: +1


[[IDe50ab3e67b177b6b4b7b4f1985748b28]]
= 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速くアクセスできる、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が以前の処理からすでにキャッシュに格納されている可
能性があるため、ドライブへのアクセスが不要になります。
*
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、System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、4、8、16、32KiBに設定できます。アプリケーションの一般的なI/Oサイズにキャッシュブロックサイズを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では一般に小さいサイズを使用し、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は大きいサイズが適しています

== 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ングにより、以降のデータ要求にキャッシュから対応できる可能性が高まります。動的キャッシュ読み取りプリフェッチは、シーケンシャルI/Oを使用するマルチメディアアプリケーションで重要ですデータがキャッシュにプリフェッチされる速度と量は、ホスト読み取りの速度と要求サイズに基づいて自動で調整されます。ランダムアクセスの場合、原因
データがキャッシュにプリフェッチされることはありません。この機能は、読み取りキャッシュが無効になっている場合は適用されません。

* *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書き込みキャッシュ内のデータは、ドライブに書き込まれるまで保持されます。書き込みキャッシュにより、I/Oパフォーマンスを向上させることができます。
+
[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。

[[ID7ef23d32fdf47552efa428bdf1288f41]]
= 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。ワークロードがコントローラ間で自動的に再分散されるため、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必要がなくなり、ストレージ管理者の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利用率を自動的に監視して負荷を分散します。
*

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、ストレージアレイの状況に応じて無効にすることができます。たとえば、次のような場合です。

*
特定のボリュームのコントローラ所有権については、ワークロードを分散するために自動的に変更されないようにする場合。
*
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を有効にするのはストレージアレイレベルですが、ホストまたはホストクラスタに選択したホストタイプがこの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際、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でき、自動ロードバランシング機能をサポートする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によってホストがボリュームにアクセスできなくなることはありませんが、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、ストレージアレイは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がワークロードを分散するためには、マルチパスドライバがTPGSをサポートしていることと、ホストタイプが次の表に含まれていることが必要です。

[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のは、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場合です。

====
[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をサポートしていないホストタイプは、この機能が有効になっているかどうかに関係なく正常に動作し続けます。例外の1つがシステムのフェイルオーバーです。データパスが復旧すると、ストレージアレイは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を所有権を持つコントローラに戻しますが、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。

====
を参照してください https://mysupport.netapp.com/matrix["Interoperability Matrix Tool で確認してください"^] サポートされるマルチパスドライバ、
OSレベル、コントローラドライブトレイの互換性情報については、を参照してください。



== 自動ロードバランシング機能とOSの互換性の確認

新しいシステムを設定（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の互換性を確認します。

. にアクセスします https://mysupport.netapp.com/matrix["Interoperability Matrix Tool で確認してください"^] をクリックして解決策
を検索し、サポートを確認してください。
+
```

Red Hat Enterprise Linux 6またはSUSE Linux Enterprise Server 11を実行しているシステムの場合は、テクニカルサポートにお問い合わせください。

. /etc/multipath.confファイルを更新して構成します
. 該当するベンダーおよび製品の「retain_attached_device_handler」と「detect_prio」の両方が「yes」に設定されていることを確認するか、デフォルトの設定を使用します。

:leveloffset: -1

= アレイを設定します

:leveloffset: +1

[[ID81125d3e642e497eab2398f392412334]]
= ストレージアレイ名を編集します
: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。

[[IDe39b6e21e3e445640fcff25c7862fb56]]
= ストレージアレイのロケーターライトを点灯します
: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特定するために、ストレージアレイのロケーター（LED）ライトを点灯できます。

.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てダイアログボックスが閉じます。

[[IDcabeec139301b5f99031f94840cd0b7a]]
= ストレージアレイのクロックを同期する
: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）が無効な場合は、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。

.このタスクについて
同期によって、イベントログ内のイベントのタイムスタンプがホストログファイルに書き込まれるタイムスタンプと一致します。同期プロセスの実行中も、コントローラを引き続き使用できます。

[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ではシンプルネットワークタイムプロトコル（SNTP）を使用してクロックを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精度が低下したりする可能性があります。また、スケジュールに影響が生じたり（ASUP、Snapshotなど）、ログデータ内のタイムスタンプが不正確になる可能性もあります。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。このダイアログには、コントローラおよび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、表示されるコントローラは1台だけです。

====
. 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。

[[ID8fbedccbb3d2512b0e0b633185d83de6]]
= ストレージアレイの構成を保存します
: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。

.作業を開始する前に
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。

.このタスクについて
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。

* バッテリの寿命です
* コントローラの時刻
* 不揮発性静的ランダムアクセスメモリ（NVSRAM）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、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。「ボリューム構成」と「ホスト構成」も保存しないと、「ホストとボリュームの割り当て」を保存できません。

====
. [保存（ Save ）] をクリックします。
+
ファイルは'storagearray-configuration.cfgという名前でブラウザのDownloadsフォルダに保存されます

.完了後
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'-fオプションを指定したSANtricity コマンド・ライン・インターフェイス（SMcli）を使用して'.cfgファイルを適用します

[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]）。

====

```
[[ID43f6e942ad5606d4ddf62340c06bd6ea]]
= ストレージアレイの構成のクリア
: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、ホストの定義、およびホストの割り当てを削除する場合は、設定のクリア処理を使用します。

.作業を開始する前に
ストレージアレイ構成をクリアする前に、データのバックアップを作成します。

.このタスクについて
ストレージアレイ構成のクリアオプションは2つあります。

* *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、本番環境用にストレージアレイをセットアップする場合があります。
* *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が新しいストレージアレイを導入することになり、現在使用しているストレージアレイを管理部門に移動する場合などです。
+
ストレージアレイオプションを選択すると、追加の設定がいくつか削除されます。



[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します
a|
X
a|
X

a|
ボリュームを削除します
a|
X
a|
X

a|
ホストとホストクラスタを削除します
a|
X
a|
X

a|
ホスト割り当てを削除します
a|
X
a|
X

a|
ストレージアレイ名を削除します
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します

```
 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破棄されます。
* すべてのドライブの割り当てが解除されます。




[[ID0c85277670b5842223611f2d7222c3f7]]
= ストレージアレイのキャッシュ設定を変更します
: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では、フラッシュおよびブロックサイズについてキャッシュメモリの設定を調整できます。

.このタスクについて
キャッシュメモリは、ドライブメディアよりも速くアクセスできる、コントローラ上の一時的な揮発性ストレージ領域です。キャッシュの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 | 説明

a|
デマンドキャッシュフラッシュを開始します
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、80%より小さいパーセントの開始パーセント値を指定すると、原因 の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。システムでは、4、8、16、または32KiBのキャッシュブロックサイズを選択できます。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小さいサイズが適しています。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可能性があります。
** **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。

```
[[ID5a0a38153828125e37f567f13c7c06c8]]
= 自動ロードバランシングを設定する
: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。

.このタスクについて
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利用率を自動的に監視して負荷を分散します。
*
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、ストレージアレイの状況に応じて無効にすることができます。たとえば、次のような場合です。

*
特定のボリュームのコントローラ所有権については、ワークロードを分散するために自動的に変更されないようにする場合。
*
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。

====

[[ID08a573c103825061836ee4f2dba520d2]]
= 従来の管理インターフェイスを有効または無効にします
: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。

.このタスクについて
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安全な通信方法（REST API over https）を使用しますが、無効にした場合、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

= アドオン機能を設定

:leveloffset: +1

[[IDfea9c36a4419ef38387d0958c6216440]]
= 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、有効にするにはキーが必要な場合があります。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。

以下に、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。これらはSystem Managerにあります。
** Feature Activation Code。機能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、有効化ID、および機能コードを指定します。
. 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。

[[ID9f03b5f763388151d567431cd75ccbb6]]

```
= 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 | 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。プレミアム機能を取得した場合、この識別子によって機能が特定のストレージアレイにのみ関連付けられます。この文字列は、[システム]ページの[アドオン]の下に表示されます。



 a|
機能キーファイル
 a|
機能キーファイルは、プレミアム機能や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。

|===
```

[[ID5b5b5fc1e1245e155103943a9f227128]]
= 機能キーファイルを取得します
: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。

.このタスクについて
このタスクでは、機能の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
* Feature Activation Code （機能アクティベーションコード）

.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、サポートセンターのタイルにマウスを合わせると表示されます。
. 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。
.
機能を有効にするコードを探して記録します。機能パックの場合、このコードは変換を実行するための適切な手順で提供されます。
+
ネットアップの手順説明にはからアクセスできます 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"^]。

+
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。

+
.. にログインします https://mysupport.netapp.com/site/global/dashboard["ネットアップサポート"^]。

.. 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。

. シャーシのシリアル番号、有効化ID、機能のアクティブ化のコードなどの情報を記載した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、機能キーファイルを要求します。
+
に進むこともできます
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"^]
機能または機能パックを入手するために必要な情報を入力します。（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）。

.完了後
機能キーファイルを取得したら、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。

[[IDbb114f6faa2782e9e90b55bda356e417]]
= プレミアム機能を有効にします
: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。

.作業を開始する前に
*
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。

.このタスクについて
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 Storage Array Featureコマンドを使用する必要があります（`disable storageArray) (featurePack | feature=featureAttributeList`）をCommand Line Interface（CLI；コマンドラインインターフェイス）でクリックします。

====
.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。
+
プレミアム機能を有効にする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。

[[IDbce48e944b3c5661384296d99d1f1164]]
= 機能パックを有効にします
: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。

.作業を開始する前に
*
新しいストレージアレイ属性の変換と準備について説明した適切な手順を実行しておきます。ホストプロトコルの変更手順については、使用している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り、ホストやアプリケーションからのアクセスがないことを確認します。
* 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]
====
システムを停止するメンテナンス時間をスケジュールして、ホストとコントローラの間のすべてのI/O処理を停止する必要があります。また、変更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。

====
.このタスクについて
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「CHANGE」と入力します。
. [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。I/Oアクティビティをなくすために、書き込み前のキャッシュデータが削除されます。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

[[ID4281f45fe69e442198adf39e48c0c4df]]
= 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。このCLIは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の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。

.作業を開始する前に
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。

= よくある質問です

:leveloffset: +1

[[ID370536ab9395ab4aee861a1c5ad24d4d]]
= 自動ロードバランシングとは何ですか？
: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はI/Oを自動的に分散する機能を提供し、ホストからの受信I/Oトラフィッ

クは動的に管理されて両方のコントローラに分散されます。

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。ワークロードがコントローラ間で自動的に再分散されるため、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必要がなくなり、ストレージ管理者の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利用率を自動的に監視して負荷を分散します。
*
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による転送の対象外となります。

====

[[ID1baba50d2c1b612847a2918d60637a29]]
= 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の間、およびコントローラとディスクの間の2種類のI/O（入出力）処理をスムーズに行うための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になります。

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通知します。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たずに代わりに、アプリケーションは処理を続行できます。また、サーバアプリケーションはキャッシュされたデータ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

読み取る必要がなくなります。

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次のように影響します。

*
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
/書き込み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、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。

====

[[IDecd6c977551c444a543d02ad3568b03a]]
= 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。デマンドベースのアルゴリズムは、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使用されます。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減ってキャッシュに残るデータ量が増えるため、キャッシュヒットの可能性が高まります。

I/Oが不規則な（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設定して、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します。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。また、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への書き込み回数が増えるため、システムオーバーヘッドが増大します。

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は、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、カウントされるのは非アクティブな期間のみです。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。

====

[[IDcff832a3b0ab9299787727bef2592b59]]
= 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8KiB、16KiB、または32KiBのメモリチャンクです。ストレージシステムのボリュームはすべて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小さいサイズが適しています。大容量のデータ転送、シーケンシャルI/O、マルチメディアなどの広帯域幅を必要と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。

[[ID4d325a7eb02f2cdaa96182ed9e65d4c2]]
= 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いつですか？
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
System Managerと管理クライアント（ブラウザ経由でSystem Managerにアクセスするコンピュータ）で表示されるタイムスタンプが異なる場合は、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。このタスクが必要になるのは、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、ストレージアレイクロックの同期化ダイアログボックスで確認できます。このダイアログボックスはシステムページから使用できます。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、同期を実行します。このダイアログボックスを定期的に表示することで、コントローラクロックの時間表示が同期されている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

[[ID3bc4c6183fcb179bfd30100175d53112]]

= 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"]
ドライブセキュリティとキー管理は、セキュリティキー管理のページで設定できます。

== ドライブセキュリティとは何ですか？

_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、それらのドライブは別のアレイに取り付けるまで動作しなくなり、取り付けた時点で正しいセキュリティキーが提供されるまで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。

詳細はこちら。

* 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"]

== キー管理を設定するにはどうすればよいですか？

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ドライブが搭載されている必要があります。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、プールと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。

詳細はこちら。

```
* xref:{relative_path}create-internal-security-
key.html["内部セキュリティキーを作成します"]
* xref:{relative_path}create-external-security-
key.html["外部セキュリティキーを作成します"]
* xref:{relative_path}../sm-storage/create-pool-
manually.html["プールを手動で作成する"]
* xref:{relative_path}../sm-storage/create-volume-
group.html["ボリュームグループを作成します"]



== ドライブのロックを解除する方法

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は、セキュリティキーを新しいストレージアレイに再度割り当てて、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必要があります。

詳細はこちら。

* xref:{relative_path}unlock-drives-using-an-internal-security-
key.html["内部キー管理を使用する場合は、ドライブのロックを解除します"]
* xref:{relative_path}unlock-drives-using-an-external-security-
key.html["外部キー管理を使用する場合は、ドライブのロックを解除します"]



== 関連情報

キー管理に関連するタスクの詳細：

* 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["セキュリティキーをバックアップする"]



= 概念

:leveloffset: +1


[[IDa5696b7270b6b6ef2b438df3bf19a9f8]]
```

= 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。

これらのドライブにドライブセキュリティ機能を使用すると、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は動作しなくなり、取り付けた時点で正しいセキュリティキーが提供されるまでは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を実装する方法

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ドライブのみを含むボリュームグループまたはプールでは、FDEドライブを追加したりスペアとして使用したりすることはできません）。
. セキュリティキーを作成します。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することができます。外部キー管理の場合、キー管理サーバとの間に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。ドライブごとに固有の暗号化キーがあり、このキーを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。ドライブセキュリティでこれらのドライブ上のボリュームグループまたはプールを選択すると、ドライブはセキュリティキーを確認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することができ、ドライブ上の既存データへの影響はありません。ただし、ドライブセキュリティを無効にするときは、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、コントローラによってセキュリティキーが適用され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を探します。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。再配置したドライブのロック解除が成功すると、以降は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ドライブのみを含むボリュームグループまたはプールでは、FDEドライブを追加したりスペアとして使用したりすることはできません）。
* 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。

[[IDc4222155fd7b62b13ce7dda4872b82ba]]
= 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、データアクセスのために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および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、コントローラによってセキュリティキーが適用され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再度取り付けると、データに再びアクセスできるようにな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上での内部キー管理。
* 外部キー管理サーバでの外部キー管理

== 内部キー管理

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問い合わせてください。
.

