SANtricity ソフトウェア11.9のドキュメント

SANtricity software

NetApp
March 17, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/e-series-santricity-119/index.html on March 17, 2026. Always check docs.netapp.com for the latest.

目次

SANtricity ソフトウェア11.9のドキュメント 1
リリース ノート 2
SANtricity OS 11.90の新機能 2
Version 11.90R5の新機能 2
Version 11.90R4の新機能 2
Version 11.90R3の新機能 2
Version 11.90R2の新機能 2
Version 11.90R1の新機能 2
バージョン11.90の新機能 3
リリース ノート 3
はじめに 4
SANtricityソフトウェアについて学ぶ 4
SANtricity System Manager 4
SANtricity Unified Manager 5
SANtricity ソフトウェアブラウザとオペレーティングシステムのサポート 7
ブラウザ 7
オペレーティング システム 8
SANtricity System Managerのセットアップ 8
SANtricity System Managerにアクセスする 8
SANtricity System Managerセットアップウィザードについて学ぶ 9
SANtricity System Managerのストレージシステム設定に関するよくある質問 11
SANtricity Unified Manager のセットアップ 12
SANtricity Unified Managerのインストール 12
SANtricity Unified Managerにアクセスします 13
SANtricity System Manager 11.9による単一アレイ管理 14
メイン画面 14
SANtricity System Managerインターフェイスについて学ぶ 14
パフォーマンス データの表示 15
SANtricity System Managerでストレージ階層を表示する 24
インターフェイス設定の管理 26
通知の管理 29
SANtricity System Managerの管理インターフェースに関するよくある質問 33
プールとボリューム グループ 37
SANtricity System Managerのプールとボリューム グループについて学ぶ 37
概念 38
ストレージを設定する 46
ストレージの管理 60
プール / グループ設定の変更 66
SSDキャッシュの管理 75

リザーブ容量の管理 82
プールとボリュームグループに関するよくある質問 SANtricity System Manager 92
ボリュームとワークロード 105
SANtricity System Managerのボリュームとワークロードについて学ぶ 105
概念 106
ストレージを設定する 124
ボリュームの管理 136
設定の管理 141
コピー サービスの使用 151
SANtricity System ManagerのボリュームとワークロードのFAQ 158
ホストとホスト クラスタ 163
SANtricity ソフトウェアのホストとホストクラスタについて学ぶ 163
概念 164
ホスト アクセスの設定 168
ホストとクラスタの管理 172
設定の管理 175
SANtricity System Managerのホスト システムとホスト クラスタに関するよくある質問 178
Snapshot 数 182
SANtricity System Managerのスナップショットについて学ぶ 182
概念 183
SnapshotおよびSnapshotオブジェクトの作成 194
Snapshotスケジュールの管理 207
Snapshotイメージの管理 210
Snapshot整合性グループの管理 215
Snapshotボリュームの管理 219
SANtricity System Managerのスナップショットに関するよくある質問 225
ミラーリング 227
概要 227
非同期の概念 229
同期の概念 240
非同期ミラー整合性グループの管理 249
非同期ミラー ペアの管理 255
同期ミラー ペアの管理 259
ミラーリングの非アクティブ化 263
SANtricity System Managerの非同期ミラーリングに関するよくある質問 264
SANtricity System Managerの同期ミラーリングに関するよくある質問 270
リモート ストレージ 273
SANtricity System Managerのリモート ストレージ機能について説明します 273
概念 274
リモート ストレージの管理 278
SANtricity System Managerのリモート ストレージに関するよくある質問 282

ハードウェア コンポーネント 285
SANtricity System Managerでハードウェアコンポーネントを表示および管理する 285
関連情報 286
概念 286
シェルフ コンポーネントの管理 296
コントローラの管理 301
iSCSIポートの管理 313
NVMeポートの管理 325
ドライブの管理 329
ホット スペアの管理 342
SANtricity System ManagerのStorage shelfに関するFAQ 345
SANtricity System Managerのストレージコントローラに関するFAQ 348
iSCSI プロトコルに関する FAQ（SANtricity System Manager） 351
SANtricity System ManagerのNVMeプロトコルに関するよくある質問 354
SANtricity System Managerのストレージ ドライブに関するFAQ 356
アラート 357
SANtricity System Managerのアラートについて学ぶ 357
概念 357
Eメール アラートの管理 359
SNMPアラートの管理 363
syslogアラートの管理 370
SANtricity System Managerのストレージシステムアラートに関するよくある質問 372
アレイ設定 373
SANtricity System Managerの設定の概要について説明します 373
概念 373
アレイの設定 376
アドオン機能の設定 383
SANtricityコマンドラインインターフェース（CLI）をダウンロード 386
SANtricity System Managerのストレージ アレイ設定に関するよくある質問 387
ドライブ セキュリティ 389
SANtricity System Managerのドライブセキュリティについて学ぶ 389
概念 390
セキュリティ キーの設定 395
セキュリティ キーの管理 399
SANtricity System Managerのストレージドライブセキュリティに関するFAQ 406
アクセス管理 410
SANtricity System Managerのアクセス管理について学ぶ 410
概念 411
ローカル ユーザ ロールの使用 418
ディレクトリ サービスの使用 420
SAMLの使用 430

アクセス トークンの使用 437
syslogの管理 439
SANtricity System Managerのユーザアクセス管理に関するFAQ 445
証明書 449
SANtricity System Managerの証明書について学ぶ 449
概念 450
証明書の使用 452
CA署名証明書と自己署名証明書に関するよくある質問SANtricity System Manager 461
サポート 462
SANtricity System Managerでサポートを受ける 462
情報と診断の表示 463
診断データの収集 467
リカバリ操作の実行 471
AutoSupportの管理 473
イベントの表示 480
アップグレードの管理 483
AutoSupport に関するよくある質問（FAQ） SANtricity System Manager 用 495
SANtricity Unified Manager 7による複数のアレイ管理 502
メイン画面 502
SANtricity Unified Managerについて学ぶ 502
SANtricity Unified Managerでサポートされるブラウザ 503
SANtricity Unified Managerの管理者パスワード保護について学ぶ 503
SANtricity Unified Managerで管理者パスワードを変更する 504
SANtricity Unified Managerでセッションタイムアウトを管理する 505
ストレージ アレイ 505
SANtricity Unified Managerでの検出について学ぶ 505
概念 506
アレイの検出 507
アレイの管理 511
設定のインポート 513
SANtricity Unified Managerでのストレージアレイ設定のインポートについて説明します 513
概念 513
バッチ インポートの使用 515
SANtricity Unified Managerのインポート設定に関するよくある質問 520
アレイ グループ 521
SANtricity Unified ManagerのGroupsの概要について説明します 521
SANtricity Unified Managerでストレージアレイグループを設定する 521
SANtricity Unified Managerのグループからストレージアレイを削除する 522
SANtricity Unified Manager でストレージアレイグループを削除する 522
SANtricity Unified Managerでストレージアレイグループの名前を変更する 522
アップグレード 523

SANtricity Unified ManagerのUpgrade Centerについて学ぶ 523
ソフトウェアとファームウェアのアップグレード 525
ミラーリング 530
SANtricity Unified Managerでのミラーリングについて学ぶ 530
概念 531
ミラーリングの設定 537
SANtricity Unified Managerのストレージミラーリングに関するよくある質問 544
証明書 547
証明書の概要 547
概念 548
管理システムのCA署名証明書の使用 550
管理証明書のリセット 552
アレイ証明書の使用 553
証明書の管理 555
アクセス管理 556
SANtricity Unified Managerのアクセス管理について学ぶ 556
概念 557
ローカル ユーザ ロールの使用 562
ディレクトリ サービスの使用 565
SAMLの使用 574
SANtricity Unified Managerのユーザアクセス管理に関するFAQ 581
以前のバージョン 585
以前のリリースのハードウェア ドキュメント 585
以前のリリースのソフトウェア ドキュメント 585
SANtricityリリース11.8 585
SANtricityリリース11.7 585
SANtricityリリース11.6 585
SANtricityリリース11.5 585
SANtricityリリース11.4 586
法律上の表示 587
著作権 587
商標 587
特許 587
プライバシー ポリシー 587
オープンソース 587

SANtricity ソフトウェア11.9のドキュメント

リリース ノート

SANtricity OS 11.90の新機能

SANtricity System Manager 11.9の新機能を次の表で説明します。

Version 11.90R5の新機能

このバージョンには欠陥の修正のみが含まれ、新しい機能は含まれていません。このリリースの変更点の詳細については、Eシリーズ SANtricity OS 11.90R5 READMEを参照してください。

Version 11.90R4の新機能

このバージョンにはマイナーな変更のみが含まれており、新しい機能は含まれていません。このリリースの変更点の詳細については、Eシリーズ SANtricity OS 11.90R4 READMEを参照してください。

Version 11.90R3の新機能

新機能	概要
IOM12CおよびDCM3のSANtricity OSサポート	コントローラファームウェア11.90R3以降では、IOM12CおよびDCM3 SAS-3シェルフのサポートが利用可能になりました。IOM12CおよびDCM3シェルフは、IOM12BおよびDCM2シェルフの後継機種です。

Version 11.90R2の新機能

このバージョンには軽微な変更のみが含まれており、新機能は追加されていません。このリリースの変更点の詳細については、 "Eシリーズ 11.90 リリースノート"を参照してください。

Version 11.90R1の新機能

新機能	概要
新しいストレージ システム モデル – EF300CおよびEF600C	今回のリリースでは、EF300CおよびEF600Cというオールフラッシュ NVMeストレージシステムを紹介します。EF300CとEF600Cは、既存のEF300およびEF600ストレージシステムの大容量フラッシュバージョンです。EF300CおよびEF600Cは、30TBまたは60TBサイズの大容量NVMe SSDドライブに対応しています。EF300C/EF600Cは、ダイナミックディスクプールでの使用のみに対応しており、従来のRAIDには対応していません。
EF4000の12Gb SASインターフェースのサポート	E4000コントローラは12Gb SASホスト インターフェイス カードをサポートするようになりました。

バージョン**11.90**の新機能

新機能	概要
新しいストレージ システム モデル – E4000	このリリースでは、低コストストレージシステムE4000が導入されました。E4000は、12台および60台のドライブと、コントローラあたり1枚のホスト インターフェイス カード（HIC）をサポートしています。初回リリースでは、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が含まれます。E4000ストレージシステムおよびその他の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 Poolの容量増加	ダイナミック ディスク プール（DDP）の容量は、プール内の個々のドライブの容量が23TBを超える場合、12PBに増加されました。個々のドライブの容量が23TB未満の場合、DDPの容量は6PBとなります。
デフォルトのメディアスキャン設定が増加しました	デフォルトのメディアスキャン間隔が120日に延長されました。
外部キー管理でプライベートキーが使用可能になりました	秘密鍵と公開鍵のペアを使用して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が利用可能になりました	REST APIを介してのみ設定可能で、組み込み型およびプロキシ型Webサービス向けに、新しいログインロックアウト設定が利用可能になりました。

リリース ノート

リリース ノートはこのサイトでは公開されていません。NetApp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ソフトウェアについて学ぶ

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。

ここでは、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/EF600CおよびEF300/EF300Cストレージアレイは、同期ミラーリングまたはシンボリュームをサポートしていません。

SANtricity System Manager

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は、次のような各種管理機能を提供します。

パフォーマンス

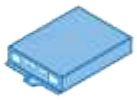
I/Oレイテンシ、IOPS、CPU使用率、スループットなどのパフォーマンス データを最大30日分表示します。

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します。

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 リカバリを実行します。



ハードウェア

コンポーネントのステータスをチェックし、コンポーネントに関連する機能（ホット スペア ドライブの割り当てなど）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。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

その他のシステム パフォーマンス機能（SSDキャッシュや自動ロード バランシングなど）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 アレイの健全性を監視してテクニカル サポートに自動ディスパッチを送信するAutoSupportを設定します。

SANtricity Unified Manager

Unified Managerは、ドメイン全体を管理するために使用するWebベースのソフトウェアです。中央ビューから、E4000、E2800、EF280、EF300、E5700、EF570、EF600、EF300C、EF600Cなど、すべての新しいEシリーズおよびEFシリーズアレイのステータスを確認できます。選択したストレージアレイに対してバッチ

操作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は、次のような各種管理機能を提供します。

ストレージアレイを検出
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。単一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。
起動
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。
インポート設定
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。

SANtricity ソフトウェアブラウザとオペレーティングシステムのサポート

SANtricityソフトウェアは、複数のブラウザとオペレーティング システムをサポートしています。

ブラウザ

サポートされるブラウザとバージョンを次に示します。

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

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

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	2016、2019、2022 / 64ビット
Ubuntu	18.04、20.04 / 64ビット

SANtricity System Managerのセットアップ

SANtricity System Managerにアクセスする

SANtricity 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 ウィザードを使用すると、システム構成を簡単に開始できます。

開始する前に

- 次のいずれかのエクスプレス構成ガイドの説明に従って、ハードウェアを設置して設定します。
  - "Linuxの簡単な設定"
  - "VMwareの簡単な設定"
  - "Windowsの簡単な設定"
- 次の要件を満たす管理ステーションを設定します。
  - 1Gbps以上のネットワークに接続されていること。
  - 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。
  - データ管理に使用されるホスト（I/O接続済み）ではなく、独立したステーションとして使用されます。
  - アウトオブバンド管理用にセットアップします。ストレージ管理ステーションは、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を送信します。
  - 対応ブラウザで設定してください。"サポートされるブラウザとオペレーティング システム"を参照してください。

手順

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

   `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。

まだ設定していないアレイでSystem Managerを初めて開くと、[管理者パスワードの設定]という画面が表示されます。

2. 管理者ロールのSystem Managerパスワードを「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。

   初回ログイン時にはセットアップ 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を確認する — 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タイプを確認します。
   - プールを受け入れる — エクスプレスインストール方法に推奨されるプール構成を受け入れます。プールとは、ドライブを論理的にグループ化したものです。
   - アラートの設定 — ストレージアレイに問題が発生した場合に、System Managerが自動的に通知を受け取れるようにします。
   - **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通知を送信します。

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

SANtricity System Managerセットアップウィザードについて学ぶ

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

初回セットアップ

System Managerを初めて開くと、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、ストレージアレイの名前付け、ホストの設定、アプリケーションの選択、ストレージプールの作成など、基本的な設定タスクを実行するように促されます。

> ⓘ 初期設定を続行する前に、アップグレードセンター（メニュー：サポート[アップグレードセンター]）にアクセスして、SANtricity OS ソフトウェアが最新の状態であることを確認してください。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てください。詳細については、"アップグレード センターの概要"を参照してください。

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。System Managerを開くかブラウザを更新し、次の条件の_少なくとも1つ_が満たされると、ウィザードが自動的に再起動します：

- プールおよびボリューム グループは検出されませんでした。
- ワークロードは検出されませんでした。
- 通知は設定されていません。

用語

セットアップ ウィザードでは、次の用語を使用します。

期間	概要
Application	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全性を監視し、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	ホストとは、ストレージアレイ上のボリュームにI/Oを送信するサーバーのことです。
オブジェクト	オブジェクトとは、論理的または物理的な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、ボリュームが含まれます。物理的なオブジェクトには、ストレージアレイ、アレイコントローラ、ホスト、およびドライブが含まれます。
プール	プールは、論理的にグループ化されたドライブの集まりです。プールを使用して、ホストからアクセスできるボリュームを作成できます（ボリュームはプールまたはボリューム グループから作成します）。
Volume	ボリュームとは、アプリケーション、データベース、ファイルシステムなどがデータを保存するコンテナのことです。これは、ホストがストレージアレイ上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で使用可能な容量から作成されます。ボリュームには、定義された容量があります。ボリュームは複数のドライブで構成される場合がありますが、ホストに対しては1つの論理コンポーネントとして表示されます。
ボリューム グループ	ボリュームグループとは、共通の特性を持つボリュームを格納するコンテナのことです。ボリュームグループには、定義された容量とRAIDレベルがあります。ボリュームグループを使用すると、ホストからアクセス可能な1つまたは複数のボリュームを作成できます。（ボリュームは、ボリュームグループまたはプールから作成します。）

期間	概要
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。ワークロード（インスタンス）はアプリケーションごとに1つ以上定義できます。一部のアプリケーションについては、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。

SANtricity System Managerのストレージシステム設定に関するよくある質問

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

一部のハードウェア コンポーネントが表示されない場合はどうすればよいですか?

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

すべてのドライブ シェルフが正しく接続されていることを確認します。互換性のあるドライブ シェルフが不明な場合は、テクニカル サポートに連絡してください。

すべてのホストが表示されない場合はどうすればよいですか?

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

ホストは、セットアップの完了後に設定できます。ホストは、次の方法で手動で作成することができます。

- メニューの「ストレージ」→「ホスト」に移動すると、ホストを手動で作成し、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。手動で作成されたホストも、*初期設定*ウィザードに表示されます。
- 自動検出が機能するためには、ターゲットとホストにホスト ポート タイプ（iSCSIやNVMe over RoCEなど）が設定されており、ストレージへのセッションが確立されている必要があります。

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

アプリケーションを特定すると、SANtricity System Managerは、アプリケーションの種類に基づいてストレージを最適化するボリューム構成を自動的に推奨します。

アプリケーションごとにボリュームを最適化することで、データストレージの運用効率を向上させることができます。ボリューム構成には、I/Oタイプ、セグメントサイズ、コントローラの所有権、読み取りおよび書き込みキャッシュなどの特性が含まれます。さらに、アプリケーション別およびワークロード別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/sを評価できます。

ワークロードとは何ですか?

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

ワークロードは、アプリケーションをサポートするストレージ オブジェクトです。ワークロード（インスタンス）はアプリケーションごとに1つ以上定義できます。一部のアプリケーションについては、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。

ボリュームを作成する際には、ワークロードの用途に関連するオプションを設定する必要があります。たとえば、Microsoft Exchange用のボリュームを作成する場合は、必要なメールボックスの数、メールボックスに必要とされる平均容量、およびデータベースのコピーをいくつ作成するかについて設定します。この情報に基づいてボリュームの構成が最適化されます。この構成は、必要に応じて編集することもできます。

AutoSupportの配信方法を設定するにはどうすればよいですか？

AutoSupport配信方法の設定タスクにアクセスするには、メニュー：Support[Support Center]に移動し、*AutoSupport*タブをクリックします。

以下のプロトコルがサポートされています：HTTPSおよびSMTP。

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。

次の質問に基づいて、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答えが「はい」の場合は、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。

SANtricity System Managerで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。

ホストは、セットアップの完了後に設定できます。ホストは、次の方法で手動で作成することができます。

- メニューの「ストレージ」→「ホスト」に移動すると、ホストを手動で作成し、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。手動で作成されたホストも、*初期設定*ウィザードに表示されます。
- 自動検出が機能するためには、ターゲットとホストにホスト ポート タイプ（iSCSIやNVMe over RoCEなど）が設定されており、ストレージへのセッションが確立されている必要があります。

SANtricity Unified Manager のセットアップ

SANtricity Unified Managerのインストール

SANtricity Unified ManagerはWeb Services Proxyに付属しており、これはホストシステ

ムに別途インストールされるRESTful APIサーバーで、NetApp Eシリーズストレージシステムの管理を行うために使用されます。

Web Services ProxyとUnified Managerをインストールするには、EシリーズおよびSANtricityの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の確認"
2. "Web Services Proxyファイルのダウンロードとインストール"

SANtricity Unified Managerにアクセスします

Webサービスプロキシをインストールしたら、SANtricity 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。