識別子とパスフレーズを定義して、内部セキュリティキーを作成します。識別子は、セキュリティキーに関連付けられる文字列で、コントローラとキーに関連付けられたすべてのドライブに格納されます。パスフレーズは、バックアップ用にセキュリティキーを暗号化するために使用されます。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、コントローラ上のアクセスできない非表示の場所に格納されます。これで、セキュリティ有効のボリュームグループまたはプールを作成したり、既存のボリュームグループまたはプールでセキュリティを有効にしたりできます。

== 外部キー管理

外部キーは、Key Management Interoperability Protocol（KMIP）を使用して別のキー管理サーバに保持されます。外部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問い合わせてください。
.
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KMIP要求を信頼できるよう、ストレージアレイのコントローラを検証します。
+
.. 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、キー管理サーバで信頼されているCAから署名済みのクライアント証明書を要求します。（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を作成したら、System Managerにアクセスしているホストにそのファイルをコピーします。
.. また、秘密鍵と公開鍵のペアを使用して、外部で証明書署名要求を生成することもできます。

. キー管理サーバから証明書ファイルを取得し、System Managerにアクセスしているホストにそのファイルをコピーします。キー管理サーバ証明書は、ストレージアレイがサーバのIPアドレスを信頼できるよう、キー管理サーバを検証します。キー管理サーバには、ルート証明書、中間証明書、またはサーバ証明書を使用できます。
. キー管理サーバのIPアドレスとKMIP通信に使用するポート番号を定義して、外部キーを作成します。このプロセスでは、証明書ファイルもロードします。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。これで、セキュリティ有効のボリュームグループまたはプールを作成したり、既存のボリュームグループまたはプールでセキュリティを有効にしたりできます。

[[ID1054d69afe551b836dbba668a135556a]]
= 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 | 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。これらのドライブにドライブセキュリティ機能を使用すると、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は動作しなくなり、取り付けた時点で正しいセキュリティキーが提供されるまではセキュリティロック状態になります。

a|
FDEドライブ
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。ハードドライブに搭載されたASICチップにより、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。

a|
FIPSドライブ
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されます。ドライブの移行やヘッドの交換でバックアップされているセキュリティキーをインポートしたときは、セキュリティキーの暗号化に使用したものと同じ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無関係です。

====

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。読み取りおよび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しか実行できません。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、コントローラによってセキュリティキーが適用され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再度取り付けると、データに再びアクセスできるようにな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管します
* 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、セキュリティ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。この識別子は、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

= セキュリティキーを設定する

:leveloffset: +1

[[ID6b7e0df3cb2f0a3819d27c43607c92ff]]

= 内部セキュリティキーを作成します
: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ために、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できます。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。

.作業を開始する前に
*
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を有効にする必要があります。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問い合わせてください。

[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、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。

====
.このタスクについて
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無関係です。

====
.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
8~32文字で指定し、以下の文字をそれぞれ1文字以上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）。
*** 英数字以外の、！、*、@などの文字（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、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になります。

====
. [作成（ Create ）] をクリックします。
+
セキュリティキーは、コントローラ上のアクセスできない場所に格納されます。実際のキーとともに、ブラウザからダウンロードされた暗号化されたキーファイルも格納されます。

+
[NOTE]
====
ダウンロードファイルのパスは、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

ループまたは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オンにするたびに、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なります。この状態のドライブのデータには、ドライブの初期化時にコントローラによって正しいセキュリティキーが適用され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。

====
.完了後
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します。

[[ID00f1ce079fb75fffcc9790325882aee6]]
= 外部セキュリティキーを作成します
: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する外部キーを作成する必要があります。

.作業を開始する前に
*
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、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を有効にする必要があります。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問い合わせてください。
*
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必要です。このファイルを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、キー管理サーバが

自身のKey Management Interoperability Protocol（
KMIP）要求を信頼できるよう、ストレージアレイのコントローラを検証します。
* 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、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。

====

.このタスクについて
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]
====
内部キー管理が現在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の確認を求めるダイアログボックスが表示されます。

====
+
[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、エラーが発生し、バックアップサーバを使用できなくなります。

+

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アクセスできない場合、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。維持しないとエラーが発生することがあります。

** *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。
** *秘密鍵ファイルの選択*-必要に応じて、2番目の*[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用の秘密鍵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*-- 3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。8~32文字で指定し、以下の文字をそれぞれ1文字以上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）。
*** 英数字以外の、！、*、@などの文字（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、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になります。

====
+
** 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てバックアップキーがない場合は、ドライブが別のストレージアレイに移行されると、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。
+
次のメッセージと外部キー管理へのリンクが表示されます。

+
現在のキー管理方法:外部

. 「* 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または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オンにするたびに、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なります。この状態のドライブのデータには、ドライブの初期化時にコントローラによって正しいセキュリティキーが適用され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。

====
.完了後
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します。



:leveloffset: -1
```

```
= セキュリティキーを管理します

:leveloffset: +1


[[ID2b3f54aaf64fd5900cab7a150d06d3b2]]
= セキュリティキーを変更する
: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、ドライブデータへの不正アクセスを防ぎたい場合は、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*--(内部セキュリティキーの場合のみ)
デフォルト値（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8~32文字で指定し、以下の文字をそれぞれ1文字以上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）。
```

*** 英数字以外の、！、*、@などの文字（1文字以上）。

.
外部セキュリティキーの場合に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オンにします。
+
[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。
+
前のキーが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。

.完了後
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します。

[[ID7bedb66114053e54204bc25655ab114c]]
= 外部キー管理から内部キー管理に切り替えます
: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の方法に変更することができます。以前に外部キー管理用に定義されたセキュリティキーが内部キー管理に使用されます。

.このタスクについて
このタスクでは、外部キー管理を無効にして、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。8~32文字で指定し、以下の文字をそれぞれ1文字以上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）。
** 英数字以外の、！、*、@などの文字（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、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になります。

====
. [*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。

.完了後
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します。

[[ID7c96c035f99474ebf7d27de4aeb49676]]
= キー管理サーバの設定を編集します
: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、キー管理サーバの設定をいつでも表示および編集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]。
. 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。

[[IDa6b794e3c06fcc7e8f84024a9c35c428]]
= セキュリティキーをバックアップする
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
セキュリティキーの作成後または変更後に、元のキー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することができます。

.このタスクについて
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同じであ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。
+
8~32文字で指定し、以下の文字をそれぞれ1文字以上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）
** 数字（1文字以上）
** アルファベット以外の文字（！、*、@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。

.完了後

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。

[[ID1aff912e744b9671a26e4c702cbc4089]]
= セキュリティキーを検証する
: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。

.このタスクについて
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場合に、あとからドライブデータにアクセスできます。

.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。

. [*Browse*](参照)をクリックし'キーファイル(たとえば'drives]
ecsecurity.slk`)を選択します
. 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手順に従います。

[[ID64840ef11ea06d4ab63acb746267390f]]

= 内部キー管理を使用する場合は、ドライブのロックを解除します
: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で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、新しいストレージアレイにセキュリティキーを再割り当てする必要があります。

.作業を開始する前に
*
ソースアレイ（ドライブを削除するアレイ）でボリュームグループをエクスポートし、ドライブを削除しておきます。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手順の詳細については、を参照してください https://kb.netapp.com/["ネットアップナレッジベース"^]。System Managerで管理されている新しいアレイや従来型システムの場合は、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を有効にする必要があります。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問い合わせてください。
*
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把握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。

.このタスクについて
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上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ると、正しいセキュリティキーを指定しないかぎり動作しません。

[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することができます。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。external_key管理を使用した場合は、を参照してください xref:{relative_path}unlock-drives-using-an-external-security-
key.html["外部キー管理を使用する場合は、ドライブのロックを解除します"]。コントローラのアップグレードを実行していて、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、Eシリーズおよび SANtricity
ドキュメントセンターのに記載されている手順を実行する必要があります
link:https://docs.netapp.com/us-en/e-series/upgrade-controllers/upgrade-unlock-drives-task.html["ドライブのロックを解除する"]。

====
セキュリティ有効ドライブを別のアレイに再インストールすると、そのアレイでドライブが検出され、「Needs Attention」状態と「Security Key Needed」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別の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、取り付けるドライブのデータのロック解除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成功すると、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テーブルに表示されます。

.
*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、「The associated secure drives have been unlocked」というメッセージを示すダイアログボックスが表示されます。

.結果
すべてのドライブがロックされたあとでロック解除されると、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の一部のドライブがすでにロック解除されている場合、コントローラはリブートされません。

.完了後
デスティネーションアレイ（新しく設置したドライブがあるアレイ）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手順の詳細については、を参照してください
https://kb.netapp.com/["ネットアップナレッジベース"^]。

[[IDc7142bb717ffbbdd0e918ed4d02e9e7b]]
= 外部キー管理を使用する場合は、ドライブのロックを解除します
: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データにアクセスできるようにするには、新しいストレージアレイにセキュリティキーを再割り当てする必要があります。

.作業を開始する前に
*
ソースアレイ（ドライブを削除するアレイ）でボリュームグループをエクスポートし、ドライブを削除しておきます。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手順の詳細については、を参照してください
https://kb.netapp.com/["ネットアップナレッジベース"^]。System
Managerで管理されている新しいアレイや従来型システムの場合は、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を有効にする必要があります。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問い合わせてください。
* 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必要です。このファイルを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、キー管理サーバが自身のKey Management Interoperability Protocol（
KMIP）要求を信頼できるよう、ストレージアレイのコントローラを検証します。
* 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、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。

====
.このタスクについて
外部キー管理を使用する場合、セキュリティキーは、安全なセキュリティキー用に設計されたサーバの外部に格納されます。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ると、正しいセキュリティキーを指定しないかぎり動作しません。

[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することができます。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。internal_key管理を使用した場合は、を参照してください
xref:{relative_path}unlock-drives-using-an-internal-security-key.html["内部キー管理を使用する場合は、ドライブのロックを解除します"]。コントローラのアップグレードを実行していて、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、Eシリーズおよび SANtricity
ドキュメントセンターのに記載されている手順を実行する必要があります
link:https://docs.netapp.com/us-en/e-series/upgrade-controllers/upgrade-

unlock-drives-task.html["ドライブのロックを解除する"]。

====
セキュリティ有効ドライブを別のアレイに再インストールすると、そのアレイでドライブが検出され、「Needs Attention」状態と「Security Key Needed」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）。
このプロセスでは、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、セキュアキーにアクセスできるようになります。ストレージアレイがセキュリティキーに接続して取得するためには、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別の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、取り付けるドライブのデータのロック解除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成功すると、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指定して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テーブルに表示されます。

.
*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、「The associated secure drives have been unlocked」というメッセージを示すダイアログボックスが表示されます。

.結果

すべてのドライブがロックされたあとでロック解除されると、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の一部のドライブがすでにロック解除されている場合、コントローラはリブートされません。

.完了後
デスティネーションアレイ（新しく設置したドライブがあるアレイ）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手順の詳細については、を参照してください
https://kb.netapp.com/["ネットアップナレッジベース"^]。

:leveloffset: -1

= よくある質問です

:leveloffset: +1

[[ID18841f7f9fb188367020a8084c3ecd48]]
= 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によって共有されます。セキュリティ有効ドライブをストレージアレイから取り外すと、セキュリティキーによってデータが不正アクセスから保護されます。

セキュリティキーは次のいずれかの方法で作成および管理できます。

* コントローラの永続的メモリ上での内部キー管理。
* 外部キー管理サーバでの外部キー管理

== 内部キー管理

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、次の作業を行う必要があります。

. 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問い合わせてください。

識別子とパスフレーズを定義して、内部セキュリティキーを作成します。識別子は、セキュリティキーに関連付けられる文字列で、コントローラとキーに関連付けられたすべてのドライブに格納されます。パスフレーズは、バックアップ用にセキュリティキーを暗号化するために使用されます。作成したセキュリティキーは、コントローラ上のアクセスできない場所に格納されます。これで、セキュリティ有効のボリュームグループまたはプールを作成したり、既存のボリュームグループまたはプールでセキュリティを有効にしたりできます。

== 外部キー管理

外部キーは、Key Management Interoperability Protocol（KMIP）を使用して別のキー管理サーバに保持されます。外部セキュリティキーを作成する前に、次の作業を行う必要があります。

. 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問い合わせてください。
.
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KMIP要求を信頼できるよう、ストレージアレイのコントローラを検証します。
+
.. 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、キー管理サーバで信頼されているCAから署名済みのクライアント証明書を要求します。（ダウンロードしたCSRファイルを使用して、キー管理サーバからクライアント証明書を作成およびダウンロードすることもできます）。
.. クライアント証明書ファイルを作成したら、System Managerにアクセスしているホストにそのファイルをコピーします。

. キー管理サーバから証明書ファイルを取得し、System Managerにアクセスしているホストにそのファイルをコピーします。キー管理サーバ証明書は、ストレージアレイがサーバのIPアドレスを信頼できるよう、キー管理サーバを検証します。キー管理サーバには、ルート証明書、中間証明書、またはサーバ証明書を使用できます。

キー管理サーバのIPアドレスとKMIP通信に使用するポート番号を定義して、外部キーを作成します。このプロセスでは、証明書ファイルもロードします。作成が完了すると、入力したクレデンシャルを使用してキー管理サーバに接続されます。これで、セキュリティ有効のボリュームグループまたはプールを作成したり、既存のボリュームグループまたはプールでセキュリティを有効にしたりできます。

[[ID1cb9d0f2151a02ba7e0a5222e76a3aa3]]
= 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、ローカルの管理クライアントに格納されているセキュリティキーファイルの暗号化と復号化に使用されます。パスフレーズがないとセキュリティキーを復号化できず、セキュリティ有効ドライブが別のストレージアレイに再設置された場合、データのロック解除にセキュリティキーを使用できません。

[[IDeb836f318c6cd6b59c009e6b523e10ab]]
= 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が失われて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たローカルホスト上の場所を書き留めておいてください。

```
[[ID3b24eed8203f369ece21a40838c5532c]]
= 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"]
バックアップを作成していない状態で元のセキュリティキーが破損すると、ドライブ上のデータがストレージアレイ間で移行される場合に、そ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際は、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、識別子の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同じであ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の格納場所を記録しておいてください。




[[IDa3b47d8ec2e9c8ecaa2b7fe3f5de87c7]]
= 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セキュリティキーがすでに設定されている必要があります。移行されたドライブのキーはターゲットストレージアレイのキーに変更されます。
*
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）上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。

```
[[ID5e1f638dcf54cd8cac34d5fee418e533]]
= 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"]
```
Drive Settings（ドライブ設定）ウィンドウには、Drive Security（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場合に表示される属性の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）。

```
[[ID8a3eb3e1ef207443173ce61b9233019f]]
= 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"]
セキュリティキーの作成後、キーファイルを検証して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。

検証が失敗した場合は、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。パスフレーズを再度確認し、必要に応じて再入力してから検証をやり直してください。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を選択し（使用可能な場合）、検証をやり直してください。
*
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。




[[ID833001d90212b11251670c444f78fd21]]
= 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することができます。

セキュリティキーは、ストレージアレイのセキュリティ有効ドライブとコントローラで共有される文字列です。内部キーは、コントローラの永続的メモリに保持されます。外部キーは、Key Management Interoperability Protocol（
KMIP）を使用して別のキー管理サーバに保持されます。
```

```
:leveloffset: -1


:leveloffset: -1


= アクセス管理

:leveloffset: +1


[[IDd162a2bfdccb5c0801889164717c3e22]]
= 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。


詳細はこちら。

* 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、RBAC機能を実装した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。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。

詳細はこちら。

* xref:{relative_path}add-directory-
server.html["LDAPディレクトリサーバを追加します"]
* xref:{relative_path}configure-saml.html["SAMLを設定する"]




== 関連情報

アクセス管理に関連するタスクの詳細：

* xref:{relative_path}change-passwords.html["パスワードを変更します"]
* xref:{relative_path}view-audit-log-
activity.html["監査ログアクティビティを表示します"]
* xref:{relative_path}configure-syslog-server-for-audit-
logs.html["監査ログ用のsyslogサーバを設定します"]




= 概念

:leveloffset: +1


[[ID5423d398864549b5546618faf84adb01]]
= 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行います。

. 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]
====
初めてのログインでは'ユーザ名adminが自動的に表示され'変更することはできませんadminユーザは'システムのすべての機能にフル・アクセスできます

====
.
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に必要な設定はありません。
** *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(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。

====
```

+
ログイン時には、次のバックグラウンドタスクが実行されます。

+
** ユーザ名とパスワードをユーザアカウントと照合して認証します。
** 割り当てられたロールに基づいてユーザの権限が決まります。
** 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なります。
** 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および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は、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を変更しています
* コントローラファームウェアをアップグレード中です
* ストレージアレイ構成をロードしています
* スクリプトを実行する
* 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

[[ID8233e418f4344ad83e04e99ccf2682e2]]
= 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 | 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）に関連付けられており、一連の権限と有効期限が含まれています。

a|
Active Directory
a|
Active Directory（AD）は、Windowsドメインネットワーク用のLDAPを使用するMicrosoftのディレクトリサービスです。

a|
結合
a|

バインド処理は、ディレクトリサーバに対するクライアントの認証に使用されます。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|
できます
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文書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、その情報について証明（署名）する信頼されたエンティティのIDが含まれます。

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。多要素認証にも対応し、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、分散型のディレクトリ情報サービスへのアクセスと管理に使用される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が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、コンピュータやネットワークリソースへのアクセスを個々のユーザのロールに基づいて制御する手法です。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用意されています。

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は、ユーザの認証時に複数の項目（パスワードとフィンガープリントなど）を求める多要素認証に対応しています。ストレージアレイに組み込みのSAML機能は、SAML2.0のアイデンティティアサーション、認証、および許可に準拠しています。

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を設定すると、ストレージアレイが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。

|===

[[IDfec055573805873b9018432b48cb0f56]]
= 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組み込みの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済みの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。

これらのロールにより、次のタスクへのアクセスが可能になります。

* * 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。

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。

[[IDcb796fcf5ad49a002f1274ce7674471a]]
= 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。これらの機能のことを「ローカルユーザロール」と呼びます。

== 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場合、管理者は次の操作を行うことができます。

. 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ユーザは'システムのすべての機能にフル・アクセスできます

====
.
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、変更することはできません。
. 必要に応じて、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。
* パスワードなしでのログインをユーザに許可します。

[[ID506212404e533c18f7d9961bda63ee3b]]
= 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、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、設定は次のようになります。

. 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ユーザは'システムのすべての機能にフル・アクセスできます

====
. LDAPサーバの設定を入力します。これには、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、
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たら、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に定義されており、変更できません。
. 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。
. ユーザは各自に割り当てられた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する。
* ディレクトリサーバを削除する。

[[ID1f8e05cabdb4efaa97da188916a2043f]]
= 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行います。

. 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ユーザはSystem Managerのすべての機能にフル・アクセスできます

====
. 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間の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。その後、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、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します
* サービスプロバイダファイルをエクスポート

== アクセス制限

SAMLが有効な場合、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てログインします

[[ID7ba6fc7fa5a872f68b9ed62849431503]]
= アクセストークン
: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、ユーザ名や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）を使用して認証する手段を提供します。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と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従来のコマンドラインツールにアクセスすることはできません。MFAワークフローで認証用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なため、REST APIとCLIは実質的に操作不能になります。そのため、ユーザがMFAで認証されることを求めるトークンをSystem Managerで生成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にはSAMLを推奨します。

== トークンを作成および使用するためのワークフロー

. 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て、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_`

詳細はこちら。

* xref:{relative_path}access-management-tokens-create.html["アクセストークンを作成します"]
* xref:{relative_path}access-management-tokens-edit.html["アクセストークンを編集します"]
* xref:{relative_path}access-management-tokens-revoke.html["アクセストークンを取り消します"]

```
:leveloffset: -1


= ローカルユーザロールを使用する

:leveloffset: +1


[[IDafe4373cab1f5c76a18a8bb69755250b]]
= ローカルユーザロールを表示します
: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たロールベースアクセス制御（RBAC）の一部です。

.作業を開始する前に
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。

.このタスクについて
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だけです。

.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。

[[ID6bf88e8ea0b84ab52ef5e2439f68606b]]
= パスワードを変更します
: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。

.作業を開始する前に
* 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。

.このタスクについて
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（[表示/編集の設定]）以上である必要があります。
* パスワードは大文字と小文字を区別します。
*
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してください。
* セキュリティを強化するために、パスワードには15文字以上の英数字を使用し、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、パスワードは、ユーザのアクティブなセッションを終了するために原因 を変更します。

====
.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低文字数が設定されていない場合は、選択したユーザがパスワードを入力しないとストレージアレイにアクセスできないようにするオプションのチェックボックスをオンにし、そのユーザの新しいパスワードを入力します。
. 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。

[[ID0cd0b9131adfaa0f89fa28f6206f6f12]]
= ローカルユーザパスワードの設定を変更します
: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新規または更新されるローカルユーザパスワードの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ストレージアレイにアクセスできるようにすることもできます。

.作業を開始する前に
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。

.このタスクについて
ローカルユーザパスワードの最小文字数を設定する際には、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の最小文字数を設定するには、「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ンにしてから、スピンボックスを使用して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、現在の設定以上の長さ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

[[ID3ea48f63fe99c65a24d5e3631fc22103]]
= LDAPディレクトリサーバを追加します
: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。

.作業を開始する前に
* 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がローカルマシンにインストールされている必要があります。


.このタスクについて
ディレクトリサーバの追加は、2つのステップで行います。まず、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、認証に使用するCA証明書が標準の署名機関によって署名されていない場合、その証明書もアップロードする必要があります。バインドアカウントのクレデンシャルがある場合は、その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]
====
手順 で
LDAPサーバを追加すると、従来の管理インターフェイスは無効になります。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に使用される方法です。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安全な通信方法（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 | 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'ldap[s]://*host*:*port*'の形式で入力します



 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、上記のサーバURLフィールドに
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やグループ内の検索で使用する読み取り専用の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」であれば、「CN=bindacct、CN=Users、DC=cpoc、DC=local」などと入力します。
```

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した場合に表示されます。

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します
a|
入力したLDAPサーバの設定でストレージアレイ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オンにした場合、テストに失敗すると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|
ユーザー名属性
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\（s \）
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 | 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ます。正規表現パターンの一部でない場合は、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|
ロール
 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選択します。このグループに含めるロールを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。
+
ストレージアレイとLDAPサーバが通信できるかどうかの検証がシステムによって実行されます。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。

[[ID6dcb0cf99f2d9e7479995c871324f5b5]]
= ディレクトリサーバ設定とロールマッピングを編集します
: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設定済みの場合は、いつでも設定を変更できます。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。

.作業を開始する前に
* 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が定義されている必要があります。

.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 | 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。形式はです `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やグループ内の検索で使用する読み取り専用のユーザアカウント。

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した場合に表示されます）。

a|
保存する前にサーバ接続をテストします
a|
ストレージアレイがLDAPサーバの設定と通信できることを確認します。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オンにした場合、テストに失敗すると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|
ユーザー名属性
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|
グループとロールのマッピングに使用される、ユーザのグループ属性のリスト。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 | 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ます。正規表現パターンの一部でない場合は、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|
ロール
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。現在のユーザセッションのみが保持されます。

[[IDf3f96672a9319bf096f0042f75aa2aaf]]
= ディレクトリサーバを削除します
: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間の接続を解除するために、アクセス管理ページからサーバ情報を削除できます。このタスクは、新しいサーバを設定して古いサーバを削除する場合などに実行します。

.作業を開始する前に
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。

.このタスクについて
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「remove」と入力し、「* Remove *」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、このサーバから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を使用する

:leveloffset: +1

[[ID353ae385bb297555fac484c24e5ecead]]
= SAMLを設定する
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセス管理の認証を設定する場合、ストレージアレイに組み込みのSecurity Assertion Markup Language（
SAML）機能を使用することができます。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。

.作業を開始する前に
* 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。

.このタスクについて
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。多要素認証にも対応し、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を設定すると、ストレージアレイが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。その後、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。あとで SAMLを無効にすると、元の設定に戻ってディレクトリサービスが使用されます。

====
[CAUTION]
====
* SAMLを編集および無効化しています。*
SAMLを有効にすると、ユーザインターフェイスで無効にすることはできず、IdP設定を編集することもできません。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からなる手順 です。

== 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。

+
アイデンティティプロバイダファイルのインポート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ために、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、コントローラのドメイン名やIPアドレスなど、IdPがサービスプロバイダと通信するために必要な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。
+
[Export Service Provider Files]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。ファイルの保存先をメモします。

. 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の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サーバで、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。

.作業を開始する前に
* 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ておきます。

.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 | 説明

a|
マッピング

a|
ユーザー属性
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ます。正規表現パターンの一部でない場合は、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|
ロール
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選択します。追加するロールを1つずつ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。また、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、*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。

.作業を開始する前に
* 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ておきます。

.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表示されます。

. 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。
+
ログインのテストを実行している間、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い場合は、エラーメッセージに詳細が表示されます。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のアドレスが正しいこと。

== 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、前の手順で説明したとおりです。

.作業を開始する前に
* 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ておきます。
* 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]
====
* SAMLを編集および無効化しています。*
SAMLを有効にすると、ユーザインターフェイスで無効にすることはできず、IdP設定を編集することもできません。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。
+
[Confirm Enable SAML（SAMLを有効にする）]ダイアログボックスが開きます。

. 「enable」と入力し、「* Enable」をクリックします。
. SSOログインのテスト用に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。

[[ID22cbc56577e7f8b938486b736a97301c]]
= SAMLのロールマッピングを変更する
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセス管理にSAMLを設定している場合、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との間のロールマッピングを変更できます。

.作業を開始する前に
* 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 | 説明

a|
マッピング

a|
ユーザー属性
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|
ロール
 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選択します。このグループに含めるロールを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。現在のユーザセッションのみが保持されます。

[[ID6f50fcb08e41e289a46238fc768d734d]]
= SAMLサービスプロバイダファイルをエクスポートする
: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のメタデータをエクスポートして、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することができます。

.作業を開始する前に
* 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。


.このタスクについて
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。
+
[Export Service Provider Files]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。

====
+
ファイルの保存先をメモします。

. 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の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の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


= アクセストークンを使用する

:leveloffset: +1


[[ID0da1a6fdfddd3f64c3180a49750a1bad]]
= アクセストークンを作成します
: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、注意して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（S
ave）]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: トークンの期限が切れると、ユーザ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:
必ずトークンテキストを保存してください。これは、ダイアログを閉じる前にテキストを確認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、トークンが指定されていない場合、CLIはユーザにコマンドラインでアクセストークン値の入力を求めるプロンプトを表示します。

[[ID980f8eabe8fabf229ca330fb5447e158]]
= アクセストークンの設定を編集します
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセストークンの設定を編集できます。これには、有効期限や新しいトークンを作成する機能が含まれます。

.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、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、期限切れ前のトークンを再使用できます。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 xref:{relative_path}access-management-tokens-revoke.html["アクセストークンを取り消します"]。

. [保存（ Save ）] をクリックします。

[[ID47bb576658e3fb92fb30ae9dfc8846fb]]
= アクセストークンを取り消します
: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ていると判断した場合、またはアクセストークンの署名と検証に使用した暗号キーの手動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、トークンの署名に使用す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。ストレージアレイが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無効にした後、新しいトークンを作成してすぐに使用できます。

```
:leveloffset: -1


= syslogを管理します

:leveloffset: +1


[[IDaaa0ac4594c9de82152769775453b835]]
= 監査ログアクティビティを表示します
: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、監査ログを表示して、ユーザによる操作、認証エラー、無効なログイ
ンの試行、およびユーザセッションの期間を監視できます。

.作業を開始する前に
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ます。各列に表示される情報は次のとおりです。

+
** *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して認証されていない操作が実行さ
れた場合は、「N/A」と表示されます。内部プロキシまたはその他のメカニズムによって、認証され
ていないアクションがトリガーされることがあります。
** *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）。

. [監査ログ]ページの選択項目を使用して、イベントを表示および管理します。
+
.選択の詳細
[%collapsible]
====
[cols="25h,~"]
|===
| 選択（Selection） | 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）で限定します。

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。単語の完全一致には引用符("")を使用し、1つ以上の単語を返すには「」または「」を入力します。単語を省略するにはダッシュ(--)を入力します。

a|
更新
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|
イベントを削除します

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/非表示を切り替えます
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["列の表示/非表示
"]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|
列フィルタを切り替えます
a|
[切り替え]アイコンをクリックするimage:../media/sam-1140-ss-access-toggle.gif["切り替え"]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|
変更を元に戻します
a|
[元に戻す（Undo）]アイコンをクリックしimage:../media/sam-1140-ss-access-undo.gif["元に戻す"]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（Export）
 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。

|===
====

[[IDa258f44e2fb8d235860d2e57fef8aafd]]
= 監査ログポリシーを定義する
: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。

.作業を開始する前に
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。

.このタスクについて
このタスクでは、監査ログの設定を変更する方法について説明します。古いイベントの上書きに関するポリシーや記録するイベントタイプに関するポリシーなどが含まれます。

.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 | 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指定します。

** *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が再びシステムにアクセスできるようにするには、Security Adminロールが割り当てられている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。

[[ID7054421bb6dca9c9bd36b65099f21751]]
= 監査ログからイベントを削除します

```
: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。

.作業を開始する前に
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「delete」と入力し、「* Delete *」をクリックします。
+
最も古いイベントは監査ログページから削除されます。

```
[[ID57a7593452f1dc9039a414dd6b382b95]]
```
= 監査ログ用のsyslogサーバを設定します
```
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]
監査ログを外部の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、監査ログは自動的にsyslogサーバに保存されます。

.作業を開始する前に
* 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。
* サーバが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）証明書が配置されている必要があります。CA証明書がWebサイトの所有者を識別することにより、サーバとクライアントの間のセキュアな接続が確立さ

.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（ Add ）] 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サーバを設定します"]。

 NOTE: If multiple syslog servers are configured, all configured syslog servers will receive an audit log.

[[IDdd57b422594204176184ba19e6c13fce]]
= 監査ログレコード用の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したり、サーバ用の新しい認証局（CA）証明書をアップロードしたりできます。

.作業を開始する前に
* 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。
* 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

= よくある質問です

:leveloffset: +1

[[ID14a00020f182cc55a7ed9a1bd961fdb0]]
= 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。
* 必要な権限がありません。
*

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。
* ログインが複数回失敗したために、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。
*
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た可能性があります。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。ログインするには、ブラウザをリフレッシュしてください。

ミラーリングタスク用のリモートストレージアレイでログインエラーが発生する場合は、次のいずれかが原因の可能性があります。

* 入力したパスワードが正しくありません。
* ログインが複数回失敗したために、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が最大数に達している。複数のユーザまたはクライアントをチェックしてください。

[[IDf058706c1af9d509a8967e3532bf1946]]
= 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がローカルマシンにインストールされている必要があります。

[[ID722028e3cd7b2d7a31bab5056f3f660d]]
=
ストレージアレイのロールを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搭載された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。

* ディレクトリサービスでユーザグループを定義しておきます。
*
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を確認しておきます。正規表現がサポートされます。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。

[[ID67573a7a13ade253811363635adfb97e]]
= 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。この設定が無効な場合、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てログインします

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。

[[ID0e4001a9f0b452187d027cd0071690d3]]
= SAMLを設定および有効にするときは、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

作業を開始する前に、次の点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く必要があります。
* 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。
* 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おく必要があります。

* 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。（SSOログインテストはSAMLが有効になる前にシステムでも実行されます）。
* 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、ディレクトリサービス、またはその両方）が自動的にリストアされます。
* 現在ユーザ認証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を設定すると、次のクライアントがストレージアレイリソースにアクセスできなくなります。
+
** 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てログインします

[[ID90c0f892b694cde1e1fee02d5edd1f2a]]
= 監査ログにはどのようなタイプ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。

[[ID19120a19e7647b50155dee33dcc65c35]]
= 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"]
監査ログは外部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。
* サーバが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）証明書が配置されている必要があります。CA証明書がWebサイトの所有者を識別することにより、サーバとクライアントの間のセキュアな接続が確立さ
* 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。

[[ID518cfb0fd6e15557cdeafa107b9b503b]]
= syslogサーバが監査ログを受信しなくなりました。どうすればよいですか？
: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、
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


[[ID789ae36e653ed8562f2110d78e5be344]]
= 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。



== 証明書とは何ですか？

_証明書_は、Webサイトやサーバなどのオンラインエンティティを識別し、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。
```

詳細はこちら。

```
* 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"]
```

== 署名済み証明書の設定方法

署名要求は、System Managerから生成することも、秘密鍵と公開鍵のペアを使用して外部から生成することもできます。署名要求がCAに送信され、証明書ファイルが生成されます。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。

詳細はこちら。

```
* xref:{relative_path}use-ca-signed-certificates-for-
controllers.html["コントローラのCA署名証明書を使用する"]
* 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

証明書に関連するタスクの詳細：

```
* xref:{relative_path}view-imported-
certificates.html["インポートされた証明書の情報を表示"]
* xref:{relative_path}enable-certificate-revocation-
checking.html["証明書失効チェックを有効にします"]
```

= 概念