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

手順

1. ブラウザを開いて次のURLを入力します。

   ```
   http[s]://<server>:<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ーの IPアドレスまたはFQDNを表し、 `<port>`はリスニングポート番号を表します（HTTPの場合はデフォルトで8080 、HTTPSの場合は8443）。

   Unified Managerのログイン ページが開きます。

2. 初回ログインの場合は、ユーザー名に `admin`を入力し、次に管理者ユーザーのパスワードを設定して確認してください。

   パスワードに指定できる文字数は最大30文字です。

ユーザーとパスワードに関する詳細については、"アクセス管理の仕組み"を参照してください。

SANtricity System Manager 11.9による単一アレイ管理

メイン画面

SANtricity System Managerインターフェイスについて学ぶ

SANtricity System Managerは、単一のビューでストレージアレイを管理できるWebベースのインターフェイスです。

[ホーム]ページ

[ホーム]ページでは、ダッシュボード ビューでストレージ アレイの日常的な管理を行えます。System Managerにログインすると、[ホーム]ページが最初の画面として表示されます。

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 アレイの状態および健常性に関する重要な情報が表示されます。概要領域から詳細情報を検索できます。

領域	概要
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。さらに、このポートレットには、ストレージ環境の他の領域に影響する前に問題のトラブルシューティングに役立つ自動アラートが表示されます。
パフォーマンス	[パフォーマンス]領域では、リソース使用量の推移を比較できます。応答時間（IOPS）、転送速度（MiB/秒）、使用中の処理能力（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、未割り当てのストレージ容量がグラフで表示されます。
ストレージ階層	[ストレージ階層]領域には、ストレージ アレイによって管理されているさまざまなハードウェア コンポーネントおよびストレージ 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、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。

画面設定

メイン画面から表示設定やその他の設定を変更できます。

設定	概要
表示設定	画面右上にある[環境設定]ドロップダウンから容量と期間を変更できます。

設定	概要
セッション タイムアウト	一定の期間非アクティブなユーザ セッションを切断するようにタイムアウトを設定できます。
ヘルプ	画面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

システムに現在ログインしているユーザが画面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、以下を参照してください。

- "管理者パスワード保護の設定"
- "パスワードの変更"

パフォーマンス データの表示

SANtricity System Managerのパフォーマンスの概要について説明します

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

パフォーマンス データから何がわかりますか**?**

[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。

詳細については、以下を参照してください。

- "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。

詳細については、以下を参照してください。

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

SANtricity System Managerのパフォーマンス グラフとガイドラインについて説明します

[パフォーマンス]ページに表示されるデータのグラフや表を使用すると、いくつかの主要

領域におけるストレージ アレイのパフォーマンスを評価できます。

パフォーマンス機能を使用すると、以下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判断する。
- 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、期間を選択する。
- 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 グラフィカル — パフォーマンス データをほぼリアルタイムでグラフにプロットします。
- ニアリアルタイム表形式 — パフォーマンス データをほぼリアルタイムで表形式で表示します。
- 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カンマ区切り値のファイルに保存して、後で表示および分析することができます。

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	表示される時間の長さ	表示されるオブジェクトの最大数	データを保存する機能
リアルタイムのグラフ、ライブ リアルタイムのグラフ、履歴	10秒（ライブ） 5分（履歴） 表示されるデータポイントは選択した期間によって異なる	デフォルトは1時間。 選択肢： • 5分 • 1時間 • 8 時間 • 1日 • 7日間 • 30日間	5	いいえ
ほぼリアルタイムの表	10秒～1時間	最新の値	無制限	はい
カンマ区切り値（CSV）ファイル	選択した期間によって異なる	選択した期間によって異なる	無制限	はい

パフォーマンス データの表示に関するガイドライン

- パフォーマンス データの収集は常にオンです。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。その他すべての期間は5分ごとのサンプリングで、選択した期間の平均が算出されます。
- グラフ表示のパフォーマンス 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、障害が発生する可能性もあります。

SANtricity ソフトウェアのパフォーマンス用語について学ぶ

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	概要
Application	アプリケーションとは、SQLやExchangeなどのソフトウェア プログラムです。
CPU	CPUは、Central Pocessing Unit（中央処理装置）の略です。ストレージ アレイの処理能力のうち使用中の割合を示します。
ホスト	ホストとは、ストレージアレイ上のボリュームにI/Oを送信するサーバーのことです。
IOPS	IOPSは、1秒あたりの入出力操作数を表します。
レイテンシ	レイテンシとは、読み取りコマンドや書き込みコマンドなどの要求から、ホストまたはストレージ アレイからの応答までの時間間隔のことです。
LUN	論理ユニット番号（LUN）とは、ホストがボリュームにアクセスするために使用するアドレス空間に割り当てられた番号のことです。ボリュームは、LUNの形式で容量としてホストに提示されます。 各ホストには独自のLUNアドレス スペースがあります。そのため、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mebibyte（mega binary byte）の略語です。1 MiBは220、つまり1,048,576バイトです。MB（10進数を表す）と比較してください。1 MBは1,024バイトに相当します。
オブジェクト	オブジェクトとは、論理的または物理的な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。

期間	概要
プール	プールは、論理的にグループ化されたドライブの集まりです。プールを使用して、ホストからアクセスできるボリュームを作成できます（ボリュームはプールまたはボリューム グループから作成します）。
読み取り	Readは「read operation（読み取り操作）」の略で、ホストがストレージアレイからデータを要求したときに発生します。
Volume	ボリュームとは、アプリケーション、データベース、ファイルシステムなどがデータを保存するコンテナのことです。これは、ホストがストレージアレイ上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で使用可能な容量から作成されます。ボリュームには、定義された容量があります。ボリュームは複数のドライブで構成される場合がありますが、ホストに対しては1つの論理コンポーネントとして表示されます。
ボリューム名	ボリューム名とは、ボリュームが作成された際に割り当てられる文字列のことです。デフォルトの名前を受け入れるか、ボリュームに保存されているデータの種類を示す、より分かりやすい名前を指定できます。
ボリューム グループ	ボリュームグループとは、共通の特性を持つボリュームを格納するコンテナのことです。ボリュームグループには、定義された容量とRAIDレベルがあります。ボリュームグループを使用すると、ホストからアクセス可能な1つまたは複数のボリュームを作成できます。（ボリュームは、ボリュームグループまたはプールから作成します。）
ワークロード	ワークロードは、アプリケーションをサポートするストレージ オブジェクトです。ワークロード（インスタンス）はアプリケーションごとに1つ以上定義できます。一部のアプリケーションについては、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」とは「書き込み操作」の略で、ホストからアレイにデータが送信され、保存される操作を指します。

SANtricity System Managerでグラフィカルなパフォーマンスデータを表示する

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

タスク概要

パフォーマンスグラフには、履歴データと現在取得中のライブデータが表示されます。グラフ上の「ライブ更新」とラベル付けされた垂直線は、履歴データとライブデータを区別します。

ホームページビュー

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とプールごと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、ボリュームが含まれます。
- 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、および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の種類とワークロードごとにグループ化された論理オブジェクト（ボリューム）のリストを表示します。

手順

1. ホーム 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]のいずれかのボタンをクリックします。
3. 詳細を表示するには、**View Performance Details** をクリックしてください。
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ビュー*タブを選択します。

   オブジェクト タイプに応じて異なるグラフが各タブに表示されます。

タブを表示	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	• **Storage array**：IOPS、MiB/s • プール：レイテンシ、IOPS、MiB/s • ボリュームグループ：レイテンシ、IOPS、MiB/s • ボリューム：レイテンシ、IOPS、MiB/s
物理ビュー	• **Controllers**：IOPS、MiB/s、CPU、Headroom • ホストチャネル：レイテンシ、IOPS、MiB/s、ヘッドルーム • ドライブチャネル：レイテンシ、IOPS、MiB/s • ドライブ：レイテンシ、IOPS、MiB/s
アプリケーションとワークロード ビュー	• **Storage array**：IOPS、MiB/s • **Applications**：レイテンシ、IOPS、MiB/s • ワークロード：レイテンシ、IOPS、MiB/s • ボリューム：レイテンシ、IOPS、MiB/s

5. オプションを使用して、必要なオブジェクトと情報を表示します。

   オプション

オブジェクトを表示するためのオプション	概要
ドロワーを展開してオブジェクトのリストを表示する。	_ナビゲーションドロワー_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ています。 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する。	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する。	[フィルタ]ボックスに、オブジェクトの名前または名前の一部を入力して、それらのオブジェクトだけをドロワーに表示します。
オブジェクトを選択した後、*グラフを更新*をクリックします。	引き出しからオブジェクトを選択した後、*グラフを更新*を選択すると、選択したアイテムのグラフデータが表示されます。
グラフの表示と非表示を切り替える。	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	概要
期間	表示する期間（5分、1時間、8時間、1日、7日、30日）を選択します。デフォルトは1時間です。 30日間のパフォーマンス データ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、期間の表示を縮小できます。ズーム バーを広げるほど、グラフの粒度が低下します。 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。

SANtricity System Managerで表形式のパフォーマンスデータを表示および保存

パフォーマンス グラフのデータを表形式で表示および保存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、*Launch table view*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、表に含める列を選択します。

   各チェック ボックスを使用して、項目を選択または選択解除できます。

4. 画面下部の*エクスポート*を選択すると、表形式のビューがカンマ区切り値（CSV）ファイルとして保存されます。

   「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数とエクスポートする

ファイル形式（カンマ区切り値、またはCSV形式）が表示されます。

5. ダウンロードに進むには **Export** をクリックし、キャンセルするには **Cancel** をクリックしてください。

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

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

SANtricity System Managerでパフォーマンス 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。次の表で、考慮が必要な主な要素について説明します。

パフォーマンス データ	パフォーマンス チューニングへの影響
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。 • 1個のボリューム 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、ディスク上の場所の移動にかかる時間は短くなります。 • ドライブの数が少なすぎると、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、システムの全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、レイテンシも大きくなります。 • レイテンシの値が高い場合、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のドライブのほうが、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大きくなります。 • 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 チューニングへの影響
IOPS	1秒あたりの入力 / 出力処理（IOPSまたはIO/秒）に影響する要因には、以下の項目があります。 • アクセス パターン（ランダムまたはシーケンシャル） • I/Oサイズ • RAIDレベル • キャッシュ ブロック サイズ • 読み取りキャッシュが有効かどうか • 書き込みキャッシュが有効かどうか • 動的キャッシュ読み取りプリフェッチ • セグメント サイズ • ボリューム グループまたはストレージ アレイ内のドライブ数 キャッシュ ヒット率が高いほど、I/O速度も高くなります。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なはずです。I/Oパターンにかかわらず、書き込みキャッシュを有効にして、I/O速度を最大限にし、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。実際に試しながら最適なセグメント 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/s	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。一般的には、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、応答時間が短縮されます。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。 アプリケーションの通常の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転送速度を特定する際に役立ちます。

パフォーマンス データ	パフォーマンス チューニングへの影響
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、あるコントローラの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る場合があります。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場合があります。ストレージ アレイを追加することにより、許容可能なパフォーマンス 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、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限の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。

SANtricity System Managerでストレージ階層を表示する

メイン画面の[ストレージ階層]には、ストレージ アレイによって管理されているさまざまなハードウェア コンポーネントおよびストレージ 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	概要
コントローラ	コントローラは、基板、ファームウェア、および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	概要
シェルフ	シェルフは、キャビネットまたはラックに取り付けられるエンクロージャです。ストレージ アレイのハードウェア コンポーネントがシェルフに格納されます。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。 異なるタイプのメディアまたは異なるタイプのインターフェイスがストレージ アレイに含まれている場合は、ドライブのタイプごとにドライブ シェルフが表示されます。
ドライブ	ドライブは、データの物理ストレージ メディアとして使用される電磁的な機械デバイスまたはソリッド ステート メモリ デバイスです。
ホスト	ホストとは、ストレージアレイ上のボリュームにI/Oを送信するサーバーのことです。
ホスト バス アダプタ（HBA）	ホスト バス アダプタ（HBA）はホストに設置されるボードで、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	管理クライアントとは、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るコンピュータのことです。

論理コンポーネント

ストレージ アレイ内のドライブは、データ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、物理容量を複数の論理コンポーネント（プール、ボリューム グループ、ボリュームなど）に分散します。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	概要
プール	プールは、論理的にグループ化されたドライブの集まりです。プールを使用して、ホストからアクセスできるボリュームを作成できます（ボリュームはプールまたはボリューム グループから作成します）。
ボリューム グループ	ボリュームグループとは、共通の特性を持つボリュームを格納するコンテナのことです。ボリュームグループには、定義された容量とRAIDレベルがあります。ボリュームグループを使用すると、ホストからアクセス可能な1つまたは複数のボリュームを作成できます。（ボリュームは、ボリュームグループまたはプールから作成します。）

コンポーネント	概要
Volume	ボリュームとは、アプリケーション、データベース、ファイルシステムなどがデータを保存するコンテナのことです。これは、ホストがストレージアレイ上のストレージにアクセスするために作成される論理コンポーネントです。
論理ユニット番号（LUN）	論理ユニット番号（LUN）とは、ホストがボリュームにアクセスするために使用するアドレス空間に割り当てられた番号のことです。ボリュームは、LUNの形式で容量としてホストに提示されます。 各ホストには独自のLUNアドレス スペースがあります。そのため、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。

インターフェイス設定の管理

SANtricity System Managerでパスワード保護を管理する

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。

パスワードの設定と変更

System Managerを初めて起動すると、管理者パスワードを設定するように求められます。管理者パスワードを持つユーザーは誰でも、ストレージアレイに対して、オブジェクトや設定の追加、変更、削除などの構成変更を行うことができます。初期起動時に管理者パスワードを設定するには、"System Managerへのアクセス"を参照してください。

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、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。

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

セッション タイムアウト後のパスワードの再入力

システムは、1回の管理セッション中にパスワードの入力を一度だけ求めます。ただし、30分間操作がないとセッションはタイムアウトし、その時点でパスワードを再度入力する必要があります。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ーが、セッション中にパスワードを変更した場合、次回構成操作または表示操作を実行しようとしたときにパスワードの入力を求められます。

セッション タイムアウトは、調整したり無効にしたりすることができます。"セッション タイムアウトの管理"を参照してください。

ドライブの取り外しとパスワード保護の削除

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保護を無効にする場合は、次の点に注意してください。

- パスワード保護付きのドライブを取り外す場合 — パスワードは、ストレージアレイ上の各ドライブの予約領域に保存されます。ストレージアレイからすべてのドライブを取り外すと、そのパスワードは機能しなくなります。この問題を解決するには、元のドライブのいずれかをストレージアレイに再取り付けしてください。
- 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したい場合は、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は空白のままにしてください。

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

SANtricity System Managerで容量値のデフォルト単位を設定します

SANtricity System Managerは、容量値をギビバイト（GiB）またはテビバイト（TiB）のいずれかで表示できます。

設定はブラウザのローカルストレージに保存されるため、すべてのユーザーがそれぞれ独自の設定を持つことができます。

手順

1. メニューの「Preferences」→「Set preferences」を選択してください。
2. *Gibibytes*または*Tebibytes*のいずれかのラジオボタンをクリックし、操作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	**Value**
GiB	$1,024^3$ バイト
TiB	$1,024^4$ バイト

SANtricity System Managerでパフォーマンスグラフのデフォルトの時間枠を設定する

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。

タスク概要

ホームページと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は、初期状態では1時間の時間枠を示しています。設定はブラウザのローカルストレージに保存されるため、すべてのユーザーがそれぞれ独自の設定を持つことができます。

手順

1. メニューの「Preferences」→「Set preferences」を選択してください。
2. ドロップダウンリストから、**5 minutes**、**1 hour**、**8 hours**、**1 day**、または*7 days*のいずれかを選択し、操作を実行することを確認します。

SANtricity System Managerでログインバナーを設定

SANtricity System Managerでセッションを確立する前に、ユーザ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、注意喚起の通知と同意メッセージを含めることができます。

タスク概要

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：Settings[System]を選択します。
2. 「一般」セクションで、**Configure Login Banner** を選択します。

   ログインバナーの設定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。

   書式設定用のHTMLタグやその他のマークアップ タグは使用しないでください。

4. *保存*をクリックします。

結果

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

SANtricity System Managerでセッションタイムアウトを管理

SANtricity System Managerでタイムアウトを設定して、ユーザの非アクティブなセッションが指定された時間の経過後に切断されるようにすることができます。

タスク概要

System Managerのセッションタイムアウトは、デフォルトでは30分です。その時間を調整することも、セッションタイムアウトを完全に無効にすることもできます。

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が構成されている場合、ユーザのSSOセッションが最大制限に達すると、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セッションタイムアウトの前に発生する可能性があります。

手順

1. メニュー：Settings[System]を選択します。
2. 「一般」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. スピン ボックスを使用して時間（分単位）を増減します。

   System Managerに設定できる最小タイムアウト時間は15分です。

セッションタイムアウトを無効にするには、*時間の長さを設定する…*チェックボックスの選択を解除します。

4. *保存*をクリックします。

通知の管理

SANtricity System Managerの問題通知について学ぶ

SANtricity System Managerは、アイコンや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発生してい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。

アイコン	概要
	最適
	最適ではない、または障害発生
	対応または修正が必要
	注意

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

- [ホーム]ページの通知領域に障害アイコンとメッセージが表示されます。
- ナビゲーション領域のホーム ページ アイコンに障害アイコンが表示されます。
- [コンポーネント]ページでは、ドライブおよびコントローラの図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 マニュアルを参照し、障害のあるコンポーネントを交換します。

SANtricity System Managerで進行中の処理を表示して操作します

長時間の処理を表示して、その処理に対する操作を実行するには、[実行中の処理]ページを使用します。

タスク概要

[実行中の処理]ページに表示される処理ごとに、進捗状況と完了までの推定残り時間が表示されます。場合によっては、処理を停止したり、処理の優先度を変更したりできます。完了したボリューム コピー処理をリストから消去することもできます。

手順

1. ホーム画面で、*進行中の操作を表示*を選択します。

   「進行中の作業」ページが表示されます。

2. 必要に応じて、[操作]列のリンクを使用して、処理の停止または優先度の変更を行います。

   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. ボリュームコピー操作が完了したら、*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、操作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、進行中の操作ページから操作をクリアできるリンクが含まれています。

[実行中の処理]ページに表示される処理には、次のものがあります。

処理	処理のステータス	対処方法
ボリューム コピー	完了	クリア
ボリューム コピー	実行中	• 優先度の変更 • 終了
ボリューム コピー	保留中	クリア
ボリューム コピー	失敗	• クリア • 再コピー
ボリューム コピー	停止	• クリア • 再コピー
ボリュームの作成（64TiBを超えるシック プール ボリュームのみ）	実行中	*none*
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	*none*
非同期ミラー グループの初期同期	実行中	中断

処理	処理のステータス	対処方法
非同期ミラー グループの初期同期	中断	再開
同期ミラーリング	実行中	中断
同期ミラーリング	中断	再開
Snapshotイメージのロールバック	実行中	キャンセル
Snapshotイメージのロールバック	保留中	キャンセル
Snapshotイメージのロールバック	一時停止	• キャンセル • 再開
ドライブの退避	実行中	キャンセル（ドライブの退避タイプによる）
プールまたはボリューム グループへの容量の追加	実行中	*none*
ボリュームのRAIDレベルの変更	実行中	*none*
プールの容量削減	実行中	*none*
シン ボリュームの再生	実行中	*none*
プール ボリュームのInstant Availability Format（IAF）処理の残り時間の確認	実行中	*none*
ボリューム グループのデータ冗長性チェック	実行中	*none*
ボリューム グループのデフラグ	実行中	*none*
ボリュームの初期化	実行中	*none*
ボリュームの容量増加	実行中	*none*
ボリュームのセグメント サイズ変更	実行中	*none*
ドライブ コピー	実行中	*none*

処理	処理のステータス	対処方法
データ再構築	実行中	*none*
コピーバック	実行中	*none*
ドライブ消去	実行中	*none*
リモート ストレージ インポート	実行中	• 優先度の変更 • 終了
リモート ストレージ インポート	停止	• 再開 • 接続解除
リモート ストレージ インポート	失敗	• 再開 • 接続解除
リモート ストレージ インポート	完了	接続解除

SANtricity System Manager Recovery Guruを使用して問題から回復する

Recovery GuruはSANtricity System Managerのコンポーネントで、ストレージアレイの問題を診断し、問題を解決するための復旧手順を推奨します。

手順

1. ホーム を選択します。
2. ウィンドウの中央上部にある*Recover from *n* problems*というラベルの付いたリンクをクリックしてください。

   [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、リカバリ手順の指示に従って問題を修正します。必要に応じて、交換手順を使用して障害のあるコンポーネントを交換します。リストにある問題ごとに、この手順を繰り返します。

   ストレージ アレイ内の複数の問題が相互に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る順序に従って、問題を選択して修正してください。

   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. 復旧手順が正常に完了したことを確認するには、*Recheck*をクリックしてください。

   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関する問題を選択した場合は、まず*クリア*をクリックしてコントローラから障害をクリアし、次に*再確認*をクリックしてRecovery Guruから

イベントを削除してください。

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進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。

   ファイルは、ブラウザのダウンロードフォルダに次の名前で保存されます `recovery-guru-failure-yyyy-mm-dd-hh-mm-ss-mmm.html`。

6. Recovery Guruの情報を印刷するには、*Print*アイコンをクリックしてください。

SANtricity System Managerの管理インターフェースに関するよくある質問

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

どのようなブラウザがサポートされますか?

SANtricity System Managerは、以下のブラウザバージョンをサポートしています。

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

キーボードだけを使ってSANtricity System Managerを操作できます。

基本的な操作

アクション	キーボードショートカット
次の項目に移動する。	タブ
前の項目に移動する。	Shift＋Tab
項目を選択する。	入力
ドロップダウン リスト - 次の項目または前の項目に移動する。	下矢印または上矢印
チェック ボックス - 項目を選択する。	スペースキー

アクション	キーボードショートカット
ラジオ ボタン - 項目を切り替える。	下矢印または上矢印
拡張可能なテキスト - 項目を展開する、または折りたたむ。	入力

表での操作

アクション	キーボードショートカット
行を選択する。	Tabキーを押して行を選択し、Enterキーを押す
上方向または下方向にスクロールする。	下矢印 / 上矢印またはPage Down / Page Up
列のソート順序を変更する。	Tabキーを押して列見出しを選択し、Enterキーを押す

カレンダーでの操作

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。	Page Up
次の月に移動する。	Page Down
前の年に移動する。	Control＋Page Up
次の年に移動する。	Ctrl + Page Down
日付ピッカーを開く（閉じている場合）。	Control＋Home
現在の月に移動する。	Ctrl / Command + Home
前の日に移動する。	Ctrl / Command + 左矢印
次の日に移動する。	Ctrl / Command + 右矢印
前の週に移動する。	Ctrl / Command + 上矢印
次の週に移動する。	Ctrl / Command + 下矢印
フォーカスした日付を選択する。	入力

アクション	キーボードショートカット
日付ピッカーを閉じて日付を消去する。	Ctrl / Command + End
選択を行わずに日付ピッカーを閉じる。	Esc

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**?**

プールおよびボリューム 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「**0**」（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。

その場合もオブジェクトの履歴データは表示可能です。オブジェクトのI/Oアクティビティが発生し次第、ゼロ以外のデータが表示されます。

次の表に、各種オブジェクトについて、データ ポイント値がゼロになる最も一般的な理由を記載します。

配列レベルのオブジェクトタイプ	理由データがゼロとして表示される
Volume	• 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 グループにはホストに割り当てられているボリュームが含まれておらず、*かつ*ボリューム グループには予約済みの容量も含まれていません。
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になっている。 • 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。

配列レベルのオブジェクトタイプ	理由データがゼロとして表示される
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ない。

[レイテンシ**]**グラフには何が表示されますか**?**

レイテンシーグラフは、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、ワークロードごとのレイテンシー統計情報をミリ秒（ms）単位で表示します。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 ビュー]の各タブに表示されます。

レイテンシーとは、データの読み書き時に発生するあらゆる遅延を指します。グラフ上の任意の点にカーソルを合わせると、その時点における以下の値がミリ秒（ms）単位で表示されます：

- 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グラフは、1秒あたりの入出力操作数の統計情報を表示します。ホームページでは、このグラフにストレージアレイの統計情報が表示されます。パフォーマンスタイルの[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ビュー]タブでは、このグラフ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、ワークロードの統計情報が表示されます。

IOPSは「1秒あたりの入出力（I/O）操作数」の略です。グラフ上の任意の点にカーソルを合わせると、その時点における以下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/sグラフは、転送速度の統計情報を1秒あたりのメビバイト単位で表示します。ホームページでは、このグラフにストレージアレイの統計情報が表示されます。パフォーマンス タイルの[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 ビュー]タブでは、このグラフにストレージ 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、ワークロードの統計情報が表示されます。

MiB/sは_mebibytes per second_の略で、1秒あたり1,048,576バイトを意味します。グラフ上の任意の点にカーソルを合わせると、その時点における以下の値が表示されます：

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

[CPU]グラフには何が表示されますか**?**

CPUグラフは、各コントローラ（コントローラAとコントローラB）の処理能力統計を表示します。CPUは_central processing unit_の略です。ホームページでは、このグラフにストレージアレイの統計情報が表示されます。パフォーマンス タイルの [物理ビュー] タブでは、このグラフにストレージ アレイとドライブの統計情報が表示されます。

[CPU]グラフには、アレイでの処理に使用中のCPU処理能力の割合が示されます。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存性能能力に関連しています。このグラフは、ホームページと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 システムの物理オブジェクトの残りのパフォーマンス容量が示されます。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は以下で確認できます。

- 容量値の表示に使用されるデフォルトの単位の詳細については、"容量値のデフォルトの単位の設定"を参照してください。
- パフォーマンスグラフを表示するデフォルトの時間枠の詳細については、"パフォーマンス グラフのデフォルト期間の設定"を参照してください。

プールとボリューム グループ

SANtricity System Managerのプールとボリューム グループについて学ぶ

ストレージ アレイ内の未割り当ての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 グループとして作成できます。

プールおよびボリューム グループとは何ですか**?**

_プール_とは、論理的にグループ化されたドライブの集合のことです。_ボリューム グループ_とは、共通の特性を持つボリュームを格納するコンテナです。ホストからアクセス可能なボリュームを作成するには、プールまたはボリューム グループのいずれかを使用できます。

詳細については、以下を参照してください。

- "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"

プールを作成するにはどうすればよいですか?

System Managerがストレージアレイ内で未割り当ての容量を検出した際に、プールを自動的に作成するように設定できます。あるいは、自動作成で最適な構成を判断できない場合は、メニューの「Storage」→「Pools & Volume Groups」から手動でプールを作成できます。

詳細については、以下を参照してください。

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

ボリューム グループを作成するにはどうすればよいですか?

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

詳細については、以下を参照してください。

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

関連情報

プールとボリューム グループに関連する概念の詳細については、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

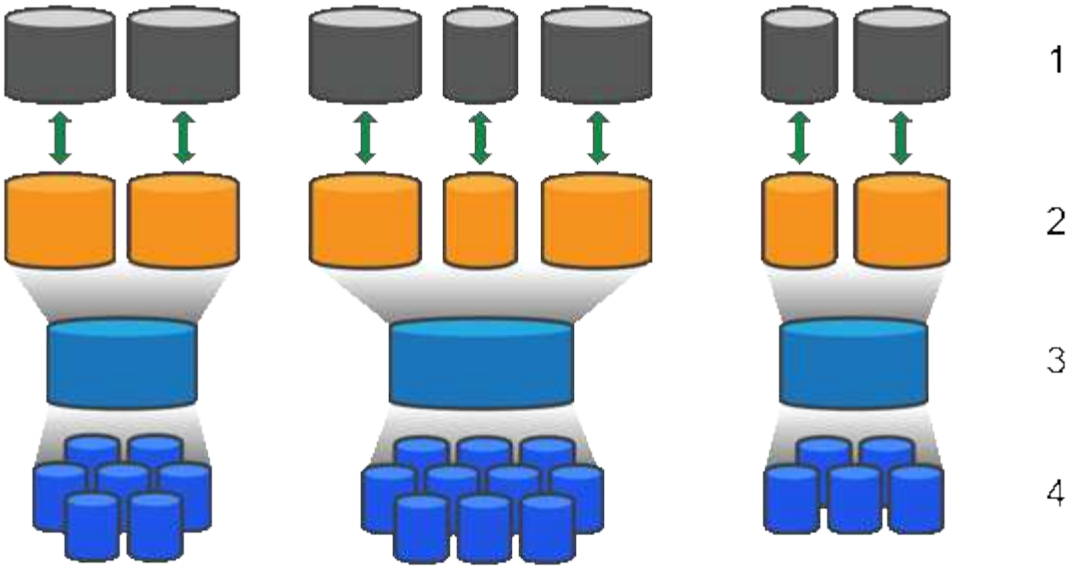
プールとボリューム グループの仕組み（**SANtricity** ソフトウェア）

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、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、データの格納先である個々のボリュームまたはLUNがあります。次の図で、この概念を説明します。



[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。

- 十分な容量を備えたプールまたはボリューム グループを作成
- 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
- 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、複数の物理ハード ディスク ドライブを1つの大きいストレージ 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により、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。

プールは別のRAIDレベルとして機能し、基盤となるRAIDアーキテクチャを仮想化することで、再構築、ドライブ拡張、ドライブ障害への対応といったタスクを実行する際のパフォーマンスと柔軟性を最適化します。System Managerは、8+2構成（データディスク8台とパリティディスク2台）の場合、RAIDレベルを自動的に6に設定します。

ドライブの一致

プールにはHDDまたはSSDの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、選択したドライブ タイプに対して十分な数のドライブを確保する必要があります。

障害ドライブの管理

プールには最低11ドライブの容量がありますが、1ドライブ分の容量は、ドライブ障害が発生した場合のスペア容量として予約されています。このスペア容量は「保存容量」と呼ばれます。

プールが作成されると、一定の容量が緊急用に保持されます。System Managerではこの容量がドライブ数として表されますが、実際にはドライブのプール全体に分散されます。予約済み容量のデフォルトは、プール内のドライブ数に基づきます。

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、実際に使用可能な容量はこれより小さい場合もあります。

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場合、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。

ドライブの一致

ボリューム グループ内のドライブのサイズとパフォーマンスを一致させる必要があります。ボリューム グループ内のドライブの容量が異なる場合、すべてのドライブが最小容量の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 アレイ内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。

SANtricity ソフトウェアの容量に関する用語について学ぶ

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。

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	概要
ホスト	ホストとは、ストレージアレイ上のボリュームにI/Oを送信するサーバーのことです。
LUN	論理ユニット番号（LUN）とは、ホストがボリュームにアクセスするために使用するアドレス空間に割り当てられた番号のことです。ボリュームは、LUNの形式で容量としてホストに提示されます。 各ホストには独自のLUNアドレス スペースがあります。そのため、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を格納するコンテナです。非同期ミラーリング操作を行うには、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ドライブの集まりです。プールを使用して、ホストからアクセスできるボリュームを作成できます（ボリュームはプールまたはボリューム グループから作成します）。
Snapshot整合性グループ	スナップショット整合性グループとは、スナップショットイメージを作成する際に単一のエンティティとして扱われるボリュームの集合です。これらの各ボリュームにはそれぞれ独自のスナップショットイメージがありますが、すべてのイメージは同じ時点で作成されます。
Snapshot グループ	スナップショットグループとは、単一のベースボリュームから抽出されたスナップショットイメージの集合です。
Snapshot ボリューム	スナップショットボリュームを使用すると、ホストはスナップショットイメージ内のデータにアクセスできます。スナップショットボリュームには独自の予約容量があり、ベースボリュームへの変更を元のスナップショットイメージに影響を与えることなく保存します。
Volume	ボリュームとは、アプリケーション、データベース、ファイルシステムなどがデータを保存するコンテナのことです。これは、ホストがストレージアレイ上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とは、共通の特性を持つボリュームを格納するコンテナのことです。ボリュームグループには、定義された容量とRAIDレベルがあります。ボリュームグループを使用すると、ホストからアクセス可能な1つまたは複数のボリュームを作成できます。（ボリュームは、ボリュームグループまたはプールから作成します。）

ストレージ容量

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

容量タイプ	概要
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。 割り当てられた容量は、ボリュームの作成やコピー サービス操作に使用されます。
空き容量	空き容量とは、プールまたはボリュームグループ内で、ボリューム作成やコピーサービス操作、ストレージオブジェクトにまだ割り当てられていない容量のことです。
プールまたはボリューム グループ容量	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、ボリュームの作成のほか、コピー サービス処理やストレージ オブジェクトのさまざまな容量ニーズに対処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とは、ドライブのサイズが一致しないために使用できないプール内のスペースのことです。
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	報告容量とは、ホストに報告され、ホストがアクセスできる容量のことです。
リザーブ容量	予約容量とは、あらゆるコピーサービス操作およびストレージオブジェクトに使用される、物理的に割り当てられた容量のことです。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 Cacheは、ストレージアレイ内で論理的にグループ化されるSolid-State Disk（SSD）ドライブのセットのことです。SSD Cache機能は、最も頻繁にアクセスされるデータ（「ホット」データ）を低遅延のSSDドライブにキャッシュすることで、アプリケーションのワークロードを動的に高速化します。
未割り当て容量	未割り当て容量とは、ストレージアレイ内で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*領域のことです。
書き込み済み容量	書き込み容量とは、シンボリューム用に割り当てられた予約容量のうち、実際に書き込まれた容量のことです。

SANtricity ソフトウェアのプールとボリュームグループについて説明します

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、およびデータ保護要件によって異なります。

プール / ボリューム グループの選択基準

プールを選択

- 迅速なドライブのリビルドやストレージ管理の簡易化が必要な場合、シン ボリュームが必要な場合、大量のランダム ワークロードを処理する場合。
- 各ボリュームのデータをプールを構成する一連のドライブにランダムに分散する場合。

  プールまたはプールに含まれるボリュームのRAIDレベルは設定または変更できません。プールではRAID 6を使用します。

- ボリュームグループを選択してください *
- システムの帯域幅を最大限に使用する場合、ストレージの設定を調整する必要がある場合、大量のシーケンシャル ワークロードを処理する場合。
- 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で、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 グループの機能比較

次の表に、ボリューム グループとプールの機能の比較を示します。

使用	プール	ボリューム グループ
ランダム ワークロード	より良い	良い
シーケンシャル ワークロード	良い	より良い
ドライブ リビルド時間	速い	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より良い	劣る：パフォーマンスが最大40%低下
複数のドライブ障害	データ保護の強化：より迅速で優先順位の高い再構築	データ保護の低下：再構築の遅延、データ損失リスクの増加
ドライブの追加	速い：オンザフライでプールに追加	遅い：Dynamic Capacity Expansion処理が必要

使用	プール	ボリューム グループ
シン ボリュームのサポート	はい	いいえ
ソリッド ステート ディスク（SSD）のサポート	はい	はい
シンプルな管理	○：ホット スペアやRAID設定の構成作業なし	×：ホット スペアを割り当てRAIDを管理
パフォーマンス調整	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、ホストがアクセスできる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レベルのサポート	×（System ManagerではRAID 6のみ）	はい。RAID 0、1、10、5、6が利用可能です。
シン ボリュームのサポート	はい	いいえ
Full Disk Encryption（FDE）のサポート	はい	はい
Data Assurance（DA）のサポート	はい	はい
シェルフ損失の保護のサポート	はい	はい
ドロワー損失の保護のサポート	はい	はい
ドライブ速度混在のサポート	同じ容量が推奨されるが、必須ではない。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。	同じ容量が推奨されるが、必須ではない。一番低速のドライブにすべてのドライブの速度が合わせられます。
ドライブ容量混在のサポート	同じ容量が推奨されるが、必須ではない。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。	同じ容量が推奨されるが、必須ではない。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る。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3本。RAID 6の最小数は5本。
最大ドライブ数	ストレージ アレイの上限まで	RAID 1および10はストレージ アレイの上限、RAID 5、6は30本
ボリューム作成時に個々のドライブを選択可能	いいえ	はい
ボリューム作成時にセグメント サイズを指定可能	はい。128Kに対応しています。	はい
ボリューム作成時にI/O特性を指定可能	いいえ	はい。ファイルシステム、データベース、マルチメディア、およびカスタムがサポートされています。
ドライブ障害保護	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。再構築はドライブのIOPによって制限されます。
容量制限に到達したときの警告	はい。使用容量が最大容量の一定割合に達した際にアラートを設定できます。	いいえ
別のストレージ アレイへの移行のサポート	×（まずボリューム グループに移行する必要がある）	はい
動的セグメント サイズ（DSS）	いいえ	はい
RAIDレベルを変更可能	いいえ	はい
ボリュームの拡張（容量の拡大）	はい	はい
容量の拡張（容量の追加）	はい	はい
容量の縮小	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。

SANtricity System Managerでの自動プール作成と手動プール作成について説明します

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。プールの作成時には、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 アレイ内で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た場合は、プールを作成するか、または未割り当て容量を既存のプールに追加するか（あるいはその両方を行うか）を確認するメッセージがSystem Managerによって自動的に表示されます。

プールの自動作成は、次のいずれかの条件に該当する場合に行われます。

- ストレージアレイ内にプールは存在せず、新しいプールを作成するのに十分な数の類似ドライブが存在します。
- 少なくとも1つのプールを含むストレージ アレイに新しいドライブが追加される。

プール内の各ドライブは、タイプ（HDDまたはSSD）が同じであり、同等の容量を備えている必要があります。次のタスクを実行するよう求めるメッセージがSystem Managerに表示されます。

- 同じタイプの十分な数のドライブがある場合は、1つのプールを作成する。
- 未割り当て容量が異なるドライブ タイプのドライブ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既にプールが定義されている場合は、ドライブを既存のプールに追加し、同じドライブタイプの新しいドライブをプールに追加します。
- 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

自動作成では最適な構成を判断できない場合は、プールを手動で作成することをお勧めします。このような状況は、以下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る。
- 新たに選定されたプール候補のうち1つ以上は、シェルフ損失の保護またはドロワー損失の保護を利用できます。
- 1つ以上の現在のプールの候補で、シェルフ損失の保護またはドロワー損失の保護のステータスを維持できない。

ストレージアレイ上に複数のアプリケーションがあり、それらが同じドライブリソースを競合しないようにしたい場合は、手動でプールを作成することもできます。この場合、1つまたは複数のアプリケーション用に、より小さなプールを手動で作成することを検討してもよいでしょう。ワークロードを、データを分散させるための多数のボリュームを持つ大規模なプールに割り当てる代わりに、1つまたは2つ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プールを手動で作成することで、ストレージアレイの操作をより迅速に、競合を少なく実行できるようになります。

ストレージを設定する

SANtricity System Manager でプールを自動的に作成します

プールの作成は、SANtricityシステムマネージャがストレージアレイ内の未割り当てドライブを検出すると自動的に開始されます。自動プール作成機能を使用すると、ストレージアレイ内の未割り当てドライブをすべて簡単に1つのプールに構成したり、既存のプールにドライブを追加したりできます。

開始する前に

[プールの自動構成]ダイアログ ボックスは、次のいずれかの条件に該当する場合に開くことができます。

- 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。
- 新しいプールを作成するため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）。

タスク概要

次の事項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、そのドライブがSystem Managerで自動的に検出され、ドライブ タイプと現在の構成に基づいて、1つまたは複数のプールを作成するように求められます。
- プールがすでに定義されている場合は、互換性があるドライブを既存のプールに追加するオプションが提示されます。新しいドライブを既存のプールに追加すると、追加した新しいドライブを含めた新しい容量にデータが自動的に再分配されます。
- EF600またはEF300ストレージ アレイを構成する際は、各コントローラが最初の12個のスロットと最後の12個のスロットそれぞれで同じ数のドライブにアクセスできるようにします。この構成により、コントローラがドライブ側の両方のPCIeバスをより効果的に使用できるようになります。

プール自動構成ダイアログボックスは、以下のいずれかの方法で起動できます：

- 割り当てられていない容量が検出されると、ホームページの通知領域にプール自動構成の推奨事項が表示されます。**View Pool Auto-Configuration** をクリックしてダイアログボックスを開きます。
- 次の手順で説明するように、「プールとボリュームグループ」ページから「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。

手順

1. メニュー：Storage[Pools & Volume Groups]を選択します。
2. メニューの「その他」→「プールの自動構成を起動」を選択します。

   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、単一のプールを作成する。
   - 未割り当て容量が異なるドライブ タイプのドライブ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、追加した新しいドライブのドライブ タイプが既存のプールと同じであれば、そのプールにドライブを追加する。

◦ 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。

3. 新しいプールの名前を変更するには、*編集*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 **Details** アイコン（ページ）の上に置くか、タップしてください。

   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 プロビジョニングとボリュームのブロック サイズについての設定も表示されます。

5. * Accept * をクリックします。

SANtricity System Manager でプールを手動で作成する

プール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、（候補のセットから）手動でプールを作成できます。

プールは、アプリケーションをホストするために使用できる個別のボリュームを作成するために必要な論理ストレージ容量を提供します。

開始する前に

- ドライブ タイプ（HDDまたはSSD）が同じドライブが少なくとも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台のドライブ 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 アレイを構成する際は、各コントローラが最初の12個のスロットと最後の12個のスロットそれぞれで同じ数のドライブにアクセスできるようにします。この構成により、コントローラがドライブ側の両方のPCIeバスをより効果的に使用できるようになります。現在、System Managerでは、ボリューム グループの作成時にドライブを選択するには、[アドバンスト]機能を使用します。プールを作成する場合、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. メニュー：Storage[Pools & Volume Groups]を選択します。
2. メニューの Create [Pool] をクリックします。

   [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種類のドライブがある場合は、使用するドライブの種類を選択してください。

   作成可能なすべてのプールの候補が表示されます。

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

特性	使用
空き容量	プール候補の空き容量（GiB）を示します。アプリケーションのストレージ ニーズに応じて、必要な容量のプール候補を選択します。 プールには予約済み（スペア）容量も含まれますが、これは空き容量には含まれません。
合計ドライブ数	プール候補に含まれるドライブの数を示します。 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）を示します。値は次のとおりです。 • 512 - 512バイト 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。 • Drive Securityを使用すればプールを保護できますが、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専用のプールを作成する場合は、「セキュア対応」列で*はい - FDE*を探してください。FIPS専用のプールを作成する場合は、*はい - FIPS*または*はい - FIPS（混合）*を探してください。「混合」とは、140-2レベルと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、プールはより低いセキュリティレベル（140-2）で動作することに注意してください。 • セキュリティ機能を備えているか否かにかかわらず、あるいはセキュリティレベルが異なるドライブが混在するドライブで構成されるプールを作成できます。プール内のドライブにセキュリティ機能を持たないドライブが含まれている場合、プールをセキュア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ためのオプションです。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。 すべてのドライブがDA対応であれば、DAが有効になります。ボリューム作成後、メニュー：Storage[Volumes > View/Edit Settings > Advanced > Permanently disable data assurance]を選択することで、DAを無効にすることができます。ボリューム上でDAが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）	このプール候補に対してリソースプロビジョニングが利用可能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利用可能な機能であり、バックグラウンドでの初期化プロセスなしでボリュームをすぐに使用できるようにします。
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 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 サイズを示します。 • 512n - 512 バイト ネイティブ。 • 512e - 512 バイト エミュレーション。 • 4K — 4,096 バイト。

SANtricity System Managerで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すると、ホストからアクセス可能な1つ以上のボリュームを作成できます。ボリュームグループとは、RAIDレベルや容量など、共通の特性を持つボリュームを格納するコンテナのことです。

大容量の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、ストレージ容量を効率的に使用してデータを適切に保護するのに役立ちます。

開始する前に

ボリューム グループを作成する前に、次のガイドラインを確認してください。

- 未割り当てのドライブが少なくとも1本必要です。
- 1つのボリューム グループに含めることができるドライブ数には制限があります。制限はRAIDレベルによって異なります。
- シェルフ / ドロワー損失の保護を有効にするには、少なくとも3台（RAID 1を使用する場合は2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。
- EF600またはEF300ストレージ アレイを使用していて、ボリューム グループを手動で作成する場合は、各コントローラが最初の12個のスロットと最後の12個のスロットそれぞれで同じ数のドライブにアクセスできるようにします。この構成により、コントローラがドライブ側の両方のPCIeバスをより効果的に使用できるようになります。現在、System Managerでは、ボリューム グループの作成時にドライブを選択するには、[アドバンスト]機能を使用します。
- 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を選択する場合は、ミラーリングされたペアが選択されるように、一度に2台のドライブを追加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として知られる）は、4台以上のドライブを選択した場合に実現されます。
  - 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. メニュー：Storage[Pools & Volume Groups]を選択します。
2. メニュー：Create[Volume group]をクリックします。

   [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応じて最適な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種類のドライブがある場合は、使用するドライブの種類を選択してください。

   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定義するために、自動方式または手動方式のいずれかを選択できます。自動方式がデフォルトの選択肢です。

   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（詳細）*リンクをクリックしてください。クリックすると、*ドライブを自動的に選択する（詳細設定）*に変わります。

   手動方式では、特定のドライブを選択してボリューム グループを構成できます。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混在している場合、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。

ドライブの冗長性と最適なドライブ構成を理解している専門家のみが、Manual方式を使用すべきです。

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

   表示されるドライブ特性は、自動方式と手動方式のどちらを選択したかによって異なります。

自動方式のドライブ特性

特性	使用
空き容量	使用可能な容量（GiB）を示します。アプリケーションのストレージ ニーズに応じて、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）を示します。値は次のとおりです。 • 512 - 512バイト 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（Full Disk Encryption（FDE）ドライブまたはFederal Information Processing Standard（FIPS）ドライブのいずれか）のみで構成されているかどうかを示します。 • ドライブセキュリティを使用してボリュームグループを保護できますが、この機能を使用するには、すべてのドライブがセキュア対応である必要があります。 • FDE専用のボリュームグループを作成する場合は、「セキュア対応」列で*はい - FDE*を探してください。FIPS専用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（混合）*を探してください。「混合」とは、140-2レベルと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はより低いセキュリティレベル（140-2）で動作することに注意してください。 • セキュリティ機能を備えているか否かにかかわらず、あるいはセキュリティレベルが異なるドライブが混在するボリュームグループを作成できます。ボリュームグループ内のドライブにセキュリティ機能に対応してい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で保護することはできません。
セキュリティを有効化	セキュリティ対応ドライブでドライブセキュリティ機能を有効にするオプションを提供します。ボリュームグループがセキュリティ対応で、セキュリティキーを設定している場合は、チェックボックスをオンにしてドライブセキュリティを有効にできます。 ドライブセキュリティを有効にした後でそれを解除する唯一の方法は、ボリュームグループを削除してドライブを消去することです。

特性	使用
DA 対応	このグループに対してデータアシュアランス（DA）が利用可能かどうかを示します。データアシュアランス（DA）は、コントローラからドライブへ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、修正します。 DAを使用する場合は、DA対応のボリュームグループを選択してください。（DA対応ドライブの場合、プール内に作成されたボリュームではDAが自動的に有効になります。） ボリュームグループには、DA対応ドライブとDA非対応ドライブの両方を含めることができますが、この機能を使用するには、すべてのドライブがDA対応である必要があります。
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Resource Provisioningが利用可能かどうかを示します。Resource Provisioningは、EF300およびEF600ストレージアレイで利用可能な機能であり、バックグラウンドでの初期化プロセスなしでボリュームをすぐに使用できるようにします。
シェルフ損失の保護	シェルフ損失保護が利用可能かどうかを示します。シェルフ損失保護は、シェルフとの通信が完全に途絶した場合でも、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を保証します。
ドロワー損失の保護	引き出し紛失保護機能が利用可能かどうかを示します。この機能は、引き出し付きのドライブシェルフを使用している場合にのみ提供されます。ドライブシェルフ内の単一の引き出しとの通信が完全に途絶した場合でも、引き出し紛失保護機能により、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 ブロック サイズ（EF300およびEF600のみ）	グループ内のボリュームに対して作成できるブロック サイズを示します。 • 512n - 512 バイト ネイティブ。 • 512e - 512 バイト エミュレーション。 • 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	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は、同じメディアタイプである必要があります（すべてSSD、またはすべてハードドライブ）。ボリュームグループには、異なるメディアタイプまたはインターフェー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）を示します。値は次のとおりです。 • 512 - 512バイト 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。 • 可能な限り、ボリュームグループ内の現在のドライブの容量と同等の容量を持つドライブを選択してください。 • 容量の小さい未割り当て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減少す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です。 • より大容量の未割り当てドライブを追加する必要がある場合は、追加した未割り当てドライブの使用可能容量が、ボリュームグループ内のドライブの現在の容量と一致するように減少す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。
論理セクタサイズ	セクターの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（Full Disk Encryption（FDE）ドライブまたはFederal Information Processing Standard（FIPS）ドライブのいずれか）のみで構成されているかどうかを示します。 • ドライブセキュリティを使用してボリュームグループを保護できますが、この機能を使用するには、すべてのドライブがセキュア対応である必要があります。 • FDE専用のボリュームグループを作成する場合は、「セキュア対応」列で*はい - FDE*を探してください。FIPS専用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（混合）*を探してください。「混合」とは、140-2レベルと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はより低いセキュリティレベル（140-2）で動作することに注意してください。 • セキュリティ機能を備えているか否かにかかわらず、あるいはセキュリティレベルが異なるドライブが混在するボリュームグループを作成できます。ボリュームグループ内のドライブにセキュリティ機能に対応してい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で保護することはできません。
DA 対応	このグループに対してデータ保証（DA）が利用可能かどうかを示します。データ保証（DA）は、コントローラからドライブへデータが伝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、修正します。 DAを使用する場合は、DA対応のボリュームグループを選択してください。（DA対応ドライブの場合、プール内に作成されたボリュームではDAが自動的に有効になります。） ボリュームグループには、DA対応ドライブとDA非対応ドライブの両方を含めることができますが、この機能を使用するには、すべてのドライブがDA対応である必要があります。
サポートされるボリューム ブロック サイズ（EF300およびEF600のみ）	グループ内のボリュームに対して作成できるブロック サイズを示します。 • 512n - 512 バイト ネイティブ。 • 512e - 512 バイト エミュレーション。 • 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Resource Provisioningが利用可能かどうかを示します。Resource Provisioningは、EF300およびEF600ストレージアレイで利用可能な機能であり、バックグラウンドでの初期化プロセスなしでボリュームをすぐに使用できるようにします。

SANtricity System Managerでプールまたはボリューム グループに容量を追加する

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。

これにより、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利用できます。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。

開始する前に

- ドライブのステータスが最適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。
- ボリューム グループに含めることができるボリュームは最大256個です。
- プールに含めることができるボリュームの最大数は、ストレージ システムのモデルに応じて次のとおりです。
  - 2,048ボリューム（EF600およびE5700シリーズ）
  - 1,024 ボリューム（EF300）
  - 512ボリューム（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。

タスク概要

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。これらの最大数よりも多くのドライブを追加するには、必要な回数だけ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予約済み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。追加しても、DA対応ドライブの機能は利用できません。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. メニュー：Storage[Pools & Volume Groups]を選択します。
2. ドライブを追加するプールまたはボリュームグループを選択し、*容量の追加*をクリックします。

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

3. *Select drives to add capacity…*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。

コントローラのファームウェアは、割り当てられていないドライブを、最適なオプションが上位に表示されるように配置します。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は、リストの下の*選択された合計容量*に表示されます。

フィールドの詳細

フィールド	概要
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、現在プールまたはボリューム グループに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。つまり、ドライブ容量はプールまたはボリューム グループ全体で同じになります。 • 容量が大きい未割り当てのドライブを追加する必要がある場合は□、現在プールまたはボリューム グループに含まれているドライブの容量に合わせて、追加する未割り当てのドライブの使用可能容量が削減されることに注意してください。
セキュリティ対応	ドライブがセキュリティ対応かどうかを示します。 • プールまたはボリューム グループをドライブ セキュリティ機能を使用して保護するには、すべてのドライブがセキュリティ対応である必要があります。 • セキュリティ対応とセキュリティ対応でないドライブが混在したプールまたはボリューム グループを作成することは可能ですが、ドライブ セキュリティ機能を有効にすることはできません。 • セキュリティ対応ドライブのみのプールまたはボリューム グループには、たとえ暗号化機能を使用していなくても、スペアや拡張用としてセキュリティ対応でないドライブを追加することはできません。 • セキュリティ対応ドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。 • FIPSドライブには140-2と140–3の2つのレベルがあり、140-3の方がセキュリティは高くなります。レベルが140-2と140-3のドライブが混在しているプールまたはボリューム グループは、低い方のセキュリティ レベル（140-2）で動作します。

フィールド	概要
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。ドライブの属性が一致しないため、プールまたはボリューム グループでDA対応ドライブの機能を利用することはできません。DAに対応していないドライブの使用を検討してください。
DULBE 対応	ドライブに、割り当て解除または未書き込みの論理ブロックエラー（DULBE）の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機能であり、EF300またはEF600ストレージアレイがリソースプロビジョニングされたボリュームをサポートできるようにするものです。

4. *[追加]*をクリックします。

   プールまたはボリューム グループにドライブを追加する場合、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。

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

   * 現在、シェルフ損失保護またはドロワー損失保護が設定されているプールにドライブを追加する場合、確認ダイアログボックスは表示されません。

1. 続行する場合は **Yes** をクリックしてください。そうでない場合は **Cancel** をクリックしてください。

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。

ストレージの管理

SANtricity System Managerでボリューム冗長性を確認

テクニカル サポートから指示があった場合、またはRecovery Guruに記載されている場

合は、プールまたはボリューム グループ内のボリュームの冗長性をチェックし、そのボリュームのデータに整合性があるかどうかを確認できます。

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

開始する前に

- プールまたはボリューム グループのステータスが、最適である必要があります。
- プールまたはボリューム グループで進行中の変更処理がないことが必要です。
- データ冗長性のないRAID 0を除き、すべてのRAIDレベルの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。

タスク概要

冗長性チェックは、一度に1つのプールまたはボリューム グループでしか実行できません。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、RAID 5、またはRAID 6ボリューム内のデータ ブロックをスキャンし、ブロックの冗長性情報をチェックします（RAID 3をボリューム グループに割り当てるには、コマンドライン インターフェイスを使用する必要があります）。
- 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、エラーが発生する場合があります。この問題を回避するためには、同じプールまたはボリューム グループで続けて冗長性チェックを実行する場合は、1～2分経ってから実行してください。

手順

1. メニュー：Storage[Pools & Volume Groups]を選択します。
2. メニューで「Uncommon Tasks」→「Check volume redundancy」を選択してください。

   [冗長性のチェック]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、 `check`と入力してこの処理の実行を確認します。
4. **Check** をクリックします。

   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。個々の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。

   - ボリュームの表内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について

ステータス	概要
保留中	最初にスキャンされるボリュームです。冗長性チェックは開始するための[開始]がまだクリックされていません。 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。
確認中	ボリュームは冗長性チェック中です。
合格	ボリュームは冗長性チェックにパスしました。冗長性情報に不整合は見つかりませんでした。
失敗	ボリュームは冗長性チェックにパスしませんでした。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に表示される指示に従ってください。
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、回復不可能なデータ損失につながる場合があります。

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のチェックが完了したら、*Done*をクリックします。

SANtricity System Managerで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。

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. メニュー：Storage[Pools & Volume Groups]を選択します。
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すると、残りのプールまたはボリューム グループが表示されます。

3. メニュー：Uncommon Tasks[Delete]を選択して確定します。

結果

System Manager は以下の操作を実行します。

- プールまたはボリューム グループ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。

SANtricity System Managerでボリュームグループの空き容量を統合する

[空き容量の統合]オプションを使用すると、選択したボリューム グループの既存の空きエクステントを統合できます。これにより、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。

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は、オンラインでOptimal状態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。

タスク概要

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

[空き容量の統合]ダイアログ ボックスは、次のいずれかの方法で起動できます。

- ボリュームグループに対して少なくとも1つの空き容量領域が検出されると、ホームページの通知領域に「空き容量を統合する」という推奨事項が表示されます。*空き容量を統合する*リンクをクリックしてダイアログボックスを開きます。
- 以下のタスクで説明しているように、[プールとボリューム グループ]ページから[空き容量の統合]ダイアログ ボックスを開くこともできます。

空き容量領域について

空き容量領域は、ボリュームを削除するか、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 グループ内の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。その結果、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まなければならなくなるため、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、新しいファイルの以降の断片化を防ぐのにも役立ちます。

手順

1. メニュー：Storage[Pools & Volume Groups]を選択します。
2. 統合したい空き容量のあるボリュームグループを選択し、メニューの「Uncommon Tasks」→「Consolidate volume group free capacity」を選択します。

   [空き容量の統合]ダイアログ ボックスが表示されます。

3. `consolidate`と入力して、この処理を実行することを確認します。
4. * Consolidate * をクリックします。

   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。

終了後の操作

Home › View Operations in Progressを選択すると、空き容量統合操作の進行状況が表示されます。この処理には時間がかかり、システムのパフォーマンスに影響を与える可能性があります。

SANtricity CLIでのボリュームグループのエクスポート/インポート

ボリューム グループの移行では、ボリューム グループをエクスポートして、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のユーザー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**キャッシュでロケーターライトをオンにします（**SANtricity System Manager**）

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. メニュー：Storage[Pools & Volume Groups]を選択します。
2. 検索したいプール、ボリュームグループ、またはSSDキャッシュを選択し、次にメニュー：その他［ロケーターライトを点灯］をクリックします。

   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. ドライブを正常に検出したら、*電源を切る*をクリックしてください。

SANtricity System Managerでプールまたは**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。

タスク概要

容量を削除する際のガイドライン

- 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本より多くのドライブを削除する必要がある場合は、この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キャッシュ内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

- 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。そのため、プールのセキュリティを有効にすることができるようになります。
- 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対応にするには、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. メニュー：Storage[Pools & Volume Groups]を選択します。
2. プールまたはSSD Cacheを選択し、menu：More[容量の削除]をクリックします。

   [容量の削除]ダイアログ ボックスが表示されます。

3. リストから1つ以上のドライブを選択します。

   リスト内でドライブを選択または選択解除すると、*選択された合計容量*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した後に作成されるプールまたはSSD Cacheの合計容量が表示されます。

4. *Remove*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キャッシュの削減後の新しい容量が、[プールとボリューム グループ]ビューに反映されます。

プール / グループ設定の変更

SANtricity System Managerでプールの構成設定を変更します

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

タスク概要

このタスクでは、プールの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. メニュー：Storage[Pools & Volume Groups]を選択します。
2. 編集するプールを選択し、*View/Edit Settings*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. *Settings*タブを選択し、必要に応じてプールの設定を編集してください。

フィールドの詳細

設定	概要
Name	ユーザが指定したプールの名前を変更できます。プールの名前を指定する必要があります。
容量のアラート	プールの空き容量が指定したしきい値以上になった場合に、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 スペースを追加したり不要なオブジェクトを削除したりすることができます。 アラートはダッシュボードの[通知]領域に表示されるほか、サーバから管理者にEメールおよびSNMPトラップ メッセージとして送信することができます。 次の容量アラートを定義できます。 • 重要アラート — この重要アラートは、プール内の空き容量が指定されたしきい値に達したか超えた場合に通知します。スピナーコントロールを使用して、しきい値のパーセンテージを調整します。この通知を無効にするには、チェックボックスを選択してください。 • 早期アラート — この早期アラートは、プール内の空き容量が指定されたしきい値に達したときに通知します。スピナーコントロールを使用して、しきい値のパーセンテージを調整します。この通知を無効にするには、チェックボックスを選択してください。
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上げると処理は早く完了しますが、ホストのI/Oパフォーマンスは低下します。優先度を下げ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。 • クリティカルな再構築の優先度 — このスライダーバーは、複数のドライブ障害によって一部のデータに冗長性がなく、追加のドライブ障害によってデータが失われる可能性がある状態になった場合のデータ再構築処理の優先度を決定します。 • 劣化再構築優先度 — このスライダーバーは、ドライブ障害が発生したが、データには依然として冗長性があり、追加のドライブ障害が発生してもデータ損失が発生しない場合のデータ再構築処理の優先度を決定します。 • バックグラウンド操作の優先度 — このスライダーバーは、プールが最適な状態にあるときに実行されるプールのバックグラウンド操作の優先度を決定します。これらの操作には、Dynamic Volume Expansion（DVE）、Instant Availability Format（IAF）、および交換または追加されたドライブへのデータ移行が含まれます。

設定	概要
保存容量（EF600またはEF300の場合は「最適化容量」）	保存容量 — ドライブの数を定義することで、潜在的なドライブ障害をサポートするためにプールに予約される容量を決定できます。ドライブ障害が発生した場合、復元されたデータを保持するために保存容量が使用されます。プールは、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の代わりに、データ再構築プロセス中に保存容量を使用します。 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）-- プールが作成されると、利用可能な容量とパフォーマンスおよびドライブの摩耗寿命のバランスを提供する推奨最適化容量が生成されます。このバランスは、スライダーを右に動かすことで、利用可能な容量の増加を犠牲にして、パフォーマンスとドライブの摩耗寿命を向上させることができます。また、左に動かすことで、パフォーマンスとドライブの摩耗寿命を犠牲にして、利用可能な容量を増やすことができます。 SSDドライブでは、その容量の一部が未割り当ての場合に寿命が長くなり、最大書き込みパフォーマンスが向上します。プールに関連付けられているドライブの未割り当て容量は、プールの予約済み容量、空き容量（ボリュームで使用されていない容量）、および使用可能容量のうちの最適化容量として確保された容量で構成されます。この最適化容量は使用可能容量を削って確保され、この容量をボリュームの作成に使用することはできません。

4. *保存*をクリックします。

SANtricity System Managerでボリューム グループの設定を変更する

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。

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レベルに変更するための十分な容量が必要です。

手順

1. メニュー：Storage[Pools & Volume Groups]を選択します。
2. 編集するボリュームグループを選択し、*設定の表示/編集*をクリックします。

   [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*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	概要
Name	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 — 高い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 グループ内のドライブが1つでも障害が発生すると、関連す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台以上のドライブを組み合わせて、1つの大きな論理ドライブにします。 • **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の機密データの保存に適しています。ミラーリングされたペアの一方のドライブの内容を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が発生した場合に保護を提供します。 • **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、データベースなど、高いパフォーマンスと耐障害性が求められる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** — 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）に最適で、一般的なI/Oサイズは小さく、読み取りアクティビティの割合が高い。 • **RAID 6** — RAID 5を超える冗長性保護を必要とするが、高い書き込みパフォーマンスを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。

設定	概要
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、ボリューム グループの空き容量（ボリュームで使用されていない容量）と、使用可能容量のうちの最適化容量として確保された容量で構成されます。この最適化容量は使用可能容量を削って確保され、この容量をボリュームの作成に使用することはできません。

4. *保存*をクリックします。

   RAIDレベルの変更により容量が減少したり、ボリュームの冗長性が失われたり、シェルフ/ドロワーの損失保護が失われたりした場合は、確認ダイアログボックスが表示されます。続行する場合は*Yes*を選択してください。そうでない場合は*No*をクリックしてください。

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。この処理の実行中は、パフォーマンスが若干低下することがあります。

SANtricity System Managerの既存のボリューム グループとプールでリソース プロビジョニングを有効または無効にします

DULBE対応のドライブでは、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に対してリソース 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利用可能な機能であり、バックグラウンドでの初期化プロセスなしでボリュームをすぐに使用開始できます。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解放（マッピング解除）されるため、SSDの寿命が延び、最大書き込み性能が向上する可能性があります。

リソース プロビジョニングは、DULBEがサポートされているシステムではデフォルトで有効になります。以前に無効にしていなければ、有効にする必要はありません。

開始する前に

- EF300またはEF600ストレージ アレイが必要です。

  現時点では、EF300CまたはEF600Cストレージアレイでは DULBEはサポートされていません。

- SSDボリューム グループまたはプール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ている必要があります。サポートされていな

い場合、リソース プロビジョニング オプションは使用できません。

タスク概要

既存のボリューム グループおよびプールに対してリソース プロビジョニングを有効にすると、選択したボリューム グループまたはプール内のすべてのボリュームではブロックの割り当て解除が許可されるようになります。その際、マッピング解除単位で一貫した割り当てが実施されるように、バックグラウンドで処理が実行されることがあります。この処理でスペースがマッピング解除されることはありません。このバックグラウンド処理が完了したら、オペレーティング システムは未使用ブロックのマッピングを解除して空きスペースを作成します。

既存のボリューム グループまたはプールに対してリソース プロビジョニングを無効にすると、すべてのボリューム内のすべての論理ブロックがバックグラウンドで再書き込みされます。既存データへの変更はありません。この書き込みによって、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がマッピングまたはプロビジョニングされます。

新しいボリュームグループとプールについては、メニュー：Settings[System > Additional Settings > Enable/Disable Resource-Provisioned Volumes] からリソースプロビジョニングを有効または無効にできます。

手順

1. メニュー：Storage[Pools & Volume Groups]を選択します。
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すると、残りのプールまたはボリューム グループが表示されます。

3. *通常とは異なるタスク*を選択し、次に*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*を選択します。
4. ダイアログ ボックスで処理を確定します。

* 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ら、ホストを再起動して DULBE 設定の変更を検出してから、すべてのファイルシステムを再マウントする必要があります。

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

デフォルトで有効になっているリソース プロビジョニングを無効にした場合、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。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利用可能な機能であり、バックグラウンドでの初期化プロセスなしでボリュームをすぐに使用開始できます。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解放（マッピング解除）されるため、SSDの寿命が延び、最大書き込み性能が向上する可能性があります。

リソース プロビジョニングは、DULBEがサポートされているシステムではデフォルトで有効になります。

開始する前に

- EF300またはEF600ストレージ アレイが必要です。
- SSDボリューム グループまたはプール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ている必要があります。

> 現時点では、EF300CまたはEF600Cストレージアレイ ではDULBEはサポートされていません。

タスク概要

リソース プロビジョニングが再度有効になるのは、新しく作成したボリューム グループとプールのみです。リソース プロビジョニングが無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には影響しません。

手順

1. メニュー：Settings[System]を選択します。
2. *追加設定*までスクロールダウンし、*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。

   オプションの表記から、リソース プロビジョニングが現在有効になっているか無効になっているかがわかります。

3. ダイアログ ボックスで処理を確定します。

結果

リソース プロビジョニングの有効化と無効化は、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 グループには影響しません。

SANtricity System Managerでプールまたはボリューム グループのセキュリティを有効にする

プールまたはボリューム グループのドライブ 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なアクセスを防止することができます。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 キーが設定されているコントローラからのみ可能です。

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が最適な状態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。

タスク概要

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。プールやボリューム 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 グループを削除したうえでドライブを消去する必要があります。

手順

1. メニュー：Storage[Pools & Volume Groups]を選択します。
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、メニューの「More」[Enable security]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、*Enable*をクリックします。

SSDキャッシュの管理

SANtricity ソフトウェアにおける SSD キャッシュの仕組み

SSDキャッシュ機能は、コントローラーベースのソリューションであり、最も頻繁にアクセスされるデータ（「ホット」データ）を低遅延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、システムパフォーマンスを動的に高速化します。SSDキャッシュは、ホストからの読み取り専用です。

SSDキャッシュとプライマリ キャッシュ

SSDキャッシュは、コントローラのダイナミック ランダム アクセス メモリ（DRAM）内のプライマリ キャッシュと併用されるセカンダリ キャッシュです。

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すると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 Cacheでは、データはボリュームからコピーされ、SSD Cacheを作成する際に自動的に作成される2つの内部RAIDボリューム（コントローラごとに1つ）に保存されます。

内部RAIDボリュームは、内部キャッシュ処理の目的で使用されます。これらのボリュームは、ユーザーインターフェースからアクセスすることも表示することもできません。ただし、これら2つのボリュームは、ストレージアレイで許可されているボリュームの総数にカウントされます。

SSDキャッシュの使用方法

インテリジェントなキャッシングは、データを低遅延のドライブに配置することで、そのデータに対する将来の要求への応答を大幅に高速化します。プログラムがキャッシュ内のデータを要求する場合（「`cache hit`」）の場合、低遅延のドライブがそのトランザクションを処理できます。そうでない場合は「`cache miss`」が発生し、データは元の低速なドライブからアクセスする必要があります。cache hitが増えるにつれて、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、データが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、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キャッシュに保存されます。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。

読み取ったデータを処理する必要がある場合、CPUは次の手順を実行します。

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ことで、I/Oパフォーマンスと応答時間が向上します。

シンプルなボリュームI/Oメカニズムを使用して、SSD Cacheとの間でデータを移動します。データがSSDにキャッシュされて保存されると、その後のデータ読み取りはSSD Cache上で実行されるため、HDDボリュームにアクセスする必要がなくなります。

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が有効になっているボリュームでSSD Cacheを使用する場合、ボリュームとSSD Cacheのドライブセキュリティ機能が一致している必要があります。それらが一致しない場合、ボリュームはセキュリティ保護が有効になりません。

SSDキャッシュの実装

SSDキャッシュを実装するには、次の処理を実行します。

1. SSDキャッシュを作成します。
2. SSDの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。

SANtricityソフトウェアのSSDキャッシュの制限について学ぶ

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10 TB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。
- ボリュームでSSDキャッシュが有効になっているかどうかにかかわらず、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 セキュリティを適用した場合の制限事項

- 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それ以外のドライブを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。

SANtricity System Managerで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。

開始する前に

ストレージ アレイにSSDドライブが含まれている必要があります。

タスク概要

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

新しいSSDキャッシュを作成する際は、次のガイドラインに従ってください。

- SSDキャッシュのセキュリティを有効にできるのは作成時だけで、あとから有効にすることはできません。
- SSDキャッシュはストレージ アレイごとに1つだけサポートされます。
- 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 アレイで使用できる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。
- ボリュームでSSDキャッシュが有効になっているかどうかにかかわらず、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. メニュー：Storage[Pools & Volume Groups]を選択します。
2. メニュー：Create[SSD Cache]をクリックします。

   [SSD キャッシュの作成]ダイアログ ボックスが表示されます。

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

特性	使用
容量	使用可能な容量（GiB）を示します。アプリケーションのストレージ ニーズに応じて容量を選択します。 SSDキャッシュの最大容量は、コントローラのプライマリ キャッシュ容量で決まります。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キャッシュで利用できるドライブの数を示します。必要なドライブ数のSSD候補を選択します。
セキュリティ対応	SSDキャッシュがセキュリティ対応ドライブだけで構成されているかどうかを示します。セキュリティ対応ドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。 セキュリティ機能が有効になった SSD キャッシュを作成する場合は、「セキュリティ対応」列で **Yes - FDE** または **Yes - FIPS** を探してください。
セキュリティを有効化	セキュリティ機能を備えたドライブで、ドライブセキュリティ機能を有効にするオプションを提供します。セキュリティ対応SSD Cacheを作成する場合は、Enable Securityチェックボックスをオンにします。 セキュリティは一度有効にするとあとで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。

特性	使用
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キャッシュを、SSD読み取りキャッシュを実装したいボリュームに関連付けます。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、*ホストにマッピング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選択します。

   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*をクリックします。

SANtricity System ManagerでSSD**キャッシュ設定を変更する**

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. メニュー：Storage[Pools & Volume Groups]を選択します。
2. 編集するSSDキャッシュを選択し、*設定の表示/編集*をクリックします。

   [SSD キャッシュ設定]ダイアログ ボックスが表示されます。

3. SSDキャッシュ設定を確認するか、必要に応じて編集します。

フィールドの詳細

設定	概要
Name	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設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 • デグレード • 失敗（重大なMELイベントが生成されます） • 中断
容量	SSDキャッシュの現在の容量および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 • 1 GiB ～ 2 GiB • 2 GiB ～ 4 GiB • 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。 • **Secure-capable** — SSD Cacheがすべて Secure-capableドライブで構成されているかどうかを示します。Secure-capableドライブとは、自己暗号化機能を備え、不正アクセスからデータを保護できるドライブのことです。 • **Secure-enabled** — SSDキャッシュでセキュリティが有効になっているかどうかを示します。 • **DA**対応 — SSDキャッシュがすべてDA対応ドライブで構成されているかどうかを示します。DA対応ドライブは、ホストとストレージアレイ間でデータが通信される際に発生する可能性のあるエラーをチェックし、修正することができます。
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*をクリックします。

SANtricity System Managerで**SSD**キャッシュ統計情報を表示する

SSDキャッシュの統計（読み取り、書き込み、キャッシュ ヒット、キャッシュの割り当て率、キャッシュの利用率など）を表示できます。

詳細統計情報の一部である基本統計情報は、「SSD Cacheの統計情報の表示」ダイアログボックスに表示されます。SSD Cacheの詳細な統計情報は、すべてのSSD統計情報を `.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. メニュー：Storage[Pools & Volume Groups]を選択します。
2. 統計情報を表示したいSSDキャッシュを選択し、次にメニュー：その他［SSDキャッシュ統計情報の表示］をクリックします。

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

フィールドの詳細

設定	概要
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。
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、対象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あり、「割り当てられたバイト数 / 使用可能なバイト数」の式で算出されます。
キャッシュ使用率（%）	有効なボリュームのデータが格納されているSSDキャッシュ ストレージの割合が表示されます。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ます。割り当てられている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	SSDキャッシュのすべての統計をCSV形式にエクスポートします。エクスポートされたファイルには、SSDキャッシュの使用可能なすべての統計（一般統計と詳細統計の両方）が含まれます。

3. *キャンセル*をクリックしてダイアログボックスを閉じます。

リザーブ容量の管理

SANtricityソフトウェアでの予約容量の仕組み

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量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、報告されている最大容量である256 TiBに達すると、その容量を増やすことはできません。シン ボリュームの予約容量が、報告されている最大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際に容量が割り当てられます。）

プール内でシン 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た場合は、リザーブ容量ボリュームが最適状態に戻り、シン ボリュームが使用可能な状態に戻ります。
- 既存のシン ボリュームを使用して非同期ミラー ペアを完成させる場合、そのシン ボリュームを新しいリザーブ容量ボリュームを使用して再初期化します。初期同期プロセス中は、プライマリ側のプロビジョニングされたブロックのみが転送されます。

容量のアラート

コピー サービス オブジェクトには、容量の警告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できます。

コピー サービス オブジェクト ボリュームのリザーブ容量がフルに近付くと、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%に達したときに送信されます。ただし、必要に応じて増減できます。このアラートを受信した場合は、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。これは、コピー サービス オブジェクトごとに設定できます。

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、関連するコピー 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。本来は、コピー サービス オブジェクトが削除されたときに、リザーブ容量ボリュームも削除されますが、リザーブ容量ボリュームの削除に失敗することがあります。

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

System Managerは、ホームページの通知エリアに「未使用容量を再利用してください」というメッセージを表示し、孤立した予約済み容量ボリュームについて警告します。*未使用容量の解放*をクリックすると、「未使用容量の解放」ダイアログボックスが表示され、そこで孤立した予約済み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。

SANtricity System Managerで予約容量を増やす

リザーブ容量（ストレージ オブジェクト上のコピー サービス処理に使用される物理的に割り当てられた容量）を拡張できます。

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。一般的には、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。

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」である必要があり、変更状態であってはなりません。
- 容量を増やすために使用するプールまたはボリューム グループには、空き容量が存在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空き容量がない場合は、未使用のドライブという形で未割り当て容量をプールまたはボリュームグループに追加できます。

タスク概要

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 ボリュームの予約容量を増やすことはできません。読み書き可能なSnapshot ボリュームのみが予約容量を必要とします。

手順

1. メニュー：Storage[Pools & Volume Groups]を選択します。
2. * Reserved Capacity * タブを選択します。
3. 予約容量を増やしたいストレージオブジェクトを選択し、*容量を増やす*をクリックします。

   「予約容量の増加」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 グループ上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. * Increase * をクリックします。

結果

System Manager は以下の操作を実行します。

- 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。

SANtricity System Manager で予約済み容量を削減

ストレージ オブジェクトのリザーブ容量を削減するには、[容量の削減]オプションを使用します。対象となるストレージ オブジェクトは、Snapshotグループ、Snapshotボリューム、および整合性グループのメンバー ボリュームです。リザーブ容量は、増やしたときの分量ずつしか削除できません。

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。

タスク概要

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. メニュー：Storage[Pools & Volume Groups]を選択します。
2. * Reserved Capacity * タブをクリックします。
3. 予約容量を減らしたいストレージオブジェクトを選択し、*容量を減らす*をクリックします。

   「予約容量の削減」ダイアログボックスが表示されます。

4. 予約容量を減らす容量を選択し、*減らす*をクリックします。

結果

System Manager は以下の操作を実行します。

- 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変更します。無効の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。

SANtricity System Managerでスナップショットグループの予約容量設定を変更します

スナップショット グループの設定を変更して、名前、自動削除設定、許可されるスナップショット イメージの最大数、SANtricity System Managerが予約容量アラート通知を送信するパーセンテージ ポイント、または予約容量が定義された最大割合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、そのグループに含まれるすべてのSnapshotイメージのデータを保存するためのリザーブ容量が作成されます。

手順

1. メニュー：Storage[Pools & Volume Groups]を選択します。
2. * Reserved Capacity * タブをクリックします。
3. 編集するSnapshotグループを選択し、*設定の表示/編集*をクリックします。

   Snapshot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	概要
Snapshotグループ設定	Name
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。ユーザが指定可能です。	Snapshotスケジュール
[はい]の場合は、Snapshotを自動的に作成するためのスケジュールが設定されます。	予約容量設定
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	概要
リザーブ容量がフルになったときの処理	次のいずれかのポリシーを選択できます。 • 最も古い**Snapshot**イメージの削除 — System Managerは、Snapshotグループ内で最も古いSnapshotイメージを自動的に削除し、グループ内で再利用するために予約されていたSnapshotイメージの容量を解放します。 • ベースボリュームへの書き込みを拒否 — 予約容量が定義された最大パーセンテージに達すると、System Managerは、予約容量へのアクセスをトリガーしたベースボリュームへのI/O書き込み要求を拒否します。
関連オブジェクト	ベース ボリューム
グループに使用されるベースボリュームの名前。ベースボリュームとは、スナップショットイメージが作成される元のボリュームのことです。シックボリュームまたはシンボリュームのいずれかであり、通常はホストに割り当てられます。ベースボリュームは、ボリュームグループまたはディスクプールのどちらにも配置できます。	スナップショット画像

5. * 保存 * をクリックして、変更内容をスナップショットグループの設定に適用します。

SANtricity System Managerでスナップショットボリュームの予約容量設定を変更します

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. メニュー：Storage[Pools & Volume Groups]を選択します。
2. * Reserved Capacity * タブをクリックします。
3. 編集するスナップショットボリュームを選択し、*設定の表示/編集*をクリックします。

   「スナップショットボリュームの予約容量設定」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	概要
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への変更を適用してください。

SANtricity System Managerで整合性グループ メンバー ボリュームの予約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予約容量がフルに近づいたときにSANtricity System Managerがアラート通知を送信するパーセンテージポイントを調整したり、予約容量が定義された最大パーセンテージ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。

タスク概要

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. メニュー：Storage[Pools & Volume Groups]を選択します。
2. * Reserved Capacity * タブをクリックします。
3. 編集したい整合性グループのメンバーボリュームを選択し、*設定の表示/編集*をクリックします。

   メンバーボリューム予約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	概要
アラートの送信しきい値…	スピナーボックスを使用して、メンバーボリュームの予約容量が満杯に近づいたときにSystem Managerがアラート通知を送信するパーセンテージポイントを調整します。 メンバーボリュームの予約容量が指定されたしきい値を超えると、System Managerはアラートを送信し、予約容量を増やすか、不要なオブジェクトを削除する時間を与えます。 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_すべて_のメンバーボリューム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	次のいずれかのポリシーを選択できます。 • 最も古い**Snapshot**イメージの削除 — System Managerは、整合性グループ内で最も古いSnapshotイメージを自動的に削除し、グループ内で再利用するためにメンバーの予約済み容量を解放します。 • ベースボリュームへの書き込みを拒否 — 予約容量が定義された最大パーセンテージに達すると、System Managerは、予約容量へのアクセスをトリガーしたベースボリュームへのI/O書き込み要求を拒否します。

5. 変更を適用するには、*保存*をクリックしてください。

結果

System Managerは、メンバーボリュームの予約容量設定を変更するだけでなく、整合性グループ内のすべてのメンバーボリュームの予約容量設定も変更します。

SANtricity System Managerでミラーペアボリュームの予約容量設定を変更する

ミラーリングされたペアボリュームの設定を変更して、ミラーリングされたペアボリュームの予約容量がいっぱいになりそうなときに SANtricity System Manager がアラート通知を送信するパーセンテージポイントを調整できます。

手順

1. メニュー：Storage[Pools & Volume Groups]を選択します。
2. * Reserved Capacity * 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、*設定の表示/編集*をクリックします。

   「ミラーリングペアボリュームの予約容量設定」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	概要
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。 ミラー ペアのリザーブ容量の使用率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. 変更を適用するには、*保存*をクリックしてください。

SANtricity System Manager で保留中のスナップショット 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。Snapshotイメージの作成は、同期処理が完了するとすぐに完了します。

タスク概要

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イメージを格納する整合性グループの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. メニュー：Storage[Pools & Volume Groups]を選択します。
2. * Reserved Capacity * タブをクリックします。
3. 保留中のスナップショット イメージをキャンセルするスナップショット グループを選択し、メニューの「Uncommon Tasks」→「Cancel pending snapshot image」をクリックします。
4. 保留中のスナップショット イメージをキャンセルすることを確認するには、*はい*をクリックします。

SANtricity System Managerでスナップショットグループを削除する

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。

タスク概要

Snapshotグループを削除すると、グループに含まれるSnapshotイメージもすべて削除されます。

手順

1. メニュー：Storage[Pools & Volume Groups]を選択します。
2. * Reserved Capacity * タブをクリックします。
3. 削除するスナップショットグループを選択し、メニューの「Uncommon Tasks」→「Delete snapshot group」をクリックします。

   「スナップショット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. `delete`と入力して確認します。

結果

System Manager は以下の操作を実行します。

- Snapshotグループに関連付けられているすべてのSnapshotイメージを削除します。
- 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。

プールとボリュームグループに関するよくある質問 **SANtricity System Manager**

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

ボリューム グループとは何ですか**?**

ボリュームグループとは、共通の特性を持つボリュームを格納するコンテナのことです。ボリュームグループには、定義された容量とRAIDレベルがあります。ボリュームグループを使用すると、ホストからアクセス可能な1つまたは複数のボリュームを作成できます。（ボリュームは、ボリュームグループまたはプールから作成します。）

プールとは何ですか**?**

プールは、論理的にグループ化されたドライブの集まりです。プールを使用して、ホストからアクセスできるボリュームを作成できます（ボリュームはプールまたはボリューム グループから作成します）。

プールを使用すると、ディスク スペースが不足しないように管理者が各ホストの使用状況を監視する必要はなくなり、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、ホストに対して透過的に容量が拡張されます。

データプールを使用すると、均衡を維持するためにデータが自動的に再分配されます。パリティ情報と予備容量をプール全体に分散させることで、プール内のすべてのドライブを使用して障害ドライブを再構築できます。この方式では専用のホットスペアドライブは使用せず、代わりにプール全体で予備容量を確保します。ドライブ障害が発生すると、データを再構築するために他のドライブ上のセグメントが読み取られます。次に、新しいドライブが選択され、障害ドライブ上にあった各セグメントが書き込まれ、これによりドライブ間でのデータ分散が維持されます。

リザーブ容量とは何ですか**?**

リザーブ容量は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 グループに含まれます。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なアクセスを防止します。

セキュリティ機能を備えたドライブは、フルディスク暗号化（FDE）ドライブまたは連邦情報処理標準（FIPS）ドライブのいずれかです。FIPSドライブは認証試験を受けています。

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。

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。

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

- RAID 3ボリューム、RAID 5ボリューム、またはRAID 6ボリュームのデータ ブロックがスキャンされ、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、エラーが発生する場合があります。この問題を回避するためには、同じプールまたはボリューム グループで続けて冗長性チェックを実行する場合は、1～2分経ってから実行してください。

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 グループと似ていますが、次の点が異なります。

- プール内のデータは、プール内のすべてのドライブにランダムに格納されます。一方、ボリューム グループ内のデータは同じ一連のドライブに格納されます。
- プールの方がドライブの障害時のパフォーマンスの低下および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がありません。

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のは次のような場合です。

- ストレージ アレイに複数のアプリケーションがあり、同じドライブ リソースを競合させたくない場合は、1つまたは複数のアプリケーション用に小さいプールを手動で作成することを検討してください。

  ワークロードを、データを分散させるための多数のボリュームを持つ大規模なプールに割り当てる代わりに、1つまたは2つ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プールを手動で作成することで、ストレージ アレイの処理をより迅速に、競合を少なく実行できるようになります。

  プールを手動で作成するには、*ストレージ*を選択し、*プールとボリューム グループ*を選択します。「すべての容量」タブから、メニュー：作成[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、プールに使用するドライブを自動で推奨できないという内容の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] ページからプールを選択し、**[容量の追加]** をクリックします。

容量アラートが重要なのはなぜですか?

容量アラートは、ドライブをプールに追加すべきタイミングを示します。ストレージ アレイの操作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された割合に達した場合、またはそれを超えた場合にアラートを送信するようにSANtricity System Managerを設定することで、これらの操作の中断を防ぐことができます。

このパーセンテージは、*プールの自動構成*オプションまたは*プールの作成*オプションのいずれかを使用してプールを作成する際に設定します。自動オプションを選択した場合、デフォルト設定により、アラート通知を受信するタイミングが自動的に決定されます。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できます。または、デフォルト設定を受け入れることもできます。これらの設定は、メニューの「設定」→「アラート」で後で調整できます。

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

予約済み容量を増やせない場合、どのような理由が考えられますか?

使用可能なすべての容量でボリュームを作成した場合、予約済み容量を増や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かぎり、予約済み容量を増やすことはできません。

保存容量は*プールとボリューム グループ*から変更できます。編集するプールを選択します。*設定の表示/編集*をクリックし、*設定*タブを選択します。

> 予約済み容量はプール内の全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**?**

SANtricity System Managerは、プールから削除できるドライブの数に制限を設けます。

- 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。
- 一度に取り外せるドライブは最大60台です。60個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台を超えるドライブを削除する必要がある場合は、「ドライブの削除」操作を繰り返してください。

ドライブではどのようなタイプのメディアがサポートされていますか**?**

以下のメディアタイプがサポートされています：Hard Disk Drive（HDD）およびSolid State Disk（SSD）。

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]ダイアログでは、既存のプールやボリューム グループに追加できないドライブは表示されません。

ドライブを追加できない理由は次のとおりです。

- 未割り当ての、セキュリティ有効でないドライブでなければなりません。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。
- ステータスが「最適」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 タイプが同じである必要があります。次のドライブ タイプを混在させることはできません。
  - 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）
  - NVMeドライブとSASドライブ
  - ボリュームのブロック サイズが512バイトのドライブと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 グループ内に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有効ボリュームを作成できないので注意してください。

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/ドロワーの損失に対する保護基準	必要な棚／引き出しの最小数
プール	シェルフの場合、プールに含めることができるドライブは1つのシェルフにつき2台までです。 ドロワーの場合、プールに各ドロワーから同数のドライブが含まれている。	6 - シェルフ 5 - ドロワー
RAID 6	ボリューム グループには、1つのシェルフまたはドロワー内に2台以下のドライブが含まれます。	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 ペア内の各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 グループへおドライブの配置を最適化するにはどうすればよいですか**?**

プールやボリューム グループを作成するときは、上段と下段のドライブ スロットからバランスよくドライブを選択してください。

EF600およびEF300コントローラでは、ドライブ スロット0～11が1つのPCIブリッジに接続され、スロット12～23が別の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、上段と下段のスロットのドライブ数がほぼ同じになるようにバランスよくドライブを選択する必要があります。このように配置すれば、ボリュームが必要以上に早く帯域幅の上限に達することはありません。

アプリケーションに最適な**RAID**レベルはどれですか**?**

ボリューム グループのパフォーマンスを最大限に高めるには、適切なRAIDレベルを選択する必要があります。適切なRAIDレベルを特定するには、ボリューム グループにアクセスしているアプリケーションでの読み

取りと書き込みの比率を把握します。この比率は[パフォーマンス]ページで確認できます。

RAIDレベルとアプリケーション パフォーマンス

RAIDは、ユーザ データと冗長データの書き込み方法とドライブからの取得方法を決定するために、_レベル_と呼ばれる一連の構成に依存しています。各RAIDレベルは、それぞれ異なるパフォーマンス特性を提供します。読み取り率の高いアプリケーションは、RAID 5およびRAID 6構成の優れた読み取り性能により、RAID 5ボリュームまたはRAID 6ボリュームを使用することで良好なパフォーマンスを発揮します。

読み取り比率が低い（書き込み中心の）アプリケーションの場合、RAID 5ボリュームまたはRAID 6ボリュームでは同様のパフォーマンスを実現できません。この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。

RAIDレベルは次の情報に基づいて選択します。

RAID 0

- 概要
  - 冗長性なし、ストライピング モード。
- 仕組み
  - 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。
- ドライブ番号の要件
  - RAIDレベル0には最低1本のドライブが必要です。
  - RAID 0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 1または**RAID 10**

- 概要
  - ストライピング / ミラー モード。
- 仕組み
  - 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同じ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、高度なパフォーマンスと最高のデータ可用性を実現します。
  - 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が、ミラー ドライブがデータへのアクセスを保証します。
- 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。

- ドライブ番号の要件
  - RAID 1には最低2本のドライブが必要です（ユーザ データ用とミラーリングされたデータ用に1本ずつ）。
  - 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が自動的に構成されます（ユーザ データ用とミラーリングされたデータ用に2本ずつ）。
  - ボリューム グループには偶数個のドライブが必要です。ドライブの数が偶数でない場合、または未割り当てのドライブが残っている場合は、*プールとボリューム グループ*に移動してボリューム グループにドライブを追加し、操作を再試行してください。
  - 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。
- 仕組み
  - 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。冗長性情報があるので、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。
- ドライブ番号の要件
  - 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。
  - 一般に、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。
- 仕組み
  - 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、冗長性情報があるので引き続きデータにはアクセスできます。
  - 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。
- ドライブ番号の要件
  - 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。
  - 一般に、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。プールは自動的にRAID 6として構成されます。

RAIDレベルとデータ保護

RAID 1、RAID 5、およびRAID 6では、フォールト トレランス用に冗長性データがドライブ メディアに書き込まれます。冗長性データは、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です。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上に迅速にデータを再構築できます。

1つのボリューム グループ全体で1つの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 グループ内に保存されます。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差し引いたものです。冗長性を確保するために必要な容量は、使用するRAIDレベルによって異なります。

Data Assuranceとは何ですか**?**

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、この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が判断されます。破損している可能性があるデータはディスクに書き込まれず、ホストにも返されません。DA機能を使用する場合は、新しいボリュームの作成時にDA対応のプールまたはボリューム グループ（[候補]の表でDAが[はい]になっている）を選択します。

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

セキュリティ対応（ドライブ セキュリティ）とは何ですか**?**

ドライブ セキュリティは、セキュリティ有効ドライブをストレージ アレイから取り外したときに、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?

通常、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、プールまたはボリューム グループには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、未使用のドライブという形で未割り当て容量を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」である必要があり、変更状態であってはなりません。
- 容量を増やすために使用するプールまたはボリューム グループには、空き容量が存在する必要があります。
- 読み取り専用のSnapshot ボリュームの予約容量を増やすことはできません。読み書き可能なSnapshot ボリュームのみが予約容量を必要とします。

スナップショット操作の場合、予約容量は通常、ベース ボリュームの40%です。非同期ミラーリング操作の場合、予約容量は通常、ベース ボリュームの20%です。ベース ボリュームが頻繁に変更される可能性がある場合、またはストレージ オブジェクトのコピー サービス操作の推定寿命が非常に長い場合は、より高い割合を使用してください。

削減する量を選択できない場合、どのような理由が考えられますか?

リザーブ容量は、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化されている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。

各メンバー ボリュームに予約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イメージに影響を及ぼすことなく、ホスト アプリケーションによる変更をベース ボリュームに保存するための独自のリザーブ容量が必要です。リザーブ容量によって、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可能となります。

整合性グループSnapshotイメージにホストが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、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可能となります。

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

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

詳細な統計情報は、すべての SSD 統計情報を `.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。統計データを検討・解釈する際には、複数の統計データを組み合わせて解釈している場合もあることを念頭に置いてください。

一般統計

SSDキャッシュの統計情報を表示するには、メニューの「ストレージ」→「プールとボリュームグループ」を選択してください。統計情報を表示したいSSDキャッシュを選択し、メニューの「詳細」→「統計情報の表示」を選択します。公称統計情報は、「SSDキャッシュ統計情報の表示」ダイアログに表示されます。

次のリストは、詳細統計のサブセットである、一般統計の一覧です。

一般統計	概要
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。
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、次のような理由が考えられます。 • 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。割り当てられている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場合があります。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。

一般統計	概要
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。キャッシュ利用率の割合は、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。この数値が100%より小さい理由は、SSDキャッシュの各割り当て単位（SSDキャッシュ ブロック）はサブブロックと呼ばれる小さい単位に分割され、サブブロックにはある程度独立してデータが格納されるためです。この数値は大きいほうが一般的には良いものの、小さい数値でもパフォーマンスが著しく向上する場合があります。

詳細統計

詳細統計は、名目統計に加えて、追加の統計で構成されます。これらの追加統計は、名目統計とともに保存されますが、名目統計とは異なり、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、統計を `.csv`ファイルに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、詳細な統計情報が名目統計情報の後にリストされていることがわかります：

詳細統計	概要
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。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、完全キャッシュ ヒットである処理に対してのみです。
部分ヒット	少なくとも1つのデータ ブロックはSSD Cacheに存在したが、すべてのデータ ブロックは存在しなかったホスト読み取りの回数。部分ヒットとは、ベース ボリュームからの読み取りが満たされたSSD Cache *ミス*のことです。
部分ヒット - ブロック	[部分キャッシュ 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]と比較して[部分キャッシュ ヒット]や[キャッシュ ミス]の数が多くなることが想定されます。

詳細統計	概要
ミス	SSDキャッシュ内にブロックがなかったホスト読み取りの数。SSDキャッシュ ミスは、ベース ボリュームから読み取りが行われた場合に発生します。SSDキャッシュのウォームアップ中は、[キャッシュ ヒット]と比較して[部分キャッシュ ヒット]や[キャッシュ ミス]の数が多くなることが想定されます。
ミス - ブロック	[キャッシュ ミス]のブロック数。
取り込み処理（ホスト読み取り）	ベース ボリュームからSSDキャッシュへデータがコピーされたホスト読み取りの数。
アクションの取得（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処理でキャッシュに書き込まないキャッシュ設定の場合、[取り込み処理（ホスト書き込み）]の数がゼロになることがあります。
取り込み処理（ホスト書き込み）- ブロック	[取り込み処理（ホスト書き込み）]のブロック数。
無効化処理	データが無効化された、またはSSDキャッシュから削除された回数。キャッシュの無効化処理は、各ホスト書き込み要求、Forced Unit Access（FUA）によるホスト読み取り要求、確認要求、およびその他一部の状況で実行されます。
リサイクル処理	別のベース ボリュームや論理ブロック 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少ない必要があります。[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い場合は、SSDキャッシュでスラッシングが発生しています。キャッシュ容量を増やす必要があります。または、ワークロードがSSDキャッシュの使用に適していません。
使用可能バイト数	SSDキャッシュ内でこのコントローラによって使用可能なバイト数。
割り当てバイト数	このコントローラによってSSDキャッシュから割り当てられたバイト数。SSDキャッシュから割り当てられたバイトは、空の場合と、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削って確保され、この容量をボリュームの作成に使用することはできません。

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

[追加の最適化容量]スライダは、EF600およびEF300ストレージ システムでのみ使用できます。

ボリューム グループの最適化容量とは何ですか**?**

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

ボリューム グループに関連付けられているドライブの未割り当て容量は、ボリューム グループの空き容量（ボリュームで使用されていない容量）と、使用可能容量のうちの最適化容量として確保された容量で構成されます。この最適化容量は使用可能容量を削って確保され、この容量をボリュームの作成に使用することはできません。

ボリューム グループの作成時に、パフォーマンス、ドライブの寿命、使用可能容量のバランスに基づいて、推奨される最適化容量が決定されます。[ボリューム グループ設定]ダイアログの[追加の最適化容量]スライダを使用すると、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 システムでのみ使用できます。

リソース プロビジョニング対応とは何ですか**?**

リソース プロビジョニングは、EF300およびEF600ストレージ アレイで使用できる機能です。オンにすると、ボリュームはバックグラウンドで初期化されることなくただちに使用できる状態になります。

リソース プロビジョニング ボリュームは、SSDボリューム グループまたはプール内のシック ボリュームで、ボリュームの作成時にドライブ容量が割り当てられますが（ボリュームに割り当てられます）、ドライブブロックは割り当て解除（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保護の情報フィールドを初期化し、各RAIDストライプでデータおよびRAIDパリティを同じにするために、すべてのドライブ ブロックがバックグラウンドのボリューム初期化処理でマッピングまたは割り当てられます。リソース プロビジョニング ボリュームの場合、バックグラウンドの初期化は決まったタイミングでは実行されません。代わりに、RAIDストライプごとに、そのストライプ内のボリューム ブロックに対して最初の書き込みが行われたときに初期化されます。

リソース プロビジョニング ボリュームは、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ている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。リソース プロビジョニング ボリュームを作成すると、そのボリュームに割り当てられてい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、最大書き込みパフォーマ

ンスが向上します。どの程度向上するかは、ドライブのモデルや容量によって異なります。

現時点では、EF300CまたはEF600CストレージアレイではDULBEはサポートされていません。

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

リソース プロビジョニングは、EF300およびEF600ストレージ アレイで使用できる機能です。オンにすると、ボリュームはバックグラウンドで初期化されることなくただちに使用できる状態になります。

リソース プロビジョニング ボリュームは、SSDボリューム グループまたはプール内のシック ボリュームで、ボリュームの作成時にドライブ容量が割り当てられますが（ボリュームに割り当てられます）、ドライブ ブロックは割り当て解除（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保護の情報フィールドを初期化し、各RAIDストライプでデータおよびRAIDパリティを同じにするために、すべてのドライブ ブロックがバックグラウンドのボリューム初期化処理でマッピングまたは割り当てられます。リソース プロビジョニング ボリュームの場合、バックグラウンドの初期化は決まったタイミングでは実行されません。代わりに、RAIDストライプごとに、そのストライプ内のボリューム ブロックに対して最初の書き込みが行われたときに初期化されます。

リソース プロビジョニング ボリュームは、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ている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。リソース プロビジョニング ボリュームを作成すると、そのボリュームに割り当てられてい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、最大書き込みパフォーマンスが向上します。どの程度向上するかは、ドライブのモデルや容量によって異なります。

ドライブがDULBEをサポートしているシステムでは、リソース プロビジョニングはデフォルトで有効になっています。*Pools & Volume Groups*から、そのデフォルト設定を無効にすることができます。

現時点では、EF300CまたはEF600CストレージアレイではDULBEはサポートされていません。

ボリュームとワークロード

SANtricity System Managerのボリュームとワークロードについて学ぶ

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は、ワークロードを選択することで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。

ボリュームおよびワークロードとは何ですか?

_volume_は、ホストがアクセスするための特定の容量を持って作成される論理コンポーネントです。ボリュームは複数のドライブで構成される場合がありますが、ホストに対しては1つの論理コンポーネントとして表示されます。ボリュームが定義されたら、ワークロードに追加できます。_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あり、そのアプリケーション用にストレージを最適化するために使用できます。

詳細については、以下を参照してください。

- "ボリュームの機能"
- "ワークロードの仕組み"
- "ボリュームに関する用語"
- "ボリュームの容量割り当て方法"
- "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作成するにはどうすればよいですか?

まず、ワークロードを作成します。メニューの「ストレージ」→「ボリューム」を選択し、手順を案内するウィザードを開いてください。次に、プールまたはボリューム グループで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。

詳細については、以下を参照してください。

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

関連情報

ボリュームに関連する概念の詳細については、以下を参照してください。

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

概念

SANtricityソフトウェアにおける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。

ボリュームは、ストレージ アレイで使用可能なストレージ容量から作成します。ボリュームを使用すると、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、すばやく簡単にファイルにアクセスできるようにする方法に似ています。

ボリュームは、ホストから認識できる唯一のデータ レイヤです。SAN環境では、論理ユニット番号（LUN）にマッピングされたボリュームをホストから認識できます。LUNには、ストレージ アレイでサポートされる1つ以上のホスト アクセス プロトコル（FC、iSCSI、およびSAS）を使用してアクセス可能なユーザ データが保持されます。

プールとボリューム 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 — プールからボリュームを作成すると、_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_のいずれかとして作成できます。

> 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にはコマンドライン 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て、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ぐにすべてのストレージが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/EF600CおよびEF300/EF300Cストレージ システムは、シンプロビジョニングをサポートしていません。

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く独自の特性があります。このような特性の一部を次に示します。

- セグメント サイズ — セグメントとは、ストレージ アレイがストライプ（RAID グループ）内の次のドライブに移動する前に、ドライブに保存されるデータ量（キロバイト（KiB））のことです。セグメント サイズは、ボリューム グループの容量以下です。セグメント サイズは固定されており、プールの場合は変更できません。
- 容量 — プールまたはボリューム グループで使用可能な空き容量からボリュームを作成します。ボリュームを作成する前に、プールまたはボリューム グループがすでに存在し、ボリュームを作成するのに十分な空き容量がある必要があります。
- コントローラの所有権 — すべてのストレージ アレイは、1つまたは2つのコントローラを持つことができます。シングルコントローラ アレイでは、ボリュームのワークロードは単一のコントローラによって管理されます。デュアルコントローラ アレイでは、ボリュームにはボリュームを「所有」する優先コントローラ（AまたはB）があります。デュアルコントローラ構成では、ワークロードがコントローラ間で移動する際に発生するロード バランスの問題を修正するために、自動ロード バランシング機能を使用してボリュームの所有権が自動的に調整されます。自動ロード バランシングは、自動化されたI/Oアプリケーション ワークロード バランシングを提供し、ホストからの受信I/Oトラフィックが両方のコントローラ間で動的に管理およびバランスされることを保証します。
- ボリュームの割り当て — ボリュームを作成するとき、または後で、ホストにボリュームへのアクセス権を付与できます。すべてのホスト アクセスは、論理ユニット番号（LUN）を通じて管理されます。ホストはLUNを検出し、それらはボリュームに割り当てられます。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、ボリュームがすべてのホストから利用可能であることを確

認してください。

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が制限されている可能性があります。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。

- 説明的な名前 — ボリュームの名前は自由に決められますが、説明的な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て、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。

SANtricityソフトウェアにおけるワークロードの仕組み

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

ワークロードは、アプリケーションをサポートするストレージ オブジェクトです。ワークロード（インスタンス）はアプリケーションごとに1つ以上定義できます。一部のアプリケーションについては、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。

ボリュームを作成する際には、ワークロードの用途に関連するオプションを設定する必要があります。たとえば、Microsoft Exchange用のボリュームを作成する場合は、必要なメールボックスの数、メールボックスに必要とされる平均容量、およびデータベースのコピーをいくつ作成するかについて設定します。この情報に基づいてボリュームの構成が最適化されます。この構成は、必要に応じて編集することもできます。この手順は必要に応じてスキップできます。

ワークロードの種類

ワークロードには、アプリケーション固有とその他の2種類を作成できます。

- 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、システムは、アプリケーション ワークロードI/Oとアプリケーション インスタンスからのその他のトラフィックと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を推奨する場合があります。I/Oタイプ、セグメント サイズ、コントローラの所有権、読み取りおよび書き込みキャッシュなどのボリューム特性は、以下のアプリケーション タイプ向けに作成されたワークロードに対して自動的に推奨され、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™（Virtual Machine File Systemで使用するボリューム用）

    提示されたボリューム構成を確認し、[ボリュームの追加 / 編集]ダイアログ ボックスを使用して推奨されたボリュームや特性を必要に応じて編集、追加、削除することができます。
- その他（またはボリューム作成を具体的にサポートしていないアプリケーション）。その他のアプリケーション ワークロードではボリューム構成を使用します。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、またはストレージ アレイで使用する予定のアプリケーションに対してシステムに最適化機能が組み込まれていない場合は、ボリューム構成を手動で指定する必要があります。ボリ

ューム構成は、「ボリュームの追加/編集」ダイアログ ボックスを使用して手動で指定する必要があります。

アプリケーションとワークロードの表示

アプリケーションとワークロードを表示するには、SANtricity System Managerを起動します。System Managerのインターフェイスから、次の2つの方法でアプリケーション固有のワークロードに関連する情報を表示できます。

- ボリューム タイルの*Applications & Workloads*タブを選択すると、ストレージ アレイのボリュームがワークロードと、ワークロードに関連付けられているアプリケーションの種類ごとにグループ化されて表示されます。
- パフォーマンス タイルの*Applications & Workloads*タブを選択すると、論理オブジェクトのパフォーマンス メトリック（レイテンシ、IOPS、および MB）を表示できます。オブジェクトは、アプリケーションと関連するワークロードごとにグループ化されています。定期的にこのパフォーマンス データを収集することで、基準となる測定値を確立し、傾向を分析することができます。これは、I/O パフォーマンスに関連する問題を調査する際に役立ちます。

SANtricity ソフトウェアのボリューム用語について学ぶ

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	概要
割り当て容量	割り当てられた容量は、ボリュームの作成やコピー サービス操作に使用されます。 割り当て容量と報告容量は、シックボリュームの場合は同じですが、シンボリュームの場合は異なります。シックボリュームの場合、物理的に割り当てられるスペースは、ホストに報告されるスペースと等しくなります。シンボリュームの場合、報告容量とはホストに報告される容量であり、割り当て容量とは現在データ書き込み用に割り当てられているドライブ容量のことです。
Application	アプリケーションとは、SQL ServerやExchangeなどのソフトウェアのことです。各アプリケーションをサポートするために、1つ以上のワークロードを定義します。アプリケーションによっては、システムがストレージを最適化するボリューム構成を自動的に推奨します。ボリューム構成には、I/Oタイプ、セグメントサイズ、コントローラの所有権、読み取りキャッシュと書き込みキャッシュなどの特性が含まれます。
容量	容量とは、ボリュームに保存できるデータ量のことです。

期間	概要
コントローラ所有権	コントローラの所有権とは、ボリュームの所有コントローラ、つまりプライマリコントローラとして指定されるコントローラを定義するものです。ボリュームには、そのボリュームを「所有」する優先コントローラ（AまたはB）を設定できます。ボリュームの所有権は、ワークロードがコントローラ間で移動する際に発生する負荷バランスの問題を修正するために、自動負荷分散機能を使用して自動的に調整されます。自動負荷分散機能は、I/Oワークロードの自動的なバランス調整を提供し、ホストからの受信I/Oトラフィックが両方のコントローラ間で動的に管理およびバランス調整されることを保証します。
動的キャッシュ読み取りプリフェッチ	動的キャッシュ読み取りプリフェッチにより、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る際に、追加の連続データブロックをキャッシュにコピーすることができます。このキャッシュ機能により、将来のデータ要求がキャッシュから満たされ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にとって重要です。キャッシュにプリフェッチされるデータの速度と量は、ホストの読み取り速度とリクエストサイズに基づいて自動的に調整されます。ランダムアクセスでは、データがキャッシュにプリフェッチされることはありません。この機能は、読み取りキャッシュが無効になっている場合は適用されません。 シンボリュームの場合、動的キャッシュ読み取りプリフェッチは常に無効になっており、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、ボリュームを削除するか、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 グループ内の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	ホストとは、ストレージアレイ上のボリュームにI/Oを送信するサーバーのことです。
ホスト クラスタ	ホスト クラスタとは、ホストのグループのことです。ホスト クラスタを作成することで、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。

期間	概要
LUN	論理ユニット番号（LUN）とは、ホストがボリュームにアクセスするために使用するアドレス空間に割り当てられた番号のことです。ボリュームは、LUNの形式で容量としてホストに提示されます。 各ホストには独自のLUNアドレス スペースがあります。そのため、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、ドライブへの通常の読み取りまたは書き込み中に検出される前に、ドライブ メディア エラーを検出する方法を提供します。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、定義されたユーザー ボリューム内のすべてのデータと冗長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ドライブの集まりです。プールを使用して、ホストからアクセスできるボリュームを作成できます（ボリュームはプールまたはボリューム グループから作成します）。
プールまたはボリューム グループ容量	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、ボリュームの作成のほか、コピー サービス処理やストレージ オブジェクトのさまざまな容量ニーズに対処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	報告容量とは、ホストに報告され、ホストがアクセスできる容量のことです。 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です。シン ボリュームの場合、レポート容量はホストにレポートされる容量ですが、割り当て容量はデータの書き込み用として現在割り当てられているドライブ スペースの量です。
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。

期間	概要
ストライピング	ストライピングとは、ストレージアレイにデータを保存する方法の一つです。ストライピングとは、データの流れを一定のサイズ（「ブロックサイズ」と呼ばれる）のブロックに分割し、これらのブロックをドライブに1つずつ書き込む処理です。このデータ保存方法は、複数の物理ドライブにデータを分散して保存するために使用されます。ストライピングはRAID 0と同義であり、パリティなしでRAIDグループ内のすべてのドライブにデータを分散させます。
Volume	ボリュームとは、アプリケーション、データベース、ファイルシステムなどがデータを保存するコンテナのことです。これは、ホストがストレージアレイ上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をボリュームに割り当てる方法です。
ボリューム名	ボリューム名とは、ボリュームが作成された際に割り当てられる文字列のことです。デフォルトの名前を受け入れるか、ボリュームに保存されているデータの種類を示す、より分かりやすい名前を指定できます。
ボリューム グループ	ボリュームグループとは、共通の特性を持つボリュームを格納するコンテナのことです。ボリュームグループには、定義された容量とRAIDレベルがあります。ボリュームグループを使用すると、ホストからアクセス可能な1つまたは複数のボリュームを作成できます。（ボリュームは、ボリュームグループまたはプールから作成します。）
ワークロード	ワークロードは、アプリケーションをサポートするストレージ オブジェクトです。ワークロード（インスタンス）はアプリケーションごとに1つ以上定義できます。一部のアプリケーションについては、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	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。

期間	概要
バッテリなしの書き込みキャッシュ	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を継続します。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、自動で一時的にオフになります。

シン ボリュームに固有の用語

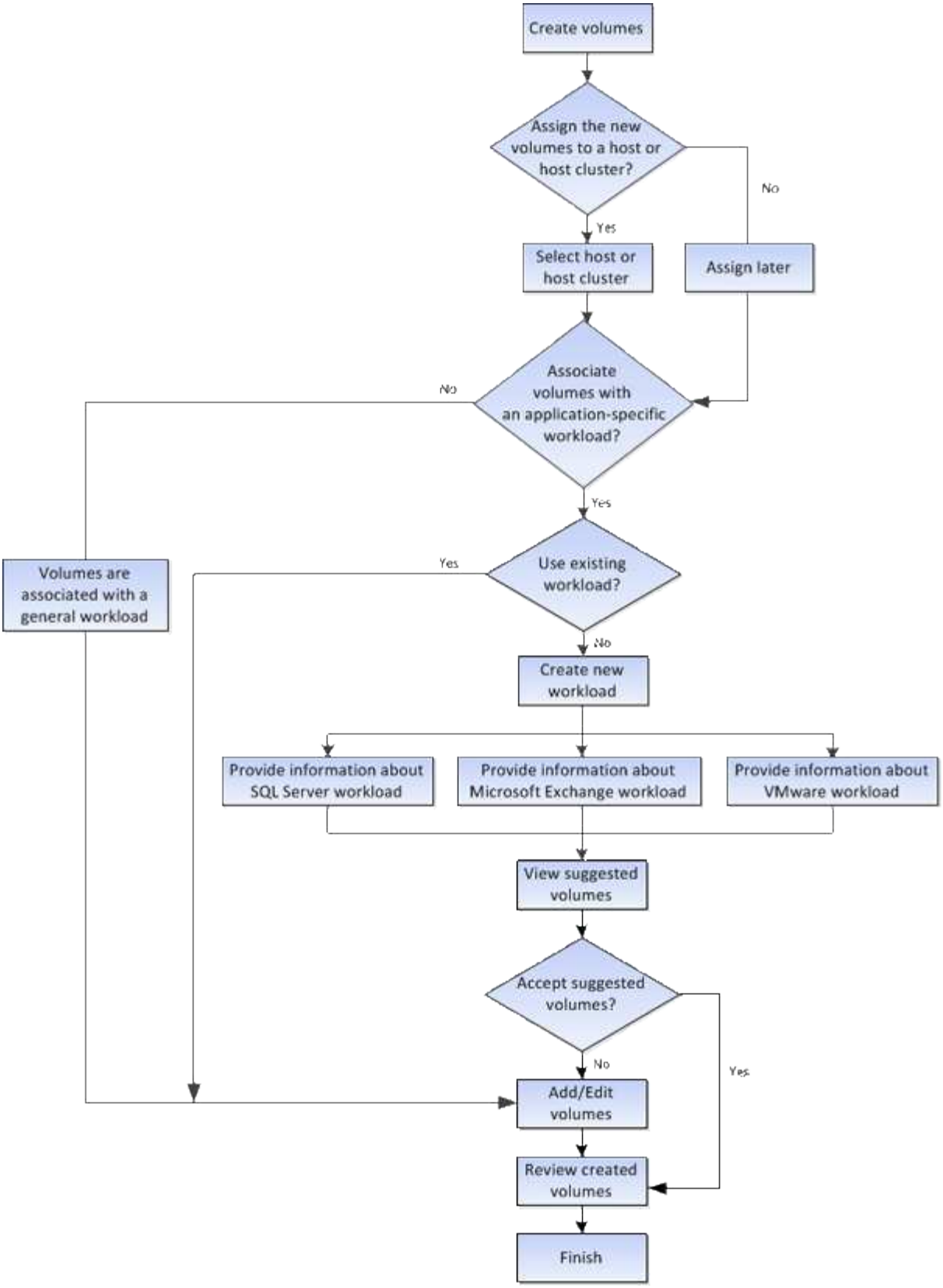
System Managerには、シン ボリュームを作成するオプションはありません。シン ボリュームを作成するにはコマンドライン インターフェイス（CLI）を使用します。

EF600/EF600CまたはEF300/EF300Cストレージシステムでは、シンボリュームは使用できません。

期間	概要
割り当て容量の制限	割り当て容量制限とは、シン ボリュームに割り当てられる物理容量がどれだけ大きくなることができるかの上限のことです。
書き込み済み容量	書き込み容量とは、シンボリューム用に割り当てられた予約容量のうち、実際に書き込まれた容量のことです。
警告しきい値	シンボリュームに割り当てられた容量が使用率（警告しきい値）に達したときに、警告しきい値アラートを発行するように設定できます。

SANtricity System Managerでのボリュームの作成方法

SANtricity System Managerでは、以下の手順に従ってボリュームを作成できます。



SANtricity ソフトウェアのボリュームのデータ整合性とデータセキュリティについて学ぶ

ボリュームを有効にすることで、データ保証（DA）機能とドライブセキュリティ機能を利用できるようになります。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表示されます。

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、この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が判断されます。破損している可能性があるデータはディスクに書き込まれず、ホストにも返されません。DA機能を使用する場合は、新しいボリュームの作成時にDA対応のプールまたはボリューム グループ（[候補]の表でDAが[はい]になっている）を選択します。

ドライブ セキュリティ

ドライブ セキュリティは、セキュリティ有効ドライブをストレージ アレイから取り外したときに、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

セキュリティ機能を備えたドライブ（FDEまたはFIPSのいずれか）は、書き込み時にデータを暗号化し、読み取り時にデータを復号化します。この暗号化および復号化は、パフォーマンスやユーザのワークフローに影響を与えません。各ドライブには独自の暗号化キーがあり、これはドライブから転送することは決してできません。

ボリューム レベルでのドライブ セキュリティの動作

セキュリティ機能を備えた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、それら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オプションを使用すると、ドライブおよび関連するボリュームグループとプールがセキュリティ_対応_になります。プールまたはボリュームグループには、セキュリティ機能を備えたドライブとセキュリティ機能を備えてい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には、すべてのドライブがセキュリティ機能を備えている必要があります。

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は、FDEドライブまたはFIPSドライブのいずれか、セキュリティ機能を備えたドライブを搭載してください。（FIPS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てください。ボリュームグループまたはプール内でFIPSドライブとFDEドライブを混在させると、すべてのドライブがFDEドライブとして扱われます。また、FDEドライブは、FIPS準拠のボリュームグループまたはプールに追加したり、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。これは、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かのいずれかを選択できます。外部キー管理の場合、キー管理サーバとの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のドライブセキュリティを有効にする：
    - プールまたはボリューム グループを作成します（候補テーブルの セキュリティ対応 列で はい を探してください）。

◦ 新しいボリュームを作成する際に、プールまたはボリュームグループを選択してください（プールおよびボリュームグループの候補テーブルで、*Secure-capable*の横に*Yes*が表示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を使用すると、ストレージアレイ内のセキュリティ対応ドライブとコントローラ間で共有されるセキュリティキーを作成できます。ドライブへの電源がオフオンされるたびに、セキュリティ対応ドライブは、コントローラがセキュリティキーを適用するまで、セキュリティロック状態になります。

SANtricityソフトウェアの**SSD**キャッシュとボリュームについて学ぶ

読み取り専用のパフォーマンスを向上する1つの方法として、SSDキャッシュにボリュームを追加できます。SSDキャッシュは、ストレージ アレイに論理的にグループ化した一連のソリッド ステート ディスク（SSD）ドライブで構成されます。

ボリューム

シンプルなボリュームI/Oメカニズムを使用して、SSD Cacheとの間でデータを移動します。データがSSDにキャッシュされて保存されると、その後のデータ読み取りはSSD Cache上で実行されるため、HDDボリュームにアクセスする必要がなくなります。

SSDキャッシュは、コントローラのダイナミック ランダム アクセス メモリ（DRAM）内のプライマリ キャッシュと併用されるセカンダリ キャッシュです。

- 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 Cacheでは、データはボリュームからコピーされ、SSD Cacheを作成する際に自動的に作成される2つの内部RAIDボリューム（コントローラごとに1つ）に保存されます。

内部RAIDボリュームは、内部キャッシュ処理の目的で使用されます。これらのボリュームは、ユーザーインターフェースからアクセスすることも表示することもできません。ただし、これら2つのボリュームは、ストレージアレイで許可されているボリュームの総数にカウントされます。

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が有効になっているボリュームでSSD Cacheを使用する場合、ボリュームとSSD Cacheのドライブセキュリティ機能が一致している必要があります。それらが一致しない場合、ボリュームはセキュリティ保護が有効になりません。

SANtricity System Managerでボリュームに対して実行できるアクション

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

容量の追加

ボリュームの容量を拡張するには、次の2つの方法があります：

- 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、メニューの Storage[Pools and Volume Groups > Add Capacity]を選択します。

- 割り当てられていない容量（未使用のドライブなど）を、ボリュームのプールまたはボリュームグループに追加します。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、このオプションを使用してください。

  割り当てられていない容量をプールまたはボリュームグループに追加するには、メニュー：Storage[Pools and Volume Groups > Add Capacity]を選択します。

  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、ボリュームの容量を増やすことはできません。まず、プールまたはボリュームグループのサイズを増やすか、使用されていない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

通常、ボリュームを削除するのは、誤ったパラメータや容量で作成されたボリューム、ストレージ構成のニーズを満たさなくなったボリューム、またはバックアップやアプリケーションテストに不要になったスナップショットイメージのボリュームの場合です。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加します。

ボリュームを削除すると、そのボリューム上のすべてのデータが失われます。ボリュームを削除すると、関連付けられているSnapshotイメージ、スケジュール、Snapshotボリュームもすべて削除され、ミラーリング関係もすべて解除されます。

コピー

ボリュームをコピーすると、同一ストレージアレイ上に、ソースボリュームとターゲットボリュームという2つの別々のボリュームのポイントインタイム コピーが作成されます。ボリュームをコピーするには、メニュー：Storage[Volumes > Copy Services > Copy volume]を選択します。

初期化

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

メニューから Storage [Volumes > More > Initialize volumes] を選択して、ボリュームを初期化できます。

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 パスに問題が生じた場合、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。

ホストのマルチパス ドライバのほとんどは、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により、ボリュームの所有権が代替コントローラに切り替わることがあります。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。

Storage › Volumes › More › Redistribute volumesを選択すると、ボリュームを再分配できます。

ボリューム所有権の変更

ボリュームの所有権を変更すると、そのボリュームの優先コントローラーの所有権も変更されます。ボリュームの優先コントローラー所有者は、メニュー：Storage（ボリューム > 設定の表示/編集 > 詳細タブ）に表示されます。

ボリュームの所有権を変更するには、メニューの Storage[Volumes > More > Change ownership] を選択します。

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によって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によって所有されます。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によって所有されるように、セカンダリ ボリュームの所有者が自動的に変更されます。プライマリ側の現在の所有権の変更は、セカンダリ側の対応する現在の所有権の変更に自動的に反映されます。

ミラー整合性グループにローカル セカンダリ ボリュームが含まれていて、コントローラの所有権が変更された場合、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。

ボリュームのコピーとボリューム所有権

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された時点で、両方のボリュームの優先コントローラが同じでない場合があります。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）。

キャッシュの設定の変更

キャッシュ メモリは、ドライブ メディアよりも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保持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：Storage[Volumes > More > Change cache settings]を選択して、次のキャッシュ設定を変更します：

- 読み取りおよび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。読み取り操作のデータは、以前の操作によってすでにキャッシュに格納されている可能性があり、ドライブにアクセスする必要がなくなります。データは、フラッシュされるまで読み取りキャッシュに保持されます。

  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。

- ミラーリングによる書き込みキャッシュ — ミラーリングによる書き込みキャッシュは、一方のコントローラのキャッシュメモリに書き込まれたデータが、もう一方のコントローラのキャッシュメモリにも書き込まれる場合に発生します。したがって、一方のコントローラが故障した場合でも、もう一方のコントローラが未完了の書き込み操作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になっており、かつ2つのコントローラが存在する場合にのみ利用可能です。ミラーリングによる書き込みキャッシュは、ボリューム作成時のデフォルト設定です。
- バッテリーなしでの書き込みキャッシュ — バッテリーなしでの書き込みキャッシュ設定により、バッテリーが欠落している、故障している、完全に放電している、または完全に充電されていない場合でも、書き込みキャッシュを継続できます。バッテリーなしでの書き込みキャッシュを選択することは、電源が切れた場合にデータが失われる可能性があるため、通常は推奨されません。通常、書き込みキャッシュは、バッテリーが充電されるか、故障したバッテリーが交換されるまで、コントローラによって一時的に無効になります。

  この設定は、書き込みキャッシュを有効にした場合にのみ利用可能です。この設定は、シンボリュームでは利用できません。

- ダイナミック読み取りキャッシュプリフェッチ — ダイナミックキャッシュ読み取りプリフェッチを使用すると、コントローラはドライブからキャッシュにデータブロックを読み取っている間に、追加の連続データブロックをキャッシュにコピーできます。このキャッシュ機能により、将来のデータ要求がキャッシュから満たされる可能性が高まります。ダイナミック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にとって重要です。キャッシュにプリフェッチされるデータの速度と量は、ホストの読み取り速度とリクエストサイズに基づいて自動的に調整されます。ランダムアクセスでは、データがキャッシュにプリフェッチされることはありません。この機能は、読み取りキャッシュが無効になっている場合は適用されません。

  シンボリュームの場合、動的キャッシュ読み取りプリフェッチは常に無効になっており、変更することはできません。

メディア スキャンの設定の変更

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、スキャンされ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。

メニューの Storage[Volumes > More > Change media scan settings] を選択すると、メディアスキャンを有効にして実行時間を設定できます。

ボリュームは、ストレージ アレイとボリュームの両方でメディア 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。ボリュームで冗長性チェックも有効になっていてボリュームに冗長性情報がある場合、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、ボリュームが作成されるとき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 エラーが検出された場合は、冗長性情報（使用可能な場合）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、あるいは最適なRAID 6ボリュームまたは1本のドライブだけで障害が発生した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 ログにそのデータ 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 ログに記録されます。

SANtricity System Managerでボリュームに容量を割り当てる方法

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、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ときは、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ときは、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、ホストにレポートされるスペースと同じになります。

  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、レポート容量はホストにレポートされる容量ですが、割り当て容量はデータの書き込み用として現在割り当てられているドライブ スペースの量です。

報告される容量は、ストレージアレイに割り当てられた容量よりも大きくなる可能性があります。シンボリュームは、現在利用可能な資産に関係なく、成長に対応できるように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がありません。シンボリュームを作成する場合は、コマンドラインインターフェイス（CLI）を使用してください。

シック 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によって決定されます。

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より大きい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、お使いのホスト オペレーティング システムのマニュアル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の向上と効率化に効果的です。シン ボリュームでは、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。

報告容量と割り当て容量に加えて、シンボリュームには書き込み容量も含まれます。書き込み容量とは、シンボリューム用に割り当てられた予約容量から書き込まれた容量です。

次の表は、シン ボリュームの容量制限を示しています。

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

シン ボリュームの場合、報告されている最大容量である256 TiBに達すると、その容量を増やすことはできません。シン ボリュームの予約容量が、報告されている最大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。

システムは、割り当てられた容量制限に基づいて、割り当てられた容量を自動的に拡張します。割り当てられた容量制限により、報告された容量を下回る範囲で、シンボリュームの自動的な増加を制限できます。書き込まれるデータ量が割り当て容量に近づいた場合、割り当て容量制限を変更できます。

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

System Managerはシンボリュームを作成する際に容量全体を割り当てないため、プール内に十分な空き容量が存在しない場合があります。空き容量が不足すると、シンボリュームだけでなく、プールの容量を必要とするその他の処理（Snapshotイメージやsnapshotボリュームなど）においても、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実行できます。このような状況が発生した場合、アラートしきい値の警告が表示されます。

SANtricityソフトウェアのシンボリューム監視について学ぶ

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容量よりも多くの論理領域を割り当てることができます。**Storage › Volumes › Thin Volume Monitoring**タブを選択すると、割り当てられた最大容量制限に達する前に、シンボリュームがどれだけ増加したかを監視できます。

Thin Monitoring ビューでは、以下の操作を実行できます：

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

シン ボリュームの容量を拡張するには、レポート容量を拡張してください。

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

> EF600/EF600CまたはEF300/EF300Cストレージシステムでは、シンボリュームは使用できません。

SANtricity ソフトウェアのシックボリュームとシンボリュームについて説明します

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にはコマンドライン インターフェイス（CLI）を使用します。

ボリューム タイプ	概要
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、一部のスペースが使用されず、ストレージ容量の利用率が下がる場合があります。 • 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、および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。スペースが十分でない場合、プールやボリューム 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であることが必要です。 • EF600/EF600CまたはEF300/EF300Cストレージシステムでは、シンボリュームは使用できません。 • シン ボリュームを作成するにはCLIを使用する必要があります。 • シック ボリュームとは異なり、シン ボリュームに必要なスペースは作成時には割り当てられず、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な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、したがって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（必要であれば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

SANtricity System Manager でワークロードを作成

あらゆるタイプのアプリケーションのワークロードを作成できます。

タスク概要

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。ワークロード（インスタンス）はアプリケーションごとに1つ以上定義できます。

手順

1. メニュー：Storage[Volumes]を選択します。
2. メニューの「作成[Workload]」を選択してください。

   [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. ワークロードを作成するアプリケーションのタイプをドロップダウン リストから選択し、ワークロードの名前を入力します。
4. *作成*をクリックします。

終了後の操作

作成したワークロードにストレージ容量を追加する準備が整いました。*Create Volume*オプションを使用して、アプリケーション用に1つまたは複数のボリュームを作成し、各ボリュームに特定の容量を割り当てます。

SANtricity System Manager でボリュームを作成する

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

タスク概要

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、ボリューム作成時に自動で構成方法が適用されるものもあります。たとえば、Microsoft Exchangeアプリケーション用のボリュームを作成する場合は、必要なメールボックスの数、メールボックスに必要とされる平均容量、およびデータベースのコピーをいくつ作成するかについて設定します。System Managerでは、この情報に基づいてボリュームの構成を最適化します。この構成は、必要に応じて編集することもできます。

ボリュームを作成するプロセスは複数の手順で構成されます。

手順**1**：ボリュームのホストを選択する

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

開始する前に

- [ホスト]タイルに有効なホストまたはホスト クラスタが表示されている必要があります。
- ホストに対してホスト ポート識別子を定義しておきます。
- 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。

タスク概要

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、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ホストまたはホスト クラスタは、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。
- ボリュームの作成にかかる時間を短くするために、ホストの割り当て手順を省略して、新しく作成されたボリュームをオフラインで初期化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. メニュー：Storage[Volumes]を選択します。
2. メニューの「Create[Volume]」を選択してください。

   [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シーケンスを続行するには、* Next * をクリックして、[手順2：ボリュームのワークロードを選択する]に進みます。

   [ワークロードの選択]ダイアログ ボックスが表示されます。

手順**2**：ボリュームのワークロードを選択する

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

タスク概要

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、システムは、アプリケーション ワークロード I/O とアプリケーションインスタンスからのその他のトラフィックと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を推奨する場合があります。推奨されるボリューム構成を確認したり、システム推奨のボリュームや特性を編集、追加、削除したりするには、（ボリュームの追加/編集）ダイアログボックスを使用できます。
- 「その他」のアプリケーション（またはボリューム作成を特にサポートしてい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には、*既存のワークロード用のボリュームを作成*オプションを選択します。
   - サポートされているアプリケーション、または「その他」のアプリケーションに対して新しいワークロードを定義するには、*新しいワークロードを作成する*オプションを選択します。
     - 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リストに表示されない場合は、いずれかの[その他]オプションを選択します。
     - 作成するワークロードの名前を入力します。
2. **Next** をクリックします。
3. ワークロードがサポートされている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てください。そうでない場合は、[手順3：ボリュームを追加または編集する]に進みます。

手順**3**：ボリュームを追加または編集する

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

開始する前に

- プールまたはボリューム グループに十分な空き容量が必要です。
- ボリューム グループに含めることができるボリュームは最大256個です。
- プールに含めることができるボリュームの最大数は、ストレージ システムのモデルに応じて次のとおりです。
  - 2,048ボリューム（EF600、EF600C、E5700シリーズ）
  - 1,024ボリューム（EF300およびEF300C）
  - 512ボリューム（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 グループの選択

DA対応ボリュームを作成する場合は、DA対応のプールまたはボリュームグループを選択してください（プールおよびボリュームグループの候補テーブルで「DA」の横に*Yes*と表示されているものを探してください）。

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 グループの選択

  セキュリティ対応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てください（プールおよびボリュームグループの候補テーブルで、「Secure-capable」の横に*Yes*と表示されているものを探してください）。

  ドライブセキュリティ機能は、System Managerではプールおよびボリュームグループレベルで表示されます。セキュリティ機能を備えたドライブは、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は、書き込み時にデータを暗号化し、読み取り時に固有の_暗号化キー_を使用してデータを復号化します。

  プールやボリューム 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）オプションのあるNVMeドライブである必要があります。

タスク概要

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。[ボリュームの追加 / 編集]ダイアログ ボックスには、ストレージ アレイ内で候補となるプールとボリューム グループがすべて表示されます。候補となる各プールおよびボリューム グループについて、利用できるドライブの数と合計空き容量が表示されます。

一部のアプリケーション固有のワークロードでは、各プールまたはボリューム グループについて、推奨されるボリューム構成に基づく容量が提示され、残りの空き容量（GiB）が表示されます。それ以外のワークロードの場合、プールまたはボリューム グループにボリュームを追加してレポート容量を指定した時点で容量が提示されます。

手順

1. [その他]とアプリケーション固有のワークロードのどちらを選択したかに基づいて、次のいずれかを実行します。

- その他 — 1つ以上のボリュームを作成するため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	概要
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、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なため、標準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。 プールの容量は、ドライブ タイプに応じて4GiBまたは8GiB単位で割り当てられます。4GiBまたは8GiBの倍数でない容量を割り当てることもできますが、倍数を超過した分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 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	概要
セグメント サイズ	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。 許可されるセグメントサイズ遷移 — System Managerは、許可されるセグメントサイズ遷移を決定します。現在のセグメントサイズから不適切な遷移となるセグメントサイズは、ドロップダウンリストに表示されません。許容される遷移サイズは通常、現在のセグメントサイズの2倍または半分です。たとえば、現在のボリュームセグメントのサイズが32 KiBの場合、新しいボリュームセグメントのサイズは16 KiBまたは64 KiBのいずれかにすることができます。 **SSD**キャッシュ対応ボリューム — SSDキャッシュ対応ボリュームには、4KiBのセグメント サイズを指定できます。4KiBのセグメント サイズを選択するのは、小ブロックのI/O処理（例：16KiB以下のI/Oブロック サイズ）を処理するSSDキャッシュ対応ボリュームに限ってください。大きなブロックのシーケンシャル処理を処理するSSDキャッシュ対応ボリュームのセグメント サイズとして4KiBを選択すると、パフォーマンスに影響が出る可能性があります。 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を変更するのにかかる時間は、以下の変数によって決まります： • ホストからのI/O負荷 • ボリュームの修正の優先順位 • ボリューム グループ内のドライブ数 • ドライブ チャネル数 • 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	プールまたはボリュームグループ内のドライブがセキュア対応の場合のみ、「セキュア対応」の横に*はい*が表示されます。 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。 プールやボリューム 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	概要
DA	「DA」の横に*Yes*が表示されるのは、プールまたはボリュームグループ内のドライブがData Assurance（DA）をサポートしている場合のみです。 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。また、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。
リソース プロビジョニング（EF300およびEF600のみ）	**Yes** が「Resource provisioned」の横に表示されるのは、ドライブがこのオプションをサポートしている場合のみです。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。オンにすると、ボリュームはバックグラウンドで初期化されることなくただちに使用できる状態になります。

- アプリケーション固有のワークロード — 選択したワークロードに対してシステムが推奨するボリュームと特性を受け入れる場合は*次へ*をクリックし、選択したワークロードに対してシステムが推奨するボリュームと特性を変更、追加、または削除する場合は*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	概要
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、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なため、標準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。 プールの容量は、ドライブ タイプに応じて4GiBまたは8GiB単位で割り当てられます。4GiBまたは8GiBの倍数でない容量を割り当てることもできますが、倍数を超過した分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 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	概要
セグメント サイズ	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。 許可されるセグメントサイズ遷移 — System Managerは、許可されるセグメントサイズ遷移を決定します。現在のセグメントサイズから不適切な遷移となるセグメントサイズは、ドロップダウンリストに表示されません。許容される遷移サイズは通常、現在のセグメントサイズの2倍または半分です。たとえば、現在のボリュームセグメントのサイズが32 KiBの場合、新しいボリュームセグメントのサイズは16 KiBまたは64 KiBのいずれかにすることができます。 **SSD**キャッシュ対応ボリューム — SSDキャッシュ対応ボリュームには、4KiBのセグメントサイズを指定できます。4KiBのセグメント サイズを選択するのは、小ブロックのI/O処理（例：16KiB以下のI/Oブロック サイズ）を処理するSSDキャッシュ対応ボリュームに限ってください。大きなブロックのシーケンシャル処理を処理するSSDキャッシュ対応ボリュームのセグメント サイズとして4KiBを選択すると、パフォーマンスに影響が出る可能性があります。 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を変更するのにかかる時間は、以下の変数によって決まります： • ホストからのI/O負荷 • ボリュームの修正の優先順位 • ボリューム グループ内のドライブ数 • ドライブ チャネル数 • 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が出ますが、データは引き続き利用可能です。

フィールド	概要
セキュリティ対応	プールまたはボリュームグループ内のドライブがセキュア対応の場合のみ、「セキュア対応」の横に*はい*が表示されます。 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。 プールやボリューム 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。
DA	「DA」の横に*Yes*が表示されるのは、プールまたはボリュームグループ内のドライブがData Assurance（DA）をサポートしている場合のみです。 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。また、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。
リソース プロビジョニング（EF300およびEF600のみ）	**Yes** が「Resource Provisioned」の横に表示されるのは、ドライブがこのオプションをサポートしている場合のみです。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。オンにすると、ボリュームはバックグラウンドで初期化されることなくただちに使用できる状態になります。

2. 選択したアプリケーションのボリューム作成シーケンスを続行するには、*次へ*をクリックして、[手順4：ボリュームの構成を確認する]に進みます。

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。変更する場合は、 * Back * をクリックします。
2. ボリューム設定に問題がなければ、*完了*をクリックしてください。

結果

System Managerによって選択したプールおよびボリューム グループに新しいボリュームが作成され、[すべてのボリューム]の表に新しいボリュームが表示されます。

終了後の操作

- 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、次にSMcliコマンド `-identifyDevices`を実行してボリューム名とホストストレージアレイ名を関連付けます。

  SMcliは、SANtricity System Managerから直接利用できます。このダウンロード可能なバージョンのSMcliは、E4000、EF600、EF600C、EF300、EF300C、E5700、EF570、E2800、およびEF280コントローラで利用できます。SANtricity System Manager内でSMcliをダウンロードするには、**Settings** > **System***および***Add-ons** > *Command Line Interface*を選択します。

SANtricity System Managerで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1つまたは複数のボリュームを、既存または新規のワークロードに追加することができます。

タスク概要

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. メニュー：Storage[Volumes]を選択します。
2. * Applications & Workloads * 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. **Add to Workload** 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 — このオプションを選択すると、既存のワークロードにボリュームを追加できます。

     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。選択した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する — このオプションを選択すると、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、新しいワークロードにボリュームを追加できます。
5. * Next * を選択して、ワークロードへの追加手順を続行してください。

   [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に問題がなければ、*完了*をクリックしてください。

ボリュームの管理

SANtricity System Managerでボリュームの容量を増やす

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

開始する前に

- ボリュームの関連付けられたプールまたはボリューム グループに十分な空き容量が必要です。
- ボリュームが最適状態で、変更中の状態ではないことが必要です。
- 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該当）。

ボリューム容量は一度に最大128TiBまで拡張できます。

タスク概要

このプールまたはボリューム グループで他のボリューム用に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 システム上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ません。

手順

1. メニュー：Storage[Volumes]を選択します。
2. 容量を増やしたいボリュームを選択し、次に*容量を増やす*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*Yes*を選択してください。

   [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. *Increase reported capacity by adding…*ボックスを使用して、現在報告されている利用可能な容量に容量を追加します。容量値の表示単位を、メビバイト（MiB）、ギビバイト（GiB）、またはテビバイト（TiB）のいずれかに変更できます。

5. * Increase * 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。
- メニューの「ホーム」→「進行中の操作を表示」を選択すると、選択したボリュームに対して現在実行中の容量増加操作の進行状況が表示されます。この処理には時間がかかり、システムのパフォーマンスに影響を与える可能性があります。

終了後の操作

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。

SANtricity System Managerでボリュームを初期化します

ボリュームは、最初に作成す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。

開始する前に

- すべてのI/O処理を停止しておく必要があります。
- 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。
- ボリュームが最適ステータスで、ボリューム上で変更処理が何も実行されていない必要があります。

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、この処理は行わないでください。この手順を開始する前に、テクニカル サポートに相談してください。

タスク概要

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、リザーブ容量の設定は保持されます。また、Data Assurance（DA）設定とセキュリティ設定も同じままです。

以下の種類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. メニュー：Storage[Volumes]を選択します。
2. いずれかのボリュームを選択し、次にメニューの「その他」[ボリュームの初期化]を選択します。

   「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 は以下の操作を実行します。

- 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）。

メニューの「ホーム」→「進行中の操作を表示」を選択すると、選択したボリュームに対して現在実行中の初期化操作の進行状況が表示されます。この処理には時間がかかり、システムのパフォーマンスに影響を与える可能性があります。

SANtricity System Managerでボリュームを再分配する

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 パスに問題が生じた場合、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。

開始する前に

- 再配置するボリュームが使用中では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。

  ホスト上にマルチパスドライバがない状態でボリュームを再配布する場合は、アプリケーションエラーを防ぐため、_再配布処理中は_ボリュームへのすべてのI/Oアクティビティを停止する必要があります。

タスク概要

ホストのマルチパス ドライバのほとんどは、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により、ボリュームの所有権が代替コントローラに切り替わることがあります。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. メニュー：Storage[Volumes]を選択します。
2. メニュー：More[Redistribute volumes]を選択します。

   [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は、選択したボリュームを優先コントローラの所有者に移動します。または、Redistribute Volumes Unnecessaryダイアログボックスが表示される場合があります。

SANtricity System Managerで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、ホスト アプリケーションのI/Oが新しいパス経由で転送されるようにすることができます。

開始する前に

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

タスク概要

プールまたはボリューム グループに含まれる1つまたは複数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. メニュー：Storage[Volumes]を選択します。
2. いずれかのボリュームを選択し、**More › Change ownership**を選択します。

   「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. *優先所有者*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、操作の実行を確認します。

結果

- System Managerは、ボリュームのコントローラ所有権を変更します。ボリュームへのI/Oは、このI/Oパスを経由して行われるようになりました。
- 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。この処理は通常、5分未満で完了します。

SANtricity System Managerでボリュームを削除する

通常、ボリュームを削除するのは、誤ったパラメータや容量で作成されたボリューム、ストレージ構成のニーズを満たさなくなったボリューム、またはバックアップやアプリケーション テストに不要になったスナップショットイメージのボリュームの場合です。

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。1つ以上のボリュームを選択して削除することができます。

開始する前に

ボリュームを削除する前に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ている。
- すべての入出力（I/O）が停止している。
- デバイスとファイルシステムがアンマウントされている。

タスク概要

次の状況に1つでも当てはま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。
- ボリュームでセグメント サイズの変更などの変更処理を実行中である（ボリュームの現在のステータスが「失敗」の場合は除く）。
- 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。

一定のサイズ（現在は128TB）を超えるボリュームに対してバックグラウンドで削除処理が実行されている場合、解放されたスペースをすぐに使用できるとはかぎりません。

手順

1. メニュー：Storage[Volumes]を選択します。
2. *削除*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*をクリックします。

結果

System Manager は以下の操作を実行します。

- 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すべて削除します。
- 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。

SANtricity System Managerでシンボリュームの割り当て容量制限を変更する

スペースをオンデマンドで割り当てることのできるシン ボリュームでは、シン ボリュームを自動的に拡張可能な（割り当て容量を制限する）上限を変更できます。

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[ホーム]ページの[通知]領域にアラート（警告しきい値の超過）が送信される割合を変更することもできます。このアラート通知を有効にするか無効にするかを選

択できます。

この機能は、EF600/EF600CまたはEF300/EF300Cストレージ システムではご利用いただけません。

システムは、割り当てられた容量制限に基づいて、割り当てられた容量を自動的に拡張します。割り当てられた容量制限により、報告された容量を下回る範囲で、シンボリュームの自動的な増加を制限できます。書き込まれるデータ量が割り当て容量に近づいた場合、割り当て容量制限を変更できます。

シン ボリュームの割り当て容量の上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. メニュー：Storage[Volumes]を選択します。
2. *Thin Volume Monitoring*タブを選択します。

   シンボリューム監視ビューが表示されます。

3. 変更するシンボリュームを選択し、*制限の変更*を選択します。

   [制限の変更]ダイアログ ボックスが表示されます。選択したシン ボリュームの割り当て容量の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、割り当て容量の上限と警告しきい値を変更します。

   フィールドの詳細

設定	概要
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*をクリックします。

設定の管理

SANtricity System Managerでボリュームの設定を変更します

ボリュームの名前や、ホストの割り当て、セグメント サイズ、修正の優先順位、キャッ

シュなど、ボリュームの設定を変更できます。

開始する前に

変更するボリュームのステータスは「最適」である必要があります。

ボリューム設定に対する変更の実行中は、一部の処理を使用できない場合があります。

手順

1. メニュー：Storage[Volumes]を選択します。
2. 変更するボリュームを選択し、*設定の表示/編集*を選択します。

   [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ダイアログ ボックスに表示されます。

3. ボリューム名とホスト割り当てを変更するには、*基本*タブを選択してください。

フィールドの詳細

設定	概要
Name	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です。シン ボリュームの場合、レポート容量はホストにレポートされる容量ですが、割り当て容量はデータの書き込み用として現在割り当てられているドライブ スペースの量です。
プール / ボリューム グループ	プールまたはボリューム グループの名前とRAIDレベルが表示されます。プールまたはボリューム グループがセキュリティ対応か、およびセキュリティ有効かが示されます。
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、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 クラスタを識別します。 • **LUN** — 論理ユニット番号（LUN）とは、ホストがボリュームにアクセスするために使用するアドレス空間に割り当てられた番号です。ボリュームは、LUNの形式で容量としてホストに提示されます。各ホストは独自のLUNアドレス空間を持ちます。したがって、同じLUNを異なるホストが使用して、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の範囲で設定できます。SCSIの論理ユニット番号（LUN）に相当します。

設定	概要
識別子	選択したボリュームの識別子が表示されます。 • **World-wide identifier**（**WWID**） — ボリュームの一意の16進数識別子。 • 拡張一意識別子（**EUI**） — ボリュームのEUI-64識別子。 • サブシステム識別子（**SSID**） — ボリュームのストレージ アレイ サブシステム識別子。

4. プール内またはボリュームグループ内のボリュームの追加構成設定を変更するには、*詳細設定*タブを選択します。

フィールドの詳細

設定	概要
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、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	データ保証を完全に無効にする — この設定は、ボリュームがデータ保証（DA）を有効にしている場合にのみ表示されます。DAは、コントローラからドライブへ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、修正します。このオプションを使用すると、選択したボリュームのDAを完全に無効にできます。無効にすると、このボリュームでDAを再度有効にすることはできません。 事前読み取り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。事前読み取り冗長性チェックは、読み取りが実行されるたびに、ボリューム上のデータが一貫しているかどうかを判断します。この機能が有効になっているボリュームは、コントローラファームウェアによってデータに一貫性がないと判断された場合、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、慎重に計画する必要があります。コントローラ間ですべてのI/Oができるだけ均等に分散される必要があります。

設定	概要
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。 許可されるセグメントサイズ遷移 — System Managerは、許可されるセグメントサイズ遷移を決定します。現在のセグメントサイズから不適切な遷移となるセグメントサイズは、ドロップダウンリストに表示されません。許容される遷移サイズは通常、現在のセグメントサイズの2倍または半分です。たとえば、現在のボリュームセグメントのサイズが32 KiBの場合、新しいボリュームセグメントのサイズは16 KiBまたは64 KiBのいずれかにすることができます。 **SSD**キャッシュ対応ボリューム — SSDキャッシュ対応ボリュームには、4KiBのセグメント サイズを指定できます。4KiBのセグメント サイズを選択するのは、小ブロックのI/O処理（例：16KiB以下のI/Oブロック サイズ）を処理するSSDキャッシュ対応ボリュームに限ってください。大きなブロックのシーケンシャル処理を処理するSSDキャッシュ対応ボリュームのセグメント サイズとして4KiBを選択すると、パフォーマンスに影響が出る可能性があります。 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を変更するのにかかる時間は、以下の変数によって決まります： • ホストからのI/O負荷 • ボリュームの修正の優先順位 • ボリューム グループ内のドライブ数 • ドライブ チャネル数 • 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が出ますが、データは引き続き利用可能です。
変更優先度	修正の優先順位に関する設定が表示されます（ボリューム グループ内のボリュームの場合のみ）。 修正の優先順位は、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。 優先順位レベルを選択するには、スライダ バーを動かします。 変更優先度 — 優先度を低く設定するとシステムのパフォーマンスが向上しますが、変更処理に時間がかかります。優先度を高く設定すると変更処理には有利ですが、システムのパフォーマンスが低下する可能性があります。
キャッシュ	キャッシング設定が表示されます。有効にすると、ボリュームの全体的なI/Oパフォーマンスが向上します。

設定	概要
SSD キャッシュ	SSD Cacheの設定を表示します。この設定は、互換性のあるボリュームで有効にすることで、読み取り専用パフォーマンスを向上させることができます。ボリュームは、同じDrive SecurityとData Assurance機能を共有している場合に互換性があります。 **SSD Cache**機能は、**1**つまたは複数の**Solid State Disk**（**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いため、アプリケーションのパフォーマンスが向上します。読み取りキャッシュはストレージアレイ内にあるため、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間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だけで、キャッシングは自動的かつ動的に実行されます。

5. *保存*をクリックします。

   System Managerは、ユーザーの選択に基づいてボリュームの設定を変更します。

終了後の操作

メニューの「ホーム」→「進行中の操作を表示」を選択すると、選択したボリュームに対して現在実行中の変更操作の進行状況が表示されます。

SANtricity System Managerでワークロード設定を変更します

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 タイプを表示できます。現在の名前が適切でない場合はワークロードの名前を変更します。

手順

1. メニュー：Storage[Volumes]を選択します。
2. * Applications & Workloads * 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、*設定の表示/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： ワークロードのユーザー指定名を変更します。
5. *保存*をクリックします。

SANtricity System Managerでボリュームのキャッシュ設定を変更します

読み取り / 書き込みキャッシュ設定を変更して、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。

タスク概要

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

- [キャッシュ設定の変更]ダイアログ ボックスを開いたあとに、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場合があります。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。

  一時停止は、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、あるいはコントローラでキャッシュ サイズの不一致が検出されたときに発生します。これら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 サポートに連絡してください。

- キャッシュ設定は、1つのボリュームまたはストレージ アレイ上の複数のボリュームに対して変更できます。すべての標準ボリュームまたはすべてのシン ボリューム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. メニュー：Storage[Volumes]を選択します。
2. いずれかのボリュームを選択し、次にその他 › キャッシュ設定の変更を選択します。

   「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. 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するには、*Basic*タブを選択します。

   フィールドの詳細

キャッシュ設定	概要
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。 ボリュームの*Write caching*が無効になると、キャッシュは自動的にフラッシュされます。

4. シックボリュームの詳細設定を変更するには、*詳細設定*タブを選択します。高度なキャッシュ設定は、シックボリュームでのみ使用できます。

フィールドの詳細

キャッシュ設定	概要
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る際に、追加の連続データブロックをキャッシュにコピーすることができます。このキャッシュ機能により、将来のデータ要求がキャッシュから満たされ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にとって重要です。キャッシュにプリフェッチされるデータの速度と量は、ホストの読み取り速度とリクエストサイズに基づいて自動的に調整されます。ランダムアクセスでは、データがキャッシュにプリフェッチされることはありません。この機能は、読み取りキャッシュが無効になっている場合は適用されません。 シンボリュームの場合、動的キャッシュ読み取りプリフェッチは常に無効になっており、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を継続します。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、自動で一時的にオフになります。 データ損失の可能性 — このオプションを選択し、保護用のユニバーサル電源がない場合、データが失われる可能性があります。さらに、コントローラバッテリがない状態で*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た場合にのみ利用可能です。この設定は、シンボリュームでは利用できません。
ミラーリングありの書き込みキャッシュ	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た場合にのみ利用可能です。この設定は、シンボリュームでは利用できません。

5. *保存*をクリックして、キャッシュ設定を変更します。

SANtricity System Managerで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。このオプションを使用して、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ことができます。

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、スキャンされ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 アレイとボリュームの両方でメディア 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。ボリュームで冗長性チェックも有効になっていてボリュームに冗長性情報がある場合、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、ボリュームが作成されるとき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 エラーが検出された場合は、冗長性情報（使用可能な場合）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、あるいは最適なRAID 6ボリュームまたは1本のドライブだけで障害が発生した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 ログにそのデータ 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 ログに記録されます。

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。

タスク概要

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する
- ストレージ アレイ全体のスキャン期間を変更する
- 1つ以上のボリュームのメディア スキャンを有効または無効にする
- 1つ以上のボリュームの冗長性チェックを有効または無効にする

手順

1. メニュー：Storage[Volumes]を選択します。
2. いずれかのボリュームを選択し、次にメニューの「その他」（More）［メディアスキャン設定の変更（Change media scan settings）］を選択します。

   [ドライブ メディア スキャン設定の変更]ダイアログ ボックスが表示されます。ストレージ アレイ上のすべてのボリュームが、このダイアログ ボックスに表示されます。

3. メディアスキャンを有効にするには、*Scan media over the course of…*チェックボックスを選択します。

   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は、メディアスキャンを実行する対象として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を有効にします。冗長性チェックを実行したくない個々のボリュームがある場合は、*冗長性チェック*チェックボックスの選択を解除してください。

6. *保存*をクリックします。

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

コピー サービスの使用

SANtricity System Managerのコピーボリュームについて学ぶ

ボリューム コピー機能では、同じストレージ アレイに2つのボリューム（ソース ボリュームとターゲット ボリューム）を作成することで、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 コピーによるアクセスの向上

ボリュームのストレージ要件が変わった場合、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することができます。ボリューム コピー機能は、たとえば次のような場合に使用できます。

- 大容量ドライブにデータを移動する。
- データ転送速度が速いドライブに変更する。
- パフォーマンスの向上を図るため、新しいテクノロジを使用するドライブに変更する。
- シン ボリュームをシック ボリュームに変更する。

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と一致し、512または4Kのいずれかです。
- エミュレートされた**512**ブロックサイズ - ドライブは4Kですが、報告されるブロックサイズは512です。

シン ボリュームからシック ボリュームへの変更

シン ボリュームをシック ボリュームに変更する場合は、ボリューム コピー処理を使用してシン ボリュームのコピーを作成します。ボリューム コピー処理のターゲットは常にシック ボリュームです。

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

データのバックアップ

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することで、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ボリュームからのベース ボリュームのデータのリストア

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ボリューム上にボリューム データのコピーを作成し、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 ボリュームおよびターゲット ボリュームとして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	オンラインボリュームコピーソースボリューム	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]	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、シンボリュームの報告容量以上である必要があります。

[2] オンラインコピー操作が完了するまで、スナップショットボリュームコピーは使用できません。

[3] ソースボリュームがプライマリボリュームである場合、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なければなりません。

SANtricity ソフトウェアのコピーボリューム操作の種類について学ぶ

_オフライン_のボリュームのコピー操作または_オンライン_のボリュームのコピー操作を実行できます。オフライン操作では、ソースボリュームからデータを読み取り、ターゲットボリュームにコピーします。オンライン操作では、スナップショットボリュームをソースとして使用し、そのデータをターゲットボリュームにコピーします。

データの整合性を確保するために、どちらのタイプのボリューム コピー処理でも、ターゲット ボリュームに対するすべてのI/Oアクティビティが中断されます。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、このような中断処理が行われます。

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

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を発行しようとすると、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、読み取り要求の発行を試行する前に書き込み要求を発行します。コントローラは書き込み要求を拒否します。書き込み要求が拒否されたために、読み取り要求が発行されない可能性があります。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。 • この問題が発生するのを回避するために、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操作を開始すると、System Managerはベースボリュームのスナップショットイメージを作成し、ベースボリュームのスナップショットイメージとターゲットボリュームとの間にコピー関係を作成します。スナップショットイメージをソースボリュームとして使用することで、コピー処理中でもストレージアレイはソースボリュームへの書き込みを継続できます。

オンライン コピー処理中は、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 ボリュームは、ボリューム グループ内の標準ボリュームまたはプール内の標準ボリュームです。ターゲット ボリュームとして、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、特定の時間にボリュームに格納され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。

SANtricity System Managerで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。

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、そのデータが必要であればバックアップしておきます。

タスク概要

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

オンライン版

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 イメージの作成元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 ボリュームの間に設定されます。

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た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. メニュー：Storage[Volumes]を選択します。
2. ボリュームコピー操作のソースとして使用するボリュームを選択し、メニュー：Copy Services［Copy volume］を選択します。

   「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

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

5. オンラインコピーを作成するか、オフラインコピーを作成するかを選択してください。オンラインコピーを作成するには、**Keep source volume online during copy operation**チェックボックスを選択してください。
6. 次のいずれかを実行します。
   - _オンライン_コピー操作を実行するには、*次へ*をクリックして*容量の予約*ダイアログボックスに進みます。
   - _オフライン_コピー処理を実行するには、*完了*をクリックしてオフラインコピーを開始します。
7. オンラインコピーを作成することを選択した場合は、オンラインコピーのデータやその他の情報を保存するために必要な予約容量を設定し、*完了*をクリックしてオンラインコピーを開始します。

   ボリューム候補テーブルには、指定された予約容量をサポートする候補のみが表示されます。予約容量とは、あらゆるコピーサービス操作およびストレージオブジェクトに使用される、物理的に割り当てられた容量のことです。ホスト側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%であり、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量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 は、ソースボリュームからターゲットボリュームにすべてのデータをコピーします。Copy Volume 操作が完了すると、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。

終了後の操作

メニューの「ホーム」→「進行中の操作を表示」を選択すると、ボリュームのコピー処理の進行状況が表示されます。この処理には時間がかかり、システムのパフォーマンスに影響を与える可能性があります。

SANtricity System Managerで**Copy Volume**処理に対してアクションを実行する

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：Home[View Operations in Progress]を選択します。

   「進行中の操作」ダイアログボックスが表示されます。

2. 操作を実行したいコピーボリューム操作を見つけて、*Actions*列のリンクをクリックし、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	概要
終了	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。
優先度の変更	ステータスが実行中であるボリューム コピー処理の優先度を変更して、ボリューム コピー処理が完了する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。 *Clear*を選択する前に、この操作を実行するかどうかをよく確認してください。確認ダイアログは表示されません。

SANtricity System Managerのボリュームとワークロードの**FAQ**

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

ボリュームとは何ですか**?**

ボリュームとは、アプリケーション、データベース、ファイルシステムなどがデータを保存するコンテナのことです。これは、ホストがストレージアレイ上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で使用可能な容量から作成されます。ボリュームには、定義された容量があります。ボリュームは複数のドライブで構成される場合がありますが、ホストに対しては1つの論理コンポーネントとして表示されます。

ボリューム グループにボリュームの作成に十分な空き容量があるにもかかわらず、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つまたは複数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、ボリュームを削除するか、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 グループ内の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少なくとも1つの空き容量領域が検出されると、ホームページの通知領域に「空き容量を統合する」という推奨事項が表示されます。*空き容量を統合する*リンクをクリックしてダイアログボックスを開きます。
- また、メニューの「プールとボリューム グループ」[通常とは異なるタスク > 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を及ぼしますか**?**

ボリュームを作成する際には、ワークロードの用途を指定する必要があります。この情報に基づいてボリュームの構成が最適化されます。この構成は、必要に応じて編集することもできます。この手順は必要に応じてスキップできます。

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。ワークロード（インスタンス）はアプリケーションごとに1つ以上定義できます。一部のアプリケーションについては、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、システムは、アプリケーション ワークロードI/Oとアプリケーション インスタンスからのその他のトラフィック間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を推奨する場合があります。I/Oタイプ、セグメント サイズ、コントローラの所有権、読み取りおよび書き込みキャッシュなどのボリューム特性は、次のアプリケーション タイプ用に作成されたワークロードに対して自動的に推奨され、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™（Virtual Machine File Systemで使用するボリューム用）

  提示されたボリューム構成を確認し、[ボリュームの追加 / 編集]ダイアログ ボックスを使用して推奨されたボリュームや特性を必要に応じて編集、追加、削除することができます。

- その他（またはボリューム作成を特にサポートしていないアプリケーション）-- その他のアプリケーション ワークロードではボリューム構成が使用されます。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、またはストレージ アレイで使用する予定のアプリケーションに対して組み込みの最適化がない場合、ボリューム構成を手動で指定する必要があります。ボリューム構成は、「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利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を完了する前に、推奨されるボリューム構成を確認し、[ボリュームの追加/編集]ダイアログ ボックスを使用して、システムが推奨するボリュームと特性を編集、追加、または削除できます。

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いいですか?

ボリュームの容量を拡張した場合は、その拡張した容量がホストによってすぐに認識されない可能性があります。

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、お使いのホスト オペレーティング システムのマニュアルを参照してください。

プールおよびボリューム 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 グループのステータスが最適でない。
- 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種類を把握しておく必要があります。アプリケーションが主にスモール 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 サイズを標準的なデータ ブロックのチャンク サイズより大きくすると、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ためで、ストレージ アレイのパフォーマンス向上にとって重要な要素です。

IOPSパフォーマンスが重視される環境

1秒あたりのI/O操作数（IOPS）環境において、ストレージアレイは、ドライブに読み書きされる一般的なデータ ブロック サイズ（「チャンク」）よりも大きいセグメント サイズを使用した場合、パフォーマンスが向上します。これにより、各チャンクが単一のドライブに書き込まれることが保証されます。

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速くなります。

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 コントローラとなる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、慎重に計画する必要があります。コントローラ間ですべてのI/Oができるだけ均等に分散される必要があります。

たとえば、一方のコントローラが主に大きなシーケンシャル 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、両者の負荷は大幅に異なります。各ボリュームに含まれているデータの種類を把握することで、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。

[ホストをあとで割り当てる]オプションはどのようなときに使用しますか?

ボリュームの作成にかかる時間を短くするために、ホストの割り当て手順を省略して、新しく作成されたボリュームをオフラインで初期化することができます。

新しく作成したボリュームは初期化する必要があります。新規ボリュームは、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で初期化されます。

ボリュームをホストにマッピングすると、同じボリューム グループ内の初期化中のボリュームはすべて強制的にバックグラウンドの初期化に切り替わります。バックグラウンドの初期化プロセスでは同時ホストI/Oが可能ですが、処理には時間がかかることがあります。

ボリューム グループ内のボリュームが1つもマッピングされていない場合、オフラインの初期化が実行されます。オフライン プロセスはバックグラウンド プロセスよりもはるかに高速です。

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

EF300およびEF600システムでは、ボリュームのブロック サイズ（「セクター サイズ」とも呼ばれます）を512バイトまたは4KiBに設定できます。ボリュームの作成時に正しい値を設定する必要があります。可能な場合は、適切な値がデフォルト値として提示されます。

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

- 一部のオペレーティング システムや仮想マシン（特に現時点ではVMware）は512バイトのブロック サイズを必要とし、4KiBをサポートしていないため、ボリュームを作成する前にホストの要件を確認してください。通常、ボリュームのブロック サイズを4KiBに設定することで最高のパフォーマンスが得られますが、ホストが4KiB（または「`4Kn`」）ブロックをサポートしていることを確認してください。
- サポートされるボリュームのブロック サイズは、次のように、プールまたはボリューム グループに対して選択するドライブのタイプによっても異なります。
  - 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、512バイト ブロックのボリュームのみを作成できます。
  - 4KiBブロックに書き込むドライブを使用してボリューム グループを作成する場合、512バイト ブロックまたは4KiBブロックのボリュームを作成できます。
- アレイにiSCSIホスト インターフェイス カードが搭載されている場合、ボリュームのブロックは（ボリューム グループのブロック サイズに関係なく）すべて512バイトに制限されます。これは、特定のハードウェアによる制限です。
- 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

SANtricity ソフトウェアのホストとホストクラスタについて学ぶ

ホストとホスト クラスタを設定して、ストレージ アレイとデータ サーバの間の接続を定義することができます。

ホストおよびホスト クラスタとは何ですか?

_ホスト_とは、ストレージ アレイ上のボリュームにI/Oを送信するサーバーのことです。_ホスト クラスタ_とは、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るホストのグループです。

詳細については、以下を参照してください。

- "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、メニューの「ストレージ」→「ホスト」を選択して、ホストを手動で設定します。2台以上のホストで同じボリュームセットへのアクセスを共有したい場合は、クラスタを定義し、ボリュームをそのクラスタに割り当てることができます。

詳細については、以下を参照してください。

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

関連情報

ホストに関連するタスクの詳細については、以下を参照してください。

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

概念

SANtricityソフトウェアのホスト用語について学ぶ

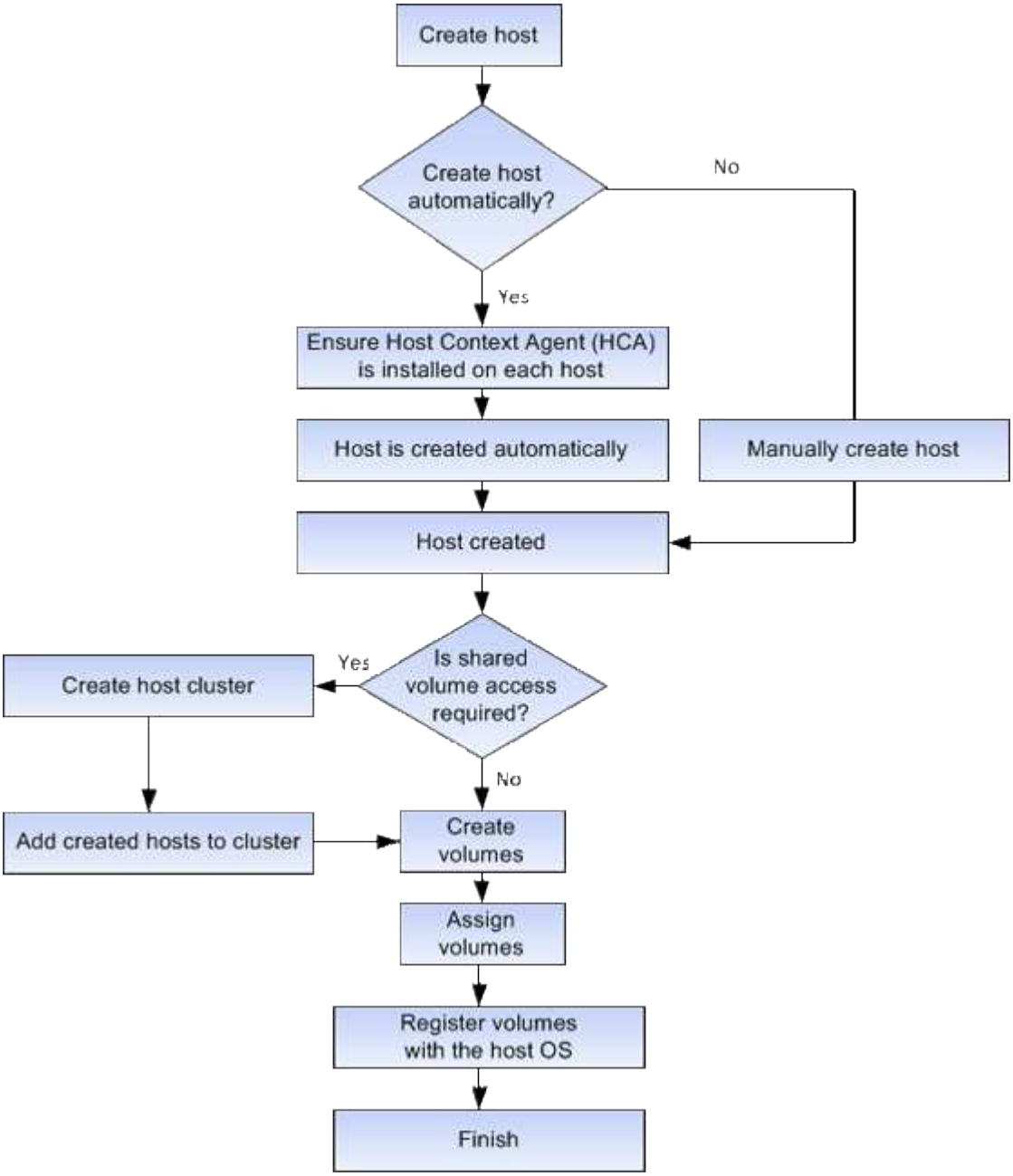
ストレージ アレイに関連するホストの用語を次に示します。

コンポーネント	定義
ホスト	ホストとは、ストレージアレイ上のボリュームにI/Oを送信するサーバーのことです。
ホスト名	ホスト名は、ホストのシステム名と同じである必要があります。
ホスト クラスタ	ホスト クラスタとは、ホストのグループのことです。ホスト クラスタを作成することで、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 プロトコルとは、コントローラとホスト間の接続（Fibre Channel、iSCSIなど）のことです。
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）はホストに設置されるボードで、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 ポート識別子とは、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、世界共通の一意の名前です。 • Internet Small Computer System Interface（iSCSI）ホスト ポート識別子は、1～233文字である必要があります。iSCSIホスト ポート識別子は、標準のIQN形式で表示されます（例： `iqn.xxx.com.xxx:8b3ad`）。 • iSCSI 以外のホスト ポート識別子（Fibre Channel や Serial Attached SCSI（SAS）など）は、2 文字ごとにコロンで区切られて表示されます（例： `xx:yy:zz`）。Fibre Channel ホスト ポート識別子は 16 文字である必要があります。
ホスト オペレーティング システム タイプ	ホスト オペレーティング システム タイプは、ストレージ アレイ内のコントローラがホストのオペレーティング システム（またはそのバリアント）に応じてI/Oにどのように反応するかを定義する構成設定です。これは略して_ホスト タイプ_と呼ばれることもあります。
コントローラのホスト ポート	コントローラ ホスト ポートとは、ホストへの物理的な接続を提供するコントローラ上のポートで、I/O処理に使用されます。

コンポーネント	定義
LUN	論理ユニット番号（LUN）とは、ホストがボリュームにアクセスするために使用するアドレス空間に割り当てられた番号のことです。ボリュームは、LUNの形式で容量としてホストに提示されます。 各ホストには独自のLUNアドレス スペースがあります。そのため、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。

SANtricity System Managerでのホストの作成とボリュームの割り当ての仕組み

次の図に、ホスト アクセスの設定方法を示します。



SANtricity System Managerでの手動ホスト作成について説明します

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。ホストは手動でのみ作成できます。

手動作成

ホストの手動作成では、ストレージ アレイ コントローラによって検出されたホスト 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、または手動で入力することによって関連付けを行います。ホストを作成したら、そのホストにボリュームを割り当てたり、ホスト クラスタにホストを追加したりできます（ボリュームへのアクセスを共有する場合）。

SANtricityソフトウェアでボリュームをホストおよびホストクラスタに割り当てる方法

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際にホストまたはホスト クラスタを選択することも、後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もできます。ホスト クラスタとは、ホストのグループのことです。ホスト クラスタを作成することで、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。

- スタンドアロン ホスト、ホスト クラスタの一部ではない — 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。このボリュームには、そのホスト1台のみがアクセスできます。
- 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々のホストにボリュームを割り当てることができます。ホストがホスト クラスタの一部であっても、ボリュームにアクセスできるのはそのホストのみであり、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。

SANtricity System Managerでボリュームにアクセスする

アクセス ボリュームは、ストレージ アレイの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 — アクセスボリュームは、ストレージアレイを管理するためのインバンド接続に使用されます。これは、コマンドラインインターフェイス（CLI）を使用してストレージアレイを管理している場合にのみ実行できます。

E4000、EF600/EF600C、またはEF300/EF300Cストレージ システムでは、Accessボリュームを使用したインバンド管理は利用できません。

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、その結果を表示すると、3つのボリュームが表示されます（Volume_1、Volume_2、Access）。

ホストを自動作成しない場合、あるいは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。

SANtricity ソフトウェアでの**LUN**の最大数について学ぶ

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 システムに応じて異なります。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。

SANtricityソフトウェアのデフォルトのホストオペレーティングシステムタイプについて説明します

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。ホスト タイプは、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。

接続されたホストに応じてストレージ アレイの動作を変更する必要がある場合は、ホスト タイプを変更することができます。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、ストレージ アレイに8台のホストを接続する場合、そのうち6台のオペレーティング システムがWindowsであれば、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[Windows]を選択する必要があります。

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

  たとえば、ストレージ アレイに8台のホストを接続する場合、そのうちの2台のオペレーティング システムがWindows、3台がVMware、残りの3台がLinuxであれば、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[工場出荷時のデフォルト]を選択する必要があります。

ホスト アクセスの設定

SANtricity System Managerでホストを手動で作成します

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。

タスク概要

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ます。
- 選択した名前がすでに使用されている場合、この処理は成功しません。
- 名前の最大文字数は30文字です。

手順

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

   [ホストの作成]ダイアログ ボックスが表示されます。

3. ホストの設定を必要に応じて選択します。

フィールドの詳細

設定	概要
Name	新しいホストの名前を入力します。
ホスト オペレーティング システム タイプ	新しいホストで実行しているオペレーティング システムをドロップダウン リストから選択します。
ホスト インターフェイス タイプ	（オプション）ストレージ アレイで複数のタイプのホスト インターフェイスがサポートされている場合、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 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、ユーティリティから（一度に1つずつ）* ホストポート * フィールドにコピー / ペーストすることができます。 ホストに関連付けるホストポート識別子は一度に1つずつ選択する必要がありますが、ホストに関連付ける識別子はいくつでも選択できます。各識別子は*Host ports*フィールドに表示されます。必要に応じて、識別子の横にある*X*を選択することで、その識別子を削除することもできます。

設定	概要
CHAPイニシエータ	（オプション）iSCSI IQN を持つホスト ポートを選択または手動で入力し、ストレージ アレイにアクセスしようとするホストにチャレンジ ハンドシェイク認証プロトコル（CHAP）を使用して認証を要求する場合は、*CHAP イニシエータ*チェックボックスを選択します。選択または手動で入力した各 iSCSI ホスト ポートについて、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 アレイに対して認証し、ストレージ アレイが自身をホストに対して認証する、双方向の認証）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。 • ホストの認証が必要ない場合は、このフィールドを空白のままにします。 現在、System Manager で使用されている唯一の iSCSI 認証方法は CHAP です。

4. *作成*をクリックします。

結果

ホストの作成が完了すると、ホストに対して設定された各ホスト ポートのデフォルト名（ユーザ ラベル）が作成されます。

デフォルトのエイリアスは<Hostname_Port Number>です。たとえば、最初に作成されたポートのデフォルトのエイリアスは `host IPT is IPT_1`です。

SANtricity System Managerでホストクラスタを作成します

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。

タスク概要

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 クラスタ内にNVMeホストとNVMe以外のホストを混在させることはできません。
- Data Assurance（DA）対応ボリュームを作成する場合は、使用するホスト接続でDAがサポートされている必要があります。

  ストレージ アレイのコントローラで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、この処理は成功しません。

- 名前の最大文字数は30文字です。

手順

1. メニュー：Storage[Hosts]を選択します。
2. メニューで Create[Host Cluster] を選択します。

   「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	概要
Name	新しいホスト クラスタの名前を入力します。
ボリューム アクセスを共有するホストを選択	ドロップダウン リストから2つ以上のホストを選択します。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*をクリックします。

   選択されたホストが、データ保証（DA）機能の異なるインターフェースタイプに接続されている場合、ホストクラスタでDAが利用できないことを示すメッセージが表示されたダイアログが表示されます。この問題により、DA対応ボリュームをホストクラスタに追加することができなくなります。*Yes*を選択して続行するか、*No*を選択してキャンセルします。

   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。

SANtricity System Manager でボリュームをホストに割り当てます

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。

タスク概要

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の場合、すべてのボリュームが作成されて初期化されるまで待ってからホストに割り当てると、ボリュームの初期化時間が短縮されます。ボリュームグループに関連付けられたボリュームがマッピングされると、_すべての_ボリュームはより低速な初期化方法に戻ることに注意してください。初期化の進行状況は、**Home › Operations in Progress**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。
- ボリュームが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る。

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 クラスタが存在しない。
- 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済みである。

このタスクの実行中に未割り当てのボリュームがすべて表示されますが、ホストが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：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。

   割り当て可能なすべてのボリュームを一覧表示するダイアログボックスが表示されます。任意の列を並べ替えたり、*Filter*ボックスに条件を入力したりすることで、特定のボリュームを簡単に見つけることができます。

3. 割り当てるボリュームごとに横にあるチェック 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、次の処理が行われます。

- 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。

ホストとクラスタの管理

SANtricity System Managerでデフォルトのホストタイプを変更する

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

タスク概要

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、ストレージ アレイに8台のホストを接続する場合、そのうち6台のオペレーティング システムがWindowsであれば、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[Windows]を選択する必要があります。

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

  たとえば、ストレージ アレイに8台のホストを接続する場合、そのうちの2台のオペレーティング システムがWindows、3台がVMware、残りの3台がLinuxであれば、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[工場出荷時のデフォルト]を選択する必要があります。

手順

1. メニュー：Settings[System]を選択します。
2. *追加設定*までスクロールダウンし、*既定のホストオペレーティングシステムの種類を変更する*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. **Change** をクリックします。

SANtricity System Managerでボリュームの割り当てを解除

ホストまたはホスト クラスタからボリュームへのI/Oアクセスが不要になった場合は、ホストまたはホスト クラスタからそのボリュームの割り当てを解除します。

タスク概要

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：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 ボックスをオンにするか、または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します。
4. *割り当て解除*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。

SANtricity System Managerでホストまたはホストクラスタを削除する

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。

タスク概要

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た他のすべてのホストまたはホスト ポート識別子には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：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、*削除*をクリックします。

   確認のダイアログ ボックスが表示されます。

3. 操作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（ある場合）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。

SANtricity System Managerでホスト接続レポートを設定

ホスト接続の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。

タスク概要

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：Settings[System]を選択します。
2. *追加設定*までスクロールダウンし、*ホスト接続レポートの有効化/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。
3. 続行するには*はい*をクリックしてください。

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

設定の管理

SANtricity System Managerでホストの設定を変更する

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：Storage[Hosts]を選択します。
2. 編集するホストを選択し、* View/Edit Settings * 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、*Properties*タブをクリックしてください。
4. 設定を適宜変更します。

フィールドの詳細

設定	概要
Name	ユーザが指定したホストの名前を変更できます。ホストの名前は必ず指定する必要があります。
関連付けられているホスト クラスタ	次のいずれかのオプションを選択できます。 • **None** — ホストはスタンドアロンホストのままです。ホストがホストクラスタに関連付けられていた場合、システムはそのホストをクラスタから削除します。 • **<Host Cluster>** — システムはホストを選択されたクラスタに関連付けます。
ホスト オペレーティング システム タイプ	定義したホストで実行されているオペレーティング システム タイプを変更できます。

5. *保存*をクリックします。

SANtricity System Managerでホストクラスタの設定を変更する

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、削除できます。

手順

1. メニュー：Storage[Hosts]を選択します。
2. 編集するホストクラスタを選択し、*設定の表示/編集*をクリックします。

   ダイアログ ボックスが表示され、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	概要
Name	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、*関連ホスト*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*をクリックします。

SANtricity System Managerで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。

タスク概要

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。

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

手順

1. メニュー：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、*設定の表示/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. *Host Ports*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	概要
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、ホストに新しいホストポート識別子を関連付けます。ホストポート識別子名の長さは、ホスト インターフェイステクノロジーによって決まります。Fibre ChannelおよびInfinibandのホストポート識別子名は16文字である必要があります。iSCSI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。 • 削除 — 削除を使用して、ホストポート識別子を削除（関連付けを解除）します。「削除」オプションでは、ホストポートが物理的に削除されるわけではありません。このオプションは、ホストポートとホスト間の関連付けを解除します。ホストバスアダプタまたはiSCSIイニシエータを取り外しない限り、ホストポートはコントローラによって認識されたままになります。 ホスト ポート識別子を削除すると、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（鉛筆マーク）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。既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、Challenge Handshake Authentication Protocol（CHAP）方式を使用し、初期リンク時にターゲットとイニシエータの身元を検証します。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*をクリックします。

SANtricity System Managerのホスト システムとホスト クラスタに関するよくある質問

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

ホストおよびホスト クラスタとは何ですか?

ホストとは、ストレージ アレイ上のボリュームにI/Oを送信するサーバーのことです。ホスト クラスタとは、ホストのグループのことです。ホスト クラスタを作成することで、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。個別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個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?

2台以上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。通常は、ボリュームへのアクセスを調整するために個々のホストに、クラスタリング ソフトウェアをインストールします。

適切なホスト 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?

[ホスト オペレーティング システム タイプ]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（最適である可能性の高い）オプションが最初に表示されます。リストに表示されたからといって、そのオプションが完全にサポートされているとはかぎりません

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

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 ソリューションと3.10以降のカーネルを使用するLinuxオペレーティング システムをサポートします。
VMware ESXi	VMware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 ソリューションを使用するLinuxオペレーティング システムをサポートします。
Linux（ATTO）	ATTO Technology, Inc.のマルチパス ドライバを使用するLinuxオペレーティング システムをサポートします。

ホスト オペレーティング システムのタイプ	オペレーティング システム（**OS**）とマルチパス ドライバ
Mac OS（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。
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。
IBM SVC	IBM SAN Volume Controller構成をサポートします。
工場出荷時のデフォルト	ストレージ アレイの初回起動用です。ホスト オペレーティング システム タイプが[工場出荷時のデフォルト]に設定されている場合は、接続されているホストで実行されているホスト オペレーティング システムとマルチパス ドライバに合わせて変更してください。
Linux DM-MP（カーネル3.9以前）	Device Mapper Multipathのフェイルオーバー ソリューションと3.9以前のカーネルを使用するLinuxオペレーティング システムをサポートします。
Windowsクラスタ（廃止）	ホスト オペレーティング システム タイプがこの値に設定されている場合は、代わりに[Windows（クラスタまたは非クラスタ）]設定を使用してください。

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）はホストに設置されるボードで、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場合に、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ホスト バス アダプタ（HBA）ユーティリティを使用して、ホストにインストールされている各HBAに関連付けられているホスト ポート識別子を特定する必要があります。

この情報が手元にある場合は、[ホストの作成]ダイアログに表示されるリストから、ストレージ アレイにログインしているホスト ポート識別子を選択します。

作成するホストに対応する正しいホスト 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、別のホストがこのデータにアクセスできるようにな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。

この処理は、System Managerを使用して、ホストの作成処理の一環として実行するか、または[設定の表示 / 編集]オプションで実行できます。

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

デフォルト クラスタとは何ですか?

デフォルト クラスタはシステム定義のエンティティです。ストレージ アレイにログインしたホスト ポート識別子がホストに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へのアクセスを許可されます。ホストに関連付けられていないホスト ポート識別子は、特定のホストに論理的に関連付けられていないが、ホストに物理的に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特定のアクセス権を持つようにする場合は、デフォルトのクラスタを使用しては いけません 。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、ホストの作成処理中に手動で実行できます。次に、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。

外部ストレージ環境が、ストレージアレイに接続されているすべてのホストとログインしているすべてのホストポート識別子に対して、ストレージアレイやユーザーインターフェイスにホストを明示的に認識させることなく、すべてのボリュームへのアクセスを許可する（全アクセスモード）ことに適している特別な状況で_のみ_、デフォルトのクラスタを使用してください。

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ユーザ インターフェイスに表示されて管理できるようになります。

ホスト接続レポートとは何ですか?

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

接続の中断は、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に発生します。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。

- ホスト冗長性が失われました — いずれ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 アレイでホストのタイプが正しく指定されていない場合に開きます。フェイルオーバーの問題が発生する可能性があります。

コントローラのリブートにかかる時間が接続タイムアウトよりも長くなる可能性がある場合は、ホスト接続レポートを無効にすることができます。この機能を無効にすると、Recovery Guruメッセージが生成されなくなります。

> ホスト接続レポートを無効にすると、コントローラ リソースの使用状況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び有効にしても、自動ロード バランシング機能は自動では有効になりません。

Snapshot 数

SANtricity System Managerのスナップショットについて学ぶ

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?

_スナップショット イメージ_は、特定のポイントインタイムで取得されたボリューム データの論理コピーです。リストア ポイントと同様に、スナップショット イメージを使用すると、既知の正常なデータ セットにロールバックできます。ホストはスナップショット イメージにアクセスできますが、直接読み書きすることはできません。

詳細については、以下を参照してください。

- "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Snapshot整合性グループ"
- "スナップショットボリューム"

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スナップショット整合性グループから、スナップショットイメージを手動で作成できます。この手順は、メニューからStorage[Snapshots]を選択して実行できます。

詳細については、以下を参照してください。

- "Snapshotの要件とガイドライン"
- "SnapshotイメージとSnapshotボリュームの作成ワークフロー"
- "Snapshotイメージの作成"
- "Snapshotイメージのスケジュール設定"
- "Snapshot整合性グループの作成"
- "Snapshotボリュームの作成"

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?

_ロールバック_とは、ベースボリューム内のデータを以前のポイントインタイムの状態に戻すプロセスです。**Storage › Snapshots**からスナップショットデータをロールバックできます。

詳細については、以下を参照してください。

- "Snapshotのロールバック"
- "ベース ボリュームのSnapshotイメージのロールバックの開始"

- "整合性グループ メンバーのSnapshotイメージのロールバックの開始"

関連情報

Snapshotに関連するタスクの詳細については、以下を参照してください。

- "Snapshotボリュームのリザーブ容量の変更"
- "Snapshotグループのリザーブ容量の変更"

概念

SANtricityソフトウェアにおけるスナップショットストレージの仕組み

Snapshot機能は、copy-on-write（COW）テクノロジを使用してSnapshotイメージを保存し、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

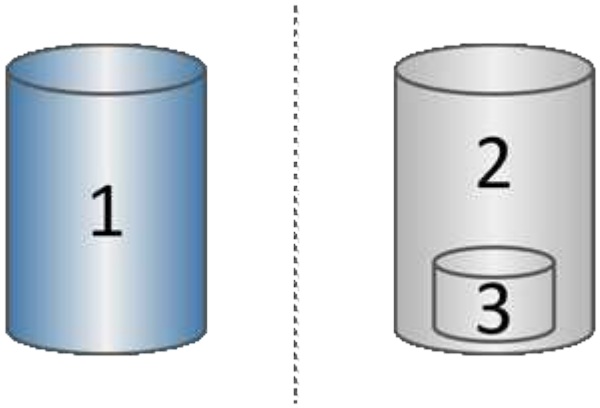
Snapshotイメージは、特定の時点でキャプチャされた、ボリュームの内容の論理的な読み取り専用コピーです。Snapshotはデータ損失からの保護に使用できます。

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って、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イメージに対する書き込み権限がないため、Snapshotは常に安全なバックアップ リソースです。

Snapshotの作成

Snapshotが作成される際、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まれる前に元のデータがリザーブ容量にコピーされます。
- 以降のSnapshotには変更されたデータ ブロックのみが含まれます。ベース ボリュームのデータが上書きされる前に、Snapshot機能は、copy-on-writeテクノロジを使用して影響を受けるセクターの必要なイメージをSnapshotのリザーブ容量に保存します。



[1] ベースボリューム（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] 予約済み容量（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変更前のデータ 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。一般的に、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。

- **Snapshot volume** — 削除されたファイルを復元する必要がある場合は、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、それをホストに割り当てます。
- スナップショット イメージ — ベースボリュームを特定のポイントインタイムに復元する必要がある場合は、以前のスナップショット 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。

SANtricityソフトウェアのSnapshotの用語について学ぶ

ストレージ アレイに関連するSnapshotの用語を次に示します。

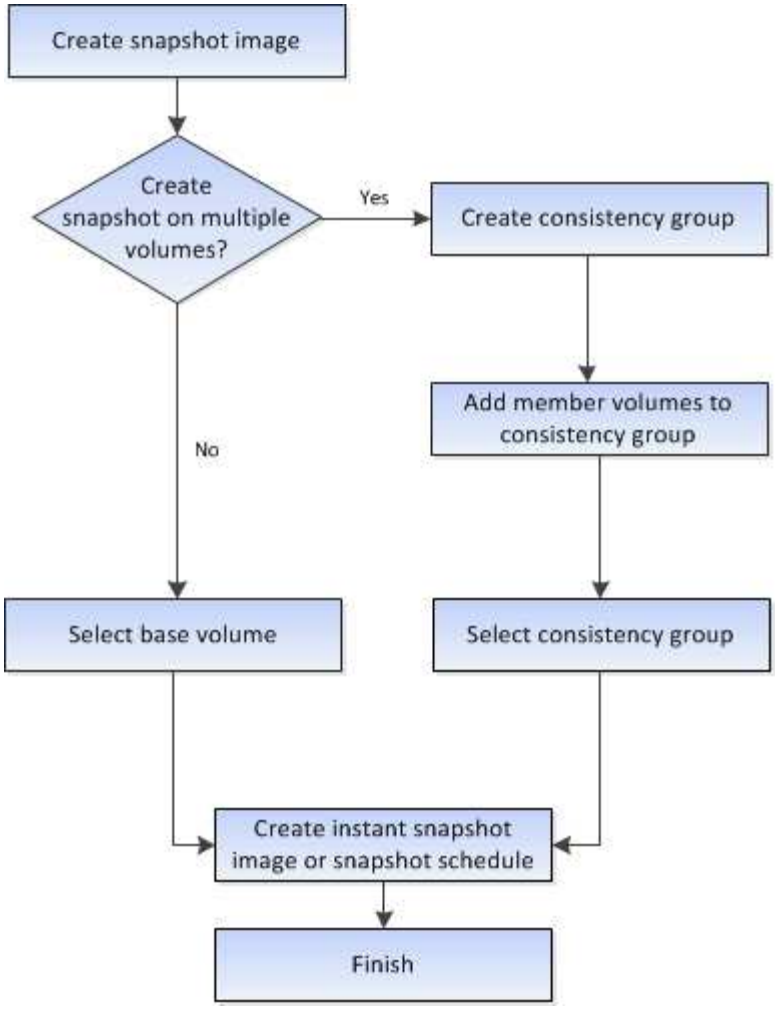
期間	概要
Snapshot機能	Snapshot機能は、ボリュームのイメージを作成および管理するために使用されます。
Snapshot イメージ	スナップショットイメージは、特定のポイントインタイムで取得されたボリュームデータの論理的なコピーです。復元ポイントと同様に、スナップショットイメージを使用すると、既知の正常なデータセットにロールバックできます。ホストはスナップショットイメージにアクセスできますが、直接読み書きすることはできません。
ベース ボリューム	ベースボリュームは、Snapshotイメージの作成元です。シックボリュームまたはシンボリュームのいずれかで、通常はホストに割り当てられます。ベースボリュームは、ボリュームグループまたはディスクプールのいずれかに配置できます。
Snapshot ボリューム	スナップショットボリュームを使用すると、ホストはスナップショットイメージ内のデータにアクセスできます。スナップショットボリュームには独自の予約容量があり、ベースボリュームへの変更を元のスナップショットイメージに影響を与えることなく保存します。
Snapshot グループ	スナップショットグループとは、単一のベースボリュームから抽出されたスナップショットイメージの集合です。
リザーブ容量ボリューム	予約容量ボリュームは、ベースボリュームのどのデータブロックが上書きされたか、およびそれらのブロックの保持されたコンテンツを追跡します。

期間	概要
Snapshotスケジュール	Snapshotスケジュールは、自動化されたSnapshotイメージを作成するためのスケジュール表です。スケジュールを通じて、イメージ作成の頻度を制御できます。
Snapshot整合性グループ	スナップショット整合性グループとは、スナップショットイメージを作成する際に単一のエンティティとして扱われるボリュームの集合です。これらの各ボリュームにはそれぞれ独自のスナップショットイメージがありますが、すべてのイメージは同じ時点で作成されます。
Snapshot整合性グループ メンバー ボリューム	スナップショット整合性グループに属する各ボリュームは、メンバーボリュームと呼ばれます。スナップショット整合性グループにボリュームを追加すると、System Managerは自動的に、そのメンバーボリュームに対応する新しいスナップショットグループを作成します。
ロールバック	ロールバックとは、ベースボリューム内のデータを以前のポイントインタイムに戻すプロセスです。
リザーブ容量	予約容量とは、あらゆるコピーサービス操作およびストレージオブジェクトに使用される、物理的に割り当てられた容量のことです。ホストから直接読み取ることはできません。

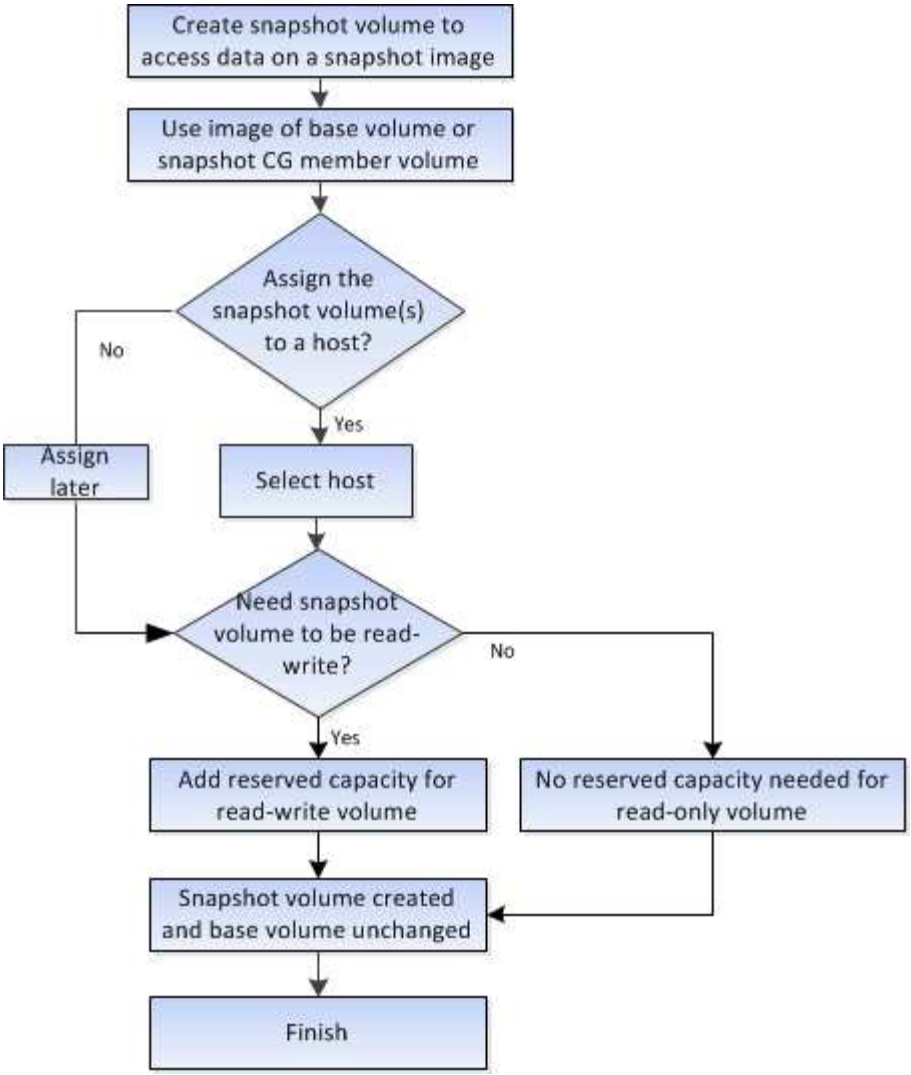
SANtricity System Managerでスナップショット イメージとスナップショット ボリュームを作成する方法

SANtricity System Managerでは、以下の手順に従ってSnapshotイメージとSnapshotボリュームを作成できます。

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



SANtricity System Managerのスナップショットの要件とガイドライン

Snapshotを作成して使用する場合は、以下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、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。

  スナップショットグループは、Pools & Volume Groupsページから表示できます。

- 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ボリュームや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イメージに再度関連付けることができます。

Snapshot整合性グループ

- Snapshot整合性グループには、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グループを個々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、大量のSnapshotイメージが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

次の条件に該当する場合は、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イメージの作成が実行されます。

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進行中は、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イメージの削除
  - 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 Policy を変更します。
- 以下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増加）
  - ボリューム グループのRAIDレベルの変更
  - ボリュームのセグメント サイズの変更
- ベース ボリュームがボリューム コピー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。

SANtricity System Managerのベースボリューム、予約容量、スナップショットグループについて説明します

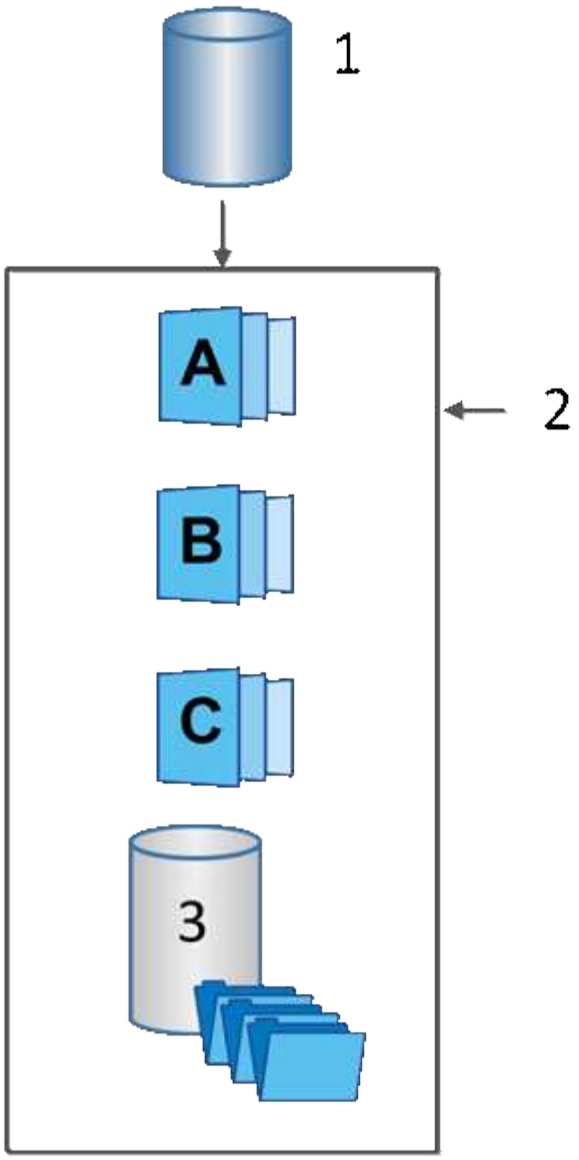
Snapshot機能は、ベース ボリューム、リザーブ容量、およびSnapshotグループを使用します。

ベース ボリューム

ベース ボリューム は、Snapshot イメージのソースとして使用されるボリュームです。ベース ボリュームには、シック ボリュームまたはシン ボリュームのいずれかを使用でき、プールまたはボリューム グループのいずれかに配置できます。

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。または、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] ベースボリューム、[2] グループ内のスナップショットオブジェクト（イメージと予約容量）、[3] スナップショットグループの予約容量。

リザーブ容量と**Snapshot**グループ

System Managerは、Snapshotイメージを_Snapshotグループ_に編成します。System ManagerがSnapshotグループを確立すると、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、関連する_リザーブ容量_が自動的に作成されます。

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できます。

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、以下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Snapshot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てください。Snapshotグループの制限値である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わなければならなくなります。

SANtricity System Managerの**Snapshot**スケジュールと**Snapshot**整合性グループについて説明します

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 — 単一のベースボリュームのSnapshotを自動化します。
- **Snapshot**整合性グループ — 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します。

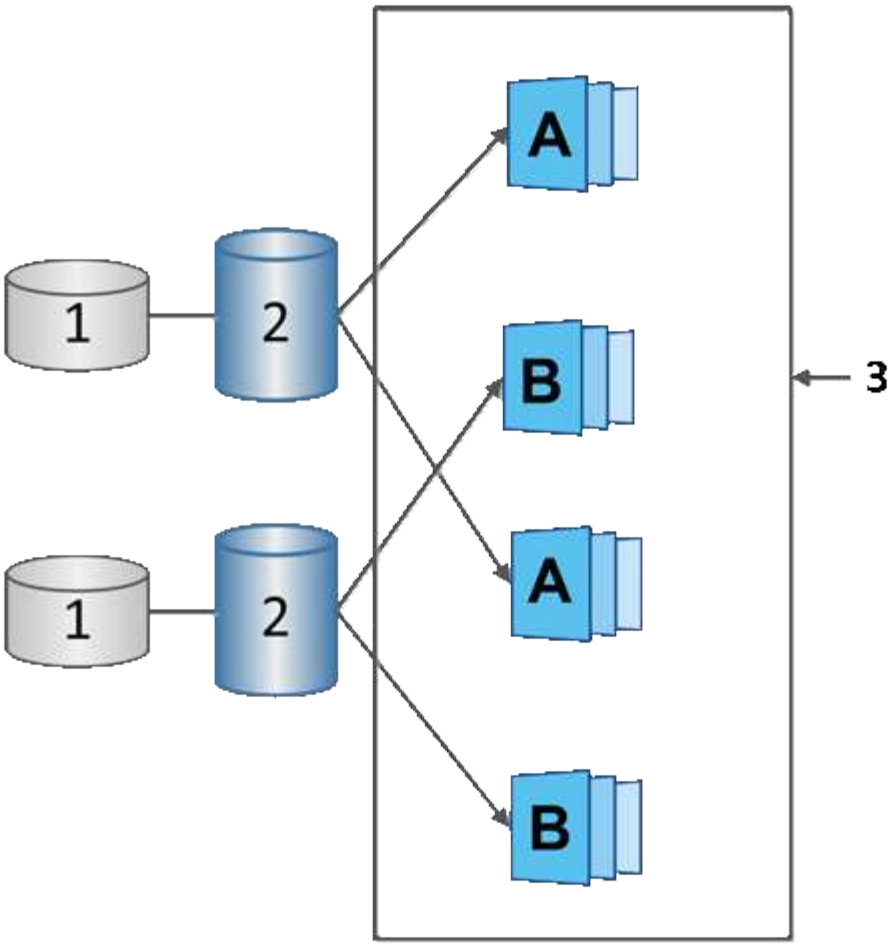
Snapshotスケジュール

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を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ら、追加のリザーブ容量を再利用できます。

Snapshot整合性グループ

複数のボリュームで同時にSnapshotイメージが作成されるようにする場合は、Snapshot整合性グループを作成します。Snapshotイメージの操作が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整合性グループは、複数のボリュームにまたがるアプリケーションに最適です（あるボリュームにログを格納して別のボリュームにデータベース ファイルを格納するデータベース アプリケーションなど）。

Snapshot整合性グループに含まれるボリュームはメンバー ボリュームと呼ばれます。整合性グループにボリュームを追加する場合は、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がSystem Managerによって自動的に作成されます。各メンバー ボリュームのSnapshotイメージを自動的に作成するスケジュールを定義できます。



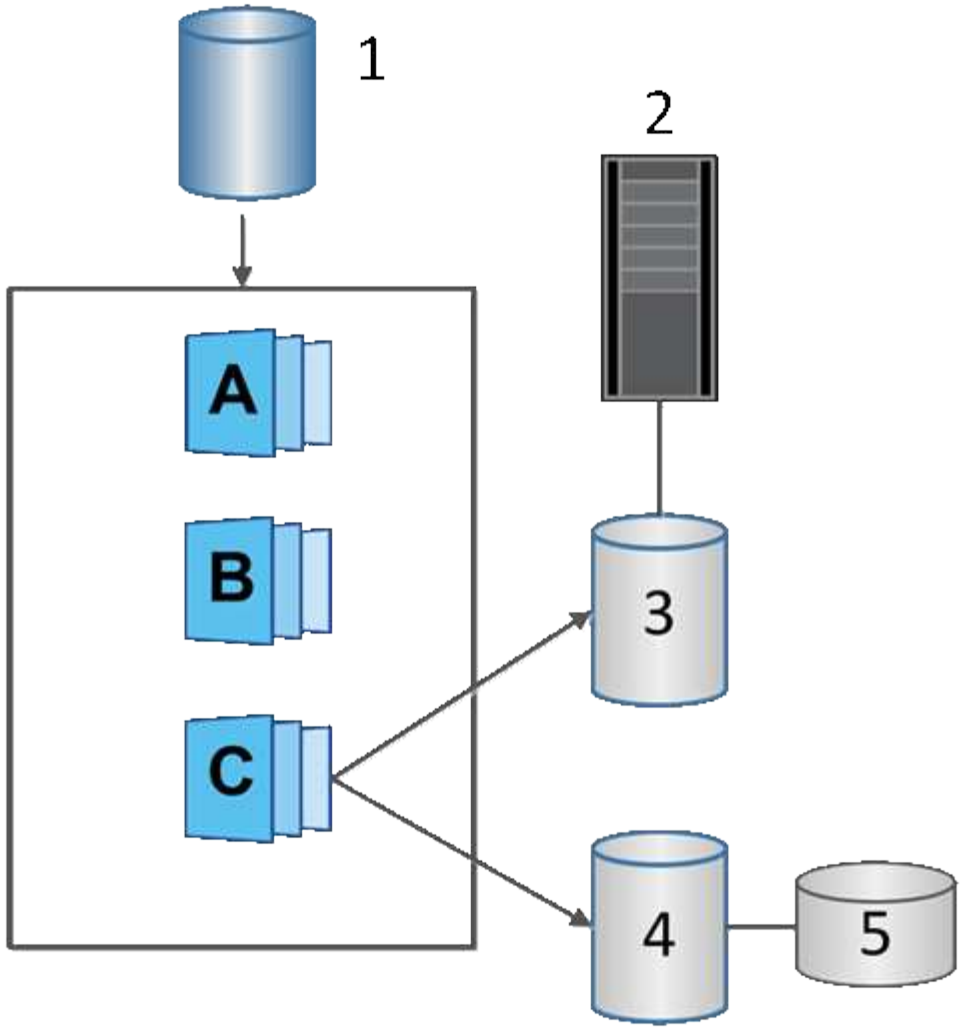
[1] 予約容量；[2] メンバーボリューム；[3] 整合性グループのSnapshotイメージ

SANtricityソフトウェアの**Snapshot**ボリュームについて学ぶ

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。

スナップショットボリュームを作成する際に、それを読み取り専用または_読み書き可能_として指定できます。

読み取り専用Snapshotボリュームを作成する場合、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] ベースボリューム；[2] ホスト；[3] 読み取り専用Snapshotボリューム；[4] 読み書き可能なSnapshotボリューム；[5] 予約済み容量

SANtricityソフトウェアのスナップショットロールバックについて学ぶ

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。

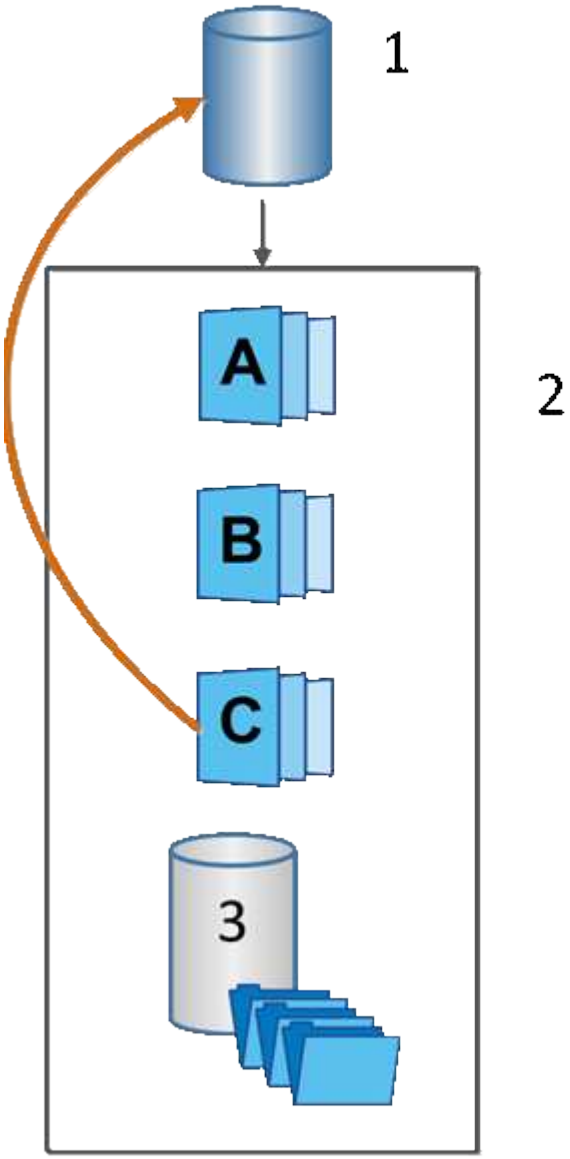
ロールバックでは、次のどちらかのソースからSnapshotイメージを選択できます。

- **Snapshot**イメージのロールバック：ベースボリュームの完全なリストア。
- *Snapshot整合性グループのロールバック*は、1つまたは複数のボリュームをロールバックするために使用できます。

ロールバック中は、グループに含まれるすべての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するため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はバックグラウンド処理として続行されます。



[1] ベースボリューム；[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Capacity

SnapshotおよびSnapshotオブジェクトの作成

SANtricity System Manager でスナップショットイメージを作成します

ベースボリュームまたはスナップショット整合性グループから、スナップショットイメージを手動で作成できます。これは_インスタントスナップショット_または_インスタントイメージ_とも呼ばれます。

開始する前に

- ベースボリュームは最適である必要があります。

- ドライブは最適である必要があります。
- スナップショットグループは「reserved.」として指定できません。
- リザーブ容量ボリュームのData Assurance（DA）の設定は、関連付けられた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イメージの作成に進みます。
   - メニュー：Storage[Volumes]を選択します。オブジェクト（ベースボリュームまたはスナップショット整合性グループ）を選択し、メニュー：Copy Services[Create instant snapshot]を選択します。
   - メニュー：Storage[Snapshots]を選択します。*Snapshot Images*タブを選択し、メニュー：Create[Instant snapshot]を選択します。

     「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スナップショット整合性グループ）を選択し、* Next * をクリックします。ボリュームまたはスナップショット整合性グループに対して以前にスナップショットイメージが作成されていた場合、システムは即座にインスタントスナップショットを作成します。それ以外の場合、ボリュームまたはスナップショット整合性グループに対してスナップショットイメージが初めて作成される場合は、「スナップショットイメージの作成の確認」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、予約容量が必要であるという通知を承認し、予約容量の手順に進みます。

   予備容量ダイアログボックスが表示されます。
3. スピナーボックスを使用して容量の割合を調整し、* Next * をクリックして、表でハイライト表示されている候補ボリュームを確定します。

   「設定の編集」ダイアログボックスが表示されます。
4. 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	概要
• スナップショット画像の設定 *	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選択したままにします。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した場合、Snapshotイメージが32個作成された時点で作成が停止します。	予約容量設定
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た場合、通知に基づいて、残りのスペースがなくなる前にリザーブ容量を増やしたり不要なオブジェクトを削除したりできます。
リザーブ容量がフルになったときの処理	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 — システムは、 Snapshot グループ内の最も古い Snapshot イメージを自動的にパージします。これにより、グループ内で再利用するために予約されていた Snapshot イメージの容量が解放されます。 • ベースボリュームへの書き込みを拒否 — 予約容量が定義された最大パーセンテージに達すると、システムは予約容量へのアクセスをトリガーしたベースボリュームへのI / O書き込み要求を拒否します。

結果

- System Manager は、新しいスナップショットイメージを Snapshot Images テーブルに表示します。このテーブルには、新しいイメージが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 Consistency Group 別に一覧表示されます。
- 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イメージの作成が実行されます。

SANtricity System ManagerでSnapshotイメージをスケジュールする

Snapshotスケジュールを作成し、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て、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を毎日、毎週、毎月、または任意の時刻に作成できます。

開始する前に

ベースボリュームは最適である必要があります。

タスク概要

このタスクでは、既存のSnapshot整合性グループまたはベース ボリュームのSnapshotスケジュールを作成する方法について説明します。

> ベース ボリュームまたはSnapshot整合性グループのSnapshotイメージの作成と同時にSnapshotスケジュールを作成することもできます。

手順

1. 次のいずれかの操作を実行してSnapshotスケジュールを作成します。
   - メニュー：Storage[Volumes]を選択します。

     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、メニューの「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：Storage[Snapshots]を選択します。

     *Schedules*タブを選択し、*Create*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、*次へ*をクリックします。

   「Snapshot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てください。*その他のオプションを表示*をクリックしてください。*スケジュールをインポート*をクリックし、インポートするスケジュールを含むオブジェクトを選択してから、*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、以下の表を参照してください。

フィールドの詳細

フィールド	概要
基本設定	期間を選択
Snapshotイメージの個々の曜日を選択します。	開始時間
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分後です。	タイムゾーン
お使いのアレイのタイム ゾーンをドロップダウン リストから選択します。	詳細設定
曜日 / 月	以下のいずれかのオプションを選択します： • 日次／週次 — 同期スナップショットを取得する日を個別に選択します。日次スケジュールを作成する場合は、右上の*すべての日を選択*チェックボックスを選択することもできます。 • 月次／年次 — 同期スナップショット用に個別の月を選択します。**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。複数の日はカンマまたはセミコロンで区切ることができます。連続する日付にはハイフンを使用します。例：1,3,4,10-15,Last。月次スケジュールが必要な場合は、右上の*Select all months*チェックボックスを選択することもできます。
開始時間	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分後です。
タイムゾーン	お使いのアレイのタイム ゾーンをドロップダウン リストから選択します。
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。1より大きい数を選択する場合は、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	概要
開始日/終了日または終了日なし	同期を開始する開始日を入力してください。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、*作成*をクリックして設定を確定し、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、*次へ*をクリックしてSnapshotイメージ用の予約容量を割り当てます。

     ボリューム候補テーブルには、指定された予約容量をサポートする候補のみが表示されます。予約容量とは、あらゆるコピーサービス操作およびストレージオブジェクトに使用される、物理的に割り当てられた容量のことです。ホスト側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、独自の予約容量設定を割り当ててください。

     デフォルトの予約容量設定を変更した場合は、* Refresh Candidates * をクリックして、指定した予約容量の候補リストを更新してください。

     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の設定はベース 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. **Next** 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Snapshot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	概要
Snapshot画像制限	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選択したままにします。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した場合、Snapshotイメージが32個作成された時点で作成が停止します。	予約容量設定
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上限に近付いたときにシステムが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た場合は、事前通知を使用して、残りのスペースを使い果たす前にリザーブ容量を拡張するか、不要なオブジェクトを削除します。
リザーブ容量がフルになったときの処理	次のいずれかのポリシーを選択します。 • 最も古い**Snapshot**イメージの削除 — システムは最も古いSnapshotイメージを自動的に削除し、Snapshotグループ内で再利用するために予約されていたSnapshotイメージの容量を解放します。 • ベースボリュームへの書き込みを拒否 — 予約容量が定義された最大パーセンテージに達すると、システムは予約容量へのアクセスをトリガーしたベースボリュームへのI / O書き込み要求を拒否します。

SANtricity System Manager でスナップショット整合性グループを作成します

一貫性のあるコピーを確保するには、複数のボリュームからなる_スナップショット整合性グループ_と呼ばれるセットを作成できます。

このグループを使用すると、一貫性を保つために、すべてのボリュームのスナップショットイメージを同時に作成できます。スナップショット整合性グループに属する各ボリュームは、_メンバーボリューム_と呼ばれます。スナップショット整合性グループにボリュームを追加すると、システムは自動的にそのメンバーボリュームに対応する新しいスナップショットグループを作成します。

タスク概要

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

量を割り当てます。

Snapshot整合性グループを作成するプロセスは複数の手順で構成されます。

ステップ1：Snapshot Consistency Group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。

開始する前に

メンバーボリュームは最適である必要があります。

手順

1. メニュー：Storage[Snapshots]を選択します。
2. * Snapshot Consistency Groups * タブをクリックします。
3. メニューを選択：Create[Snapshot consistency group]

   「 Snapshot Consistency Group 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1つ以上選択します。
5. * 次へ * をクリックして、ステップ2：Snapshotコンシステンシグループの容量を確保するに移動します。

ステップ2：Snapshotコンシステンシグループの容量を確保する

予約済みの容量をスナップショット整合性グループに関連付けます。System Managerは、スナップショット整合性グループのプロパティに基づいて、ボリュームと容量を提案します。推奨される予約容量構成を受け入れるか、割り当てられるストレージをカスタマイズすることができます。

タスク概要

予約容量ダイアログボックスのボリューム候補テーブルには、指定された予約容量をサポートする候補のみが表示されます。予約容量とは、あらゆるコピーサービス操作およびストレージオブジェクトに使用される、物理的に割り当てられた容量のことです。ホスト側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。
   - * デフォルト設定を受け入れます *。

     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、独自の予約容量設定を割り当ててください。

     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の設定はベース 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： デフォルトの予約容量設定を変更した場合は、*候補者を更新*をクリックして、指定した予約容量の候補者リストを更新してください。
3. * 次へ * をクリックして、ステップ3：Snapshotコンシステンシグループの設定を編集するに移動します。

ステップ3：Snapshotコンシステンシグループの設定を編集する

Snapshot整合性グループの自動削除に関する設定とリザーブ容量に関するアラートのしきい値を確認し、必要に応じて変更します。

タスク概要

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	概要
• Snapshot 整合性グループの設定 *	Name
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選択したままにします。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した場合、Snapshotイメージが32個作成された時点で作成が停止します。	予約容量設定
アラートの送信しきい値…	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の値をスピン ボックスを使用して調整します。 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	次のいずれかのポリシーを選択します。 • 最も古いスナップショットイメージの削除 — システムはスナップショット整合性グループ内で最も古いスナップショットイメージを自動的に削除し、グループ内で再利用するために予約されていたスナップショットイメージの容量を解放します。 • ベースボリュームへの書き込みを拒否 — 予約容量が定義された最大パーセンテージに達すると、システムは予約容量へのアクセスをトリガーしたベースボリュームへのI / O書き込み要求を拒否します。

2. スナップショットの整合性グループの設定に問題がなければ、* 完了 * をクリックします。

SANtricity System Manager でスナップショットボリュームを作成します

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するには、Snapshotボリュームを作成します。Snapshotボリュームは読み取

り専用または読み取り / 書き込みに指定できます。

タスク概要

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に対する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ます。

ステップ**1**：スナップショットボリュームのメンバーを確認する

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：Storage[Snapshots]を選択します。
2. * Snapshot Volumes * タブを選択します。
3. *Create*を選択します。

   「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. スナップショットボリュームに変換するスナップショットイメージ（ボリュームまたはスナップショット整合性グループ）を選択し、*次へ*をクリックします。*フィルター*フィールドにテキストを入力して、リストを絞り込んでください。

   Snapshot整合性グループのSnapshotイメージを選択した場合は、[メンバーの確認]ダイアログ ボックスが表示されます。

   「メンバーの確認」ダイアログボックスで、スナップショットボリュームへの変換対象として選択され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. [ステップ2：スナップショットボリュームをホストに割り当てる]へ移動。

ステップ**2**：スナップショット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。ホストの割り当ては、必要に応じてあとで実行することもできます。

開始する前に

- 有効なホストまたはホストクラスタが [ホスト] ページに存在します。

- ホストに対してホスト ポート識別子が定義されている必要があります。
- 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機能がサポートされていることを事前に確認しておきます。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。

タスク概要

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、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 * 後で割り当てる * 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、ホストにスナップショットボリュームへの読み取り / 書き込みアクセスを提供し、予約済み容量が必要です。
   - 読み取り専用 — このオプションは、ホストにスナップショットボリュームへの読み取り専用アクセスを提供し、予約容量を必要としません。
3. * Next * をクリックし、次のいずれかを実行します。
   - スナップショットボリュームが読み取り / 書き込みの場合、「容量の確認」ダイアログボックスが表示されます。ステップ3：Snapshotボリュームの容量を確保するに進みます。
   - スナップショットボリュームが読み取り専用の場合、「優先度の編集」ダイアログボックスが表示されます。[ステップ4：スナップショットボリュームの設定を編集する]に進みます。

ステップ3：Snapshotボリュームの容量を確保する

予約容量を読み取り / 書き込みスナップショットボリュームに関連付けます。System Managerは、ベースボリュームまたはスナップショット整合性グループのプロパティに基づいて、ボリュームと容量を提案します。推奨される予約容量構成を受け入れるか、割り当てられるストレージをカスタマイズすることができます。

タスク概要

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]の表には、指定したリザーブ容量をサポートするボリュームだけが候補として表示されます。

   次のいずれかを実行します。

   - * デフォルト設定を受け入れます *。

     Snapshotボリュームにデフォルトの設定でリザーブ容量を割り当てるには、このオプションを使用します（推奨）。

   - データストレージのニーズに合わせて、独自の予約容量設定を割り当ててください。

     デフォルトの予約容量設定を変更した場合は、* Refresh Candidates * をクリックして、指定した予約容量の候補リストを更新してください。

     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%であり、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：*スナップショット整合性グループのスナップショットボリュームを作成する場合、「予約済み容量候補」テーブルに「候補の変更」オプションが表示されます。*候補の変更*をクリックして、別の予約済み容量候補を選択します。
3. * 次へ * をクリックして、[ステップ4：スナップショットボリュームの設定を編集する]に移動します。

ステップ4：スナップショットボリュームの設定を編集する

名前、キャッシュ、リザーブ容量に関するアラートしきい値など、Snapshotボリュームの設定を変更します。

タスク概要

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	概要
Snapshot ボリュームの設定	Name
Snapshotボリュームの名前を指定します。	SSD キャッシュの有効化
SSDで読み取り専用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。	予約容量設定
アラートの送信しきい値…	読み取り */* 書き込みスナップショットボリュームの場合にのみ表示されます。 このスピン ボックスを使用して、Snapshotグループのリザーブ容量が残り少なくなったときにシステムからアラート通知を送信する割合を調整します。 Snapshotグループのリザーブ容量が指定したしきい値を超えた場合、通知に基づいて、残りのスペースがなくなる前にリザーブ容量を増やしたり不要なオブジェクトを削除したりできます。

2. スナップショットボリュームの設定を確認してください。変更を加えるには * 戻る * をクリックしてください。
3. スナップショットボリュームの設定に問題がなければ、* 完了 * をクリックしてください。

Snapshotスケジュールの管理

SANtricity System Managerでスナップショットスケジュールの設定を変更する

Snapshotスケジュールでは、自動収集時間または収集の頻度を変更できます。

タスク概要

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：Storage[Snapshots]を選択します。
2. **Schedules** タブをクリックします。
3. 変更するスナップショットスケジュールを選択し、*編集*をクリックします。

「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され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を含むオブジェクトを選択してから、*インポート*をクリックします。
   - スケジュール設定を編集する — 以下のフィールドの詳細を参照してください。

     フィールドの詳細

設定	概要
曜日 / 月	以下のいずれかのオプションを選択します： • 日次／週次 — 同期スナップショットを取得する日を個別に選択します。日次スケジュールを作成する場合は、右上の*すべての日を選択*チェックボックスを選択することもできます。 • 月次／年次 — 同期スナップショット用に個別の月を選択します。**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。複数の日はカンマまたはセミコロンで区切ることができます。連続する日付にはハイフンを使用します。例：1,3,4,10-15,Last。月次スケジュールが必要な場合は、右上の*Select all months*チェックボックスを選択することもできます。
開始時間	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。選択肢には30分単位の時間が表示されます。開始時間のデフォルトは現在時刻の30分後です。
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。 1より大きい値を選択した場合は、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、十分なリザーブ容量があることを確認してください。
開始日 終了日 終了日なし	同期を開始する開始日を入力してください。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*をクリックします。

SANtricity System Managerでスナップショット スケジュールをアクティブ化および一時停止する

ストレージ スペースを節約する必要があるときは、スケジュールされているSnapshotイメージの収集を一時的に停止することができます。この方法は、Snapshotスケジュールを削除して作成し直すよりも効率的です。

タスク概要

スナップショット スケジュールの状態は、* Activate *オプションを使用し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まで、一時停止状態のままになります。

手順

1. メニュー：Storage[Snapshots]を選択します。
2. 表示されていない場合は、*スケジュール*タブをクリックしてください。

   スケジュールの一覧が表示されます。

3. 一時停止したいアクティブなスナップショットスケジュールを選択し、*アクティブ化／一時停止*をクリックします。

   「状態」列のステータスが*一時停止*に変更され、スナップショットスケジュールはすべてのスナップショットイメージの収集を停止します。

4. スナップショット イメージの収集を再開するには、再開する一時停止中のスナップショット スケジュールを選択し、*アクティブ化/一時停止*をクリックします。

   「状態」列のステータスが アクティブ に変更されます。

SANtricity System Managerでスナップショットスケジュールを削除する

Snapshotイメージを収集する必要がなくなった場合は、既存のSnapshotスケジュールを削除できます。

タスク概要

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。将来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おきます。

手順

1. メニュー：Storage[Snapshots]を選択します。
2. **Schedules** タブをクリックします。
3. 削除するSnapshotスケジュールを選択し、処理を確定します。

結果

ベース ボリュームまたはSnapshot整合性グループからすべてのスケジュール設定が削除されます。

Snapshotイメージの管理

SANtricity System Managerでスナップショット画像の設定を表示する

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、関連オブジェクトを表示できます。

タスク概要

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、関連するSnapshotグループ、およびSnapshotイメージから作成されたSnapshotボリュームが含まれます。Snapshotの設定を使用して、Snapshotイメージをコピーするか変換するかを判断します。

手順

1. メニュー：Storage[Snapshots]を選択します。
2. * Snapshot Images * タブをクリックします。
3. 表示するスナップショットイメージを選択し、*View Settings*をクリックします。

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

4. Snapshotイメージの設定を確認します。

SANtricity System Managerでベースボリュームのスナップショット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。

開始する前に

- ロールバック処理を開始するには、十分なリザーブ容量を確保しておく必要があります。
- 選択したSnapshotイメージとボリュームがどちらも最適な状態である必要があります。
- 選択したボリュームですでに実行中のロールバック処理がないことを確認します。

タスク概要

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：Storage[Snapshots]を選択します。

2. *Snapshot Images*タブを選択します。
3. Snapshot画像を選択し、メニューの「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てください。

   「予約容量の増加」ダイアログ ボックスが表示されます。

   a. スピン ボックスを使用して容量の割合を調整します。

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

   b. * Increase * をクリックします。

5. この操作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 は以下の操作を実行します。

- 選択したSnapshotイメージに保存された内容を使用してボリュームをリストアします。
- ホストからロールバックされたボリュームにすぐにアクセスできるようにします。ロールバック処理が完了するまで待つ必要はありません。

終了後の操作

メニュー：Home[View Operations in Progress]を選択して、ロールバック操作の進行状況を表示します。

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の手順に従って問題を修正するか、テクニカル サポートにお問い合わせください。

SANtricity System Managerで**Snapshot**コンシステンシグループメンバーボリュームの**Snapshot**イメージ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。

開始する前に

- ロールバック処理を開始するには、十分なリザーブ容量を確保しておく必要があります。
- 選択したSnapshotイメージとボリュームがどちらも最適な状態である必要があります。
- 選択したボリュームですでに実行中のロールバック処理がないことを確認します。

タスク概要

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、次に示す複数の手順で構成されます。

ステップ1：メンバーを選択する

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：Storage[Snapshots]を選択します。
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個または複数のメンバー ボリュームを選択します。
5. * Next * をクリックし、次のいずれかを実行します。
   - 選択したメンバーボリュームのいずれかが、Snapshotイメージを格納する複数の予約済み容量オブジェクトに関連付けられている場合、「容量の確認」ダイアログボックスが表示されます。[ステップ2：容量を確認する]に移動します。
   - 選択され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予約済み容量オブジェクトに複数関連付けられていない場合、「優先度の編集」ダイアログボックスが表示されます。[ステップ3：優先順位を編集する]に進みます。

ステップ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*編集*列の*容量を増やす*リンクをクリックします。

   「予約容量の増加」ダイアログ ボックスが表示されます。
2. スピナーボックスを使用して容量の割合を調整し、*増加*をクリックします。

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

3. *Next*をクリックして、[ステップ3：優先順位を編集する]に移動します。

   「優先度の編集」ダイアログボックスが表示されます。

ステップ**3**：優先順位を編集する

必要に応じて、ロールバック処理の優先度を編集することができます。

タスク概要

ロールバックの優先度により、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たら、*完了*をクリックしてください。

結果

System Manager は以下の操作を実行します。

- 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。

終了後の操作

メニュー：Home[View Operations in Progress]を選択して、ロールバック操作の進行状況を表示します。

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の手順に従って問題を修正するか、テクニカル サポートにお問い合わせください。

SANtricity System Managerでスナップショット 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：Storage[Snapshots]を選択します。
2. * Snapshot Images * タブをクリックします。
3. 一時停止中のロールバックをハイライト表示し、メニューから「Rollback[Resume]」を選択します。

   処理が再開されます。

結果

System Manager は以下の操作を実行します。

- ロールバック処理が正常に再開された場合は、進行中の処理ウィンドウでロールバック処理の進行状況を

確認できます。

- ロールバック処理が失敗すると、処理は再び一時停止します。Recovery Guruの手順に従って問題を修正するか、テクニカル サポートにお問い合わせください。

SANtricity System Manager でスナップショット イメージのロールバックをキャンセル

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）、（リソースの起動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。

タスク概要

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：Storage[Snapshots]を選択します。
2. * Snapshot Images * 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：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 * をクリックして確認します。

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。

終了後の操作

ロールバック処理をキャンセルしたあとで、次のいずれかの操作を行う必要があります。

- 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。

SANtricity System Managerでスナップショット画像を削除する

Snapshotイメージの削除は、SnapshotグループまたはSnapshot整合性グループから最も古いSnapshotイメージをクリーンアップする場合に行います。

タスク概要

Snapshotイメージは単独で削除できるほか、作成時のタイムスタンプが同じ複数の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。また、SnapshotグループからSnapshotイメージを削除することもできます。

削除できるのは、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イメージだけです。

手順

1. メニュー：Storage[Snapshots]を選択します。
2. * Snapshot Images * 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*をクリックします。

結果

System Manager は以下の操作を実行します。

- ストレージ アレイからSnapshotイメージが削除されます。
- SnapshotグループまたはSnapshot整合性グループ内で再利用できるようにリザーブ容量が解放されます。
- 削除したSnapshotイメージに関連付けられていたSnapshotボリュームがすべて無効化されます。
- Snapshot整合性グループから削除した場合は、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変わります。

Snapshot整合性グループの管理

SANtricity System Managerでスナップショット整合性グループにメンバーボリュームを追加する

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確保する必要があります。

開始する前に

- メンバーボリュームは最適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）以内となる必要があります。
- 各リザーブ容量ボリュームのData Assurance（DA）とセキュリティ設定が、関連付けられたメンバー ボリュームと同じである必要があります。

タスク概要

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：Storage[Snapshots]を選択します。
2. * Snapshot Consistency Groups * 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. 変更するスナップショット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」ダイアログボックスが表示されます。