```
:leveloffset: +1


[[ID132e27ffd74c361c8683c074d331d334]]
= 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、指定されたサーバとクライアント間でのみ、Web通信が非公開かつ変更されずに暗号化された形式で送信されます。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、第三者が所有者のIDを検証し、そのデバイスが信頼できると判断したことを意味します。ストレージアレイの各コントローラには、自動生成された自己署名証明書が付属しています。自己署名証明書を引き続き使用することも、CA署名証明書を取得してコントローラとホストシステム間のよりセキュアな接続を確立することもできます。

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

====


== 署名済み証明書

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

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

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

* *ルート*--
```

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

== 自己署名証明書

ストレージアレイの各コントローラには、自己署名証明書が事前にインストールされています。自己署名証明書はCA署名証明書と似ていますが、第三者ではなくエンティティの所有者によって検証される点が異なります。CA署名証明書と同様に、自己署名証明書には独自の秘密鍵が含まれており、サーバとクライアントの間のHTTPS接続を介してデータが暗号化および送信されることも保証されます。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を含むWebサイトに接続しようとするたびに、ブラウザに警告メッセージが表示されます。Webサイトに進むには、警告メッセージ内のリンクをクリックする必要があります。これにより、基本的には自己署名証明書が受け入れられます。

== キー管理サーバに使用する証明書

ドライブセキュリティ機能を持つ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を管理することもできます。

```
[[ID703f91d0332d6af8875db91a8c3fa3eb]]
= 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 | 説明


 a|
できます
 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文書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が証明書の問題 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、その情報について証明（署名）する信頼されたエンティティのIDが含まれます。



 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、チェーンの最上位にはルート証明書が1つ、中間証明書が1つ以上、エンティティを識別するサーバ証明書が1つ含まれます。



 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を使用する場合は、ルート証明書が1つだけ必要です。

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、サーバとクライアントの間でHTTPS接続を介してデータが暗号化された形式で送信されることが保証され

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、サーバとクライアントの間でHTTPS接続を介してデータが暗号化された形式で送信されることが保証されます。また、アルファベットと数字で構成されるデジタル署名も含まれます。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

[[ID4121585b352648c4d2c75ff013c84d68]]
= コントローラの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"]

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。

.作業を開始する前に
* 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、証明書の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。

.このタスクについて
CA署名証明書の使用は、3つの手順で構成される手順 です。

== 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。

.このタスクについて
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、組織に関する情報とコントローラのIPアドレスまたはDNS名のいずれかを提供します。このタスクでは、ストレージアレイにコントローラが1つあり、CSRファイルが2つある場合は1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、に進むこともできます <<手順2：CSRファイルを送信します>>。

====
.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.などの接尾辞も含めて入力してください
** *組織単位（オプション）*--証明書を処理している組織の部門。

** *市区町村*--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名の先頭にワイルドカードを使用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指定する場合は、カンマで区切って入力します。
** *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指定する場合は、カンマで区切って入力します。代替DNS名がない場合は、最初のフィールドに入力したDNS名をここにコピーします。DNS名の先頭にワイルドカードを使用することはできません。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、エラーからリカバリする場合に使用します。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。ダウンロードフォルダの場所は、ブラウザによって異なります。

. に進みます <<手順2：CSRファイルを送信します>>。

== 手順2：CSRファイルを送信します

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ています。

.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、別のCSRファイルを再生成しないでください。*
CSRを生成するたびに、システムは秘密鍵と公開鍵のペアを作成します。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から返された署名済み証明書については、を参照してください <<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

署名済み証明書を認証局（CA）から受け取ったあと、コントローラのファイルをインポートします。

.作業を開始する前に
* 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（たとえば、

.p7bファイル）が提供された場合は、チェーンファイルを個々のファイル（ルート証明書、1つ以上の中間証明書、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のcertmgrユーティリティーを使用して'ファイルを展開できます(右クリックしてメニューを選択しますすべてのタスク[エクスポート])base-64エンコーディングが推奨されます。エクスポートが完了すると、チェーン内の証明書ファイルごとに1つのCERファイルが表示されます。
* 証明書ファイルをSystem Managerにアクセスするホストシステムに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表示されます。

. 「
*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。

[[IDf25139f3c02c00057735276bb28d568f]]
= 管理証明書をリセットします
: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。

.作業を開始する前に
* 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、証明書の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。

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

.結果
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。そのため、セッションの自己署名証明書を手動で承認するように求められます。

[[ID10cd71ea20ad9daf29f639e6be04cc51]]
= インポートされた証明書の情報を表示
: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、ストレージアレイの証明書タイプ、発行元、および有効な証明書の日付範囲を確認できます。

.作業を開始する前に

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、証明書の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,~"]
|===
| タブをクリックする | 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|
高い信頼性
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。

|===

```
[[ID9713b2110ad0f7413f347308c48ae2f6]]
= クライアントとして機能するコントローラの証明書をインポートする
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
コントローラが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できます。このタブでは、コントローラ（クライアントとして動作）がそのサーバからの通信を受け入れることができます。

.作業を開始する前に
* 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、証明書の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。


.このタスクについて
別のサーバがコントローラ（LDAPサーバやTLSを使用するsyslogサーバなど）に接続できるようにするには、[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表示されます。

. 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。



[[IDbae2702a8409ec4d03b104e77dc6108b]]
= 証明書失効チェックを有効にします
: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。

.作業を開始する前に
* 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、証明書の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。


.このタスクについて
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。

[[IDaed8700aa1f6ff43b74ba7f93d385858]]
= 信頼された証明書を削除する
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
以前に[信頼済み]タブからインポートした、ユーザーがインストールした証明書を削除できます。

.作業を開始する前に
* 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、証明書の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LDAPサーバなどの別のサーバの認証に使用している証明書を新しい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。

====
.このタスクについて
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。
+
ストレージアレイの信頼された証明書が表に表示されます。

. 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「delete」と入力し、「* Delete *」をクリックします。

[[IDe8e29f1326aa735fb9c5d1800c568f8c]]
= 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確立するためには、適切な証明書セットを設定する必要があります。

.作業を開始する前に
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、証明書の機能は表示されません。

.このタスクについて
コントローラとキー管理サーバ間の認証は、2段階の手順 です。

== 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、キー管理サーバで信頼されている認証局（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は、キー管理サーバが自身のKey Management Interoperability Protocol（
KMIP）要求を信頼できるよう、ストレージアレイのコントローラを検証します。

NOTE: 秘密鍵と公開鍵のペアによって外部で生成されたCSRファイルは、
[外部セキュリティキーの作成]ダイアログを使用してインポートできます。外部生成されたCSRファイルのインポートの詳細については、を参照してください https://docs.netapp.com/us-en/e-series-santricity/sm-settings/use-ca-signed-certificates-for-

authentication-with-a-key-management-server.html#step-2-import-certificates-for-the-key-management-server["手順2：キー管理サーバの証明書をインポートする"]。

.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*--
クライアントを識別する名前。一般的には、クライアント証明書の命名規則に関するKMSサーバの要件と共通名の内容を一致させることが一般的です。一般的な名前は、ハンドシェイク中にクライアントの証明書が提示されたときに、KMSがクライアントの証明書を識別するのに役立ちます。
** *組織*--会社または組織の正式名称。Inc.やCorp.などの接尾辞も含めて入力してください
** *組織単位（オプション）*--証明書を処理している組織の部門。
** *市区町村*--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。
+

NOTE: キー管理サーバは独自の
CAとして機能するため、署名済み証明書を直接生成する機能を備えているのが一般的です。

. 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

次の手順として、ストレージアレイとキー管理サーバの間の認証用に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。

.作業を開始する前に
* 署名済みのクライアント証明書ファイルがある（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>>）をクリックし、System Managerにアクセスするホストにファイルをコピーしておきます。クライアント証明書は、キー管

理サーバが自身のKey Management Interoperability Protocol（
KMIP）要求を信頼できるよう、ストレージアレイのコントローラを検証します。
* 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、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表示されます。

. 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。

. 秘密鍵と公開鍵のペアを使用して外部で証明書ファイルを生成した場合は、
*[秘密鍵ファイルの選択]*の横にある*[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。
+
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。

[[ID67e520b940a5bb0cb95f802712469337]]

= キー管理サーバ証明書をエクスポートする
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
キー管理サーバ用の証明書をローカルマシンに保存できます。

.作業を開始する前に
* 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、証明書の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

= よくある質問です

:leveloffset: +1

[[IDf1065f5b9d8ff5b1bd410b3390291a4d]]
= Cannot Access Other Controller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び表示され、証明書の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。

[[ID1034123b2493b2f30059b3516a84af5e]]
= 外部キー管理を行うために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が互いに信頼関係を確立できるように、2つのエンティティの間の認証用に2種類の証明書をインポートします。

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。秘密鍵と公開鍵のペアを使用して、CSRを外部で生成することもできます。

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、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、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。

[[IDb78627b61b4b6b181c89d25aac52f28a]]
= 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。その証明書について、サーバから「good」、「revoked」「unknown」のいずれかの値が返されます。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。

====

[[ID9ce79f631721164ef4344b921088c655]]
= 失効チェックが有効になるのはどのタイプのサーバですか？
: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、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


[[IDb3ec1e68edec54c05b19f2329e0bca08]]
= 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"]
サポートページでは、テクニカルサポート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がありますか？

サポートでは、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、ソフトウェアアップグレードの実行を行うことができます。

詳細はこちら。

* 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["Upgrade Center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。

= 情報と診断を表示します

```
:leveloffset: +1
```

```
[[IDe4cee5c69d61ca35ee2a9061a03a41a7]]
```
= ストレージアレイプロファイルを表示します
```
: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概要 を提供します。

.このタスクについて
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。管理クライアントにストレージアレイプロファイルのコピーを保存して、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することができます。構成を変更した場合は、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てください。