4. 追加するメンバーボリュームを選択し、*次へ*をクリックします。

   [容量のリザーブ]の手順が表示されます。[ボリューム候補]の表には、指定したリザーブ容量をサポートするボリュームだけが候補として表示されます。

5. スピン ボックスを使用して、メンバー ボリュームにリザーブ容量を割り当てます。次のいずれかを実行します。
   - * デフォルト設定を受け入れます。*

     メンバー ボリュームにデフォルトの設定でリザーブ容量を割り当てるには、このオプションを使用します（推奨）。

   - データストレージのニーズに合わせて、独自の予約容量設定を割り当ててください。

     デフォルトの予約容量設定を変更した場合は、* Refresh Candidates * をクリックして、指定した予約容量の候補リストを更新してください。

     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%であり、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。

SANtricity System Managerでスナップショット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。

タスク概要

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：Storage[Snapshots]を選択します。
2. * Snapshot Consistency Groups * タブをクリックします。
3. 変更するSnapshot整合性グループを、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たら、*削除*をクリックしてください。

結果

System Manager は以下の操作を実行します。

- 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。

SANtricity System Managerでスナップショット整合性グループの設定を変更する

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：Storage[Snapshots]を選択します。
2. * Snapshot Consistency Groups * タブをクリックします。
3. 編集するスナップショット整合性グループを選択し、*設定の表示/編集*をクリックします。

   [Snapshot 整合性グループ設定]ダイアログ ボックスが表示されます。

4. Snapshot整合性グループの設定を適宜変更します。

フィールドの詳細

設定	概要
• Snapshot 整合性グループの設定 *	Name
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選択したままにします。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した場合、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*をクリックします。

SANtricity System Managerでスナップショット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。

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必要ないことを確認します。

タスク概要

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Sapshotイメージやスケジュールがすべて削除されます。

手順

1. メニュー：Storage[Snapshots]を選択します。
2. * Snapshot Consistency Groups * タブを選択します。
3. 削除するスナップショット整合性グループを選択し、メニュー：Uncommon Tasks[Delete]を選択します。

   「Snapshot整合性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 は以下の操作を実行します。

- 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ボリュームの管理

SANtricity System Managerでスナップショットボリュームを読み書きモードに変換

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：Storage[Snapshots]を選択します。
2. * Snapshot Volumes * タブを選択します。

   [Snapshot ボリューム]の表に、ストレージ アレイに関連付けられているすべてのSnapshotボリュームが表示されます。

3. 変換したい読み取り専用のスナップショットボリュームを選択し、*読み書き可能に変換*をクリックします。

   「読み書きに変換」ダイアログボックスが表示され、*容量の予約*ステップが有効になっています。ボリューム候補テーブルには、指定された予約容量をサポートする候補のみが表示されます。

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る — スナップショットボリュームの予約容量をデフォルト設定で割り当てるには、この推奨オプションを使用してください。
   - データストレージのニーズに合わせて、独自の予約容量設定を割り当ててください — 次のガイドラインに従って予約容量を割り当ててください。
     - 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40%であり、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. *次へ*を選択して、設定を確認または編集します。

   「設定の編集」ダイアログボックスが表示されます。

6. スナップショットボリュームの設定を適切に承認または指定し、* Finish *を選択してスナップショットボリュームを変換します。

   フィールドの詳細

設定	概要
予約容量設定	アラートの送信しきい値…

SANtricity System Managerでスナップショットボリュームのボリューム設定を変更する

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キャッシングを有効化 / 無効化したり、ホスト、ホスト クラスタ、または論理ユニット番号（LUN）の割り当てを変更できます。

手順

1. メニュー：Storage[Snapshots]を選択します。
2. *Snapshot Volumes*タブをクリックします。
3. 変更するスナップショットボリュームを選択し、*設定の表示/編集*をクリックします。

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

4. Snapshotボリュームの設定を適宜表示、編集します。

フィールドの詳細

設定	概要
• Snapshot ボリューム*	Name
Snapshotボリュームの名前を変更できます。	割り当て先
Snapshotボリュームのホストまたはホスト クラスタの割り当てを変更できます。	LUN
Snapshotボリュームのlunの割り当てを変更できます。	SSD キャッシュ
ソリッド ステート ディスク（SSD）の読み取り専用キャッシュを有効 / 無効にできます。	関連オブジェクト
Snapshot イメージ	スナップショットボリュームに関連付けられたスナップショットイメージを表示できます。スナップショットイメージは、特定のポイントインタイムで取得されたボリュームデータの論理的なコピーです。復元ポイントと同様に、スナップショットイメージを使用すると、既知の正常なデータセットにロールバックできます。ホストはスナップショットイメージにアクセスできますが、直接読み書きすることはできません。
ベース ボリューム	スナップショット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。ベースボリュームとは、スナップショットイメージが作成される元のボリュームのことです。シックボリュームまたはシンボリュームのいずれかであり、通常はホストに割り当てられます。ベースボリュームは、ボリュームグループまたはディスクプールのどちらにも配置できます。
Snapshot グループ	スナップショットボリュームに関連付けられているスナップショットグループを表示できます。スナップショットグループとは、単一のベースボリュームから抽出されたスナップショットイメージの集合です。

SANtricity System Managerでスナップショット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。

タスク概要

Snapshotボリュームをターゲット ボリュームにコピーする方法は、通常のボリューム コピー処理と同じです。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：Storage[Snapshots]を選択します。
2. * Snapshot Volumes * タブを選択します。

   [Snapshot ボリューム]の表に、ストレージ アレイに関連付けられているすべてのSnapshotボリュームが表示されます。

3. コピーするスナップショットボリュームを選択し、次に*ボリュームのコピー*を選択します。

   「ボリュームのコピー」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、*完了*をクリックします。

SANtricity System Managerでスナップショット 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、新規作成より短時間で実施できます。

開始する前に

- Snapshotボリュームが最適または無効のどちら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。

タスク概要

メンバーであるSnapshotボリュームを個々に再作成することはできません。再作成できるのは、Snapshot整合性グループのSnapshotボリューム全体のみです。

> SnapshotボリュームまたはSnapshot整合性グループのSnapshotボリュームがオンライン コピー関係の一部である場合は、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：Storage[Snapshots]を選択します。
2. * Snapshot Volumes * タブを選択します。

   [Snapshot ボリューム]の表に、ストレージ アレイに関連付けられているすべてのSnapshotボリュームが表示されます。

3. 再作成するスナップショット ボリュームを選択し、メニューUncommon Tasks（通常とは異なるタスク）[Recreate（再作成）]を選択します。

   「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スナップショットイメージ

     既存のSnapshotイメージを指定し、それを元に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

     このオプションを選択すると、スナップショット ボリュームを再作成するための新しいスナップショット イメージが作成されます。

5. * Recreate * をクリックします。

結果

System Manager は以下の操作を実行します。

- 関連す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 `write`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、以前無効になっ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。

SANtricity System Managerでスナップショットボリュームを無効にする

Snapshotボリューム、またはSnapshot整合性グループのSnapshotボリュームが不要になった場合や一時的に使用を停止する場合は、それらのボリュームを無効にすることができます。

タスク概要

[無効化]オプションは、次のいずれかの状況に当てはまる場合に使用します。

- 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。
- 後日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、再度作成しなくてもい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ことで、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することができます。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際は、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ボリュームをオンライン コピー関係で使用している場合、[無効化]オプションは実行できません。

手順

1. メニュー：Storage[Snapshots]を選択します。

2. * Snapshot Volumes * 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. 無効にするスナップショットボリュームを選択し、メニューの「Uncommon Tasks」[Disable]を選択します。
4. 操作を実行することを確認し、*無効にする*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）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。

SANtricity System Managerでスナップショット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。

スナップショットに関連付けられた予約容量ボリュームを削除するか `read-write`、スナップショット予約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。

タスク概要

ベースボリュームを削除すると、関連付けられているスナップショットボリュームまたは整合性グループスナップショットボリュームも自動的に削除されます。「進行中」ステータスのボリュームコピー中のスナップショットボリュームは削除できません。

手順

1. メニュー：Storage[Snapshots]を選択します。
2. * Snapshot Volumes * 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. 削除するスナップショットボリュームを選択し、メニュー：通常とは異なるタスク[削除]を選択します。
4. 操作を実行することを確認し、*Delete*をクリックします。

結果

System Manager は以下の操作を実行します。

- 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。

SANtricity System Managerのスナップショットに関するよくある質問

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

ボリューム、ホスト、またはホスト クラスタが一部表示されないのはなぜですか?

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

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

- DA対応でないI/Oインターフェイスを介してストレージ 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、およびミラーに関連付けられているボリュームでは、DAを無効にできません。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。以降の各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（Snapshot整合性グループ）を選択し、次のいずれかの方法でSnapshotイメージをキャプチャします。

- 1つのベース ボリューム、または複数のベース ボリュームで構成されるSnapshot整合性グループのSnapshotイメージを作成できます。
- 手動でSnapshotを作成するか、ベース ボリュームまたはSnapshot整合性グループの定期的なSnapshotイメージを自動的に作成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、ある時点の既知の有効なデータ セットにロールバックすることができます。ロールバック機能は、偶発的なデータの削除や破損からの保護を提供します。

Snapshotに使用できるボリューム タイプはどれですか**?**

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**?**

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は、Snapshot整合性グループを作成します。

たとえば、リカバリ目的で整合性を保つ必要がある複数のボリュームで構成されるデータベースが該当します。この場合、すべてのボリュームのSnapshotを同時に収集し、収集したSnapshotを使用してデータベース全体をリストアするために、Snapshot整合性グループが必要です。

スナップショット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。

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**?**

スナップショット ボリュームを使用すると、ホストはスナップショット イメージ内のデータにアクセスできます。スナップショット ボリュームには独自の予約容量があり、ベース ボリュームへの変更を元のスナップショット イメージに影響を与えることなく保存します。スナップショット イメージは、ホストから読み書きアクセスできません。スナップショット データへの読み書きを行う場合は、スナップショット ボリュームを作成し、それをホストに割り当ててください。

2種類のSnapshotボリュームを作成できます。Snapshotボリュームの種類によって、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、ホスト アプリケーションにスナップショット 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提供します。読み取り専用のスナップショット ボリュームは、予約済み容量を使用しません。
- 読み書き可能 — 読み書き可能として作成されたスナップショット ボリュームを使用すると、参照されているスナップショット イメージに影響を与えることなく、スナップショット ボリュームに変更を加えることができます。読み書き可能なスナップショット ボリュームは、予約済みの容量を使用してこれらの変更を保存します。読み取り専用のスナップショット ボリュームは、いつでも読み書き可能なボリュームに

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は、スナップショット イメージを_スナップショット グループ_に編成します。スナップショット グループにユーザによる操作は必要ありませんが、スナップショット グループの予約容量はいつでも調整できます。また、次の条件が満たされた場合は、予約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Snapshotグループを自動的に作成します。その際、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ときには、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、そのボリュームを無効にするのではなく、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イメージによって決まります。無効状態のSnapshotボリュームでは、読み取り / 書き込みアクティビティは停止されています。

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、スケジュールに沿った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的に停止し、あとでスケジュールされたSnapshotを開始できます。

Snapshotスケジュールが必要ない場合は、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

SANtricity ソフトウェアの非同期ミラーリングについて学ぶ

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 サイトは即座に更新でき、セカンダリ サイトは帯域幅の許す限り更新できます。情報はキャッシュされ、ネットワーク リソースが利用可能になると後で送信されます。

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。

詳細については、以下を参照してください。

- "非同期ミラーリングの仕組み"
- "非同期ミラーリングの用語"
- "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?

アレイ間の最初のミラーリングは、Unified Managerを使用して設定する必要があります。設定後は、System Managerでミラー ペアと整合性グループを管理できます。

詳細については、以下を参照してください。

- "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にミラーリングするためのワークフロー"
- "Create asynchronous mirrored pair（Unified Manager）"

関連情報

非同期ミラーリングに関連する概念の詳細については、以下を参照してください。

- "ミラー整合性グループを作成するときは、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は何ですか?"

SANtricity ソフトウェアの同期ミラーリングについて学ぶ

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/EF600CまたはEF300/EF300Cストレージ システムではご利用いただけません。

同期ミラーリングとは何ですか?

_同期ミラーリング_は、データボリュームをリアルタイムでレプリケートし、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はミラーリング操作を管理しますが、これはホストマシンやソフトウェアアプリケーションに対して透過的です。

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。

詳細については、以下を参照してください。

- "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?

アレイ間の最初のミラーリングは、Unified Managerを使用して設定する必要があります。設定後は、System Managerでミラー ペアを管理できます。

詳細については、以下を参照してください。

- "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"
- "Create synchronous mirrored pair（Unified Manager）"

関連情報

同期ミラーリングに関連する概念の詳細については、以下を参照してください。

- "ミラー ペアを作成するときは、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は何ですか?"

非同期の概念

SANtricity System Managerにおける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、あとからネットワーク リソースが利用可能になったときに送信されます。

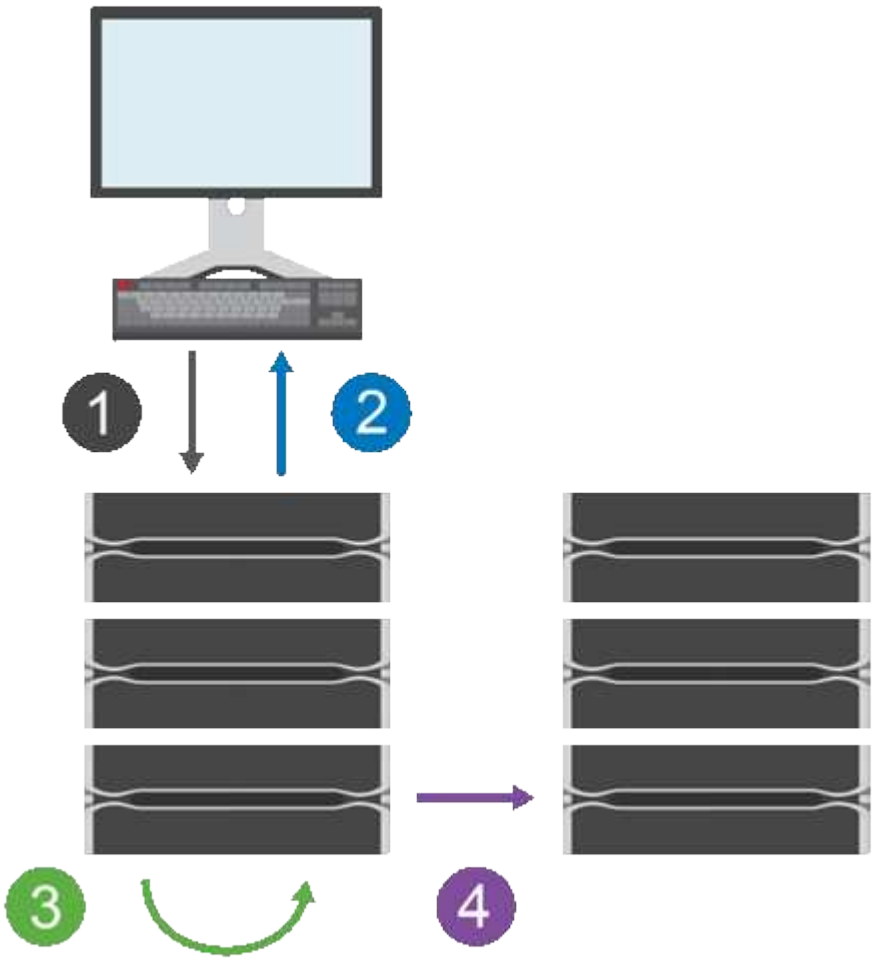
このタイプのミラーリングはノンストップ オペレーションの要求に応えるための手段として最適であり、一般的には、バックアップやアーカイブなどの定期的なプロセスをはるかに少ないネットワーク負荷で実施できます。非同期ミラーリングを使用する状況としては以下が考えられます。

- 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。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、あとからネットワーク 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 セッションには大きく分けて4つの手順で実行されます。



1. まず、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行われます。
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、定義済みの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、設定済みの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影響はありません。したがって、非同期ミラーリングは、iSCSIのような低速接続を使用して、地理的に離れたローカルとリモートのストレージ システム間で実行することができます。

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（ストレージ アレイごとに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関係を確立します。非同期ミラー関係はミラー ペア（あるストレージ アレイ上のプライマリ ボリュームと別のストレージ アレイ上のセカンダリ ボリューム）で構成されます。

プライマリ ボリュームを含むストレージ アレイは、一般にプライマリ 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、一般にセカンダリ 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 コピーが含まれていて、ディザスタ リカバリ（災害復旧）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。この状況の原因として次の問題が考えられます。

- ローカル ストレージ アレイとリモート ストレージ アレイ間のネットワークの問題
- セカンダリ ボリュームの障害
- ミラー ペアの同期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、自動のどちらでも同期できます。

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。

SANtricityソフトウェアの非同期ミラーリング用語について説明します

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	概要
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。 「ローカルロール」列に*Primary*と表示されている場合、そのストレージアレイにはミラーリング関係におけるプライマリロールを保持するボリュームが含まれていることを示します。「ローカルロール」列に*Secondary*と表示されている場合、そのストレージアレイにはミラーリング関係におけるセカンダリロールを保持するボリュームが含まれていることを示します。
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を格納するコンテナです。非同期ミラーリング操作を行うには、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、ミラーリングされたペアは常にミラー整合性グループに属します。書き込み操作はまずプライマリ ボリュームに対して実行され、次にセカンダリ ボリュームにレプリケートされます。ミラー整合性グループ内の各ミラーペアは、同じ同期設定を共有します。
プライマリ ボリューム	ミラーリングされたペアのプライマリボリュームは、ミラーリングされるソースボリュームです。
リモート ストレージ アレイ	リモートストレージアレイは通常、セカンダリサイトとして指定され、ミラーリング構成でデータのレプリカを保持するのが一般的です。
リザーブ容量	予約容量とは、あらゆるコピーサービス操作およびストレージオブジェクトに使用される、物理的に割り当てられた容量のことです。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、プライマリ ボリュームにセカンダリ 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、セカンダリサイトに配置され、データの複製を保持します。

期間	概要
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間の初期同期時に発生します。通信の中断後にプライマリボリュームとセカンダリ ボリュームの同期が解除された場合にも、同期処理が行われます。通信リンクが再び機能すると、複製されていないデータはすべてセカンダリ ボリュームのストレージアレイに同期されます。

SANtricityソフトウェアでボリュームを非同期でミラーリングする

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、または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、実行する同期方法（手動またはスケジュール）を指定します。
   c. ローカル ストレージ アレイからプライマリ ボリュームを選択し、リザーブ容量を確認します。リザーブ容量は、コピー処理に使用される物理割り当て容量です。
   d. 転送先としてリモート ストレージ アレイを選択し、セカンダリ ボリュームを選択して、リザーブ容量を確認します。
   e. プライマリ ボリュームからセカンダリ ボリュームへの初回のデータ転送を開始します。ボリュームサイズによっては、この初回転送に数時間かかることがあります。
2. 初期同期の進捗状況を確認します。
   a. Unified Managerで、ローカルアレイのSystem Managerを起動します。
   b. System Managerで、ミラーリング操作のステータスを確認します。ミラーリングが完了すると、ミラーリングされたペアのステータスは「Optimal」になります。
3. オプション： System Managerで、後続のデータ転送のスケジュールを変更したり、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、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。

SANtricityソフトウェアで非同期ミラーリングを使用するための要件

非同期ミラーリングを使用する場合は、次の要件に注意してください。

Unified Manager

2つのアレイ間のミラーリングを有効にして設定するには、Unified Managerインターフェイスを使用する必要があります。Unified Managerは、Web Services Proxyとともにホスト システムにインストールされます。

- Web Services Proxyサービスが実行されている必要があります。
- Unified ManagerがHTTPS接続経由でローカル ホストで実行されている必要があります。
- Unified Managerは、ストレージアレイに対して有効なSSL証明書を表示している必要があります。Unified Managerを使用して、メニューの「証明書」[証明書管理]に移動することで、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 アレイ内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。（ストレージ アレイごとに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。
- リモート ストレージ アレイにセカンダリ ボリュームを作成するための十分な空き容量（ミラーリングするプライマリ ボリュームと同等以上）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。タイプが異なるチャネル間ではフェイルオーバーは発生しません。

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。

- ファイバチャネル（**FC**）インターフェイスを介したミラーリング

  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。このポートに対しては、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** インターフェースを介したミラーリング

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接続が確立されると、接続に最初に成功したポートがリモート 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、使用可能な残り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されます。設定の通知やデータ転送などのコントローラ間の通信には、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 システムの両方が通信するには、同じ VLAN 設定である必要があります
- iSCSIリスン 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。

> E4000は、iSCSIプロトコル使用時の非同期ミラーリングをサポートしていません。

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のコントローラでは、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 ボリュームで、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。そうでない非同期ミラー 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。
- ボリュームの候補は、同じデータ セキュリティ機能を使用している必要があります。
  - プライマリ ボリュームがFIPS対応の場合、セカンダリ ボリュームもFIPS対応である必要があります。
  - プライマリ ボリュームがFDE対応の場合、セカンダリ ボリュームもFDE対応である必要があります。

- プライマリ ボリュームがDrive Securityを使用していない場合は、セカンダリ ボリュームもDrive Securityを使用してはいけません。

- 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。
- プライマリ ボリュームとセカンダリ ボリュームでは、リソース パーティショニングを有効にしてはなりません。

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。
  - 予約容量ボリュームがNVMeドライブ上に作成される場合、そのミラー ボリュームもNVMeドライブ上に作成する必要があります。
  - 予約容量ボリュームが SAS ドライブ上に作成される場合、そのミラー ボリュームも SAS ドライブ上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。

SANtricity System Managerで非同期ミラーのステータスを表示する

ミラー ステータスは、ミラー整合性グループおよびミラー 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	概要
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、ボリュームは次の状態に移行する可能性があります：Degraded/Failed/Optimal/Unknown。

ステータス	概要
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。
システムによる中断	ミラー整合性グループ レベルで、すべてのミラー ペアに関して、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。
ユーザによる中断	ミラー整合性グループ レベルで、すべてのミラー ペアに関して、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、ホスト アプリケーションのパフォーマンスへの影響（ローカル ストレージ アレイで変更されたデータがリモート ストレージ アレイにコピーされるときに発生する可能性があります）を削減する際に役立ちます。
一時停止	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	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、選択されている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起きたため、ミラー整合性グループ間でロールの競合が発生しています。 ロールの競合は通信の問題が解決され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的な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 ボリューム上とセカンダリ ボリューム上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	概要
同期	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、[長時間実行中の処理]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 アレイの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	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によって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	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	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。

SANtricity ソフトウェアの非同期ミラーリングにおけるボリューム所有権について学ぶ

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によって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によって所有されます。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によって所有されるように、セカンダリ ボリュームの所有者が自動的に変更されます。プライマリ側の現在の所有権の変更は、セカンダリ側の対応する現在の所有権の変更に自動的に反映されます。

たとえば、コントローラAが所有するプライマリ ボリュームの所有者をコントローラBに変更したとします。この場合、次回のリモート書き込み時に、セカンダリ ボリュームの所有者がコントローラAからコントローラBに切り替わります。セカンダリ側のコントローラ所有権の切り替えはプライマリ側で制御されるため、ストレージ管理者による特別な対応は必要ありません。

コントローラのリセット

コントローラをリセットすると、プライマリ側でボリューム所有権が優先コントローラ所有者からストレージ アレイ内の別のコントローラに変更されます。

セカンダリ ボリュームに対するリモートでの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その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 ペアのフル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の際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。続いて、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 ボリュームのフル同期が不要になります。

SANtricity ソフトウェアでミラー整合性グループのロールを変更

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 ミラー整合性グループ内のメンバー ボリュームの降格を実行できない場合は、ミラー整合性グループ間で強制的にロールを変更できます。

セカンダリ側のミラー整合性グループを強制的にプライマリ ロールに移行できます。これで、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 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。

Role-Change-In-Progress状態

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、通信が復旧した場合に、両方のストレージ アレイのミラー整合性グループがRole-Change-In-Progress状態になります。

システムでは、変更ログを転送し、再同期を実行し、ミラー整合性グループを通常の動作状態に戻して、定期的な同期を続行することで、ロール変更プロセスを完了します。

同期の概念

SANtricity System Managerにおける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。

EF600/EF600CまたはEF300/EF300Cストレージアレイでは、同期ミラーリングは利用できません。

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。

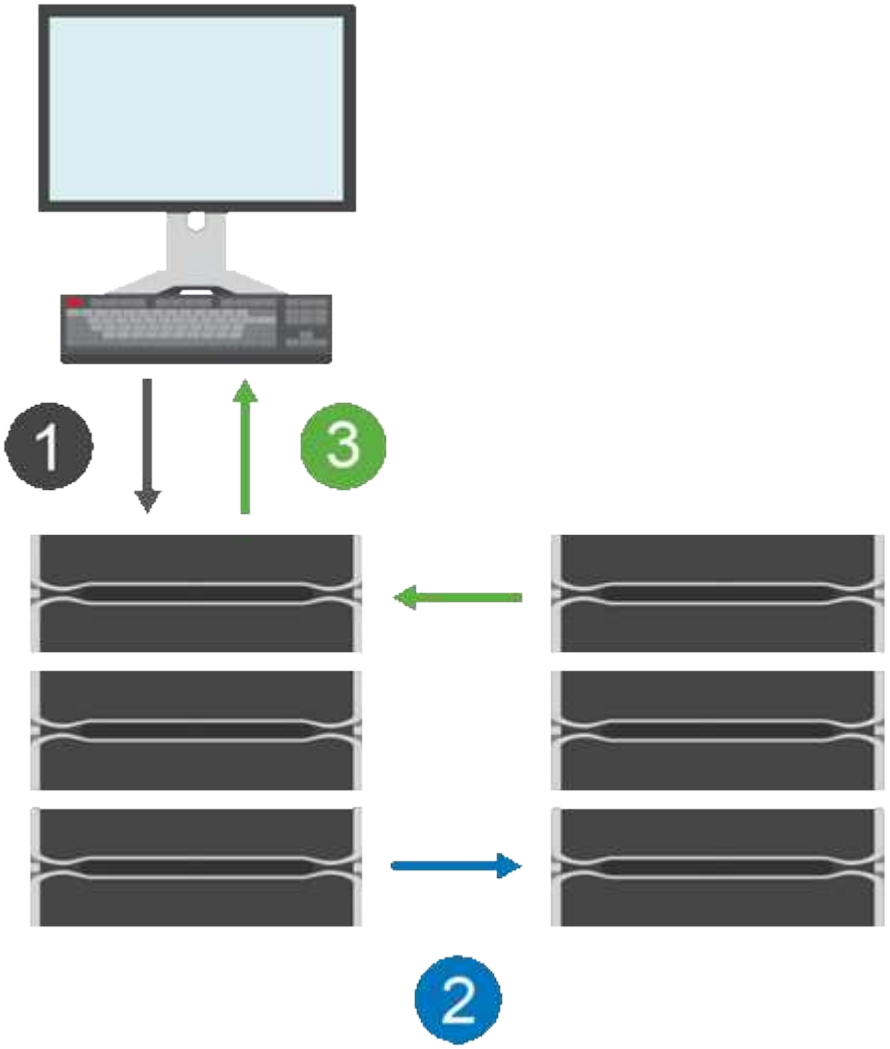
このタイプのミラーリングは、ディザスタ リカバリなどのビジネス継続性の確保に最適です。

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、一般にプライマリ 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、一般にセカンダリ 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。ミラー ペア（ストレージ アレイ上のプライマリ ボリュームと別のストレージ アレイ上のセカンダリ ボリュームで構成）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行われます。



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 アレイは、両方の書き込み操作が正常に完了した_後に_、ホスト システムに I/O 完了メッセージを送信します。

ホストからの書き込み要求に関する情報の記録には、リザーブ容量が使用されます。

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信すると、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。次にコントローラはプライマリ 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全体で書き込みが行われるまで待機する必要があります。そのため、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ためには、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 サイトにある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、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。リカバリ ホストは新しく昇格されたボリュームにアクセスできるため、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している場合は、リンクの再開時にミラー ペアが自動的に再同期されます。手動再同期ポリシーを使用している場合は、通信問題の発生後に同期を手動で再開する必要があります。手動再同期ポリシーが推奨されるポリシーです。

ミラー ペアの同期設定は、プライマリ ボリュームを含むストレージ アレイでのみ編集できます。

非同期のデータ

プライマリ ボリュームのストレージ アレイがセカンダリ ボリュームにデータを書き込むことができなくなった場合、プライマリ ボリュームとセカンダリ ボリュームは非同期状態になります。この原因として次の問題が考えられます。

- 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。

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。

SANtricity ソフトウェアの同期ミラーリング用語について説明します

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	概要
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。 「ローカルロール」列に*Primary*と表示されている場合、そのストレージアレイにはミラーリング関係におけるプライマリロールを保持するボリュームが含まれていることを示します。「ローカルロール」列に*Secondary*と表示されている場合、そのストレージアレイにはミラーリング関係におけるセカンダリロールを保持するボリュームが含まれていることを示します。
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	ミラーリングされたペアのプライマリボリュームは、ミラーリングされ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を示す目標を表します。RPOがゼロの場合、プライマリ ボリュームとセカンダリ ボリュームの間に差を許容できないことを示します。RPOがゼロより大きい場合、セカンダリ ボリュームがプライマリ ボリュームよりも最新でない、または遅れていることを示します。
リモート ストレージ アレイ	リモートストレージアレイは通常、セカンダリサイトとして指定され、ミラーリング構成でデータのレプリカを保持するのが一般的です。
リザーブ容量	予約容量とは、あらゆるコピーサービス操作およびストレージオブジェクトに使用される、物理的に割り当てられた容量のことです。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、プライマリ ボリュームにセカンダリ 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、セカンダリサイトに配置され、データの複製を保持します。

期間	概要
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間の初期同期時に発生します。通信の中断後にプライマリボリュームとセカンダリ ボリュームの同期が解除された場合にも、同期処理が行われます。通信リンクが再び機能すると、複製されていないデータはすべてセカンダリ ボリュームのストレージアレイに同期されます。

SANtricity ソフトウェアでボリュームを同期的にミラーリングする

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/EF600CまたはEF300/EF300Cストレージ システムではご利用いただけません。

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、ミラーリング操作のステータスを確認します。ミラーリングが完了すると、ミラーリングされたペアのステータスは「Optimal」になります。2つのアレイは、通常の動作を通じ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提供する必要があります。

SANtricity ソフトウェアで同期ミラーリングを使用するための要件

同期ミラーリングを使用する場合は、次の要件に注意してください。

Unified Manager

2つのアレイ間のミラーリングを有効にして設定するには、Unified Managerインターフェイスを使用する必要があります。Unified Managerは、Web Services Proxyとともにホスト システムにインストールされます。

- Web Services Proxyサービスが実行されている必要があります。
- Unified ManagerがHTTPS接続経由でローカル ホストで実行されている必要があります。

- Unified Managerは、ストレージアレイに対して有効なSSL証明書を表示している必要があります。Unified Managerを使用して、メニューの「証明書」[証明書管理]に移動することで、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

EF300/EF300C または EF600/EF600C ストレージ アレイでは、同期ミラーリングは利用できません。

- 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 アレイ内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。（ストレージ アレイごとに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。
- リモート ストレージ アレイにセカンダリ ボリュームを作成するための十分な空き容量（ミラーリングするプライマリ ボリュームと同等以上）が必要です。
- 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は、Fibre Channelファブリックを介して接続されています。

サポートされる接続

同期ミラーリングのための通信は、Fibre Channel（FC）ホスト ポートを備えたコントローラでのみサポートされています。

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おいて、各コントローラ上で最も番号の大きいホストポートが使用されます。コントローラホストバスアダプタ（HBA）のホストポート4は、通常、ミラーデータの送信用に予約されています。

ミラー ボリュームの候補

- 同期ミラーリングされたペアのプライマリ ボリュームとセカンダリ ボリュームでは、RAID レベル、キャッシュ パラメータ、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。
- スナップショットを関連付けることができるのはプライマリ ボリュームのみであり、また、ボリューム コピー操作におけるソース ボリュームまたはターゲット ボリュームとなることが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。お使いのストレージ 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個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

- プライマリ ボリュームとセカンダリ ボリュームには、コントローラのリセットやその他の一時的な中断から復旧するための書き込み情報をログ記録するために、予約済み容量が必要です。
- 同期ミラーリングが有効になると、予約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 ボリュームの両方で予約容量が必要になるため、同期ミラー関係に参加している両方のストレージ アレイに十分な空き容量があることを確認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。
  - プライマリ ボリュームがフルディスク暗号化（FDE）ドライブを使用している場合、セカンダリ ボリュームはFDEドライブを使用する必要があります。
  - プライマリ ボリュームが連邦情報処理規格140-2（FIPS）検証済みドライブを使用している場合、セカンダリ ボリュームはFIPS 140-2検証済み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。

SANtricity System Managerでの同期ミラーリングのステータスについて説明します

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/EF600CまたはEF300/EF300Cストレージ システムではご利用いただけません。

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 ペアに含まれる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、各ボリュームが良好な稼働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ない。
- 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ない。
- 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。

- 一時停止中

  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 ボリュームに対する書き込みは、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通常どおり実行できないことを示します。

SANtricityソフトウェアの同期ミラーリングにおけるボリューム所有権について学ぶ

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/EF600CまたはEF300/EF300Cストレージ システムにおける同期ミラーリングでは利用できません。

ミラーペアのプライマリボリュームがコントローラAによって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によって所有されます。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によって所有されるように、セカンダリ ボリュームの所有者が自動的に変更されます。プライマリ側の現在の所有権の変更は、セカンダリ側の対応する現在の所有権の変更に自動的に反映されます。

たとえば、コントローラAが所有するプライマリ ボリュームの所有者をコントローラBに変更したとします。この場合、次回のリモート書き込み時に、セカンダリ ボリュームの所有者がコントローラAからコントローラBに切り替わります。セカンダリ側のコントローラ所有権の切り替えはプライマリ側で制御されるため、ストレージ管理者による特別な対応は必要ありません。

コントローラのリセット

コントローラをリセットすると、プライマリ側でボリューム所有権が優先コントローラ所有者からストレージ アレイ内の別のコントローラに変更されます。

セカンダリ ボリュームに対するリモートでの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その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 ペアのフル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の際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。続いて、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 ボリュームのフル同期が不要になります。

SANtricity ソフトウェアのミラー ペアにおけるボリューム ロールの変更について説明します

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。

EF600/EF600CまたはEF300/EF300Cストレージ システムでは、同期ミラーリングは利用できません。

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 アレイが復旧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。

Role-Change-In-Progress状態

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、通信が復旧した場合に、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の管理

SANtricity System Manager でミラー整合性グループの通信をテストします

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。

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。

タスク概要

次の4つのテストを実行できます。

- * 接続性 * — 2 つのコントローラ間に通信経路が存在することを確認します。接続性テストでは、ストレージ アレイ間でアレイ間メッセージを送信し、リモート ストレージ アレイ上の対応するミラー整合性グループが存在することを検証します。また、リモート ストレージ アレイ上のミラー整合性グループのメンバー ボリュームが、ローカル ストレージ アレイ上のミラー整合性グループのメンバー ボリュームと一致することも検証します。
- レイテンシ — SCSI Test Unitコマンドを、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 ボリュームに送信して、最小、平均、および最大のレイテンシをテストします。
- 帯域幅 — リモート ストレージ アレイに 2 つのアレイ間メッセージを送信し、テストを実行するアレイ上のポートの最小、平均、最大帯域幅、および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 アレイでミラーリングに使用されているポートと、リモート ストレージ アレイでミラー データを受信しているポートが表示されます。

手順

1. メニュー：Storage[Asynchronous Mirroring]を選択します。
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. **Test Communication** 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たローカル ストレージ アレイとリモート ストレージ アレイ間で実行する通信テストを 1 つ以上選択し、* Test * をクリックします。
5. [結果]ウィンドウに表示される情報を確認します。

通信テストのステータス	概要
正常（エラーなし）	ミラー整合性グループが正常に通信しています。
合格（ただし、正常ではない）	発生している可能性のあるネットワークまたは接続の問題を確認してから、テストをやり直してください。

通信テストのステータス	概要
不合格	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	ローカル ストレージ アレイが接続されていない、またはリモート 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。

SANtricity System Managerでミラー整合性グループの同期を一時停止または再開する

ミラー整合性グループ内にあるすべてのミラー ペアでデータの同期を中断または再開できます。これは、個々のミラー ペアで同期を中断または再開するよりも効率的です。

タスク概要

グループに対する同期の中断と再開は、ホスト アプリケーションのパフォーマンスへの影響（ローカル ストレージ アレイで変更されたデータがリモート ストレージ アレイにコピーされるときに発生する可能性があります）を削減する際に役立ちます。

ミラー整合性グループおよびそのミラー 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ます。

手順

1. メニュー：Storage[Asynchronous Mirroring]を選択します。
2. *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ます。このテーブルには、ストレージ アレイに関連付けられているミラー整合性グループがすべて表示されます。

3. 一時停止または再開するミラー整合性グループを選択し、menu：More[Suspend]またはmenu：More[Resume]を選択します。

   確認のメッセージが表示されます。

4. *はい*を選択して確認します。

結果

System Manager は以下の操作を実行します。

- 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。フル同期は必要ありません。
- _停止中_のミラー整合性グループの場合、ミラー整合性グループテーブルに*user-suspended*と表示されます。
- _再開された_ミラー整合性グループの場合、ミラー整合性グループが中断されていた間にプライマリ ボリュームに書き込まれたデータは、直ちにセカンダリ ボリュームに書き込まれます。自動同期間隔が設定されている場合、定期的な同期が再開されます。

SANtricity System Managerでミラー整合性グループの同期設定を変更する

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。

タスク概要

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：Storage[Asynchronous Mirroring]を選択します。
2. *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ます。このテーブルには、ストレージ アレイに関連付けられているミラー整合性グループがすべて表示されます。

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 （その他） [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. 必要に応じて同期設定とアラート設定を編集し、*保存*をクリックします。

フィールドの詳細

フィールド	概要
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上のミラーリングされたペアを、手動で同期するか自動で同期するかを指定します。 • 手動 – このオプションを選択すると、リモート ストレージ アレイ上のミラーリングされたペアを手動で同期できます。 • 自動的に、毎回 – このオプションを選択すると、前回の更新の開始から次回の更新の開始までの時間間隔を指定して、リモートストレージアレイ上のミラーペアを自動的に同期します。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に、次のアラートを設定します。 • 同期 – System Managerが同期が完了していないことを警告するまでの時間を設定します。 • リモート リカバリ ポイント – System Manager が、リモート ストレージ アレイ上のリカバリ ポイント データが定義した時間制限よりも古いことを示すアラートを送信するまでの時間制限を設定します。前回の更新終了時点からの時間制限を定義します。 • リザーブ容量のしきい値 – System Manager がリザーブ容量のしきい値に近づいていることを通知するアラートを送信するリザーブ容量の量を定義します。残り容量のパーセンテージでしきい値を定義します。

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。

SANtricity System Manager で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：Storage[Asynchronous Mirroring]を選択します。
2. *Mirror Consistency Groups*タブを選択します。

   [ミラー整合性グループ]の表に、ストレージ アレイに関連付けられているすべてのミラー整合性グループが表示されます。

3. 再同期するミラー整合性グループを選択し、メニューの「その他」［手動で再同期］を選択します。

   確認のメッセージが表示されます。

4. *はい*を選択して確認します。

結果

次の処理が実行されます。

- 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。

SANtricity System Managerでミラー整合性グループ間の同期されていないデータ量を表示する

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。

タスク概要

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行うことができます。

手順

1. メニュー：Storage[Asynchronous Mirroring]を選択します。
2. *Mirror Consistency Groups*タブを選択します。

   [ミラー整合性グループ]の表に、ストレージ アレイに関連付けられているすべてのミラー整合性グループが表示されます。

3. メニューをクリックします：その他［同期されていないデータ量を表示］。

   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。

SANtricity System Managerでリモートストレージアレイの**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。

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 アレイを設定する必要があります。

手順

1. メニュー：Storage[Asynchronous Mirroring]を選択します。
2. *Mirror Consistency Groups*タブを選択します。

   [ミラー整合性グループ]の表に、ストレージ アレイに関連付けられているすべてのミラー整合性グループが表示されます。

3. 更新するミラー整合性グループを選択し、メニュー：その他［リモート IP アドレスの更新］を選択します。

   システムに [リモート IP アドレスの更新] ダイアログ ボックスが表示されます。

4. リモート ストレージ アレイの iSCSI IP アドレスを更新するには、*更新*を選択します。

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て、ローカル ストレージ アレイとの接続が再確立されます。

SANtricity System Managerで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、あるいはローカル 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。

タスク概要

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：Storage[Asynchronous Mirroring]を選択します。
2. *Mirror Consistency Groups*タブを選択します。

   [ミラー整合性グループ]の表に、ストレージ アレイに関連付けられているすべてのミラー整合性グループが表示されます。

3. 役割を変更するミラー整合性グループを選択し、メニュー：その他[役割を<Primary | Secondary>に変更]*>*を選択します。

   確認の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、*ロールの変更*をクリックします。

   役割変更が要求されたにもかかわらず、リモートストレージアレイに接続できない場合、システムは「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を表示します。*Yes*をクリックして役割変更を強制します。

結果

System Manager は以下の操作を実行します。

- ミラー整合性グループテーブルには、役割変更中のミラー整合性グループの横に「保留中」または「処理中」のステータスが表示されます。保留中の役割変更操作は、表のセル内にある **Cancel** リンクをクリックすることで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。

SANtricity System Managerで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 アレイおよびリモート 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。

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：Storage[Asynchronous Mirroring]を選択します。
2. *Mirror Consistency Groups*タブを選択します。

   [ミラー整合性グループ]の表に、ストレージ アレイに関連付けられているすべてのミラー整合性グループが表示されます。

3. 削除するミラー整合性グループを選択し、メニュー：Uncommon Tasks[Delete]を選択します。

   確認のメッセージが表示されます。

4. ミラー整合性グループを削除するには、*Yes*を選択してください。

結果

System Manager は以下の操作を実行します。

- 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]の表からミラー整合性グループを削除します。

終了後の操作

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 ペアの管理

SANtricity System Managerで非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。

タスク概要

孤立したミラー ペアに関して以下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：Storage[Asynchronous Mirroring]を選択します。

2. **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ミラー ペアがすべて表示されます。

3. 削除するミラー ペアを選択し、*削除*をクリックします。
4. ミラー ペアを削除することを確認し、* 削除 * をクリックします。

結果

System Manager は以下の操作を実行します。

- 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へ、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 ペアの削除を反映して[非同期ミラーリング]タイルを更新します。

SANtricity System Managerで予約容量を増やす

リザーブ容量（ストレージ オブジェクト上のコピー サービス処理に使用される物理的に割り当てられた容量）を拡張できます。

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。一般的には、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。

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」である必要があり、変更状態であってはなりません。
- 容量を増やすために使用するプールまたはボリューム グループには、空き容量が存在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空き容量がない場合は、未使用のドライブという形で未割り当て容量をプールまたはボリュームグループに追加できます。

タスク概要

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 ボリュームの予約容量を増やすことはできません。読み書き可能なSnapshot ボリュームのみが予約容量を必要とします。

手順

1. メニュー：Storage[Pools & Volume Groups]を選択します。
2. * Reserved Capacity * タブを選択します。
3. 予約容量を増やしたいストレージオブジェクトを選択し、*容量を増やす*をクリックします。

   「予約容量の増加」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 グループ上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. * Increase * をクリックします。

結果

System Manager は以下の操作を実行します。

- 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。

SANtricity System Managerでミラーペアボリュームの予約容量設定を変更する

ミラーリングされたペアボリュームの設定を変更して、ミラーリングされたペアボリュームの予約容量がいっぱいになりそうなときに SANtricity System Manager がアラート通知を送信するパーセンテージポイントを調整できます。

手順

1. メニュー：Storage[Pools & Volume Groups]を選択します。
2. * Reserved Capacity * 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、*設定の表示/編集*をクリックします。

   「ミラーリングペアボリュームの予約容量設定」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	概要
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。 ミラー ペアのリザーブ容量の使用率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. 変更を適用するには、*保存*をクリックしてください。

レガシー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**SANtricity System Manager**で完成させます

SANtricity System Managerで管理できないレガシーストレージアレイ上にプライマリボリュームを作成した場合は、SANtricity System Managerを使用してこのアレイ上にセカンダリ ボリュームを作成できます。

タスク概要

別のインターフェイスを使用する従来のアレイと、System Managerで管理できる新しいアレイの間で非同期ミラーリングを実行できます。

- System Managerを使用する2つのストレージ アレイをミラーリングする場合は、ミラー ペア作成手順ですでにミラー ペアの作成が完了しているため、このタスクはスキップできます。
- このタスクはリモート ストレージ アレイで実行します。

手順

1. メニュー：Storage[Asynchronous Mirroring]を選択します。
2. **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ミラー ペアがすべて表示されます。
3. ステータスが「未完了」となっているミラーペアボリュームを見つけ、ミラーペア列に表示されている*ミラーペアを完了する*リンクをクリックします。
4. 次のどちらかのラジオ ボタンを使用して、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。セカンダリ ボリュームにデフォルトの設定でリザー

ブ容量を割り当てるには、このオプションを使用します（推奨）。

- 手動 — 既存のボリュームを選択します。

  セカンダリ ボリュームのパラメータを独自に定義します。

  i. * 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、*次へ*をクリックして予約済み容量を割り当てます。

  iii. リザーブ容量を割り当てます。次のいずれかを実行します。

  - デフォルト設定を使用する。

    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 ボリュームへのI/O書き込みの頻度とサイズ、および容量を維持する必要がある期間によって異なります。一般的に、以下の条件のいずれか、または両方が当てはまる場合は、予約容量としてより大きな容量を選択してください：

    - 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 ボリューム上のデータブロックの大部分が変更されます。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て、プライマリ ボリュームへの典型的なI/Oアクティビティを把握してください。

5. * Complete * を選択します。

結果

System Manager は以下の操作を実行します。

- リモート ストレージ アレイ上にセカンダリ 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。これにより、初期同期で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の両方に、ミラーリングされたペア用の予約容量を作成します。

同期ミラー ペアの管理

SANtricity System Manager での同期ミラーリングの通信テスト

ローカル ストレージ アレイとリモート ストレージ アレイ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。

タスク概要

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 アレイ間に通信経路が存在す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こと、およびミラー ペアに関連付けられたセカンダリ ボリュームがリモート ストレージ アレイ上に存在することを検証します。
- レイテンシ — 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、および最大レイテンシをテストします。

手順

1. メニュー：Storage[Synchronous Mirroring]を選択します。
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る情報を確認し、表示される修正措置を必要に応じて実行します。

> 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。

SANtricity System Managerでミラーペアの同期を一時停止および再開します

[中断]オプションと[再開]オプションを使用すると、ミラー ペアのプライマリ ボリュームとセカンダリ ボリュームのデータを同期するタイミングを制御できます。

タスク概要

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. メニュー：Storage[Synchronous Mirroring]を選択します。
2. 一時停止または再開するミラー ペアを選択し、**More › Suspend**または**More › Resume**を選択します。

   確認のメッセージが表示されます。
3. *はい*を選択して確認します。

結果

System Manager は以下の操作を実行します。

- 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。
- _resumed_ミラー ペアの場合、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が自動的に書き込まれます。完全な同期は必要ありません。

SANtricity System Managerでミラーペア内のボリューム間の役割を変更する

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になることがあります。

タスク概要

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 / 書き込みアクセス権があります。プライマリ ボリュームがセカンダリ ボリュームになった場合、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. メニュー：Storage[Synchronous Mirroring]を選択します。
2. 役割を変更するボリュームを含むミラーペアを選択し、メニュー：その他[役割の変更]を選択します。

   確認のメッセージが表示されます。

3. ボリュームの役割を変更することを確認し、*役割の変更*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、役割変更が要求された際にリモートストレージアレイに接続できないと、システムは「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を表示します。*はい*をクリックして役割変更を強制します。

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。

SANtricity System Managerでミラーペアの同期設定を変更する

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。

タスク概要

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. メニュー：Storage[Synchronous Mirroring]を選択します。
2. 編集するミラーペアを選択し、メニュー：その他［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。

同期優先度について

同期優先度は5段階で設定できます。

- 最低
- 低
- 中
- 高
- 最高

同期優先度を最低レートに設定すると、I/Oアクティビティが優先され、再同期処理に時間がかかります。同期優先度を最高レートに設定すると、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が出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。

   - **Manual**（推奨オプション）-- ミラーリングされたペアとの通信が復旧した後、同期を手動で再開する必要がある場合は、このオプションを選択してください。このオプションは、データ復旧のための最良の機会を提供します。
   - 自動 — このオプションを選択すると、ミラーリングされたペアとの通信が復旧した後、自動的に再同期が開始されます。

5. *保存*を選択します。

SANtricity System Managerで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。

タスク概要

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 ペアに関して以下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. メニュー：Storage[Synchronous Mirroring]を選択します。
2. 削除するミラー ペアを選択し、メニューの Uncommon Tasks [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 ペアを削除することを確認し、* 削除 * をクリックします。

結果

System Manager は以下の操作を実行します。

- 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へ、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 ペアの削除を反映して[同期ミラーリング]タイルを更新します。

ミラーリングの非アクティブ化

SANtricity System Managerで非同期ミラーリングを無効にする

ローカルとリモートのストレージ アレイ間の非同期ミラーリングを非アクティブ化すると、ストレージ アレイの専用ポートを通常の用途に戻すことができます。

開始する前に

- すべてのミラー関係を削除しておく必要があります。ローカルとリモートのストレージ アレイからすべてのミラー整合性グループとミラー ペアが削除されていることを確認してください。
- 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。

タスク概要

非同期ミラーリングを非アクティブ化すると、ローカルとリモートのストレージ アレイでミラー処理が実行されなくなります。

手順

1. メニュー：Storage[Asynchronous Mirroring]を選択します。
2. メニューで「Uncommon Tasks」[Deactivate]を選択してください。

   確認のメッセージが表示されます。

3. *はい*を選択して確認します。

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。

SANtricity System Managerで同期ミラーリングを無効にする

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。

開始する前に

すべての同期ミラー関係を削除しておく必要があります。ストレージ アレイからすべてのミラー ペアが削除されていることを確認してください。

手順

1. メニュー：Storage[Synchronous Mirroring]を選択します。
2. メニューで「Uncommon Tasks」[Deactivate]を選択してください。

   確認のメッセージが表示されます。

3. *はい*を選択して確認します。

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。

SANtricity System Managerの非同期ミラーリングに関するよくある質問

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

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 ボリュームの状態が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。同期ミラーリングではプライマリ 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、セカンダリ ボリュームは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。

非同期ミラーリング	同期ミラーリング
• 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。	予約容量
• 複数 ミラー ペアごとにリザーブ容量ボリュームが1個必要です。	• 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。
コミュニケーション	• **iSCSI** および **Fibre Channel** 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場合、どのような理由が考えられますか**?**

ミラーリングは、SANtricity Unified Managerインターフェイスで設定されます。

EF600/EF600CまたはEF300/EF300Cストレージアレイでは、同期ミラーリングは利用できません。

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は、Unified Managerで検出されている必要があります。
- Unified Managerは、ストレージアレイ用の有効なSSL証明書を備えている必要があります。Unified

Managerから、自己署名証明書を受け入れるか、CA署名証明書をインストールすることができます。

設定手順については、次を参照してください。

- "Create asynchronous mirrored pair（Unified Manager）"
- "Create synchronous mirrored pair（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。

EF600/EF600CまたはEF300/EF300Cストレージ システムでは、同期ミラーリングは利用できません。

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ます。

Unified Managerの以下の要件を満たしてください：

- 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は、ストレージアレイに対して有効なSSL証明書を表示している必要があります。Unified Managerを使用して、メニューの「証明書」[証明書管理]に移動することで、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 アレイ内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。（ストレージ アレイごとに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 SANtricity Unified Manager インターフェイスで設定し、SANtricity System Manager でペアを管理します。

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 アレイ内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。（ストレージ アレイごとに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。
- リモート ストレージ アレイにセカンダリ ボリュームを作成するための十分な空き容量（ミラーリングするプライマリ ボリュームと同等以上）が必要です。
- Web Services ProxyとUnified Managerをインストールしました。ミラーリングされたペアは、Unified Managerのインターフェースで設定されます。
- Unified Managerで2つのストレージアレイが検出されます。
- ストレージアレイには、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**?**

一般的には、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 ボリューム上のデータブロックの大部分が変更されます。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て、プライマリ ボリュームへの典型的なI/Oアクティビティを把握してください。

ミラー ペアのリザーブ容量を増やすには、次のいずれかの手順を実行します。

- ミラーリングされたペアボリュームの容量パーセンテージを調整するには、メニューの Storage[Pools 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。

  プールにもボリューム グループにも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、プールまたはボリューム グループには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、未使用のドライブという形で未割り当て容量を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」である必要があり、変更状態であってはなりません。

- 容量を増やすために使用するプールまたはボリューム グループには、空き容量が存在する必要があります。

非同期ミラーリング処理の予約容量は、通常、ベースボリュームの20%です。ベースボリュームに多くの変更が発生すると思われる場合、またはストレージオブジェクトのコピーサービス処理の推定寿命が非常に長い場合は、より高い割合を使用してください。

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、この容量で十分です。必要な容量は、ベース ボリュームへの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 サービス操作を使用する予定期間によって異なります。

一般的に、以下の条件のいずれか、または両方が当てはまる場合は、予約容量の割合を高く設定してください：

- 特定のストレージオブジェクトのコピーサービス操作の寿命が非常に長い場合。
- 大量のI/Oアクティビティにより、ベースボリューム上のデータブロックの大部分が変更される場合。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て、ベースボリュームへの典型的なI/Oアクティビティを把握してください。

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**?**

この表は、リモート ストレージ アレイ上のデータが表示できない場合に「利用不可」という値を表示します。

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。

プールおよびボリューム 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際には、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 グループのステータスが最適でない。
- 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。次のいずれかに該当するボリュームは対応しない場合があります。

- 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る。

> EF600およびEF300のコントローラでは、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 ボリュームで、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。そうでない非同期ミラー 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 アレイ上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。

使用に適さないボリュームはリストには表示されません。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 ボリュームがDA対応の場合、セカンダリ ボリュームもDA対応である必要があります。
  - プライマリ ボリュームがDA有効になっていない場合、セカンダリ ボリュームもDA有効になっていてはいけません。

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アドレスが変更されると、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構成されているミラー整合性グループに関連付けられた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信し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、リモートストレージアレイにアレイ間メッセージを送信できない場合、システムは接続の問題に関するアラートを送信します。ローカルストレージアレイとの接続を再確立するには、「リモートIPアドレスの更新」オプションを使用してください。

SANtricity System Managerの同期ミラーリングに関するよくある質問

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

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 ボリュームの状態が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。同期ミラーリングではプライマリ 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、セカンダリ ボリュームは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。	予約容量
• 複数 ミラー ペアごとにリザーブ容量ボリュームが1個必要です。	• 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。
コミュニケーション	• **iSCSI** および **Fibre Channel** 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。

- ボリュームが標準以外のボリューム（Snapshotボリューム、シン ボリュームなど）である。
- 最適状態でない。
- すでにミラー関係に参加している。

同期ミラーリング - リモート ストレージ アレイのボリュームが一部表示されないのはなぜですか?

リモート ストレージ アレイ上のセカンダリ ボリュームを選択すると、そのミラー ペアに対応するすべてのボリュームのリストが表示されます。

使用に適さないボリュームはリストには表示されません。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。

- ボリュームが標準以外のボリューム（Snapshotボリューム、シン ボリュームなど）である。
- 最適状態でない。
- すでにミラー関係に参加している。
- Data Assurance（DA）を使用する場合、プライマリ ボリュームとセカンダリ ボリュームでDA設定を同じにする必要があります。
  - プライマリ ボリュームがDA対応の場合、セカンダリ ボリュームもDA対応である必要があります。
  - プライマリ ボリュームがDA有効になっていない場合、セカンダリ ボリュームもDA有効になっていてはいけません。

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 SANtricity Unified Manager インターフェイスで設定し、SANtricity System Manager でペアを管理します。

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 アレイ内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。
- ローカルストレージアレイとリモートストレージアレイは、Fibre Channelファブリックを介して接続されています。
- 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。（ストレージ アレイごとに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。
- リモート ストレージ アレイにセカンダリ ボリュームを作成するための十分な空き容量（ミラーリングするプライマリ ボリュームと同等以上）が必要です。
- Web Services ProxyとUnified Managerをインストールしました。ミラーリングされたペアは、Unified Managerのインターフェースで設定されます。
- Unified Managerで2つのストレージアレイが検出されます。

同期の優先順位は同期速度にどのような影響を与えますか？

同期優先度は、システム パフォーマンスに対して同期アクティビティにどれだけの処理時間を割り当てるかを定義します。

プライマリ ボリュームのコントローラ所有者が、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I/O書き込みと、セカンダリ ボリュームへの関連するリモート書き込みを処理します。再同期はコントローラの処理リソースをI/Oアクティビティから転用するため、ホスト アプリケーションのパフォーマンスに影響を与える可能性があります。

同期の優先順位付けにかかる時間や、同期の優先順位付けがシステムパフォーマンスに及ぼす影響を判断する際は、以下のガイドラインを参考にしてください。

同期優先度について

指定できる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、再同期に時間がかかります。最高では再同期が優先されますが、システム パフォーマンスが低下する可能性があります。

次のガイドラインは、各優先度の大まかな違いを示しています。

完全同期の優先レート	最高同期率と比較した経過時間
最低	約8倍
低	約6倍
中	約3.5倍
高	約2倍

ボリューム サイズとホスト I/O レート負荷は、同期時間の比較に影響します。

手動同期ポリシーの使用が推奨されるのはなぜですか**?**

手動での再同期を推奨します。なぜなら、手動での再同期を行うことで、データ復旧の可能性を最大限に高める方法で再同期プロセスを管理できるからです。

自動再同期ポリシーを使用し、再同期中に断続的な通信問題が発生した場合、セカンダリ ボリュームのデータが一時的に破損している可能性があります。再同期が完了すると、データが修正されます。

リモート ストレージ

SANtricity System Managerのリモート ストレージ機能について説明します

リモート ストレージ機能が搭載されている場合、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**?**

_Remote Storage_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 システムは、別のEシリーズ システムまたは別のベンダーのシステムにすることができます。この機能は、機器のアップグレード時など、ダウンタイムを最小限に抑えながらデータ移行を効率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、この機能をサブモデルID（SMID）で有効にする必要があります。

詳細については、以下を参照してください。

- "リモート ストレージの仕組み"
- "リモート ストレージに関する用語"
- "リモート ストレージの要件"
- "リモート ストレージ ボリュームの要件"

この機能でデータをインポートするにはどうすればよいですか?

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。このウィザードは、メニューの「ストレージ」→「リモートストレージ」から利用できます。

詳細については、以下を参照してください。

- "リモート ストレージのインポート"
- "データ インポートの進捗管理"

概念

SANtricity ソフトウェアでのリモート 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に、データ移行を合理化してダウンタイムを最小限に抑えるのに役立ちます。

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てから、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、ハードウェアの接続を準備します。

これらの手順については、リモートストレージ機能のユーザーガイドで詳しく説明されています。ユーザーガイドは、EシリーズおよびSANtricityドキュメンテーションセンター "Remote Storage Volumesの概要"、および "リモート ストレージ テクニカル レポート"から入手できます。

> 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 システムで以下を実行します。

1. 各コントローラからリモート ストレージ システムへのiSCSI接続が確立されていることを確認します。この接続により、ローカルのEシリーズ ストレージ システムがiSCSIイニシエータとして機能し、リモート ストレージ システムでホストとして設定できます。
2. インポート処理のデスティネーション ボリュームを作成します。リモート ストレージ システム上のソース ボリューム以上の容量があり、ブロック サイズが同じで、マッピングされていないボリュームを作成してください。"ボリュームの作成"を参照してください。
3. ローカルのEシリーズ システムのiSCSI修飾名（IQN）をSystem Managerインターフェイスから取得します。IQNは後でローカルのEシリーズ システムをリモート ストレージ システムのホストとして設定する際に使用されます。System Managerで、メニュー：Settings[System > iSCSI settings > Target IQN]に移動します。

リモート ストレージ システムで以下を実行します。

1. IQNを使用して、ローカルのEシリーズ システムをリモート システムでホストとして設定します。その際、適切なホスト タイプを設定してください。
   - リモート システムがEシリーズ モデルの場合は、"ホストとホスト クラスタの概要"を参照してください。ホスト タイプは「Factory Default」を使用してください。
   - リモート システムが別のベンダーの製品の場合は、利用可能なオプションに基づいて適切なホスト タイプを選択してください。
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. 新しく作成したローカルのEシリーズ ストレージ システムの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次の情報をリモート ストレージ システムから収集します。
   - iSCSI Qualified Name（IQN）
   - iSCSI IPアドレス
   - ソースボリュームのLUN番号

System Managerのセットアップ

次のワークフローに従って、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. システムマネージャインターフェイスのリモートストレージウィザードを使用して、リモートストレージデバイス（データ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. [処理の表示]ダイアログまたは[実行中の処理]パネルで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. インポートが完了したら、必要に応じてソース ボリュームとターゲット ボリュームの間の接続を解除します。将来のインポート用に接続を残しておくこともできます。

SANtricity ソフトウェアのリモートストレージの用語について学ぶ

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	概要
IQN	iSCSI Qualified Name（IQN）の頭字語。iSCSIイニシエータまたはiSCSIターゲットの一意の名前です。
LUN	論理ユニット番号。論理ユニットを識別するために使用し、アクセス用にホストに提示可能です。
リモート ストレージ システム	最初にデータが存在するストレージ システム。リモート ストレージ システムは、Eシリーズ システムでも、別のベンダーのシステムでもかまいません。
リモート ストレージ デバイス	リモート システム上の、最初にデータが保存されてい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」と呼びます。

期間	概要
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するための情報を含むオブジェクト。リモート ストレージ システムのIQNとIPアドレスです。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 システムの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。
Volume	データが格納されているコンテナ。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。

SANtricity ソフトウェアのリモートストレージ機能の要件について説明します

リモート ストレージ機能を使用する前に、次の要件と制限事項を確認してください。

サポートされるプロトコル

サポートされるプロトコルは次のとおりです。

- iSCSI
- IPv4

最新のEシリーズのサポートおよび構成情報については、 "NetApp Interoperability Matrix Tool"を参照してください。

ハードウェア要件

Eシリーズ ストレージ システムの要件は次のとおりです。

- コントローラ×2（デュプレックス モード）
- 1つ以上のiSCSI接続でリモート ストレージ システムと通信できるよう、両方のEシリーズ コントローラにiSCSIが必要
- SANtricity OS 11.71以降
- サブモデルID（SMID）でリモート ストレージ機能が有効になっている

リモート システムは、Eシリーズ ストレージ システムでも別のベンダーのシステムでもかまいません。リモート システムの要件は次のとおりです。

- 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。

- ミラーリングが無効になっている必要がある
- Eシリーズ システム上のデスティネーション ボリュームにSnapshotがない

- インポート開始前に、Eシリーズ システム上のデスティネーション ボリュームがどのホストにもマッピングされていない
- Eシリーズ システム上のデスティネーション ボリュームでリソース プロビジョニングが無効になっている
- リモート ストレージ ボリュームを1つ以上のホストに直接マッピングすることはできない
- 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ていません。
- SMcliはサポートされていません。
- VMware Datastoreはサポートされていません。
- インポートペアが存在する場合、関係性／インポートペア内のストレージ システムは一度に1つしかアップグレードできません。

SANtricityソフトウェアのリモートストレージボリューム要件について学ぶ

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 ボリュームは「リモート ストレージ ボリューム」と呼ばれます。このボリュームは次の基準を満たす必要があります。

- 別のインポートには使用できない
- ステータスがオンラインでなければならない

インポートが開始すると、コントローラ ファームウェアがバックグラウンドでリモート ストレージ ボリュームを作成します。このバックグラウンド プロセスのため、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 システムの他の標準ボリュームと同様に扱われますが、次の点が異なります。

- 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る
- 他のボリューム コピーやSnapshotの候補として使用できない
- インポートの実行中はData Assuranceの設定を変更できない
- 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ない

各リモート ストレージ ボリュームは1つのリモート ストレージ オブジェクトにのみ関連付けられますが、リモート ストレージ オブジェクトは複数のリモート 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 ボリュームは次の情報を組み合わせて一意に識別されます。

- リモート ストレージ オブジェクトID
- リモート ストレージ デバイスのLUN番号

ターゲット ボリュームの候補

ターゲット ボリュームは、ローカルのEシリーズ システム上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 ボリュームは次の基準を満たす必要があります。

- RAID / DDPボリュームである
- リモート ストレージ ボリューム以上の容量がある
- リモート ストレージ ボリュームとブロック サイズが同じ
- 有効な状態（最適）である
- 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どの関係も確立できない
- 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、動的容量削減、またはデフラグメンテーションなどの再構成操作を実行中にすることはできません。
- インポート開始前にホストにマッピングすることはできない（インポート完了後はマッピングできる）
- Flash Read Cache（FRC）が有効になっていない

System Managerのリモート ストレージ インポート ウィザードではこれらの要件が自動的にチェックされます。デスティネーション ボリュームの選択肢には、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 ストレージの管理

SANtricity System Manager でリモート ストレージをインポート

リモート システムからローカルのEシリーズ ストレージ システムへのストレージのインポートを開始するには、リモート ストレージ インポート ウィザードを使用します。

開始する前に

- Eシリーズ ストレージ システムがリモート ストレージ システムと通信するように設定されている必要があります。

> ハードウェア構成については、 "ハードウェアの設定"のEシリーズおよびSANtricityドキュメントセンターから入手できるリモート ストレージ機能のユーザーガイド、および "リモート ストレージ テクニカル レポート"に記載されています。

- リモート ストレージ システムについて、次の情報を収集します。
  - iSCSI IQN
  - iSCSI IPアドレス
  - リモート ストレージ デバイス（ソース ボリューム）のLUN番号
- ローカルのEシリーズ ストレージ システムで、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。"ボリュームの作成"を参照してください。ターゲット ボリュームは次の要件を満たす必要があります。
  - ブロック サイズがリモート ストレージ デバイス（ソース ボリューム）と同じである。
  - リモート ストレージ デバイス以上の容量がある。
  - 状態が「最適」で、かつ使用可能である。

要件の全リストについては、"リモート ストレージ ボリューム要件"を参照してください。

- 推奨事項： インポート処理を開始する前に、リモート システムのボリュームをバックアップしてください。

タスク概要

このタスクでは、リモート ストレージ デバイスとローカルのEシリーズ ストレージ システム上のボリュームの間にマッピングを作成します。設定を終了すると、インポートが開始します。

> インポート操作とその完了時間には多くの要因が影響するため、まずは小規模な「test」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、すべての接続が期待どおりに機能し、インポート操作が適切な時間内に完了することを確認してください。

手順

1. メニュー：Storage[Remote storage]を選択します。
2. **Import Remote Storage** 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「ステップ 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 システム用のIPアドレスを追加してください。完了したら、「次へ」をクリックしてください。

   フィールドの詳細

設定	概要
Name	System Managerでリモート ストレージ デバイスを識別するための名前を入力します。 名前は最大30文字までで、文字、数字、およびアンダースコア（_）、ダッシュ（-）、ハッシュ記号（#）などの特殊文字のみを含めることができます。名前にスペースを含めることはできません。
iSCSI接続プロパティ	リモート ストレージ デバイスの接続プロパティを入力します。 • **iSCSI Qualified Name（IQN）**：iSCSI IQN を入力してください。 • **IP Address**：IPv4アドレスを入力してください。 • ポート：送信元デバイスと送信先デバイス間の通信に使用するポート番号を入力してください。デフォルトでは、ポート番号は3260です。

   *Next*をクリックすると、Configure Sourceパネルの*Step 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なるボリュームの候補が表示されます。一部のボリュームは、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候補リストに表示されま

せん。

5. 表から、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選択します。必要に応じて、スライダーを使用してインポートの優先順位を変更します。*Next*をクリックします。次のダイアログボックスで、 `continue`と入力して操作を確認し、*Continue*をクリックします。

   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追加分の容量は報告されません。新たな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]パネルが表示されます。

6. Reviewパネルで設定が正確であることを確認し、*Finish*をクリックしてインポートを開始します。

   別のダイアログ ボックスが開き、別のインポートを開始するかどうかを確認するメッセージが表示されます。

7. 必要に応じて、*Yes*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てください。*Yes*をクリックすると、Configure Sourceパネルの*Step 1a*に戻り、既存の設定を選択するか、新しい設定を追加できます。別のインポートを作成しない場合は、*No*をクリックしてダイアログボックスを閉じます。

   インポート プロセスが開始すると、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。このプロセスの実行中にホストがターゲット ボリュームに新しいデータを書き込んだ場合、新しく書き込まれたデータはリモート 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[処理を表示]ダイアログで、処理の進捗状況を確認します。

結果

インポート処理が完了するまでの時間は、リモート ストレージ システムのサイズ、インポートの優先度設定、ストレージ システムと関連ボリュームの両方のI/O負荷によって異なります。

インポートが完了すると、ローカル ボリュームはリモート ストレージ デバイスの複製となります。

終了後の操作

2つのボリューム間の関連付けを解除する準備ができたら、「進行中の操作」ビューからインポートオブジェクトの*切断*を選択します。接続が切断されると、ローカルボリュームのパフォーマンスは正常に戻り、リモート接続の影響を受けなくなります。

SANtricity System Managerでリモートストレージインポートの進捗状況を管理

インポート プロセスが開始したら、その進捗状況を表示して操作を実行できます。

タスク概要

インポート処理ごとに、[実行中の処理]ダイアログに進捗状況と推定残り時間が表示されます。実行できる操作には、インポート優先度の変更、処理の停止と再開、処理の切断があります。

ホーム画面（メニュー：ホーム［進行中の操作を表示］）からも、進行中の操作を表示できます。

手順

1. リモートストレージページから、*操作の表示*を選択します。

   [実行中の処理]ダイアログ ボックスが表示されます。

2. 必要に応じて、*Actions*列のリンクを使用して、操作の停止と再開、優先順位の変更、または操作からの切断を行うことができます。
   - 優先度の変更 — 進行中または保留中の操作の処理優先度を変更するには、*優先度の変更*を選択します。操作に優先順位を付けてから、*OK*をクリックしてください。
   - 停止 — *停止*を選択すると、リモートストレージデバイスからのデータコピーが一時停止します。インポートペア間の関係は維持されており、インポート操作を再開する準備ができたら*再開*を選択できます。
   - **Resume** — *Resume*を選択すると、停止または失敗したプロセスが中断したところから再開されます。次に、Resume操作に優先度を設定し、*OK*をクリックします。この操作は、インポートを最初からやり直すものでは_ありません_。プロセスを最初からやり直す場合は、*Disconnect*を選択し、Import Remote Storage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間の関係を解除するには、*切断*を選択します。

SANtricity System Managerでリモートストレージの接続設定を変更します

[設定の表示 / 編集]オプションを使用して、リモート ストレージ構成の接続設定を編集、追加、または削除できます。

タスク概要

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。処理の中断を回避するため、接続プロパティの変更はインポートを実行していないときに行ってください。

手順

1. メニュー：Storage[Remote storage]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. *View/Edit Settings*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. *Connection Properties*タブをクリックします。

   リモート ストレージ インポートに対して設定されているIPアドレスとポートが表示されます。
5. 次のいずれかを実行します。
   - **Edit** — リモートストレージオブジェクトに対応する行項目の横にある **Edit** をクリックします。修正後のIPアドレスおよび/またはポート情報を該当欄に入力してください。
   - 追加 — *追加*をクリックし、指定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、新しい接続がリモートストレージオブジェクトのリストに表示されます。
   - 削除 — リストから目的の接続を選択し、*削除*をクリックします。操作を確認するには、 `delete`を指定されたフィールドに入力し、*削除*をクリックします。接続はリモートストレージオブジェクトのリストから削除されます。
6. *保存*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。

SANtricity System Managerでリモートストレージオブジェクトを削除する

インポート完了後に、ローカル デバイスとリモート デバイスの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。

開始する前に

削除するリモート ストレージ オブジェクトにインポートが関連付けられていないことを確認します。

タスク概要

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 デバイスの間の接続が削除されます。

手順

1. メニュー：Storage[Remote storage]を選択します。
2. 削除するリモート ストレージ オブジェクトをリストから選択します。
3. *削除*をクリックします。

   [リモート ストレージ接続の削除を確認]ダイアログ ボックスが表示されます。

4. `remove`と入力し、*削除*をクリックして操作を確定します。

   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。

SANtricity System Managerのリモート ストレージに関するよくある質問

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

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システム接続のセットアップについては、以下を参照してください。

- "iSCSIポートの設定"
- "リモート ストレージ テクニカル レポート"

リモート ボリュームを削除するように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 ボリュームが最大数に達すると、使用されていないリモート ボリュームが自動的に検出され、削除するように求められます。

ごくまれに、使用されていないリモート ボリュームが作成プロセスでクリーンアップされないことがあります。追加のインポート処理を開始する前に、システムが最適でネットワーク接続が安定していることを確認してください。

デスティネーション アレイ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 ストレージ機能のインポートを設定する際に、ブロック サイズ、容量、またはボリュームの可用性が原因で一部のボリュームがターゲットの候補リストに表示されないことがあります。

リストに表示されるには、ボリューム候補が以下の条件を満たしている必要があります。

- リモート ボリュームと同じまたはそれ以上の容量がある。
- ブロック サイズがリモート ボリュームと同じである。
- 現在のステータスが「最適」である。

次の条件に該当するボリューム候補はリストから除外されます。

- ボリューム コピー、Snapshot、ミラーリングのいずれかの関係が確立されている。
- 再構成処理を実行中である。
- 別のデバイス（ホストまたはホスト クラスタ）にマッピングされている。
- 読み取りフラッシュ キャッシュが有効になっている。

インポートするリモート ボリュームについて、どのような点に注意する必要がありますか?

リモート ストレージ機能を使用する場合は、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、ブロック サイズが同じ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 ストレージ機能では、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 システムのボリュームにデータをコピーできます。この機能を使用する前に、次のガイドラインを確認してください。

構成

リモート ストレージのインポートを開始する前に、次の項目を実施、確認しておく必要があります。

- ローカルEシリーズ ストレージ システムの各コントローラーがリモート システムへのiSCSI接続を備え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。ソース ボリューム以上の容量があり、ブロック サイズがソース ボリュームと同じで、マッピングされていないボリュームを作成してください。"ボリュームの作成"を参照してください。
- iSCSI修飾名（IQN）を使用して、ローカルEシリーズ ストレージ システムをリモート システムのホストとして設定します。IQNは、メニューの「設定」[システム > iSCSI設定 > ターゲットIQN]から確認できます。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するようにしてください。
- リモート ストレージ システム上の選択したボリュームについて、すべてのI/Oを停止し、ファイルシステムをアンマウントして、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Eシリーズ ストレージ システムホストに、リモート システムのボリュームを割り当てます。

- インポートを作成できるように、リモート ストレージ システムから次の情報を収集します。
  - iSCSI Qualified Name（IQN）
  - iSCSI IPアドレス
  - ソースデータの発生元となるリモート ストレージ デバイスのLUN番号
- インポート プロセスを開始すると、ローカル デスティネーション ボリューム全体がコピーされたデータで上書きされます。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、インポートの完了後にリモート ストレージ デバイス上のボリュームにすべて伝播されます。そのため、インポート プロセスを開始する前に、リモート ストレージ システム上のボリュームをバックアップすることを推奨します。

インポート プロセス

インポート プロセスの手順を次に示します。

1. System Managerインターフェイスにアクセスし、*リモート ストレージ*ページに移動します。*インポート*を選択して、新しいインポートの作成を開始します。詳細な手順については、"リモート ストレージのインポート"を参照してください。

   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。

   インポートが開始したら、ターゲット ボリュームをマッピングできます。インポート処理の所要時間は、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 システムと関連ボリュームの両方のI/O負荷によって異なります。

   インポートが完了すると、ターゲット ボリュームがソース ボリュームの複製となります。

3. マッピング関係を解除する準備ができたら、*進行中の操作*パネルからインポート オブジェクトに対して*切断*を実行します。

インポートが切断されると、ローカル デスティネーション 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。

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。

- ミラーリングが無効になっている必要がある
- Eシリーズ システム上のデスティネーション ボリュームにSnapshotがない
- インポート開始前に、Eシリーズ システム上のデスティネーション ボリュームがどのホストにもマッピングされていない
- Eシリーズ システム上のデスティネーション ボリュームでリソース プロビジョニングが無効になっている
- リモート ストレージ ボリュームを1つ以上のホストに直接マッピングすることはできない
- 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ていません。

- SMcliはサポートされていません。
- VMware Datastoreはサポートされていません。
- インポートペアが存在する場合、関係性／インポートペア内のストレージ システムは一度に1つしかアップグレードできません。

追加情報

リモートストレージ機能に関する詳細情報は、 "リモート ストレージ テクニカル レポート"から入手できます。

ハードウェア コンポーネント

SANtricity System Managerでハードウェアコンポーネントを表示および管理する

[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、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?

以下のコンポーネントについて、ステータスを確認し、関連するいくつかの機能を実行できます。

- シェルフ — シェルフ は、ストレージアレイのハードウェア（コントローラ、電源/ファンキャニスター、ドライブ）を格納するコンポーネントです。シェルフは、最大12台、24台、または60台のドライブを収納できる3つのサイズをご用意しています。
- コントローラ — _コントローラ_とは、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 — _ドライブ_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）のいずれかです。シェルフのサイズに応じて、最大12台、24台、または60台のドライブをシェルフに設置できます。

詳細については、以下を参照してください。

- "[ハードウェアページ"]
- "ハードウェアの用語"

ハードウェア コンポーネントを表示するにはどうすればよいですか?

ストレージアレイの物理コンポーネントを図解した Hardware ページをご覧ください。アレイシェルフの前面表示と背面表示を切り替えるには、シェルフビューの右上にある **Drives** タブまたは **Controllers** タブを選択します。

詳細については、以下を参照してください。

- "シェルフ コンポーネントのステータスと設定の表示"
- "コントローラの設定の表示"
- "ドライブのステータスと設定の表示"

関連情報

ハードウェアに関連する概念の詳細については、以下を参照してください。

- "コントローラの状態"
- "ドライブの状態"
- "シェルフ損失の保護およびドロワー損失の保護"

概念

SANtricity System Managerのハードウェアページとコンポーネント

[ハードウェア]ページでは、ストレージ アレイの物理コンポーネントが図解されています。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、およびコントローラーを収納します。
- 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2つの入出力モジュール（IOM）が含まれています。IOM（環境サービスモジュール（ESM）とも呼ばれる）には、ドライブシェルフとコントローラシェルフを接続するSASポートが含まれています。

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。シェルフビューの右上にある*ドライブ*タブまたは*コントローラ*タブを選択することで、2つのビューを切り替えることができます。ページ下部から*前面をすべて表示*または*背面をすべて表示*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、次の内容が表示されます：

- 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（コントローラシェルフの場合）、またはIOMと電源/ファンキャニスタ（ドライブシェルフの場合）。

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）サーバを設定します。
- コントローラのステータスおよび設定を表示します。
- 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、設定を変更することを許可します。
- 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。

システムの

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）を搭載することができます。シェルフのサイズに応じて、最大12本、24本、または60本のドライブをシェルフに設置できます。

ドライブに関連して次の機能を実行できます。

- シェルフ内でドライブの場所を確認しやすいように、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および設定を表示します。
- 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すると、交換前にドライブの内容をコピーすることができます）。
- 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。

SANtricity ソフトウェアで使用されるハードウェア用語について学ぶ

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の用語：

コンポーネント	概要
ベイ	ベイとは、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内のスロットのことです。
コントローラ	コントローラは、基板、ファームウェア、および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が収容されています。コントローラキャニスタには、コントローラ、ホスト インターフェイス カード（HIC）、およびバッテリが収納されています。
ドライブ	ドライブは、データの物理ストレージ メディアとして使用される電磁的な機械デバイスまたはソリッド ステート メモリ デバイスです。
ドライブ シェルフ	ドライブシェルフ（拡張シェルフとも呼ばれる）には、一連のドライブと2つの入出力モジュール（IOM）が含まれています。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とは、ドライブシェルフとコントローラシェルフを接続するためのSASポートを備えた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取り付けられるエンクロージャです。ストレージ アレイのハードウェア コンポーネントがシェルフに格納されます。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	概要
コントローラ	コントローラは、基板、ファームウェア、および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が収容されています。コントローラキャニスタには、コントローラ、ホスト インターフェイス カード（HIC）、およびバッテリが収納されています。
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	ドメイン ネーム システム（DNS）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用の命名システムです。DNSサーバが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つのコントローラ 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です。
全二重 / 半二重接続	全二重通信と半二重通信は、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のみ通信できます（一方のデバイスがメッセージを送信している間、もう一方のデバイスがそれを受信します）。
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	インターネット制御メッセージプロトコル（ICMP）は、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がメッセージを送信するために使用するプロトコルです。ICMPメッセージは、ホストに到達可能かどうか、およびそのホストとの間でパケットを送受信するのにかかる時間を決定します。
MACアドレス	イーサネットでは、メディアアクセスコントロール識別子（MACアドレス）を使用して、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	概要
管理クライアント	管理クライアントとは、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るコンピュータのことです。
MTU	最大転送単位（MTU）は、ネットワーク内で送信できるパケットまたはフレームの最大サイズです。
NTP	ネットワーク タイム プロトコル（NTP）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に使用されるネットワーク プロトコルです。
シンプレックス構成	シンプレックスとは、ストレージアレイ内の単一コントローラモジュール構成のことです。シンプレックスシステムは、コントローラやディスクパスの冗長性を提供しませんが、冗長なファンと電源を備えています。
VLAN	仮想LAN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	概要
DA	Data Assurance（DA）は、データがコントローラ経由でドライブに転送される際に発生する可能性があるエラーをチェックして修正する機能です。Data Assuranceは、Fibre ChannelなどのDA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際にセキュリティ キーが要求されるようになります。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、取り付けたあとも正しいセキュリティ キーが提供されないかぎりセキュリティ 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（拡張シェルフとも呼ばれる）には、一連のドライブと2つの入出力モジュール（IOM）が含まれています。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、EF300またはEF600ストレージ アレイがリソース プロビジョニングされたボリュームをサポートできるようにするためのものです。
FDEドライブ	フルディスク暗号化（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。ハードディスクには、書き込み時にデータを暗号化し、読み取り時にデータを復号化するASICチップが搭載されています。
FIPSドライブ	FIPSドライブは、連邦情報処理規格（FIPS）140-2レベル2を使用します。これらは基本的に、強力な暗号化アルゴリズムと方法を確保するための米国政府の基準に準拠したFDEドライブです。FIPSドライブは、FDEドライブよりも高いセキュリティ基準を満たしています。
HDD	ハードディスクドライブ（HDD）は、磁気コーティングされた回転式の金属プラッタ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ボリュームグループにおいて、スタンバイドライブとして機能します。これらはデータが含まれていないものの、完全に機能するドライブです。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、コントローラは障害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。

コンポーネント	概要
NVMe	NVMe（Non-Volatile Memory Express）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ースです。NVMeは、従来の論理デバイスインターフェースと比較して、I/Oオーバーヘッドを削減し、パフォーマンスを向上させています。
SAS	Serial Attached SCSI（SAS）は、コントローラとディスクドライブを直接接続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	セキュリティ機能を備えたドライブには、フルディスク暗号化（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあり、いずれも書き込み時にデータを暗号化し、読み取り時にデータを復号化します。これらのドライブは、ドライブセキュリティ機能を使用して追加のセキュリティ対策を講じることができるため、セキュリティ対応ドライブとみなされます。これらのドライブで使用されるボリュームグループおよびプールに対してドライブセキュリティ機能が有効になっている場合、ドライブはセキュア有効状態になります。
セキュリティ有効ドライブ	セキュリティ対応ドライブは、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てから、セキュア対応ドライブ上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、ドライブはセキュリティ対応になります。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を介してのみ可能です。この追加のセキュリティ対策により、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します。
SSD	ソリッドステートディスク（SSD）は、ソリッドステートメモリ（フラッシュメモリ）を使用してデータを永続的に保存するデータストレージデバイスです。SSDは従来のハードディスクをエミュレートするものであり、ハードディスクと同じインターフェースを備えています。

iSCSIの用語：

期間	概要
CHAP	チャレンジハンドシェイク認証プロトコル（CHAP）方式は、初期接続時にターゲットとイニシエータの身元を検証します。認証は、CHAP *secret*と呼ばれる共有セキュリティキーに基づいています。
コントローラ	コントローラは、基板、ファームウェア、および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サーバーとストレージシステム間のデータ伝送のための通信規格です。
ICMP PING応答	インターネット制御メッセージプロトコル（ICMP）は、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がメッセージを送信するために使用するプロトコルです。ICMPメッセージは、ホストに到達可能かどうか、およびそのホストとの間でパケットを送受信するのにかかる時間を決定します。
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EthernetなどのRDMAトランスポート上で動作するようにiSCSIプロトコルを拡張するプロトコルです。
iSNS	Internet Storage Name Service（iSNS）は、TCP/IPネットワーク上のiSCSIおよび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	イーサネットでは、メディアアクセスコントロール識別子（MACアドレス）を使用して、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	管理クライアントとは、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るコンピュータのことです。
MTU	最大転送単位（MTU）は、ネットワーク内で送信できるパケットまたはフレームの最大サイズです。

期間	概要
RDMA	リモート ダイレクト メモリ アクセス（RDMA）は、ネットワーク コンピュータ同士が、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やり取り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	概要
InfiniBand	InfiniBand（IB）は、ハイパフォーマンスサーバーとストレージシステム間のデータ伝送のための通信規格です。
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の範囲で設定できます。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	NVMe（Non-Volatile Memory Express）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ースです。NVMeは、従来の論理デバイスインターフェースと比較して、I/Oオーバーヘッドを削減し、パフォーマンスを向上させています。
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、ホストとストレージ アレイ内のネームスペースの間のアクセス パスを提供します。
NVMeキュー	NVMeインターフェイス経由でのコマンドやメッセージの受け渡しに使用されるキューです。
NVMe サブシステム	NVMeホストに接続されているストレージ アレイです。
RDMA	リモート ダイレクト メモリ アクセス（RDMA）では、ネットワーク インターフェイス カード（NIC）ハードウェアに転送プロトコルを実装することで、サーバはよりダイレクトにデータを送受信できます。
RoCE	RDMA over Converged Ethernet（RoCE）は、イーサネット ネットワーク経由でリモート 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	概要
SSD	ソリッドステートディスク（SSD）は、ソリッドステートメモリ（フラッシュメモリ）を使用してデータを永続的に保存するデータストレージデバイスです。SSDは従来のハードディスクをエミュレートするものであり、ハードディスクと同じインターフェースを備えています。

シェルフ コンポーネントの管理

SANtricity System Managerでハードウェアコンポーネントを表示

[ハードウェア]ページには、コンポーネントを検索しやすくするソートとフィルタの機能が表示されます。

手順

1. *ハードウェア*を選択します。
2. 次の表に記載されている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	概要
ドライブ、コントローラ、およびコンポーネントのビュー	前面と背面の棚表示を切り替えるには、右端から*Drives*または*Controllers & Components*を選択します（表示されるリンクは現在の表示によって異なります）。*Drives*ビューには、ドライブと空いているドライブベイが表示されます。*Controllers & Components*ビューには、コントローラー、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ーベイが表示されます。ページ下部にある*Show all drives*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、物理的属性と論理的属性が異なるタイプのドライブが含まれている場合、*Hardware*ページにはドライブビューフィルターが表示されます。これらのフィルターフィールドを使用すると、ページに表示されるドライブの種類を絞り込むことで、特定のドライブをすばやく見つけることができます。*Show drives that are…*の下にある左側のフィルターフィールドをクリックすると（デフォルトでは*Any drive type*が表示されます）、物理的な属性（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。右側のフィルターフィールドをクリックすると（デフォルトでは*Anywhere in the storage array*と表示されます）、論理属性のドロップダウンリスト（ボリュームグループの割り当てなど）が表示されます。これらのフィルターは、組み合わせて使用することも、個別に使用することもできます。 ストレージアレイに含まれるドライブがすべて同じ物理属性を共有している場合、左側の*Any drive type*フィールドは表示されません。ドライブがすべて同じ論理的な場所にある場合、右側の*Anywhere in the storage array*フィールドは表示されません。
凡例	各コンポーネントは、それぞれの役割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したり折りたたんだりするには、*Legend*をクリックしてください。

機能	概要
ステータス アイコンの詳細の表示	ステータス表示には、可用性の状態に関するテキストによる説明を含めることができます。*Show status icon details*をクリックすると、このステータステキストの表示/非表示を切り替えることができます。
シェルフ / シェルフ アイコン	各シェルフビューには、関連するコマンドのリストと、そのプロパティおよびステータスが表示されます。*Shelf*をクリックすると、コマンドのドロップダウンリストが表示されます。上部にあるアイコンのいずれかを選択すると、コントローラー、IOM（ESM）、電源、ファン、温度、バッテリー、SFPなどの個々のコンポーネントの状態とプロパティを表示することもできます。
シェルフの順序	棚の配置は、ハードウェアのページで変更できます。各棚ビューの右上にある上下の矢印を使用して、棚の上下の順序を変更します。

SANtricity System Managerでコンポーネントのステータスを表示または非表示にする

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. コンポーネントの背面または前面を表示するには、次の手順を実行します。
   - コントローラーと電源/ファンキャニスターのコンポーネントを表示したいのに、ドライブが表示されている場合は、*Controllers & Components*タブをクリックしてください。
   - ドライブを表示したいのに、コントローラーと電源/ファンキャニスターのコンポーネントが表示されている場合は、*Drives*タブをクリックしてください。
3. ポップオーバーのステータスの説明の表示と非表示を切り替えるには、次の手順を実行します。
   - ステータスアイコンの説明をポップオーバーで表示する場合は、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オンにします）。
   - 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確認したい場合は、棚ビューでコンポーネントを選択し、次に*設定の表示*を選択してください。
5. 色分けされたコンポーネントの説明を表示するには、**Legend** を選択してください。

SANtricity System Managerで前面図と背面図を表示

[ハードウェア]ページでは、シェルフの前面ビューまたは背面ビューを表示できます。

タスク概要

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. グラフィックにドライブが表示されている場合は、*Controllers & Components*タブをクリックしてください。

   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. グラフィック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。

   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、ページ下部にある*Show all front*または*Show all back*を選択することもできます。

SANtricity System Managerでシェルフの表示順序を変更する

[ハードウェア]ページに表示されるシェルフの順番を、キャビネット内のシェルフ実際の順番と同じになるように変更できます。

手順

1. *ハードウェア*を選択します。
2. シェルフビューの右上にある上向きまたは下向きの矢印を選択すると、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できます。

SANtricity System Managerで棚の位置表示ライトを点灯する

[ハードウェア]ページに表示されているシェルフの物理的な場所を特定するために、シェルフのロケーター ライトを点灯できます。

手順

1. *ハードウェア*を選択します。
2. コントローラー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、次に*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. 棚の位置が確定したら、ダイアログボックスに戻り、*オフにする*を選択してください。

SANtricity System Managerでシェルフ**ID**を変更する

シェルフIDは、ストレージ アレイ内のシェルフを一意に識別する番号です。シェルフに00または01から始まる連番が振られており、シェルフ画面の左上に表示されます。

タスク概要

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ができます。

手順

1. *ハードウェア*を選択します。

2. コントローラー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、次に*IDの変更*を選択します。
3. 棚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. 利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の棚の並び順が変更される場合があります。必要に応じて、各棚の右上にある上下の矢印を使用して、順番を変更できます。

SANtricity System Managerでシェルフコンポーネントのステータスと設定を表示

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

タスク概要

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一式を1つのシェルフに収納します。
- **Controller shelf** — 1つの棚に、ドライブ一式、1つまたは2つのコントローラーキャニスター、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を収納します。

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、次に*設定の表示*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を示すタブが表示されます。選択したシェルフのタイプによっては、表に記載されている一部のタブが表示されない場合があります。

タブ	概要
シェルフ	**Shelf** タブには、以下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。コントローラファームウェアがこの番号を割り当てますが、menu：Shelf[Change ID]を選択して変更できます。 • シェルフパス冗長性 — シェルフとコントローラ間の接続に代替方法が設定されているか（はい）、設定されていないか（いいえ）を指定します。 • 現在のドライブの種類 — ドライブに組み込まれているテクノロジーの種類を示します（たとえば、セキュリティ機能を備えたSASドライブなど）。ドライブの種類が複数ある場合は、両方のテクノロジーが表示されます。 • シリアル番号 — シェルフのシリアル番号を表示します。

タブ	概要
IOM（ESM）	*IOMs（ESMs）*タブには、入出力モジュール（IOM）のステータスが表示されます。IOMは環境サービスモジュール（ESM）とも呼ばれます。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（配線ミス）、または未認証のいずれかになります。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。 *その他の設定を表示*を選択すると、最大データレートと現在のデータレート、およびカード通信の状態（はいまたはいいえ）が表示されます。 このステータスは、Shelfドロップダウンリストの横にあるIOMアイコンを選択して確認することもできます。
電源装置	*Power Supplies*タブには、電源キャニスタと電源自体のステータスが表示されます。ステータスは、Optimal、Failed、Removed、またはUnknownのいずれかになります。電源の部品番号も表示されます。 このステータスは、Shelfドロップダウンリストの横にある電源アイコンを選択して確認することもできます。
ファン	*ファン*タブには、ファンキャニスターとファン本体の状態が表示されます。ステータスは、最適、失敗、削除済み、または不明のいずれかになります。 ファンアイコン（シェルフドロップダウンリストの横）を選択することでも、このステータスを確認できます。
温度	*Temperature*タブには、センサー、コントローラー、電源/ファンキャニスターなど、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、Optimal、Nominal temperature exceeded、Maximum temperature exceeded、またはUnknownのいずれかになります。 温度アイコン（シェルフドロップダウンリストの横）を選択することで、このステータスを確認することもできます。
バッテリ	*Batteries*タブには、コントローラーのバッテリーの状態が表示されます。ステータスは、Optimal、Failed、Removed、またはUnknownのいずれかになります。その他の情報には、バッテリーの寿命、交換までの日数、学習サイクル数、学習サイクル間の週数などが含まれます。 シェルフのドロップダウンリストの横にあるバッテリーアイコンを選択することでも、このステータスを確認できます。

タブ	概要
SFP	*SFPs*タブには、コントローラ上の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、Optimal、Failed、またはUnknownのいずれかになります。 **Show more settings** を選択すると、SFPの部品番号、シリアル番号、およびベンダーが表示されます。 このステータスは、Shelfドロップダウンリストの横にあるSFPアイコンを選択して確認することもできます。

3. 閉じる をクリックします。

SANtricity System Managerでバッテリー学習サイクルを更新

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スケジュール設定されます。別のスケジュールを設定する場合は、学習サイクルを調整できます。

タスク概要

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反映されます。

手順

1. *ハードウェア*を選択します。
2. コントローラーシェルフのドロップダウンリストを選択し、次に*設定を表示*を選択します。
3. **Batteries** タブを選択してください。
4. **Update battery learn cycles** を選択します。

   「バッテリー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*をクリックします。

コントローラの管理

SANtricity System Managerのコントローラの状態について説明します

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

オンライン状態は、コントローラの通常動作時の状態です。コントローラが正常に動作しており、I/O処理に使用できます。

コントローラをオンラインにすると、ステータスが最適になります。

オフライン状態

オフライン状態は、通常、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実行した場合、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台ある場合だけです。

コントローラがオフライン状態のときは次の状況になります。

- 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すべて移動されます。
- 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もう一方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、そのコントローラにシリアル ポートまたはネットワーク接続を介してアクセスし、潜在的な問題の分析を行うことができます。
- 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すべて移動されます。
- 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。

Eシリーズコントローラの**IP**アドレス割り当てについて説明します

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アドレスを設定したあと、System Managerを使用して管理ポートでIPv6を有効にすることができます。

ネットワーク ポートが「リンク停止」状態（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に接続された状態）になると、システムはDHCPを介してIPアドレスの取得を試みます。

コントローラの特定のネットワーク ポートでDHCPアドレスを取得できない場合はデフォルトのIPアドレスに

戻りますが、これには3分近く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ときは、次の点に注意してください。

- 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 System Managerを使用します。E2700およびE5600のコントローラに静的IPアドレスを設定するには、SANtricity Storage Managerを使用します。静的IPアドレスの設定後は、リンク停止 / 稼働イベントが発生しても設定が維持されます。
- 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の試行に失敗したときは、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。

SANtricity System Managerで管理ポートを設定

コントローラには、システム管理に使用されるイーサネット ポートが搭載されています。必要に応じて、このポートの送信パラメータとIPアドレスを変更できます。

タスク概要

この手順では、ポート1を選択し、速度およびアドレス指定方式を決定します。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. グラフィックにドライブが表示されている場合は、*Controllers & Components*タブをクリックしてくだ

さい。

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。

   [管理ポートの設定]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	概要
速度と二重モード	ストレージ アレイとネットワークの間の送信パラメータをSystem Managerで自動的に設定する場合は、[自動ネゴシエーション]設定をそのままにします。ネットワークの速度とモードがわかっている場合は、ドロップダウン リストからパラメータを選択します。このリストには、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*をクリックした後に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、最初にIPv4設定のダイアログボックスが開き、次に*次へ*をクリックすると、IPv6設定のダイアログボックスが開きます。

7. IPv4、IPv6、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	概要
DHCP サーバから自動的に設定を取得	設定を自動的に取得する場合は、このオプションを選択します。
静的な設定を手動で指定	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、カット アンド ペーストでアドレスをフィールドに貼り付けることもできます）。IPv4の場合は、ネットワークのサブネットマスクとゲートウェイも指定します。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、メニューの[管理][検出]に移動します。SANtricity Storage Managerを使用する場合は、デバイスをエンタープライズ管理ウィンドウ（EMW）から削除し、メニューの[編集][ストレージアレイの追加]を選択してEMWに再度追加してから、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

コントローラ設定の[管理ポート]タブに、管理ポート設定が表示されます。

SANtricity System Managerで**NTP**サーバアドレスを設定

ネットワーク タイム プロトコル（NTP）サーバへの接続を設定すると、コントローラがNTPサーバを定期的に照会して内部のクロックを更新できるようになります。

開始する前に

- ネットワークにNTPサーバをインストールし、設定する必要があります。
- プライマリNTPサーバとオプションのバックアップNTPサーバのアドレスを確認しておく必要があります。これらのアドレスには、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスを使用できます。

NTPサーバのドメイン名を1つ以上入力した場合は、NTPサーバ アドレスを解決できるようにDNSサーバも設定する必要があります。DNSサーバの設定が必要となるのは、NTPを設定してドメイン名を指定したコントローラだけです。

タスク概要

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. グラフィックにドライブが表示されている場合は、*Controllers & Components*タブをクリックしてください。

   図の表示が切り替わり、ドライブではなくコントローラが表示されます。

3. 設定するコントローラをクリックします。

   コントローラのコンテキスト メニューが表示されます。

4. * Configure NTP server *を選択します。

   [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. コントローラで**NTP**を有効にする（**A***または***B***）を選択します。

   ダイアログ ボックスにその他のオプションが表示されます。

6. 次のいずれかのオプションを選択します。
   - **DHCP**サーバーから**NTP**サーバーアドレスを自動的に取得 — 検出されたNTPサーバー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**サーバーアドレスを手動で指定 — プライマリNTPサーバーアドレスとバックアップNTPサーバーアドレスを入力します。バックアップサーバーはオプションです。（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。）サーバーアドレスは、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す。
7. *オプション：*バックアップNTPサーバーのサーバー情報と認証クレデンシャルを入力します。
8. *保存*をクリックします。

結果

NTPサーバの設定は、コントローラ設定の*DNS / NTP*タブに表示されます。

SANtricity System Managerで**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。

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。このアドレスは、IPv4アドレスでもIPv6アドレスでもかまいません。

タスク概要

この手順では、プライマリDNSサーバとバックアップDNSサーバの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ため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。ただしその場合でも、次の手順でダイアログ 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. グラフィックにドライブが表示されている場合は、*Controllers & Components*タブをクリックしてください。

   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**サーバーから**DNS**サーバーアドレスを自動的に取得 — 検出されたDNSサーバーアドレスが表示されます。

     > 静的な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**サーバーアドレスを手動で指定 — プライマリDNSサーバーアドレスとバックアップDNSサーバーアドレスを入力してください。バックアップサーバーはオプションです。（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。）これらのアドレスは、IPv4アドレスまたはIPv6アドレスのいずれかです。
6. *保存*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、コントローラー設定の*DNS / NTP*タブに表示されます。

SANtricity System Managerでコントローラ設定を表示する

コントローラに関する情報（ホスト インターフェイス、ドライブ インターフェイス、管理ポートのステータスなど）を表示できます。

手順

1. *ハードウェア*を選択します。
2. グラフィックにドライブが表示されている場合は、*Controllers & Components*タブをクリックしてください。

   図の表示が切り替わり、ドライブではなくコントローラが表示されます。

3. 次のいずれかの操作を実行してコントローラの設定を表示します。
   - コントローラー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*のいずれかを選択し、*Next*をクリックします。

     [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、表示するプロパティ設定を切り替えます。

   一部のタブには、右上に*その他の設定を表示*のリンクがあります。

フィールドの詳細

タブ	概要
基本	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。
Cache	コントローラのキャッシュの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、互換性なしのいずれかです。
ホスト インターフェイス	ホスト インターフェイスの情報と各ポートのリンク ステータスが表示されます。ホスト インターフェイスは、コントローラとホスト間の接続です（Fibre ChannelやiSCSIなど）。 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間の接続です（SASなど）。
管理ポート	管理ポートの詳細（コントローラへのアクセスに使用されるホスト名、リモート ログインが有効になっているかどうかなど）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（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るシステム）を接続します。
DNS / NTP	DNSサーバとNTPサーバのアドレス指定方法およびIPアドレスが表示されます（これらのサーバがSystem Managerで設定されている場合）。 ドメイン ネーム システム（DNS）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用の命名システムです。DNSサーバが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。 ネットワーク タイム プロトコル（NTP）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に使用されるネットワーク プロトコルです。

5. 閉じる をクリックします。

SANtricity System Managerでリモートログイン（**SSH**）を設定

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ます。

SANtricityバージョン11.74以降では、ユーザーにSSHキーやSSHパスワードの入力を要求することで、多要素認証（MFA）を設定することもできます。SANtricityバージョン11.73以前では、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ていません。

セキュリティリスク — セキュリティ上の理由から、リモートログイン機能はテクニカルサポート担当者のみが使用してください。

手順

1. *ハードウェア*を選択します。
2. グラフィックにドライブが表示されている場合は、*Controllers & Components*タブをクリックしてください。

   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. *リモートログイン（SSH）の設定*を選択します。（SANtricityバージョン11.73以前の場合、このメニュー項目は*リモートログインの変更*です。）

   リモート ログインを有効にするためのダイアログ ボックスが開きます。
5. *リモートログインを有効にする*チェックボックスを選択します。

   リモート ログインでは、次の3つの認証方法を使用できます。

   - パスワードのみ。このオプションについては、これで完了です。*保存*をクリックしてください。デュプレックスシステムを使用している場合は、上記の手順に従って、2番目のコントローラー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のいずれか。このオプションの場合は、次の手順に進みます。
   - パスワードと**SSH**キーの両方。このオプションの場合は、*リモートログインに認証済みの公開鍵とパスワードを要求する*チェックボックスを選択し、次のステップに進んでください。
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*ファイルの形式で承認された公開鍵のリストが含まれます。

   *承認済み公開鍵*フィールドに入力する際は、以下のガイドラインに注意してください：

   - *Authorized public key*フィールドは両方のコントローラに適用されますが、最初のコントローラでのみ設定する必要があります。
   - **authorized_keys** ファイルには、1 行につき 1 つのキーのみを記述する必要があります。#で始まる行と空行は無視されます。ファイル形式の詳細については、"OpenSSH の認証キーの設定"を参照してください。
   - **authorized_keys** ファイルは、次の例のような内容になります：

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDJlG20rYTk4ok+xFjkPHYp/R0LfJqEYDLXA5AJ4
9w3DvAWLrUg+1CpNq76WSqmQBmoG9jgbcAB5ABGdswdeMQZHilJcu29iJ3OKKv6SlCulA
j1tHymwtbdhPuipd2wIDAQAB
```

7. 完了したら、*保存*をクリックします。
8. デュプレックスシステムの場合、上記の手順に従って、2番目のコントローラー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、必ず*リモートログインに認証済みの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. 技術サポートによる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ーでリモートログインが有効になっている場合、確認ダイアログが表示され、2台目のコントローラーでもリモートログインを無効にすることができます。

   リモート ログインを無効にすると、現在のSSHセッションがすべて終了し、新しいログイン要求はすべて拒否されます。

SANtricity System Manager でコントローラをオンラインにする

コントローラがオフライン状態またはサービス モードの場合は、オンラインに戻すことができます。

手順

1. *ハードウェア*を選択します。
2. グラフィックにドライブが表示されている場合は、*Controllers & Components*タブをクリックしてください。

   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、操作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、最大で10分かかることがあります。

このコントローラが元々所有していたボリュームは、各ボリュームに対するI/O要求を受信すると、自動的にコントローラに戻されます。場合によっては、*ボリュームの再配布*コマンドを使用してボリュームを手動で再配布する必要があるかもしれません。

SANtricity System Manager で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。

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と、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ます。

タスク概要

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

1. *ハードウェア*を選択します。
2. グラフィックにドライブが表示されている場合は、*Controllers & Components*タブをクリックしてください。

   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。
4. *オフラインにする*を選択し、操作を実行することを確認します。

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。

SANtricity System Managerでコントローラをサービスモードにする

指示があった場合は、コントローラをサービス モードに切り替えることができます。

開始する前に

- ストレージ アレイに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と、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ます。

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

1. *ハードウェア*を選択します。
2. グラフィックにドライブが表示されている場合は、*Controllers & Components*タブをクリックしてください。

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. 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。

4. *サービスモードにする*を選択し、操作を実行することを確認します。

SANtricity System Managerでコントローラをリセット（リブート）する

一部の問題に対処するには、コントローラのリセット（リブート）が必要です。コントローラに物理的にアクセスできない場合でも、コントローラをリセットできます。

開始する前に

- ストレージ アレイに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と、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ます。

手順

1. *ハードウェア*を選択します。
2. グラフィックにドライブが表示されている場合は、*Controllers & Components*タブをクリックしてください。

   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。

4. *リセット*を選択し、操作を実行することを確認します。

iSCSIポートの管理

SANtricity System ManagerでiSCSIポートを設定

コントローラにiSCSIホスト接続が搭載されている場合は、[ハードウェア]ページからiSCSIポートを設定できます。

開始する前に

- コントローラにiSCSIポートが搭載されている必要があります。そうでない場合、iSCSI設定は使用できません。
- ネットワーク速度（ポートとホストの間のデータ転送率）を把握しておく必要があります。

> 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

1. *ハードウェア*を選択します。
2. グラフィックにドライブが表示されている場合は、*Controllers & Components*タブをクリックしてください。

   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. 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。

4. * Configure iSCSI ports *を選択します。

   *iSCSI ポートの構成*オプションは、System Manager がコントローラ上で iSCSI ポートを検出した場合にのみ表示されます。

   [iSCSI ポートの設定]ダイアログ ボックスが開きます。

5. ドロップダウンリストから設定するポートを選択し、*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。

   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*その他のポート設定を表示*リンクをクリックしてください。

フィールドの詳細

ポート設定	概要
設定されているイーサネット ポート速度（特定のタイプのホスト インターフェイス カードの場合のみ表示）	ポートのSFPの速度と同じ速度を選択します。
前方誤り訂正（FEC）モード（特定のタイプのホスト インターフェイス カードの場合のみ表示）	必要に応じて、指定したホスト ポートに対していずれかのFECモードを選択します。 Reed Solomonモードでは、25Gbpsのポート速度がサポートされません。
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。 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。
TCPリスニングポート（*その他のポート設定を表示*をクリックすると表示されます。）	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。
MTUサイズ（*その他のポート設定を表示*をクリックすると表示されます。）	必要に応じて、最大伝送ユニット（MTU）の新しいサイズ（バイト）を入力します。 デフォルトのMTU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。
ICMP PING応答を有効にする	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。

*Enable IPv4*を選択した場合、*Next*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。*Enable IPv6*を選択した場合、*Next*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、最初にIPv4設定のダイアログボックスが開き、次に*Next*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および/またはIPv6の設定を、自動または手動で構成します。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*その他の設定を表示*リンクをクリックしてください。

フィールドの詳細

ポート設定	概要
設定を自動的に取得	設定を自動的に取得する場合は、このオプションを選択します。
静的な設定を手動で指定	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、カット アンド ペーストでアドレスをフィールドに貼り付けることもできます）。IPv4の場合は、ネットワークのサブネットマスクとゲートウェイも指定します。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。
VLANサポートを有効にする（*詳細設定を表示*をクリックすると利用可能になります）。	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。
イーサネットの優先順位を有効にする（*その他の設定を表示*をクリックすると表示されます）。	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アクセスを停止して再試行まで待機します。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スイッチ イーサネットでは、このプロセスが最小化されます。

8. *完了*をクリックします。

SANtricity System Managerで**iSCSI**認証を設定する

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、Challenge Handshake Authentication Protocol（CHAP）方式を使用し、初期リンク時にターゲットとイニシエータの身元を検証します。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います。

開始する前に

イニシエータ（iSCSIホスト）のCHAPシークレットは、ターゲット（コントローラ）のCHAPシークレットを設定する前でもあとでも設定できます。このタスクの手順を実行する前に、ホストがiSCSI接続を確立するのを待ってから、個々のホストでCHAPシークレットを設定する必要があります。接続が確立されると、iSCSI認証のダイアログ ボックス（このタスクで説明）にホストのIQN名とCHAPシークレットが表示され、手動で入力する必要はありません。

タスク概要

次のいずれかの認証方式を選択できます。

- 一方向認証 — この設定を使用すると、コントローラが iSCSI ホストの ID を認証できるようになります（一方向認証）。
- 双方向認証（：）この設定を使用すると、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なります（双方向認証）。この設定により、コントローラが iSCSI ホストの ID を認証し、さらに iSCSI ホストがコントローラの ID を認証することで、2 段階目のセキュリティレベルが提供されます。

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のみ、[設定]ページに表示されます。

手順

1. メニュー：Settings[System]を選択します。
2. iSCSI設定で、*認証の設定*をクリックします。

   [認証の設定]ダイアログ ボックスが開き、現在設定されている方式が表示されます。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。

3. 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場合は、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、設定は完了です。
   - 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、［次へ］をクリックして［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ホストの両方で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、*次へ*をクリックして*ターゲットCHAPの構成*ダイアログボックスを表示します。
4. 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。

   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、既存のシークレットを置き換えることができます（新しいシークレットは表示されます）。

5. 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。
   - _双方向_認証を設定する場合は、*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。
6. 双方向認証の場合、iSCSIホスト（イニシエータ）のいずれかのCHAPシークレットを入力または確認してください。CHAPシークレットは、12～57文字の印刷可能なASCII文字で指定できます。特定のホストに対して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てください。

   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、既存のシークレットを置き換えることができます（新しいシークレットは表示されます）。

7. *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。

SANtricity System ManagerでiSCSI検出設定を有効にする

iSCSIネットワーク内のストレージ デバイスの検出に関連する設定を有効にすることができます。

[ターゲット検出設定]では、Internet Storage Name Service（iSNS）プロトコルを使用してストレージ アレイのiSCSI情報を登録し、名前のない検出セッションを許可するかどうかを決定できます。

開始する前に

iSNSサーバで静的IPアドレスが使用されている場合は、そのアドレスをiSNSの登録に使用できる必要があります。IPv4とIPv6の両方がサポートされています。

タスク概要

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**サーバー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iSCSI修飾名（IQN）とポート情報をiSNSサーバーに登録します。この設定によりiSNSの検出が可能になり、イニシエータはiSNSサーバーからIQNとポート情報を取得できるようになります。
- 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が有効になっている場合、イニシエータ（iSCSI ホスト）は、検出タイプの接続のログイン シーケンス中にターゲット（コントローラ）の IQN を提供する必要がありません。無効化されている場合、ホストはコントローラとの検出セッションを確立するために IQN を提供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 が必要となります。この設定を無効にすると、不正な 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のを防ぐことができます。

> 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のみ、[設定]ページに表示されます。

手順

1. メニュー：Settings[System]を選択します。
2. *iSCSI設定*で、*ターゲット検出設定の表示/編集*をクリックします。

   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。*iSNSサーバーを有効にする*フィールドの下に、コントローラーが既に登録されているかどうかがダイアログボックスに表示されます。

3. 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** サーバーから構成を自動的に取得する — Dynamic Host Configuration Protocol（DHCP）サーバーを使用して iSNS サーバーを構成する場合は、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、コントローラ上のすべての iSCSI ポートも DHCP を使用するように構成する必要があることに注意してください。必要に応じて、コントローラの iSCSI ポート設定を更新して、このオプションを有効にしてください。

DHCP サーバーが iSNS サーバーのアドレスを提供するには、DHCP サーバーをオプション 43 — “Vendor Specific Information” を使用するように構成する必要があります。このオプションには、データ バイト 0xa-0xd （10-13） に iSNS サーバーの IPv4 アドレスが含まれている必要があります。

- 静的設定を手動で指定する — iSNSサーバーに静的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、アドレスをフィールドにカット＆ペーストできます。）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、IPv4がデフォルトになります。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の値を入力します）。

4. ストレージ アレイが名前のない検出セッションに参加できるようにするには、*名前のない検出セッションを有効にする*を選択します。
   - 有効にすると、iSCSIイニシエータは、コントローラの情報を取得するためにターゲットIQNを指定する必要はありません。
   - 無効にすると、イニシエータがターゲットIQNを指定しないかぎり、検出セッションは実行されません。名前のない検出セッションを無効にすると、セキュリティが強化されます。
5. *保存*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と、進行状況バーが表示されます。この処理には最大5分かかる場合があります。

SANtricity System Managerで**iSCSI**統計パッケージを表示する

ストレージ アレイへのiSCSI接続に関するデータを表示できます。

タスク概要

System Managerには、次のタイプのiSCSI統計が表示されます。すべての統計は読み取り専用であり、設定することはできません。

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 コントロール（MAC）の統計情報を提供します。MACは、物理アドレスまたはMACアドレスと呼ばれるアドレス指定メカニズムも提供します。MACアドレスは、各ネットワーク アダプタに割り当てられる一意のアドレスです。MACアドレスは、サブネットワーク内の宛先へのデータ パケットの配信に役立ちます。
- イーサネット**TCP/IP**統計--iSCSIデバイスの伝送制御プロトコル（TCP）およびインターネットプロトコル（IP）であるTCP/IPの統計情報を提供します。TCPを使用すると、ネットワーク上のホスト上のアプリケーションは互いに接続を確立し、その接続を介してパケット単位でデータを交換できます。IPは、パケット交換方式のネットワーク間でデータを通信するためのデータ指向プロトコルです。IPv4の統計情報とIPv6の統計情報は別々に表示されます。
- 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情報を提供します。カーネル統計は、TCP/IP統計オプションと同様のネットワークデータを表示します。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 — iSCSIターゲットの統計を表示します。iSCSIタ

ーゲットは、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します。また、非同期ミラーリング操作においてイニシエータとして使用された場合のストレージアレイのiSCSI統計情報も表示します。

- **DCBX** 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**統計 — Link Layer Discovery Protocol（LLDP）Type Length Value（TLV）統計を表示します。
- **DCBX TLV**統計 — データセンターブリッジング（DCB）環境におけるストレージアレイホストポートを識別する情報を表示します。この情報は、識別および機能確認の目的でネットワークピアと共有されます。

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

手順

1. メニューの「Support」→「Support Center」→「Diagnostics」タブを選択します。
2. * View iSCSI Statistics Packages * を選択します。
3. タブをクリックして、さまざまな統計を表示します。
4. 基準値を設定するには、*Set new baseline*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。

SANtricity System Managerで**iSCSI**セッションを表示する

ストレージ アレイへのiSCSI接続に関する詳細情報を表示できます。iSCSIセッションは、非同期ミラー関係にあるホストまたはリモート ストレージ アレイとの間で発生します。

手順

1. メニュー：Settings[System]を選択します。
2. *View/End iSCSI Sessions*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。

3. オプション： 特定のiSCSIセッションに関する詳細情報を表示するには、セッションを選択し、*詳細を表示*をクリックします。

フィールドの詳細

項目	概要
セッション識別子（SSID）	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。
イニシエータ セッション ID（ISID）	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。
ターゲット ポータル グループ	iSCSIターゲット。
ターゲット ポータル グループ タグ（TPGT）	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。
イニシエータの iSCSI 名	世界規模で一意なイニシエータの名前。
イニシエータの iSCSI ラベル	System Managerで設定されたユーザ ラベル。
イニシエータの iSCSI エイリアス	iSCSIノードにも関連付けることのできる名前。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、ホストでのみ設定可能です。
ホスト	ストレージ アレイに入出力を送信するサーバ。
接続 ID（CID）	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の際にも提供されます。
ポート識別子	接続に関連付けられているコントローラ ポート。
イニシエータ IP アドレス	イニシエータのIPアドレス。
ネゴシエーション済みのログイン パラメータ	iSCSIセッションのログイン時に処理されるパラメータ。
認証方式	iSCSIネットワークへのアクセスを希望するユーザーを認証するための技術。有効な値は **CHAP** と **None** です。

項目	概要
ヘッダー ダイジェスト方式	iSCSIセッションで使用可能なヘッダー値を示す手法。HeaderDigestとDataDigestは、*None*または*CRC32C*のいずれかになります。両方のデフォルト値は*None*です。
データ ダイジェスト方式	iSCSIセッションで使用可能なデータ値を示す手法。HeaderDigestとDataDigestは、*None*または*CRC32C*のいずれかになります。両方のデフォルト値は*None*です。
最大接続数	iSCSIセッションで許可される最大接続数。最大接続数は1～4です。デフォルト値は*1*です。
ターゲット エイリアス	ターゲットに関連付けられているラベル。
イニシエータ エイリアス	イニシエータに関連付けられているラベル。
ターゲット IP アドレス	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。
初期 R2T	初期転送準備完了状態。ステータスは*Yes*または*No*のいずれかです。
最大バースト長	このiSCSIセッションの最大SCSIペイロード（バイト単位）。最大バースト長は512～262,144（256KB）です。デフォルト値は*262,144（256KB）*です。
第 1 バースト長	このiSCSIセッションにおける、未承諾データのSCSIペイロード（バイト単位）。最初のバースト長は512から131,072（128KB）までです。デフォルト値は*65,536（64KB）*です。
デフォルトの待機時間	接続が切断された後、または接続がリセットされた後に、再度接続を試みるまでに待機する最小秒数。デフォルトの待機時間値は0から3600までの範囲で設定できます。デフォルトは*2*です。
デフォルトの保持時間	接続の終了または接続のリセット後も接続が可能な最大秒数。デフォルトの保持時間は0～3600です。デフォルト値は*20*です。
最大未処理 R2T	このiSCSIセッションで未処理の「転送準備完了」状態の最大数。未処理の転送準備完了の最大値は1～16です。デフォルト値は*1*です。
エラー リカバリ レベル	このiSCSIセッションにおけるエラー回復レベル。エラー回復レベルの値は常に*0*に設定されます。
受信データ最大セグメント長	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。

項目	概要
ターゲット名	ターゲットの正式名称（エイリアスではない）。_iqn_形式のターゲット名。
イニシエータ名	イニシエータの正式名称（エイリアスではない）。*iqn* または *eui* 形式を使用するイニシエータ名。

4. *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。

   ファイルは、ブラウザのダウンロードフォルダにファイル名 `iscsi-session-connections.txt`で保存されます。

SANtricity System Managerで**iSCSI**セッションを終了する

不要になったiSCSIセッションを終了できます。iSCSIセッションは、非同期ミラー関係にあるホストまたはリモート ストレージ アレイとの間で発生します。

タスク概要

iSCSIセッションを終了する理由として以下が考えられます。

- 不正アクセス — iSCSI イニシエータがログオンしていて、アクセス権限がない場合は、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。iSCSI イニシエータは、None 認証方式が使用可能だったためログオンできた可能性があります。
- システムのダウンタイム — 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ことが確認された場合は、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

1. メニュー：Settings[System]を選択します。
2. *View/End iSCSI Sessions*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。

3. 終了するセッションを選択します。
4. *セッション終了*をクリックし、操作を実行することを確認してください。

SANtricity System Manager で **InfiniBand** ポート経由の **iSER** を設定します

コントローラにiSER over InfiniBandポートが搭載されている場合は、ホストとのネットワーク接続を設定できます。

開始する前に

- コントローラにiSER over InfiniBandポートが搭載されている必要があります。そうでないと、System ManagerでiSER over InfiniBand設定を使用できません。
- ホスト接続のIPアドレスを確認しておく必要があります。

手順

1. *ハードウェア*を選択します。
2. グラフィックにドライブが表示されている場合は、*Controllers & Components*タブをクリックしてください。

   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. 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。

4. *InfiniBandポート経由のiSERの設定*を選択します。

   [iSER over InfiniBand ポートの設定]ダイアログ ボックスが表示されます。

5. 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。
6. *Configure*をクリックします。
7. 設定を完了したら、*はい*をクリックしてInfiniBandポート経由のiSERをリセットします。

SANtricity System Manager で **iSER over InfiniBand** の統計を表示します

ストレージ アレイのコントローラにiSER over InfiniBandポートが搭載されている場合は、ホスト接続に関するデータを表示できます。

タスク概要

System Managerには、次のタイプのiSER over InfiniBand統計が表示されます。すべての統計は読み取り専用であり、設定することはできません。

- ローカルターゲット（プロトコル）統計 — InfiniBand上のiSERターゲットに関する統計情報を提供します。これは、ストレージ メディアへのブロックレベルのアクセスを示します。
- **iSER**オーバー**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ポートの統計情報を提供します。これには、各スイッチ ポートに関連付けられた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

1. メニュー：Settings[System]を選択します。
2. *View iSER over InfiniBand Statistics*を選択します。
3. タブをクリックして、さまざまな統計を表示します。
4. オプション： 基準値を設定するには、*Set new baseline*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。

NVMeポートの管理

NVMeとSANtricityソフトウェアについて学ぶ

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実現します。

NVMeとは何ですか？

*NVM_*は「不揮発性メモリ」の略で、多くの種類のストレージデバイスで使用される永続メモリです。*_NVMe*（NVM Express）は、NVMデバイスとのハイパフォーマンスマルチキュー通信専用に設計された標準化されたインターフェー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とデータをホストコンピュータとストレージ間でネットワーク経由で転送できるようにする技術仕様です。NVMeストレージアレイ（_サブシステム_と呼ばれる）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において、トランスポート抽象化レイヤー内で有効化され、カプセル化されています。これにより、ハイパフォーマンスNVMeインターフェースがホストからストレージまでエンドツーエンドで拡張され、コマンドセットが標準化および簡素化されます。

NVMe-oFストレージは、ホストに対してローカルブロックストレージデバイスとして認識されます。ボリューム（_namespace_と呼ばれる）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。REST API、SMcli、またはSANtricity System Managerを使用して、必要に応じ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

ネームスペースはSCSIの論理ユニットに相当し、アレイ内のボリュームに関連付けられています。ネームスペースID（NSID）は、SCSIの論理ユニット番号（LUN）に相当します。NSIDはネームスペースの作成時に作成し、1~255の値を設定できます。

NVMeコントローラとは

SCSI I_T nexus（ホストのイニシエータからストレージ システムのターゲットへのパス）と同様に、NVMeコントローラはホストの接続プロセス中に作成され、ホストとストレージ アレイ内のネームスペースの間のアクセス パスを提供します。NVMeコントローラはホストのNQNとホスト ポート識別子によって一意に識別されます。NVMeコントローラを関連付け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。

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、SANtricity System Managerを使用してホストのネームスペースIDを設定します。次に、NVMeコントローラが作成されると、NVMeコントローラがアクセスできるネームスペース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。

SANtricity System Manager で NVMe over InfiniBand ポートを設定します

コントローラにNVMe over InfiniBand接続が搭載されている場合は、[ハードウェア]ページからNVMeポートを設定できます。

開始する前に

- コントローラにNVMe over InfiniBandホスト ポートが搭載されている必要があります。そうでないと、System ManagerでNVMe over InfiniBand設定を使用できません。
- ホスト接続のIPアドレスを確認しておく必要があります。

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

1. *ハードウェア*を選択します。
2. グラフィックにドライブが表示されている場合は、*Controllers & Components*タブをクリックしてください。

   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. 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。

4. *NVMe over InfiniBandポートの設定*を選択します。

   [NVMe over InfiniBand ポートの設定]ダイアログ ボックスが開きます。

5. 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。これらの設定によって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。

6. *Configure*をクリックします。
7. 設定を完了したら、*はい*をクリックしてNVMe over InfiniBandポートをリセットします。

SANtricity System Manager で NVMe over RoCE ポートを設定する

コントローラにNVMe over RoCE（RDMA over Converged Ethernet）の接続が搭載されている場合は、[ハードウェア]ページからNVMeポートを設定できます。

開始する前に

- コントローラにNVMe over RoCEホスト ポートが搭載されている必要があります。そうでないと、System ManagerでNVMe over RoCE設定を使用できません。
- ホスト接続のIPアドレスを確認しておく必要があります。

手順

1. *ハードウェア*を選択します。
2. グラフィックにドライブが表示されている場合は、*Controllers & Components*タブをクリックしてください。

   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. 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。

4. *NVMe over RoCE ポートの構成*を選択します。

   [NVMe over RoCE ポートの設定]ダイアログ ボックスが開きます。

5. 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。
6. **Next** 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*その他のポート設定を表示*リンクをクリックしてください。

   フィールドの詳細

ポート設定	概要
設定されたイーサネット ポート速度	ポートのSFPの速度と同じ速度を選択します。
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。 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。
MTUサイズ（*その他のポート設定を表示*をクリックすると表示されます。）	必要に応じて、最大伝送ユニット（MTU）の新しいサイズ（バイト）を入力します。 デフォルトのMTU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。

   *Enable IPv4*を選択した場合、*Next*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。*Enable IPv6*を選択した場合、*Next*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、最初にIPv4設定のダイアログボックスが開き、次に*Next*をクリックすると、IPv6設定のダイアログボックスが開きます。

7. IPv4、IPv6、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

ポート設定	概要
設定を自動的に取得	設定を自動的に取得する場合は、このオプションを選択します。
静的な設定を手動で指定	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、カット アンド ペーストでアドレスをフィールドに貼り付けることもできます）。IPv4の場合は、ネットワークのサブネットマスクとゲートウェイも指定します。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。これらの設定によって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。

8. *完了*をクリックします。

SANtricity System Managerで**NVMe over Fabrics**の統計を表示する

ストレージ アレイへのNVMe over Fabrics接続に関するデータを表示できます。

タスク概要

System Managerには、次のタイプのNVMe over Fabrics統計が表示されます。すべての統計は読み取り専用であり、設定することはできません。

- **NVMe**サブシステム統計 — NVMeコントローラとそのキューの統計情報を表示します。NVMeコントローラは、ホストとストレージアレイ内の名前空間との間のアクセスパスを提供します。NVMeサブシステムの統計情報を確認することで、接続障害、リセット、シャットダウンなどの項目を把握できます。
- **RDMA**インターフェイス統計：RDMAインターフェイス上のすべてのNVMe over Fabricsポートの統計情報を提供します。これには、各スイッチ ポートに関連付けられたパフォーマンス統計情報とリンクエラー情報が含まれます。このタブは、NVMe over Fabricsポートが利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

1. メニュー：Settings[System]を選択します。
2. *View NVMe over Fabrics Statistics*を選択します。
3. オプション： 基準値を設定するには、*Set new baseline*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。

ドライブの管理

SANtricity System Managerのドライブの状態について説明します

SANtricity System Managerは、ドライブのさまざまな状態を報告します。

アクセスの状態

都道府県	定義
バイパス	ドライブは物理的に存在しているが、コントローラはどちらのポートでもドライブと通信できない。
互換性なし	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互換性のないファームウェア バージョンのものであり、使用できません。
取り外し	ドライブがストレージ アレイから取り外されています。
現在	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。
応答なし	ドライブがコマンドに応答していません。

ロールの状態

都道府県	定義
割り当て	プールまたはボリューム グループのメンバーです。
使用中のホット スペア	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。
スタンバイのホット スペア	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。
未割り当て	このドライブは、プールまたはボリュームグループのメンバーではありません。

可用性の状態

都道府県	定義
失敗	ドライブは動作していません。ドライブ上のデータは使用できません。

都道府県	定義
障害の兆候	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。
オフライン	ドライブをデータの格納に使用できません。通常は、所属先のボリューム グループをエクスポート中であるか、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。
最適	ドライブは正常に動作しています。

SANtricity System ManagerのSolid State Disk（SSD）について学ぶ

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（フラッシュメモリ）を使用してデータを永続的に保存するデータストレージデバイスです。SSDは従来のハードディスクをエミュレートするものであり、ハードディスクと同じインターフェースを備えています。

SSDのメリット

ハード ドライブと比べたSSDのメリットは次のとおりです。

- 高速起動（スピン アップなし）
- 低レイテンシ
- 高IOPS（1秒あたりの入出力処理数）
- 少ない可動部品で信頼性を向上
- 消費電力を削減
- 熱の発生を抑え、冷却コストを削減

SSDの識別

[ハードウェア]ページのシェルフ前面ビューでSSDを特定できます。稲妻アイコン（SSDが設置されていることを示します）が表示されているドライブ ベイを探してください。

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は、同じメディアタイプである必要があります（すべてSSD、またはすべてハードドライブ）。ボリュームグループには、異なるメディアタイプまたはインターフェー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できます。SSDキャッシュでは、データがボリュームからコピーされ、2個の内部RAIDボリューム（コントローラごとに1個）に格納されます。

物理属性および論理属性のタイプが異なる複数のドライブがストレージ アレイに含まれている場合、[ハードウェア]ページのフィルタ フィールドを使用して、ドライブの表示を絞り込んでドライブを特定することができます。

タスク概要

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、別々に使用することもできます。

すべてのドライブが同じ物理的属性を共有している場合、*次の条件を満たすドライブを表示…*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、*ストレージアレイ内の任意の場所*フィルタフィールドは表示されません。

手順

1. *ハードウェア*を選択します。
2. 最初のフィルターフィールド（*表示するドライブ…*の下）で、ドロップダウン矢印をクリックすると、利用可能なドライブの種類とセキュリティ属性が表示されます。

   ドライブ タイプには次のものがあります。

   - ドライブのメディア タイプ（SSD、HDD）
   - ドライブ インターフェイス タイプ
   - ドライブの容量（最大から最小）
   - ドライブ速度（最高から最低まで）セキュリティ属性には以下が含まれる場合があります：
   - セキュリティ対応
   - セキュリティ有効
   - DA（Data Assurance）対応
   - FIPS準拠
   - FIPS準拠（FIPS 140-2）
   - FIPS準拠（FIPS 140-3）

     これらの属性のいずれかがすべてのドライブで同じ場合は、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。

   フィールドからオプションを選択すると、フィルタ条件に一致しないドライブは、グラフィカル ビューでグレー表示されます。

3. 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、ドライブの選択可能な論理的場所を表示します。

フィルター条件をクリアする必要がある場合は、フィルターボックスの一番右にある*Clear*を選択してください。

論理的な場所には次のものがあります。

- プール
- ボリューム グループ
- ホット スペア
- SSD キャッシュ
- 未割り当て

フィールドからオプションを選択すると、フィルタ条件に一致しないドライブは、グラフィカル ビューでグレー表示されます。

4. オプションとして、フィルターフィールドの右端にある*ロケーターライトを点灯*を選択すると、表示されている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。

SANtricity System Managerでドライブロケーターライトを点灯する

[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特定できます。

タスク概要

[ハードウェア]ページに表示される1本または複数のドライブを特定できます。

手順

1. *ハードウェア*を選択します。
2. 1本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、アレイ内で物理的に配置するドライブを見つけます。（グラフィックにコントローラーが表示されている場合は、*ドライブ*タブをクリックしてください。）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。

     ドライブの位置情報ランプが点灯します。ドライブを物理的に特定したら、ダイアログに戻り、*Turn off*を選択してください。

   - 複数のドライブ — フィルターフィールドで、左側のドロップダウンリストから物理ドライブの種類を選択し、右側のドロップダウンリストから論理ドライブの種類を選択します。条件に一致するドライブの数は、各フィールドの右端に表示されます。次に、*Turn on locator lights*をクリックするか、コンテキストメニューから*Locate all filtered drives*を選択します。ドライブを物理的に特定したら、ダイアログに戻り、*Turn off*を選択してください。

SANtricity System Managerでドライブのステータスと設定を表示する

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および設定を表示できます。

手順

1. *ハードウェア*を選択します。
2. グラフィック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。

   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。

3. 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。

4. 設定の表示 を選択します。

   [ドライブ設定]ダイアログ ボックスが開きます。

5. 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 **Show more settings** をクリックしてください。

フィールドの詳細

設定	概要
ステータス	最適、オフライン、非重大障害、失敗のいずれかが表示されます。最適ステータスは良好な稼働状態を示します。
モード	割り当て、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。
Location	ドライブが装着されているシェルフおよびベイの番号が表示されます。
割り当て先/保護対象/保護	ドライブがプール、ボリューム グループ、またはSSDキャッシュに割り当てられている場合は「割り当て先」と表示されます。値は、プール名、ボリューム グループ名、SSDキャッシュ名のいずれかです。ドライブが「スタンバイ」モードのホット スペアに割り当てられている場合は「保護対象」と表示されます。そのホット スペアが1つ以上のボリューム グループを保護できる場合は、ボリューム グループ名が表示されます。ボリューム グループを保護できない場合、「0」と表示されます。 ドライブが「使用中」モードのホット スペアに割り当てられている場合は「保護」と表示されます。値は、影響を受けるボリューム グループの名前です。 ドライブが未割り当ての場合、このフィールドは表示されません。
メディア タイプ	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）のどちらかです。
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）	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。
インターフェイス タイプ	ドライブが使用するインターフェイスのタイプ（SASなど）が表示されます。
ドライブ パスの冗長性	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。
容量 (GiB)	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。
速度（rpm）	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）。
現在のデータ速度	ドライブとストレージ アレイ間のデータ転送速度が表示されます。

設定	概要
論理セクター サイズ（バイト）	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。
物理セクター サイズ（バイト）	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。
ドライブ ファームウェア バージョン	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。
World Wide Identifier	ドライブの一意の16進数の識別子が表示されます。
製品 ID	メーカーが割り当てた製品の識別子が表示されます。
シリアル番号	ドライブのシリアル番号が表示されます。
メーカー	ドライブのベンダーが表示されます。
製造日	ドライブが組み込まれた日付が表示されます。 NVMeドライブでは使用できません。
セキュリティ対応	ドライブがセキュリティに対応しているか（はい）、対応していないか（いいえ）を示します。セキュリティ機能を備えたドライブには、Full Disk Encryption（FDE）ドライブまたはFederal Information Processing Standard（FIPS）ドライブ（レベル140-2または140-3）があり、これらは書き込み時にデータを暗号化し、読み取り時にデータを復号化します。これらのドライブは、Drive Security機能を使用して追加のセキュリティ対策を講じることができるため、セキュリティ対応ドライブとみなされます。これらのドライブで使用されるボリュームグループおよびプールに対してDrive Security機能が有効になっている場合、ドライブはセキュアな状態になります。
セキュリティ有効	ドライブがセキュリティ保護されているかどうか（はい：有効、いいえ：無効）を表示します。セキュリティ機能が有効になっているドライブは、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てから、セキュア対応ドライブ上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、ドライブはセキュア有効になります。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を介してのみ可能です。この追加のセキュリティ対策により、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します。
読み取り / 書き込みアクセス	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。

設定	概要
ドライブ セキュリティ キー識別子	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際にセキュリティ キーが要求されるようになります。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、取り付けたあとも正しいセキュリティ キーが提供されないかぎりセキュリティ ロック状態になります。
Data Assurance（DA）対応	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。
DULBE 対応	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 ボリュームがサポートされます。

6. 閉じる をクリックします。

SANtricity System Managerでドライブを論理的に交換する

ドライブに障害が発生した場合、またはその他の理由で交換する場合は、障害ドライブを未割り当てドライブまたは完全に統合されたホットスペアと論理的に交換できます。

タスク概要

論理的に交換したドライブは割り当て済みとなり、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となります。

論理的交換オプションは、次のタイプのドライブを交換する際に使用します。

- 障害ドライブ
- 不明なドライブ
- 寿命に近付いていることがRecovery Guruによって通知されたSSDドライブ
- ドライブ障害が発生する可能性があることが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）

開始する前に

交換用のドライブには次の特性が必要です。

- 最適状態

- 未割り当て状態
- 交換対象のドライブと属性（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

1. *ハードウェア*を選択します。
2. グラフィック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。

   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。

3. 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。

4. *論理置換*をクリックします。
5. オプション： 交換後に元のドライブを障害ドライブにするには、*交換後にドライブを障害ドライブにする*チェックボックスを選択します。

   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。

6. *交換用ドライブの選択*表から、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。可能な場合は、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ます。

7. * Replace * 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（見つからない）場合は、パリティ情報を使用して交換用ドライブにデータが再構築されます。この再構築は自動的に開始されます。ドライブの障害を示すインジケータ 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動作を示すインジケータ 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なります。

SANtricity System Managerでドライブを手動で再構築する

ドライブの再構築は通常、ドライブの交換後に自動的に開始されます。ドライブの再構築が自動的に開始されない場合は、再構築を手動で開始できます。

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

1. *ハードウェア*を選択します。

2. グラフィック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。

   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。

3. 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。

4. * Reconstruct * を選択し、操作を実行することを確認します。

SANtricity System Manager でドライブを初期化（フォーマット）します

ストレージ アレイから別のストレージ アレイへ、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。

タスク概要

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、ドライブは、新しいストレージ アレイの新しいプールまたはボリューム グループに追加可能になります。

単一のドライブを移動する場合は、ドライブの初期化処理を使用します。あるストレージ アレイから別のストレージ アレイへ、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。

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。この操作は、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. *ハードウェア*を選択します。
2. グラフィック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。

   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。

3. 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。

4. * Initialize * を選択し、操作を実行することを確認します。

SANtricity System Managerでドライブを手動で障害状態にする

指示があった場合は、ドライブを手動で使用停止できます。

タスク概要

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。

データアクセスが失われる可能性 — この操作により、データ損失またはデータ冗長性の喪失が発生する可能性があります。この操作は、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

1. *ハードウェア*を選択します。
2. グラフィック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。

   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。

3. 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。

4. **Fail** を選択します。
5. *障害発生前にドライブの内容をコピーする*チェックボックスは選択したままにしてください。

   コピー オプションは、割り当て済みのドライブおよび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。設定によっては、ドライブの内容を最初にコピーしておかないと、関連付けられた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。

6. 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。

SANtricity System Managerでドライブを消去

[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。この手順では、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。

開始する前に

ドライブが未割り当てである必要があります。

タスク概要

[消去]オプションは、ドライブ上のすべてのデータを完全に削除する場合にのみ使用します。セキュリティ有効ドライブに対して[消去]オプションを使用すると、暗号化データが消去され、セキュリティ属性がセキュリティ対応にリセットされます。

消去機能は、一部の古いドライブ モデルには対応していません。該当するモデル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

1. *ハードウェア*を選択します。
2. グラフィック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。

   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。

3. 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、その他はすべてグレー表示になります。

4. ドライブのコンテキスト メニューを開くには、消去するドライブをクリックします（複数のドライブを選択する場合は、[ドライブを消去]ダイアログ ボックスで選択できます）。

   > データ損失の可能性あり — 消去操作は元に戻せません。手順を実行する際は、必ず正しいドライブを選択してください。

5. コンテキストメニューから*消去*を選択します。

   [ドライブを消去]ダイアログ ボックスが開き、消去処理を実行可能なすべてのドライブが表示されます。

6. 必要に応じて、表から追加のドライブを選択してください。_すべて_のドライブを選択することはできません。必ず1つのドライブが選択解除された状態になっていることを確認してください。
7. `erase`と入力して操作を確認し、*消去*をクリックします。

   > この処理が本当に必要かどうかを続行前に確認してください。次のダイアログで[はい]をクリックすると、処理を中止することはできません。

8. 「完了予定時間」ダイアログボックスで、*はい*をクリックして消去操作を続行します。

結果

消去操作には数分から数時間かかる場合があります。ステータスは**Home › View Operations in Progress**で確認できます。消去操作が完了すると、ドライブは別のボリュームグループまたはディスクプール、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。

終了後の操作

ドライブを再度使用するには、まず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*を選択してください。

SANtricity System Manager でロックされた **NVMe** 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

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たセキュリティ キー ファイルを追加することでドライブ データのロックを解除できます。セキュリティ キーがない場合は、ドライブの物理セキュリティID（PSID）を入力してロックされた各ドライブでリセットを実行し、セキュリティ属性をリセットしてドライブ データを消去できます。

開始する前に

- ロック解除オプションの場合、セキュリティキーファイル（拡張子 `.slk`付き）が管理クライアント（System Managerにアクセスするために使用するブラウザを備えたシステム）で利用可能であることを確認してください。キーに関連付けられたパスフレーズも知っておく必要があります。
- リセットする場合は、リセットする各ドライブのPSIDを確認する必要があります。PSIDを確認するには、ドライブを物理的に取り外し、ドライブのラベルに記載されたPSID（最大32文字）を確認してから、ドライブを取り付け直します。

タスク概要

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。

ドライブが外部キー管理サーバーを使用してロックされている場合は、System Managerでメニュー：Settings［System ＞ 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てください。

ロック解除機能は、ハードウェアページまたはメニューの「Settings」[System > Security key management]からアクセスできます。以下のタスクは、ハードウェアページの手順を示しています。

手順

1. *ハードウェア*を選択します。
2. グラフィック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。

   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。

3. 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。

4. セキュリティキーファイルを適用するには*ロック解除*を選択し、セキュリティキーファイルがない場合は*リセット*を選択してください。

   これらのオプションは、ロックされたNVMeドライブまたはFIPSドライブを選択した場合にのみ表示されます。

   リセット操作中は、すべてのデータが消去されます。セキュリティキーをお持ちでない場合にのみ、リセットを実行してください。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、有効化はされません。この操作は元に戻せません。

5. 次のいずれかを実行します。

   a. 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。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。

   b. リセット：*ロックされたドライブのリセット*ダイアログボックスで、フィールドにPSID文字列を入力し、次に `RESET`と入力して確認します。*リセット*をクリックします。

      ロック解除の場合、1回の処理ですべてのNVMeドライブまたはFIPSドライブのロックを解除できます。リセットの場合、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、このドライブは、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 アレイで使用可能になります。

ホット スペアの管理

SANtricity System Managerのホットスペアドライブについて学ぶ

ホットスペアは、SANtricity System ManagerのRAID 1、RAID 5、またはRAID 6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同じである必要があります。

- 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またはSSD）
- 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 ウィザードで、または[ハードウェア]ページから割り当てることができます。ホット スペアが割り当てられているかどうかを確認するには、[ハードウェア]ページに移動して、ピンクで表示されているドライブ ベイを探します。

ホット スペアの適用方法

ホット スペアは次のように適用されます。

- RAID 1、RAID 5、またはRAID 6のボリューム グループのホット スペアとして、未割り当てのドライブを予約します。

> ホットスペアは、データ保護方法が異なるプールには使用できません。プールは、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内に予備容量（_保存容量_と呼ばれる）を確保します。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予備容量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。
- 障害のあるドライブを物理的に交換すると、ホット スペア ドライブから代替ドライブへと、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でトレイ損失の保護とドロワー損失の保護を使用できるかどうかは、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 ボリュームは引き続きオンラインでアクセス可能です。

ホット スペア ドライブの容量に関する考慮事項

保護対象の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。

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 スペアとして使用してもかまいません。

メディアとインターフェイス 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、保護対象のドライブにセキュリティ機能があるかどうかにかかわらず、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。

セキュリティ保護が有効になっているドライブをホットスペアとして使用する場合、System Managerは続行する前にSecure Eraseを実行するように促します。Secure Eraseを実行すると、ドライブのセキュリティ属性はセキュリティ対応状態にリセットされますが、セキュリティが有効になるわけではありません。

ドライブセキュリティ機能を有効にしてから、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と、ドライブは_セキュリティ有効_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を介してのみ可能です。この追加のセキュリティ対策により、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します。

推奨されるホット スペア ドライブの数

初期設定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は、特定のメディアタイプとインターフェースタイプのドライブ30台ごとに1台のホットスペアを作成します。あるいは、ストレージアレイ内のボリュームグループ間で、ホットスペアドライブを手動で作成することもできます。

SANtricity System Managerでホットスペアを割り当てる

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。

開始する前に

- RAID 1、RAID 5、またはRAID 6のボリューム グループを作成する必要があります（ホット スペアはプールには使用できません。プールでは、データ保護用に各ドライブ内のスペア容量を使用します）。
- 次の条件を満たすドライブが使用可能な必要があります。
  - 未割り当てで最適ステータス
  - ボリューム グループ内のドライブと同じメディア タイプ（SSDなど）
  - ボリューム グループ内のドライブと同じインターフェイス タイプ（SASなど）
  - ボリューム グループ内のドライブの使用容量以上の容量

タスク概要

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 セットごとにホット スペア2つです。

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]ページにピンクで表示されるドライブ ベイで確認できます。

手順

1. *ハードウェア*を選択します。
2. グラフィック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。

   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。

3. 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。

4. * ホットスペアの割り当て * を選択します。

   セキュリティ有効なドライブの場合は、[ドライブの完全消去]ダイアログ ボックスが開きます。セキュリティ有効なドライブをホット スペアとして使用するには、まず「Secure Erase（完全消去）」処理を実行してドライブのすべてのデータを削除し、セキュリティ属性をリセットする必要があります。

   データ損失の可能性あり — 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。セキュア消去操作が完了すると、データの復元は一切できません。

   ドライブがセキュリティ保護に対応して*いない*場合、「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。

5. 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。

   [ハードウェア]ページでピンクで表示されるドライブは、ホット スペアとして使用できる状態にあります。

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、自動的に冗長性データを使用して、データは障害ドライブからホット スペアへ再構築されます。

SANtricity System Managerでホットスペアの割り当てを解除

ホット スペアを未割り当てのドライブに戻すことができます。

開始する前に

ホット スペアのステータスが「最適, スタンバイ」である必要があります。

タスク概要

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

1. *ハードウェア*を選択します。
2. グラフィック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。

   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。

3. 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。

4. 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を解除*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。

5. 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（灰色で表示）。

SANtricity System ManagerのStorage shelfに関するFAQ

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

シェルフ損失の保護およびドロワー損失の保護とは何ですか?

シェルフ損失の保護とドロワー損失の保護は、シェルフまたはドロワーで単一障害が発生した場合にデータ アクセスを維持するためのプールとボリューム グループの属性です。

シェルフ損失の保護

シェルフは、ドライブまたはドライブとコントローラを格納するエンクロージャです。シェルフ損失の保護が有効な場合、1台のドライブ シェルフとの通信が完全に失われた場合でもプールまたはボリューム グループ内のボリューム上のデータへのアクセスが保証されます。通信が完全に失われるケースには、ドライブ シェルフの電源喪失や、両方のI/Oモジュール（IOM）の障害などがあります。

プールまたはボリューム グループでドライブにすでに障害が発生している場合は、シェルフ損失の保護は保証されません。この状況で、ドライブ シェルフへのアクセス、さらにその結果プールまたはボリューム グループ内の別のドライブへのアクセスを失うと、データが失われます。

シェルフ損失の保護の条件は、次の表で説明するように、保護の手法によって異なります。

レベル	シェルフ損失保護の基準	必要なシェルフの最小数
プール	プールに少なくとも5つのシェルフからそれぞれ同じ数のドライブが含まれる。シェルフ損失の保護は大容量シェルフには適用されません。大容量シェルフがあるシステムの場合は、ドロワー損失の保護を参照してください。	5
RAID 6	ボリュームグループには、1つのシェルフ内に2台以下のドライブが含まれます。	3
RAID 3またはRAID 5	ボリューム グループ内のドライブがすべて別々のシェルフに配置されている。	3
RAID 1	RAID 1ペアのドライブがそれぞれ別のシェルフに配置されている。	2
RAID 0	シェルフ損失の保護は実現できない。	該当なし

ドロワー損失の保護

ドロワーはシェルフのコンパートメントの1つで、引き出してドライブを設置します。ドロワーを備えているのは大容量のシェルフだけです。ドロワー損失の保護が有効な場合、1つのドロワーとの通信が完全に失われた場合でもプールまたはボリューム グループ内のボリューム上のデータへのアクセスが保証されます。通信が完全に失われるケースには、ドロワーの電源喪失や、ドロワー内のコンポーネント障害などがあります。

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 グループの別のドライブにアクセスできなくなり）、データが失われます。

ドロワー損失の保護の条件は、次の表で説明するように、保護の手法によって異なります。

レベル	ドロワー損失保護の基準	必要な最小ドロワ数
プール	プールにすべてのドロワーからそれぞれ同じ数のドライブが含まれる。 プールに少なくとも5つのドロワーからそれぞれ同じ数のドライブが含まれる。 60ドライブのシェルフでは、プールに含まれるドライブの数が15、20、25、30、35、40、45、50、55、または60のいずれかである場合にドロワー損失の保護を実現できます。プールの作成後は5本単位でドライブを追加できます。	5
RAID 6	ボリューム グループに同じドロワーのドライブが3本以上含まれない。	3
RAID 3またはRAID 5	ボリューム グループ内のドライブがすべて別々のドロワーに配置されている。	3
RAID 1	ミラー ペアのドライブがそれぞれ別のドロワーに配置されている。	2
RAID 0	ドロワー損失の保護は実現できない。	該当なし

バッテリ学習サイクルとは何ですか**?**

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。

学習サイクルは以下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ために必要な条件は次のとおりです。

- フル充電されたバッテリ
- 過熱していないバッテリ

デュプレックス コントローラ システムでは、学習サイクルが同時に実行されます。複数のバッテリまたは一連のバッテリ セルから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するようスケジュール設定されます。サイクルの間隔は週単位で設定されます。

学習サイクルの完了には数時間かかることがあります。

SANtricity System Managerのストレージコントローラに関するFAQ

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

自動ネゴシエーションとは何ですか?

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。

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。

IPv6ステートレス アドレス自動設定とは何ですか?

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設定する方法も定義します。IPv6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。

1. リンクローカルアドレスの生成 — デバイスは、10ビットの後に54個のゼロが続き、その後に64ビットのインターフェイスIDが続くリンクローカルアドレスを生成します。
2. リンクローカルアドレスの一意性をテストする — ノードは、生成したリンクローカルアドレスがローカルネットワーク上で既に使用されていないことを確認するためのテストを実行します。ノードはNDプロトコルを使用して、近隣ノード要請メッセージを送信します。これに対し、ローカルネットワークは近隣デバイスからのアドバタイズメントメッセージを待ち受けます。このメッセージは、別のデバイスが既にそのリンクローカルアドレスを使用していることを示します。その場合は、新しいリンクローカルアドレスを生成するか、自動構成が失敗し、別の方法を使用する必要があります。

3. リンクローカルアドレスの割り当て — デバイスが一意性テストに合格した場合、デバイスはリンクローカルアドレスをIPインターフェイスに割り当てます。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の通信には使用できません。
4. ルーターに接続 — ノードは、設定を続行するための詳細情報を取得するために、ローカルルーターに接続を試みます。この通信は、ルーターが定期的に送信するルーター広告メッセージを受信することによって、またはルーターに次に何をすべきかについての情報を要求するために、特定のルーター要請メッセージを送信することによって行われます。
5. ノードに指示を与える — ルーターは、自動構成の進め方についてノードに指示を与えます。あるいは、ルーターはホストに対してグローバルインターネットアドレスの決定方法を指示します。
6. グローバルアドレスの設定 — 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使用して自身を設定します。このアドレスは通常、ルーターによってホストに提供されたネットワークプレフィックスから形成されます。

DHCP と手動設定のどちらを選択すればよいですか？

デフォルトのネットワーク設定方式は、動的ホスト構成プロトコル（DHCP）です。ネットワークにDHCPサーバがない場合を除いて、必ずこのオプションを使用してください。

DHCPサーバとは何ですか**?**

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。このデバイスにはストレージ アレイ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の処理を開始する際にアドレス情報の要求を送信します。この要求を受け取ったDHCPサーバは、新しいアドレスを特定の時間（リース期間）だけ割り当てて、そのアドレスをクライアントに送信します。DHCPを使用する場合は、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、デバイスが接続中でもデバイスのIPアドレスが変わることがあります。

DHCPサーバ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、有効期限付きのリース期間があるため変わる可能性があります。サーバやルータなど、デバイスによっては、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の詳細については、DHCPサーバのドキュメントを参照してください。

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**?**

アウトオブバンド管理を使用するときは、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 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。

ネットワーク設定はどこで確認できますか**?**

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。

ICMP PING応答とは何ですか**?**

Internet Control Message Protocol（ICMP）は、TCP / IPスイートのプロトコルの1つです。

> `ICMP echo request`と(`ICMP echo reply`メッセージは一般的に`ping`メッセージとして知られています。
> `Ping`は、システム管理者がネットワークデバイス間の接続性を手動でテストしたり、ネットワーク遅延やパケット損失をテストしたりするために使用するトラブルシューティングツールです。
> `ping`コマンドは `ICMP echo request`をネットワーク上のデバイスに送信し、デバイスは即座に(`ICMP echo reply`で応答します。場合によっては、企業のネットワークセキュリティポリシーにより、権限のない人物による発見をより困難にするため、すべてのデバイスで `ping` (`ICMP echo reply`を無効にすることが求められます。

ポート設定はいつ更新するべきですか**?**

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 アレイと使用する予定のストレージ 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。

> ポート設定を更新すると、そのポート上のiSCSI接続はすべて停止します。

管理ポートを設定したあとに何をすればよいですか**?**

ストレージアレイのIPアドレスを変更した場合は、SANtricity Unified Managerのグローバルアレイビューを更新する必要があるかもしれません。

Unified Manager のグローバル配列ビューを更新するには、インターフェースを開き、メニューの［管理］［検出］に移動します。

まだSANtricity Storage Managerを使用している場合は、エンタープライズ管理ウィンドウ（EMW）に移動し、そこで新しいIPアドレスを削除してから再度追加する必要があります。

ストレージ システムが最適モードにならない場合、どのような理由が考えられますか**?**

ストレージシステムが最適モードではないのは、システム構成が無効状態になっているためです。この状態にもかかわらず、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ています。ただし、SANtricity System Managerは一部の操作を禁止します。

ストレージ システムが無効なシステム構成になる理由としては、次のいずれかが考えられます。

- サブモデルID（SMID）コードが正しくない、プレミアム機能の制限を超えているなど、コントローラに規定違反がある。
- ドライブ ファームウェアのダウンロードなどの内部サービス処理を実行中である。
- 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にロックダウンされた。
- 一般的なロックダウンの状況が発生した。

iSCSI プロトコルに関する FAQ（SANtricity System Manager）

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

iSNSサーバを登録に使用するとどうなりますか**?**

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）から情報を読み出すようにホスト（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。

iSCSIではどの登録方法が自動的にサポートされますか**?**

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を設定しない場合は、iSCSIホストが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。

iSER over InfiniBand統計には何が表示されますか**?**

View iSER over InfiniBand Statistics ダイアログボックスには、ローカルターゲット（プロトコル）統計とiSER over InfiniBand（IB）インターフェイス統計が表示されます。すべての統計は読み取り専用であり、設定できません。

- ローカルターゲット（プロトコル）統計 — InfiniBand上のiSERターゲットに関する統計情報を提供します。これは、ストレージ メディアへのブロックレベルのアクセスを示します。
- **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ポートの統計情報を提供します。これには、各スイッチ ポートに関連付けられた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。

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**?**

以下の表は、InfiniBand 上の iSER セッションを構成および管理するために使用できる SANtricity System Manager 機能を示しています。

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。

アクション	**Location**
iSER over InfiniBandポートの設定	1. *ハードウェア*を選択します。 2. **Controllers & Components** タブを選択します。 3. コントローラを選択します。 4. *InfiniBandポート経由のiSERの設定*を選択します。 または 1. メニュー：Settings[System]を選択します。 2. **iSER over InfiniBand settings** までスクロールし、**Configure iSER over InfiniBand Ports** を選択します。
iSER over InfiniBandの統計の表示	1. メニュー：Settings[System]を選択します。 2. **iSER over InfiniBand settings** までスクロールして、**View iSER over InfiniBand Statistics** を選択します。

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**?**

iSCSIセッションは、非同期ミラーリング関係にあるホストまたはリモートストレージアレイとの間で発生する可能性があります。以下の表に、これらのiSCSIセッションの設定と管理に使用できるSANtricity System Managerの機能を示します。

iSCSIを設定できるのは、ストレージ アレイがiSCSIをサポートしている場合のみです。

iSCSIの設定

アクション	**Location**
iSCSI設定の管理	1. メニュー：Settings[System]を選択します。 2. *iSCSI設定*までスクロールして、すべての管理機能を表示します。

アクション	Location
iSCSIポートの設定	1. *ハードウェア*を選択します。 2. **Controllers & Components** タブを選択します。 3. コントローラを選択します。 4. * Configure iSCSI ports *を選択します。
ホストのCHAPシークレットの設定	1. メニュー：Settings[System]を選択します。 2. 下にスクロールして **iSCSI**設定 を探し、次に 認証の設定 を選択してください。 または 1. メニュー：Storage[Hosts]を選択します。 2. ホスト メンバーを選択します。 3. メニューの View/Edit Settings → Host Ports タブをクリックします。

iSCSIの診断

アクション	Location
iSCSIセッションの表示または終了	1. メニュー：Settings[System]を選択します。 2. 下にスクロールして*iSCSI設定*を選択し、*iSCSIセッションの表示/終了*を選択してください。 または 1. メニューの「Support」→「Support Center」→「Diagnostics」タブを選択します。 2. *View/End iSCSI Sessions*を選択します。
iSCSI統計の表示	1. メニュー：Settings[System]を選択します。 2. 下にスクロールして **iSCSI**設定 を探し、次に **iSCSI**統計パッケージの表示 を選択します。 または 1. メニューの「Support」→「Support Center」→「Diagnostics」タブを選択します。 2. * View iSCSI Statistics Packages * を選択します。

SANtricity System ManagerのNVMeプロトコルに関するよくある質問

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

NVMe over Fabrics統計には何が表示されますか?

「NVMe over Fabrics 統計情報の表示」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情報が表示されます。すべての統計情報は読み取り専用であり、設定することはできません。

- **NVMe**サブシステム統計 — NVMeコントローラとそのキューの統計情報を表示します。NVMeコントローラは、ホストとストレージアレイ内の名前空間との間のアクセスパスを提供します。NVMeサブシステムの統計情報を確認することで、接続障害、リセット、シャットダウンなどの項目を把握できます。これらの統計に関する詳細については、*表の見出しの凡例を表示*をクリックしてください。
- **RDMA**インターフェイス統計 — RDMAインターフェイス上のすべてのNVMe over Fabricsポートの統計情報を提供します。これには、各スイッチ ポートに関連付けられたパフォーマンス統計情報とリンクエラー情報が含まれます。このタブは、NVMe over Fabricsポートが利用可能な場合にのみ表示されます。統計に関する詳細については、*表の見出しの凡例を表示*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。

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?

以下の表は、NVMe over InfiniBandセッションの構成と管理に使用できるSANtricityシステムマネージャの機能を示しています。

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。

アクション	Location
NVMe over InfiniBandポートの設定	1. *ハードウェア*を選択します。 2. **Controllers & Components** タブを選択します。 3. コントローラを選択します。 4. *NVMe over InfiniBandポートの設定*を選択します。 または 1. メニュー：Settings[System]を選択します。 2. **NVMe over InfiniBand settings** までスクロールダウンし、**Configure NVMe over InfiniBand Ports** を選択します。
NVMe over InfiniBandの統計の表示	1. メニュー：Settings[System]を選択します。 2. *NVMe over InfiniBand設定*までスクロールダウンし、*NVMe over Fabricsの統計情報の表示*を選択します。

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**?**

NVMe over RoCEの設定と管理は、[ハードウェア]ページと[設定]ページで行うことができます。

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。

アクション	**Location**
NVMe over RoCEポートの設定	1. *ハードウェア*を選択します。 2. **Controllers & Components** タブを選択します。 3. コントローラを選択します。 4. *NVMe over RoCE ポートの構成*を選択します。 または 1. メニュー：Settings[System]を選択します。 2. * NVMe over RoCE 設定 * までスクロールダウンし、* NVMe over RoCE ポートの設定 * を選択します。
NVMe over Fabricsの統計の表示	1. メニュー：Settings[System]を選択します。 2. *NVMe over RoCE設定*までスクロールダウンし、*NVMe over Fabrics統計情報の表示*を選択します。

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**?**

EF600ストレージ アレイには、2つのHIC（外部用と内部用）を含めることができます。

この構成では、外部HICが内部の補助HICに接続されます。外部HICからアクセス可能な各物理ポートには、内部HICの仮想ポートが関連付けられています。

最大200Gbのパフォーマンスを実現するには、物理ポートと仮想ポートの両方に一意のIPアドレスを割り当てて、ホストが各ポートへの接続を確立できるようにする必要があります。仮想ポートにIPアドレスを割り当てない場合、HICの実行速度は約半分になります。

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**?**

EF600ストレージ アレイには、2つのHIC（外部用と内部用）を含めることができます。

この構成では、外部HICが内部の補助HICに接続されます。外部HICからアクセス可能な各物理ポートには、内部HICの仮想ポートが関連付けられています。

最大200Gbのパフォーマンスを実現するには、物理ポートと仮想ポートの両方にパラメータを割り当てて、ホストが各ポートへの接続を確立できるようにする必要があります。仮想ポートにパラメータを割り当てない場合、HICの実行速度は約半分になります。

SANtricity System Managerのストレージ ドライブに関するFAQ

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

ホット スペア ドライブとは何ですか?

ホットスペアは、RAID 1、RAID 5、またはRAID 6ボリュームグループにおいて、スタンバイドライブとして機能します。これらはデータが含まれていないものの、完全に機能するドライブです。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、コントローラは障害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。

ストレージ アレイ内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。代わりに、ストレージ アレイ内の同じ容量または小さい容量の障害ドライブに対して、ホットスペア ドライブを使用できます。ホットスペア ドライブは、保護対象のドライブと同じメディア タイプ（HDDまたはSSD）である必要があります。

> ホットスペア ドライブはプールではサポートされていません。ホットスペア ドライブの代わりに、プールはプールを構成する各ドライブ内の保存容量を利用します。

予約済み容量とは何ですか?

予約済み容量は、ドライブ障害に備えてプール内に確保されている容量（ドライブ数）です。

プールが作成されると、プール内のドライブ数に応じて自動的にデフォルトの予約済み容量が確保されます。

プールの予約済み容量は再構築時に使用されますが、ボリューム グループでは同じ目的でホット スペア ドライブが使用されます。予約済み容量を使用する方式は、再構築の時間を短縮できることから、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 ドライブのように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わたって確保されるため、特定のドライブの速度や可用性に制限されません。

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?

ドライブに障害が発生した場合など、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。

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?

ドライブの再構築ステータスは、[実行中の処理]ダッシュボードで確認できます。

ホームページから、右上の*進行中の操作を表示*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。

アラート

SANtricity System Managerのアラートについて学ぶ

SANtricity System Managerを設定して、Eメール、SNMPトラップ、syslogメッセージでストレージアレイアラートを送信できます。

アラートとは何ですか?

_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。イベントには、バッテリ障害、コンポーネントが最適からオフラインに移行、コントローラの冗長性エラーなどの問題が含まれます。すべての重大イベントは、一部の警告イベントおよび情報イベントとともに、「アラート対象」とみなされます。

詳細については、以下を参照してください。

- "アラートの仕組み"
- "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メールアドレスへのメッセージ、SNMPサーバへのSNMPトラップ、またはsyslogサーバへのメッセージとして送信されるように設定できます。アラート設定は、**Settings › Alerts**から使用できます。

詳細については、以下を参照してください。

- "メール サーバとアラートの受信者の設定"
- "アラート用のsyslogサーバの設定"
- "SNMPアラートの設定"

関連情報

アラートに関連する概念の詳細については、以下を参照してください。

- "イベント ログの概要"
- "一致しないタイムスタンプ"

概念

SANtricity System Managerにおけるアラートの仕組み

アラートは、ストレージ アレイ上で発生した重要なイベントについて管理者に通知するもので、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。

1. 管理者は、System Managerで次のいずれかのアラート方法を設定します。

- * Email * — メッセージはEmailアドレスに送信されます。
- **SNMP** — SNMPトラップはSNMPサーバに送信されます。
- **Syslog** — メッセージはsyslogサーバに送信されます。

2. ストレージアレイのイベントモニター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]からアクセスできます）。例えば、問題としては、バッテリーの故障、コンポーネントが最適状態からオフライン状態に移行する、コントローラの冗長性エラーなどが挙げられます。
3. 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、初期設定ウィザード（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、メニューの［設定］→［アラート］を選択してください。

[アラート]タイルには、次のいずれかのアラート設定が表示されます。

- 設定されていません。
- 設定：少なくとも1つのアラート方法が設定されています。どのアラート方法が設定されているかを確認するには、カーソルでタイルをポイントします。

アラート情報

アラートには次の種類の情報を含めることができます。

- ストレージ アレイの名前
- イベント ログ エントリに関連するイベント エラー タイプ
- イベントが発生した日時
- イベントの簡単な説明

syslogアラートはRFC 5424のメッセージ標準に準拠します。

SANtricity ソフトウェアのアラート用語について学ぶ

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。

コンポーネント	概要
イベント モニタ	イベントモニタはストレージアレイ上に存在し、バックグラウンドタスクとして実行されます。イベントモニタがストレージアレイ上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。問題としては、バッテリの障害、コンポーネントが最適状態からオフライン状態に移行する、コントローラの冗長性エラーなどが挙げられます。イベントモニタがイベントを「アラート可能」と判断した場合、設定されたアラート方法（Eメール、SNMP、syslog）を使用して通知を送信します。すべての重大イベントは「アラート可能」とみなされ、一部の警告イベントおよび情報イベントも同様です。

コンポーネント	概要
メール サーバ	メール サーバはEメール アラートを送受信するために使用されます。サーバは簡易メール転送プロトコル（SMTP）を使用します。
SNMP	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。
SNMPトラップ	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。
SNMPトラップの送信先	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。
コミュニティ名	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。
MIBファイル	管理情報ベース（MIB）ファイルは、ストレージアレイ内で監視および管理されるデータを定義します。SNMPサービスアプリケーションがインストールされているサーバー上で、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、サポートサイトにあるSystem Managerソフトウェアに同梱されています。
MIB変数	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。
syslog	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。
UDP	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。

Eメール アラートの管理

SANtricity System Managerでメールサーバとアラート受信者を設定

Eメール アラートを設定するには、メール サーバ アドレスとアラート受信者のEメール アドレスを指定する必要があります。Eメール アドレスは20個まで指定できます。

開始する前に

- メール サーバのアドレスを確認しておく必要があります。アドレスには、IPv4アドレス、IPv6アドレス、または完全修飾ドメイン名を使用できます。

> 完全修飾ドメイン名を使用するには、両方のコントローラにDNSサーバを設定する必要があります。DNSサーバは[ハードウェア]ページで設定できます。

- アラート送信者として使用するEメール アドレスを確認しておく必要があります。このアドレスは、アラート メッセージの「送信元」フィールドに表示されます。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や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。

タスク概要

このタスクでは、メール サーバを設定し、送信者と受信者のEメール アドレスを入力し、入力したすべてのEメール アドレスを[アラート]ページからテストする方法について説明します。

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

1. メニューの「設定」→「アラート」を選択します。
2. * 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。

3. **Configure Mail Server** を選択します。

   メールサーバの設定ダイアログボックスが開きます。

4. メールサーバ情報を入力し、*保存*をクリックします。
   - * メールサーバアドレス * — 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 アドレスを入力します。

     完全修飾ドメイン名を使用するには、両方のコントローラにDNSサーバを設定する必要があります。DNSサーバは[ハードウェア]ページで設定できます。

   - * Eメール送信者アドレス*--Eメールの送信者として使用する有効なEメールアドレスを入力します。このアドレスは、Eメールメッセージの「From」フィールドに表示されます。
   - 暗号化 — メッセージを暗号化する場合は、暗号化の種類として **SMTPS** または **STARTTLS** を選択し、暗号化されたメッセージ用のポート番号を選択してください。それ以外の場合は、 **None** を選択してください。
   - ユーザ名とパスワード — 必要に応じて、送信者とメールサーバーとの認証のためにユーザ名とパスワードを入力してください。
   - メールに連絡先情報を含める — アラートメッセージに送信者の連絡先情報を含めるには、このオプションを選択し、名前と電話番号を入力してください。
     - Save * をクリックすると、 E メールアドレスが Alerts ページの Email タブに表示されます。
5. **Add Emails** を選択します。

   「メールアドレスの追加」ダイアログボックスが開きます。

6. アラートの受信者として1つ以上のメールアドレスを入力し、*追加*をクリックします。

   メールアドレスは Alerts ページに表示されます。

7. メールアドレスが有効かどうかを確認したい場合は、*Test All Emails*をクリックして、受信者にテストメッセージを送信してください。

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。

SANtricity System Managerでアラート用のメールアドレスを編集

Eメール アラートを受け取る受信者のEメール アドレスを変更できます。

開始する前に

編集するEメールアドレスは、「アラート」ページの「Eメール」タブで定義されている必要があります。

手順

1. メニューの「設定」→「アラート」を選択します。
2. * Email * タブを選択します。
3. **Email Address***表から変更したいアドレスを選択し、右端にある***Edit**（鉛筆）アイコンをクリックします。

   行が編集可能になります。
4. 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。

   変更をキャンセルする場合は、**Cancel**（X）アイコンを選択してください。

結果

アラートページの「メール」タブには、更新されたメールアドレスが表示されます。

SANtricity System Managerでアラートの**E**メールアドレスを追加

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

1. メニューの「設定」→「アラート」を選択します。
2. * Email * タブを選択します。
3. **Add Emails** を選択します。

   「メールアドレスの追加」ダイアログボックスが開きます。
4. 空欄に新しいメールアドレスを入力してください。複数のアドレスを追加する場合は、*Add another email*を選択して別の入力欄を開いてください。
5. *[追加]*をクリックします。

結果

アラートページの「メール」タブに、新しいメールアドレスが表示されます。

SANtricity System Managerで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

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

1. メニューの「設定」→「アラート」を選択します。
2. * Email * タブを選択します。
3. 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。
   - アラートが送信されないようにメールアドレスを削除するには、削除したいメールアドレスの行を選択してください。表の右上にある*削除*ボタンが選択可能になります。
4. *Delete*をクリックし、操作を確定してください。

SANtricity System Managerでアラート用のメールサーバを編集

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。

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。

> ⓘ 完全修飾ドメイン名を使用するには、両方のコントローラにDNSサーバを設定する必要があります。DNSサーバは[ハードウェア]ページで設定できます。

手順

1. メニューの「設定」→「アラート」を選択します。
2. * Email * タブを選択します。
3. **Configure Mail Server** を選択します。

   メールサーバの設定ダイアログボックスが開きます。

4. メール サーバのアドレス、送信元情報、および連絡先情報を編集します。
   - * メールサーバアドレス * — 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。

     > ⓘ 完全修飾ドメイン名を使用するには、両方のコントローラにDNSサーバを設定する必要があります。DNSサーバは[ハードウェア]ページで設定できます。

   - **Email sender address** — メール送信者として使用するメールアドレスを編集してください。このアドレスは、メールメッセージの「差出人」欄に表示されます。
   - 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。

5. *保存*をクリックします。

SNMPアラートの管理

SANtricity System ManagerでSNMPアラートを設定

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1つ以上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とサーバのIPアドレスが必要です。

開始する前に

- ネットワーク サーバで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）が必要になります。サーバは最大で10台まで使用することができます。
- 管理情報ベース（MIB）ファイルは、SNMPサービスアプリケーションがインストールされているサーバー上にコピーされ、コンパイルされました。このMIBファイルは、監視および管理されるデータを定義します。

  MIBファイルがない場合は、NetAppサポート サイトから入手できます。

  - "NetAppサポート"に進みます。
  - * ダウンロード * タブをクリックし、次に * ダウンロード * を選択します。
  - **E**シリーズ **SANtricity OS Controller Software** をクリックします。
  - *Download Latest Release*を選択します。
  - ログインします。
  - 注意事項を確認してライセンス契約に同意します。
  - 下にスクロールしてコントローラ タイプに対応するMIBファイルを見つけ、リンクをクリックしてファイルをダウンロードします。

タスク概要

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

1. メニューの「設定」→「アラート」を選択します。
2. * SNMP *タブを選択します。

   初回セットアップ時は、[SNMP]タブに「コミュニティ / ユーザの設定」と表示されます。

3. **Configure Communities/Users** を選択します。

   [SNMP バージョンの選択]ダイアログ ボックスが開きます。

4. 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 ユーザの設定]ダイアログ ボックスが開きます。

5. SNMPv2c（コミュニティ）またはSNMPv3（ユーザ）の該当する手順に従います。
   - **SNMPv2c**（コミュニティ） — [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文字列を1つ以上入力します。コミュニティ名は、既知の管理ステーションのセットを識別する文字列であり、通常はネットワーク管理者によって作成されます。印刷可能なASCII文字のみで構成されています。最大256のコミュニティを追加できます。完了したら、*保存*をクリックします。
   - **SNMPv3**（ユーザ） — Configure SNMPv3 Users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。
     - **Engine 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Engine IDを選択します。このIDは管理ドメイン内で一意である必要があります。ほとんどの場合、*Local*を選択してください。標準以外の構成の場合は、*Custom*を選択してください。別のフィールドが表示されるので、そこに権限のあるエンジンIDを10～32文字の偶数文字の16進数文字列として入力する必要があります。
     - 認証クレデンシャル — 認証プロトコルを選択します。これにより、ユーザーの ID が保証されます。次に、認証パスワードを入力します。これは、認証プロトコルが設定または変更されたときに必要です。パスワードは 8 ～ 128 文字である必要があります。
     - プライバシークレデンシャル — メッセージの内容の暗号化に使用されるプライバシープロトコルを選択します。次に、プライバシーパスワードを入力します。これは、プライバシープロトコルが設定または変更されるときに必要です。パスワードは8～128文字である必要があります。完了したら、*追加*をクリックし、次に*閉じる*をクリックします。
6. SNMPタブを選択したアラートページから、*トラップ宛先の追加*をクリックします。

   「トラップの宛先を追加」ダイアログボックスが開きます。

7. 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ー名を選択してから、*追加*をクリックします。
   - トラップの宛先 — 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 — ドロップダウンリストから、このトラップの宛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。（1つだけ定義した場合は、その名前が既にこのフィールドに表示されます。）
   - 認証失敗トラップの送信 — 認識されないコミュニティ名またはユーザ名が原因でSNMPリクエストが拒否された場合に、トラップの宛先にアラートを送信する場合は、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、トラップの宛先と関連付けられた名前が、*アラート*ページの*SNMP*タブに表示されます。
8. トラップが有効であることを確認するには、表からトラップの送信先を選択し、*トラップ送信先のテスト*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。

SANtricity System Managerで**SNMP**アラートのトラップ宛先を追加する

SNMPトラップの送信に使用するサーバは最大で10台まで追加できます。

開始する前に

- 追加するネットワーク サーバで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）が必要になります。サーバは最大で10台まで使用することができます。
- 管理情報ベース（MIB）ファイルは、SNMPサービスアプリケーションがインストールされているサーバー上にコピーされ、コンパイルされました。このMIBファイルは、監視および管理されるデータを定義します。

  MIBファイルがない場合は、NetAppサポート サイトから入手できます。

  - "NetAppサポート"に進みます。
  - *ダウンロード*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 Controller Software** をクリックします。
  - *Download Latest Release*を選択します。
  - ログインします。
  - 注意事項を確認してライセンス契約に同意します。
  - 下にスクロールしてコントローラ タイプに対応するMIBファイルを見つけ、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

1. メニューの「設定」→「アラート」を選択します。
2. * 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。

3. *Add Trap Desinations*を選択します。

   「トラップの宛先を追加」ダイアログボックスが開きます。

4. 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ー名を選択してから、*追加*をクリックします。
   - トラップの宛先 — 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 — ドロップダウンリストから、このトラップの宛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。（1つだけ定義した場合は、その名前が既にこのフィールドに表示されます。）
   - 認証失敗トラップの送信 — 認識されないコミュニティ名またはユーザー名が原因でSNMPリクエストが拒否された場合に、トラップの宛先にアラートを送信する場合は、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、それに関連付けられたコミュニティ名またはユーザー名が表に表示されます。
5. トラップが有効であることを確認するには、表からトラップの送信先を選択し、*トラップ送信先のテスト*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。

SANtricity System ManagerでのSNMP MIB変数の設定

SNMPアラートの設定では、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）変数を設定することができます。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。

開始する前に

SNMPサービス アプリケーションがあるサーバに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。

- "NetAppサポート"に進みます。
- *ダウンロード*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 Controller Software** をクリックします。
- *Download Latest Release*を選択します。
- ログインします。
- 注意事項を確認してライセンス契約に同意します。
- 下にスクロールしてコントローラ タイプに対応するMIBファイルを見つけ、リンクをクリックしてファイルをダウンロードします。

タスク概要

このタスクでは、SNMPトラップ用の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に応答して以下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

1. メニューの「設定」→「アラート」を選択します。
2. * SNMP *タブを選択します。
3. * 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。

4. 以下の値を1つ以上入力し、*保存*をクリックします。
   - 名前 — MIB変数の値 `sysName`。たとえば、ストレージアレイの名前を入力します。
   - 場所 — MIB変数の値 `sysLocation`。たとえば、ストレージアレイの場所を入力します。
   - 連絡先 — 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。

SANtricity System Managerで**SNMPv2c**トラップのコミュニティを編集します

SNMPv2cトラップのコミュニティ名を編集できます。

開始する前に

コミュニティ名が作成されている必要があります。

手順

1. メニュー:Setting[Alerts]を選択します。
2. * 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。

3. * Configure Communities * を選択します。
4. 新しいコミュニティ名を入力し、*保存*をクリックします。コミュニティ名には、印刷可能なASCII文字のみを使用できます。

結果

[アラート]ページの[SNMP]タブに、更新されたコミュニティ名が表示されます。

SANtricity System Managerで**SNMPv3**トラップのユーザー設定を編集します

SNMPv3トラップのユーザ定義を編集できます。

開始する前に

SNMPv3トラップのユーザが作成されている必要があります。

手順

1. メニューの「設定」→「アラート」を選択します。
2. * 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。

3. ユーザー定義を編集するには、表からユーザーを選択し、*ユーザー設定*をクリックします。
4. ダイアログで、**View/Edit Settings** をクリックします。
5. 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。
   - **Engine 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Engine IDを選択します。このIDは管理ドメイン内で一意である必要があります。ほとんどの場合、*Local*を選択してください。標準以外の構成の場合は、*Custom*を選択してください。別のフィールドが表示されるので、そこに権限のあるエンジンIDを10～32文字の偶数文字の16進数文字列として入力する必要があります。
   - 認証クレデンシャル — 認証プロトコルを選択します。これにより、ユーザーの ID が保証されます。次に、認証パスワードを入力します。これは、認証プロトコルが設定または変更されたときに必要です。パスワードは 8 ～ 128 文字である必要があります。
   - プライバシークレデンシャル — メッセージの内容の暗号化に使用されるプライバシープロトコルを選

択します。次に、プライバシーパスワードを入力します。これは、プライバシープロトコルが設定または変更されたときに必要です。パスワードは8～128文字である必要があります。

結果

[アラート]ページの[SNMP]タブに、更新された設定が表示されます。

SANtricity System ManagerでSNMPv2cトラップのコミュニティを追加

SNMPv2cトラップのコミュニティ名は最大で256個追加できます。

手順

1. メニューの「設定」→「アラート」を選択します。
2. * 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。

3. * Configure Communities * 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。

4. **Add another community** を選択します。
5. 新しいコミュニティ名を入力し、*保存*をクリックします。

結果

新しいコミュニティ名は、アラートページの SNMP タブに表示されます。

SANtricity System ManagerでSNMPv3トラップのユーザーを追加

SNMPv3トラップのユーザは最大で256個追加できます。

手順

1. メニューの「設定」→「アラート」を選択します。
2. * 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。

3. *Configure Users*を選択します。

   [SNMPv3 ユーザの設定]ダイアログ ボックスが開きます。

4. *追加*を選択します。
5. 以下の情報を入力し、*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。
   - **Engine 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Engine IDを選択します。このIDは管理ドメイン内で一意である必要があります。ほとんどの場合、*Local*を選択してください。標準以外の構成の場合は、*Custom*を選択してください。別のフィールドが表示されるので、そこに権限のあるエンジンIDを10～32文字の偶数文字の16進数文字列として入力する必要があります。

- 認証クレデンシャル — 認証プロトコルを選択します。これにより、ユーザーの ID が保証されます。次に、認証パスワードを入力します。これは、認証プロトコルが設定または変更されたときに必要です。パスワードは 8 ～ 128 文字である必要があります。
- プライバシークレデンシャル — メッセージの内容の暗号化に使用されるプライバシープロトコルを選択します。次に、プライバシーパスワードを入力します。これは、プライバシープロトコルが設定または変更されたときに必要です。パスワードは8～128文字である必要があります。

SANtricity System Managerで**SNMPv2c**トラップのコミュニティを削除する

SNMPv2cトラップのコミュニティ名を削除できます。

手順

1. メニューの「設定」→「アラート」を選択します。
2. * 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、*アラート*ページに表示されます。

3. * Configure Communities * 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。

4. 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。

   トラップの宛先がこのコミュニティ名に関連付けられている場合、［コミュニティの削除の確認］ダイアログボックスに、影響を受けるトラップの宛先アドレスが表示されます。

5. 操作を確認し、*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たトラップの送信先は、アラートページから削除されます。

SANtricity System Managerで**SNMPv3**トラップのユーザーを削除する

SNMPv3トラップのユーザを削除できます。

手順

1. メニューの「設定」→「アラート」を選択します。
2. * SNMP *タブを選択します。

   トラップの送信先とユーザ名が[アラート]ページに表示されます。

3. *Configure Users*を選択します。

   [SNMPv3 ユーザの設定]ダイアログ ボックスが開きます。

4. 削除するユーザー名を選択し、*削除*をクリックします。
5. 操作を確認し、*削除*をクリックします。

結果

ユーザ名および関連付けられているトラップ送信先が[アラート]ページから削除されます。

SANtricity System Managerでトラップの宛先を削除します

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

1. メニューの「設定」→「アラート」を選択します。
2. * 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。

3. 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。
4. 操作を確認し、*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した。

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。

syslogアラートの管理

SANtricity System Managerでアラート用のsyslogサーバーを設定する

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。最大で5台のsyslogサーバを指定できます。

開始する前に

- syslogサーバのアドレスを確認しておく必要があります。このアドレスは、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスのいずれかで指定できます。
- syslogサーバのUDPポート番号を確認しておく必要があります。通常は514です。

タスク概要

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

1. メニューの「設定」→「アラート」を選択します。
2. *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、[アラート]ページに「syslog サーバの追加」と表示されます。

3. * Add Syslog Servers * をクリックします。

   [syslogサーバの追加]ダイアログ ボックスが開きます。

4. 1つ以上のsyslogサーバーの情報を入力し（最大5台）、*追加*をクリックします。
   - 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 — 通常、syslogのUDPポートは514です。この表には、設定済みのsyslogサーバーが表示されます。
5. サーバアドレスにテストアラートを送信するには、* Test All Syslog Servers *を選択します。

結果

イベントモニタは、アラート可能なイベントが発生するたびに syslog サーバにアラートを送信します。監査ログの syslog 設定をさらに設定するには、 "監査ログ用のsyslogサーバの設定"を参照してください。

> 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。

SANtricity System Managerでアラート用の**syslog**サーバーを編集

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

1. メニューの「設定」→「アラート」を選択します。
2. *Syslog*タブを選択します。
3. 表から syslog サーバーアドレスを選択し、右端にある 編集 （鉛筆）アイコンをクリックします。

   行が編集可能になります。
4. 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てください。

結果

更新されたサーバ アドレスが表に表示されます。

SANtricity System Managerでアラート用の**syslog**サーバーを追加

syslogアラート用に最大5台のサーバを追加することができます。

開始する前に

- syslogサーバのアドレスを確認しておく必要があります。このアドレスは、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスのいずれかで指定できます。
- syslogサーバのUDPポート番号を確認しておく必要があります。通常は514です。

手順

1. メニューの「設定」→「アラート」を選択します。
2. *Syslog*タブを選択します。
3. *syslogサーバーの追加*を選択します。

   [syslogサーバの追加]ダイアログ ボックスが開きます。

4. *別のsyslogサーバを追加*を選択します。
5. syslogサーバーの情報を入力し、*追加*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 — 通常、syslogのUDPポートは514です。

   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。

SANtricity System Managerでアラート用の**syslog**サーバを削除

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

1. メニューの「設定」→「アラート」を選択します。
2. *Syslog*タブを選択します。
3. syslogサーバアドレスを選択し、右上の*削除*をクリックします。

   「syslogサーバの削除の確認」ダイアログボックスが開きます。
4. 操作を確認し、*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。

SANtricity System Managerのストレージシステムアラートに関するよくある質問

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

アラートが無効になっている場合はどうすればよいですか**?**

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け取るためには、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メッセージで送信できます。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。

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**?**

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アラートを設定するには、メニューの「設定」→「アラート」を選択してください。

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?

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時間を加算するか減算します。

アレイ設定

SANtricity System Managerの設定の概要について説明します

一般的なアレイ設定やアドオン機能について、SANtricity System Managerを設定できます。

何を設定できますか?