.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 | 説明
```

a|
ストレージアレイ
a|
ストレージアレイについ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。コントローラ数、ドライブシェルフ数、ドライブ数、ディスクプール数、ボリュームグループ数などを指定できます。
ボリューム、およびホットスペアドライブ、使用可能なドライブシェルフ、ドライブ、ソリッドステートディスク（SSD）、およびボリュームの最大数、Snapshotグループ、Snapshotイメージ、Snapshotボリュームおよび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
ステータスおよびAutoSupport スケジュール情報。
サポートデータの自動収集とサポートデータのスケジュール収集、ストレージアレイのWorld-Wide Identifier（WWID）、およびメディアスキャンとキャッシュの設定。

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セクションにこれら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、開始のタイムスタンプ、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|
ストレージアレイにおける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。追加情報
の一覧には、トポロジの定義とホストタイプの定義が含まれています。

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」セクションにこれら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ドライブは、シェルフID、ドロワーID、スロットIDの順に表示されます。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。ドライブのセクションには、ドライブチャネル情報、ホットスペアの適用範囲情報、および摩耗度に関する情報も含まれます（SSDドライブの場合のみ）。寿命情報には、使用済み寿命の割合（これまでにSSDドライブに書き込まれたデータの量）と、ドライブの理論上の合計書き込み制限値を合わせた値が含まれます。
** *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）、ドライブの本数、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、ドライブタイプおよび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、または入出力モジュール（IOM）キャニスターなどが含まれます。ストレージアレイでセキュリティキーを使用している場合は、Hardware（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|
の機能
 a|
インストールされている機能パックのリスト、および1つのホストまたはホストクラスタで許可されているSnapshotグループ、Snapshot（従来のもの）、ボリュームの最大数が表示されます。機能セクションには、ドライブセキュリティ、つまりストレージアレイがセキュリティ有効かセキュリティ無効かについても記載されています。

|===
====
. 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。
+
一致するすべてのキーワード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「storage-array-profile.txt」という名前でファイルが保存されます。

[[ID80581f09e9b34c0df0e7bfd770072f60]]
= 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
: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表示されます。

.このタスクについて
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。ファームウェアのバージョンによっては、他のバージョンのファームウェアに依存しているものもあります。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、「firmware-inventory.txt」というファイル名でファイルが保存されます。

. テクニカルサポートからの指示に従ってファイルを送信します。

:leveloffset: -1

= 診断データを収集します

:leveloffset: +1

[[IDe8f4921320af03035446869dd9f002e9]]
= サポートデータを手動で収集する
: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各種のインベントリ、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することができます。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分析に使用できます。

.このタスクについて

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つずつしか実行できません。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、「 upport-data.7z 」という名前でファイルが保存されます。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「tray -component-state-capture.7z」という別の圧縮ファイルにアーカイブされます。

4. テクニカルサポートからの指示に従ってファイルを送信します。

構成データを収集

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、コントローラからRAID構成データを保存できます。データのリストア方法については、テクニカルサポートにお問い合わせください。

このタスクについて

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メモリの場所から取得されます。

Collect Configuration Data機能では’save storageArray dbmDatabaseのCLIコマンドと同じ情報が保存されます

このタスクは、Recovery Guruの処理またはテクニカルサポートの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「configurationdata-<ArrayName>-<dateTime >.7z」は、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を取得します

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。

作業を開始する前に

トラブルシューティング用の追加ファイルを送信するようテクニカルサポートから依頼されます。

このタスクについて

リカバリサポートファイルには、次の種類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。

   ストレージアレイが収集したすべてのリカバリサポートファイルがダイアログボックスに表示されます。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からの指示に従ってファイルを送信します。

トレースバッファを取得します

コントローラからトレースバッファを取得して、分析用のファイルをテクニカルサポートに送信できます。

このタスクについて

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を記録します。特に例外条件です。トレースバッファを取得する際には、ストレージアレイの処理は中断されず、パフォーマンスへの影響は最小限に抑えられます。

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. [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オンにします。

   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表示されるコントローラステータスメッセージが「失敗」または「無効」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、「trace-buffers.7z」というファイル名でファイルが保存されます。

5. テクニカルサポートからの指示に従ってファイルを送信します。

I/Oパスの統計を収集

I/Oパス統計のファイルを保存し、分析用にテクニカルサポートに送信できます。

このタスクについて

テクニカルサポートは、I/Oパス統計をパフォーマンスの問題の診断に使用します。アプリケーションパフォーマンスの問題は、メモリ利用率、CPU利用率、ネットワークレイテンシ、I/Oレイテンシなどの問題が原因で発生する可能性があります。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パスの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。コントローラのリセット（リブート）時にもカウンタがリセットされます。

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. 操作を実行することを確認するには’collect’と入力してから'*Collect*をクリックします

   ブラウザのDownloadsフォルダに、「io-path-statistics」というファイル名でファイルが保存されます。7z

4. テクニカルサポートからの指示に従ってファイルを送信します。

ヘルスイメージを取得します

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のデータダンプです。テクニカルサポートがコントローラの問題を診断する際に使用します。

このタスクについて

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たあとで、エラーが発生したコントローラがリブートされ、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問い合わせる必要があります。

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. [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、「health-image.7z」という名前でファイルが保存されます。

4. テクニカルサポートからの指示に従ってファイルを送信します。

リカバリ操作の実行

読み取り不能セクターのログを表示します

読み取り不能セクターのログを保存して、分析用のファイルをテクニカルサポートに送信できます。

このタスクについて

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処理中、および再構築などの変更処理中に検出されます。読み取り不能セクターが検出されたストレージアレイに対しては、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が1、000個のエントリに達すると、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たRAID 5の書き込みとRAID 6の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ログを保存するには、次の手順を実行

   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、「unreadable-sectors.txt」という名前でファイルが保存されます。

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依頼があった場合は、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

ドライブポートを再度有効にします

誤配線状態からリカバリするための修正措置が実行されたことをコントローラに通知できます。

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。

リカバリモードをクリアします

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、通常動作に戻します。

作業を開始する前に

- 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。

このタスクについて

ストレージアレイには、その論理構成（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含まれています。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が停止され、構成データベースがフリーズされるため、その間に次のいずれかの作業を実行できます。

- 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リストアする。この作業を行う場合は、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）を使用して実行されます。
- ストレージアレイを一から再構成する。

ストレージアレイの構成がリストアまたは再定義され、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は一度開始するとキャンセルできません。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 を管理します

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 データを事後対応として使用してお客様の問題の診断と解決を迅速に行い、潜在的な問題をプロアクティブに検出および回避します。

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。ディスパッチはただちに送信することも、スケジュール（毎日または毎週）に基づいて送信することもできます。

主なメリット

AutoSupport 機能の主な利点は次のとおりです。

- 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
- スケジュールに従って自動レポートを作成し、重要なイベントに関する自動レポートも作成できます
- ドライブなどの選択したコンポーネントのハードウェア交換要求の自動化
- 問題発生時に、お客様の妨げにならない形で通知し、修正措置を講じるための情報をテクニカルサポートに伝えます
- 設定に関する既知の問題がないかどうか、ディスパッチを監視する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。送信はすべて、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。送信はすべて、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、保留中の新規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

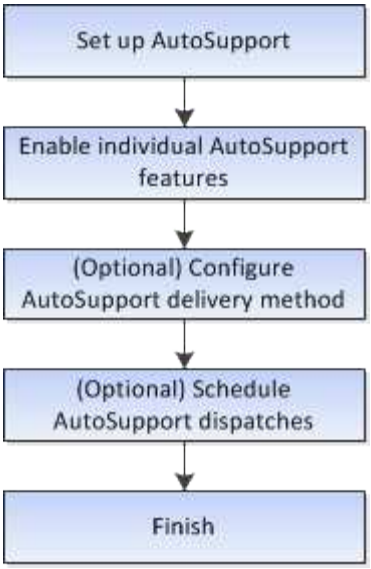
ストレージアレイでは、次の2つの方法でサポートデータを収集できます。

- * 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および送信されるため、AutoSupport 機能の方が使いやすくなります。AutoSupport データをプロアクティブに使用すると、発生前に問題を防ぐことができます。テクニカルサポートはすでにデータにアクセスできるため、AutoSupport 機能を使用した方がトラブルシューティングにかかる時間が短縮されます。これらの理由から、AutoSupport 機能がデータ収集方法として推奨されます。

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 機能を有効または無効にします

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か、あとから有効または無効にすることができます。

作業を開始する前に

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。

このタスクについて

AutoSupport 機能はいつでも無効にできますが、有効なままにしておくことを強く推奨します。AutoSupport 機能を有効にしておくと、ストレージアレイに問題が発生したときに、迅速に原因を判断して解決できます。

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。送信はすべて、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。送信はすべて、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、保留中の新規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レイアウトからわかるように、機能は相互に依存しています。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 の配信方法を設定する

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プロトコルとSMTPプロトコルがサポートされます。

作業を開始する前に

- 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サーバのアドレスはSystem Managerで設定する必要があります（このタスクはハードウェアページから実行できます）。

このタスクについて

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・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。
- **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とEメール方式の違い*。SMTPを使用するEメール配信方法は、HTTPS配信方法と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、HTTPS配信方式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]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）は必要な場合にのみ入力します。
     - 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の確立に適したプロキシサーバをシステムで自動的に選択できます。

- [電子メール]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アドレスを指定します。
  - AutoSupport ディスパッチのEメールの送信元フィールドに表示されるEメールアドレスです。
  - 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、送信元とメールサーバとの認証用の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ブロックするファイアウォールがある場合は、ホワイトリストに次のURLを追加します。 `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、設定を確認してから、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を設定します

System Managerでは、AutoSupport ディスパッチのデフォルト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。

作業を開始する前に

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。

このタスクについて

- 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では、期間内のランダムな時刻が選択されます。協定世界時（UTC）が使用されるため、ストレージアレイのローカルの時刻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の時刻を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、指定した複数の日にちからランダムな1日が選択されます。週次ディスパッチを実行しない曜日がある場合は、選択を解除します。System Managerでは、許可した複数の日にちからランダムな1日が選択されます。
- 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では、期間内のランダムな時刻が選択されます。協定世界時（UTC）が使用されるため、ストレージアレイのローカルの時刻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の時刻を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 ディスパッチを送信します

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。

作業を開始する前に

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。

このタスクについて

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るため、問題のトラブルシューティングに役立ちます。

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。

   AutoSupport ディスパッチの送信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 のステータスを確認します

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参照して、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 ログを表示します

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。

このタスクについて

複数のログファイルを使用できます。現在のログファイルが200KBに達すると、そのファイルはアーカイブされ、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・ファイル名は'ASUPMessages.n'ですここで'_n_は1～9の整数です複数のログファイルが存在する場合は、最新のログと以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。

   現在のAutoSupport ログを示すダイアログボックスが表示されます。

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 メンテナンス期間を有効にします

AutoSupport メンテナンス期間を有効にして、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します。通常運用モードでは、問題 がある場合、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. メンテナンス期間の要求が処理されたときに確認のEメールを受け取るEメールアドレスを入力します。

   設定によっては、Eメールアドレスを5つまで入力できます。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。

   指定した期間の間、AutoSupport によるエラー発生時の自動チケット作成が一時的に停止されます。

完了後

メンテナンス期間は、ストレージアレイからの要求がAutoSupport サーバで処理された時点で開始されます。ストレージアレイでメンテナンス作業を行う前に確認のEメールが届いたことを確認してください。

AutoSupport メンテナンス期間を無効にします

AutoSupport メンテナンス期間を無効にして、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します。AutoSupport メンテナンス期間を無効にすると、問題 がある場合に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. メンテナンス期間を無効にする要求が処理されたときに確認のEメールを受け取るEメールアドレスを入力します。

   設定によっては、Eメールアドレスを5つまで入力できます。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。

   AutoSupport では、エラーイベント時の自動チケット作成が有効になっています。

完了後

メンテナンス期間は、ストレージアレイからの要求がAutoSupport サーバで処理された時点で終了します。確認のEメールが届いたことを確認してから次の手順に進んでください。

イベントを表示します

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含まれます。これは、テクニカルサポートが障害につながるイベントをトラブルシューティングする際に役立ちます。

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。ストレージアレイ内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。

- 重要
- 警告

情報提供目的で、すぐに対処する必要のないイベントは次のとおりです。

- 情報

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れば、データアクセスの中断を回避できる場合があります。

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手順 で重大イベントの詳細な概要 を参照してください。Recovery Guru「手順 」に情報を入力して、重大イベントを修正します。一部の重大イベントについては、修正時にテクニカルサポートへの連絡が必要になることがあります。

イベントログを使用してイベントを表示します

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	説明
すべてのフィールドを表示します	すべてのイベントを表示するか、重大/警告イベントだけ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特定のイベントなどに関連するイベントだけを表示する場合に便利です
列アイコンを選択します。	表示する他の列を選択できます。他の列には、イベントに関する追加情報が表示されます。
チェックボックスを選択します	保存するイベントを選択できます。テーブルのヘッダーにある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付と時刻のタイムスタンプ。 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をソートします。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ない可能性があります。この場合、イベントログに表示されるイベントと日時に不整合が生じる可能性があります。
[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、すぐに対処すれば、データにアクセスできなくなる状況を回避できる可能性があります。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、SNMPトラップを使用してネットワーク管理クライアントに送信されるか、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。
概要 列	イベントの概要 。 例-- Drive write failure-retries exhausted

項目	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が生成されるたびに1ずつ増えます。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タイプのイベントを識別する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	イベントをログに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’major-event-log-timestamp.log’という名前でファイルが保存されます

4. イベントログからイベントをクリアするには、次の手順を実行します

   イベントログに約8、000個のイベントが格納されると、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、イベントを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。

アップグレードを管理する

Upgrade Center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。

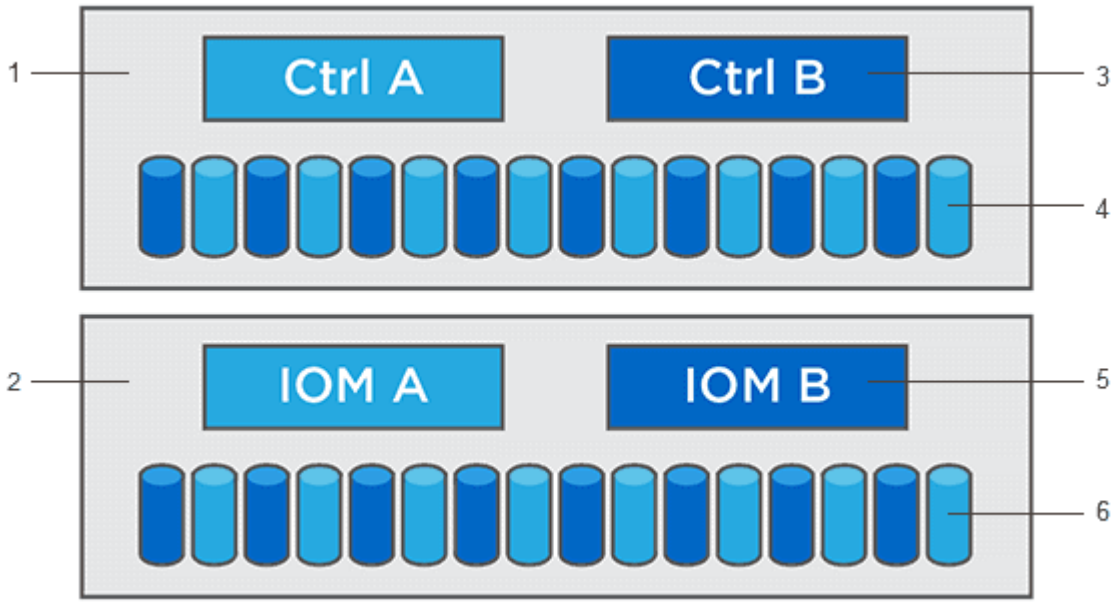
コントローラのアップグレードの概要

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することができます。

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いくつかのコンポーネントには、適宜アップグレードが必要な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、Software and Firmware Inventory（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するように、ホストのマルチパス/フェイルオーバードライバやHBAドライバのアップグレードも必要になることがあります。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の処理を継続できます。アップグレードでは、コントローラAのすべてのボリュームがコントローラBにフェイルオーバーしてコントローラAがアップグレードされます。その後、コントローラAに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オーバーされ、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常性チェック

アップグレードプロセスの一環として、アップグレード前の健常性チェックが実行されます。アップグレード前の健常性チェックでは、ストレージアレイのすべてのコンポーネントについて、アップグレードを実行できる状態であるかがチェックされます。次の状況に該当する場合、アップグレードを実行できないことがあり

- 割り当てられたドライブで障害が発生し
- ホットスペアを使用中です
- 不完全なボリュームグループです
- 同時に実行できません
- 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が多すぎます
- 構成データベースの検証に失敗しました
- ドライブの DACstore のバージョンが古い

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、ドライブの細かな動作特性を制御します。新機能の追加、パフォーマンスの向上、および不具合の修正のために、ドライブメーカーはドライブファームウェアの更新を定期的にリリースしています。

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式には、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。ストレージアレイでの I/O の処理はアップグレードの実行中も継続されます。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には、次のものがあります。

- 「最適」状態のプール内のドライブ
- 「最適」状態の冗長化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、その間は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状況で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、あるドライブをアップグレードしているときに 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、あるドライブをアップグレードしているときに別の 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、同じドライブタイプのすべてのドライブが同時にアップグレードされます。この方式では、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。ファームウェアファイルは互換性の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をアップグレードします

ストレージアレイのソフトウェア、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できます。

作業を開始する前に

- 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、パッチを適用していたり、カスタムバージョンのコントローラ NVSRAM ファイルを使用していて、上書きしたくない場合は、アップグレードを中止することもできます。

- 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ます。

  あとでアクティブ化する理由には、次のものがあります

  - 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から切り替えるか、内部でセキュリティ保護されているドライブから切り替えるか、ドライブのセキュリティを確保するために外部キー管理サーバ（KMS）を使用するかを確認します。
- 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決めます。

このタスクについて

OSのソフトウェアファイルまたはコントローラのNVSRAMファイルのどちらかのみをアップグレードすることも、両方のファイルをアップグレードすることもできます。

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。ストレージアレイの電源は切らないでください。

手順

1. ストレージアレイにコントローラが 1 台しかない場合やマルチパスドライバが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 以降のデジタル署名されたファームウェアが必要です。署名のないファームウェアをダウンロードしようとすると、エラーが表示されてダウンロードが中止されます。

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。

SANtricity OSソフトウェアのアップグレード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 'N2800-830000-000.dll' のようになります

次の処理が行われます。

- 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だけが表示されます。
- 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間は処理をキャンセルできますが、転送またはアクティブ化の実行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、「 drive upgrade_log-timestamp.txt 」という名前でファイルが保存されます。

完了後

- 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 に適用されてい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。カスタム設定については、アクティブ化のプロセスの完了後に

NVSRAM に再度適用する必要があります。

コントローラソフトウェアとファームウェアをアクティブ化します

アップグレードファイルはただちにアクティブ化することも、都合のいいタイミングでアクティブ化することもできます。

このタスクについて

ファイルは、アクティブ化せずにダウンロードおよび転送できます。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パスすると、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問い合わせ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しているコンポーネントによって異なります。

3. *オプション：*ア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、「 drive upgrade_log-timestamp.txt 」という名前でファイルが保存されます。

完了後

- 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 に適用されてい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。カスタム設定については、アクティブ化のプロセスの完了後に NVSRAM に再度適用する必要があります。

ドライブファームウェアをアップグレードします

ドライブファームウェアをアップグレードして、最新の機能やバグ修正をすべて適用することができます。

作業を開始する前に

- 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」であることを確認します。
- すべてのドライブのステータスが最適な状態である必要があります
- ストレージアレイで構成の変更が実行されていないことを確認します。
- 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アクティビティを停止します。

手順

1. メニューを選択します。Support [Upgrade Center]を選択します。
2. 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。
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。

   使用中のドライブファームウェアファイルを示すダイアログボックスが表示されます。

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、「 .dhUC101212CSS600_30602291_MS01_2800_0002 」のようになります。拡張子は「 .dlp 」です。

   ドライブファームウェアファイルは一度に 1 つずつ、最大 4 つまで選択できます。同じドライブに複数のドライブファームウェアファイルが対応している場合は、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、それ以外のファイルは削除します。

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。

   対応してい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は、これらの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。これらのドライブは、ストレージアレイによるドライブへの I/O の処理中に 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すると、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。冗長性がないドライブはオフラインで処理する必要があります。この要件には、 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。オフライン（並行）アップグレードは、通常、オンライン（デフォルト）方式よりも高速です。

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、「 drive upgrade_log-timestamp.txt 」という名前でファイルが保存されます。

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
割り当てられたドライブで障害が発生し	エラーの理由の 1 つとして、ドライブに適切な署名がない可能性があります。該当するドライブが認定済みの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交換する障害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
ストレージアレイをチェックしてください	• 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。
不完全なボリュームグループです	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。
すべて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/パリティスキャン以外）	1 つ以上の排他的な処理を実行中の場合は、その処理を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 で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の状態が最適以外である必要があります	いずれかのストレージアレイコントローラを確認する必要があります。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 の検証でデータベースコントローラの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マッピング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。
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 関連のチェック	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 個を超える DDE 情報または重大 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。
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。
2 個を超えるデグレードドライブチャネル重大 MEL イベントが過去 7 日以内に報告されました	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 個を超える重大 MEL エントリが生成されます	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。

完了後

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。

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の可能性を確認します

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エラーが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	説明	推奨される対処方法
割り当てられたドライブで障害が発生し	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。	エラーの理由の 1 つとして、ドライブに適切な署名がない可能性があります。該当するドライブが認定済みの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交換する障害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ている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。
不完全なボリュームグループです	ボリュームグループに含まれるドライブが迂回された、削除された、または応答しない場合、そのボリュームグループ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は、ファームウェアをアップグレードできなくなります。	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。
すべてのボリュームグループで実行中の排他的処理（バックグラウンドメディア / パリティスキャン以外）	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。	1 つ以上の排他的な処理を実行中の場合は、その処理を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 で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。

ファームウェアのダウンロードエラーです	説明	推奨される対処方法