アレイ設定には以下のものがあります。

- "キャッシュの設定とパフォーマンス"
- "自動ロード バランシング"
- "アドオン機能"
- "ドライブ セキュリティ"

関連タスク

システム設定に関連するタスクの詳細については、以下を参照してください。

- "コマンドライン インターフェイス（CLI）のダウンロード"
- "内部セキュリティ キーの作成"
- "外部セキュリティ キーの作成"
- "iSCSIポートの設定"
- "NVME over IBポートの設定"
- "NVMe over RoCEポートの設定"

概念

SANtricityソフトウェアのキャッシュ設定とパフォーマンスについて学ぶ

キャッシュ メモリは、ドライブ メディアよりも高速なアクセスが可能な、コントローラ上の揮発性の一時ストレージの領域です。

キャッシュを使用すると、全体的なI/Oパフォーマンスが次のように向上します。

- 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保持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対して、[システム]ページで次の値を指定できます。

- フラッシュ開始値 — 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、キャッシュ内の未書き込みデータの割合。キャッシュに指定された開始割合の未書き込みデータが蓄積されると、フラッシュ処理がトリガーされます。デフォルトでは、キャッシュが80%満たされると、コントローラは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 — キャッシュ管理における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は8 KiBですが、4、8、16、または32 KiBに設定できます。理想的には、キャッシュブロックサイズはアプリケーションの主要なI/Oサイズに設定する必要があります。ファイルシステムやデータベースアプリケーションは一般的に小さめのサイズを使用する一方、大容量のデータ転送やシーケンシャルなI/Oが必要なアプリケーションには大きめの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は、[ボリューム]ページ（メニュー：ストレージ[ボリューム]）から以下の値を指定できます：

- 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。読み取り操作に必要なデータは、以前の操作によって既にキャッシュに格納されている場合があり、その場合はドライブにアクセスする必要がなくなります。データは、フラッシュされるまで読み取りキャッシュに保持されます。
  - ダイナミック読み取りキャッシュプリフェッチ — ダイナミックキャッシュ読み取りプリフェッチを使用すると、コントローラはドライブからキャッシュにデータブロックを読み取っている間に、追加の連続データブロックをキャッシュにコピーできます。このキャッシュ機能により、将来のデータ要求がキャッシュから満たされる可能性が高まります。ダイナミック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にとって重要です。キャッシュにプリフェッチされるデータの速度と量は、ホストの読み取り速度とリクエストサイズに基づいて自動的に調整されます。ランダムアクセスでは、データがキャッシュにプリフェッチされることはありません。この機能は、読み取りキャッシュが無効になっている場合は適用されません。
- 書き込みキャッシュ — 書き込みキャッシュは、ホストからドライブにまだ書き込まれていないデータを格納するバッファです。データは、ドライブに書き込まれるまで書き込みキャッシュに保持されます。書き込みキャッシュはI/Oサイズのパフォーマンスを向上させることができます。

> データ損失の可能性 — *バッテリーなしで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がない場合、データが失われる可能性があります。さらに、コントローラバッテリがなく、*バッテリーなしで書き込みキャッシュ*オプションを有効にした場合、データが失われる可能性があります。

  - バッテリーなしでの書き込みキャッシュ — バッテリーなしでの書き込みキャッシュ設定により、バッ

テリーが欠落している、故障している、完全に放電している、または完全に充電されていない場合でも、書き込みキャッシュを継続できます。バッテリーなしでの書き込みキャッシュを選択することは、電源が切れた場合にデータが失われる可能性があるため、通常は推奨されません。通常、書き込みキャッシュは、バッテリーが充電されるか、故障したバッテリーが交換されるまで、コントローラによって一時的に無効になります。

- ミラーリングによる書き込みキャッシュ — ミラーリングによる書き込みキャッシュは、一方のコントローラのキャッシュメモリに書き込まれたデータが、もう一方のコントローラのキャッシュメモリにも書き込まれる場合に発生します。したがって、一方のコントローラが故障した場合でも、もう一方のコントローラが未完了の書き込み操作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になっており、かつ2つのコントローラが存在する場合にのみ利用可能です。ミラーリングによる書き込みキャッシュは、ボリューム作成時のデフォルト設定です。

SANtricity ソフトウェアの自動ロード バランシングについて学ぶ

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が継続的に監視され、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調整することができます。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応じ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が自動的に監視されて負荷が分散されます。
- 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 アレイ上でデフォルトで有効に設定されています。

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もできます。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したい。
- 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。

これは、負荷分散の処理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を防ぐための措置ですが、

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ません。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。

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。

自動ロード バランシングをサポートするホストタイプ	このマルチパスドライバを使用
WindowsまたはWindowsクラスタ	MPIOとNetApp EシリーズDSM
Linux DM-MP（カーネル3.10以降）	DM-MPと `scsi_dh_alua`デバイス ハンドラー
VMware	`VMW_SATP_ALUA Storage Array Type`プラグインを使用したネイティブマルチパス プラグイン（NMP）

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。

特定のマルチパス ドライバ、OS レベル、およびコントローラ ドライブ トレイのサポートに関する互換性情報については、 "Interoperability Matrix Tool"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との互換性を確認します。

1. "Interoperability Matrix Tool"にアクセスして、ソリューションを見つけ、サポート状況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に関しては、テクニカル サポートにお問い合わせください。

2. `/etc/multipath.conf file`を更新して設定します。
3. `retain_attached_device_handler`と `detect_prio`の両方が、該当するベンダーおよび製品に対して `yes`に設定されていることを確認するか、デフォルト設定を使用してください。

アレイの設定

SANtricity System Managerでストレージアレイ名を編集

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できます。

手順

1. メニュー：Settings[System]を選択します。
2. **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は、このフィールドに「不明」と表示されます。

3. ストレージアレイ名の横にある*編集*（鉛筆）アイコンをクリックします。

   フィールドを編集できるようになります。

4. 新しい名前を入力します。

   名前には、文字、数字、および特殊文字であるアンダースコア（_）、ダッシュ（-）、ハッシュ記号（#）を含めることができます。名前にスペースを含めることはできません。名前の最大長は30文字です。名前は一意である必要があります。

5. 保存（チェックマーク）アイコンをクリックします。

   変更を加えずに編集可能なフィールドを閉じたい場合は、**Cancel**（X）アイコンをクリックしてください。

結果

新しい名前は SANtricity System Manager のタイトルバーに表示されます。

SANtricity System Managerでストレージアレイロケーターライトをオンにする

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

1. メニュー：Settings[System]を選択します。
2. *General*で、*Turn on Storage Array Locator Lights*をクリックします。

   「ストレージ アレイ ロケータ ライトをオンにする」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 ライトが点灯します。

3. ストレージアレイの物理的な位置を確認したら、ダイアログボックスに戻り、*オフにする*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。

SANtricity System Managerでストレージアレイのクロックを同期します

ネットワークタイムプロトコル（NTP）が有効になっていない場合は、コントローラーの時計を手動で設定して、管理クライアント（SANtricity System Managerにアクセスするブラウザを実行するシステム）と同期させることができます。

タスク概要

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。同期プロセス中でも、コントローラを引き続き使用できます。

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時計を同期しないでください。その代わりに、NTPはSNTP（Simple Network Time Protocol）を使用して外部ホストと自動的に時計を同期します。

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を使用して、この問題を回避します。

手順

1. メニュー：Settings[System]を選択します。
2. *全般*で、*ストレージアレイのクロックを同期する*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 ボックスには、コントローラおよび管理クライアントとして使用されるコンピュータの現在の日時が表示されます。

   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つだけです。

3. ダイアログボックスに表示されている時刻が一致しない場合は、*Synchronize*をクリックしてください。

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。

SANtricity System Managerでストレージアレイ構成を保存

ストレージアレイの設定情報をスクリプトファイルに保存することで、同じ設定を持つ追加のストレージアレイをセットアップする際の時間を節約できます。

開始する前に

ストレージアレイは、論理構成設定を変更するような操作を受けていない状態である必要があります。これらの操作の例としては、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）の追加などが挙げられます。

タスク概要

ストレージアレイの設定を保存すると、ストレージアレイの設定、ボリュームの設定、ホストの設定、またはストレージアレイの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。この生成されたCLIスクリプトを使用すると、まったく同じハードウェア構成を持つ別のストレージアレイに構成を複製できます。

ただし、この生成されたCLIスクリプトを災害復旧に使用しないでください。代わりに、システム復元を行うには、手動で作成した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連絡して最新のAuto-Supportデータからこのデータを入手してください。

この操作では、以下の設定は保存_されません_：

- バッテリの寿命
- 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および状態
- ボリューム グループの動作ステータス（最適を除く）および状態
- ミラーリング、ボリューム コピーなどのコピー サービス

> アプリケーションエラーのリスク — ストレージアレイが論理構成設定を変更する操作を実行している場合は、このオプションを使用しないでください。これらの操作の例としては、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）の追加などが挙げられます。

手順

1. メニュー：Settings[System]を選択します。
2. **Save Storage Array Configuration** を選択します。
3. 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
   - ホスト構成
   - ホスト / ボリューム間の割り当て

   > *Host-to-volume assignments*項目を選択すると、*Volume configuration*項目と*Host configuration*項目もデフォルトで選択されます。「Volume configuration」と「Host configuration」を保存せずに「Host-to-volume assignments」を保存することはできません。

4. *保存*をクリックします。

   ファイルは、ブラウザのダウンロードフォルダに次の名前で保存されます `storage-array-configuration.cfg`。

終了後の操作

保存したストレージアレイ構成を別のストレージアレイにロードするには、SANtricityコマンドラインインターフェイス（SMcli）と `-f`オプションを使用して `.cfg`ファイルを適用します。

Unified Managerインターフェイスを使用して、ストレージアレイ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（メニュー：Manage[Import Settings]を選択）。

SANtricity System Managerでストレージアレイ構成をクリアします

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、構成のクリア処理を使用します。

開始する前に

ストレージ アレイ構成をクリアする前に、データのバックアップを作成します。

タスク概要

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、ボリュームオプションを使用して、テスト用ストレージアレイを本番用ストレージアレイとして再構成することがあります。例えば、テスト用にストレージアレイを構成し、テストが完了したら、テスト構成を削除して本番環境用にストレージアレイをセットアップすることができます。
- **Storage Array** — 通常、Storage Arrayオプションを使用して、ストレージアレイを別の部門またはグループに移動します。例えば、Engineering部門でストレージアレイを使用しているとします。Engineering部門に新しいストレージアレイが導入されることになったため、現在のストレージアレイをAdministration部門に移動して再構成したい場合などです。

  [ストレージ アレイ]オプションでは、いくつかの設定が追加で削除されます。

	Volume	ストレージ アレイ
ARVMを非アクティブ化	X	X
プールとボリューム グループを削除	X	X
ボリュームを削除	X	X
ホストとホスト クラスタを削除	X	X
ホスト割り当てを削除	X	X
ストレージ アレイ名を削除		X
ストレージ アレイのキャッシュ設定をデフォルトに戻す		X

データ損失のリスク — この処理により、ストレージアレイからすべてのデータが削除されます。（セキュアイレースは実行されません。）この処理は、開始後にキャンセルできません。この処理は、テクニカルサポートから指示された場合にのみ実行してください。

手順

1. メニュー：Settings[System]を選択します。
2. * Clear Storage Array Configuration * を選択します。
3. ドロップダウンリストから、* Volume または Storage Array *のいずれかを選択します。
4. オプション： 設定（データではなく）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てください。
5. 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。

ストレージアレイはリカバリモードで起動します。ストレージアレイを使用する前に、リカバリモードを解除する必要があります。詳細については、 "リカバリ モードのクリア"を参照してください。

SANtricity System Managerでストレージアレイのキャッシュ設定を変更する

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。

タスク概要

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チューニングする場合は、次の設定を調整できます。

キャッシュ設定	概要
デマンド キャッシュ フラッシュの開始	デマンドキャッシュフラッシュの開始は、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未書き込みデータの割合を指定します。デフォルトでは、未書き込みデータが容量の80%に達するとキャッシュフラッシュが開始されます。書き込み処理が主な環境では、より高い割合を設定することをお勧めします。これにより、新しい書き込み要求をディスクにアクセスすることなくキャッシュで処理できます。I/Oが不安定な環境（データバーストを伴う環境）では、低い設定の方が適しています。これにより、システムはデータバーストの合間にキャッシュを頻繁にフラッシュします。ただし、開始率が80%を下回ると、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	キャッシュブロックサイズは、キャッシュ管理における組織単位である各キャッシュブロックの最大サイズを決定します。デフォルトでは、ブロックサイズは32 KiBです。このシステムでは、キャッシュブロックサイズを4、8、16、または32 KiBsに設定できます。アプリケーションによって使用するブロックサイズが異なるため、ストレージのパフォーマンスに影響が出ます。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、より小型のサイズが適しています。より大きなサイズは、マルチメディアなど、シーケンシャルI/Oを行うアプリケーションに最適です。

手順

1. メニュー：Settings[System]を選択します。
2. *Additional Settings*までスクロールダウンし、*Change Cache Settings*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。

3. 次の値を調整します。
   - デマンドキャッシュのフラッシュを開始します — ご使用の環境で使用されるI/Oサイズに適したパーセンテージを選択してください。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。
4. *保存*をクリックします。

SANtricity System Managerで自動ロード バランシングを設定します

自動ロード バランシング機能により、ホストからの受信I/Oトラフィックが両方のコントローラ間で動的に管理および分散されます。この機能はデフォルトで有効になっていますが、SANtricity System Managerから無効にすることができます。

タスク概要

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が自動的に監視されて負荷が分散されます。
- 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もできます。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したい。
- 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

1. メニュー：Settings[System]を選択します。
2. *追加設定*までスクロールダウンし、*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。

3. *はい*をクリックして確認します。

   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。

   > この機能を無効から有効に切り替えた場合は、ホスト接続のレポート機能も自動的に有効になります。

SANtricity System Managerでレガシー管理インターフェイスを有効または無効にする

ストレージ アレイと管理クライアントの間の通信方法である、従来の管理インターフェイス（SYMbol）を有効または無効にすることができます。

タスク概要

デフォルトでは、従来の管理インターフェイスは有効になっています。無効にすると、ストレージ アレイと管理クライアントはよりセキュアな通信方法（REST API over https）を使用します。ただし、無効にした場合、特定のツールやタスクに影響が出る場合があります。

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。

- オン（デフォルト）-- CLI や OCI アダプタなどの他のツールを使用してミラーリングを構成するために必要な設定です。
- オフ — ストレージ アレイと管理クライアント間の通信における機密性を確保し、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 サーバー（LDAP）を設定する際の推奨設定。

手順

1. メニュー：Settings[System]を選択します。
2. *追加設定*までスクロールダウンし、*管理インターフェイスの変更*をクリックします。
3. ダイアログボックスで **Yes** をクリックして続行してください。

アドオン機能の設定

SANtricity System Managerでのアドオン機能の仕組み

アドオンは、SANtricity System Managerの標準構成に含まれていない機能であり、有効化するためにキーが必要になる場合があります。アドオン機能は、単一のプレミアム機能またはバンドル機能パックのいずれかです。

以下は、プレミアム機能または機能パックを有効化するおおまかな手順です。

1. 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で確認できます。
   - Feature Activation Code。機能購入時にサポート サイトから入手できます。
2. 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。シャーシのシリアル番号、有効識別子、およびFeature Activation Codeを指定します。
3. 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。

SANtricity ソフトウェアのアドオン機能の用語について説明します

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。

期間	概要
機能有効識別子	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]に表示されます。
機能キー ファイル	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。
機能パック	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。
プレミアム機能	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。

SANtricity System Managerでフィーチャーキーファイルを取得する

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 アレイのみに関連付けられます。

タスク概要

このタスクでは、必要な情報を収集し、機能キー ファイルのリクエスト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

手順

1. System Managerで、シャーシのシリアル番号を確認し、記録してください。このシリアル番号は、[サポート センター]タイルの上にマウスを移動すると表示されます。
2. System Managerで、Feature Enable Identifierを探します。メニューの「Settings」→「System」を選択し、下にスクロールして*Add-ons*を探してください。*Feature Enable Identifier*を探してください。Feature Enable Identifierの番号を記録してください。
3. 機能をアクティブ化するためのコードを確認して記録します。機能パックの場合、このコードの確認方法は該当するドキュメントの変換手順に記載されています。

   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 コードを入手できます。

   a. "NetAppサポート"にログインします。
   b. お使いの製品の*ソフトウェアライセンス*に移動します。
   c. 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。
   d. *ライセンスキー*列で機能有効化コードを確認します。

e. 必要な機能のFeature Activation Codeを記録します。

4. シャーシのシリアル番号、有効識別子、機能をアクティブ化するためのコードを記載したEメールまたは文書をストレージ サプライヤに送信して、機能キー ファイルをリクエストします。

   また、 "NetAppライセンスアクティベーション：ストレージアレイプレミアム機能のアクティベーション" にアクセスして、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てください。（このサイトの説明は、プレミアム機能に関するものであり、機能パックに関するものではありません。）

終了後の操作

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できます。

SANtricity System Managerでプレミアム機能を有効にする

プレミアム機能は追加オプションであり、有効にするにはキーが必要です。

開始する前に

- 機能キーを取得しておきます。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がインストールされているシステム）にキーファイルをロードしました。

タスク概要

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。

> プレミアム機能を無効にする場合は、コマンドラインインターフェイス（CLI）で Disable Storage Array Feature コマンド(`disable storageArray) (featurePack | feature=featureAttributeList`を使用する必要があります。

手順

1. メニュー：Settings[System]を選択します。
2. *アドオン*で、*プレミアム機能を有効にする*を選択します。

   [プレミアム機能の有効化]ダイアログ ボックスが開きます。

3. **Browse** 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。

4. * Enable * をクリックします。

SANtricity System Managerで機能パックを有効にする

機能パックは、ストレージ アレイの属性を変更する（プロトコルをFibre ChannelからiSCSIに変更するなど）バンドルです。機能パックを有効にするには特別なキーが必要です。

開始する前に

- 該当する手順に従って、新しいストレージ アレイ属性に応じた変換と準備を完了しておきます。ホストプロトコルの変更手順については、コントローラのモデルに対応したハードウェア 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ている。
- 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）にロードされます。

> ⓘ システムを停止するメンテナンス期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、変換を完了するまでは、ストレージ アレイ上のデータにアクセスできないことに注意してください。

タスク概要

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。作業が完了したら、ストレージアレイを再起動する必要があります。

手順

1. メニュー：Settings[System]を選択します。
2. **Add-ons** の下にある **Change Feature Pack** を選択します。
3. **Browse** 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。
4. フィールドに `change`と入力します。
5. **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。

SANtricityコマンドラインインターフェース（CLI）をダウンロード

SANtricity System Managerから、コマンドラインインターフェース（CLI）パッケージをダウンロードできます。

CLIでは、テキストベースのコマンドを使用してストレージ 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。

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

1. メニュー：Settings[System]を選択します。
2. *アドオン*で*Command Line Interface*を選択します。

   ZIPパッケージがブラウザにダウンロードされます。

3. 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のC：プロンプトなど、オペレーティングシステムのプロンプトからCLIコマンドを実行できるようになりました。CLIコマンドのリファレンスは、System Managerのユーザーインターフェイス右上にあるヘルプメニューから入手できます。

SANtricity System Managerのストレージ アレイ設定に関するよくある質問

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

自動ロード バランシングとは何ですか?

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配されます。

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が継続的に監視され、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調整することができます。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応じ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が自動的に監視されて負荷が分散されます。
- 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。

> 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。

コントローラ キャッシュとは何ですか?

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。ところが、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高速ではありません。

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。

> データ損失の可能性 — *バッテリーなしで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がない場合、データが失われる可能性があります。さらに、コントローラバッテリがなく、*バッテリーなしで書き込みキャッシュ*オプションを有効にした場合、データが失われる可能性があります。

キャッシュのフラッシュとは何ですか**?**

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上回った場合に使用されます。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、「要求キャッシュのフラッシュを開始する」しきい値を設定することで、環境で使用されるI/Oの種類を最適にサポートできます。主に書き込み操作が行われる環境では、「要求キャッシュのフラッシュを開始する」のパーセンテージを高く設定して、新しい書き込み要求がディスクにアクセスすることなくキャッシュによって処理される可能性を高める必要があります。高いパーセンテージ設定はキャッシュのフラッシュ回数を制限するため、より多くのデータがキャッシュに保持され、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て、システム オーバーヘッドが増大します。

使用期間ベースのアルゴリズムは、書き込みデータがディスクにフラッシュされる前にキャッシュ内に保持できる期間を指定します。コントローラーは、キャッシュフラッシュのしきい値に達するまで使用期間ベースのアルゴリズムを使用します。デフォルト値は10秒ですが、この期間は非アクティブ期間中のみカウントされます。System Managerではフラッシュのタイミングを変更できません。代わりに、コマンドラインインターフェイス（CLI）で*Set Storage Array*コマンドを使用する必要があります。

データ損失の可能性 — *バッテリーなしで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がない場合、データが失われる可能性があります。さらに、コントローラバッテリがなく、*バッテリーなしで書き込みキャッシュ*オプションを有効にした場合、データが失われる可能性があります。

キャッシュ ブロック サイズとは何ですか?

ストレージ アレイのコントローラは、キャッシュを「ブロック」と呼ばれるメモリの塊に編成します。ブロックのサイズは8、16、32 KiBのいずれかです。ストレージ システム上のすべてのボリュームは同じキャッシュ領域を共有するため、ボリュームごとに設定できるキャッシュ ブロック サイズは1種類のみです。

アプリケーションによって使用するブロック サイズが異なるため、ストレージのパフォーマンスに影響を与える可能性があります。System Managerのブロック サイズはデフォルトでは32 KiBですが、8、16、32 KiBsに設定することもできます。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、またはマルチメディアなどの高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。

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?

SANtricity System Managerに表示されるタイムスタンプが管理クライアント（ブラウザを介してSANtricity System Managerにアクセスしているコンピュータ）に表示されるタイムスタンプと一致していない場合は、ストレージ アレイ内のコントローラ クロックを手動で同期する必要があります。このタスクは、SANtricity System ManagerでNTP（Network Time Protocol）が有効になっていない場合にのみ必要です。

クロックを手動で同期する代わりに、NTPサーバを使用することを強く推奨します。NTPは、SNTP（Simple Network Time Protocol）を使用して自動的にクロックを外部サーバと同期します。

同期ステータスは、[システム]ページからアクセスする[ストレージ アレイ クロックの同期]ダイアログ ボックスで確認できます。ダイアログ ボックスに表示される時間が一致していない場合は、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 クロックの時刻表示が同期されているかどうかを確認できます。

ドライブ セキュリティ

SANtricity System Managerのドライブセキュリティについて学ぶ

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]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、ストレージアレイから取り外されたセキュリティ対応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。これらのドライブは、Full Disk Encryption（FDE）ドライブまたはFederal Information Processing Standard（FIPS）ドライブのいずれかです。FDEまたはFIPSドライブがアレイから物理的に取り外された場合、別のアレイにインストールされるまで動作せず、インストールされた時点で、正しいセキュリティキーが提供されるまで、ドライブはSecurity Locked状態になります。_セキュリティキー_とは、これらのタイプのドライブとストレージアレイ内のコントローラ間で共有される文字列のことです。

詳細については、以下を参照してください。

- "ドライブ セキュリティ機能の仕組み"
- "セキュリティ キー管理の仕組み"
- "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**?**

Drive Securityを実装するには、アレイにFDEドライブまたはFIPSドライブのいずれかがインストール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、メニューの「Settings」→「System」→「Security key management」に移動し、コントローラの永続メモリからの内部キー、またはキー管理サーバーからの外部キーを作成できます。最後に、ボリューム設定で「secure-capable」を選択することで、プールとボリュームグループのDrive Securityを有効にします。

詳細については、以下を参照してください。

- "内部セキュリティ キーの作成"
- "外部セキュリティ キーの作成"
- "プールの手動作成"
- "ボリュームグループを作成する"

ドライブのロックを解除するにはどうすればよいですか**?**

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 キーを再度割り当てる必要があります。

詳細については、以下を参照してください。

- "内部キー管理を使用する場合のドライブのロック解除"
- "外部キー管理を使用する場合のドライブのロック解除"

関連情報

キー管理に関連するタスクの詳細については、以下を参照してください。

- "CA署名証明書を使用したキー管理サーバでの認証"
- "セキュリティ キーのバックアップ"

概念

SANtricity System Managerにおけるドライブセキュリティ機能の仕組み

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際にセキュリティ キーが要求されるようになります。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、取り付けたあとも正しいセキュリティ キーが提供されないかぎりセキュリティ 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。

1. ストレージアレイには、FDEドライブまたはFIPSドライブのいずれか、セキュリティ機能を備えたドライブを搭載してください。（FIPS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てください。ボリュームグループまたはプール内でFIPSドライブとFDEドライブを混在させると、すべてのドライブがFDEドライブとして扱われます。また、FDEドライブは、FIPS準拠のボリュームグループまたはプールに追加したり、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。これは、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かのいずれかを選択できます。外部キー管理の場合、キー管理サーバとの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のドライブセキュリティを有効にする：
   - プールまたはボリューム グループを作成します（候補テーブルの セキュリティ対応 列で はい を探してください）。
   - 新しいボリュームを作成する際に、プールまたはボリュームグループを選択してください（プールおよびボリュームグループの候補テーブルで、*Secure-capable*の横に*Yes*が表示されていることを確認してください）。

ドライブ レベルでのドライブ セキュリティの動作

セキュリティ機能を備えたドライブ（FDEまたはFIPSのいずれか）は、書き込み時にデータを暗号化し、読み取り時にデータを復号化します。この暗号化および復号化は、パフォーマンスやユーザのワークフローに影響を与えません。各ドライブには独自の暗号化キーがあり、これはドライブから転送することは決してできません。

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に対して追加の保護層を提供します。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がドライブ セキュリティの対象として選択されると、ドライブはデータへのアクセスを許可する前にセキュリティ キーを要求します。ドライブ上の既存データに影響を与えることなく、プールやボリューム グループに対していつでもドライブ セキュリティを有効にすることができます。ただし、ドライブ上のすべてのデータを消去せずにドライブ セキュリティを無効にすることはできません。

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と、ストレージアレイ内のセキュリティ対応ドライブとコントローラ間で共有されるセキュリティキーを作成できます。ドライブへの電源がオフオンされるたびに、セキュリティ対応ドライブは、コントローラがセキュリティキーを適用するまで、セキュリティロック状態になります。

セキュリティが有効になっているドライブをストレージアレイから取り外し、別のストレージアレイに再インストールすると、そのドライブはセキュリティロック状態になります。移動されたドライブは、データへのアクセスを再び可能にする前に、セキュリティキーを検索します。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取得したセキュリティキーを適用します。ロック解除処理が正常に完了すると、移動されたドライブはターゲットストレージアレイに既に保存されているセキュリティキーを使用するようになり、インポートされたセキュリティキーファイルは不要になります。

内部キー管理の場合、実際のセキュリティキーはコントローラ上のアクセス不可能な場所に保存されます。人間が読める形式ではなく、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

セキュリティ機能を備えた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、それら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オプションを使用すると、ドライブおよび関連するボリュームグループとプールがセキュリティ_有効_になります。

セキュリティ保護機能が有効になっているボリュームグループとプールを作成する前に、次のガイドラインに留意してください：

- ボリュームグループおよびボリュームプールは、すべてセキュリティ機能を備えたドライブで構成されなければなりません。（FIPS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てください。ボリュームグループまたはプール内でFIPSドライブとFDEドライブを混在させると、すべてのドライブがFDEドライブとして扱われます。また、FDEドライブは、FIPS準拠のボリュームグループまたはプールに追加したり、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である必要があります。

SANtricity System Managerにおけるセキュリティキー管理の仕組み

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 ロック状態となります。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。そのドライブを別のストレージ アレイに取り付けた場合、データに再びアクセスするにはセキュリティ キーが必要になります。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上での外部キー管理

内部キー管理

内部キーは、コントローラの永続メモリ上のアクセス不可能な場所に保持され、「`hidden`」されます。内部鍵管理を実装するには、以下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ドライブを取り付けます。対応するドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。
2. ドライブ セキュリティ機能が有効になっていることを確認します。ドライブ セキュリティ機能を有効にする手順については、必要に応じてストレージ ベンダーに問い合わせてください。
3. 内部セキュリティキーを作成するには、識別子とパスフレーズを定義する必要があります。識別子はセキュリティキーに関連付けられた文字列であり、コントローラおよびキーに関連付けられたすべてのドライブに保存されます。パスフレーズは、バックアップ目的で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、メニューの［Settings］→［System］→［Security key management］→［Create Internal Key］を選択してください。

セキュリティ キーが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。

1. ストレージ アレイにセキュリティ対応ドライブを取り付けます。対応するドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。
2. ドライブ セキュリティ機能が有効になっていることを確認します。ドライブ セキュリティ機能を有効にする手順については、必要に応じてストレージ ベンダーに問い合わせてください。
3. 署名済みのクライアント証明書ファイルを取得します。クライアント証明書は、キー管理サーバがコントローラのKMIP要求を信頼できるよう、ストレージ アレイのコントローラを検証します。
   a. まず、クライアント証明書署名要求（CSR）を作成してダウンロードします。メニュー：Settings[Certificates > Key Management > Complete CSR]に移動します。
   b. 次に、キー管理サーバで信頼されているCAに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してダウンロードすることもできます）。
   c. クライアント証明書ファイルを用意したら、そのファイルをSystem Managerにアクセスするホストにコピーします。
   d. 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。
4. キー管理サーバから証明書ファイルを取得し、そのファイルをSystem Managerにアクセスするホストにコピーします。キー管理サーバ証明書は、ストレージ アレイがサーバのIPアドレスを信頼できるよう、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。
5. 外部キーを作成するには、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ます。このプロセス中に、証明書ファイルも読み込まれます。外部キーを作成するには、メニューの［設定］→［システム］→［セキュリティ キー管理］→［外部キーの作成］を選択してください。

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。

SANtricityソフトウェアのドライブセキュリティ用語について学ぶ

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。

期間	概要
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際にセキュリティ キーが要求されるようになります。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、取り付けたあとも正しいセキュリティ キーが提供されないかぎりセキュリティ ロック状態になります。

期間	概要
FDEドライブ	フルディスク暗号化（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。ハードディスクには、書き込み時にデータを暗号化し、読み取り時にデータを復号化するASICチップが搭載されています。
FIPSドライブ	FIPSドライブは、連邦情報処理規格（FIPS）140-2レベル2を使用します。これらは基本的に、強力な暗号化アルゴリズムと方法を確保するための米国政府の基準に準拠したFDEドライブです。FIPSドライブは、FDEドライブよりも高いセキュリティ基準を満たしています。
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搭載したローカルシステム（コンピュータ、タブレットなど）。
パス フレーズ	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。 ドライブ セキュリティのパス フレーズは、ストレージ アレイの管理者パスワードとは別のものです。
セキュリティ対応ドライブ	セキュリティ機能を備えたドライブには、フルディスク暗号化（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあり、いずれも書き込み時にデータを暗号化し、読み取り時にデータを復号化します。これらのドライブは、ドライブセキュリティ機能を使用して追加のセキュリティ対策を講じることができるため、セキュリティ対応ドライブとみなされます。これらのドライブで使用されるボリュームグループおよびプールに対してドライブセキュリティ機能が有効になっている場合、ドライブはセキュア有効状態になります。
セキュリティ有効ドライブ	セキュリティ対応ドライブは、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てから、セキュア対応ドライブ上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、ドライブはセキュリティ対応になります。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を介してのみ可能です。この追加のセキュリティ対策により、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します。

期間	概要
セキュリティ キー	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 ロック状態となります。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。そのドライブを別のストレージ アレイに取り付けた場合、データに再びアクセスするにはセキュリティ キーが必要になります。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。
セキュリティ キー識別子	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。

セキュリティ キーの設定

SANtricity System Managerで内部セキュリティキーを作成します

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。

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。有効になっていない場合、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 ボックスが表示されます。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。

タスク概要

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。

ドライブ セキュリティのパス フレーズは、ストレージ アレイの管理者パスワードとは別のものです。

手順

1. メニュー：Settings[System]を選択します。

2. * Security key management * で、 * Create Internal Key * を選択します。

   セキュリティキーをまだ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。

3. 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します — 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るストレージアレイ名とタイムスタンプ）を受け入れるか、独自の値を入力することができます。スペース、句読点、記号を含めずに、最大189文字の英数字を入力できます。

     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する/パスフレーズを再入力する — パスフレーズを入力して確認します。値は8文字から32文字までで、以下のすべてを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ます。
     - 数字（1文字以上）。
     - 英数字以外の「!」、「*」、「@」などの文字（1文字以上）。

     後で使用するために、必ず入力内容を記録してください。セキュリティ保護が有効になっているドライブをストレージアレイから移動する必要がある場合は、ドライブのデータをロック解除するための識別子とパスフレーズを知っている必要があります。

4. *作成*をクリックします。

   セキュリティ キーが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。

   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応じて異なる場合があります。

5. キー識別子、パスフレーズ、およびダウンロードしたキーファイルの場所を記録してから、*閉じる*をクリックしてください。

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。

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作成した正しいセキュリティ キーがコントローラによって適用されないかぎりアクセスできません。第三者がロックされたドライブを物理的に取り外して別のシステムに取り付けた場合でも、データへの不正アクセスを防止することができます。

終了後の操作

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。

SANtricity System Managerで外部セキュリティキーを作成する

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、外部キーを作成し、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必要があります。

開始する前に

- アレイにセキュリティ対応ドライブが搭載されている必要があります。対応するドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。

  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。有効になっていない場合、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 ボックスが表示されます。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の署名済みクライアント証明書ファイルを用意し、そのファイルをSystem Managerにアクセスするホストにコピーしておきます。クライアント証明書は、キー管理サーバがコントローラの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。

  サーバ証明書の詳細については、キー管理サーバのドキュメントを参照してください。

タスク概要

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

1. メニュー：Settings[System]を選択します。
2. * Security key management で、 Create External Key *を選択します。

   現在内部キー管理が設定されている場合は、外部キー管理に切り替えるかどうか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。

3. *Connect to Key Server*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。キー管理サーバ通信で最も一般的に使用されるポート番号は5696です。

*オプション：*バックアップキーサーバを設定する場合は、*Add Key Server*をクリックし、そのサーバの情報を入力します。2つ目のキーサーバは、プライマリキーサーバに到達できない場合に使用されます。各キーサーバが同じキーのデータベースにアクセスできることを確認してください。そうでない場合、アレイはエラーを通知し、バックアップサーバを使用できません。

一度に使用されるキー サーバは1つだけです。プライマリ キー サーバにアクセスできない場合、ストレージ アレイはバックアップ キー サーバに接続します。両方のサーバが同等である必要があります。そうでない場合、エラーになる可能性があります。

- クライアント証明書の選択 — 最初の 参照 ボタンをクリックして、ストレージアレイのコントローラ用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。
- キー管理サーバーのサーバー証明書を選択します — 3番目の*参照*ボタンをクリックして、キー管理サーバーの証明書ファイルを選択します。キー管理サーバーには、ルート証明書、中間証明書、またはサーバー証明書のいずれかを選択できます。

4. **Next** をクリックします。
5. *Create/Backup Key*では、セキュリティ目的で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には、チェックボックスを選択したまま、パスフレーズを入力して確認します。値は8~32文字で、次の各項目を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ます。
     - 数字（1文字以上）。
     - 英数字以外の「!」、「*」、「@」などの文字（1文字以上）。

後で使用するために、必ず入力内容を記録してください。セキュリティ保護が有効になっているドライブをストレージアレイから移動する必要がある場合は、ドライブのデータをロック解除するためのパスフレーズを知っている必要があります。

+

   - バックアップキーを作成しない場合は、チェックボックスの選択を解除してください。

バックアップ キーがないと、外部キー サーバへのアクセスが失われた場合に、別のストレージ アレイに移行されたドライブ上のデータにはアクセスできなくなります。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。

6. *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。

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応じて異なる場合があります。

7. 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てから、*閉じる*をクリックしてください。

次のメッセージと外部キー管理に関連したリンクが表示されます。

```
Current key management method: External
```

8. *Test Communication*を選択して、ストレージアレイとキー管理サーバ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。

> 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作成した正しいセキュリティ キーがコントローラによって適用されないかぎりアクセスできません。第三者がロックされたドライブを物理的に取り外して別のシステムに取り付けた場合でも、データへの不正アクセスを防止することができます。

終了後の操作

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。

セキュリティ キーの管理

SANtricity System Managerでセキュリティキーを変更する

セキュリティ キーは、いつでも新しいキーに差し替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、ドライブの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 キーを変更する必要があります。

手順

1. メニュー：Settings[System]を選択します。
2. *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。

3. 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します --（内部セキュリティキーのみ）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るストレージアレイ名とタイムスタンプ）を受け入れるか、独自の値を入力してください。スペース、句読点、記号を含めずに、最大189文字の英数字を入力できます。

     > 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。

   - パスフレーズの定義/パスフレーズの再入力 — これらの各フィールドに、パスフレーズを入力します。値は8~32文字で、次の各項目を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ます。
     - 数字（1文字以上）。

- 英数字以外の「!」、「*」、「@」などの文字（1文字以上）。

4. 外部セキュリティ キーを新しく作成する際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[現在のセキュリティ キーを削除する]チェックボックスをオンにします。

> 後で使用するために、入力内容を必ず記録してください — セキュリティが有効になっているドライブをストレージアレイから移動する必要がある場合は、ドライブのデータのロックを解除するための識別子とパスフレーズを知っている必要があります。

5. **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。

> 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応じて異なる場合があります。

6. キー識別子、パスフレーズ、およびダウンロードしたキーファイルの場所を記録してから、*閉じる*をクリックしてください。

終了後の操作

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。

SANtricity System Managerで外部キー管理から内部キー管理に切り替える

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。

タスク概要

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

1. メニュー：Settings[System]を選択します。
2. *Security key management*で、*Disable External Key Management*を選択します。

   「外部キー管理を無効にする」ダイアログボックスが開きます。

3. *Define a pass phrase/Re-enter pass phrase*で、キーのバックアップ用のパスフレーズを入力し、確認します。値は8文字から32文字までで、以下のすべてを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ます。
   - 数字（1文字以上）。
   - 英数字以外の「!」、「*」、「@」などの文字（1文字以上）。

> 後で使用するために、必ず入力内容を記録してください。セキュリティ保護が有効になっているドライブをストレージ アレイから移動する必要がある場合は、ドライブのデータをロック解除するための識別子とパスフレーズを知っている必要があります。

4. **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。

5. キー識別子、パスフレーズ、およびダウンロードしたキーファイルの場所を記録してから、*閉じる*をクリックしてください。

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す。

終了後の操作

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。

SANtricity System Managerでキー管理サーバの設定を編集します

外部キー管理を設定済みの場合、キー管理サーバ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

1. メニュー：Settings[System]を選択します。
2. *セキュリティキー管理*で、*キー管理サーバー設定の表示/編集*を選択します。
3. 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：*別のキーサーバーを追加するには、*キーサーバーの追加*をクリックします。
4. *保存*をクリックします。

SANtricity System Managerでセキュリティキーをバックアップする

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。

タスク概要

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

1. メニュー：Settings[System]を選択します。
2. *Security key management*で*Back Up Key*を選択します。

   Back Up Security Keyダイアログボックスが開きます。

3. *Define a pass phrase/Re-enter pass phrase*フィールドに、このバックアップ用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。

   - アルファベットの大文字（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）

   後で使用するために、必ず入力内容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。

4. * Back Up * 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、その後*セキュリティキーのバックアップの確認/記録*ダイアログボックスが開きます。

   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。

5. パスフレーズを安全な場所に記録してから、*閉じる*をクリックしてください。

終了後の操作

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。

SANtricity System Managerでセキュリティキーを検証します

セキュリティ キーを検証して、セキュリティ キーが破損していないこと、およびパスフレーズが正しいことを確認できます。

タスク概要

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

1. メニュー：Settings[System]を選択します。
2. *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。

3. *Browse*をクリックし、キー ファイルを選択します（例： `drivesecurity.slk`）。
4. 選択したキー 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。

   有効なキーファイルとパスフレーズを選択すると、*検証*ボタンが有効になります。

5. *検証*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。

6. 結果に「セキュリティキーの検証に成功しました」と表示されたら、*閉じる*をクリックしてください。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指示に従ってください。

SANtricity System Managerで内部キー管理を使用する場合のドライブのロック解除

内部キー管理を設定したあとにセキュリティ有効ドライブをストレージ アレイ間で移動した場合、ドライブ上の暗号化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 キーを再度割り当てる必要があります。

開始する前に

- ソース アレイ（ドライブを取り外すアレイ）で、ボリューム グループをエクスポートし、ドライブを取り外します。ターゲット アレイにドライブを取り付けます。

> System Managerではエクスポート / インポート機能が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 グループの移行に関する詳細な手順は、 "NetAppのナレッジ ベース"に記載されています。System Managerで管理される新しいアレイ、または旧システムの場合は、それぞれの適切な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。有効になっていない場合、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 ボックスが表示されます。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されるブラウザを搭載したシステム）上にあります。ドライブを別のシステムで管理されているストレージアレイに移動する場合は、セキュリティキーファイルをその管理クライアントに移動する必要があります。

タスク概要

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た場合、正しいセキュリティ キーを指定するまでドライブは動作しません。

> コントローラーの永続メモリから内部キーを作成するか、キー管理サーバーから外部キーを作成するかのいずれかを選択できます。このトピックでは、_内部_キー管理を使用する場合のデータのロック解除について説明します。_外部_キー管理を使用した場合は、"外部キー管理を使用する場合のドライブのロック解除"を参照してください。コントローラーのアップグレードを実行してすべてのコントローラー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ドキュメンテーションセンターの"ドライブのロック解除"に記載されている別の手順に従う必要があります。

セキュリティ有効ドライブを別のアレイに取り付けると、そのアレイでドライブが検出され、「要対応」状態となって「セキュリティ キーが必要です」というステータスが表示されます。ドライブ データのロックを解除するには、セキュリティ キー ファイルを選択し、キーのパス フレーズを入力します（このパス フレーズはストレージ アレイの管理者パスワードとは異なります）。

新しいストレージアレイに他のセキュリティ対応ドライブがインストールされている場合、それらのドライブはインポートしようとしているものとは異なるセキュリティキーを使用する可能性があります。インポート処理中、古いセキュリティキーは、インストールするドライブのデータをロック解除するためだけに使用されます。ロック解除処理が成功すると、新しくインストールされたドライブは、ターゲットストレージアレイのセキュリティキーに合わせて再キー設定されます。

手順

1. メニュー：Settings[System]を選択します。
2. *Security key management*で、*Unlock Secure Drives*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。セキュリティキーが必要なドライブは、表に表示されます。

3. **Optional:** ドライブ番号にマウスカーソルを合わせると、ドライブの位置（シェルフ番号とベイ番号）が表示されます。
4. *Browse*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。

5. 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。

6. **Unlock** 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。

終了後の操作

デスティネーション アレイ（ドライブを新たに取り付けたアレイ）でボリューム グループをインポートできるようになりました。

> System Managerではエクスポート / インポート機能が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 グループの移行に関する詳細な手順は、 "NetAppのナレッジ ベース"に記載されています。

SANtricity System Managerで外部キー管理を使用する際にドライブのロックを解除します

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 キーを再度割り当てる必要があります。

開始する前に

- ソース アレイ（ドライブを取り外すアレイ）で、ボリューム グループをエクスポートし、ドライブを取り外します。ターゲット アレイにドライブを取り付けます。

> System Managerではエクスポート / インポート機能が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 グループの移行に関する詳細な手順は、 "NetAppのナレッジ ベース"に記載されています。System Managerで管理される新しいアレイ、または旧システムの場合は、それぞれの適切な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。有効になっていない場合、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 ボックスが表示されます。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把握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の署名済みクライアント証明書ファイルを用意し、そのファイルをSystem Managerにアクセスするホストにコピーしておきます。クライアント証明書は、キー管理サーバがコントローラの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。

> サーバ証明書の詳細については、キー管理サーバのドキュメントを参照してください。

タスク概要

外部キー管理を使用する場合、セキュリティ キーは、セキュリティ キーの保護を目的とする外部サーバに格納されます。セキュリティ キーは、読み取り / 書き込みアクセス用にコントローラとドライブで共有される文字列です。ドライブをアレイから物理的に取り外して別のドライブに取り付けた場合、正しいセキュリティ キーを指定するまでドライブは動作しません。

> コントローラの永続メモリから内部キーを作成するか、キー管理サーバから外部キーを作成できます。このトピックでは、_外部_キー管理を使用する場合のデータのロック解除について説明します。_内部_キー管理を使用した場合は、"内部キー管理を使用する場合のドライブのロック解除"を参照してください。コントローラのアップグレードを実行し、すべてのコントローラを最新のハードウェアに交換する場合は、EシリーズおよびSANtricityドキュメントセンターの"ドライブのロック解除"に記載されている別の手順に従う必要があります。

セキュリティ有効ドライブを別のアレイに取り付けると、そのアレイでドライブが検出され、「要対応」状態となって「セキュリティ キーが必要です」というステータスが表示されます。ドライブ データのロックを解除するには、セキュリティ キー ファイルをインポートし、キーのパス フレーズを入力します（このパス フレーズはストレージ アレイの管理者パスワードとは異なります）。その際に、外部キー管理サーバを使用するようにストレージ アレイを設定すると、セキュリティ キーにアクセスできるようになります。ストレージ アレイが接続してセキュリティ キーを取得できるように、サーバの接続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他のセキュリティ対応ドライブがインストールされている場合、それらのドライブはインポートしようとしているものとは異なるセキュリティキーを使用する可能性があります。インポート処理中、古いセキュリティキーは、インストールするドライブのデータをロック解除するためだけに使用されま

す。ロック解除処理が成功すると、新しくインストールされたドライブは、ターゲットストレージアレイのセキュリティキーに合わせて再キー設定されます。

手順

1. メニュー：Settings[System]を選択します。
2. * Security key management で、 Create External Key *を選択します。
3. ウィザードの手順に従って、接続情報と証明書を入力します。
4. *Test Communication*をクリックして、外部キー管理サーバーへのアクセスを確認します。
5. *Unlock Secure Drives*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。セキュリティキーが必要なドライブは、表に表示されます。

6. **Optional:** ドライブ番号にマウスカーソルを合わせると、ドライブの位置（シェルフ番号とベイ番号）が表示されます。
7. *Browse*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。

8. 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。

9. **Unlock** 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。

終了後の操作

デスティネーション アレイ（ドライブを新たに取り付けたアレイ）でボリューム グループをインポートできるようになりました。

> System Managerではエクスポート / インポート機能が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 グループの移行に関する詳細な手順は、 "NetAppのナレッジ ベース"に記載されています。

SANtricity System Managerのストレージドライブセキュリティに関するFAQ

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

セキュリティ キーを作成するときは、どのような点に注意する必要がありますか**?**

セキュリティ キーは、ストレージ アレイ内のコントローラとセキュリティ有効ドライブによって共有されます。セキュリティ有効ドライブがストレージ アレイから削除されると、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上での外部キー管理

内部キー管理

内部キーは、コントローラの永続メモリ上のアクセス不可能な場所に保持され、「hidden」されます。内部セキュリティキーを作成する前に、以下の手順を実行する必要があります：

1. ストレージ アレイにセキュリティ対応ドライブを取り付けます。対応するドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。
2. ドライブ セキュリティ機能が有効になっていることを確認します。ドライブ セキュリティ機能を有効にする手順については、必要に応じてストレージ ベンダーに問い合わせてください。

識別子とパス フレーズを定義して、内部セキュリティ キーを作成します。識別子は、セキュリティ キーに関連付けられる文字列で、コントローラとキーに関連付けられたすべてのドライブに格納されます。パス フレーズは、バックアップ用にセキュリティ キーを暗号化するために使用されます。作成したセキュリティ キーは、コントローラ上のアクセスできない場所に格納されます。これで、セキュリティ有効のボリューム グループまたはプールを作成したり、既存のボリューム グループまたはプールでセキュリティを有効にしたりできます。

外部キー管理

外部キーは、Key Management Interoperability Protocol（KMIP）を使用して別のキー管理サーバに保持されます。外部セキュリティ キーを作成する前に、以下を実行する必要があります。

1. ストレージ アレイにセキュリティ対応ドライブを取り付けます。対応するドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。
2. ドライブ セキュリティ機能が有効になっていることを確認します。ドライブ セキュリティ機能を有効にする手順については、必要に応じてストレージ ベンダーに問い合わせてください。
3. 署名済みのクライアント証明書ファイルを取得します。クライアント証明書は、キー管理サーバがコントローラのKMIP要求を信頼できるよう、ストレージ アレイのコントローラを検証します。
   a. まず、クライアント証明書署名要求（CSR）を作成してダウンロードします。メニュー：Settings[Certificates > Key Management > Complete CSR]に移動します。
   b. 次に、キー管理サーバで信頼されているCAに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してダウンロードすることもできます）。
   c. クライアント証明書ファイルを用意したら、そのファイルをSystem Managerにアクセスするホストにコピーします。
4. キー管理サーバから証明書ファイルを取得し、そのファイルをSystem Managerにアクセスするホストにコピーします。キー管理サーバ証明書は、ストレージ アレイがサーバのIPアドレスを信頼できるよう、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、証明書ファイルもロードします。外部キーの作成が完了すると、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。

パス フレーズを定義する必要があるのはなぜですか?

パス フレーズは、ローカルの管理クライアントに保存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 アレイに再配置された場合、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。

セキュリティ キーの情報を記録しておく必要があるのはなぜですか?

セキュリティ キー情報を紛失し、バックアップがない場合、セキュリティ有効ドライブの移動時または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。

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?

バックアップを作成していない状況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いてください。

> ⓘ 識別子を使用するのは内部キーのみです。識別子の作成時には、追加の文字が自動的に生成され、識別子の文字列の先頭と末尾に追加されます。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。

> ⓘ 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応じて異なる場合があります。セキュリティ キーの情報を格納した場所を記録しておいてください。

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?

セキュリティ有効ドライブのデータをロック解除するには、ドライブのセキュリティ キーをインポートする必要があります。

セキュリティ有効ドライブのロックを解除する際は、次のガイドラインに注意してください。

- ストレージ アレイにすでにセキュリティ キーがあることが必要です。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IDおよびセキュリティ 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。
- 管理クライアント（ブラウザからSystem Managerにアクセスするシステム）にセキュリティ キー ファイルを用意しておく必要があります。
- 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、ドライブを物理的に取り外し、ドライブのラベルに記載されているPSID文字列（最大32文字）を探す必要があります。操作を開始する前に、ドライブが再インストールされていることを確認してください。

読み取り / 書き込みアクセスとは何ですか?

[ドライブ設定]ウィンドウには、ドライブ セキュリティ属性に関する情報が表示されます。「読み取り / 書き込みアクセス」はドライブのデータがロックされているときに表示される属性です。

ドライブの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*をクリックしてから、*その他の設定を表示*をクリックします。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、ドライブのロックが解除されている場合は*はい*となります。ドライブがロックされている場合、読み取り / 書き込みアクセス可能属性の値は*いいえ、無効なセキュリティキー*となります。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：Settings[System > Unlock Secure Drives]に移動します）。

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?

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、次の操作を行います。

- 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（ある場合）を選択して検証をやり直してください。
- 前述の手順を実行してもセキュリティ 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。

内部セキュリティ キー管理と外部セキュリティ キー管理の違いは何ですか?

ドライブ セキュリティ機能を実装している場合は、内部セキュリティ キーまたは外部セキュリティ キーを使用して、セキュリティ有効ドライブがストレージ アレイから取り外されたときにデータをロックダウンすることができます。

セキュリティ キーは、ストレージ アレイのセキュリティ有効ドライブとコントローラで共有される文字列です。内部キーは、コントローラの永続的メモリに保持されます。外部キーは、Key Management Interoperability Protocol（KMIP）を使用して別のキー管理サーバに保持されます。

アクセス管理

SANtricity System Managerのアクセス管理について学ぶ

アクセス管理は、SANtricity System Managerでユーザ認証を確立する方法です。

使用可能な認証方式にはどのようなものがありますか**?**

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/**ローカルユーザロール — 認証は、ストレージアレイで適用されるRBAC機能によって管理されます。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 — 認証は、LDAP（Lightweight Directory Access Protocol）サーバと、MicrosoftのActive Directoryなどのディレクトリサービスを介して管理されます。
- **SAML** — 認証は、SAML 2.0 を使用する ID プロバイダー（IdP）を介して管理されます。

詳細については、以下を参照してください。

- "アクセス管理の仕組み"
- "アクセス管理の用語"
- "マッピングされたロールの権限"
- "ローカル ユーザ ロール"
- "ディレクトリ サービス"
- "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機能の実装であるローカルユーザロールを使用するように事前設定されています。別の方法を設定する場合は、メニューの［設定］［アクセス管理］に移動します。

詳細については、以下を参照してください。

- "LDAPディレクトリ サーバの追加"
- "SAMLの設定"

関連情報

アクセス管理に関連するタスクの詳細については、以下を参照してください。

- "パスワードの変更"
- "監査ログ アクティビティの表示"
- "監査ログ用のsyslogサーバの設定"

概念

SANtricity System Managerにおけるアクセス管理の仕組み

アクセス管理は、SANtricity System Managerでユーザ認証を確立する方法です。

設定およびユーザ認証は次のように行います。

1. 管理者は、Security Admin権限を含むユーザープロファイルを使用してSystem Managerにログインします。

   初回ログイン時のユーザー名 `admin`は自動的に表示されるため、変更できません。`admin`ユーザーはシステム内のすべての機能に完全にアクセスできます。

2. 管理者は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、RBAC（ロールベースのアクセス制御）機能の実装であるローカルユーザロールを使用するように事前設定されています。
3. 次の認証方式を1つ以上設定します。
   - ローカル ユーザ ロール — 認証は、ストレージ アレイで適用されるRBAC機能によって管理されます。ローカル ユーザ ロールには、事前に定義されたユーザ 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 ロールを認証の唯一の方法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、特別な設定は必要ありません。
   - ディレクトリ サービス — 認証は、LDAP（Lightweight Directory Access Protocol）サーバと、MicrosoftのActive Directoryなどのディレクトリ サービスを介して管理されます。管理者はLDAPサーバに接続し、LDAPユーザをストレージ アレイに組み込まれたローカル ユーザ ロールにマッピングします。
   - **SAML** — 認証は、Security Assertion Markup Language（SAML）2.0を使用するIdentity Provider（IdP）を介して管理されます。管理者は、IdPシステムとストレージアレイ間の通信を確立し、IdPユーザを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マッピングします。
4. 管理者は、System Managerへのログイン認証情報をユーザーに提供します。
5. 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。

   認証がSAMLとSSO（シングル サインオン）で管理されている場合、システムはSystem Managerのログインダイアログをスキップする可能性があります。

   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がユーザ アカウントと照合して認証されます。
   - 割り当てられたロールに基づいてユーザの権限が決定されます。
   - ユーザ インターフェイス内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で利用可能なタスク

タスクへのアクセスは、ユーザに割り当てられたロールによって決まります。ロールには以下のものが含まれます：

- * 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）へのフル読み取り / 書き込みアクセスは可能ですが、セキュリティ構成へのアクセスはできません。
- **Security admin** — Access Managementのセキュリティ設定、証明書管理、監査ログ管理へのアクセス、およびレガシー管理インターフェイス（SYMbol）のオン/オフを切り替える機能。
- サポート管理者 — 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、MELイベント、およびコントローラファームウェアの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へのアクセス権はありません。
- **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、セキュリティ構成へのアクセスはできません。

利用できないタスクは、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。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。*Copy Services*や*Add to Workload*などの機能のタブはグレー表示され、*View/Edit Settings*のみが使用可能になります。

Unified Managerと**Storage Manager**の制限事項

ストレージ アレイにSAMLが設定されている場合、ユーザはそのアレイのストレージをUnified Managerや従来のStorage Managerの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 アレイの名前変更
- コントローラ ファームウェアのアップグレード
- ストレージ アレイ構成のロード
- スクリプトの実行
- 未使用のセッションがタイムアウトした状態で、アクティブな操作を実行しようとした

SANtricity ソフトウェアのアクセス管理用語について学ぶ

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。

期間	概要
アクセス トークン	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設定されています。
Active Directory	Active Directory（AD）は、MicrosoftのWindowsドメイン ネットワーク用のLDAPを使用したディレクトリ サービスです。
バインド	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。

期間	概要
CA	認証局（CA）は、インターネット セキュリティに関するデジタル電子文書（証明書と呼ばれる）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。
Certificate	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あり、攻撃者がサイトになりすますことを防ぎます。証明書には、サイト所有者に関する情報と、この情報を認証（署名）する信頼できる組織の身元情報が含まれています。
IdP	IDプロバイダー（IdP）とは、ユーザーから認証情報を要求し、そのユーザーが正常に認証されたかどうかを判断するために使用される外部システムです。IdPは、多要素認証を提供するように構成でき、Active Directoryなどの任意のユーザーデータベースを利用できます。セキュリティチームは、IdPの維持管理を担当します。
LDAP	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。LDAPを使用して、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、ユーザを検証することができます。
RBAC	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。
SAML	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（パスワードと指紋など）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。
SP	サービスプロバイダー（SP）は、ユーザ認証とアクセスを制御するシステムです。アクセス管理がSAMLで構成されている場合、ストレージアレイは、IDプロバイダーに認証を要求するためのサービスプロバイダーとして機能します。
SSO	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。

SANtricity System Managerでマッピングされたロールの権限について説明します

ストレージアレイに適用されるRBAC（ロールベースアクセス制御）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ます。各ロールには、SANtricity System Managerでタスクにアクセスするための権限が含まれています。

ユーザープロファイルとマッピングされたロールは、System Managerのユーザーインターフェイスのメニュー：Settings[Access Management > Local User Roles]からアクセスできます。

各ロールは、次のタスクへのアクセスを提供します。

- * Storage admin * — ストレージオブジェクト（ボリュームやディスクプールなど）へのフル読み取り / 書き込みアクセスは可能ですが、セキュリティ構成へのアクセスはできません。
- **Security admin** — Access Managementのセキュリティ設定、証明書管理、監査ログ管理へのアクセス、およびレガシー管理インターフェイス（SYMbol）のオン/オフを切り替える機能。
- サポート管理者 — 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、MELイベント、およびコントローラファームウェアの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へのアクセス権はありません。
- **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、セキュリティ構成へのアクセスはできません。

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。

SANtricity System Managerでローカルユーザロールを使用したアクセス管理を設定する

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 ロールを使用するための手順は次のとおりです。

1. 管理者は、Security Admin権限を含むユーザープロファイルを使用してSystem Managerにログインします。

> ℹ `admin`ユーザには、システム内のすべての機能へのフルアクセス権があります。

2. ユーザ プロファイルを確認します。ユーザ プロファイルは事前に定義されており、変更できません。
3. 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。
4. 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。

- パスワードを変更する。
- パスワードの最小文字数を設定する。
- パスワードなしでログインできるようにユーザに許可する。

SANtricity System Managerでディレクトリサービスを使用したアクセス管理を設定する

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 サービスを使用している場合の設定は次のようになります。

1. 管理者は、Security Admin権限を含むユーザープロファイルを使用してSystem Managerにログインします。

> `admin`ユーザには、システム内のすべての機能へのフルアクセス権があります。

2. 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。
3. 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。
4. 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、変更することはできません。
5. 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。
6. 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で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 サーバを追加する。
- ディレクトリ サーバの設定を編集する。
- 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。

SANtricity System Managerで**SAML**を使用したアクセス管理を設定する

アクセス管理に関しては、管理者はアレイに組み込まれているSecurity Assertion Markup Language（SAML）2.0の機能を使用できます。

設定ワークフロー

SAML設定は次のように行います。

1. 管理者は、Security Admin権限を含むユーザープロファイルを使用してSystem Managerにログインします。

`admin`ユーザには、System Managerのすべての機能へのフルアクセス権があります。

2. 管理者は、アクセス管理の下にある **SAML** タブに移動します。
3. 管理者は、IDプロバイダー（IdP）との通信を設定します。IdPは、ユーザーから認証情報を要求し、ユーザーが正常に認証されたかどうかを判断するために使用される外部システムです。ストレージアレイとの通信を設定するには、管理者は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。
4. 管理者は、サービスプロバイダーと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認証を制御します。この場合、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として機能します。通信を設定するには、管理者は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。管理者は、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。

管理者は、IdPが認証時に名前IDを返す機能をサポートしていることを確認する必要もあります。

5. 管理者は、ストレージアレイのロールを、IdPで定義された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。
6. 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。

SAMLを有効にすると、ユーザインターフェイスから無効にすることはできませんし、IdP設定を編集することもできません。SAML設定を無効化または編集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。

7. System Managerから、管理者はストレージアレイのSAMLを有効にします。
8. 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

SAML を使用して認証を行う場合、管理者は次の管理タスクを実行できます：

- 新しいロール マッピングの変更または作成
- Service Providerファイルのエクスポート

アクセス制限

SAMLが有効な場合、ユーザはそのアレイのストレージをUnified Managerや従来のStorage Managerの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）
- 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
- 標準のREST APIエンドポイントを使用したログイン

SAMLが有効になっている場合の接続制限

以下のストレージアレイ機能は、SAMLが有効になっている場合、JSON Web Token認証との接続が制限されます。

- コマンドライン インターフェイス（CLI）
- HTTPベーシック認証REST APIクライアント

アクセストークンと **SANtricity** ソフトウェアについて学ぶ

アクセス トークンは、REST APIまたはコマンドライン インターフェイス（CLI）で使用可能な、ユーザ名とパスワードを使用しない認証方式です。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設定されています。

SAMLおよび**JSON**の**Web**トークン アクセス

SAMLが有効になっているシステムでは、デフォルトで従来のコマンドライン ツールへのアクセスが許可されません。MFAワークフローは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を必要とするため、 REST API と CLI は事実上動作しなくなります。そのため、System Managerでトークンを生成する必要があります。この場合、ユーザはMFA経由で認証される必要があります。

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、セキュリティの観点からSAMLが推奨されます。

トークンの作成と使用のワークフロー

1. System Managerでトークンを作成し、有効期限を指定します。
2. トークンの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、安全な場所に保存します。
3. 次の方法でトークンを使用します。
   - **REST API**：REST APIリクエストでトークンを使用するには、HTTPヘッダーをリクエストに追加します。例：
     `Authorization: Bearer <access-token-value>`
   - セキュア**CLI**：CLIでトークンを使用するには、コマンドラインに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：
     - コマンドライン上のトークン値： `-t access-token-value`
     - トークン値を含むファイルへのパス： `-T access-token-file`

詳細については、以下を参照してください。

- "アクセス トークンの作成"
- "アクセス トークンの編集"

- "アクセス トークンの取り消し"

ローカル ユーザ ロールの使用

SANtricity System Managerでローカルユーザーロールを表示する

「ローカルユーザーロール」タブでは、ユーザープロファイルと既定のロールのマッピングを表示できます。これらのマッピングは、ストレージアレイで適用されるRBAC（ロールベースアクセス制御）の一部です。

開始する前に

Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、アクセス管理の機能は表示されません。

タスク概要

ユーザ プロファイルとマッピングを変更することはできません。変更できるのはパスワードのみです。

手順

1. メニューの「設定」→「アクセス管理」を選択します。
2. *ローカルユーザーロール*タブを選択します。

   ユーザ プロファイルがテーブルに表示されます。

   - ルート管理者（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。このユーザープロファイルには、すべてのロールが含まれています。
   - ストレージ管理者（storage）-- すべてのストレージ プロビジョニングを管理する管理者。このユーザープロファイルには、Storage Admin、Support Admin、Monitorの役割が含まれています。
   - セキュリティ管理者（セキュリティ）-- セキュリティ設定を担当するユーザー。アクセス管理、証明書管理、およびセキュリティ対応ドライブ機能が含まれます。このユーザープロファイルには、Security AdminとMonitorという役割が含まれています。
   - サポート管理者（サポート）-- 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。このユーザ プロファイルには、サポート管理者とモニタの役割が含まれます。
   - **Monitor** (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。このユーザープロファイルには、Monitorロールのみが含まれています。

SANtricity System Managerでパスワードを変更する

アクセス管理でユーザ プロファイルごとにユーザ パスワードを変更できます。

開始する前に

- ローカル管理者としてログインする必要があります。これにはRoot管理者権限が含まれます。
- ローカル管理者のパスワードを確認しておきます。

タスク概要

パスワードを決める際は、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 パスワードは現在の最小文字数の設定（[設定の表示 / 編集]）以上にする必要があります。
- パスワードでは大文字と小文字が区別されます。
- パスワードの末尾のスペースは削除されません。設定時に末尾にスペースを含めた場合は、入力時に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、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。

> 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。さらに、パスワードを変更すると、ユーザーのアクティブなセッションが終了します。

手順

1. メニューの「設定」→「アクセス管理」を選択します。
2. *ローカルユーザーロール*タブを選択します。
3. 表からユーザを選択します。

   パスワード変更ボタンが有効になります。
4. *パスワードの変更*を選択します。

   パスワードの変更ダイアログボックスが開きます。
5. ローカル ユーザ パスワードの最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。
6. 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。

SANtricity System Managerでローカルユーザーのパスワード設定を変更します

ストレージ アレイで新規作成または更新されるローカル ユーザ パスワードの最低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。

開始する前に

ローカル管理者としてログインする必要があります。これにはRoot管理者権限が含まれます。

タスク概要

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、パスワードの最低文字数を設定しないでください。

手順

1. メニューの「設定」→「アクセス管理」を選択します。
2. *ローカルユーザーロール*タブを選択します。
3. *View/Edit Settings*ボタンを選択します。

   ローカル ユーザー パスワード設定ダイアログ ボックスが開きます。

4. 次のいずれかを実行します。
   - ローカルユーザー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ーのパスワードを少なくとも必要とする」チェックボックスのチェックを外します。
   - すべてのローカル ユーザ パスワードを対象にパスワードの最低文字数を設定するには、[Require all local user passwords to be at least]チェック ボックスをオンにし、スピン ボックスで最低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。
5. *保存*をクリックします。

ディレクトリ サービスの使用

SANtricity System ManagerでLDAPディレクトリサーバを追加する

アクセス管理用に認証を設定するために、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することができます。

開始する前に

- Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、アクセス管理の機能は表示されません。
- ユーザグループはディレクトリサービス内で定義する必要があります。
- LDAPサーバの認証情報（ドメイン名、サーバURL、および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を含む）が必要です。
- 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。

タスク概要

ディレクトリ サーバの追加は2段階のプロセスです。最初に、ドメイン名とURLを入力します。サーバでセキュアなプロトコルを使用していて、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。その後、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。

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。無効になると、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

1. メニューの「設定」→「アクセス管理」を選択します。
2. ディレクトリサービス タブから、*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の追加」ダイアログボックスが開きます。

3. サーバー設定タブで、LDAPサーバの資格情報を入力します。

フィールドの詳細

設定	概要
設定	ドメイン
LDAPサーバのドメイン名を入力します。複数のドメインを指定する場合は、ドメインをカンマ区切りのリストで入力します。ドメイン名は、ログイン（*username@domain*）で使用され、認証先のディレクトリサーバを指定します。	サーバ URL
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。	証明書のアップロード（オプション）
このフィールドは、上記の[サーバ URL]フィールドでLDAPSプロトコルを指定した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できる証明書または証明書チェーンです。	バインド アカウント（オプション）

設定	概要
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。	バインド パスワード（オプション）
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。	追加する前にサーバ接続をテストする
ストレージアレイが入力したLDAPサーバ設定と通信できることを確認する場合は、このチェックボックスを選択します。テストは、ダイアログボックスの下部にある*追加*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が選択されていて、テストが失敗した場合、設定は追加されません。エラーを解決するか、チェックボックスの選択を解除してテストをスキップし、設定を追加する必要があります。	権限設定

設定	概要
検索ベース DN	ユーザを検索するLDAPコンテキストを入力します。通常は `CN=Users, DC=cpoc, DC=local`の形式です。
ユーザ名属性	認証用のユーザIDにバインドされた属性を入力します。例えば：`sAMAccountName`
グループ属性	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。例えば：`memberOf, managedObjects`

4. **Role Mapping**タブをクリックします。
5. 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

設定	概要
マッピング	グループDN
マッピングするLDAPユーザーグループのグループ識別名（DN）を指定します。正規表現がサポートされています。次の特殊な正規表現文字が正規表現パターンの一部でない場合は、バックスラッシュ(`\`でエスケープする必要があります：\.[]{}()<>*+-=!?^$	
ロール	フィールドをクリックして、グループDNにマッピングするストレージアレイのロールを1つ選択します。このグループに含めるロールは、それぞれ個別に選択する必要があります。Monitorロールは、他のロールと組み合わせてSANtricity System Managerにログインするために必要です。マッピングされたロールには、以下の権限が含まれます： • * 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）へのフル読み取り / 書き込みアクセスは可能ですが、セキュリティ構成へのアクセスはできません。 • **Security admin** — Access Managementのセキュリティ設定、証明書管理、監査ログ管理へのアクセス、およびレガシー管理インターフェイス（SYMbol）のオン/オフを切り替える機能。 • サポート管理者 — 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、MELイベント、およびコントローラファームウェアの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へのアクセス権はありません。 • **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、セキュリティ構成へのアクセスはできません。

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。

6. 必要に応じて、*別のマッピングを追加*をクリックして、グループと役割のマッピングをさらに入力してください。
7. マッピングが完了したら、*Add*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。

SANtricity System Managerでディレクトリサーバの設定とロールマッピングを編集します

アクセス管理でディレクトリ サーバを設定済みの場合、その設定をいつでも変更することができます。設定には、サーバ接続情報とグループとロールのマッピングが含まれます。

開始する前に

- Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、アクセス管理の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

1. メニューの「設定」→「アクセス管理」を選択します。
2. *Directory Services*タブを選択します。
3. 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。
4. *View/Edit Settings*を選択します。

   ディレクトリサーバ設定ダイアログボックスが開きます。
5. 「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

設定	概要
設定	ドメイン
LDAPサーバのドメイン名。複数のドメインを指定する場合は、ドメインをカンマ区切りで入力してください。ドメイン名は、ログイン時（*username @domain*）に使用され、認証を行うディレクトリサーバを指定するために使用されます。	サーバ URL
LDAPサーバにアクセスするためのURLの形式は `ldap[s]://host:port`です。	バインド アカウント（オプション）
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。	バインド パスワード（オプション）
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）。	保存する前にサーバ接続をテストする

設定	概要
ストレージアレイがLDAPサーバ構成と通信できることを確認します。テストは、ダイアログボックスの下部にある*保存*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が選択されていて、テストが失敗した場合、設定は変更されません。エラーを解決するか、チェックボックスの選択を解除してテストをスキップし、設定を再編集する必要があります。	権限設定
検索ベース DN	ユーザーを検索するためのLDAPコンテキストは、通常、次の形式で提供されます `CN=Users, DC=cpoc, DC=local`。
ユーザ名属性	認証用のユーザIDにバインドされた属性。例えば： `sAMAccountName`
グループ属性	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。例えば： `memberOf, managedObjects`

6. 「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

設定	概要
マッピング	グループDN
マッピングするLDAPユーザグループのドメイン名。正規表現がサポートされています。正規表現パターンの一部でない場合、これらの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：\.[]{}()<>*+-=!?^$	
ロール	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各ロールを個別に選択する必要があります。SANtricity System Managerにログインするには、Monitorロールを他のロールと組み合わせて使用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）へのフル読み取り / 書き込みアクセスは可能ですが、セキュリティ構成へのアクセスはできません。 • **Security admin** — Access Managementのセキュリティ設定、証明書管理、監査ログ管理へのアクセス、およびレガシー管理インターフェイス（SYMbol）のオン/オフを切り替える機能。 • サポート管理者 — 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、MELイベント、およびコントローラファームウェアの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へのアクセス権はありません。 • **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、セキュリティ構成へのアクセスはできません。

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。

7. 必要に応じて、*別のマッピングを追加*をクリックして、グループと役割のマッピングをさらに入力してください。
8. *保存*をクリックします。

結果

このタスクが完了すると、アクティブなユーザーセッションはすべて終了します。現在のユーザーセッションのみが保持されます。

SANtricity System Managerでディレクトリサーバを削除

ディレクトリ サーバとストレージ アレイの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、新しいサーバの設定が完了して古いサーバを削除する場合などに実行します。

開始する前に

Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、アクセス管理の機能は表示されません。

タスク概要

このタスクが完了すると、アクティブなユーザーセッションはすべて終了します。現在のユーザーセッションのみが保持されます。

手順

1. メニューの「設定」→「アクセス管理」を選択します。
2. *Directory Services*タブを選択します。
3. 削除するディレクトリ サーバをリストから選択します。
4. *削除*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。
5. フィールドに `remove`と入力し、*削除*をクリックします。

   ディレクトリ サーバ設定、権限設定、ロール マッピングが削除されます。ユーザは、以降このサーバからのクレデンシャルを使用してログインすることはできません。

SAMLの使用

SANtricity System ManagerでSAMLを設定

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。認証を設定すると、アイデンティティ プロバイダとストレージ プロバイダの間の接続が確立されます。

開始する前に

- Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、アクセス管理の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メタデータファイルはIdPシステムからダウンロードされ、System Managerへのアクセスに使用され

るローカルシステム上で利用可能になります。

タスク概要

IDプロバイダー（IdP）とは、ユーザーから認証情報を要求し、そのユーザーが正常に認証されたかどうかを判断するために使用される外部システムです。IdPは、多要素認証を提供するように構成でき、Active Directoryなどの任意のユーザーデータベースを利用できます。セキュリティチームは、IDプロバイダー（IdP）の維持管理を担当します。サービスプロバイダー（SP）は、ユーザ認証とアクセスを制御するシステムです。アクセス管理がSAMLで構成されている場合、ストレージアレイは、IDプロバイダーに認証を要求するためのサービスプロバイダーとして機能します。IdPとストレージアレイ間の接続を確立するには、これら2つのエンティティ間でメタデータファイルを共有します。次に、IdPユーザーエンティティをストレージアレイの役割にマッピングします。最後に、SAMLを有効にする前に、接続とSSOログインのテストを行います。

- SAML およびDirectory Services *Directory Servicesが認証方法として設定されている場合にSAMLを有効にすると、System ManagerではSAMLがDirectory Servicesよりも優先されます。後でSAMLを無効にすると、Directory Servicesの設定は以前の設定に戻ります。

*編集と無効化*SAMLを有効にすると、ユーザインターフェイスから無効にすることはできませんし、IdPの設定を編集することもできません。SAML設定を無効化または編集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認証の設定プロセスは複数の手順で構成されます。

ステップ**1**：**IdP**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接続情報を提供するには、IdPメタデータをSystem Managerにインポートします。IdPシステムは、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、このメタデータを必要とします。ストレージアレイには、コントローラが2つあっても、メタデータファイルは1つだけアップロードすれば十分です。

手順

1. メニューの「設定」→「アクセス管理」を選択します。
2. * SAML * タブを選択します。

   設定手順の概要が表示されます。

3. * Import Identity Provider（IdP）file *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。

4. * 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。

5. *インポート*をクリックします。

ステップ**2**：**Service Provider**ファイルのエクスポート

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

1. * Export Service Provider files * リンクをクリックします。

   [サービス プロバイダ ファイルのエクスポート]ダイアログ ボックスが開きます。

2. *コントローラA*フィールドにコントローラのIPアドレスまたはDNS名を入力し、*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2つのコントローラが含まれている場合は、*コントローラB*フィールドで2つ目のコントローラについてこの手順を繰り返します。

   Export をクリックすると、Service Provider 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。ファイルの保存場所をメモしておいてください。

3. 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。

4. 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

ユーザにSystem Managerへの認証とアクセス権を付与するには、IdPのユーザ属性とグループメンバーシップをストレージアレイの事前定義されたロールにマッピングする必要があります。

開始する前に

- IdP管理者が、IdPシステムでユーザの属性とグループ メンバーシップを設定しておく必要があります。
- IdPメタデータファイルがSystem Managerにインポートされます。
- 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

1. **System Manager** ロールのマッピングについては、リンクをクリックしてください。

   ロールマッピングダイアログボックスが開きます。

2. 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

設定	概要
マッピング	ユーザ属性
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。	属性値
マッピングするグループの属性値を指定します。正規表現がサポートされています。正規表現パターンの一部でない場合は、次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：\.[]{}()<>*+-=!?^$	
ロール	フィールドをクリックして、属性にマッピングするストレージアレイのロールを1つ選択します。含めたい各ロールを個別に選択する必要があります。System Managerにログインするには、他のロールと組み合わせてMonitorロールが必要です。Security Adminロールは、少なくとも1つのグループに対しても必要です。 各ロールの権限は次のとおりです。 • * Storage admin * — ストレージオブジェクト（ボリュームやディスクプールなど）へのフル読み取り / 書き込みアクセスは可能ですが、セキュリティ構成へのアクセスはできません。 • **Security admin** — Access Managementのセキュリティ設定、証明書管理、監査ログ管理へのアクセス、およびレガシー管理インターフェイス（SYMbol）のオン/オフを切り替える機能。 • サポート管理者 — 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、MELイベント、およびコントローラファームウェアの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へのアクセス権はありません。 • **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、セキュリティ構成へのアクセスはできません。

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。

3. 必要に応じて、*別のマッピングを追加*をクリックして、グループと役割のマッピングをさらに入力してください。

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。

4. マッピングが完了したら、*保存*をクリックします。

ステップ**4**：**SSO**ログインのテスト

IdPシステムとストレージ アレイが通信できることを確認するために、必要に応じてSSOログインをテストできます。このテストは、SAMLを有効にする最後の手順でも実行します。

開始する前に

- IdPメタデータファイルがSystem Managerにインポートされます。
- 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

1. *Test SSO Login*リンクを選択します。

   SSOクレデンシャルの入力を求めるダイアログ ボックスが開きます。

2. 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中であることを示すダイアログ ボックスが開きます。

3. 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。

   テストに失敗した場合は、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。

ステップ**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。

開始する前に

- IdPメタデータファイルがSystem Managerにインポートされます。
- 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。

*編集と無効化*SAMLを有効にすると、ユーザインターフェイスから無効にすることはできませんし、IdPの設定を編集することもできません。SAML設定を無効化または編集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

1. **SAML** タブから、 **Enable SAML** リンクを選択します。

   [SAML の有効化の確認]ダイアログ ボックスが開きます。

2. 入力 `enable`し、*有効にする*をクリックします。
3. 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。

SANtricity System ManagerでSAMLロールマッピングを変更する

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。

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、アクセス管理の機能は表示されません。
- IdP管理者が、IdPシステムでユーザの属性とグループ 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

1. メニューの「設定」→「アクセス管理」を選択します。
2. * SAML * タブを選択します。
3. **Role Mapping** を選択します。

   ロールマッピングダイアログボックスが開きます。

4. 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。

   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、System Managerへのアクセス権を失います。

フィールドの詳細

設定	概要
マッピング	ユーザ属性
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。	属性値
マッピングするグループの属性値を指定します。	ロール

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。

5. 必要に応じて、*別のマッピングを追加*をクリックして、グループと役割のマッピングをさらに入力できます。
6. *保存*をクリックします。

結果

このタスクが完了すると、アクティブなユーザーセッションはすべて終了します。現在のユーザーセッションのみが保持されます。

SANtricity System ManagerでSAMLサービスプロバイダファイルをエクスポート

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。

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、アクセス管理の機能は表示されません。
- SAMLを設定して有効にします。

タスク概要

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

1. メニューの「設定」→「アクセス管理」を選択します。
2. * SAML * タブを選択します。

3. *エクスポート*を選択します。

   [サービス プロバイダ ファイルのエクスポート]ダイアログ ボックスが開きます。

4. 各コントローラーについて、*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てください。

   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ておいてください。

5. 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。

6. 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か、ファイル内のコントローラ情報を手動で入力できます。
7. 閉じる をクリックします。

アクセス トークンの使用

SANtricity System Managerでアクセストークンを作成する

アクセス トークンを作成して、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）で認証を行うことができます。

トークンにはパスワードがないため、慎重に管理する必要があります。

手順

1. メニューの「設定」→「アクセス管理」を選択します。
2. * Access Tokens * タブを選択します。
3. *View/Edit Access Token Settings*を選択します。ダイアログボックスで、*Enable access tokens*チェックボックスが選択されていることを確認します。*Save*をクリックしてダイアログボックスを閉じます。
4. **Create Access Token** を選択します。
5. 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。

   トークンの有効期限が切れると、ユーザの認証は失敗します。

6. * Create * をクリックします。
7. ダイアログ ボックスで、以下のいずれかを選択します。
   - トークンテキストをクリップボードに保存するには、 * コピー * をクリックします。
   - *ダウンロード*をクリックして、トークンテキストをファイルに保存します。

     トークンのテキストは必ず保存してください。ダイアログを閉じると、その後テキストを確認することはできません。

8. 閉じる をクリックします。
9. 次の方法でトークンを使用します。
   - **REST API**：REST APIリクエストでトークンを使用するには、HTTPヘッダーをリクエストに追加します。例：
     `Authorization: Bearer <access-token-value>`
   - セキュア**CLI**：CLIでトークンを使用するには、コマンドラインに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：
     - コマンドライン上のトークン値： `-t access-token-value`
     - トークン値を含むファイルへのパス： `-T access-token-file`

> ユーザ名、パスワード、またはトークンが指定されていない場合、アクセス トークン値をコマンドラインで入力するよう求められます。

SANtricity System Managerでアクセストークン設定を編集する

アクセス トークンの設定（有効期限や新しいトークンを作成する機能など）を編集できます。

手順

1. メニューの「設定」→「アクセス管理」を選択します。
2. * Access Tokens * タブを選択します。
3. * View/Edit Access Token Settings * を選択します。
4. このダイアログ ボックスでは、次のいずれかまたは両方のタスクを実行できます。
   - トークンの作成を有効または無効にする。
   - 既存のトークンの有効期限を変更する。

> *アクセストークンを有効にする*設定の選択を解除すると、トークンの作成とトークン認証の両方が防止されます。後でこの設定を再度有効にした場合、有効期限が切れていないトークンを再利用できます。既存のトークンをすべて永久に取り消す場合は、"アクセス トークンの取り消し"を参照してください。

5. *保存*をクリックします。

SANtricity System Managerでアクセストークンを取り消す

トークンが漏えいしたと判断した場合、またはアクセス トークンの署名と検証に使用する暗号化キーを手動でローテーションしたい場合は、すべてのアクセス トークンを取り消すことができます。

この操作は、トークンの署名に使用される鍵を再生成します。鍵がリセットされると、発行済みのトークンは_すべて_即座に無効になります。ストレージアレイはトークンを追跡しないため、個々のトークンを取り消すことはできません。

手順

1. メニューの「設定」→「アクセス管理」を選択します。
2. * Access Tokens * タブを選択します。
3. * すべてのアクセストークンを取り消す * を選択します。
4. ダイアログボックスで * はい * をクリックします。

すべてのトークンを取り消したら、新しいトークンを作成してすぐに使用できます。

syslogの管理

SANtricity System Managerで監査ログのアクティビティを表示する

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。

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、アクセス管理の機能は表示されません。

手順

1. メニューの「設定」→「アクセス管理」を選択します。
2. 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時刻のタイムスタンプ（GMT）。
   - ユーザー名 — イベントに関連付けられたユーザー名。ストレージ アレイに対する認証されていない操作については、ユーザー名として「N/A」が表示されます。認証されていない操作は、内部プロキシまたはその他のメカニズムによってトリガーされる可能性があります。
   - ステータスコード — 操作の HTTP ステータスコード（200、400 など）と、イベントに関連付けられた説明テキスト。
   - アクセスした**URL** — 完全なURL（ホストを含む）とクエリ文字列。
   - **Client IP Address** — イベントに関連付けられたクライアントのIPアドレス。
   - ソース — イベントに関連付けられたログソース。System Manager、CLI、Web Services、またはSupport Shellのいずれかになります。
   - 概要 — イベントに関する追加情報（該当する場合）。
3. [監査ログ]ページで選択した内容を使用して、イベントを表示および管理します。

選択項目の詳細

選択内容	概要
イベントを表示する期間を選択…	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、カスタムの日付範囲）で限定します。
フィルタ	フィールドに入力された文字によって表示されるイベントを制限します。完全一致の場合は引用符（""）を使用し、`OR`を入力して1つ以上の単語を返すか、ダッシュ（--）を入力して単語を省略します。
更新	最新のイベント情報にページを更新するには、*更新*を選択してください。
設定の表示 / 編集	*View/Edit Settings*を選択すると、ログポリシー全体とログに記録する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。
イベントの削除	*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。
列の表示 / 非表示	*表示/非表示*列アイコンをクリックして、テーブルに表示する追加の列を選択します。追加の列には次のものがあります： • メソッド — HTTPメソッド（例：POST、GET、DELETEなど）。 • **CLI Command Executed** — Secure CLIリクエストに対して実行された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 — SYMbol手順が実行されました。 • **SSH** イベントタイプ — ログイン、ログアウト、login_failなどのSecure Shell（SSH）イベントタイプ。 • **SSH Session PID** — SSHセッションのプロセスID番号。 • **SSH Session Duration(s)** — ユーザーがログインしていた秒数。 • 認証タイプ — タイプには、Local user、LDAP、SAML、およびAccess tokenが含まれます。 • **Authentication ID** — 認証されたセッションのID。
列フィルタを切り替え	**Toggle** アイコン をクリックして、各列のフィルタリングフィールドを開きます。列フィールドに文字を入力すると、その文字によって表示されるイベントが制限されます。フィルタリングフィールドを閉じるには、もう一度アイコンをクリックします。
元に戻す変更	*元に戻す*アイコンをクリックして、テーブルをデフォルト設定に戻します。

選択内容	概要
エクスポート	*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。

SANtricity System Managerで監査ログポリシーを定義する

上書きポリシーや監査ログに記録するイベントのタイプを変更することができます。

開始する前に

Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、アクセス管理の機能は表示されません。

タスク概要

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と記録するイベント タイプに関するポリシーを変更できます。

手順

1. メニューの「設定」→「アクセス管理」を選択します。
2. * Audit Log * タブを選択します。
3. *View/Edit Settings*を選択します。

   監査ログ設定ダイアログボックスが開きます。

4. 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

設定	概要
上書きポリシー	最大容量に達したときに古いイベントを上書きする場合のポリシーを指定します。 • 監査ログがいっぱいになったときに、監査ログ内の最も古いイベントを上書きすることを許可する — 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。 • 監査ログイベントを手動で削除する必要がある — イベントが自動的に削除されないことを指定します。代わりに、設定された割合に達するとしきい値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。 上書きポリシーが無効になっており、監査ログのエントリが最大制限に達した場合、Security Admin権限を持たないユーザーはSystem Managerへのアクセスを拒否されます。Security Admin権限を持たないユーザーにシステムアクセスを復元するには、Security Adminロールが割り当てられたユーザーが古いイベントレコードを削除する必要があります。 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。
ログに記録する操作のレベル	記録するイベントのタイプを指定します。 • レコード変更イベントのみ — ユーザー操作によってシステムに変更が加えられたイベントのみを表示します。 • すべての変更および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含むユーザー操作など、すべてのイベントを表示します。

5. *保存*をクリックします。

SANtricity System Managerの監査ログからイベントを削除します

監査ログの古いイベントをクリアすることができます。これにより、イベントの検索が容易になります。削除時に古いイベントをCSV（カンマ区切り値）ファイルに保存することもできます。

開始する前に

Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、アクセス管理の機能は表示されません。

手順

1. メニューの「設定」→「アクセス管理」を選択します。
2. * Audit Log * タブを選択します。
3. *Delete*を選択します。

   監査ログの削除ダイアログボックスが開きます。

4. 削除する古いイベントの数を選択または入力します。
5. 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（推奨）、チェックボックスをオンにしたままにしてください。次のステップで*削除*をクリックすると、ファイル名と保存場所を入力するよう求められます。それ以外の場合、イベントをCSVファイルに保存したくない場合は、チェックボックスをクリックして選択を解除してください。
6. *削除*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。

7. フィールドに `delete`と入力し、*削除*をクリックします。

   [監査ログ]ページから古いイベントが削除されます。

SANtricity System Managerで監査ログ用の**syslog**サーバーを設定する

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、以降は監査ログが自動的にsyslogサーバに保存されます。

開始する前に

- Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、アクセス管理の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れます。

手順

1. メニューの「設定」→「アクセス管理」を選択します。
2. 「監査ログ」タブから * syslogサーバの設定 * を選択します。

   [syslogサーバの設定]ダイアログ ボックスが開きます。

3. *[追加]*をクリックします。

   [syslogサーバの追加]ダイアログ ボックスが開きます。

4. サーバの情報を入力し、*追加*をクリックします。
   - 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。

- プロトコル — ドロップダウンリストからプロトコルを選択します（例：TLS、UDP、TCP）。
- 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、署名済みの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てください。監査ログは、信頼できる証明書のないsyslogサーバにはアーカイブされません。

> ⓘ 証明書が後から無効になった場合、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、メッセージはsyslogサーバに送信されなくなります。この問題を解決するには、syslogサーバ上の証明書を修正してから、メニュー：Settings[Audit Log > Configure Syslog Servers > Test All]に移動する必要があります。

- ポート — syslog受信機のポート番号を入力してください。*追加*をクリックすると、syslogサーバの設定ダイアログボックスが開き、設定済みのsyslogサーバがページに表示されます。

5. 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

設定後、すべての新しい監査ログはsyslogサーバに送信されます。以前のログは転送されません。アラートのsyslog設定をさらに設定するには、 "アラート用のsyslogサーバの設定"を参照してください。

```
NOTE: If multiple syslog servers are configured, all configured syslog
servers will receive an audit log.
```

SANtricity System Managerで監査ログレコードの**syslog**サーバー設定を編集する

監査ログのアーカイブに使用するsyslogサーバの設定を変更できます。サーバ用の新しい認証局（CA）証明書をアップロードすることもできます。

開始する前に

- Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、アクセス管理の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 システムに証明書を用意しておく必要があります。

手順

1. メニューの「設定」→「アクセス管理」を選択します。
2. 「監査ログ」タブから * syslogサーバの設定 * 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。

3. サーバー情報を編集するには、サーバー名の右側にある 編集 （鉛筆）アイコンを選択し、以下のフィールドで必要な変更を行ってください：
   - 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。
   - プロトコル — ドロップダウンリストからプロトコルを選択します（例：TLS、UDP、TCP）。

◦ ポート — syslog受信機のポート番号を入力してください。

4. プロトコルを（UDPまたはTCPから）セキュアなTLSプロトコルに変更した場合は、*信頼できる証明書のインポート*をクリックしてCA証明書をアップロードしてください。
5. 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。過去のログは転送されません。

SANtricity System Managerのユーザアクセス管理に関するFAQ

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

ログインできない理由は何ですか?

SANtricity System Managerへのログイン時にエラーが発生した場合は、考えられる原因を確認してください。

System Managerへのログインエラーは、以下のいずれかの理由で発生する可能性があります。

- 入力したユーザ名またはパスワードが間違っている。
- 必要な権限がない。
- 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。この場合は、ローカル ユーザの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、ロックアウトされた。この場合は、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発生したため、監査ログがいっぱいになっている可能性があります。アクセス管理に移動し、監査ログから古いイベントを削除してください。
- SAML認証が有効化された。この場合は、ブラウザをリフレッシュしてからログインしてください。

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間違っている。
- ログインが複数回失敗したために、ロックアウトされた。この場合は、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中のクライアント接続が最大数に達している。この場合は、複数のユーザまたはクライアントが使用していないか確認してください。

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?

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する必要があります。

- ユーザグループはディレクトリサービス内で定義する必要があります。
- LDAPサーバの認証情報（ドメイン名、サーバURL、および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を含む）が必要です。

- 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。

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**?**

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）機能には以下のロールが含まれています。

- * 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）へのフル読み取り / 書き込みアクセスは可能ですが、セキュリティ構成へのアクセスはできません。
- **Security admin** — Access Managementのセキュリティ設定、証明書管理、監査ログ管理へのアクセス、およびレガシー管理インターフェイス（SYMbol）のオン/オフを切り替える機能。
- サポート管理者 — 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、MELイベント、およびコントローラファームウェアの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へのアクセス権はありません。
- **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、セキュリティ構成へのアクセスはできません。

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把握している。正規表現がサポートされています。次の特殊な正規表現文字は、正規表現パターンの一部でない場合、バックスラッシュ(`\`でエスケープする必要があります（：）

```
\.[]{}()<>*+-=!?^$|
```

- 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 アレイに搭載されたSecurity Assertion Markup Language（SAML）機能を使用する場合は、次のこと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把握しておきます。
- マッピング対象グループの属性値は分かっている。正規表現がサポートされています。これらの特殊な正規表現文字は、正規表現パターンの一部でない場合、バックスラッシュ(`\`でエスケープする必要があります：

```
\.[]{}()<>*+-=!?^$|
```

- 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。

この変更の影響を受ける外部管理ツールはどれですか**?**

SANtricity System Managerで管理インターフェイスの切り替えや認証方法としてのSAMLの使用など、特定の変更を行うと、一部の外部ツールや機能の使用が制限される場合があります。

管理インターフェイス

レガシー管理インターフェイス（SYMbol）と直接通信するツール（SANtricity SMI-Sプロバイダー やOnCommand Insight（OCI）など）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と動作しません。さらに、この設定が無効になっている場合、レガシーCLIコマンドを使用したり、ミラーリング操作を実行したりすることはできません。

詳細については、テクニカル サポートにお問い合わせください。

SAML認証

SAMLが有効な場合、次のクライアントはストレージ アレイのサービスとリソースにアクセスできません。

- Enterprise Management Window（EMW）
- コマンドライン インターフェイス（CLI）
- ソフトウェア開発キット（SDK）クライアント
- インバンド クライアント
- HTTPベーシック認証REST APIクライアント
- 標準のREST APIエンドポイントを使用したログイン

詳細については、テクニカル サポートにお問い合わせください。

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**?**

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、次の点を確認します。

- ネットワーク内にIDプロバイダー（IdP）が設定されています。IdPは、ユーザーから認証情報を要求し、ユーザーが正常に認証されたかどうかを判断するために使用される外部システムです。セキュリティチームは、IdPの維持管理を担当します。
- 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メタデータファイルはIdPシステムからダウンロードされ、System Managerへのアクセスに使用されるローカルシステム上で利用可能になります。
- 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きます。

- SAMLを有効にすると、ユーザインターフェイスから無効にすることは_できません_し、IdP設定を編集することもできません。SAML設定を無効化または編集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。最終設定手順でSAMLを有効にする前に、SSOログインのテストを行うことをお勧めします。（システムはSAMLを有効にする前にSSOログインテストも実行します。）
- 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たログイン

監査ログにはどのタイプのイベントが記録されますか**?**

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 — System Manager内で行われる、ストレージのプロビジョニングなど、システムに変更を加えるユーザ操作。
- 変更および読み取り専用イベント — システムの変更を伴うユーザ操作、およびボリューム割り当ての表示など、情報の表示またはダウンロードを伴うイベント。

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**?**

外部syslogサーバに監査ログを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 アドレス、プロトコル、ポート番号を確認しておいてください。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れます。

- 設定が完了すると、以降すべての監査ログがsyslogサーバに送信されるようになります。過去のログは転送されません。
- 上書きポリシー設定（*設定の表示/編集*から利用可能）は、syslogサーバ設定でログを管理する方法には影響しません。
- 監査ログは、RFC 5424のメッセージ形式に従います。

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**?**

syslogサーバにTLSプロトコルを設定している場合、何らかの理由で証明書が無効になるとサーバはメッセージを受信できなくなります。無効な証明書に関するエラー メッセージが監査ログに記録されます。

この問題を解決するには、まずsyslogサーバの証明書を修正する必要があります。有効な証明書チェーンが設定されたら、メニューの「設定」→「監査ログ」→「Syslogサーバの設定」→「すべてテスト」に進みます。

証明書

SANtricity System Managerの証明書について学ぶ

SANtricity 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、インターネット上での安全な通信のために、ウェブサイトやサーバー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す。証明書には2つのタイプがあります：_署名付き証明書_は認証局（CA）によって検証され、_自己署名証明書_は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ます。

詳細については、以下を参照してください。

- "証明書の仕組み"
- "証明書の用語"

署名済み証明書を設定するにはどうすればよいですか**?**

署名要求は、System Managerで生成することも、秘密鍵と公開鍵のペアを使用して外部で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を受け取ったら、System Managerを使用してインポートします。

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CA署名証明書の使用"
- "CA署名証明書を使用したキー管理サーバでの認証"

関連情報

証明書に関連するタスクの詳細については、以下を参照してください。

- "インポートされた証明書情報の表示"
- "証明書失効チェックの有効化"

概念

SANtricity System Managerにおける証明書の仕組み

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 ファイルであり、インターネット上のセキュアな通信を実現します。

証明書は、Web通信が暗号化された形式で、プライバシーが保護され、改ざんされることなく、指定されたサーバとクライアント間でのみ送信されることを保証します。System Managerを使用すると、ホスト管理システム上のブラウザ（クライアントとして機能）とストレージ システム内のコントローラ（サーバとして機能）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確認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実現することもできます。

> CA署名証明書ではセキュリティ保護が強化されますが（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、自己署名証明書の場合、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、証明書の発行日と有効期限、エンティティの有効なドメイン、およびアルファベットと数字で構成されるデジタル署名が含まれています。

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、サイトがセキュリティで保護されていないことを示す警告がブラウザに表示されます。

CAは、申請プロセス中にユーザ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。申請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 — 階層構造の最上位にはルート証明書があり、これには他の証明書に署名するために使用される秘密鍵が含まれています。ルートは、特定のCA組織を識別するものです。すべてのネットワーク機器で同じCAを使用する場合は、ルート証明書は1つだけで済みます。
- 中間 — ルートから分岐するのは中間証明書です。CAは、保護されたルート証明書とサーバ証明書の間の仲介役として機能する、1つまたは複数の中間証明書を発行します。
- サーバ — チェーンの最下層にはサーバ証明書があり、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。ストレージアレイ内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で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によって「`trusted`」されません。自己署名証明書のみを含むウェブサイトに接続しようとするたびに、ブラウザは警告メッセージを表示します。警告メッセージ内のリンクをクリックしてウェブサイトに進む必要があります。そうすることで、実質的に自己署名証明書を承認したことになります。

キー管理サーバに使用される証明書

ドライブ セキュリティ機能がある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。

SANtricityソフトウェアの証明書の用語について学ぶ

証明書管理に関連する用語を次に示します。

期間	概要
CA	認証局（CA）は、インターネット セキュリティに関するデジタル電子文書（証明書と呼ばれる）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。
CSR	証明書署名要求（CSR）は、申請者から認証局（CA）に送信されるメッセージです。CSRは、CAが証明書を発行するために必要な情報を検証します。
Certificate	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あり、攻撃者がサイトになりすますことを防ぎます。証明書には、サイト所有者に関する情報と、この情報を認証（署名）する信頼できる組織の身元情報が含まれています。
証明書チェーン	証明書にセキュリティ レイヤを追加するファイルの階層。通常、チェーンには1つのルート証明書（階層の最上位）、1つ以上の中間証明書、およびエンティティを識別するサーバ証明書が含まれています。
クライアント証明書	セキュリティキー管理においては、クライアント証明書によってストレージアレイのコントローラが検証され、キー管理サーバーはそれらのIPアドレスを信頼できるようになります。
中間証明書	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。
キー管理サーバ証明書	セキュリティキー管理においては、キー管理サーバ証明書によってサーバが検証されるため、ストレージアレイはそのIPアドレスを信頼できるようになります。

期間	概要
キーストア	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。これらの鍵と証明書によって、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。
OCSP サーバ	オンライン証明書ステータスプロトコル（OCSP）サーバーは、認証局（CA）が予定されている有効期限前に証明書を失効させたかどうかを判断し、証明書が失効している場合は、ユーザーがサーバーにアクセスすることをブロックします。
ルート証明書	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。
署名済み証明書	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。
自己署名証明書	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ています。自己署名証明書はCA署名証明書と同じ信頼チェーンを使用しないため、テスト環境で最もよく使用されます。「事前にインストールされている」証明書とも呼ばれます。
サーバ証明書	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。

証明書の使用

SANtricity System Managerでコントローラに **CA**署名付き証明書を使用する

コントローラーとSANtricity System Managerへのアクセスに使用するブラウザ間の安全な通信のために、CA署名付き証明書を取得できます。

開始する前に

- Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、証明書関連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名を把握しておく必要があります。

タスク概要

CA署名証明書を使用するには、次の3つの手順を実行します。

ステップ**1**：コントローラの**CSR**を完了する

最初にストレージ アレイの各コントローラの証明書署名要求（CSR）ファイルを生成する必要があります。

タスク概要

このタスクでは、System Managerで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名を提供します。このタスクでは、ストレージ アレイにコントローラが1つある場合はCSRファイルが1つ、コントローラが2つある場合は2つ生成されます。

> または、OpenSSLなどのツールを使用してCSRファイルを生成し、手順2：CSRファイルを送信するにスキップできます。

手順

1. メニュー：Settings[Certificates]を選択します。
2. 「アレイ管理」タブから*CSRを完了する*を選択します。

> 2番目のコントローラー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、*Accept Self-Signed Certificate*をクリックして続行してください。

3. 以下の情報を入力し、*次へ*をクリックします。
   - 組織名 — 貴社または貴団体の正式な法的名称。Inc. や Corp. などの接尾辞を含めます。
   - 組織単位（任意） — 証明書を取り扱う組織内の部門。
   - 都市/地域 — ストレージアレイまたは事業所が所在する都市。
   - 都道府県/地域（任意） — ストレージアレイまたは事業所が所在する都道府県または地域。
   - 国の**ISO**コード — USなど、あなたの国の2桁のISO（International Organization for Standardization）コード。

> 一部のフィールドには、コントローラーのIPアドレスなど、適切な情報があらかじめ入力されている場合があります。入力済みの値は、それが明らかに間違っていると確信できる場合を除き、変更しないでください。例えば、CSRをまだ完了していない場合、コントローラーのIPアドレスは「`localhost.`」に設定されています。この場合、「`localhost`」をコントローラーのDNS名またはIPアドレスに変更する必要があります。

4. ストレージアレイ内のコントローラAに関する以下の情報を確認または入力してください：
   - コントローラ**A**の共通名 — デフォルトでは、コントローラAのIPアドレスまたはDNS名が表示されます。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するアドレスと完全に一致している必要があります。DNS名はワイルドカードで始め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、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任意で入力できます。複数のエントリを入力する場合は、カンマ区切り形式を使用してください。
   - コントローラ**A**の代替**DNS**名 — 共通名がDNS名である場合、コントローラAの追加のDNS名を入力してください。複数のエントリを入力する場合は、カンマ区切り形式を使用してください。代替DNS名がない場合でも、最初のフィールドにDNS名を入力した場合は、その名前をここにコピーしてください。DNS名はワイルドカードで始め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つしかない場合は、*完了*ボタンが使用可能です。

ストレージアレイにコントローラが2つある場合、*Next*ボタンが使用可能になります。

> CSRリクエストを最初に作成する際は、*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、エラー回復時に提供されます。まれに、CSRリクエストが一方のコントローラでは失敗するが、もう一方のコントローラでは失敗しない場合があります。このリンクを使用すると、コントローラAでCSRリクエストが既に定義されている場合、その作成手順をスキップして、コントローラBでCSRリクエストを再作成する次のステップに進むことができます。

5. コントローラが1つしかない場合は、*完了*をクリックします。コントローラが2つある場合は、*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。

6. 手順2：CSRファイルを送信するへ移動。

手順2：CSRファイルを送信する

証明書署名要求（CSR）ファイルを作成したら、ファイルを認証局（CA）に送信します。Eシリーズ システムには、PEM形式（Base64 ASCIIエンコード）の署名済み証明書が必要です。該当するファイル形式はpem、.crt、.cer、または.keyです。

手順

1. ダウンロードしたCSRファイルの場所を確認します。
2. CSRファイルをCA（VerisignやDigiCertなど）に送信し、PEM形式の署名済み証明書を要求します。

> *CSRファイルをCAに送信した後は、別のCSRファイルを再生成しないでください。*CSRを生成するたびに、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存されます。署名済み証明書を受け取ってインポートすると、システムは秘密鍵と公開鍵の両方が元のペアであることを確認します。鍵が一致しない場合、署名済み証明書は機能しないため、CAに新しい証明書を要求する必要があります。

3. CAが署名済み証明書を返送したら、[手順3：コントローラ用の署名済み証明書をインポートする]に移動します。

手順3：コントローラ用の署名済み証明書をインポートする

認証局（CA）から署名済み証明書を受け取ったら、コントローラのファイルをインポートします。

開始する前に

- 署名済み証明書ファイルをCAから受け取っておきます。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ています。
- CAがチェーン証明書ファイル（.p7bファイルなど）を提供した場合は、チェーンファイルを個々のファイルに展開する必要があります。ルート証明書、1つ以上の中間証明書、およびコントローラを識別するサーバ証明書です。Windows `certmgr`ユーティリティ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：すべてのタスク[エクスポート]を選択）。Base-64エンコーディングを推奨します。エクスポートが完了すると、チェーン内の各証明書ファイルのCERファイルが表示されます。

- System Managerにアクセスするホスト システムに、証明書ファイルをコピーしておきます。

手順

1. メニュー：設定［証明書］を選択します
2. Array Managementタブから*Import*を選択します。

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

3. *参照*ボタンをクリックして、まずルート証明書ファイルと中間証明書ファイルを選択し、次にコントローラー用の各サーバー証明書を選択します。ルート証明書ファイルと中間証明書ファイルは、両方のコントローラーで同じです。サーバー証明書のみが、各コントローラーごとに固有です。外部ツールからCSRを生成した場合は、CSRとともに作成された秘密鍵ファイルもインポートする必要があります。

   ファイル名がダイアログ ボックスに表示されます。

4. *インポート*をクリックします。

   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、ログインし直す必要があります。再度ログインすると、新しいCA署名済み証明書がセッションに使用されます。

SANtricity System Managerで管理証明書をリセットします

コントローラの証明書をCA署名証明書から工場出荷時の自己署名証明書に戻すことができます。

開始する前に

- Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、証明書関連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。

タスク概要

リセット機能では、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

1. メニュー：Settings[Certificates]を選択します。
2. 「アレイ管理」タブから*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。

3. フィールドに `reset`と入力し、*リセット*をクリックします。

   ブラウザをリフレッシュしたあとに、サイトがHTTP Strict Transport Securityを使用しているという理由で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る場合があります。この状況は自己署名証明書に戻した場合に発生します。問題を解決するには、ブラウザから閲覧データを削除する必要があります。

結果

コントローラで自己署名証明書が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求められます。

SANtricity System Managerでインポートされた証明書情報を表示する

[証明書]ページでは、証明書のタイプ、発行元認証局、およびストレージ アレイの証明書の有効な日付範囲を表示できます。

開始する前に

Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、証明書関連の機能は表示されません。

手順

1. メニュー：Settings[Certificates]を選択します。
2. 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。

タブ	概要
アレイ管理	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。
信頼済み	コントローラー用にインポートされたその他のすべての種類の証明書に関する情報を表示します。*Show certificates that are…*の下にあるフィルターフィールドを使用して、ユーザーがインストールした証明書またはプリインストールされた証明書のいずれかを表示します。 • ユーザーインストール — 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。コントローラがクライアントとして動作する場合（サーバーではなく）の信頼された証明書、LDAPS証明書、およびIDフェデレーション証明書が含まれます。 • プリインストール済み — ストレージアレイに付属している自己署名証明書。
キー管理	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。

SANtricity System Managerでコントローラがクライアントとして動作する場合の証明書のインポート

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コントローラが接続を拒否する場合は、[信頼済み]タブから証明書をインポートして、コントローラ（クライアントとして機能）がそのサーバからの通信を受け入れるようにすることができます。

開始する前に

- Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、証明書関連の機能は表示されません。

- 証明書ファイルはローカルシステムにインストールされています。

タスク概要

別のサーバ（LDAPサーバや、TLSを使用するsyslogサーバなど）がコントローラにアクセス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しなければならない場合があります。

手順

1. メニュー：Settings[Certificates]を選択します。
2. 「信頼済み」タブから*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。

3. *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。

4. *インポート*をクリックします。

結果

ファイルがアップロードされて検証されます。

SANtricity System Managerで証明書失効チェックを有効にする

失効した証明書の自動チェックを有効にすると、Online Certificate Status Protocol（OCSP）サーバーが、ユーザーが安全でない接続を行うことをブロックします。

開始する前に

- Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、証明書関連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おり、これによりOCSPサーバに完全修飾ドメイン名を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利用できます。
- 独自のOCSPサーバーを指定する場合は、そのサーバーのURLを知っている必要があります。

タスク概要

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。

この作業では、OCSPサーバーを設定するか、証明書ファイルで指定されているサーバーを使用できます。OCSPサーバーは、認証局が予定されている有効期限前に証明書を失効させたかどうかを判断し、証明書が失効している場合は、ユーザーがサイトにアクセスすることをブロックします。

手順

1. メニュー：Settings[Certificates]を選択します。
2. *Trusted*タブを選択します。

   *鍵管理*タブから失効チェックを有効にすることもできます。

3. 通常とは異なるタスク 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。

4. *取り消しチェックを有効にする*を選択すると、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ます。
5. *OCSPレスポンダーアドレス*フィールドには、必要に応じてOCSPレスポンダーサーバーのURLを入力できます。アドレスを入力しない場合、システムは証明書ファイルに記載されているOCSPサーバーのURLを使用します。
6. *Test Address*をクリックして、システムが指定されたURLへの接続を開くことができることを確認してください。
7. *保存*をクリックします。

結果

ストレージ アレイが失効した証明書を持つサーバーに接続しようとした場合、接続は拒否され、イベントがログに記録されます。

SANtricity System Managerで信頼済み証明書を削除する

以前にインポートした、ユーザがインストールした証明書を[信頼済み]タブから削除できます。

開始する前に

- Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、証明書関連の機能は表示されません。
- 信頼済み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。

> コントローラおよび別のサーバ（LDAPサーバなど）の認証に使用していた証明書を、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。

タスク概要

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

1. メニュー：Settings[Certificates]を選択します。
2. *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。
3. 削除する証明書を表から選択します。
4. メニュー：Uncommon Tasks[Delete]をクリックします。

   [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。
5. フィールドに `delete`と入力し、*削除*をクリックします。

SANtricity System Managerでキー管理サーバーとの認証に**CA**署名付き証明書を使用

キー管理サーバとストレージ アレイ コントローラの間にセキュアな通信を確立するに

は、適切な証明書セットを設定する必要があります。

開始する前に

Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、証明書関連の機能は表示されません。

タスク概要

コントローラとキー管理サーバ間の通信は、次の2つの手順で認証されます。

ステップ**1**：**CSR**を記入し、キー管理サーバーに認証のために送信します

最初に証明書署名要求（CSR）ファイルを生成し、そのCSRを使用して、キー管理サーバが信頼する認証局（CA）に署名済みクライアント証明書を要求する必要があります。ダウンロードしたCSRファイルを使用して、キー管理サーバからクライアント証明書を作成してダウンロードすることもできます。クライアント証明書は、キー管理サーバがコントローラの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。

秘密鍵と公開鍵のペアを使用し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」ダイアログからインポートできます。外部で生成された CSR ファイルのインポートに関する詳細については、 "ステップ2：キー管理サーバー用の証明書をインポートする"を参照してください。

手順

1. メニュー：Settings[Certificates]を選択します。
2. 「キー管理」タブから*Complete CSR*を選択します。
3. 以下の情報を入力してください：
   - 共通名 — クライアントを識別する名前。共通名に含まれる内容を、KMSサーバーのクライアント証明書命名規則の要件に合わせることは一般的な慣行です。共通名は通常、ハンドシェイク中にクライアント証明書が提示された際に、KMSがクライアント証明書を識別するのに役立ちます。
   - 組織名 — 貴社または貴団体の正式な法的名称。Inc. や Corp. などの接尾辞を含めます。
   - 組織単位（任意） — 証明書を取り扱う組織内の部門。
   - **City/Locality** — 組織が所在する都市または地域。
   - **State/Region**（任意） — 組織が所在する州または地域。
   - 国別**ISO**コード — 組織が所在する国を表す、USなどの2桁のISO（International Organization for Standardization）コード。
4. *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。

5. キー管理サーバが信頼するCAに署名済みクライアント証明書を要求します。

   キー管理サーバは、独自のCAとして機能するために、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。

6. クライアント証明書をお持ちの場合は、[ステップ2：キー管理サーバー用の証明書をインポートする]にアクセスします。

ステップ**2**：キー管理サーバー用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の証明書をインポートします。証明書には2種類あります。クライアント証明書はストレージ アレイのコントローラを検証し、キー管理サーバ証明書はサーバを検証します。コントローラのクライアント証明書ファイルとキー管理サーバのサーバ証明書ファイルの両方をロードする必要があります。

開始する前に

- 署名済みのクライアント証明書ファイルがあります（ステップ1：CSRを記入し、キー管理サーバーに認証のために送信しますを参照）。また、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した。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するため、キー管理サーバはKey Management Interoperability Protocol（KMIP）要求を信頼できます。
- 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。

> 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

1. メニュー：Settings[Certificates]を選択します。
2. キー管理タブから * 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。
3. *クライアント証明書の選択*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。
4. 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、*秘密鍵ファイルを選択*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用の証明書ファイルを選択してください。

   ダイアログ ボックスにファイル名が表示されます。
5. *Select key management server’s server certificate*の横にある*Browse*ボタンをクリックして、キー管理サーバーのサーバー証明書ファイルを選択します。キー管理サーバーには、ルート証明書、中間証明書、またはサーバー証明書のいずれかを選択できます。

   ダイアログ ボックスにファイル名が表示されます。
6. *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。

SANtricity System Managerでキー管理サーバー証明書をエクスポート

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。

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、証明書関連の機能は表示されません。
- 証明書を事前にインポートしておく必要があります。

手順

1. メニュー：Settings[Certificates]を選択します。
2. **Key Management** タブを選択します。
3. 表からエクスポートする証明書を選択し、*エクスポート*をクリックします。

   [保存]ダイアログ ボックスが開きます。

4. ファイル名を入力して * 保存 * をクリックします。

CA署名証明書と自己署名証明書に関するよくある質問SANtricity System Manager

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

[もう一方のコントローラにアクセスできません**]**ダイアログ ボックスが表示されるのはなぜですか**?**

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 つのコントローラを備えたストレージ アレイ（デュプレックス構成）では、SANtricity System Manager が 2 番目のコントローラと通信できない場合、または操作中のある時点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、**Accept Self-Signed Certificate** をクリックして続行してください。別のダイアログボックスでパスワードの入力を求められた場合は、System Manager へのアクセスに使用する Administrator パスワードを入力してください。

このダイアログ ボックスが再び表示され、証明書関連の処理を完了できない場合は、次のいずれかの操作を試してください。

- 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。
- 2台目のコントローラにwithSystem Managerでアクセスし、自己署名証明書を承認した後、1台目のコントローラに戻って続行します。

外部キー管理のために**SANtricity System Manager**にアップロードする必要がある証明書をどのように確認できますか？

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、キー管理サーバがコントローラの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。

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、クライアント証明書を生成します。クライアント証明書を作成したら、そのファイルをSystem Managerにアクセスするホストにコピーします。

キー管理サーバ証明書は、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、そのファイルをSystem Managerにアクセスするホストにコピーします。

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**?**

SANtricity System Manager を使用すると、証明書失効リスト（CRL）をアップロードする代わりに、オンライン証明書ステータスプロトコル（OCSP）サーバーを使用して失効証明書を確認できます。

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、External Key Management Server（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が失効していないことを確認するために、証明書の検証を試みます。サーバは、その証明書に対して「good」、「revoked」、または「unknown」のいずれかの値を返します。証明書が失効している場合、またはアレイがOCSPサーバに接続できない場合は、接続が拒否されます。

> System Managerまたはコマンドラインインターフェイス（CLI）でOCSPレスポンダアドレスを指定すると、証明書ファイルに記載されているOCSPアドレスが上書きされます。

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**?**

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。

サポート

SANtricity System Managerでサポートを受ける

サポート ページからテクニカル サポートのリソースにアクセスできます。

どのようなサポート タスクを実行できますか**?**

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が可能です。

詳細については、以下を参照してください。

- "AutoSupport機能の概要"
- "イベント ログの概要"
- "アップグレード センターの概要"

テクニカル サポートに連絡するにはどうすればよいですか?

メイン ページから、**Support › Support Center › Support Resources tab**をクリックします。技術サポートの連絡先情報は、インターフェイスの右上に記載されています。

情報と診断の表示

SANtricity System Managerでストレージアレイのプロファイルを表示する

ストレージ アレイ プロファイルには、ストレージ アレイのすべてのコンポーネントとプロパティの説明が表示されます。

タスク概要

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たり、ストレージ アレイ プロファイルのハード コピーをストレージ アレイとともに保管したりすることもできます。構成を変更する場合は、ストレージ アレイ プロファイルの新しいコピーを作成してください。

手順

1. メニューの「サポート」→「サポートセンター」→「サポートリソース」タブを選択します。
2. **Launch detailed storage array information** までスクロールダウンし、 **Storage Array Profile** を選択します。

   画面にレポートが表示されます。

フィールドの詳細

セクション	概要
ストレージ アレイ	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。これらのオプションには、コントローラ / ドライブ シェルフ / ドライブ / ディスク プール / ボリューム グループ / ボリューム / ホットスペア ドライブの数、ドライブ シェルフ / ドライブ / ソリッド ステート ディスク（SSD） / ボリュームの許可される最大数、Snapshotグループ / Snapshotイメージ / Snapshotボリューム / 整合性グループの数、機能に関する情報、ファームウェア バージョンに関する情報、シャーシのシリアル番号に関する情報、AutoSupportのステータスとAutoSupportのスケジュールの情報、サポート データの自動収集とスケジュールされたサポート データ収集の設定、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が含まれます。
ストレージ	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 アレイの構成に応じて、[ストレージ]セクションには以下のサブセクションが表示される場合があります。 • **Disk Pools** — ストレージアレイ内のすべてのDisk Poolsの一覧を表示します。 • 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一覧を表示します。ボリュームと空き容量は、作成された順に記載されています。 • ボリューム — 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、ボリュームの状態、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、ドライブの種類、およびその他の詳細情報が含まれます。 • 欠落ボリューム — 現在欠落状態となっている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。記載されている情報には、各欠落ボリュームのWorld Wide Identifier（WWID）が含まれています。

セクション	概要
コピー サービス	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 アレイの構成に応じて、[コピー サービス]セクションには以下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、コピー数、コピーペア名、ステータス、開始タイムスタンプ、およびその他の詳細情報が含まれます。 • **Snapshot Groups** — 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一覧を表示します。 • * Snapshot イメージ * — ストレージアレイ内のすべての Snapshot のリストを表示します。 • * Snapshot Volumes * — 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。 • 整合性グループ — ストレージアレイ内のすべての整合性グループの一覧を表示します。 • メンバーボリューム — ストレージアレイ内のすべての整合性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 — ミラーリングされたすべてのボリュームのリストを表示します。 • **Reserved Capacity** — ストレージアレイ内のすべてのReserved Capacityボリュームのリストを表示します。
ホストの割り当て	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。そのほか、トポロジの定義やホスト タイプの定義も表示されます。

セクション	概要
ハードウェア	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 アレイの構成に応じて、[ハードウェア]セクションには以下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が表示され、コントローラの場所、ステータス、および構成が含まれます。また、ドライブチャネル情報、ホストチャネル情報、および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の順にリストされています。表示される情報には、各ドライブのシェルフID、ドロワーID、スロットID、ステータス、raw容量、メディアタイプ、インターフェイスタイプ、現在のデータレート、製品ID、およびファームウェアバージョンが含まれます。ドライブセクションには、ドライブチャネル情報、ホットスペアのカバー範囲情報、および摩耗寿命情報（SSDドライブのみ）も含まれています。摩耗寿命に関する情報には、使用済み耐久性の割合が含まれます。これは、SSDドライブにこれまでに書き込まれたデータ量を、ドライブの理論上の総書き込み制限量で割った値です。 • ドライブチャネル — ストレージアレイ内のすべてのドライブチャネルの情報を表示します。表示される情報には、チャネルの状態、リンクの状態（該当する場合）、ドライブ数、および累積エラー数が含まれます。 • シェルフ — 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。記載されている情報には、ドライブの種類、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含まれます。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、または入出力モジュール（IOM）キャニスタなどが含まれる場合があります。ストレージアレイでセキュリティキーが使用されている場合、ハードウェアセクションにはセキュリティキー識別子も表示されます。
機能	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 クラスタで許容される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]セクションの情報には、ドライブ セキュリティ（ストレージ アレイのセキュリティが有効か無効か）も含まれます。

3. ストレージアレイプロファイルを検索するには、*Find*テキストボックスに検索語を入力し、*Find*をクリックします。

   一致するすべての用語が強調表示されます。すべての結果を1つずつスクロールするには、*検索*をクリックし続けます。

4. ストレージアレイプロファイルを保存するには、*保存*をクリックします。

   ファイルは、ブラウザのダウンロードフォルダに次の名前で保存されます `storage-array-profile.txt`。

SANtricity System Managerでソフトウェアとファームウェアのインベントリを表示する

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。

タスク概要

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間には依存関係が存在します。ストレージ アレイ内のすべてのファームウェア バージョンに関する情報を取得するには、ソフトウェアとファームウェアのインベントリを表示します。テクニカル サポートでは、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

1. メニューの「サポート」→「サポートセンター」→「サポートリソース」タブを選択します。
2. *Launch detailed storage array information*までスクロールダウンし、*Software and Firmware Inventory*を選択します。

   ソフトウェアとファームウェアのインベントリ レポートが画面に表示されます。
3. 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。

   ファイルは、ブラウザのダウンロードフォルダにファイル名 `firmware-inventory.txt`で保存されます。
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。

診断データの収集

SANtricity System Managerでサポートデータを手動で収集します

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。

タスク概要

AutoSupport機能が有効になっている場合は、*AutoSupport*タブに移動して*AutoSupportディスパッチの送信*を選択することで、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. メニューの「Support」→「Support Center」→「Diagnostics」タブを選択します。
2. **Collect Support Data** を選択します。

3. *Collect*をクリックします。

   ファイルは、ブラウザのダウンロードフォルダに次の名前で保存されます `support-data.7z`。棚に引き出しがある場合、その棚の診断データは別の圧縮ファイルにアーカイブされます `tray-component-state-capture.7z`。

4. テクニカル サポートからの指示に従ってファイルを送信します。

SANtricity System Managerで構成データを収集します

ボリューム グループとディスク プールのすべてのデータを含むRAID構成データをコントローラから保存できます。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。

タスク概要

ここでは、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。データはコントローラのRPAメモリ上の場所から取得します。

> 構成データの収集機能は、 `save storageArray dbmDatabase`のCLIコマンドと同じ情報を保存します。

このタスクは、Recovery Guruの手順に記載されているかテクニカル 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. メニューの「Support」→「Support Center」→「Diagnostics」タブを選択します。
2. **Collect Configuration Data** 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、お使いのブラウザのダウンロードフォルダに保存されます。

4. テクニカル サポートへのファイルの送信とシステムへのデータの再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。

SANtricity System Managerでリカバリサポートファイルを取得する

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。SANtricity System Managerはこれらのファイルを自動的に保存します。

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。

タスク概要

リカバリ サポート ファイルには以下のタイプのファイルが含まれます。

- サポート データ ファイル

- AutoSupport履歴
- 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. メニューの「Support」→「Support Center」→「Diagnostics」タブを選択します。
2. **Retrieve Recovery Support Files** を選択します。

   ダイアログボックスには、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一覧表示されます。特定のファイルを検索するには、いずれかの列を並べ替えるか、*Filter*ボックスに文字を入力してください。

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。

SANtricity System Manager でトレース バッファを取得する

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。

タスク概要

ファームウェアでは、トレース バッファを使用して処理（特に例外的な状況）を記録します。これはデバッグに役立つ可能性があります。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、パフォーマンスに及ぼす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. メニューの「Support」→「Support Center」→「Diagnostics」タブを選択します。
2. * Retrieve Trace Buffers * 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ているコントローラのステータス メッセージが「失敗」または「無効」の場合、そのチェック ボックスは無効です。

4. *はい*をクリックします。

   ファイルは、ブラウザのダウンロードフォルダにファイル名 `trace-buffers.7z`で保存されます。

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。

SANtricity System Managerで入出力パス統計情報を収集する

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。

タスク概要

テクニカル サポートは、I/Oパスの統計情報をパフォーマンス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、メモリの利用率や、CPU利用率、ネットワーク遅延、I/Oレイテンシなどの問題が原因の可能性があります。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。あとで収集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。また、コントローラがリセット（リブート）した場合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. メニューの「Support」→「Support Center」→「Diagnostics」タブを選択します。
2. *I/Oパス統計情報を収集する*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、*Collect*をクリックします。

   ファイルは、ブラウザのダウンロードフォルダにファイル名 `io-path-statistics.7z`で保存されます。

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。

SANtricity System Managerで健全性イメージを取得

コントローラのヘルス イメージを確認できます。ヘルス イメージは、コントローラのプロセッサ メモリの生のデータ 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。

タスク概要

ファームウェアは、特定のエラーを検出すると、自動的にヘルスイメージを生成します。ヘルスイメージが生成されると、エラーが発生したコントローラが再起動し、イベントログにイベントが記録されます。

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. メニューの「Support」→「Support Center」→「Diagnostics」タブを選択します。
2. *Retrieve Health Image*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*をクリックします。

   ファイルは、ブラウザのダウンロードフォルダに次の名前で保存されます `health-image.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。

リカバリ操作の実行

SANtricity System Managerで読み取り不能セクターのログを表示する

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。

タスク概要

読み取り不能セクターのログには、リカバリ不可能なメディア エラーが報告されたドライブが原因で発生した読み取り不能セクターの詳細なレコードが含まれます。読み取り不能セクターは、通常のI/Oおよび変更処理（再構築など）の際に検出されます。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のエントリが1,000個に達すると、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。

これらの操作には、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。

データ損失の可能性 — 読み取り不能セクターからの復旧は、複数の異なる方法を用いる複雑な手順です。この操作は、技術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. メニューの「Support」→「Support Center」→「Diagnostics」タブを選択します。
2. * View/Clear Unreadable Sectors *を選択します。
3. 読み取り不能セクターのログを保存するには、次の手順を実行します。

   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、いずれかの列を並べ替えるか、*Filter*ボックスに文字を入力してください。

b. *保存*をクリックします。

ファイルは、ブラウザのダウンロードフォルダに次の名前で保存されます `unreadable-sectors.txt`。

4. テクニカル サポートから読み取り不能セクターのログを消去するよう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. *クリア*をクリックし、操作を実行することを確認します。

SANtricity System Managerでドライブポートを再度有効にする

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認識させることができます。

手順

1. メニューの「Support」→「Support Center」→「Diagnostics」タブを選択します。
2. *ドライブ ポートを再度有効にする*を選択し、操作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。

SANtricity ソフトウェアでリカバリ モードをクリア

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、正常運用に戻します。

開始する前に

- ストレージアレイを以前の構成に戻す場合は、リカバリモードをクリアする前にバックアップから構成をリストアする必要があります。
- リストアが正常に完了したことを確認するには、検証チェックを実行するか、テクニカルサポートに確認する必要があります。リストアが正常に完了したことを確認したら、リカバリ モードをクリアできます。

タスク概要

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 モードに切り替わります。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構成をリストアする。この作業を行う場合、テクニカル サポートに連絡する必要があります。
- 前回の構成データベース保存処理から構成をリストアする。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）から実行されます。
- 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場合があります。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. メニューの「Support」→「Support Center」→「Diagnostics」タブを選択します。
2. リカバリ モードのクリア を選択し、この操作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 モードのときにのみ表示されます。

AutoSupportの管理

EシリーズのAutoSupportについて学ぶ

AutoSupport機能は、ストレージアレイの健全性を監視し、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、事後対応としてAutoSupportデータを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、状態、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データにはユーザーデータは含まれていません。ディスパッチは即時送信することも、スケジュールに基づいて（毎日または毎週）送信することも可能です。

主なメリット

AutoSupport機能の主なメリットは次のとおりです。

- ケースの解決時間の短縮
- 高度な監視でインシデント管理を迅速化
- スケジュールに従った自動レポート作成と重大イベントに関する自動レポート作成
- 選択したコンポーネント（ドライブなど）のハードウェアの交換要求を自動化
- 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 サポートに転送
- 設定に関する既知の問題がないかどうか、AutoSupport分析ツールがディスパッチを監視

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。

- 基本**AutoSupport** — ストレージ アレイがデータを自動的に収集し、テクニカル サポートに送信できるようにします。
- **AutoSupport OnDemand** — 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。すべての送信は、AutoSupportサーバか

らではなく、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定期的にAutoSupportサーバと通信して、保留中の再送信要求があるかどうかを確認し、それに応じて応答します。

- 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、テクニカルサポートが最新のAutoSupportディスパッチを要求できるようにします。すべての送信は、AutoSupportサーバからではなく、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定期的にAutoSupportサーバと通信し、保留中の新しい要求があるかどうかを確認して、それに応じて応答します。

AutoSupportと[サポート データの収集]の違い

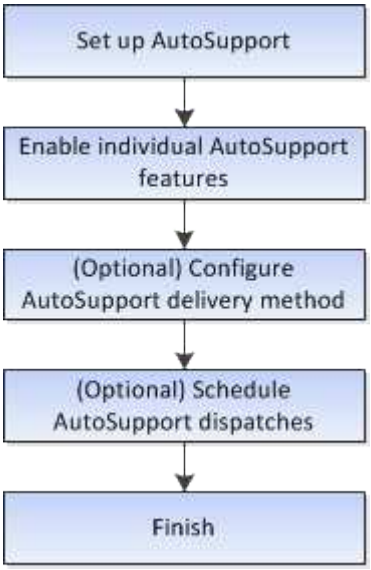
ストレージ アレイでは、次の2つの方法でサポート データを収集できます。

- **AutoSupport** 機能 — データは自動的に収集されます。
- サポートデータ収集オプション — データは手動で収集して送信する必要があります。

データが自動的に収集、送信されるAutoSupport機能の方が使いやすいです。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 サポートはデータへのアクセス権をすでに持っているため、AutoSupport機能を使用した方がトラブルシューティングを迅速に行うことができます。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。

SANtricity System ManagerでAutoSupportを設定する

SANtricity System Managerで、次の手順に従ってAutoSupport機能を設定します。



SANtricity System ManagerでAutoSupport機能を有効または無効にする

AutoSupport機能およびAutoSupportの個々の機能は、初期セットアップ時に設定するか、あとから有効または無効にすることができます。

開始する前に

AutoSupport OnDemandまたはRemote Diagnosticsを有効にする場合は、AutoSupportの配信方法をHTTPSに設定する必要があります。

タスク概要

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。

- 基本**AutoSupport** — ストレージ アレイがデータを自動的に収集し、テクニカル サポートに送信できるようにします。
- **AutoSupport OnDemand** — 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。すべての送信は、AutoSupportサーバからではなく、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定期的にAutoSupportサーバと通信して、保留中の再送信要求があるかどうかを確認し、それに応じて応答します。
- 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、テクニカルサポートが最新のAutoSupportディスパッチを要求できるようにします。すべての送信は、AutoSupportサーバからではなく、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定期的にAutoSupportサーバと通信し、保留中の新しい要求があるかどうかを確認して、それに応じて応答します。

手順

1. メニューを選択：サポート[サポートセンター > AutoSupport]タブ。
2. *Enable/Disable AutoSupport Features*を選択します。
3. 有効にするAutoSupport機能の横にあるチェック ボックスを選択します。

   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*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、通知を非表示にできます。

SANtricity System ManagerでAutoSupportの配信方法を設定する

AutoSupport機能は、ディスパッチをテクニカル サポートに配信するために、HTTPSおよびSMTPのプロトコルをサポートしています。

開始する前に

- AutoSupport機能が有効になっている必要があります。有効になっているかどうかは[AutoSupport]ページで確認できます。
- ネットワークにDNSサーバをインストールし、設定する必要があります。DNSサーバのアドレスがSystem Managerで設定されている必要があります（[ハードウェア]ページから設定できます）。

タスク概要

各プロトコルを確認します。

- **HTTPS** — HTTPSを使用して、宛先のテクニカルサポートサーバーに直接接続できます。AutoSupport OnDemandまたはリモート診断のいずれかを有効にする場合は、AutoSupport配信方法をHTTPSに設定する必要があります。
- **Email** — AutoSupportディスパッチの送信方法として、メールサーバーを使用できます。

HTTPSと電子メール方式の違い。SMTPを使用する電子メール配信方式は、HTTPS配信方式とはいくつかの重要な点で異なります。まず、電子メール方式での送信サイズは5MBに制限されているため、一部のASUPデータ収集データは送信されません。第二に、AutoSupport OnDemand機能はHTTPS配信方式でのみ利用可能です。

手順

1. メニューを選択：サポート[サポートセンター > AutoSupport]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、以下の配信パラメータのいずれかを選択してください：
     - 直接 — この配信パラメータはデフォルトの選択です。このオプションを選択すると、HTTPSプロトコルを使用して接続先のテクニカル サポート 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、宛先の技術サポートシステムへの接続を確立するために必要なHTTPプロキシ サーバの詳細情報を指定できます。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、ホスト認証情報（ユーザー名とパスワード）を入力する必要があるのは、必要な場合のみです。
     - プロキシ自動構成スクリプト（**PAC**）経由 — プロキシ自動構成（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、宛先の技術サポートシステムとの接続を確立するための適切なプロキシ サーバをシステムが自動的に選択できます。
   - [E 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 アドレス（完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレス）
     - AutoSupportディスパッチEメールの[差出人]フィールドに表示されるEメール アドレス
     - オプション。構成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メールアドレス。
     - メッセージを暗号化する場合は、暗号化の種類として*SMTPS*または*STARTTLS*を選択し、暗号化されたメッセージ用のポート番号を選択してください。それ以外の場合は、*なし*を選択してください。
     - 必要に応じて、送信者および送信元メール サーバの認証に使用するユーザ名とパスワードを入力します。
4. これらのASUPディスパッチの配信をブロックするファイアウォールを使用している場合は、次のURLをホワイトリストに追加してください： `https://support.netapp.com/put/AsupPut/`
5. *構成のテスト*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 サーバへの接続をテストします。AutoSupport On-Demand機能を有効にした場合、システムはAutoSupport OnDemandディスパッチ配信の接続もテストします。

   設定テストに失敗した場合は、設定を確認してから、再度テストを実行してください。テストが何度も失敗する場合は、テクニカル サポートにお問い合わせください。

6. *保存*をクリックします。

SANtricity System ManagerでAutoSupportの送信をスケジュールする

SANtricity System Managerは、AutoSupportディスパッチのデフォルトスケジュールを自動的に作成します。必要に応じて、独自のスケジュールを指定できます。

開始する前に

AutoSupport機能が有効になっている必要があります。有効になっているかどうかは[AutoSupport]ページで確認できます。

タスク概要

- 毎日の時刻 — 指定した時間範囲内に、毎日ディスパッチが収集され送信されます。System Managerは、その範囲内でランダムな時刻を選択します。すべての時刻は協定世界時（UTC）で表示されます。これは、ストレージアレイのローカル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時刻をUTCに変換する必要があります。
- 週ごとの配信 — 週ごとの配信は週に一度まとめて送信されます。System Managerは、指定した曜日の中からランダムに1日を選択します。週ごとの配信を許可しない曜日は、選択を解除してください。System Managerは、許可した曜日の中からランダムに1日を選択します。
- 週単位 — 週ごとの配信は、お客様が指定した期間内に週に一度収集され、送信されます。System Managerは、指定された範囲内でランダムな時刻を選択します。時刻はすべて協定世界時（UTC）であり、ストレージアレイの現地時間とは異なる場合があります。ストレージアレイのローカル時刻をUTCに変換する必要があります。

手順

1. メニューを選択：サポート[サポートセンター > AutoSupport]タブ。
2. *スケジュール AutoSupport ディスパッチ*を選択します。

   スケジュールAutoSupportディスパッチ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。

SANtricity System ManagerでAutoSupportディスパッチを送信

SANtricity System Managerを使用すると、スケジュールされたディスパッチを待たずに、AutoSupportディスパッチをテクニカルサポートに送信できます。

開始する前に

AutoSupport機能が有効になっている必要があります。有効になっているかどうかは[AutoSupport]ページで確認できます。

タスク概要

この処理では、サポート データが収集され、問題のトラブルシューティングのためにテクニカル サポートに自動的に送信されます。

手順

1. メニューを選択：サポート[サポートセンター > AutoSupport]タブ。
2. **Send AutoSupport Dispatch**を選択。

   [AutoSupport ディスパッチを送信]ダイアログ ボックスが表示されます。

3. *Send*を選択して操作を確定します。

SANtricity System ManagerでAutoSupportステータスを表示

[AutoSupport]ページには、AutoSupport機能および個々の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：サポート[サポートセンター > AutoSupport]タブ。
2. タブのすぐ下にあるページの右側を参照して、AutoSupportの基本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て、個々のAutoSupport機能が有効になっているかどうかを確認します。

SANtricity System ManagerでAutoSupportログを表示

AutoSupportログには、ステータス、ディスパッチの履歴、およびAutoSupportディスパッチの配信中に発生したエラーに関する情報が記録されます。

タスク概要

複数のログファイルが存在する可能性があります。現在のログファイルが200KBに達すると、アーカイブされ、新しいログファイルが作成されます。アーカイブされたログファイル名は `ASUPMessages.n`です。ここで、_n_は1から9までの整数です。複数のログファイルが存在する場合、最新のログまたは以前のログを表示するかを選択できます。

- 現在のログ — キャプチャされた最新のイベントの一覧を表示します。
- 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：サポート[サポートセンター > AutoSupport]タブ。
2. *View AutoSupport Log*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、*Archived*ラジオボタンを選択し、次に*Select AutoSupport log*ドロップダウンリストからログを選択します。

   [アーカイブ]オプションが表示されるのは、ストレージ アレイにログがアーカイブされている場合のみです。

   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*ボックスに用語を入力して*検索*をクリックします。
   - Find * をもう一度クリックして、その用語の他の出現箇所を検索します。

SANtricity System ManagerでAutoSupportメンテナンス期間を有効にします

エラー イベント発生時に自動でチケットが作成されないようにするには、AutoSupport

メンテナンス期間を有効にします。通常の動作モードでは、問題が発生したときにストレージ 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：サポート[サポートセンター > AutoSupport]タブ。
2. **AutoSupport** メンテナンス ウィンドウを有効にする 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、最大5つのメールアドレスを入力できる場合があります。複数のアドレスを追加する場合は、*別のメールを追加*を選択して別のフィールドを開いてください。

4. メンテナンス期間を有効にする期間（時間数）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生成が一時的に実行されなくなります。

終了後の操作

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。

SANtricity System ManagerでAutoSupportメンテナンス期間を無効にします

エラー イベント発生時に自動でチケットが作成されるようにするには、AutoSupportメンテナンス期間を無効にします。AutoSupportメンテナンス期間を無効にすると、問題が発生したときにストレージ 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：サポート[サポートセンター > AutoSupport]タブ。
2. **AutoSupport** メンテナンス ウィンドウの無効化 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、最大5つのメールアドレスを入力できる場合があります。複数のアドレスを追加する場合は、*別のメールを追加*を選択して別のフィールドを開いてください。

4. *はい*をクリックします。

   エラー イベント発生時のAutoSupportによる自動チケット作成が有効になります。

終了後の操作

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作業に進んでください。

イベントの表示

SANtricity ソフトウェアのイベント ログについて学ぶ

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、障害に至ったイベントをトラブルシューティングする際のテクニカル サポートに役立ちます。

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 カテゴリ

イベント ログ内のイベントは、さまざまなステータスで分類されます。処理が必要なイベントのステータスは次のとおりです。

- 致命的
- 警告

情報提供目的で、ただちに処理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

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。重大イベントが発生しても、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け取るように設定したEメール受信者に送信されます。イベントが発生した時点でシェルフIDが不明な場合、シェルフIDは「Shelf unknown」と記載されます。

重大イベントを受け取った場合は、Recovery Guruの手順を参照してイベントの詳細を確認してください。Recovery Guruの手順に従って重大イベントを解決します。一部の重大イベントについては、解決にあたってテクニカル サポートへの連絡が必要となることがあります。

SANtricity System Managerの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. メニューの「Support」→「Event Log」を選択してください。

   イベント ログ ページが表示されます。

ページの詳細

項目	概要
[すべて表示]フィールド	すべてのイベントを表示するか、重大 / 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。たとえば、特定のコンポーネントに関連するイベントや特定のイベントだけを表示する場合に役立ちます。
[列を選択]アイコン	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	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 クロックに準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。 • **Critical** — ストレージアレイに問題が発生しています。ただし、すぐに対処すれば、データへのアクセスが失われるのを防ぐことができます。Criticalイベントは、アラート通知に使用されます。すべてのCriticalイベントは、ネットワーク管理クライアント（SNMPトラップ経由）または設定したEメール受信者に送信されます。 • 警告 — エラーが発生し、ストレージ アレイのパフォーマンスと、別のエラーからの復旧能力が低下しました。 • 情報 — ストレージ アレイに関連する重要度の低い情報。
[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。ハードウェア（ドライブ、コントローラなど）またはソフトウェア（コントローラ ファームウェア）のどちらかです。
[コンポーネントの場所]列	ストレージ アレイ内のコンポーネントの物理的な場所。
[説明]列	イベントの説明。 例 — `Drive write failure - retries exhausted`

項目	概要
[シーケンス番号]列	ストレージアレイ内の特定のログエントリを一意に識別する64ビットの数値。この数値は、新しいイベントログエントリが追加されるたびに1ずつ増加します。この情報を表示するには、*列の選択*アイコンをクリックします。
[イベント タイプ]列	記録されたイベントの種類ごとに識別する4桁の数字。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によって使用されます。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 – ストレージアレイ内のコンポーネントに障害が発生しました。たとえば、ドライブ障害またはバッテリー障害。 • 状態変化 – ストレージ アレイの要素の状態が変化したこと。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。 • 内部 – ユーザー操作を必要としない内部コントローラ操作（コントローラが一日の開始処理を完了した場合など）。 • コマンド – ストレージアレイに対して発行されたコマンド（例：ホットスペアが割り当てられた）。 • 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の同期とパージを実行できない、またはストレージアレイで冗長性エラーが検出された場合などです。 • 一般 – 他のどのカテゴリーにもうまく当てはまらないイベント全般。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てください。
[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。

   イベントが記録され、イベントログページに表示されるまでには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*をクリックします。

      ファイルは、ブラウザのダウンロードフォルダに次の名前で保存されます `major-event-log-timestamp.log`。

4. イベント ログからイベントをクリアするには、次の手順を実行します。

   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、その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. 最初に、イベント ログを保存します。

b. *すべてクリア*をクリックし、操作を実行することを確認します。

アップグレードの管理

SANtricity ソフトウェアのアップグレードについて説明します

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やファームウェアをダウンロードしたり、コントローラやドライブをアップグレードしたりします。

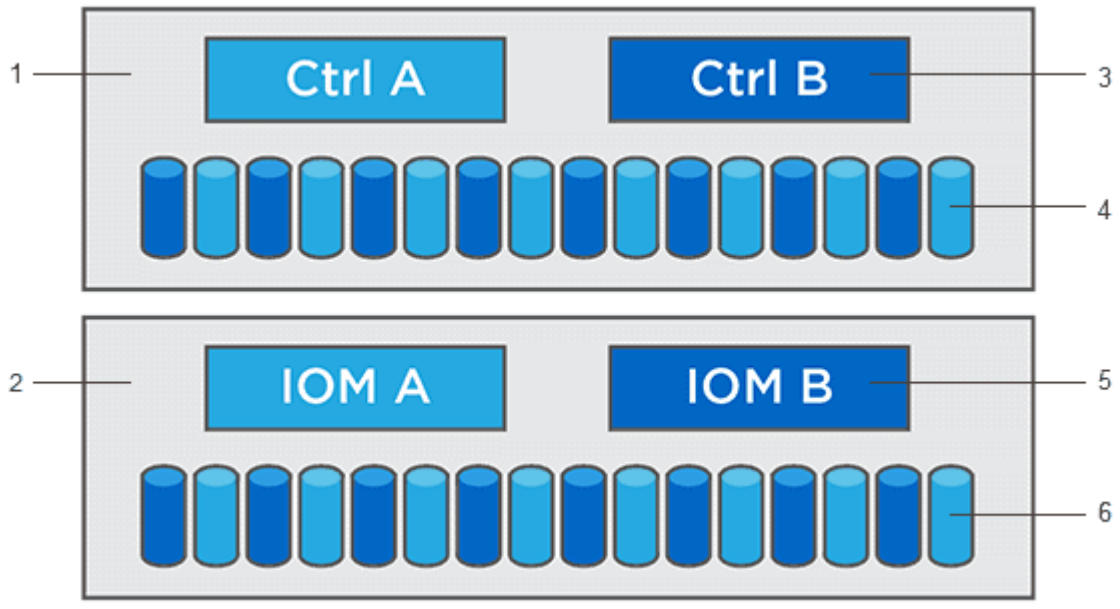
コントローラのアップグレードの概要

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 アレイの複数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。
- **Supervisor software** — Supervisor software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 ソフトウェア；[4] ドライブ ファームウェア；[5] IOM ファームウェア；[6] ドライブ ファームウェア

現在のソフトウェアとファームウェアのバージョンは、「ソフトウェアとファームウェアのインベントリ」ダイアログボックスで確認できます。メニュー：サポート[アップグレードセンター]に移動し、*ソフトウェアとファームウェアのインベントリ*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通信できるように、ホストのマルチパス/フェイルオーバードライバやHBAドライバもアップグレードする必要がある場合があります。これが当てはまるかどうかを確認するには、 "NetApp Interoperability Matrix Tool"を参照してください。

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 アレイはI/Oの処理を継続できます。アップグレードでは、まず、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にボリュームが戻され、さらにコントローラBのすべてのボリュームもフェイルオーバーしてコントローラBがアップグレードされます。

アップグレード前の健全性チェック

アップグレード プロセスの一環として、アップグレード前の健全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ます。

- 割り当てドライブに障害が発生している
- ホット スペアを使用中である
- 不完全なボリューム グループがある
- 同時に実行できない処理を実行中である
- 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 ログのイベント数が多すぎる
- 構成データベースの検証にエラーがある
- 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、ドライブの製造元はドライブ 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。

Online

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します。

- 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に対する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。

- 冗長化されていないボリューム 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 ファイルは互換性があるドライブにのみダウンロードすることができます。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。

SANtricity System Managerでコントローラ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SRAM（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利用できます。

開始する前に

- IOMファームウェアをアップグレードするかどうかを決めます。

通常は、すべてのコンポーネントを同時にアップグレードする必要があります。ただし、SANtricity OSソフトウェアのアップグレードの一部としてIOMファームウェアをアップグレードしたくない場合、またはテクニカルサポートからIOMファームウェアのダウングレードを指示された場合は、IOMファームウェアをアップグレードしないことに決めることもできます（ファームウェアのダウングレードはコマンドラインインターフェイスを使用した場合のみ可能です）。

- 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、お使いのコントローラのNVSRAMファイルにパッチを適用した場合や、ファイルがカスタム バージョンであるため上書きしない場合は、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、後でアクティブ化するかを決定します。

  あとでアクティブ化する理由としては、次のようなものがあります。

  - 時間帯 — ソフトウェアとファームウェアの有効化には時間がかかる場合があるため、I/O負荷が軽い時間帯まで待つことをお勧めします。コントローラはアクティベーション中に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パフォーマンスが通常より低下する場合があります。
  - パッケージの種類 — 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、1つのストレージ アレイで新しいソフトウェアとファームウェアをテストすることをお勧めします。

- 非セキュア ドライブまたは内部的にセキュアなドライブから切り替えて、外部キー管理サーバ（KMS）をドライブ セキュリティに使用するかどうかを決めます。
- 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。

タスク概要

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だけ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。

データ損失またはストレージ アレイの損傷のリスク — アップグレード中はストレージ アレイに変更を加えないでください。ストレージ アレイへの電源供給を維持してください。

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 エラーを防ぐためにストレージ アレイに対する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. メニューの「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. **NetApp Support** 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*タブをクリックし、次に*Downloads*を選択してください。
   c. *E-Series SANtricity OS Controller Software*を選択します。
   d. 残りの指示に従ってください。

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. 現時点でIOMファームウェアをアップグレードしたくない場合は、*IOM自動同期を一時停止*をクリックしてください。

   ストレージ アレイで1つのコントローラを使用している場合は、IOMファームウェアがアップグレードされません。

5. SANtricity OS ソフト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。

   [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. 1つ以上のファイルを選択してアップグレード プロセスを開始します。

   a. *参照*をクリックしてサポート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に移動し、SANtricity OSソフトウェアファイルを選択します。

   b. *参照*をクリックして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、コントローラNVSRAMファイルを選択します。コントローラNVSRAMファイルのファイル名は `N2800-830000-000.dlp`のようになります。

      これらの操作の注意事項を次に示します。

      - 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。
      - アップグレード用の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、*今すぐファイルを転送するが、アップグレードは行わない（後でアップグレードを有効にする）*チェックボックスを選択することで、ファイルをアクティブ化せずにコントローラに転送できます。

8. *Start*をクリックし、操作を実行することを確認してください。

   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、転送や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項目の一覧を表示するには、*ログを保存*をクリックしてください。

   ファイルは、ブラウザのダウンロードフォルダに次の名前で保存されます `drive_upgrade_log-timestamp.txt`。

終了後の操作

- 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てください。
- 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を確認して、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てください（メニュー：サポート[アップグレードセンター]に移動し、*ソフトウェアとファームウェアのインベントリ*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。

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。

タスク概要

アップグレード 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有効化には時間がかかる場合があるため、I/O負荷が軽い時間帯まで待つことをお勧めします。コントローラはアクティベーション中に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パフォーマンスが通常より低下する場合があります。
- パッケージの種類 — 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、1つのストレージ アレイで新しいソフトウェアとファームウェアをテストすることをお勧めします。

転送されたがアクティブ化されていないソフトウェアまたはファームウェアがある場合は、System Manager ホーム ページの通知領域とアップグレード センター ページに通知が表示されます。

一度開始したアクティブ化プロセスは停止できません。

手順

1. メニューの「Support[Upgrade Center]」を選択します。
2. SANtricity OS Controller Software upgradeというラベルの付いた領域で、*Activate*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全性チェックが開始されます。アップグレード前の健全性チェックに合格した場合、アップグレードプロセスはファイルの有効化に進みます。アップグレード前の健全性チェックが失敗した場合は、Recovery Guruを使用するか、テクニカルサポートに連絡して問題を解決してください。状況によっては、テクニカルサポートから*Allow Upgrade*チェックボックスを選択して、エラーが発生してもアップグレードを続行するように指示される場合があります。

   アップグレード前の健全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項目の一覧を表示するには、*ログを保存*をクリックしてください。

   ファイルは、ブラウザのダウンロードフォルダに次の名前で保存されます `drive_upgrade_log-timestamp.txt`。

終了後の操作

- 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てください。
- 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を確認して、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てください（メニュー：サポート[アップグレードセンター]に移動し、*ソフトウェアとファームウェアのインベントリ*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。

SANtricity System Managerでドライブ ファームウェアをアップグレード

ドライブのファームウェアをアップグレードして、最新の機能とバグ修正をすべて適用することができます。

開始する前に

- ディスクツーディスク バックアップ、（計画的なファームウェア アップグレードの影響を受けないボリューム グループへの）ボリューム コピー、またはリモート ミラーを使用してデータをバックアップしておく必要があります。
- ストレージ アレイのステータスが最適な状態である必要があります。
- 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 アレイでの構成の変更は実行されません。
- ドライブのオフライン アップグレードのみが可能な場合は、ドライブに関連付けられているすべてのボリュームへのI/Oアクティビティを停止します。

手順

1. メニューの「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. *参照*をクリックして、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 `D_HUC101212CSS600_30602291_MS01_2800_0002`のようになり、拡張子は `.dlp`です。

   ドライブ ファームウェア ファイルを1つずつ（最大4つ）選択できます。複数のドライブ ファームウェア ファイルが同じドライブに対応している場合は、ファイルの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 ファイルを指定し、それ以外のファイルは削除してください。

6. **Next** をクリックします。

   *ドライブの選択*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の一覧が表示されます。

   対応しているドライブのみ表示されます。

   ドライブ用に選択されたファームウェアは、「提案されたファームウェア」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ってください。

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処理を行っている_間に_ファームウェアの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法を選択した場合、これらのドライブを使用している関連ボリュームへのI/Oを停止する必要はありません。これらのドライブは、ストレージアレイがそれらのドライブへのI/O処理を行っている間に、1台ずつアップグレードされます。
- オフライン（並列） — ドライブを使用するボリューム上のすべてのI/Oアクティビティが停止している間_のみ_、ファームウェアの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法を選択する場合は、アップグレード対象のドライブを使用しているすべてのボリュームで、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。冗長性を持たないドライブは、オフライン処理として扱う必要があります。この要件には、SSDキャッシュ、RAID 0ボリュームグループ、または劣化しているプールや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が含まれます。オフライン（並列）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. 表の最初の列で、アップグレードするドライブを選択します（複数可）。
9. *Start*をクリックし、操作を実行することを確認してください。

   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。現在進行中のファームウェアのダウンロードが完了します。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項目の一覧を表示するには、*ログを保存*をクリックしてください。

    ファイルは、ブラウザのダウンロードフォルダに次の名前で保存されます `drive_upgrade_log-timestamp.txt`。

11. アップグレード手順の実行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に従います。

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
割り当てドライブに障害が発生している	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。エラーが発生したドライブが認定済みのドライブであることを確認してください。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、障害が発生したドライブ以上の容量を持つドライブと交換してください。 ストレージ アレイによるI/Oの受信中に、障害が発生したドライブを交換できます。
Check storage array	• 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正しく接続されていることを確認します。
Integrated hot spare drives	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 グループがある	1つ以上のボリューム グループまたはディスク プールが不完全な場合は、ファームウェアをアップグレードする前に、このエラーを修正する必要があります。System Managerを起動し、Recovery Guruを使用して問題を解決します。
Exclusive operations \(other than background media/parity scan\) currently running on any volume groups	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。
Either controller in a state other than Optimal	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。
Mismatched Storage Partition information between Controller Object Graphs	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。

ファームウェアのダウンロード エラー	対処方法
SPM Verify Database Controller check fails	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。
Configuration Database Validation \(If supported by the storage array's controller version\)	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 Related Checks	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。
More than 10 DDE Informational or Critical MEL events were reported in the last 7 days	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。
More than 2 Page 2C Critical MEL Events were reported in the last 7 days	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。
More than 2 Degraded Drive Channel Critical MEL events were reported in the last 7 days	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。
More than 4 critical MEL entries in the last 7 days	この問題を解決するには、テクニカル サポートにお問い合わせください。

終了後の操作

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。

SANtricity ソフトウェアおよびファームウェアのアップグレード エラーについて学ぶ

コントローラ ソフトウェアのアップグレードまたはドライブ ファームウェアのアップグレードの際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	概要	推奨される対処方法
割り当てドライブに障害が発生している	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。	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。エラーが発生したドライブが認定済みのドライブであることを確認してください。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、障害が発生したドライブ以上の容量を持つドライブと交換してください。 ストレージ アレイによるI/Oの受信中に、障害が発生したドライブを交換できます。
Integrated hot spare drives	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 グループがある	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。
Exclusive operations (other than background media/parity scan) currently running on any volume groups	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。
Either controller in a state other than Optimal	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。

ファームウェアのダウンロードエラー	概要	推奨される対処方法
SPM Verify Database Controller check fails	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。
Configuration Database Validation (If supported by the storage array's controller version)	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 Related Checks	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。
More than 10 DDE Informational or Critical MEL events were reported in the last 7 days	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。
More than 2 Page 2C Critical MEL Events were reported in the last 7 days	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。
More than 2 Degraded Drive Channel Critical MEL events were reported in the last 7 days	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。
More than 4 critical MEL entries in the last 7 days	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。
A valid management IP address is required.	この処理を実行するには、有効なコントローラの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。
The command requires an active management IP address for each controllers to be provided.	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。
Unhandled download file type returned.	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エラー	概要	推奨される対処方法
An error occurred during the firmware download upload procedure.	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 アレイが最適であることを確認し、操作を再試行してください。	ストレージ アレイが最適であることを確認した後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問題を解決してください。
An error occurred during the firmware activation procedure.	コントローラが要求を処理できないため、ファームウェアの有効化に失敗しました。ストレージアレイが最適であることを確認し、操作を再試行してください。	ストレージ アレイが最適であることを確認した後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問題を解決してください。
コントローラー{0}の再起動を待機中にタイムアウトが発生しました。	管理ソフトウェアは、再起動後にコントローラ{0}に再接続できません。ストレージアレイへの動作可能な接続パスが存在することを確認し、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 アレイが最適であることを確認した後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、一部の状態については、テクニカル サポートへの問い合わせ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。

AutoSupport に関するよくある質問（FAQ） SANtricity System Manager 用

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

収集されるデータは何ですか?

AutoSupportおよび手動のサポート 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 アレイに関するあらゆる種類の情報が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 データです。この情報は、テクニカル サポートがストレージ アレイの問題を解決するためにのみ使用されます。

読み取り不能セクターのデータは何を示していますか？

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することができます。

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んでいるボリュームに関する次の情報が記録されます。各フィールドはソートできます。

フィールド	概要
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 ID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、あるいはデフォルト クラスタからボリュームにアクセスできない場合は、「NA」と表示されます。

読み取り不能セクターに関するその他の情報を表示するには、ボリュームの横にあるプラス（+）記号をクリックします。

フィールド	概要
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。 • 物理的 — 物理メディア エラー。 • 論理 — ストライプ内の別の場所で読み取りエラーが発生し、データが読み取れなくなりました。例えば、ボリューム内の別の箇所におけるメディアエラーが原因で、読み取り不能なセクターが存在する場合など。 • **Inconsistent** — 冗長性データに矛盾があります。 • **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。

ファームウェアは、特定のエラーを検出すると、自動的にヘルスイメージを生成します。特定のトラブルシューティングシナリオでは、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求められる場合があります。

AutoSupportとはどのような機能ですか**?**

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。

- 基本**AutoSupport** — ストレージ アレイがデータを自動的に収集し、テクニカル サポートに送信できるようにします。
- **AutoSupport OnDemand** — 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。すべての送信は、AutoSupportサーバからではなく、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定期的にAutoSupportサーバと通信して、保留中の再送信要求があるかどうかを確認し、それに応じて応答します。
- 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、テクニカルサポートが最新のAutoSupportディスパッチを要求できるようにします。すべての送信は、AutoSupportサーバからではなく、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定期的にAutoSupportサーバと通信し、保留中の新しい要求があるかどうかを確認して、それに応じて応答します。

AutoSupport機能ではどういう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、OnDemand / Remote Diagnosticsディスパッチの3つがあります。

AutoSupportデータにはユーザーデータは含まれていません。

- 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 イベントが発生すると送信されます。
  - 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。
- スケジュール済みディスパッチ

  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。

  - 毎日配信 — ユーザーが設定した時間間隔で、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。
  - 週次配信 — ユーザーが設定可能な時間帯と曜日に、毎週1回配信されます。構成情報およびシステム状態情報が含まれます。
- **AutoSupport OnDemand**およびリモート診断のディスパッチ
  - **AutoSupport OnDemand** — 問題のトラブルシューティングに必要な場合に、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。すべての送信は、AutoSupportサーバからではなく、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定期的にAutoSupportサーバと通信して、保留中の再送信要求があるかどうかを確認し、それに応じて応答します。
  - 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、テクニカルサポートが最新のAutoSupportディスパッチを要求できるようにします。すべての送信は、AutoSupportサーバからではなく、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定期的にAutoSupportサーバと通信し、保留中の新しい要求があるかどうかを確認して、それに応じて応答します。

AutoSupport機能の配信方法を設定するにはどうすればよいですか?

AutoSupport機能は、テクニカル サポートへのAutoSupportディスパッチの配信にHTTPSとSMTPのプロトコルをサポートしています。

開始する前に

- AutoSupport機能が有効になっている必要があります。有効になっているかどうかは[AutoSupport]ページで確認できます。
- ネットワークにDNSサーバをインストールし、設定する必要があります。DNSサーバのアドレスがSystem Managerで設定されている必要があります（[ハードウェア]ページから設定できます）。

タスク概要

各プロトコルを確認します。

- **HTTPS** — HTTPSを使用して、宛先のテクニカルサポートサーバーに直接接続できます。AutoSupport OnDemandまたはリモート診断のいずれかを有効にする場合は、AutoSupport配信方法をHTTPSに設定する必要があります。
- **Email** — AutoSupportディスパッチの送信方法として、メールサーバーを使用できます。

> **HTTPS**と電子メール方式の違い。SMTPを使用する電子メール配信方式は、HTTPS配信方式とはいくつかの重要な点で異なります。まず、電子メール方式での送信サイズは5MBに制限されているため、一部のASUPデータ収集データは送信されません。第二に、AutoSupport OnDemand機能はHTTPS配信方式でのみ利用可能です。

手順

1. メニューを選択：サポート[サポートセンター > AutoSupport]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、以下の配信パラメータのいずれかを選択してください：
     - 直接 — この配信パラメータはデフォルトの選択です。このオプションを選択すると、HTTPSプロトコルを使用して接続先のテクニカル サポート 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、宛先の技術サポートシステムへの接続を確立するために必要なHTTPプロキシ サーバの詳細情報を指定できます。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、ホスト認証情報（ユーザー名とパスワード）を入力する必要があるのは、必要な場合のみです。
     - プロキシ自動構成スクリプト（**PAC**）経由 — プロキシ自動構成（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、宛先の技術サポートシステムとの接続を確立するための適切なプロキシ サーバをシステムが自動的に選択できます。
   - [E 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 アドレス（完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレス）
     - AutoSupportディスパッチEメールの[差出人]フィールドに表示されるEメール アドレス
     - *オプション。構成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メールアドレス。

- メッセージを暗号化する場合は、暗号化の種類として*SMTPS*または*STARTTLS*を選択し、暗号化されたメッセージ用のポート番号を選択してください。それ以外の場合は、*なし*を選択してください。
- 必要に応じて、送信者および送信元メール サーバの認証に使用するユーザ名とパスワードを入力します。

4. *構成のテスト*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 サーバへの接続をテストします。AutoSupport On-Demand機能を有効にした場合、システムはAutoSupport OnDemandディスパッチ配信の接続もテストします。

   設定テストに失敗した場合は、設定を確認してから、再度テストを実行してください。テストが何度も失敗する場合は、テクニカル サポートにお問い合わせください。

5. *保存*をクリックします。

構成データとは何ですか**?**

[構成データの収集]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。構成データの収集機能は、 `save storageArray dbmDatabase`のCLIコマンドと同じ情報を保存します。

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定しました。
- IOMファームウェアをアップグレードするかどうかを決めます。

  通常は、すべてのコンポーネントを同時にアップグレードする必要があります。ただし、SANtricity OSコントローラ ソフトウェアのアップグレードの一環としてIOMファームウェアをアップグレードしない場合、あるいはテクニカル サポートからIOMファームウェアのダウングレードを指示された場合（ファームウェアをダウングレードするにはコマンドライン インターフェイスを使用する必要があります）は、IOMファームウェアをアップグレードしないという選択も可能です。

- 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、お使いのコントローラのNVSRAMファイルにパッチを適用した場合や、ファイルがカスタム バージョンであるため上書きしない場合は、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としては、次のようなものがあります。

  - 時間帯 — ソフトウェアとファームウェアの有効化には時間がかかる場合があるため、I/O負荷が軽い時間帯まで待つことをお勧めします。コントローラはアクティベーション中に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パフォーマンスが通常より低下する場合があります。
  - パッケージの種類 — 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、1つのストレージ アレイで新しいソフトウェアとファームウェアをテストすることをお勧めします。

次のコンポーネントは、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。
- **Supervisor software** — Supervisor software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。

これが当てはまるかどうかを確認するには、 "NetApp Interoperability Matrix Tool"を参照してください。

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 エラーを防ぐためにストレージ アレイに対する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。

アップグレードが実行されている間は、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、次回 SANtricity OS コントローラ ソフトウェアのアップグレードが実行されたときに 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の自動同期を中断することができます。停止しない場合、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左右されます。

ドライブ ファームウェアのオンライン アップグレードで、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違ってきます。

ドライブ ファームウェアをアップグレードする前に知っておくべきことは何ですか？

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には、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します。新しいファームウェアが正しく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理しておきます。
- 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にストレージ 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はどのように選択すればよいですか**?**

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 グループが冗長性をサポートし、最適である場合、オンライン方式を使用してドライブ ファームウェアをアップグレードできます。オンライン方式では、ストレージ アレイがこれらのドライブを使用して関連ボリュームへのI/O処理を行っている間に、ファームウェアをダウンロードします。これらのドライブを使用している関連ボリュームへのI/Oを停止する必要はありません。これらのドライブは、ドライブに関連付けられたボリュームに合わせて、1台ずつアップグレードされます。ドライブが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場合、ファームウェアはオンラインまたはオフラインの方法で更新できます。オンライン方式でドライブ 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 グループが冗長性（RAID 0）をサポートしていない場合、または劣化している場合は、オフライン方式を使用してドライブ ファームウェアをアップグレードする必要があります。オフライン方式では、これらのドライブを使用している関連ボリュームへのすべてのI/Oアクティビティが停止している間_のみ_ファームウェアをアップグレードします。これらのドライブを使用している関連ボリュームへのすべてのI/Oを停止する必要があります。ドライブが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場合、ファームウェアはオンライン方式またはオフライン方式で更新できます。

SANtricity Unified Manager 7による複数のアレイ管理

メイン画面

SANtricity Unified Managerについて学ぶ

SANtricity Unified ManagerはWebベースのインターフェイスで、複数のストレージアレイを単一のビューで管理できます。

メイン ページ

Unified Managerにログインすると、メイン ページが*管理 - すべて*に開きます。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一覧をスクロールして確認したり、そのステータスを表示したり、単一のアレイまたはアレイのグループに対して操作を実行したりできます。

ナビゲーション サイドバー

ナビゲーション サイドバーからUnified Managerの各機能にアクセスできます。

領域	概要
管理	ネットワーク内のストレージアレイを検出し、アレイのSANtricity System Managerを起動し、1つのアレイから複数のアレイに設定をインポートし、アレイグループを管理します。アレイ名の横にあるチェックボックスを選択すると、設定のインポートやアレイグループの作成など、アレイに対して操作を実行できます。各行の末尾にある省略記号は、名前変更など、単一のアレイに対する操作を行うためのインラインメニューを提供します。
処理	バッチ処理（アレイ間での設定のインポートなど）の進捗状況が表示されます。 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間の認証を行う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、および連絡先が表示されます。

画面の設定とヘルプ

画面右上から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

システムに現在ログインしているユーザが画面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、以下を参照してください。

- "管理者パスワード保護の設定"
- "管理者パスワードの変更"
- "ローカル ユーザ プロファイルのパスワードの変更"

SANtricity Unified Managerでサポートされるブラウザ

SANtricity Unified Managerは、複数の種類のブラウザからアクセスできます。

サポートされるブラウザとバージョンを次に示します。

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

Webサービス プロキシがインストールされていて、ブラウザから使用できる必要があります。

SANtricity Unified Managerの管理者パスワード保護について学ぶ

不正アクセスから保護するために、管理者パスワードを使用してSANtricity Unified Managerを設定する必要があります。

管理者パスワードとユーザ プロファイル

Unified Managerを初めて起動したとき、管理者パスワードを設定するように求められます。管理者パスワードを知っているユーザは、ストレージ アレイの設定を変更することができます。

管理者パスワードに加えて、Unified Managerには、ロールが1つ以上割り当てられたユーザ プロファイルがあらかじめ設定されています。詳細については、"アクセス管理の仕組み"を参照してください。

ユーザとマッピングは変更できません。変更できるのはパスワードのみです。パスワードの変更については、以下を参照してください。

- "管理者パスワードの変更"
- "ローカル ユーザ プロファイルのパスワードの変更"

セッション 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。この状態の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分間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、"セッション タイムアウトの管理"を参照してください。

SANtricity Unified Managerで管理者パスワードを変更する

SANtricity Unified Managerへのアクセスに使用する管理者パスワードを変更できます。

開始する前に

- ローカル管理者としてログインする必要があります。これにはRoot管理者権限が含まれます。
- 現在の管理者パスワードを知っている必要があります。

タスク概要

パスワードを決める際は、次のガイドラインに注意してください。

- パスワードでは大文字と小文字が区別されます。
- パスワードの末尾のスペースは削除されません。設定時に末尾にスペースを含めた場合は、入力時に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、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. メニューの「設定」→「アクセス管理」を選択します。
2. *ローカルユーザーロール*タブを選択します。
3. テーブルから*admin*ユーザを選択します。

   パスワード変更ボタンが有効になります。

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. この操作を確定するには、ローカル管理者パスワードを入力し、*変更*をクリックしてください。

SANtricity Unified Managerでセッションタイムアウトを管理する

SANtricity Unified Managerのタイムアウトを設定して、指定された時間が経過した後にユーザーの非アクティブなセッションを切断できます。

タスク概要

Unified Managerのセッション タイムアウトは、デフォルトでは30分です。その時間を調整することも、セッション タイムアウトを完全に無効にすることもできます。

> 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が構成されている場合、ユーザーのSSOセッションが最大制限に達すると、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セッションタイムアウトの前に発生する可能性があります。

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. スピン ボックスを使用して時間（分単位）を増減します。

   設定できる最小値は15分です。

   > セッションタイムアウトを無効にするには、*時間の長さを設定する...*チェックボックスをオフにします。
4. *保存*をクリックします。

ストレージ アレイ

SANtricity Unified Managerでの検出について学ぶ

ストレージ リソースを管理するには、最初に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。

アレイを検出するにはどうすればよいですか?

組織のネットワークから管理対象のストレージ アレイを検索して追加するには、[追加 / 検出]ページを使用します。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。検出するためには、ネットワークIPアドレスを入力します。指定したアドレス範囲内の各IPアドレスへの接続がUnified Managerで個別に試行されます。

詳細については、以下を参照してください。

- "アレイの検出に関する考慮事項"
- "複数のストレージ アレイの検出"

- "単一のアレイの検出"

アレイを管理するにはどうすればよいですか?

アレイを検出したら、*管理 - すべて*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、ステータスを表示したり、単一のアレイまたはアレイのグループに対して操作を実行したりできます。

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を開くことができます。

詳細については、以下を参照してください。

- "System Managerへのアクセスに関する考慮事項"
- "個々のストレージ アレイの管理"
- "ストレージ アレイのステータスの表示"

概念

SANtricity Unified Managerでのストレージアレイの検出について学ぶ

SANtricity Unified Managerがストレージリソースを表示および管理する前に、組織のネットワーク内で管理するストレージアレイを検出する必要があります。複数のアレイを検出することも、単一のアレイを検出することもできます。

複数のストレージ アレイの検出

複数のアレイを検出することを選択した場合、ネットワークIPアドレスの範囲を入力すると、Unified Managerはその範囲内の各IPアドレスに対して個別に接続を試みます。アクセスに成功したストレージアレイは「検出」ページに表示され、管理ドメインに追加できます。

単一のストレージ アレイの検出

単一のアレイを検出する場合は、ストレージ アレイ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、コントローラに割り当てられた単一の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。これらのコントローラに割り当てられた代替コントローラまたはIPアドレスが、この単一のIPアドレスまたはIPアドレス範囲外にある場合、Unified Managerはそれらを検出または表示しません。ただし、ストレージアレイを追加すると、関連付けられているすべてのIPアドレスが検出され、管理ビューに表示されます。

ユーザ クレデンシャル

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

検出プロセスの一環として、Unified Managerは検出されたストレージアレイが信頼できるソースの証明書を使用していることを確認します。Unified Managerは、ブラウザとのすべての接続において、2種類の証明書ベースの認証方式を使用します：

- 信頼できる証明書

  Unified Managerによって検出されたアレイの場合、認証局から提供される追加の信頼できる証明書をインストールする必要がある場合があります。

  これらの証明書をインポートするには、*Import*ボタンを使用してください。以前にこのアレイに接続したことがある場合、コントローラー証明書の一方または両方が期限切れ、失効、あるいは証明書チェーンにルート証明書または中間証明書が欠落している可能性があります。ストレージアレイを管理する前に、期限切れまたは失効した証明書を交換するか、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

  自己署名証明書も使用できます。管理者が署名付き証明書をインポートせずにアレイの検出を試みた場合、Unified Manager はエラーダイアログボックスを表示し、管理者が自己署名証明書を受け入れることができます。ストレージアレイの自己署名証明書は信頼済みとしてマークされ、ストレージアレイは Unified Manager に追加されます。

  ストレージアレイへの接続を信頼しない場合は、キャンセル を選択し、ストレージアレイを Unified Manager に追加する前に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ください。

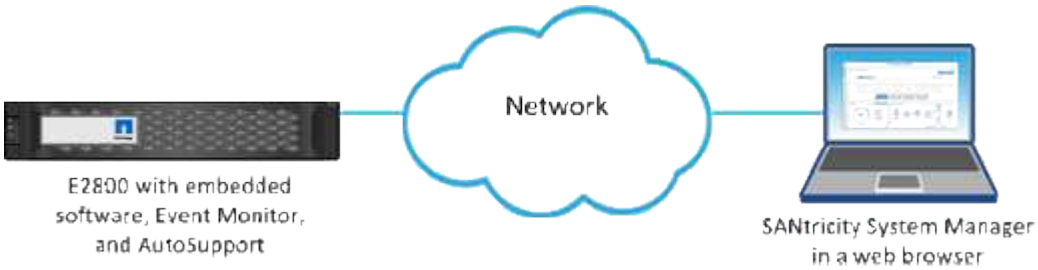
Unified Managerから**SANtricity System Manager**へのアクセスについて学ぶ

1つ以上のストレージアレイを選択し、ストレージアレイを設定および管理する場合は、[起動]オプションを使用してSANtricity System Managerを開きます。

System Managerはコントローラに組み込みのアプリケーションで、イーサネット管理ポートを介してネットワークに接続されます。System Managerにはアレイベースの機能がすべて含まれています。

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。

- ここに挙げられている配列モデルの一つ："Eシリーズハードウェアの概要"
- Webブラウザを使用したネットワーク管理クライアントへのアウトオブバンド接続



アレイの検出

SANtricity Unified Managerで複数のストレージアレイを検出

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。

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 アレイのセットアップが完了し、正しく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がSystem Managerの[アクセス管理]タイルで設定されている必要があります。
- 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ローカル システム上にある必要があります。

アレイの検出は複数の手順で構成されます。

ステップ**1**：ネットワークアドレスを入力する

ローカルサブネットワーク全体を検索するには、ネットワークアドレス範囲を入力します。アクセスに成功したストレージアレイは「検出」ページに表示され、管理ドメインに追加される場合があります。

何らかの理由で検出操作を停止する必要がある場合は、*Stop Discovery*をクリックしてください。

手順

1. 「管理」ページから*追加/発見*を選択します。

   [追加 / 検出]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. ローカルサブネットワーク全体を検索するには、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、*Start Discovery*をクリックしてください。

   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入力されます。

   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正しく接続され、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。*New Discovery Parameters*をクリックすると、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選択し、*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. ウィザードの次のステップに進むには、*次へ*をクリックしてください。

ステップ**2**：検出中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、ストレージ アレイはUnified Managerに追加されます。
- ストレージアレイへの接続を信頼しない場合は、キャンセル を選択し、いずれかのストレージアレイを Unified Manager に追加する前に、それぞれの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ください。

2. ウィザードの次のステップに進むには、*次へ*をクリックしてください。

ステップ**3**：検出中に信頼でき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、接続が安全であることが確認できないと発生します。アレイの検出時に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選択し、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. *参照*をクリックして、ストレージアレイ用の証明書ファイルを選択してください。

   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。

   信頼できない証明書の問題が解決されていないストレージアレイは、Unified Managerに追加されません。

4. ウィザードの次のステップに進むには、*次へ*をクリックしてください。

ステップ**4**：パスワードを入力する

管理ドメインにストレージ アレイを追加するときは、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る：ドロップダウンリストから、選択したストレージアレイに関連付けるグループを選択します。
3. *完了*をクリックします。

終了後の操作

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。

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

SANtricity Unified Managerで単一のアレイを検出

単一のストレージ アレイを手動で検出して組織のネットワークに追加するには、[単一のストレージ アレイを追加 / 検出]オプションを使用します。

開始する前に

- ストレージ アレイのセットアップが完了し、正しく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がSystem Managerの[アクセス管理]タイルで設定されている必要があります。

手順

1. 「管理」ページから*追加/発見*を選択します。

   [追加 / 検出]ダイアログ ボックスが表示されます。

2. * 単一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. ストレージアレイ内のコントローラーのいずれかのIPアドレスを入力し、*Start Discovery*をクリックします。

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

   指定されたコントローラのIPアドレスへの接続が失敗した場合、Storage Array Not Accessibleというメッセージが表示されます。

4. 自己署名証明書についての確認が求められた場合は解決します。

   検出プロセスの一環として、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場合は解決します。

   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、接続が安全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. **Next** 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

レージアレイに関連付けるグループを選択します。

デフォルトでは、[すべて]が選択されています。

8. 管理ドメインに追加するストレージアレイの管理者パスワードを入力し、*OK*をクリックします。

終了後の操作

ストレージ アレイがUnified Managerに追加され、指定した場合は選択したグループにも追加されます。

サポート データの自動収集が有効になっている場合は、追加したストレージ アレイのサポート データが自動的に収集されます。

アレイの管理

SANtricity Unified Managerでストレージアレイのステータスを表示する

SANtricity Unified Managerは、検出された各ストレージアレイのステータスを表示します。

*管理 - すべて*ページに移動してください。このページから、Web Services Proxyとストレージアレイ間の接続状態を確認できます。

ステータス インジケータの説明を次の表に示します。

ステータス	状況
最適	ストレージ アレイが最適な状態です。証明書の問題は存在せず、パスワードは有効です。
無効なパスワード	無効なストレージ アレイ パスワードが指定されました。
信頼されていない証明書	HTTPS証明書が自己署名証明書でインポートされていないか、または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	ストレージ アレイに一度も接続していません。この状態は、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	Webサービス プロキシは以前にストレージ アレイに接続しましたが、現在はすべての接続が失われています。

SANtricity Unified Managerで個々のストレージアレイを管理する

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つまたは複数のストレージアレイのブラウザベースのSANtricity System Managerを開くことができます。

手順

1. [管理]ページで、管理処理を実行する1つ以上のストレージ アレイを選択します。
2. *起動*をクリックします。

   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. ユーザ名とパスワードを入力し、* Log in *をクリックします。

SANtricity Unified Managerでストレージアレイのパスワードを変更する

SANtricity Unified Managerでストレージアレイの表示とアクセスに使用するパスワードを更新できます。

開始する前に

- Storage Adminの権限を含むユーザ プロファイルでログインする必要があります。
- ストレージ アレイの現在のパスワード（System Managerで設定されているパスワード）を確認しておきます。

タスク概要

このタスクでは、ストレージアレイの現在のパスワードを入力して、Unified Manager からアクセスできるようにします。System Manager でアレイのパスワードが変更され、さらに Unified Manager でも変更する必要がある場合は、この操作が必要になる可能性があります。

手順

1. 「管理」ページから、1つまたは複数のストレージアレイを選択します。
2. メニュー：Uncommon Tasks[Provide Storage Array Passwords]を選択します。
3. 各ストレージアレイのパスワードを入力し、*保存*をクリックします。

ストレージアレイを**SANtricity Unified Manager**から削除

SANtricity Unified Managerから管理する必要がなくなった場合は、1つ以上のストレージアレイを削除できます。

タスク概要

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*ページを選択してください。

2. 削除するストレージ アレイを選択します。
3. メニュー：Uncommon Tasks[Remove storage array]を選択します。

   ストレージアレイは、SANtricity Unified Managerのすべてのビューから削除されます。

設定のインポート

SANtricity Unified Managerでのストレージアレイ設定のインポートについて説明します

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、ネットワークの複数のアレイを設定する場合に時間を短縮できます。

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。

詳細については、以下を参照してください。

- "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 インポートを実行するにはどうすればよいですか?