いずれかのコントローラの状態が最適以外である必要があります	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を確認する必要があります。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。
SPM の検証でデータベースコントローラの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マッピング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。
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の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 関連のチェック	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 個を超える DDE 情報または重大 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。
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。
2 個を超えるデグレードドライブチャネル重大 MEL イベントが過去 7 日以内に報告されました	2個を超えるデグレードドライブチャネル重大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 4 個を超える重大 MEL エントリが生成されます	4個を超える重大イベントログエントリが過去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。
有効な管理IPアドレスを指定してください。	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。

ファームウェアのダウンロードエラーです	説明	推奨される対処方法
このコマンドでは、各コントローラにアクティブな管理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。
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。
ファームウェアのダウンロード中にエラーが発生しました。手順 のアップロード。	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I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も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この問題 を解決してください。
ファームウェアアクティベーション手順 の実行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I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も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この問題 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、処理が正常に完了しなかった場合は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も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この問題 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な場合があります。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やダウンロードを妨げているエラーの状態をテクニカルサポートが把握するために役立ちます。

よくある質問です

収集するデータ

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用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も収集できます。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について、どのようなデータが表示されますか？

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。これらのフィールドはソートできます。

フィールド	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、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追加情報 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	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、ボリューム内のどこかで発生したメディアエラーに起因する読み取り不能セクターなど。 • 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何ですか？

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のデータダンプです。テクニカルサポートがコントローラの問題を診断する際に使用します。

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場合があります。

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。送信はすべて、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。送信はすべて、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、保留中の新規要求がないかどうかをチェックし、適切に応答します。

AutoSupport 機能ではどのような種類のデータが収集されますか。

AutoSupport 機能には、標準のディスパッチタイプとして、イベントディスパッチ、スケジュールディスパッチ、オンデマンドディスパッチ、リモート診断ディスパッチの3つがあります。

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設定されている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。
  - イベント発生時のストレージアレイの状況を包括的に記録した情報が含まれます。
- スケジュールディスパッチ

  AutoSupport 機能によって、複数のディスパッチが定期的に送信されます。

  - 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回送信されます現在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。送信はすべて、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。送信はすべて、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、保留中の新規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機能では、テクニカルサポートへのAutoSupportディスパッチの配信にHTTPSプロトコルとSMTPプロトコルがサポートされます。

作業を開始する前に

- 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サーバのアドレスはSystem Managerで設定する必要があります（このタスクはハードウェアページから実行できます）。

このタスクについて

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・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。
- **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とEメール方式の違い*。SMTPを使用するEメール配信方法は、HTTPS配信方法と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、HTTPS配信方式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]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）は必要な場合

にのみ入力します。

- 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の確立に適したプロキシサーバをシステムで自動的に選択できます。

◦ [電子メール]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アドレスを指定します。
- AutoSupport ディスパッチのEメールの送信元フィールドに表示されるEメールアドレスです。
- 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、送信元とメールサーバとの認証用の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、設定を確認してから、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。

構成データとは何ですか？

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とディスクプールに関するすべてのデータが含まれています。Collect Configuration Data機能では'save storageArray dbmDatabaseのCLIコマンドと同じ情報が保存されます

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「readme.txt」ファイルを読み、アップグレードを実行することを決めておきます。
- 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、IOMファームウェアを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、パッチを適用していたり、カスタムバージョンのコントローラ NVSRAM ファイルを使用していて、上書きしたくない場合は、アップグレードを中止することもできます。

- 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には、次のものがあります

  - 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するように、ホストのマルチパス/フェイルオーバードライバやHBAドライバのアップグレードも必要になることがあります。

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"。

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ファームウェアは一緒にアップグレードされます。エンクロージャに残したいIOMファームウェアの特定の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。

ファームウェアアップグレードに時間がかかる場合、どのような理由が考えられますか？

ファームウェアアップグレードの進捗は、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で、高速の再構築プロセス中にボリュームの転送が実行されると、システムは転送されたボリューム上で完全な再構築を開始します。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、次の項目を確認しておきます。

- 予防措置として、ディスクツーディスクバックアップ、（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、ドライブを数本だけアップグレードしてファームウェアの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おきます。
- 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タイプを選択するにはどうすればよいですか？

ドライブ上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、ステータスが最適の場合は、オンライン方式を使用してドライブの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、オンライン方式でもオフライン方式でも更新できます。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が出る場合があります。

- * 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（RAID 0）か、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の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 7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。このページから、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、そのステータスを表示し、1つのアレイまたはアレイ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（ **Area** ）	説明
管理	ネットワーク内のストレージアレイの検出、アレイのSANtricity System Managerの起動、1つのアレイから複数のアレイへの設定のインポート、およびアレイグループの管理を行います。設定のインポートやアレイグループの作成など、アレイに対する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選択します。各行の最後にある省略記号には'名前の変更など'1つのアレイでの操作を実行するためのインラインメニューがあります
処理	あるアレイから別のアレイへの設定のインポートなど、バッチ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、一部の処理は使用できません。
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、および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、次の項を参照してください。

- "管理者パスワード保護を設定します"
- "adminパスワードを変更"
- "ローカルユーザプロファイルのパスワードを変更します"

サポートされているブラウザ

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	八九
Mozilla Firefox	8時80分
Safari	14
Microsoft Edge の場合	90

Web Services Proxyをインストールしてブラウザから使用できるようにしておく必要があります。

管理者パスワード保護を設定します

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。

管理パスワードとユーザプロファイル

Unified Managerを初めて起動したときは、管理者パスワードの設定を求めるプロンプトが表示されます。管理者パスワードを持つユーザは、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、adminパスワードのほかに、1つ以上のロールがマッピングされたユーザプロファイルが事前に設定されています。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だけです。パスワードを変更するには、以下を参照してください

- "adminパスワードを変更"

- "ローカルユーザプロファイルのパスワードを変更します"

セッションタイムアウト

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、ソフトウェアはその後のパスワード入力を拒否します。パスワードを再度入力するには、「通常」状態にリセットされるまで10分待つ必要があります。

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"。

adminパスワードを変更

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。

作業を開始する前に

- 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。

このタスクについて

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を区別します。
- 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してください。
- セキュリティを強化するために、パスワードには15文字以上の英数字を使用し、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に対して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、Unified Managerでタイムアウトを設定できます。

このタスクについて

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できます。

   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

Add/Discoverページで、組織のネットワークで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、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。

詳細はこちら。

- "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を検出する"
- "単一のアレイを検出します"

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。このページから、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、そのステータスを表示し、1つのアレイまたはアレイ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、そのアレイを選択してSystem Managerを起動できます。

詳細はこちら。

- "System Managerにアクセスする際の考慮事項"
- "個々のストレージアレイを管理します"
- "ストレージアレイのステータスを表示します"

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して管理するには、組織のネットワークから管理対象のストレージアレイを検出する必要があります。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を検出しています

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を検出しています

単一のアレイを検出する場合は、ストレージアレイのいずれかのコントローラのIPアドレスを1つ入力すると、そ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、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が必要になります。

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。

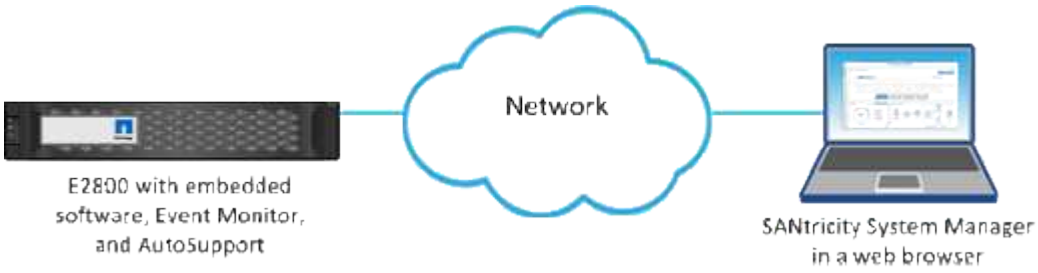
System Managerにアクセスする際の考慮事項

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、Launch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あり、イーサネット管理ポートを介してネットワークに接続されます。アレイベースのすべての関数が含まれています。

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が表示されます。 "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。



アレイを検出します

複数のアレイの検出では、管理サーバが配置されているサブネット全体からすべてのストレージアレイを検出し、検出されたアレイを管理ドメインに自動的に追加します。

作業を開始する前に

- 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。証明書ファイルはローカルシステムにあります。

アレイの検出は、複数の手順からなる手順 です。

手順**1**：ネットワークアドレスを入力します

ローカルの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いて、割り当てられたアドレスが範囲内にあることを確認してください。[新規検出パラメータ *] をクリックして、 [追加 / 検出] ページに戻ります。

4. 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。自己署名証明書は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、*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の問題は、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が確認できないと発生します。アレイの検出プロセスでは、信頼されていない証明書を解決するために、信頼できる第三者機関が発行した認証局（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新たに追加した。
- 一方または両方の証明書の期限が切れている。
- 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表示されます。

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。

完了後

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

Unified Managerから指定のストレージアレイへの接続が確立されるまでに数分かかることがあります。

単一のアレイを検出します

単一ストレージアレイの追加/検出オプションを使用して、ストレージアレイを手動で検出し、組織のネットワークに追加します。

作業を開始する前に

- 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。

   Unified Managerが指定のストレージアレイに接続するまでに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、承認された認証局（CA）の署名がない証明書について、セキュリティ例外を追加して解決するように求められます。

5. 信頼されていない証明書についての確認が求められたら解決し

   信頼されていない証明書の問題は、ストレージアレイから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が確認できないと発生します。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、「すべて」の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。

完了後

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。

アレイを管理します

ストレージアレイのステータスを表示します

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間の接続のステータスを確認できます。

次の表では、ステータスインジケータについて説明します。

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、パスワードが有効です。
パスワードが無効です	無効なストレージアレイパスワードが指定されました。
信頼できない証明書です	HTTPS証明書が自己署名証明書でインポートされていないか、CA署名証明書でルート証明書と中間CA証明書がインポートされていないため、ストレージアレイとの1つ以上の接続が信頼されていません。
要注意	ストレージアレイにユーザによる修正操作が必要な問題があります。
ロックダウン	ストレージアレイがロックダウン状態です。
不明です	ストレージアレイに一度も接続していません。この状況は、Webサービスプロキシ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サービスプロキシの起動後に一度も接続されていない場合に発生することがあります。
オフラインです	Web Services Proxyをストレージアレイに接続しましたが、現在はすべての接続が失われています。

個々のストレージアレイを管理します

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

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を変更する

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ときに使用するパスワードを更新できます。

作業を開始する前に

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

このタスクについて

このタスクでは、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

ストレージアレイをUnified Managerで管理する必要がなくなった場合は、削除することができます。

このタスクについて

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

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

手順

1. [* Manage *（管理）]ページを選択します。

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。

設定をインポートします

設定インポートの概要

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。

どの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。

詳細はこちら。

- "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

ソースとして使用するストレージアレイで、System Managerを開いて目的の設定を行います。その後、Unified Managerの管理ページに移動し、設定を1つ以上のアレイにインポートします。

詳細はこちら。

- "アラート設定をインポートします"
- "AutoSupport 設定をインポートします"
- "ディレクトリサービス設定をインポートします"
- "ストレージ構成の設定をインポートします"
- "システム設定をインポートします"

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、ネットワーク内で複数のアレイを設定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でないシックボリュームのみ）
  - ボリュームグループとプール
  - ホットスペアドライブの割り当て
- 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、要件およびガイドラインを確認してください。

シェルフ

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

コントローラ

- コントローラタイプはソースとターゲットのアレイで同一である必要はない（E2800からE5700にインポートする場合など）が、RBODエンクロージャのタイプは同一である必要がある。

- ホストのDA機能を含むHICが、ソースとターゲットのアレイで同じである必要があります。
- デュプレックス構成からシンプレックス構成へのインポートはサポートされていませんが、シンプレックス構成からデュプレックス構成へのインポートは可能です。
- FDE設定はインポートプロセスに含まれない。

ステータス

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

ストレージ

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

バッチインポートを使用します

アラート設定をインポートします

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

作業を開始する前に

- 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]）。

このタスクについて

インポート処理では、Eメール、SNMP、またはsyslogのいずれかのアラートを選択できます。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'新しい設定を受信するアレイを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や、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ページには、インポート処理の結果が表示されます。処理が失敗した場合は、その行をクリックすると詳細を確認できます。

結果

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

AutoSupport 設定をインポートします

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

作業を開始する前に

- 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]）。

このタスクについて

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

手順

1. [管理]ページで、[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'新しい設定を受信するアレイを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や、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ページには、インポート処理の結果が表示されます。処理が失敗した場合は、その行をクリックすると詳細を確認できます。

結果

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

ディレクトリサービス設定をインポートします

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

作業を開始する前に

- 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]）。

このタスクについて

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

手順

1. [管理]ページで、[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’新しい設定を受信するアレイを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や、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ページには、インポート処理の結果が表示されます。処理が失敗した場合は、その行をクリッ

クすると詳細を確認できます。

結果

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

システム設定をインポートします

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

作業を開始する前に

- 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]）。

このタスクについて

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

手順

1. [管理]ページで、[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’新しい設定を受信するアレイを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や、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ページには、インポート処理の結果が表示されます。処理が失敗した場合は、その行をクリックすると詳細を確認できます。

結果

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

ストレージ構成の設定をインポートします

ストレージアレイから別のストレージアレイにストレージ構成をインポートできます。

このバッチ処理により、ネットワーク内に複数のアレイを設定する必要がある場合に時間を節約できます。

作業を開始する前に

- 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。
  - 拡張シェルフの同一のスロットに同じドライブタイプが搭載されている。
  - RBODエンクロージャタイプが同一である。
  - HICが、ホストのData Assurance機能を含めて同一である。
  - ターゲットアレイのステータスが最適Iである必要があります。
  - ターゲットアレイのボリューム容量がソースアレイよりも大きい。
- 次の制限事項を理解しておきます。
  - デュプレックス構成からシンプレックス構成へのインポートはサポートされていませんが、シンプレックス構成からデュプレックス構成へのインポートは可能です。
  - ソースアレイのディスクプールのボリュームが64TB以上の場合、ターゲットでインポートプロセスを実行できない。
  - シンボリュームはインポートプロセスに含まれません。

このタスクについて

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

手順

1. [管理]ページで、[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’新しい設定を受信するアレイを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や、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ページには、インポート処理の結果が表示されます。処理が失敗した場合は、その行をクリックすると詳細を確認できます。

結果

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

よくある質問です

どの設定がインポートされますか？

設定のインポート機能は、1つのストレージアレイから複数のストレージアレイに構成をロードするバッチ処理です。この処理でインポートされる設定は、System Managerでソースストレージアレイがどのように設定されているかによって異なります。

複数のストレージアレイにインポートできる設定は次のとおりです。

- **Email alerts**--メールサーバのアドレスとアラート受信者の電子メールアドレスを設定します
- **Syslog**アラート-- syslogサーバのアドレスとUDPポートを含む設定。
- *snmp alerts *-- SNMPサーバのコミュニティ名とIPアドレスを含む設定。
- * AutoSupport *--個別の機能（Basic AutoSupport 、AutoSupport OnDemand、Remote Diagnostics）、メンテナンス時間、配信方法、 およびディスパッチスケジュール。
- ディレクトリサービス-- LDAP (Lightweight Directory Access Protocol)サーバーのドメイン名とURL、およびLDAPサーバーのユーザーグループとストレージアレイの定義済みロールとのマッピングが含まれます。
- ストレージ構成--ボリューム(リポジトリボリューム以外のシックボリュームのみ)、ボリュームグループ、プール、およびホットスペアドライブの割り当てが含まれます。
- システム設定--ボリュームのメディアスキャン設定、コントローラのSSDキャッシュ、および自動ロードバランシングが含まれます(ホスト接続レポートは含まれません)。

ストレージアレイが一部表示されないのはなぜですか？

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

ストレージアレイが表示されない理由は次のとおりです。

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

アレイグループ

グループの概要

グループの管理ページでは、一連のストレージアレイグループを作成することで管理を容易にすることができます。

アレイグループとは何ですか？

一連のストレージアレイを1つのグループにまとめて物理インフラや仮想インフラを管理することができます。ストレージアレイをグループ化すると、ジョブの監視やレポートが簡単になります。

グループには次の2つのタイプがあります。

- 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。Allグループには、メインビューからアクセスできます。
- ユーザーが作成したグループ--ユーザーが作成したグループには'手動で選択してそのグループに追加するストレージアレイが含まれますユーザが作成したグループには、メインビューからアクセスできます。

グループを設定するにはどうすればよいですか？

[グループの管理]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。

詳細はこちら。

- "ストレージアレイグループを設定する"

ストレージアレイグループを設定する

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ステップの手順 です。

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では、ボリュームを構成するストレージをどのドライブから提供するかを定義します。

手順

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

手順**2**：ストレージアレイをグループに追加する

ユーザが作成したグループにストレージアレイを追加することができます。

手順

1. メインビューで、* Manage *を選択し、ストレージ・アレイを追加するグループを選択します。

2. 選択メニュー：グループの管理[グループへのストレージアレイの追加]。
3. グループに追加するストレージアレイを選択します。
4. [* 追加] をクリックします。 *

グループからストレージアレイを削除します

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

このタスクについて

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

手順

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

ストレージアレイグループを削除します

不要になった1つ以上のストレージアレイグループを削除することができます。

このタスクについて

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

手順

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

ストレージアレイグループの名前を変更します

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

このタスクについて

これらのガイドラインに注意してください。

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

- わかりやすい一意の名前を使用してください。
- わかりにくい名前は使用しないでください。

手順

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

アップグレード

Upgrade Center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ています。

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（ファイルが格納されているWebサービスプロキシサーバの領域）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. リポジトリにファイルをロードしたら、アップグレードに使用するファイルを選択できます。SANtricity OSソフトウェアのアップグレードページ（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でアップグレードするストレージアレイを選択します。（互換性のないアレイは選択できません）。
4. ソフトウェアの転送とアクティブ化をすぐに開始することも、ファイルをステージングしてあとでアクティブ化することもできます。アップグレードプロセスを実行すると、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の妨げとなる状況がないかどうかが確認されます。健全性チェックでいずれかのアレイに問題が見つかった場合は、そのアレイをスキップして他のアレイのアップグレードを続行するか、プロセス全体を停止して該当するアレイのトラブルシューティングを行うことができます。
   b. 各コントローラにアップグレードファイルが転送されます。

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に通常 15~25 分かかります。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。

ヘルスチェック

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状態であるかがチェックされます。次の状況に該当する場合、アップグレードを実行できないことがあり

- 割り当てられたドライブで障害が発生し
- ホットスペアを使用中です
- 不完全なボリュームグループです
- 同時に実行できません
- 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が多すぎます
- 構成データベースの検証に失敗しました
- ドライブの DACstore のバージョンが古い

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場合は、計画段階で主な考慮事項を確認してください。

現在のバージョン

検出された各ストレージアレイについて、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するように、ホストのマルチパス/フェイルオーバードライバやHBAドライバのアップグレードも必要になることがあります。

互換性の情報については、を参照してください "NetApp Interoperability Matrix を参照してください"。手順については、使用す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、から入手できます "E シリーズおよび SANtricity に関するドキュメント"。

デュアルコントローラ

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

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

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

ソフトウェアとファームウェアをアップグレードします

アップグレード前の健常性チェックを実行

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

手順

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

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

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

   健全性チェックの実行中、ダイアログボックスに進捗状況が表示されます。

5. 健全性チェックが完了したら、各行の右側にある省略記号（ … ）をクリックして、詳細情報を表示した

り他のタスクを実行したりできます。

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

SANtricity OSをアップグレードします

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

作業を開始する前に

- 最新のSANtricity OSファイルは、SANtricity 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あります。
- ソフトウェアのアップグレードをすぐにアクティブ化するかあとでアクティブ化するかを決めます。

  あとでアクティブ化する理由は次のとおりです。

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

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。

このタスクについて

```
[NOTE]
====
データ損失のリスク、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にストレージアレイに対する変更を行わないでください。ストレージアレイの電源は切らないでください。

====
.手順
. ストレージアレイにコントローラが 1
台しかない場合やマルチパスドライバが使用されていない場合は、アプリケーションエラーを回避するためにストレージアレイへの I/O
アクティビティを停止します。ストレージアレイにコントローラが 2
台あり、マルチパスドライバがインストールされている場合は、 I/O
アクティビティを停止する必要はありません。
. 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。
+
SANtricity OS ソフトウェアのアップグレードページが表示されます。

. ネットアップサポートサイトからローカルマシンに最新の SANtricity OS ソフトウェアパッケージをダウンロードします。
+
.. [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 以降のデジタル署名されたファームウェアが必要です。署名のないファームウェアをダウンロードしようとすると、エラーが表示されてダウンロードが中止されます。

====
. 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 サービスプロキシ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。

. [Compatible Storage Array] テーブルで ' 選択した OS

ソフトウェア・ファイルと互換性のあるストレージ・アレイを確認し '
アップグレードするアレイを選択します
+
** [管理]
ビューで選択したストレージ・アレイおよび選択したファームウェア・ファイルと互換性のあるストレージ・アレイは ' デフォルトで [互換性のあるストレージ・アレイ]
テーブルで選択されています
** 選択したファームウェアファイルで更新できないストレージアレイは、ステータス * incompatible * と表示される互換性があるストレージアレイテーブルで選択できません。

. *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、ストレージアレイがリブートされてファイルがアクティブ化されます。

+
アップグレード処理では次の処理が実行されます。

+
**
アップグレードプロセスの一環として、アップグレード前の健常性チェックが実行されます。アップグレード前の健常性チェックでは、ストレージアレイのすべてのコンポーネントについて、アップグレードを実行できる状態であるかがチェックされます。
**
いずれかの健全性チェックでストレージアレイに問題が見つかった場合、アップグレードが停止します。省略符号 (...) 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することができます。

. *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、「upgrade_log-<date>.json」という名前でファイルが保存されます。

[[IDacf01731b13c3b6ce35ebcb8ee89c511]]
= ステージング済みOSソフトウェアをアクティブ化します
: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ただちにアクティブ化することも、都合のいいタイミングでアクティブ化することもできます。この手順では、ソフトウェアファイルをあとでアクティブ化するように選択した場合を想定しています。

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

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

[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、ステータス列をクリックしてページ上部の「OS Upgrade（waiting activation）」というステータスのすべてのストレージアレイをソートします。
. 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、アクティブ化を実行できる状態であるかがチェックされます。
**
いずれかの健全性チェックでストレージアレイに問題が見つかった場合、アクティブ化は停止します。省略符号（...）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することができます。アップグレード前の健常性チェックが正常に完了すると、アクティブ化が実行されます。アクティブ化にかかる時間は、ストレージアレイの構成とアクティブ化しているコンポーネントによって異なります。

. *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 'activate_log-<date>.json
という名前でファイルが保存されます

[[ID10367b2b614eba20614951f2d5238dbe]]
= ソフトウェアリポジトリを管理します
: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

サービスプロキシ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。

.作業を開始する前に
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（ソフトウェアリポジトリの管理）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「N2800-830000-000.dlp」のようになります。

.. 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。削除を選択した場合は、ファイルがソフトウェアリポジトリから削除されます。

[[IDffffe75bef22e3c94f8be83a1925f239]]
= ステージング済みOSソフトウェアをクリアします
: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。
+
Clear Staged OS Software（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、検出されたすべてのストレージシステムの中に保留中のソフトウェアまたはNVSRAMが表示されます。

.
必要に応じて、ストレージシステムのリストをフィルタまたはソートして、ソフトウェアがステージング済みのすべてのシステムを確認します。
. 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


[[ID5d14b1366ed923c16f4fb8e0bbc235eb]]
= 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。

====


== ミラーリングとは何ですか？

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、データボリュームをオンデマンドで、またはスケジュールに基づいてコピーします。これにより、データの破損や損失が原因で発生するダウンタイムを回避または最小限に抑えることができます。同期ミラーリングでは、データボリュームをリアルタイムでレプリケートして、継続的な可用性を確保します。

詳細はこちら。

* 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。
```

詳細はこちら。

```
* 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["非同期ミラーペアを作成する"]
* xref:{relative_path}create-synchronous-mirrored-pair-
um.html["同期ミラーペアを作成する"]
```

= 概念

```
:leveloffset: +1


[[ID86768a719eb0ba7443d092913dca8720]]
```
= 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、データボリュームをオンデマンドで、またはスケジュールに基づいてコピーします。これにより、データの破損や損失が原因で発生するダウンタイムを回避または最小限に抑えることができます。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ったときに送信されます。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、データボリュームをリアルタイムでレプリケートして、継続的な可用性を確保します。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、どの時点においてもコピーは本番環境のデータと同一です。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。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確保に最適です。

== 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、またはユーザ定義のスケジュールに従って自動的に実行されます。
a|
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。

a|
距離（Distance）
a|
アレイ間の長距離をサポートします。通常、この距離は、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い距離に制限されています。レイテンシおよび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。

|===

[[ID835825f4579b7b03a3e540d92f33ca75]]
= 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、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、手動同期とスケジュールされた同期のどちらを実

行するかを指定します。
..
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のみ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、システムでは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、通常の動作を行って同期を維持しようとします。新しいブロックと変更されたブロックのみ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に行われるため、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を確保する必要があります。

====

[[ID5e320821242a1fa46896ff2ac8f1ae1c]]
= 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 | 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、一貫した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。書き込み処理はまずプライマリボリュームに対して実行され、その後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。また、通信が中断されて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ときにも実行されます。通信リンクが再確立されると、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。

|===

[[ID31fd8968c823b2576a919e8b59c6abb7]]
= 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 の略

* 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各コントローラにイーサネット管理ポートが設定されていて、各コントローラが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（それぞれ異なるバージョンのOS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。このポートでは、ミラーリング処理の対象となるコントローラからのI/O要求のみが許可されます。
*
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には、プライマリボリュームと同等以上のサイズが必要です。
* ボリュームに設定できるミラー関係は1つだけです。
*
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、作成済みの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を使用する場合は、プライマリボリュームとセカンダリボリュームでドライブセキュリティ機能が同じでなければなりません。
+
** 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

= ミラーリングを設定します

:leveloffset: +1

[[ID670a4e7e7d9aeb8265c09a74a12e6003]]
= 非同期ミラーペアを作成する
: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。

.作業を開始する前に
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、ストレージアレイとボリュームに関する次の要件を満たしていることも確認してください。

* 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各コントローラにイーサネット管理ポートが設定されていて、各コントローラが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（それぞれ異なるバージョンのOS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には、プライマリボリュームと同等以上のサイズが必要です。

.このタスクについて
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る手順 です。

== 手順1：ミラー整合性グループを作成または選択します

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対して必要な再同期方法（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。整合性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のデータを表す、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、およびアンダースコア（_）、ダッシュ（-）、ハッシュ記号（#）のみです。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、同期間隔を30分に設定し、同期プロセスを午後4時に開始すると、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。
*** 自動同期の場合は、次の3つのアラート方法を設定できます。
同期が特定の時間内に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期限よりも古くなった場合、およびリザーブ容量が特定のしきい値（残りの容量の割合によって定義）に近づいている場合。

. [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
. 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%であり、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。
+
*** ミラーペアを長期にわたって維持する場合。

*** 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
.
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%であり、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。
+
*** ミラーペアを長期にわたって維持する場合。
*** 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で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があるデータの量が削減されます。

[[IDd7fe2b4d9a8b403ba35639d8109aa5d7]]
= 同期ミラーペアを作成する
: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。

====
.作業を開始する前に
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、ストレージアレイとボリュームに関する次の要件を満たしていることも確認してください。

* 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各コントローラにイーサネット管理ポートが設定されていて、各コントローラが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（それぞれ異なるバージョンのOS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ボリュームは使用できません。
* 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ボリュームは使用できません。
* セカンダリボリュームには、プライマリボリュームと同等以上のサイズが必要です。

.このタスクについて
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る手順 です。

== 手順1：プライマリボリュームを選択します

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、対応するストレージアレイ名別に表示されます。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*」をクリックして、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

この手順では、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。

+
このダイアログ環境
で設定した優先度。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。このオプションを選択すると、最適なタイミングでデータをリカバリできます。
** *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で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における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。

.完了後
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

= よくある質問です

:leveloffset: +1

[[ID70b40d547efc15f29041ead006ba555a]]
= 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を満たしていることも確認してください。

* 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各コントローラにイーサネット管理ポートが設定されていて、各コントローラが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（それぞれ異なるバージョンのOS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。

====

[[IDa616b08d2e950249fe2ff102948672b1]]
= 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際は、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各コントローラにイーサネット管理ポートが設定されていて、各コントローラが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（それぞれ異なるバージョンのOS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。

====

[[IDe85414f1993b01aa34145ac911ab6213]]
= この割合を変更するのはどのような場合ですか？
: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、一般に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。

[[IDd325b78b789e058ce8eeedd7e407269d]]
= 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複数のボリュームがある場合は、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、推奨される候補の一覧が更新されます。選択内容に基づいて最適な候補が表示されます。

[[ID5479616c79ffd26080d361781f524566]]
= 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は、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。

[[ID4f647c5e0ba5c76aa68af9a3419240ec]]
= 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、ボリュームが対象外になっている可能性があります。

* ボリュームが、Snapshotボリュームなどの標準以外のボリュームである。
* 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では、プライマリボリュームとセカンダリボリュームの間のシンボリューム属性が一致しません。
* 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を使用する場合は、プライマリボリュームとセカンダリボリュームでドライブセキュリティ機能が同じでなければなりません。
+
** 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。

[[IDe0835e3c97ae891e5661b8a00f34667a]]
= 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、同期アクティビティに割り当てられる処理時間をシステムパフォーマンスと比較して決定します。

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。

優先度は次のとおりです。

* 最低
* 低
* 中
* 高
* 最高

最低ではシステムパフォーマンスが優先されますが、再同期化に時間がかかります。最高では再同期化が優先されますが、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、各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|

最高の優先度であれば、約8倍の時間を要します。

a|
低
a|
最高の優先度であれば、約6回。

a|
中
a|
最高の優先度であれば、約3倍から半分。

a|
高
a|
優先度が最高の場合は、約2倍です。

|===
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。

[[IDb94b2d3de7268dcbe3b90876f5cb07a3]]
= 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


[[IDaf8eee537051591816075bb1d9faa652]]
= 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。



== 証明書とは何ですか？

_証明書_は、Webサイトやサーバなどのオンラインエンティティを識別し、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。

詳細はこちら。

* 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"]



== 証明書の設定方法

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るほか、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。

詳細はこちら。
```

```
* xref:{relative_path}use-ca-signed-certificate-um.html["管理システムの
CA署名証明書を使用します"]
* xref:{relative_path}import-array-certificates-
unified.html["アレイの証明書をインポートします"]




= 概念

:leveloffset: +1


[[ID75906e76fd82bcfa8aed4ff5f4a2f696]]
= 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、指定されたサーバとクライアント間でのみ、Web通信が非公開かつ変更されずに暗号化された形式で送信されます。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、第三者が所有者のIDを検証し、そのデバイスが信頼できると判断したことを意味します。ストレージアレイの各コントローラには、自動生成された自己署名証明書が付属しています。自己署名証明書を引き続き使用することも、CA署名証明書を取得してコントローラとホストシステム間のよりセキュアな接続を確立することもできます。

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

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

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

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

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

== 自己署名証明書

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

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

== 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。

[[ID418fecc86e63ba81aeadc1c1f72d03aa]]
= 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 | 説明

a|
できます
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文書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が証明書の問題 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、その情報について証明（署名）する信頼されたエンティティのIDが含まれます。

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、チェーンの最上位にはルート証明書が1つ、中間証明書が1つ以上、エンティティを識別するサーバ証明書が1つ含まれます。

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を使用する場合は、ルート証明書が1つだけ必要です。

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、サーバとクライアントの間でHTTPS接続を介してデータが暗号化された形式で送信されることが保証されます。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、サーバとクライアントの間でHTTPS接続を介してデータが暗号化された形式で送信されることが保証されます。また、アルファベットと数字で構成されるデジタル署名も含まれます。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

```
[[ID545b5b6ed08b624c003e4f3489f057d8]]
= 管理システムのCA署名証明書を使用します
: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。