ソースとして使用するストレージ アレイで、System Managerを開いて希望するオプションを設定します。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。

詳細については、以下を参照してください。

- "アラート設定のインポート"
- "AutoSupport設定のインポート"
- "ディレクトリ サービス設定のインポート"
- "ストレージ構成のインポート"
- "システム設定のインポート"

概念

SANtricity Unified Managerでの複数のストレージアレイの設定について説明します

SANtricity Unified Managerを使用すると、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、ネットワーク内の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るバッチ処理機能です。

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設定は次のとおりです。

- アラート — 重要なイベントを管理者に送信するアラート方法（電子メール、syslogサーバ、またはSNMPサーバを使用）。
- **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的に通知を送信する機能。
- ディレクトリサービス — LDAPサーバ（Lightweight Directory Access Protocol）およびMicrosoftのActive Directoryなどのディレクトリサービスを通じて管理されるユーザ認証の方法。
- 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から*管理*ページに移動し、設定をインポートします。
4. *Operations*ページから、Import Settings操作の結果を確認してください。

SANtricity Unified Managerでストレージアレイ構成を複製するための要件

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一である。
- 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（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。

- HIC（ホストのDA機能を含む）がソースとターゲットのアレイで同一である。
- 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ないが、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。
- 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」である。
- ソース アレイのステータスは「最適」である必要はない。

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違っていてもかまわない（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割り当てら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 プロセスに含まれない。

バッチ インポートの使用

SANtricity Unified Managerでアラート設定をインポート

ストレージ アレイから別のストレージ アレイにアラート設定をインポートできます。この方法でバッチ処理すると、ネットワークの複数のアレイを設定する場合に時間を短縮できます。

開始する前に

- アラートは、ソースとして使用するストレージ アレイに対してSystem Managerで設定します（メニュー：Settings[Alerts]）。
- 対象ストレージアレイの既存の構成は、System Manager（メニュー：Settings［System ＞ Save Storage Array Configuration］）にバックアップされます。

タスク概要

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することができます。インポートされる設定は次のとおりです。

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

手順

1. 「管理」ページから*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 ボックスが表示されます。

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を含む配列を選択し、*次へ*をクリックします。
4. [ターゲットの選択]ダイアログ ボックスで、新しい設定をインポートするアレイを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。

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

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。

SANtricity Unified Managerで**AutoSupport**設定をインポートする

ストレージ アレイから別のストレージ アレイにAutoSupport設定をインポートできます。この方法でバッチ処理すると、ネットワークの複数のアレイを設定する場合に時間を短縮できます。

開始する前に

- AutoSupportは、ソースとして使用するストレージアレイについて、System Managerで設定します（メニュー：サポート[サポートセンター]）。
- 対象ストレージアレイの既存の構成は、System Manager（メニュー：Settings［System ＞ Save Storage Array Configuration］）にバックアップされます。

タスク概要

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 スケジュールが含まれます。

手順

1. 「管理」ページから*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 ボックスが表示されます。

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を含む配列を選択し、*次へ*をクリックします。

4. [ターゲットの選択]ダイアログ ボックスで、新しい設定をインポートするアレイを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。

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

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。

SANtricity Unified Managerでディレクトリサービス設定をインポート

ストレージ アレイから別のストレージ アレイにディレクトリ サービス設定をインポートできます。この方法でバッチ処理すると、ネットワークの複数のアレイを設定する場合に時間を短縮できます。

開始する前に

- ディレクトリサービスは、ソースとして使用するストレージアレイに対してSystem Managerで構成します（メニュー：Settings[Access Management]）。
- 対象ストレージアレイの既存の構成は、System Manager（メニュー：Settings［System ＞ Save Storage Array Configuration］）にバックアップされます。

タスク概要

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 アレイの定義済みロールとのマッピングが含まれます。

手順

1. 「管理」ページから*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 ボックスが表示されます。

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を含む配列を選択し、*次へ*をクリックします。
4. [ターゲットの選択]ダイアログ ボックスで、新しい設定をインポートするアレイを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。

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

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。

SANtricity Unified Managerでシステム設定をインポート

ストレージ アレイから別のストレージ アレイにシステム設定をインポートできます。この方法でバッチ処理すると、ネットワークの複数のアレイを設定する場合に時間を短縮できます。

開始する前に

- ソースとして使用するストレージ アレイのシステム設定をSystem Managerで設定しておきます。
- 対象ストレージアレイの既存の構成は、System Manager（メニュー：Settings［System ＞ Save Storage Array Configuration］）にバックアップされます。

タスク概要

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」ページから*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、*System*を選択し、*Next*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 ボックスが表示されます。

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を含む配列を選択し、*次へ*をクリックします。
4. [ターゲットの選択]ダイアログ ボックスで、新しい設定をインポートするアレイを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。

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

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。

SANtricity Unified Managerでストレージ構成設定をインポート

ストレージ アレイから別のストレージ アレイにストレージ構成をインポートできます。この方法でバッチ処理すると、ネットワークの複数のアレイを設定する場合に時間を短縮できます。

開始する前に

- ストレージは、ソースとして使用するストレージアレイのSANtricity System Managerで設定されています。
- 対象ストレージアレイの既存の構成は、System Manager（メニュー：Settings［System ＞ Save Storage Array Configuration］）にバックアップされます。
- ソースとターゲットの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一である。
  - シェルフIDが同一である。
  - 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。
  - 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」である。
  - 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。
- 次の制限事項に留意してください。
  - デュプレックス構成からシンプレックス構成へのインポートはサポートされていないが、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。
  - 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 プロセスに含まれない。

タスク概要

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」ページから*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 ボックスが表示されます。

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を含む配列を選択し、*次へ*をクリックします。
4. [ターゲットの選択]ダイアログ ボックスで、新しい設定をインポートするアレイを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。

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

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。

SANtricity Unified Managerのインポート設定に関するよくある質問

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

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読み込むバッチ処理です。この処理でインポートされる設定は、SANtricity 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。

- **E**メールアラート — 設定には、メールサーバのアドレスとアラート受信者のEメールアドレスが含まれます。
- **syslog** アラート — 設定には syslog サーバアドレスと UDP ポートが含まれます。
- **SNMP**アラート — 設定には、SNMPサーバのコミュニティ名とIPアドレスが含まれます。
- **AutoSupport** — 設定には個別の機能（基本AutoSupport、AutoSupport OnDemand、およびリモート診断）、メンテナンス期間、配信方法、および配信スケジュールが含まれます。
- ディレクトリサービス — 構成には、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。
- ストレージ構成 — 構成には、ボリューム（シック ボリュームと非リポジトリ ボリュームのみ）、ボリューム グループ、プール、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 — 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キャッシュ、および自動ロード バランシング（ホスト接続レポートは含まれません）が含まれます。

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。

- システムがアレイと通信できない（アレイに証明書、パスワード、ネットワークの問題がある場合など）。

アレイ グループ

SANtricity Unified ManagerのGroupsの概要について説明します

[グループの管理]ページでストレージ アレイのグループを作成すると管理が簡単になります。

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種類があります。

- すべてのグループ — 「すべてのグループ」はデフォルトのグループであり、組織内で検出されたすべてのストレージアレイが含まれます。「すべて」グループはメインビューからアクセスできます。
- ユーザ作成グループ — ユーザ作成グループには、そのグループに追加するために手動で選択したストレージアレイが含まれます。ユーザ作成グループは、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、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。

詳細については、以下を参照してください。

- "ストレージ アレイ グループの設定"

SANtricity Unified Managerで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つの手順で構成されます。

ステップ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. 管理ページから、メニューの「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. **Name** 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*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. メイン画面から*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. メニュー：Manage Groups[Add storage arrays to group]を選択します。
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. * Add * をクリックします。

SANtricity Unified Managerのグループからストレージアレイを削除する

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。

タスク概要

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. 管理ページから、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*をクリックします。

SANtricity Unified Manager でストレージアレイグループを削除する

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。

タスク概要

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、[すべて管理]ビューや関連付けられている他のグループから引き続きアクセスできます。

手順

1. 管理ページから、メニューの「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*をクリックします。

SANtricity Unified Managerでストレージアレイグループの名前を変更する

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することができます。

タスク概要

次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（-）、シャープ記号（#）を使用できます。それ以外の文字を使用しようとすると、エラー メッセージが表示され、別の名前を入力するように求められます。
- 名前は30文字以内で指定します。名前の先頭と末尾のスペースは削除されます。
- すぐに思い出せるような、わかりやすい一意の名前を使用します。
- わかりにくい名前は使用しないでください。

手順

1. メイン画面から*管理*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. メニューの「グループの管理」→「ストレージアレイグループの名前変更」を選択します。
3. *Group Name*フィールドに、グループの新しい名前を入力します。
4. **Rename** をクリックします。

アップグレード

SANtricity Unified ManagerのUpgrade Centerについて学ぶ

アップグレードセンターから、複数のストレージアレイ向けのSANtricity OSソフトウェアおよびNVSRAMのアップグレードを管理できます。

アップグレードはどのように行いますか**?**

最新のOSソフトウェアをダウンロードしてから、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

ソフトウェアのアップグレードを実行する手順の大まかなワークフローを以下に記載します。

1. 最新のSANtricity OSソフトウェアファイルをサポートサイトからダウンロードします（Unified Managerのサポートページからリンクを入手できます）。ファイルを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）に保存し、ファイルを解凍します。
2. Unified Managerでは、SANtricity OSソフトウェアファイルとNVSRAMファイルをリポジトリ（Webサービスプロキシサーバー上のファイル保存領域）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 Center[Upgrade SANtricity OS Software]、またはUpgrade Center > Manage Software Repositoryから追加できます。
3. ファイルがリポジトリにロードされた後、アップグレードに使用するファイルを選択できます。Upgrade SANtricity OS softwareページ（メニュー：Upgrade Center[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、互換性のあるストレージアレイの一覧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。（互換性のない配列を選択することはできません。）
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か、ファイルをステージングしてあとでアクティブ化するかを選択できます。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、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、プロセス全体を中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と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ベーションには時間がかかる場合があるため、I/O負荷が軽い時間帯まで待つことをお勧めします。I/O負荷とキャッシュサイズにもよりますが、コントローラのアップグレードは通常15分から25分程度で完了します。コントローラはアクティベーション中に再起動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パフォーマンスが通常より低下する場合があります。
- パッケージの種類 — 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、1つのストレージ アレイで新しいソフトウェアとファームウェアをテストすることをお勧めします。

ステージングされたソフトウェアをアクティブ化するには、メニュー：Support[Upgrade Center]に移動し、SANtricity OS Controller Software upgradeというラベルの付いた領域で*Activate*をクリックします。

健全性チェック

アップグレードプロセスの一環としてヘルスチェックが実行されますが、開始前に別途ヘルスチェックを実行することもできます（メニュー：Upgrade Center［Pre-Upgrade Health Check］に移動してください）。

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ます。

- 割り当てドライブに障害が発生している
- ホット スペアを使用中である
- 不完全なボリューム グループがある
- 同時に実行できない処理を実行中である
- 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 ログのイベント数が多すぎる
- 構成データベースの検証にエラーがある
- 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に、計画段階で確認が必要な考慮事項を以下に記載します。

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]ページでSANtricity OSの現在のバージョンを確認できます。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。

互換性情報については、 "NetApp Interoperability Matrix"を参照してください。また、お使いの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の手順も参照してください。エクスプレスガイドは "EシリーズおよびSANtricityのドキュメント"から入手できます。

デュアル コントローラ

ストレージ アレイにコントローラが2台あり、マルチパス ドライバがインストールされている場合は、アップグレードの実行中もストレージ アレイでI/Oの処理を継続できます。アップグレードのプロセスは次のとおりです。

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のアップグレード

SANtricity Unified Managerでアップグレード前のヘルスチェックを実行する

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. メイン画面から*管理*を選択し、次に**Upgrade Center › Pre-Upgrade Health Check**を選択します。

   [アップグレード前の健全性チェック]ダイアログ ボックスが開き、検出されたすべてのストレージ システムが表示されます。

2. 必要に応じて、ストレージ システムのリストをフィルタまたはソートして、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. **Start** 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、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、プロセス全体を中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のアップグレード

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設定を指定するコントローラ ファイルです。

開始する前に

- 最新の SANtricity OS ファイルは、SANtricity Web Services Proxy と Unified Manager が実行されているホスト システムで利用できます。
- ソフトウェアのアップグレードを今すぐアクティブ化するか、後でアクティブ化するかを把握しておく必要があります。

  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ベーションには時間がかかる場合があるため、I/O負荷が軽い時間帯まで待つことをお勧めします。コントローラはアクティベーション中に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パフォーマンスが通常より低下する場合があります。
  - パッケージの種類 — 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、1つのストレージアレイで新しいOSソフトウェアをテストすることをお勧めします。

> 11.80.x以降にアップグレードするには、システムでSANtricity OS 11.70.5が実行されている必要があります。

タスク概要

> 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 アレイに対する変更を行わないでください。ストレージ アレイへの電源を維持してください。

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 ドライバを使用していない場合は、アプリケーション エラーを防ぐためにストレージ アレイに対するI/Oアクティビティを停止します。ストレージ アレイにコントローラが2台あり、マルチパス ドライバがインストールされている場合は、I/Oアク

ティビティを停止する必要はありません。

2. メイン画面から*管理*を選択し、アップグレードするストレージアレイを1つ以上選択します。
3. メニューを選択：Upgrade Center[Upgrade SANtricity OS Software]。

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

4. NetApp サポート サイトからローカル マシンに最新のSANtricity OSソフトウェア パッケージをダウンロードします。

   a. **Add new file to software repository** をクリックします。
   b. 最新の*SANtricity OS Downloads*を見つけるには、リンクをクリックしてください。
   c. **Download Latest Release** リンクをクリックします。
   d. 残りの手順に従って、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てください。

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

5. コントローラのアップグレードに使用するOSソフトウェア ファイルとNVSRAMファイルを選択します。

   a. **SANtricity OS** ソフトウェア ファイルの選択 ドロップダウンから、ローカル マシンにダウンロードした OS ファイルを選択します。

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

   > ソフトウェアリポジトリには、Web Services Proxyに関連付けられているすべてのソフトウェアファイルが一覧表示されます。使用したい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に新しいファイルを追加*というリンクをクリックして、追加したいOSファイルが格納されている場所を参照してください。

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

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

6. [互換性があるストレージ アレイ]の表で、選択したOSソフトウェア ファイルと互換性があるストレージアレイを確認し、アップグレードするアレイを選択します。
   - [互換性があるストレージ アレイ]の表では、[管理]ビューで選択したストレージ アレイのうち、選択したファームウェア ファイルと互換性があるアレイがデフォルトで選択されます。
   - 選択したファームウェアファイルで更新できないストレージアレイは、ステータスが*互換性なし*と表示されているため、互換性のあるストレージアレイの表で選択できません。
7. オプション： ストレージアレイをアクティブ化せずにソフトウェアファイルを転送するには、*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、後でアクティブ化する*チェックボックスを選択します。
8. **Start** をクリックします。
9. すぐにアクティブ化するかあとでアクティブ化するかに応じて、次のいずれかを実行します。
   - 選択したアップグレード対象アレイに提案されたOSソフトウェア バージョンを転送することを確認

するには、*TRANSFER*と入力し、*転送*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化するには、**Upgrade Center › Activate Staged OS Software** を選択します。

- **UPGRADE** と入力して、アップグレード対象として選択したアレイに提案されたOSソフトウェア バージョンを転送してアクティブ化することを確認し、**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全性チェックが実行されます。アップグレード前の健全性チェックでは、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。
- ストレージアレイの健全性チェックでいずれかの項目が失敗した場合、アップグレードは停止します。エラーを確認するには、省略記号（...）をクリックして*ログを保存*を選択してください。ヘルスチェックのエラーを無視して、*続行*をクリックしてアップグレードを進めることもできます。
- アップグレード前の健全性チェックのあとに、アップグレード処理をキャンセルすることができます。

10. *オプション：*アップグレードが完了したら、省略記号（...）をクリックし、*ログの保存*を選択すると、特定のストレージアレイでアップグレードされた項目の一覧が表示されます。

    ファイルは、ブラウザのダウンロードフォルダに次の名前で保存されます `upgrade_log-<date>.json`。

SANtricity Unified Managerで段階的にインストールされたOSソフトウェアをアクティブ化します

ソフトウェア ファイルはただちにアクティブ化することも、都合のいいタイミングでアクティブ化することもできます。ここでは、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の手順を示します。

タスク概要

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ベーションには時間がかかる場合があるため、I/O負荷が軽い時間帯まで待つことをお勧めします。コントローラーが再起動し、アクティベーション中に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パフォーマンスが通常より低下する場合があります。
- パッケージの種類 — 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、1つのストレージ アレイで新しいソフトウェアとファームウェアをテストすることをお勧めします。

> 一度開始したアクティブ化プロセスは停止できません。

手順

1. メイン画面から*Manage*を選択します。必要に応じて、ページ上部の「ステータス」列をクリックすると、「OS Upgrade（awaiting activation）」ステータスのすべてのストレージアレイが並べ替えられます。

2. ソフトウェアをアクティベートするストレージアレイを1つ以上選択し、メニュー：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。

   - アクティブ化プロセスの一環として、アップグレード前の健全性チェックが実行されます。アップグレード前の健全性チェックでは、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。
   - ストレージアレイの健全性チェックが失敗した場合、アクティベーションは停止します。省略記号（…）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。健全性チェックエラーを無視して*続行*をクリックし、アクティベーションを続行することもできます。
   - アップグレード前の健全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全性チェックが正常に完了すると、アクティブ化が実行されます。アクティブ化にかかる時間は、ストレージ アレイの構成とアクティブ化しているコンポーネントによって異なります。

3. *オプション：*アクティベーションが完了したら、省略記号（…）をクリックして*ログの保存*を選択すると、特定のストレージアレイでアクティベートされた項目の一覧が表示されます。

   ファイルは、ブラウザのダウンロードフォルダに次の名前で保存されます `activate_log-<date>.json`。

Unified Manager で **SANtricity** ソフトウェアリポジトリを管理する

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、1つ以上のSANtricity OSファイルをWeb Services ProxyおよびUnified Managerが実行されているホストシステムにインポートできます。また、ソフトウェアリポジトリで使用可能な1つ以上のSANtricity OSファイルを削除することもできます。

開始する前に

SANtricity OSファイルを追加する場合は、OSファイルがローカルシステムで使用可能であることを確認してください。

手順

1. メイン画面から*管理*を選択し、次にアップグレードセンター › ソフトウェアリポジトリの管理を選択します。

   [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。

2. 次のいずれかを実行します。

オプション	これをやってください...
インポート	a. *インポート*をクリックします。 b. *参照*をクリックし、追加するOSファイルが格納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`に似ています。 c. 追加する OS ファイルを 1 つ以上選択し、* インポート * をクリックします。
削除	a. ソフトウェア リポジトリから削除するOSファイルを選択します。 b. *削除*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。

SANtricity Unified Manager でステージング済み **OS** ソフトウェアをクリアします

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

手順

1. メイン画面から*管理*を選択し、次に**Upgrade Center › Clear Staged OS Software**を選択します。

   [ステージング済みOSソフトウェアのクリア]ダイアログ ボックスが開き、保留中のソフトウェアまたはNVSRAMがあるストレージ アレイがすべて検出されて表示されます。

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

ミラーリング

SANtricity Unified Managerでのミラーリングについて学ぶ

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。

EF600/EF600CまたはEF300/EF300Cストレージ システムでは、同期ミラーリングは利用できません。

ミラーリングとは何ですか**?**

SANtricityアプリケーションには2種類のミラーリング（非同期と同期）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。

詳細については、以下を参照してください。

- "ミラーリングの仕組み"
- "ミラーリングに関する用語"

ミラーリングを設定するにはどうすればよいですか**?**

Unified Managerで非同期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。

詳細については、以下を参照してください。

- "ミラーリングの設定ワークフロー"
- "ミラーリングを使用するための要件"
- "非同期ミラー ペアの作成"
- "同期ミラー ペアの作成"

概念

SANtricityミラーリングについて学ぶ

SANtricity Unified Managerには、SANtricityミラーリング機能の構成オプションが含まれており、管理者はデータ保護のために2つのストレージアレイ間でデータを複製できます。

EF600/EF600CまたはEF300/EF300Cストレージ システムでは、同期ミラーリングは利用できません。

ミラーリングのタイプ

SANtricityアプリケーションには2種類のミラーリング（非同期と同期）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、あとからネットワーク 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。

同期ミラーリングは、データボリュームをリアルタイムで複製することで、継続的な可用性を確保します。その目的は、2つのストレージアレイのうち1つで災害が発生した場合に重要なデータのコピーを利用できるようにすることで、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 ボリュームへの書き込みが行われるたびにセカンダリ ボリュームへの書き込みが行われるため、コピーは常に本番データと同一です。ホストは、プライマリ ボリュームに加えられた変更内容でセカンダリ ボリュームが更新されるまで、書き込みが成功したという確認を受け取りません。このタイプのミラーリングは、災害復旧などの事業継続目的において理想的です。

ミラーリングのタイプの違い

次の表は、2種類のミラーリングの主な違いを示しています。

属性	非同期	同期
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。	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。
距離	地理的に離れたアレイをサポートします。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の機能によってのみ制限されます。	アレイ間の距離は短い距離に制限されます。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。
通信手段	標準のIPまたはFibre Channelネットワーク。	Fibre Channelネットワークのみ。
ボリューム タイプ	標準またはシン。	標準のみ。

SANtricity構成ワークフローのミラーリング

SANtricity Unified Managerで非同期または同期ミラーリングを設定し、SANtricity 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。

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、または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、実行する同期方法（手動またはスケジュール）を指定します。
   c. ローカル ストレージ アレイからプライマリ ボリュームを選択し、リザーブ容量を確認します。リザ

ーブ容量は、コピー処理に使用される物理割り当て容量です。

d. 転送先としてリモート ストレージ アレイを選択し、セカンダリ ボリュームを選択して、リザーブ容量を確認します。

e. プライマリ ボリュームからセカンダリ ボリュームへの初回のデータ転送を開始します。ボリュームサイズによっては、この初回転送に数時間かかることがあります。

2. 初期同期の進捗状況を確認します。

a. Unified Managerで、ローカルアレイのSystem Managerを起動します。

b. System Managerで、ミラーリング操作のステータスを確認します。ミラーリングが完了すると、ミラーリングされたペアのステータスは「Optimal」になります。

3. 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変更したり、手動で実行したりできます。新しい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、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。

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、ミラーリング操作のステータスを確認します。ミラーリングが完了すると、ミラーリングされたペアのステータスは「Optimal」になります。2つのアレイは、通常の動作を通じ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. 必要に応じて、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提供する必要があります。

SANtricity Unified Managerのミラーリング用語について学ぶ

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。

期間	概要
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。
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を格納するコンテナです。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。
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、ミラーリングされたペアは常にミラー整合性グループに属します。書き込み操作はまずプライマリ ボリュームに対して実行され、次にセカンダリ ボリュームにレプリケートされます。ミラー整合性グループ内の各ミラーペアは、同じ同期設定を共有します。
プライマリ ボリューム	ミラーリングされたペアのプライマリボリュームは、ミラーリングされるソースボリュームです。
リモート ストレージ アレイ	リモートストレージアレイは通常、セカンダリサイトとして指定され、ミラーリング構成でデータのレプリカを保持するのが一般的です。
リザーブ容量	予約容量とは、あらゆるコピーサービス操作およびストレージオブジェクトに使用される、物理的に割り当てられた容量のことです。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。
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、セカンダリサイトに配置され、データの複製を保持します。
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間の初期同期時に発生します。通信の中断後にプライマリボリュームとセカンダリ ボリュームの同期が解除された場合にも、同期処理が行われます。通信リンクが再び機能すると、複製されていないデータはすべてセカンダリ ボリュームのストレージアレイに同期されます。

SANtricity Unified Managerでミラーリングを使用するための要件

ミラーリングを設定する場合は、次の要件に注意してください。

Unified Manager

- Web Services Proxyサービスが実行されている必要があります。
- Unified ManagerがHTTPS接続経由でローカル ホストで実行されている必要があります。
- Unified Managerは、ストレージアレイに対して有効なSSL証明書を表示している必要があります。Unified Managerを使用して、メニューの「証明書」[証明書管理]に移動することで、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

EF600/EF600CまたはEF300/EF300Cストレージアレイでは、同期ミラーリングは利用できません。

- 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 アレイ内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。（ストレージ アレイごとに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。
- リモート ストレージ アレイにセカンダリ ボリュームを作成するための十分な空き容量（ミラーリングするプライマリ ボリュームと同等以上）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 ポートを備え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 ポートを備え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。
- コントローラーにベースFCポートとホスト インターフェイス カード（HIC）FCポートの両方がある場合、最も番号の大きいポートはHIC上にあります。専用ポートにログインしているホストはすべてログアウトされ、ホストのログイン要求は一切受け付けられません。このポートへのI/O要求は、ミラーリング操作に参加しているコントローラからのみ受け付けられます。
- 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接続が確立されると、接続に最初に成功したポートがリモート 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、使用可能な残り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。

  E4000コントローラはiSCSIミラーリングをサポートしていません。

- iSCSIポートはアレイレベルでポート単位で設定されます。設定の通知やデータ転送などのコントローラ間の通信には、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 システムの両方が通信するには、同じ VLAN 設定である必要があります
  - iSCSIリスン 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。

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。

  EF600およびEF300のコントローラでは、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 ボリュームで、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。そうでない非同期ミラー 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。お使いのストレージ 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個のリザーブ容量ボリュームがボリュームの制限に含まれます。
- 非同期ミラーリングの場合、プライマリ ボリュームとセカンダリ ボリュームでドライブ セキュリティ機能が同じである必要があります。
  - プライマリ ボリュームがFIPS対応の場合、セカンダリ ボリュームもFIPS対応である必要があります。
  - プライマリ ボリュームがFDE対応の場合、セカンダリ ボリュームもFDE対応である必要があります。
  - プライマリ ボリュームがDrive Securityを使用していない場合は、セカンダリ ボリュームもDrive Securityを使用してはいけません。
- プライマリ ボリュームとセカンダリ ボリュームでは、リソース パーティショニングを有効にしてはなりません。

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：

- プライマリ ボリュームとセカンダリ ボリュームには、コントローラのリセットやその他の一時的な中断から復旧するための書き込み情報をログ記録するために、予約済み容量が必要です。
- 同期ミラーリングが有効になると、予約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 ボリュームの両方で予約容量が必要になるため、同期ミラー関係に参加している両方のストレージ アレイに十分な空き容量があることを確認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。

ミラーリングの設定

SANtricity Unified Managerで非同期ミラーペアを作成する

非同期ミラーリングを設定するには、ローカル アレイのプライマリ ボリュームとリモート アレイのセカンダリ ボリュームを含むミラー ペアを作成します。

開始する前に

ミラーペアを作成する前に、Unified Manager の以下の要件を満たしてください：

- 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は、ストレージアレイに対して有効なSSL証明書を表示している必要があります。Unified Managerを使用して、メニューの「証明書」[証明書管理]に移動することで、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 アレイ内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。（ストレージ アレイごとに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。
- リモート ストレージ アレイにセカンダリ ボリュームを作成するための十分な空き容量（ミラーリングするプライマリ ボリュームと同等以上）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。

タスク概要

非同期ミラー ペアを作成するプロセスは複数の手順で構成されます。

手順**1**：ミラー整合性グループを作成または選択する

この手順では、新しいミラー整合性グループを作成するか既存の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

1. *管理*ページから、ソースとして使用するローカルストレージアレイを選択します。
2. メニューの「Actions」→「Create Asynchronous Mirrored Pair」を選択します。

   非同期ミラー ペアの作成ウィザードが開きます。

3. 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、*既存のミラー整合性グループ*が選択されていることを確認してから、テーブル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。

   a. *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。
   b. 2つのストレージアレイ間でミラーリングされるボリューム上のデータを最もよく表す一意の名前を入力してください。名前は、文字、数字、および特殊文字であるアンダースコア（_）、ハイフン（-）、ハッシュ記号（#）のみで構成できます。名前は30文字以内とし、スペースを含めることはできません。
   c. ローカルストレージアレイとの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。

   > 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、パスワードを入力するように求められます。

d. 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 — このオプションを選択すると、このグループ内のすべてのミラーペアの同期を手動で開始できます。後で再同期を実行する場合は、プライマリストレージアレイのSystem Managerを起動し、メニューの Storage[Asynchronous Mirroring]を選択し、*Mirror Consistency Groups*タブからグループを選択してから、メニューの More[Manually resynchronize]を選択する必要があることに注意してください。
- 自動 — 前回の更新開始から次回の更新開始までの間隔を、分、時間、または*日*で選択します。例えば、同期間隔が30分に設定されていて、同期処理が午後4：00に開始された場合、次の処理は午後4：30に開始されます。

e. 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、3つのアラート方法として、特定の時間内に同期が完了していない場合、リモート アレイのリカバリ ポイント データが特定の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を設定できます。

4. 「次へ」を選択して、[手順2：プライマリボリュームを選択します]に移動します。

新しいミラー整合性グループを定義した場合、Unified Managerはまずローカルストレージアレイ上にミラー整合性グループを作成し、次にリモートストレージアレイ上にミラー整合性グループを作成します。各アレイのSystem Managerを起動することで、ミラー整合性グループを表示および管理できます。

Unified Managerがローカルストレージアレイ上にミラー整合性グループを正常に作成したが、リモートストレージアレイ上に作成できなかった場合、ローカルストレージアレイからミラー整合性グループを自動的に削除します。Unified Managerがミラー整合性グループの削除を試行中に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します

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画面には、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

1. 使用可能なボリュームの一覧から、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、*次へ*をクリックして予約容量を割り当てます。
2. 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。

- 予約容量のデフォルト設定は基本ボリューム容量の20%であり、通常はこの容量で十分です。パーセンテージを変更した場合は、*候補者を更新*をクリックしてください。
- 必要な容量は、プライマリ ボリュームへのI/O書き込みの頻度とサイズ、および容量を維持する必要がある期間によって異なります。
- 一般的に、以下の条件のいずれか、または両方が当てはまる場合は、予約容量としてより大きな容量

を選択してください：

- 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 ボリューム上のデータブロックの大部分が変更されます。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て、プライマリ ボリュームへの典型的なI/Oアクティビティを把握してください。

3. 「次へ」を選択して、ステップ3：セカンダリ ボリュームを選択しますに移動します。

ステップ3：セカンダリ ボリュームを選択します

このステップでは、ミラー関係で使用するセカンダリ ボリュームを選択し、その予約容量を割り当てます。リモートストレージアレイ上でセカンダリ ボリュームを選択すると、システムはそのミラーリングペアに使用可能なすべてのボリュームのリストを表示します。使用資格のないボリュームは、そのリストには表示されません。

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

1. 使用可能な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、*次へ*をクリックして予約容量を割り当てます。
2. 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。

   - 予約容量のデフォルト設定は基本ボリューム容量の20%であり、通常はこの容量で十分です。パーセンテージを変更した場合は、*候補者を更新*をクリックしてください。
   - 必要な容量は、プライマリ ボリュームへのI/O書き込みの頻度とサイズ、および容量を維持する必要がある期間によって異なります。
   - 一般的に、以下の条件のいずれか、または両方が当てはまる場合は、予約容量としてより大きな容量を選択してください：
     - 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 ボリューム上のデータブロックの大部分が変更されます。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て、プライマリ ボリュームへの典型的なI/Oアクティビティを把握してください。
3. 非同期ミラーリングシーケンスを完了するには、*Finish*を選択します。

結果

Unified Manager は以下の動作を実行します：

- 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の両方に、ミラーリングされたペア用の予約容量を作成します。

ミラーリングされるボリュームがシンボリュームの場合、初期同期中に、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量が削減されます。

SANtricity Unified Managerで同期ミラーペアを作成します

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。

この機能は、EF600/EF600CまたはEF300/EF300Cストレージ システムではご利用いただけません。

開始する前に

ミラーペアを作成する前に、Unified Manager の以下の要件を満たしてください：

- 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は、ストレージアレイに対して有効なSSL証明書を表示している必要があります。Unified Managerを使用して、メニューの「証明書」[証明書管理]に移動することで、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予定の2つのストレージアレイは、Unified Managerで検出されます。
- 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 アレイ内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。（ストレージ アレイごとに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。
- ローカルストレージアレイとリモートストレージアレイは、Fibre Channelファブリックを介して接続されています。
- 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。

タスク概要

同期ミラー ペアを作成するプロセスは複数の手順で構成されます。

ステップ**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画面には、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

1. *管理*ページから、ソースとして使用するローカルストレージアレイを選択します。
2. メニューの「アクション」→「同期ミラーペアの作成」を選択します。

   同期ミラー ペアの作成ウィザードが開きます。

3. 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。
4. 「次へ」を選択して、ステップ2：セカンダリ ボリュームを選択しますに移動します。

ステップ**2**：セカンダリ ボリュームを選択します

このステップでは、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上のセカンダリ ボリュームを選択すると、システムはそのミラーペアに使用可能なすべてのボリュームのリストを表示します。使用資格のないボリュームは、そのリストには表示されません。選択したボリュームは、ミラー関係においてセカンダリロールを保持します。

手順

1. ローカルストレージアレイとの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。

   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、パスワードを入力するように求められます。

   - ストレージ アレイは、リストに名前で表示されます。ストレージ アレイに名前を付けていない場合は、「unnamed」と表示されます。
   - 使用したいストレージアレイがリストにない場合は、Unified Managerで検出されていることを確認してください。

2. 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。

   セカンダリ ボリュームがプライマリ ボリュームよりも大きな容量で選択された場合、使用可能な容量はプライマリ ボリュームのサイズに制限されます。

3. 「次へ」をクリックして、[ステップ3：同期設定を選択する]に移動します。

ステップ**3**：同期設定を選択する

この手順では、通信中断後のデータの同期方法に関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

1. 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、サービス I/O 要求と比較して、初期同期および通信中断後の再同期操作を完了するためにシステムリソースがどれだけ使用されるかを決定します。

   このダイアログで設定された優先順位は、プライマリボリュームとセカンダリ ボリュームの両方に適用されます。プライマリボリュームのレートは、後でシステムマネージャを開き、メニュー：ストレージ[同期ミラーリング > その他 > 設定の編集]を選択することで変更できます。

同期優先度は5段階で設定できます。

- 最低
- 低
- 中
- 高
- 最高

同期優先度を最低レートに設定すると、I/Oアクティビティが優先され、再同期処理に時間がかかります。同期優先度を最高レートに設定すると、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が出る可能性があります。

2. リモートストレージアレイ上のミラーリングされたペアの再同期を、手動で行うか自動で行うかを選択してください。
   - **Manual**（推奨オプション）-- ミラーリングされたペアとの通信が復旧した後、同期を手動で再開する必要がある場合は、このオプションを選択してください。このオプションは、データ復旧のための最良の機会を提供します。
   - 自動 — このオプションを選択すると、ミラーリングされたペアとの通信が復旧した後、自動的に再同期が開始されます。

     同期を手動で再開するには、System Managerに移動し、メニューの Storage[Synchronous Mirroring]を選択し、テーブル内のミラーペアをハイライト表示して、*More*の下にある*Resume*を選択します。
3. **Finish** をクリックして、同期ミラーリングシーケンスを完了します。

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 リクエストは、ミラーペアのセカンダリ ボリュームのリモート優先コントローラ所有者からのみ受け入れられます。（プライマリボリュームでの予約は許可されます。）
- コントローラごとに1つずつ、合計2つの予約容量ボリュームを作成します。これらは、コントローラのリセットやその他の一時的な中断から復旧するための書き込み情報をログに記録するために使用されます。

  各ボリュームの容量は128 MiB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、各ボリュームに4 GiBが予約されます。

終了後の操作

System Managerに移動し、メニュー：Home[View Operations in Progress]を選択して、同期ミラーリング処理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。

SANtricity Unified Managerのストレージミラーリングに関するよくある質問

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

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の以下の要件を満たしてください：

- 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は、ストレージアレイに対して有効なSSL証明書を表示している必要があります。Unified Managerを使用して、メニューの「証明書」[証明書管理]に移動することで、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 アレイ内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。（ストレージ アレイごとに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。

> EF600/EF600CまたはEF300/EF300Cストレージ システムでは、同期ミラーリングは利用できません。

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 アレイ内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。（ストレージ アレイごとに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。
- リモート ストレージ アレイにセカンダリ ボリュームを作成するための十分な空き容量（ミラーリングするプライマリ ボリュームと同等以上）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 ポートを備え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 ポートを備えたコントローラでのみサポートされます。

> EF600/EF600CまたはEF300/EF300Cストレージ システムでは、同期ミラーリングは利用できません。

この割合を変更するのはどのような場合ですか**?**

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、ベースボリュームへの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操作を使用する予定期間によって異なります。一般的に、以下の条件のいずれか、または両方が当てはまる場合は、予約容量の割合を高く設定してください：

- 特定のストレージオブジェクトのコピーサービス操作の寿命が非常に長い場合。
- 大量のI/Oアクティビティにより、ベースボリューム上のデータブロックの大部分が変更される場合。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て、ベースボリュームへの典型的なI/Oアクティビティを把握してください。

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。

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。
- 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。

> EF600およびEF300のコントローラでは、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 ボリュームで、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。そうでない非同期ミラー 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。

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。

使用に適さないボリュームはリストには表示されません。次のいずれかに該当するボリュームは対応しない場合があります。

- 標準以外のボリューム（Snapshotボリュームなど）である。
- 最適状態でない。
- すでにミラー関係に参加している。
- （非同期ミラーリングの場合）シン ボリューム属性が、プライマリ ボリュームとセカンダリ ボリュームで一致しない。
- 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 ボリュームがDA対応の場合、セカンダリ ボリュームもDA対応である必要があります。
  - プライマリ ボリュームがDA有効になっていない場合、セカンダリ ボリュームもDA有効になっていてはいけません。
- 非同期ミラーリングの場合、プライマリ ボリュームとセカンダリ ボリュームでドライブ セキュリティ機能が同じである必要があります。
  - プライマリ ボリュームがFIPS対応の場合、セカンダリ ボリュームもFIPS対応である必要があります。
  - プライマリ ボリュームがFDE対応の場合、セカンダリ ボリュームもFDE対応である必要があります。
  - プライマリ ボリュームがDrive Securityを使用していない場合は、セカンダリ ボリュームもDrive Securityを使用してはいけません。

同期の優先順位は同期速度にどのような影響を与えますか？

同期優先度は、システム パフォーマンスに対して同期アクティビティにどれだけの処理時間を割り当てるかを定義します。

プライマリ ボリュームのコントローラ所有者が、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I/O書き込みと、セカンダリ ボリュームへの関連するリモート書き込みを処理します。再同期はコントローラの処理リソースをI/Oアクティビティから転用するため、ホスト アプリケーションのパフォーマンスに影響を与える可能性があります。

同期の優先順位付けにかかる時間や、同期の優先順位付けがシステムパフォーマンスに及ぼす影響を判断する際は、以下のガイドラインを参考にしてください。

指定できる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、再同期に時間がかかります。最高では再同期が優先されますが、システム パフォーマンスが低下する可能性があります。

次のガイドラインは、各優先度の大まかな違いを示しています。

完全同期の優先レート	最高同期率と比較した経過時間
最低	約8倍
低	約6倍
中	約3.5倍
高	約2倍

ボリューム サイズとホスト I/O レート負荷は、同期時間の比較に影響します。

手動同期ポリシーの使用が推奨されるのはなぜですか**?**

手動での再同期を推奨します。なぜなら、手動での再同期を行うことで、データ復旧の可能性を最大限に高める方法で再同期プロセスを管理できるからです。

自動再同期ポリシーを使用し、再同期中に断続的な通信問題が発生した場合、セカンダリ ボリュームのデータが一時的に破損している可能性があります。再同期が完了すると、データが修正されます。

証明書

証明書の概要

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、インターネット上での安全な通信のために、ウェブサイトやサーバー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す。証明書には2つのタイプがあります：_署名付き証明書_は認証局（CA）によって検証され、_自己署名証明書_は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ます。

詳細については、以下を参照してください。

- "証明書の仕組み"
- "証明書の用語"

証明書を設定するにはどうすればよいですか**?**

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、アレイ内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。

詳細については、以下を参照してください。

- "管理システムのCA署名証明書の使用"
- "アレイの証明書のインポート"

概念

SANtricity Unified Managerでの証明書の仕組み

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 ファイルであり、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

証明書は、ウェブ通信が暗号化された形式で、プライバシーが保護され、改ざんされることなく、指定されたサーバーとクライアント間でのみ送信されることを保証します。Unified Managerを使用すると、ホスト管理システム上のブラウザの証明書と、検出されたストレージアレイ内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確認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実現することもできます。

> CA署名証明書ではセキュリティ保護が強化されますが（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、自己署名証明書の場合、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、証明書の発行日と有効期限、エンティティの有効なドメイン、およびアルファベットと数字で構成されるデジタル署名が含まれています。

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、サイトがセキュリティで保護されていないことを示す警告がブラウザに表示されます。

CAは、申請プロセス中にユーザ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。申請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 — 階層構造の最上位にはルート証明書があり、これには他の証明書に署名するために使用される秘密鍵が含まれています。ルートは、特定のCA組織を識別するものです。すべてのネットワーク機器で同じCAを使用する場合は、ルート証明書は1つだけで済みます。
- 中間 — ルートから分岐するのは中間証明書です。CAは、保護されたルート証明書とサーバ証明書の間の仲介役として機能する、1つまたは複数の中間証明書を発行します。
- サーバ — チェーンの最下層にはサーバ証明書があり、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。ストレージアレイ内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で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によって「`trusted`」されません。自己署名証明書のみを含むウェブサイトに接続しようとするたびに、ブラウザは警告メッセージを表示します。警告メッセージ内のリンクをクリックしてウェブサイトに進む必要があります。そうすることで、実質的に自己署名証明書を承認したことになります。

Unified Manager の証明書

Unified Managerインターフェイスは、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。ブラウザを開いてUnified Managerに接続しようとすると、ブラウザはデジタル証明書を確認することで、ホストが信頼できるソースであることを検証しようとします。ブラウザがサーバのCA署名付き証明書を見つけられない場合、警告メッセージが表示されます。そこからWebサイトに進み、そのセッション用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から署名付きのデジタル証明書を取得すれば、警告メッセージが表示されなくなります。

コントローラの証明書

Unified Managerセッション中に、CA署名付き証明書を持た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場合があります。この場合、自己署名証明書を永続的に信頼するか、コントローラ用の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の受信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。

SANtricity Unified Managerの証明書の用語について学ぶ

証明書管理に関連する用語を次に示します。

期間	概要
CA	認証局（CA）は、インターネット セキュリティに関するデジタル電子文書（証明書と呼ばれる）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。
CSR	証明書署名要求（CSR）は、申請者から認証局（CA）に送信するメッセージです。CSRは、CAが証明書を発行するために必要な情報を検証します。
Certificate	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あり、攻撃者がサイトになりすますことを防ぎます。証明書には、サイト所有者に関する情報と、この情報を認証（署名）する信頼できる組織の身元情報が含まれています。
証明書チェーン	証明書にセキュリティ レイヤを追加するファイルの階層。通常、チェーンには1つのルート証明書（階層の最上位）、1つ以上の中間証明書、およびエンティティを識別するサーバ証明書が含まれています。

期間	概要
中間証明書	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。
キーストア	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。これらの鍵と証明書によって、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。
ルート証明書	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。
署名済み証明書	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。
自己署名証明書	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ています。自己署名証明書はCA署名証明書と同じ信頼チェーンを使用しないため、テスト環境で最もよく使用されます。「事前にインストールされている」証明書とも呼ばれます。
サーバ証明書	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。
信頼ストア	信頼ストアは、信頼できる第三者（CAなど）からの証明書を格納するリポジトリです。

管理システムの**CA**署名証明書の使用

SANtricity Unified Managerをホストする管理システムへの安全なアクセスのために、CA署名付き証明書を取得してインポートできます。

開始する前に

Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、証明書関連の機能は表示されません。

タスク概要

CA署名証明書を使用するには、次の3つの手順を実行します。

手順**1**：**CSR**ファイルを作成する

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。CSRファイルは組織、およびWeb Services ProxyとUnified Managerがインストールされているホスト システムを識別します。

> または、OpenSSLなどのツールを使用してCSRファイルを生成し、手順2：CSRファイルを送信するにスキップすることもできます。

手順

1. * Certificate Management * を選択します。
2. 「管理」タブから*CSRを完了する*を選択します。
3. 以下の情報を入力し、*次へ*をクリックします。
   - 組織名 — 貴社または貴団体の正式な法的名称。Inc. や Corp. などの接尾辞を含めます。
   - 組織単位（任意） — 証明書を取り扱う組織内の部門。
   - **City/Locality** — ホストシステムまたはビジネスが所在する都市。
   - 都道府県/地域（任意） — ホストシステムまたはビジネスが所在する都道府県または地域。
   - 国の**ISO**コード — USなど、あなたの国の2桁のISO（International Organization for Standardization）コード。
4. Web Services Proxyがインストールされているホスト システムについて、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するアドレスと完全に一致している必要があります。http://またはhttps://は含めないでください。DNS名はワイルドカードで始めることはできません。
   - 代替**IP**アドレス — 共通名がIPアドレスである場合、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任意で入力できます。複数の項目を入力する場合は、カンマ区切り形式を使用してください。
   - 代替**DNS**名 — 共通名がDNS名である場合は、ホストシステムの追加のDNS名を入力します。複数の項目を入力する場合は、カンマ区切り形式を使用してください。代替DNS名がない場合でも、最初のフィールドにDNS名を入力した場合は、その名前をここにコピーしてください。DNS名はワイルドカードで始めることはできません。
5. ホスト情報が正しいことを確認します。正しくないと、CAから受け取った証明書をインポートできません。
6. *完了*をクリックします。
7. 手順2：CSRファイルを送信するへ移動。

手順**2**：**CSR**ファイルを送信する

証明書署名要求（CSR）ファイルを作成したら、そのファイルを認証局（CA）に送信して、Unified ManagerとWeb Services Proxyをホストするシステムの署名済み管理証明書をリクエストします。

> Eシリーズシステムでは、署名付き証明書にPEM形式（Base64 ASCIIエンコーディング）が必要です。これには、.pem、.crt、.cer、.keyなどのファイルタイプが含まれます。

手順

1. ダウンロードしたCSRファイルの場所を確認します。

ダウンロード フォルダの場所は、ブラウザによって異なります。

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

> *CSRファイルをCAに送信した後は、別のCSRファイルを再生成しないでください。*CSRを生成するたびに、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存されます。署名済み証明書を受け取ってインポートすると、システムは秘密鍵と公開鍵の両方が元のペアであることを確認します。鍵が一致しない場合、署名済み証明書は機能しないため、CAに新しい証明書を要求する必要があります。

3. CAが署名済み証明書を返送したら、[手順3：管理証明書をインポートする]に移動します。

手順**3**：管理証明書をインポートする

認証局（CA）から署名済み証明書を受け取ったら、Web Services ProxyとUnified Managerインターフェイスがインストールされているホスト システムに証明書をインポートします。

開始する前に

- CAから署名済み証明書を受け取っておきます。これらのファイルには、ルート証明書、1つ以上の中間証明書、およびサーバ証明書が含まれます。
- 認証局が連鎖証明書ファイル（例えば、.p7bファイル）を提供した場合、その連鎖ファイルをルート証明書、1つ以上の中間証明書、およびサーバー証明書という個別のファイルに展開する必要があります。Windows `certmgr`ユーティリティ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：すべてのタスク[エクスポート]を選択）。Base-64エンコードを推奨します。エクスポートが完了すると、チェーン内の各証明書ファイルに対応するCERファイルが表示されます。
- Web Services Proxyが実行されているホスト システムに証明書ファイルをコピーしておきます。

手順

1. * Certificate Management * を選択します。
2. 「管理」タブから*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。

3. *Browse*をクリックして、まず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とともに作成された秘密鍵ファイルもインポートする必要があります。

   ファイル名がダイアログ ボックスに表示されます。

4. *インポート*をクリックします。

結果

ファイルがアップロードされて検証されます。[証明書管理]ページに証明書の情報が表示されます。

管理証明書のリセット

管理証明書を工場出荷時の自己署名証明書の状態に戻すことができます。

開始する前に

Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、証明書関連の機能は表示されません。

タスク概要

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

1. * Settings > Certificates *を選択します。
2. * Array Management * タブを選択し、* Reset * を選択します。

   [管理証明書のリセットの確認]ダイアログ ボックスが開きます。

3. フィールドに `reset`と入力し、*リセット*をクリックします。

   ブラウザをリフレッシュしたあとに、サイトがHTTP Strict Transport Securityを使用しているという理由で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る場合があります。この状況は自己署名証明書に戻した場合に発生します。問題を解決するには、ブラウザから閲覧データを削除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求められます。

アレイ証明書の使用

SANtricity Unified Managerでアレイの証明書をインポート

必要に応じて、ストレージアレイの証明書をインポートして、SANtricity Unified Managerをホストしているシステムで認証できるようにすることができます。証明書は、認証局（CA）によって署名される場合もあれば、自己署名される場合もあります。

開始する前に

- Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、証明書関連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

1. * Certificate Management * を選択します。
2. *Trusted*タブを選択します。

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

3. CA証明書をインポートするには、**Import › Certificates**を選択するか、自己署名証明書をインポートするには、**Import › Self-signed storage array certificates**を選択してください。

表示を絞り込むには、*Show certificates that are…*フィルタリングフィールドを使用するか、列見出しをクリックして証明書の行を並べ替えることができます。

4. ダイアログボックスで証明書を選択し、* Import *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。

SANtricity Unified Managerで信頼済み証明書を削除する

期限切れになった証明書など、不要になった証明書を削除することができます。

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ます。

> ルート証明書または中間証明書を削除する場合は、同じ証明書ファイルが共有されていることがあるため、複数のストレージ アレイに影響する可能性があることに注意してください。

手順

1. * Certificate Management * を選択します。
2. *Trusted*タブを選択します。
3. 表から1つ以上の証明書を選択し、*削除*をクリックします。

   > プリインストールされている証明書に対しては、*Delete*機能は利用できません。

   [信頼された証明書の削除の確認]ダイアログ ボックスが開きます。

4. 削除を確認し、* Delete * をクリックします。

   証明書が表から削除されます。

信頼されていない証明書の解決

信頼できない証明書は、ストレージアレイがSANtricity Unified Managerへのセキュアな接続を確立しようとしたときに、接続の安全性が確認できない場合に発生します。

[証明書]ページで信頼されていない証明書を解決するには、ストレージ アレイの自己署名証明書をインポートするか、信頼できる第三者機関が発行した認証局（CA）証明書をインポートします。

開始する前に

- Security Adminの権限を含むユーザ プロファイルでログインする必要があります。
- CA署名証明書をインポートする場合は次の準備が必要です。
  - ストレージ アレイの各コントローラの証明書署名要求（.CSRファイル）を生成してCAに送信しておく必要があります。
  - 信頼された証明書ファイルをCAから受け取っておきます。
  - 証明書ファイルがローカル システム上にある必要があります。

タスク概要

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. * Certificate Management * を選択します。
2. *Trusted*タブを選択します。

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

3. CA証明書をインポートする場合はメニュー：インポート[証明書]を選択し、自己署名証明書をインポートする場合はメニュー：インポート[自己署名ストレージアレイ証明書]を選択します。

   表示を絞り込むには、*Show certificates that are…*フィルタリングフィールドを使用するか、列見出しをクリックして証明書の行を並べ替えることができます。

4. ダイアログボックスで証明書を選択し、* Import *をクリックします。

   証明書がアップロードされて検証されます。

証明書の管理

証明書の表示

証明書を使用している組織、発行元の機関、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。

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、証明書関連の機能は表示されません。

手順

1. * Certificate Management * を選択します。
2. 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しているシステムの証明書を表示します。管理証明書は、自己署名式または認証局（CA）による承認式のいずれかを選択できます。これにより、Unified Managerへの安全なアクセスが可能になります。
   - 信頼済み — Unified Manager がストレージ アレイやその他のリモート サーバー（LDAPサーバなど）にアクセスするために使用できる証明書を表示します。証明書は認証局（CA）から発行することも、自己署名することも可能です。
3. 証明書に関する詳細情報を表示するには、該当する行を選択し、行末尾の省略記号を選択してか

ら、*View*または*Export*をクリックします。

SANtricity Unified Managerで証明書をエクスポート

証明書をエクスポートして詳細を確認することができます。

開始する前に

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

手順

1. * Certificate Management * を選択します。
2. 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しているシステムの証明書を表示します。管理証明書は、自己署名式または認証局（CA）による承認式のいずれかを選択できます。これにより、Unified Managerへの安全なアクセスが可能になります。
   - 信頼済み — Unified Manager がストレージ アレイやその他のリモート サーバー（LDAPサーバなど）にアクセスするために使用できる証明書を表示します。証明書は認証局（CA）から発行することも、自己署名することも可能です。
3. 証明書をページから選択し、行の最後にある省略記号をクリックします。
4. * Export * をクリックし、証明書ファイルを保存します。
5. 証明書ビューア アプリケーションでファイルを開きます。

アクセス管理

SANtricity Unified Managerのアクセス管理について学ぶ

アクセス管理は、SANtricity Unified Managerでユーザ認証を設定する方法です。

使用可能な認証方式にはどのようなものがありますか?

次の認証方式を使用できます。

- ローカルユーザロール — 認証はRBAC（ロールベースのアクセス制御）機能を通じて管理されます。ローカルユーザロールには、特定のアクセス権限を持つ事前定義されたユーザプロファイルとロールが含まれます。
- ディレクトリサービス — ユーザ認証は、LDAP（Lightweight Directory Access Protocol）サーバと、MicrosoftのActive Directoryなどのディレクトリサービスを介して管理されます。
- **SAML** — 認証は、SAML 2.0 を使用する ID プロバイダー（IdP）を介して管理されます。

詳細については、以下を参照してください。

- "アクセス管理の仕組み"
- "アクセス管理の用語"
- "マッピングされたロールの権限"

- "SAML"

アクセス管理を設定するにはどうすればよいですか?

SANtricityソフトウェアは、ローカル ユーザ ロールを使用するように事前に設定されています。LDAPを使用する場合は[アクセス管理]ページで設定できます。

詳細については、以下を参照してください。

- "ローカル ユーザ ロールを使用したアクセス管理"
- "ディレクトリ サービスを使用したアクセス管理"
- "SAMLの設定"

概念

SANtricity Unified Managerでのアクセス管理の仕組み

SANtricity Unified ManagerでAccess Managementを使用してユーザ認証を確立します。

設定ワークフロー

アクセス管理設定は次のように行います。

1. 管理者は、Security admin権限を含むユーザープロファイルを使用してUnified Managerにログインします。

   初回ログイン時のユーザ名 `admin`は自動的に表示されるため、変更できません。 `admin` ユーザはシステム内のすべての機能に完全にアクセスできます。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。

2. 管理者はユーザインターフェイスのアクセス管理に移動します。そこには、事前に設定されたローカルユーザロールが含まれています。これらのロールは、RBAC（ロールベースのアクセス制御）機能の実装です。
3. 次の認証方式を1つ以上設定します。
   - ローカルユーザロール — 認証はRBAC機能によって管理されます。ローカルユーザロールには、特定のアクセス権限を持つ事前定義されたユーザと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認証の唯一の方法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、設定は必要ありません。
   - ディレクトリサービス — 認証は、LDAP（Lightweight Directory Access Protocol）サーバと、MicrosoftのActive Directoryなどのディレクトリサービスを介して管理されます。管理者はLDAPサーバに接続し、LDAPユーザをローカルユーザロールにマッピングします。
   - **SAML** — 認証は、Security Assertion Markup Language（SAML）2.0を使用するIdentity Provider（IdP）を介して管理されます。管理者は、IdPシステムとストレージアレイ間の通信を確立し、IdPユーザを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マッピングします。
4. 管理者は、Unified Managerのログイン クレデンシャルをユーザに提供します。
5. 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がユーザ アカウントと照合して認証されます。
- 割り当てられたロールに基づいてユーザの権限が決定されます。
- 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なります。
- 上部のバナーにユーザ名が表示されます。

Unified Managerで利用可能な機能

アクセスできる機能は、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完全な読み取り / 書き込み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できません。
- セキュリティ管理者 — アクセス管理および証明書管理のセキュリティ設定へのアクセス。
- サポート管理者 — 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へのアクセス権はありません。
- **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、セキュリティ構成へのアクセスはできません。

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。

SANtricity Unified Managerのアクセス管理の用語について学ぶ

アクセス管理の用語がSANtricity Unified Managerにどのように適用されるかを学びましょう。

期間	概要
Active Directory	Active Directory（AD）は、MicrosoftのWindowsドメイン ネットワーク用のLDAPを使用したディレクトリ サービスです。
バインド	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。
CA	認証局（CA）は、インターネット セキュリティに関するデジタル電子文書（証明書と呼ばれる）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。
Certificate	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あり、攻撃者がサイトになりすますことを防ぎます。証明書には、サイト所有者に関する情報と、この情報を認証（署名）する信頼できる組織の身元情報が含まれています。
LDAP	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。LDAPを使用して、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、ユーザを検証することができます。

期間	概要
RBAC	ロールベースアクセス制御（RBAC）は、個々のユーザーのロールに基づいてコンピュータまたはネットワーク リソースへのアクセスを制御する方法です。Unified Managerには、事前定義されたロールが含まれています。
SAML	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（パスワードと指紋など）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、SAML 2.0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。
SSO	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。
Web Services Proxy	標準的なHTTPSメカニズムを介してアクセスを提供するWeb Services Proxyを使用すると、管理者はストレージアレイの管理サービスを構成できます。プロキシはWindows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で利用できます。

マッピングされたロールの権限

RBAC（ロールベースアクセス制御）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ユーザが含まれます。各ロールには、SANtricity Unified Managerのタスクにアクセスするための権限が含まれています。

各ロールは、次のタスクへのアクセスを提供します。

- * Storage admin * — アレイ上のストレージオブジェクトへの完全な読み取り / 書き込み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できません。
- セキュリティ管理者 — アクセス管理および証明書管理のセキュリティ設定へのアクセス。
- サポート管理者 — 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へのアクセス権はありません。
- **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、セキュリティ構成へのアクセスはできません。

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状態になるか、ユーザ インターフェイスに表示されません。

SANtricity Unified Managerでのローカルユーザーロールによるアクセス管理

管理者は、SANtricity Unified Managerで実施されるRBAC（ロールベースのアクセス制御）機能を使用できます。これらの機能は「ローカルユーザロール」と呼ばれます。

設定ワークフロー

ローカル ユーザ ロールはシステムで事前に設定されています。認証にローカル ユーザ ロールを使用するための手順は次のとおりです。

1. 管理者は、Security admin権限を含むユーザープロファイルを使用してUnified Managerにログインします。

`admin`ユーザには、システム内のすべての機能へのフルアクセス権があります。

2. ユーザ プロファイルを確認します。ユーザ プロファイルは事前に定義されており、変更できません。
3. 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。
4. 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。

- パスワードを変更する。
- パスワードの最小文字数を設定する。
- パスワードなしでログインできるようにユーザに許可する。

SANtricity Unified Managerにおけるディレクトリサービスによるアクセス管理

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 サービスを使用している場合の設定は次のようになります。

1. 管理者は、Security admin権限を含むユーザープロファイルを使用してUnified Managerにログインします。

`admin`ユーザには、システム内のすべての機能へのフルアクセス権があります。

2. 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。
3. 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。
4. 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、変更することはできません。
5. 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。
6. 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で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 サーバを追加する。
- ディレクトリ サーバの設定を編集する。
- 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。
- パスワードを変更する。
- パスワードの最小文字数を設定する。
- パスワードなしでログインできるようにユーザに許可する。

SANtricity Unified ManagerでのSAMLを使用したアクセス管理

アクセス管理に関しては、管理者はアレイに組み込まれているSecurity Assertion Markup Language（SAML）2.0の機能を使用できます。

設定ワークフロー

SAML設定は次のように行います。

1. 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。

> `admin`ユーザには、System Managerのすべての機能へのフルアクセス権があります。

2. 管理者は、アクセス管理の下にある **SAML** タブに移動します。
3. 管理者は、IDプロバイダー（IdP）との通信を設定します。IdPは、ユーザーから認証情報を要求し、ユーザーが正常に認証されたかどうかを判断するために使用される外部システムです。ストレージアレイとの通信を設定するには、管理者は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。
4. 管理者は、サービスプロバイダーと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ー認可を制御します。この場合、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として機能します。通信を設定するには、管理者はUnified Managerを使用して、コントローラ用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。管理者は、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。

> 管理者は、IdPが認証時に名前IDを返す機能をサポートしていることを確認する必要もあります。

5. 管理者は、ストレージアレイのロールを、IdPで定義された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Unified Managerを使用してマッピングを作成します。
6. 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。

SAMLを有効にすると、ユーザインターフェイスから無効にすることはできませんし、IdP設定を編集することもできません。SAML設定を無効化または編集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。

7. Unified Managerから、ストレージ アレイのSAMLを有効にします。
8. 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

SAML を使用して認証を行う場合、管理者は次の管理タスクを実行できます：

- 新しいロール マッピングの変更または作成
- Service Providerファイルのエクスポート

アクセス制限

SAMLが有効な場合、ユーザはそのアレイのストレージを従来のStorage Managerの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たログイン

ローカル ユーザ ロールの使用

ローカル ユーザ ロールの表示

「ローカルユーザーロール」タブでは、ユーザーとデフォルトロールのマッピングを確認できます。これらのマッピングは、SANtricity Unified ManagerのWebサービスプロキシで適用されるRBAC（ロールベースのアクセス制御）の一部です。

開始する前に

Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、アクセス管理の機能は表示されません。

タスク概要

ユーザとマッピングは変更できません。変更できるのはパスワードのみです。

手順

1. *アクセス管理*を選択します。
2. *ローカルユーザーロール*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。
- ストレージ — すべてのストレージ プロビジョニングを管理する管理者。このユーザには、ストレージ管理、サポート管理、および監視という役割が含まれています。
- **security** — アクセス管理や証明書管理を含むセキュリティ設定を担当するユーザ。このユーザには、Security AdminおよびMonitorのロールが含まれます。
- **support** — ハードウェアリソース、障害データ、ファームウェアのアップグレードを担当するユーザ。このユーザには、Support AdminとMonitorという役割が含まれています。
- **monitor** — システムへの読み取り専用アクセス権を持つユーザ。このユーザにはMonitorロールのみが含まれます。
- **rw** （読み取り / 書き込み） — このユーザには、Storage Admin、Support Admin、およびMonitorのロールが含まれます。
- **ro** （読み取り専用） — このユーザには Monitor ロールのみが含まれます。

SANtricity Unified Managerでローカルユーザープロファイルのパスワードを変更する

[アクセス管理]で各ユーザのユーザ パスワードを変更できます。

開始する前に

- ローカル管理者としてログインする必要があります。これにはRoot管理者権限が含まれます。
- ローカル管理者のパスワードを確認しておきます。

タスク概要

パスワードを決める際は、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 パスワードは現在の最小文字数の設定（[設定の表示 / 編集]）以上にする必要があります。
- パスワードでは大文字と小文字が区別されます。
- パスワードの末尾のスペースは削除されません。設定時に末尾にスペースを含めた場合は、入力時に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、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. *アクセス管理*を選択します。
2. *ローカルユーザーロール*タブを選択します。
3. 表からユーザを選択します。

   パスワード変更ボタンが有効になります。

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できます。
6. 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。
7. この操作を確定するには、ローカル管理者パスワードを入力し、*変更*をクリックしてください。

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。

SANtricity Unified Managerでローカルユーザのパスワード設定を変更する

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。

開始する前に

ローカル管理者としてログインする必要があります。これにはRoot管理者権限が含まれます。

タスク概要

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

1. *アクセス管理*を選択します。
2. *ローカルユーザーロール*タブを選択します。
3. *View/Edit Settings*を選択します。

   ローカル ユーザー パスワード設定ダイアログ ボックスが開きます。

4. 次のいずれかを実行します。
   - ローカルユーザー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には、「すべてのローカルユーザーのパスワードを少なくとも」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 パスワードを対象に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 パスワードに対して最低文字数を設定する]チェック ボックスをオンにし、スピン ボックスで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。

5. *保存*をクリックします。

ディレクトリ サービスの使用

SANtricity Unified Managerでディレクトリサーバを追加

アクセス管理の認証を設定するには、LDAPサーバと、SANtricity Unified Manager用のWeb Services Proxyを実行しているホストとの間の通信を確立します。次に、LDAPユーザ グループをローカル ユーザ ロールにマッピングします。

開始する前に

- Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、アクセス管理の機能は表示されません。
- ユーザグループはディレクトリサービス内で定義する必要があります。
- LDAPサーバの認証情報（ドメイン名、サーバURL、および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を含む）が必要です。
- 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。

タスク概要

ディレクトリ サーバの追加は2段階のプロセスです。最初に、ドメイン名とURLを入力します。サーバでセキュアなプロトコルを使用していて、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。その後、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

1. *アクセス管理*を選択します。
2. **Directory Services** タブから **Add Directory Server** を選択します。

   「ディレクトリサーバの追加」ダイアログボックスが開きます。

3. * 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

設定	概要
設定	ドメイン
LDAPサーバのドメイン名を入力します。複数のドメインを指定する場合は、ドメインをカンマ区切りのリストで入力します。ドメイン名は、ログイン（*username@domain*）で使用され、認証先のディレクトリサーバを指定します。	サーバ URL
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。	証明書のアップロード（オプション）
このフィールドは、上記の[サーバ URL]フィールドでLDAPSプロトコルを指定した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できる証明書または証明書チェーンです。	バインド アカウント（オプション）

設定	概要
LDAPサーバに対する検索クエリおよびグループ内の検索用の読み取り専用ユーザアカウントを入力します。アカウント名はLDAP形式で入力してください。たとえば、バインドユーザが「bindacct」という名前の場合、`CN=bindacct,CN=Users,DC=cpoc,DC=local`のような値を入力します。	バインド パスワード（オプション）
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。	追加する前にサーバ接続をテストする
システムが入力したLDAPサーバ設定と通信できることを確認する場合は、このチェックボックスを選択します。テストは、ダイアログボックスの下部にある*追加*をクリックした後に実行されます。 このチェックボックスを選択した場合、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。	権限設定

設定	概要
検索ベース DN	ユーザを検索するLDAPコンテキストを入力します。通常は `CN=Users, DC=cpoc, DC=local`の形式です。
ユーザ名属性	認証用のユーザIDにバインドされた属性を入力します。例えば：`sAMAccountName`
グループ属性	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。例えば：`memberOf, managedObjects`

4. * ロール マッピング * タブをクリックします。
5. 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

設定	概要
マッピング	グループDN
マッピングするLDAPユーザーグループのグループ識別名（DN）を指定します。正規表現がサポートされています。これらの特殊な正規表現文字は、正規表現パターンの一部でない場合はバックスラッシュ（\）でエスケープする必要があります：\.[]{}()<>*+-=!?^$	
ロール	フィールドをクリックし、グループDNにマッピングするローカルユーザーロールのいずれかを選択します。このグループに含める各ロールは個別に選択する必要があります。SANtricity Unified Managerにログインするには、Monitorロールを他のロールと組み合わせて使用する必要があります。マッピングされたロールには、次の権限が含まれます： • * Storage admin * — アレイ上のストレージオブジェクトへの完全な読み取り / 書き込み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できません。 • セキュリティ管理者 — アクセス管理および証明書管理のセキュリティ設定へのアクセス。 • サポート管理者 — 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へのアクセス権はありません。 • **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、セキュリティ構成へのアクセスはできません。

Monitorロールは、管理者を含むすべてのユーザに必要です。

6. 必要に応じて、*別のマッピングを追加*をクリックして、グループと役割のマッピングをさらに入力してください。
7. マッピングが完了したら、*Add*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。

SANtricity Unified Managerでディレクトリサーバの設定とロールマッピングを編集します

アクセス管理でディレクトリ サーバを設定済みの場合、その設定をいつでも変更することができます。設定には、サーバ接続情報とグループとロールのマッピングが含まれます。

開始する前に

- Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、アクセス管理の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

1. *アクセス管理*を選択します。
2. *Directory Services*タブを選択します。
3. 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。
4. *View/Edit Settings*を選択します。

   ディレクトリサーバ設定ダイアログボックスが開きます。
5. *Server Settings*タブで、必要な設定を変更します。

フィールドの詳細

設定	概要
設定	ドメイン
LDAPサーバのドメイン名。複数のドメインを指定する場合は、カンマで区切って入力してください。ドメイン名は、ログイン時（*username@domain*）に使用され、認証を行うディレクトリサーバを指定します。	サーバ URL
LDAPサーバにアクセスするためのURLの形式は `ldap[s]://host:port`です。	バインド アカウント（オプション）
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。	バインド パスワード（オプション）
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）。	保存する前にサーバ接続をテストする
システムがLDAPサーバ構成と通信できることを確認します。テストは*保存*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が選択されていて、テストが失敗した場合、設定は変更されません。エラーを解決するか、チェックボックスをオフにしてテストをスキップし、設定を再編集する必要があります。	権限設定

設定	概要
検索ベース DN	ユーザーを検索するためのLDAPコンテキストは、通常、次の形式で提供されます `CN=Users, DC=cpoc, DC=local`。
ユーザ名属性	認証用のユーザIDにバインドされた属性。例えば： `sAMAccountName`
グループ属性	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。例えば： `memberOf, managedObjects`

6. *ロールマッピング*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

設定	概要
マッピング	グループDN
マッピングするLDAPユーザ グループのドメイン名。正規表現を使用できます。次の特殊文字を正規表現のパターン以外で使用する場合は、バックスラッシュ（\）でエスケープする必要があります。 \.[]{}()<>*+-=!?^$	
ロール	グループDNにマッピングされるロール。このグループに含めるロールは、それぞれ個別に選択する必要があります。SANtricity Unified Managerにログインするには、Monitorロールを他のロールと組み合わせて使用する必要があります。ロールには次のものが含まれます： • * Storage admin * — アレイ上のストレージオブジェクトへの完全な読み取り / 書き込み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できません。 • セキュリティ管理者 — アクセス管理および証明書管理のセキュリティ設定へのアクセス。 • サポート管理者 — 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へのアクセス権はありません。 • **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、セキュリティ構成へのアクセスはできません。

Monitorロールは、管理者を含むすべてのユーザに必要です。

7. 必要に応じて、*別のマッピングを追加*をクリックして、グループと役割のマッピングをさらに入力してください。
8. *保存*をクリックします。

結果

このタスクが完了すると、アクティブなユーザーセッションはすべて終了します。現在のユーザーセッションのみが保持されます。

ディレクトリ サーバの削除

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切断するには、[アクセス管

理]ページでサーバ情報を削除します。このタスクは、新しいサーバの設定が完了して古いサーバを削除する場合などに実行します。

開始する前に

Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、アクセス管理の機能は表示されません。

タスク概要

このタスクが完了すると、アクティブなユーザーセッションはすべて終了します。現在のユーザーセッションのみが保持されます。

手順

1. *アクセス管理*を選択します。
2. *Directory Services*タブを選択します。
3. 削除するディレクトリ サーバをリストから選択します。
4. *削除*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。

5. フィールドに `remove`と入力し、*削除*をクリックします。

   ディレクトリ サーバ設定、権限設定、ロール マッピングが削除されます。ユーザは、以降このサーバからのクレデンシャルを使用してログインすることはできません。

SAMLの使用

SANtricity Unified ManagerでSAMLを設定

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。認証を設定すると、アイデンティティ プロバイダとストレージ プロバイダの間の接続が確立されます。

開始する前に

- Security Adminの権限を含むユーザ プロファイルでログインする必要があります。そうしないと、アクセス管理の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、Unified Managerへのアクセスに使用するローカル システムで使用できるようにしておきます。

タスク概要

IDプロバイダー（IdP）とは、ユーザーから認証情報を要求し、そのユーザーが正常に認証されたかどうかを判断するために使用される外部システムです。IdPは、多要素認証を提供するように構成でき、Active Directoryなどの任意のユーザーデータベースを利用できます。セキュリティチームは、IDプロバイダー（IdP）の維持管理を担当します。サービスプロバイダー（SP）は、ユーザ認証とアクセスを制御するシステムです。アクセス管理がSAMLで構成されている場合、ストレージアレイは、IDプロバイダーに認証を要求するためのサービスプロバイダーとして機能します。IdPとストレージアレイ間の接続を確立するには、これら2つのエンティティ間でメタデータファイルを共有します。次に、IdPユーザーエンティティをストレージアレイの役割にマッピングします。最後に、SAMLを有効にする前に、接続とSSOログインのテストを行います。

SAMLおよび**Directory Services**。認証方法としてDirectory Servicesが設定されている場合にSAMLを有効にすると、Unified ManagerではSAMLがDirectory Servicesよりも優先されます。後でSAMLを無効にすると、Directory Servicesの設定は以前の設定に戻ります。

*編集と無効化*SAMLを有効にすると、ユーザインターフェイスから無効にすることはできませんし、IdPの設定を編集することもできません。SAML設定を無効化または編集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認証の設定プロセスは複数の手順で構成されます。

ステップ**1**：**IdP**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の接続情報を渡すために、Unified 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。

手順

1. メニューの「設定」→「アクセス管理」を選択します。
2. * SAML * タブを選択します。

   設定手順の概要が表示されます。

3. * Import Identity Provider（IdP）file *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。

4. * 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。

5. *インポート*をクリックします。

ステップ**2**：**Service Provider**ファイルのエクスポート

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

1. * Export Service Provider files * リンクをクリックします。

[サービス プロバイダ ファイルのエクスポート]ダイアログ ボックスが開きます。

2. *Controller A*フィールドにコントローラのIPアドレスまたはDNS名を入力し、*Export*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、Service Provider 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。ファイルの保存場所をメモしておいてください。

3. 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 プロバイダのメタデータ ファイルを探します。
4. 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

Unified Managerへのアクセスをユーザに許可するために、IdPユーザの属性とグループ メンバーシップをストレージ アレイの事前定義されたロールにマッピングする必要があります。

開始する前に

- IdP管理者が、IdPシステムでユーザの属性とグループ 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にインポートしておきます。
- 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

1. *Unified Managerの役割のマッピング*については、こちらのリンクをクリックしてください。

   ロールマッピングダイアログボックスが開きます。

2. 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

設定	概要
マッピング	ユーザ属性
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。	属性値
マッピングするグループの属性値を指定します。正規表現がサポートされています。正規表現パターンの一部でない場合は、次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：\.[]{}()<>*+-=!?^$	
ロール	フィールド内をクリックし、属性にマッピングするストレージ アレイのロールを1つ選択します。マッピングするロールを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ロールをマッピング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）へのフル読み取り / 書き込みアクセスは可能ですが、セキュリティ構成へのアクセスはできません。 • **Security admin** — Access Managementのセキュリティ設定、証明書管理、監査ログ管理へのアクセス、およびレガシー管理インターフェイス（SYMbol）のオン/オフを切り替える機能。 • サポート管理者 — 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、MELイベント、およびコントローラファームウェアの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へのアクセス権はありません。 • **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、セキュリティ構成へのアクセスはできません。

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、Unified Managerは正常に動作しません。

3. 必要に応じて、*別のマッピングを追加*をクリックして、グループと役割のマッピングをさらに入力して

ください。

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。

4. マッピングが完了したら、*保存*をクリックします。

ステップ4：SSOログインのテスト

IdPシステムとストレージ アレイが通信できることを確認するために、必要に応じてSSOログインをテストできます。このテストは、SAMLを有効にする最後の手順でも実行します。

開始する前に

- IdPのメタデータ ファイルをUnified Managerにインポートしておきます。
- 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

1. *Test SSO Login*リンクを選択します。

   SSOクレデンシャルの入力を求めるダイアログ ボックスが開きます。

2. 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中であることを示すダイアログ ボックスが開きます。

3. 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。

   テストに失敗した場合は、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は正しいです。

ステップ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。

開始する前に

- IdPのメタデータ ファイルをUnified Managerにインポートしておきます。
- 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。

*編集と無効化*SAMLを有効にすると、ユーザインターフェイスから無効にすることはできませんし、IdPの設定を編集することもできません。SAML設定を無効化または編集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

1. **SAML** タブから、 **Enable SAML** リンクを選択します。

   [SAML の有効化の確認]ダイアログ ボックスが開きます。

2. 入力 `enable`し、*有効にする*をクリックします。
3. 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。

SANtricity Unified Managerでの**SAML**ロールマッピングの変更

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。

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、アクセス管理の機能は表示されません。
- IdP管理者が、IdPシステムでユーザの属性とグループ 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

1. メニューの「設定」→「アクセス管理」を選択します。
2. * SAML * タブを選択します。
3. **Role Mapping** を選択します。

   ロールマッピングダイアログボックスが開きます。

4. 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。

   > SAMLが有効になっている間は権限を削除しないようにしてください。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

設定	概要
マッピング	ユーザ属性
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。	属性値
マッピングするグループの属性値を指定します。	ロール

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、Unified Managerは正常に動作しません。

5. 必要に応じて、*別のマッピングを追加*をクリックして、グループと役割のマッピングをさらに入力できます。
6. *保存*をクリックします。

結果

このタスクが完了すると、アクティブなユーザーセッションはすべて終了します。現在のユーザーセッションのみが保持されます。

SANtricity Unified ManagerでSAMLサービスプロバイダファイルをエクスポート

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。

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、アクセス管理の機能は表示されません。
- SAMLを設定して有効にします。

タスク概要

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

1. メニューの「設定」→「アクセス管理」を選択します。
2. * SAML * タブを選択します。

3. *エクスポート*を選択します。

   [サービス プロバイダ ファイルのエクスポート]ダイアログ ボックスが開きます。

4. * Export * 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。

   ドメイン名の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ておいてください。

5. 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 プロバイダのメタデータ ファイルを探します。
6. 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か、コントローラ情報を手動で入力できます。
7. 閉じる をクリックします。

SANtricity Unified Managerのユーザアクセス管理に関するFAQ

質問に対する簡単な回答をお探しの場合は、このFAQが役立ちます。

ログインできない理由は何ですか?

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。

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間違っている。
- 必要な権限がない。
- ログインが複数回失敗したために、ロックアウトされた。この場合は、10分待ってから再度ログインしてください。
- SAML認証が有効化された。この場合は、ブラウザをリフレッシュしてからログインしてください。

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?

アクセス管理でディレクトリ サーバを追加する際は、一定の要件を満たしている必要があります。

- ユーザグループはディレクトリサービス内で定義する必要があります。
- LDAPサーバの認証情報（ドメイン名、サーバURL、および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を含む）が必要です。
- 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。

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?

グループをロールにマッピングする際は、次のガイドラインに注意してください。

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完全な読み取り / 書き込み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できません。
- セキュリティ管理者 — アクセス管理および証明書管理のセキュリティ設定へのアクセス。
- サポート管理者 — 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へのアクセス権はありません。
- **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、セキュリティ構成へのアクセスはできません。

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 アレイに搭載されたSecurity Assertion Markup Language（SAML）機能を使用する場合は、次のこと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把握しておきます。
- マッピング対象グループの属性値は分かっている。正規表現がサポートされています。これらの特殊な正規表現文字は、正規表現パターンの一部でない場合、バックスラッシュ(`\`でエスケープする必要があります：

```
\.[]{}()<>*+-=!?^$|
```

- 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、Unified Managerは正常に動作しません。

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**?**

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、次の点を確認します。

- ネットワーク内にIDプロバイダー（IdP）が設定されています。IdPは、ユーザーから認証情報を要求し、ユーザーが正常に認証されたかどうかを判断するために使用される外部システムです。セキュリティチームは、IdPの維持管理を担当します。
- 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、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きます。

- SAMLを有効にすると、ユーザインターフェイスから無効にすることは_できません_し、IdP設定を編集することもできません。SAML設定を無効化または編集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。最終設定手順でSAMLを有効にする前に、SSOログインのテストを行うことをお勧めします。（システムはSAMLを有効にする前にSSOログインテストも実行します。）
- 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たログイン

ローカル ユーザとは何ですか**?**

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 ユーザには次のものがあります。

- **admin** — システム内のすべての機能にアクセスできるスーパー管理者。このユーザにはすべてのロールが含まれます。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管理する管理者。このユーザには、Storage Admin、Support Admin、およびMonitorのロールが含まれます。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** — アクセス管理および証明書管理を含むセキュリティ設定を担当するユーザ。このユーザには、Security AdminおよびMonitorのロールが含まれます。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、ファームウェアのアップグレードを担当するユーザ。このユーザには、Support AdminおよびMonitorのロールが含まれます。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。このユーザにはMonitorロールのみが含まれます。パスワードが設定されるまで、このアカウントは無効になっています。
- **rw**（読み取り / 書き込み）-- このユーザには、Storage Admin、Support Admin、およびMonitorのロールが含まれます。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） — このユーザには Monitor ロールのみが含まれます。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。

以前のバージョン

以前のバージョンのEシリーズ ハードウェアとSANtricityソフトウェアのドキュメントには、以下のリンクからアクセスできます。リンクをクリックすると、別のドキュメントサイトに移動します。

以前のリリースのハードウェア ドキュメント

- "E2712、E2724、E5612、E5624コントローラドライブトレイ、およびDE1600、DE5600拡張ドライブトレイを取り付けます"
- "E2760および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取り付けます"
- "EF560フラッシュアレイとDE5600フラッシュ拡張トレイを設置する"
- "古いシステムをインストールする"
- "古いシステムを維持する"
- "E2600およびE2700に2つ目のコントローラを追加する"
- "ホストプロトコルを変更または追加する"
- "AC電力をDC電力に変換する"
- "コントローラアップグレードガイド - 従来の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

- "System Managerヘルプ"
- "Unified Manager のヘルプ"

SANtricityリリース11.7

- "System Managerヘルプ"
- "Unified Manager のヘルプ"

SANtricityリリース11.6

- "System Managerヘルプ"
- "Unified Manager のヘルプ"

SANtricityリリース11.5

- "System Managerヘルプ"

SANtricityリリース11.4

- "Array Management Window（E2700、E5600/EF560）ヘルプ"
- "EMW（E2700、E5600/EF560）ヘルプ"

法律上の表示

法的通知から、著作権情報、商標、特許などを確認できます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp、NetAppのロゴ、NetAppの商標一覧のページに掲載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

特許

現在NetAppが所有する特許の一覧は以下のページから閲覧できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

プライバシー ポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

オープンソース

通知ファイルは、NetAppソフトウェアで使用されるサードパーティの著作権とライセンスに関する情報を提供します。

"EシリーズおよびEFシリーズSANtricity OSに関する通知"

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

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

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

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。