.作業を開始する前に
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、証明書の
機能は表示されません。

.このタスクについて
CA署名証明書の使用は、3つの手順で構成される手順 です。



== 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）ファイルを生成する必要があります。これにより、Web Services
ProxyとUnified Managerがインストールされている組織とホストシステムが特定されます。

[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
. [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.などの接尾辞も含めて入力してください
** *組織単位（オプション）*--証明書を処理している組織の部門。
** *市区町村*--ホストシステムまたは事業の所在地である市区町村。
** *都道府県(オプション)*--ホストシステムまたは事業の所在地である都道府県。
** *国のISOコード*--自国を表す2桁のISO（国際標準化機構）コード（USなど）。
```

. 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：//を含めないでください。DNS名の先頭にワイルドカードを使用することはできません。
** *代替IPアドレス*--共通名がIPアドレスの場合は'オプションでホストシステムの追加の
IPアドレスまたはエイリアスを入力できます複数指定する場合は、カンマで区切って入力します。
** *代替DNS名*--共通名がDNS名の場合は'ホストシステムの追加の
DNS名を入力します複数指定する場合は、カンマで区切って入力します。代替DNS名がない場合は、
最初のフィールドに入力したDNS名をここにコピーします。DNS名の先頭にワイルドカードを使用す
ることはできません。

. ホスト情報が正しいことを確認します。証明書が含まれていないと、
CAから返された証明書をインポートしようとしたときに失敗します。
. [完了] をクリックします。
. に進みます <<手順2：CSRファイルを送信する>>。

== 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、Unifie
d ManagerとWebサービスプロキシをホストするシステムの署名付き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、別のCSRファイルを再生成しないでください。*
CSRを生成するたびに、システムは秘密鍵と公開鍵のペアを作成します。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から返された署名済み証明書については、を参照してください <<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）から署名入りの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。

.作業を開始する前に
* 署名済みの証明書を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（たとえば、.p7bファイル）が提供された場合は、チェーンファイルを個々のファイル（ルート証明書、1つ以上の中間証明書、サーバ証明書）に展開する必要があります。Windowsのcertmgrユーティリティーを使用して'ファイルを展開できます(右クリックしてメニューを選択しますすべてのタスク[エクスポート])base-64エンコーディングが推奨されます。エクスポートが完了すると、チェーン内の証明書ファイルごとに1つのCERファイルが表示されます。
* 証明書ファイルを
Webサービスプロキシが実行されているホストシステムに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表示されます。

.
[*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。証明書の情報は、証明書の管理ページに表示されます。

[[ID0a2833c38c24957324d7cdf7b95369df]]
= 管理証明書をリセットします
: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。

.作業を開始する前に
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、証明書の機能は表示されません。

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

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

= アレイ証明書を使用する

:leveloffset: +1

[[ID2054c241387f5ef637da2cc657b6fe61]]
= アレイの証明書をインポートします
: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することができます。証明書には、認証局（CA）が署名した証明書と自己署名の証明書があります。

.作業を開始する前に
* 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、証明書の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のコントローラの証明書をインポートする必要があります。

.手順
. [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。

```
[[IDab73a862abeb0f749ff8f63fdda5798f]]
= 信頼された証明書を削除する
: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。

.作業を開始する前に
古い証明書を削除する前に、新しい証明書をインポートしてください。

[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が共有されている可能性があるため、複数のストレージアレイに影響する可能性があります。

====
.手順
. [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。




[[IDefef0d68993d10b13f3c37de8eaa1eb8]]
= 信頼されていない証明書を
: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の問題は、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が確認できないと発生します。

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

.作業を開始する前に
* 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、次の点に注意してください。
+
** ストレージアレイの各コントローラの証明書署名要求（.CSRファイル）を生成してCAに送信しておく必要があります。
** 信頼された証明書ファイルをCAから受け取っておきます。
** 証明書ファイルがローカルシステム上にある必要があります。




.このタスクについて
信頼された追加のCA証明書のインストールが必要になる可能性があるのは、次のいずれかに該当する場合です。

* ストレージアレイを新たに追加した。
* 一方または両方の証明書の期限が切れている。
* 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

= 証明書を管理します

:leveloffset: +1

[[ID3c320b38fbe2e0c257cdef45c46c8704]]
= 証明書を表示します
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

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

.作業を開始する前に
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、証明書の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。

[[ID66e7b8a842a82d206a3004a690cad3d9]]
= 証明書をエクスポートします
: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。

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

.手順
. [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

[[ID952ca6bc552443c006d8f90684346f15]]
= 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"]
アクセス管理では、Unified Managerでユーザ認証を設定することができます。

== 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。

詳細はこちら。

* 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、[Access Management]ページでLDAPを設定できます。

詳細はこちら。

* 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を設定する"]

= 概念

:leveloffset: +1

[[ID715f56d01c8bf8d17642f7395ca687b7]]
= 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でのユーザ認証を確立する。

== 設定ワークフロー

アクセス管理の設定は次のように行います。

. 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]
====
初めてのログインでは'ユーザ名adminが自動的に表示され'変更することはできませんadminユーザは'システムのすべての機能にフル・アクセスでき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に必要な設定はありません。
** *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(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、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。

. 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。ログイン時には、次のバックグラウンドタスクが実行されます。
+
** ユーザ名とパスワードをユーザアカウントと照合して認証します。
** 割り当てられたロールに基づいてユーザの権限が決まります。
** 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

機能へのアクセスは、ユーザに割り当てられたロールによって次のように異なります。

* * 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、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。

[[ID62a8509d128fffd8429b18c0fba38645]]
= 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 | 説明

a|
Active Directory
a|
Active Directory（AD）は、Windowsドメインネットワーク用のLDAPを使用するMicrosoftのディレクトリサービスです。

a|
結合
a|
バインド処理は、ディレクトリサーバに対するクライアントの認証に使用されます。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|
できます
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文書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、その情報について証明（署名）する信頼されたエンティティのIDが含まれます。

a|
LDAP
a|
Lightweight Directory Access Protocol（
LDAP）は、分散型のディレクトリ情報サービスへのアクセスと管理に使用される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が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、コンピュータやネットワークリソースへのアクセスを個々のユーザのロールに基づいて制御する手法です。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は、ユーザの認証時に複数の項目（パスワードとフィンガープリントなど）を求める多要素認証に対応しています。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の使用方法
 a|
Web Services Proxyは標準の
HTTPSメカニズムによるアクセスを提供するプロキシで、管理者にストレージアレイの管理サービスの設定を許可します。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。

|===

[[ID8cc51aa14b1e6a6f0a3236fd792c2931]]
= 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済みのユーザが含まれています。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。

これらのロールにより、次のタスクへのアクセスが可能になります。

* * 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。

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。

[[ID0bfee05bf2f88914a7af0058df443ef2]]
= 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に組み込みのロールベースアクセス制御（
RBAC）機能を使用できます。これらの機能のことを「ローカルユーザロール」と呼びます。



== 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
する場合、管理者は次の操作を行うことができます。

. 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ユーザは'システムのすべての機能にフル・アクセスできます

====
.
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、変更することは
できません。
. 必要に応じて、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。
* パスワードなしでのログインをユーザに許可します。



[[ID8bde0874c25edfc6b7955c4313cafd97]]
= 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"]
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）を使用して認証を管理することができます。



== 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、設定は次のようになります。

. 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ユーザは'システムのすべての機能にフル・アクセスできます

====
. LDAPサーバの設定を入力します。これには、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、
LDAPサーバとホストシステム（Webサービスプロキシがインストールされているシステム）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たら、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に定義されており、変更できません。
. LDAPサーバとWebサービスプロキシの間の接続をテストします。
. ユーザは各自に割り当てられた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する。
* ディレクトリサーバを削除する。
```

* 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。
* パスワードなしでのログインをユーザに許可します。

[[IDb7ef46e57bba2da2a416a8b8321cb864]]
= 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行います。

. 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ユーザはSystem Managerのすべての機能にフル・アクセスできます

====
. 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間の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、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します
* サービスプロバイダファイルをエクスポート

== 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てログインします

```
:leveloffset: -1


= ローカルユーザロールを使用する

:leveloffset: +1


[[ID826bf2ee72743f9eb85924cb91b74d72]]
= ローカルユーザロールを表示します
: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RBAC（ロールベースアクセス制御）の一部です。

.作業を開始する前に
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。

.このタスクについて
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だけです。

.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ています
** * 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、Securi
```

ty 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。

[[ID1e94cd0b7e2e69e8e445c1aabd5bc9bb]]
= ローカルユーザプロファイルのパスワードを変更します
: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。

.作業を開始する前に
* 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。

.このタスクについて
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（[表示/編集の設定]）以上である必要があります。
* パスワードは大文字と小文字を区別します。
*
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してください。
* セキュリティを強化するために、パスワードには15文字以上の英数字を使用し、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に対して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。

[[IDd6dcf967433a2a296840ab7d2e5b39b8]]
= ローカルユーザパスワードの設定を変更します
: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の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。

.作業を開始する前に
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。

.このタスクについて
ローカルユーザパスワードの最小文字数を設定する際には、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の最小文字数を設定するには、「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選択し、スピンボックスを使用して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、現在の設定以上の長さ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

[[IDc2e1116846c5afd168293bb3e7926855]]
= ディレクトリサーバを追加します
: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。その後、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。

.作業を開始する前に
* 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がローカルマシンにインストールされている必要があります。

.このタスクについて
ディレクトリサーバの追加は、2つのステップで行います。まず、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、認証に使用するCA証明書が標準の署名機関によって署名されていない場合、その証明書もアップロードする必要があります。バインドアカウントのクレデンシャルがある場合は、その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 | 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'ldap[s]://*host*:*port*'の形式で入力します

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、上記のサーバURLフィールドに
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やグループ内の検索で使用する読み取り専用の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」であれば、「CN=bindacct、CN=Users、DC=cpoc、DC=local」などと入力します。

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、バインドアカウントを入力した場合に表示されます。

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します
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オンにした場合、テストに失敗すると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|
ユーザー名属性
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 | 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|
ロール
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選択します。このグループに含めるロールを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。
+
ストレージアレイとLDAPサーバが通信できるかどうかの検証がシステムによって実行されます。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。

[[ID25593f25de1b8cfb9fadcc9383d0955b]]
= ディレクトリサーバ設定とロールマッピングを編集します
: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設定済みの場合は、いつでも設定を変更できます。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。

.作業を開始する前に
* 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が定義されている必要があります。

.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 | 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。形式はです `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やグループ内の検索で使用する読み取り専用のユーザアカウント。

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した場合に表示されます）。

a|
保存する前にサーバ接続をテストします
a|
システムがLDAPサーバの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オンにした場合、テストに失敗すると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|
ユーザー名属性
 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|
グループとロールのマッピングに使用される、ユーザのグループ属性のリスト。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 | 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|
ロール
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。現在のユーザセッションのみが保持されます。

[[IDa86852a9792f763f2241910f764a1da3]]
= ディレクトリサーバを削除します
: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から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て古いサーバを削除する場合などに実行します。

.作業を開始する前に
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。

.このタスクについて
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「remove」と入力し、「* Remove *」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、このサーバから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を使用する

:leveloffset: +1


[[ID2f5fd85366d390964a9ed71c339c9dbd]]
= SAMLを設定する
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]
アクセス管理の認証を設定する場合、ストレージアレイに組み込みのSecurity Assertion Markup Language（
SAML）機能を使用することができます。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。

.作業を開始する前に
* 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。

.このタスクについて
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。多要素認証にも対応し、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を設定すると、ストレージアレイが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。その後、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。あとでSAMLを無効にすると、元の設定に戻ってディレクトリサービスが使用されます。

====
[CAUTION]
====
* SAMLを編集および無効化しています。*
SAMLを有効にすると、ユーザインターフェイスで無効にすることはできず、IdP設定を編集することもできません。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からなる手順 です。

== 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。
+
アイデンティティプロバイダファイルのインポート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ために、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、コントローラのドメイン名やIPアドレスなど、IdPがサービスプロバイダと通信するために必要な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。
+
[Export Service Provider Files]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。ファイルの保存先をメモします。

. 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。

.作業を開始する前に
* 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 | 説明

a|
マッピング

a|
ユーザー属性
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ます。正規表現パターンの一部でない場合は、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|
ロール
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選択します。追加するロールを1つずつ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。また、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、*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。

.作業を開始する前に
* 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表示されます。

. 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。
+
ログインのテストを実行している間、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い場合は、エラーメッセージに詳細が表示されます。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、前の手順で説明したとおりです。

.作業を開始する前に
* 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]
====
* SAMLを編集および無効化しています。*
SAMLを有効にすると、ユーザインターフェイスで無効にすることはできず、IdP設定を編集することもできません。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。
+
[Confirm Enable SAML（SAMLを有効にする）]ダイアログボックスが開きます。

. 「enable」と入力し、「* Enable」をクリックします。
. SSOログインのテスト用に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。

[[ID31a4f4c5c65c71fd9d4783d1843b9857]]
= SAMLのロールマッピングを変更する
:allow-uri-read:
:experimental:
:icons: font

```
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
アクセス管理にSAMLを設定している場合、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との間のロールマッピングを変更できます。

.作業を開始する前に
* 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 | 説明


 a|
*マッピング*
```

a|
ユーザー属性
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|
ロール
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選択します。このグループに含めるロールを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。現在のユーザセッションのみが保持されます。

[[ID15d663e72b071934db0f626159086d24]]
= SAMLサービスプロバイダファイルをエクスポートする
: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。

.作業を開始する前に
* 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。

.このタスクについて
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。
+
[Export Service Provider Files]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。

```
====
+
ファイルの保存先をメモします。

. 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


= よくある質問です

:leveloffset: +1


[[ID3c3123972db4339096d5dcf22860963c]]
= 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"]
ログイン試行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。
* 必要な権限がありません。
* ログインが複数回失敗したために、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。
* SAML認証が有効になりました。ログインするには、ブラウザをリフレッシュしてください。




[[IDb1d6039dd885fd7d1ad89a603228a8b4]]
= 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がローカルマシンにインストールされている必要があります。




[[IDb6ba99e85494df227eaecaaa6eff6b5e]]
=
ストレージアレイのロールを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。

* ディレクトリサービスでユーザグループを定義しておきます。
* 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を確認しておきます。正規表現がサポートされます。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。

[[ID650dad5784c537fb2af887196db93968]]
= SAMLを設定および有効にするときは、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

作業を開始する前に、次の点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く必要があります。
* 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。
* 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おく必要があります。

* 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。（SSOログインテストはSAMLが有効になる前にシステムでも実行されます）。
* 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、ディレクトリサービス、またはその両方）が自動的にリストアされます。
* 現在ユーザ認証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を設定すると、次のクライアントがストレージアレイリソースにアクセスできなくなります。
+
** 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てログインします

```
[[ID3dc7de11f74f74b56bcd0a980b15816b]]
= 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たユーザで、特定の権限が含まれています。

ローカルユーザの例を次に示します。

* *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てい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、Securi
ty 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


[[ID7b6bca62b837b821736a793ccbe7300e]]
= 以前のバージョン
:allow-uri-read:
:icons: font
:relative_path: ./
:imagesdir: {root_path}{relative_path}./media/


[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"^]
*
https://library.netapp.com/ecm/ecm_download_file/ECMLP2589397["コントローラアップグレードガイド-レガシーコントローラモデル"^]
```

== 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11.8

* https://docs.netapp.com/us-en/e-series-santricity-118/index.html["System Managerのヘルプ"^]
* https://docs.netapp.com/us-en/e-series-santricity-118/index.html["Unified Managerのヘルプ"^]

=== 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）ヘルプ"^]
* https://mysupport.netapp.com/ecm/ecm_get_file/ECMLP2862588["EMW（E2700
、E5600 / EF560）のヘルプ"^]




[[ID7df3e36f743b6f3a12b8e4343a6da20a]]
= 法的通知
:hardbreaks:
:allow-uri-read:
:icons: font
:linkattrs:
:relative_path: ./
:imagesdir: {root_path}{relative_path}./media/


[role="lead lead"]
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。その他の会社名および製品名は、それぞれの所有者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

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

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/ECMLP3334467["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