システム
SANtricity 11.5

NetApp
February 12, 2024

目次

システム

ストレージアレイの設定

概念

キャッシュの設定とパフォーマンス

キャッシュメモリは、ドライブメディアよりも速くアクセスできる、コントローラ上の一時的な揮発性ストレージ領域です。

キャッシュを使用すると、全体的なI/Oパフォーマンスを次のように向上させることができます。

- 読み取り用にホストから要求されたデータが以前の処理からすでにキャッシュに格納されている可能性があるため、ドライブへのアクセスが不要になります。
- 書き込みデータは最初にキャッシュに書き込まれるため、データがドライブに書き込まれるのを待つことなくアプリケーションが処理を続行できます。

デフォルトのキャッシュ設定はほとんどの環境の要件を満たしていますが、必要に応じて設定を変更できます。

ストレージアレイキャッシュの設定

ストレージアレイ内のすべてのボリュームについて、Systemページで次の値を指定できます。

- フラッシュの開始値--キャッシュフラッシュ（ディスクへの書き込み）をトリガーするキャッシュ内の書き込み前のデータの割合。指定した開始の割合の書き込み前のデータがキャッシュに格納されると、フラッシュがトリガーされます。デフォルトでは、キャッシュが80%フルに達すると、コントローラがキャッシュのフラッシュを開始します。
- キャッシュブロックサイズ--キャッシュ管理の組織単位である各キャッシュブロックの最大サイズ。キャッシュブロックサイズはデフォルトで8KiBですが、4、8、16、32KiBに設定できます。アプリケーションの一般的なI/Oサイズにキャッシュブロックサイズを設定するのが理想的です。ファイルシステムやデータベースアプリケーションでは一般に小さいサイズを使用し、大規模なデータ転送やシーケンシャルI/Oを必要とするアプリケーションには大きいサイズが適しています

ボリュームキャッシュの設定

ストレージアレイ内の個々のボリュームについて、Volumes（ボリューム）ページで次の値を指定できます（メニュー：Storage [Volumes]）。

- 読み取りキャッシュ--読み取りキャッシュは'ドライブから読み取られたデータを格納するバッファです読み取り処理の対象となるデータが以前の処理ですでにキャッシュに格納されていれば、ドライブにアクセスする必要はありません。読み取りキャッシュのデータは、フラッシュされるまで保持されます。
    - 動的キャッシュ読み取りプリフェッチ--動的キャッシュ読み取りプリフェッチにより'コントローラは'ドライブからキャッシュにデータ・ブロックを読み取っているときに'追加のシーケンシャル・データ・ブロックをキャッシュにコピーすることができますこのキャッシングにより、以降のデータ要求にキャッシュから対応できる可能性が高まります。動的キャッシュ読み取りプリフェッチは、シーケンシャルI/Oを使用するマルチメディアアプリケーションで重要ですデータがキャッシュにプリフェッチされる速度と量は、ホスト読み取りの速度と要求サイズに基づいて自動で調整されます。ランダムア

クセスの場合、原因 データがキャッシュにプリフェッチされることはありません。この機能は、読み取りキャッシュが無効になっている場合は適用されません。

- 書き込みキャッシュ--書き込みキャッシュは'まだドライブに書き込まれていないホストからのデータを格納するバッファです書き込みキャッシュ内のデータは、ドライブに書き込まれるまで保持されます。書き込みキャッシュにより、I/Oパフォーマンスを向上させることができます。

> データ損失の可能性-バッテリなしの書き込みキャッシュオプションを有効にし、保護用のユニバーサル電源装置がない場合、データが失われる可能性があります。また、コントローラのバッテリがない場合にWrite caching without Batteriesオプションを有効にすると、データが失われる可能性があります。

  - バッテリなしの書き込みキャッシュ--バッテリなしの書き込みキャッシュ設定により、バッテリがない、故障している、完全に放電されている、またはフル充電されていない場合でも書き込みキャッシュを続行できます。バッテリなしの書き込みキャッシュを選択すると電源の喪失時にデータが失われる可能性があるため、一般には推奨されません。通常、書き込みキャッシュは、バッテリが充電されるか障害が発生したバッテリが交換されるまで、コントローラによって一時的にオフにされます。
  - ミラーリングありの書き込みキャッシュ--ミラーリングありの書き込みキャッシュは'一方のコントローラのキャッシュ・メモリに書き込まれたデータがもう一方のコントローラのキャッシュ・メモリにも書き込まれたときに発生しますそのため、一方のコントローラで障害が発生した場合、もう一方のコントローラで未処理の書き込み処理をすべて完了できます。書き込みキャッシュのミラーリングは、書き込みキャッシュが有効で、2台のコントローラが配置されている場合にのみ使用できます。ミラーリングありの書き込みキャッシュは、ボリュームの作成時にデフォルトで設定されます。

自動ロードバランシングの概要

自動ロードバランシングを使用すると、負荷の変化に動的に対応してボリュームのコントローラ所有権が自動的に調整されるため、コントローラ間でワークロードが移動する際の負荷の不均衡が解消され、I/Oリソースの管理が強化されます。

各コントローラのワークロードは継続的に監視され、ホストにインストールされたマルチパスドライバとの連携により、必要に応じて自動的に負荷を分散できます。ワークロードがコントローラ間で自動的に再分散されるため、ストレージアレイの負荷の変化に合わせてボリュームのコントローラ所有権を手動で調整する必要がなくなり、ストレージ管理者の負担が軽減されます。

自動ロードバランシングを有効にすると、次の機能が実行されます。

- コントローラのリソース利用率を自動的に監視して負荷を分散します。
- ボリュームのコントローラ所有権が必要に応じて自動的に調整され、ホストとストレージアレイの間のI/O帯域幅が最適化されます。

自動ロードバランシングの有効化と無効化

自動ロードバランシングは、すべてのストレージアレイでデフォルトで有効になっています。

自動ロードバランシングは、ストレージアレイの状況に応じて無効にすることができます。たとえば、次のような場合です。

- 特定のボリュームのコントローラ所有権については、ワークロードを分散するために自動的に変更されないようにする場合。
- 高度に調整された環境で、コントローラ間の負荷分散が特定の要件を満たすように意図的に設定されてい

る。

自動ロードバランシング機能をサポートするホストタイプ

自動ロードバランシングを有効にするのはストレージアレイレベルですが、ホストまたはホストクラスタに選択したホストタイプがこの機能の動作に直接影響します。

ストレージアレイのワークロードをコントローラ間で分散する際、自動ロードバランシング機能は、両方のコントローラからアクセスでき、自動ロードバランシング機能をサポートするホストまたはホストクラスタにのみマッピングされたボリュームの移動を試みます。

これにより、ロードバランシングプロセスによってホストがボリュームにアクセスできなくなることはありませんが、自動ロードバランシングをサポートしていないホストにマッピングされたボリュームがあると、ストレージアレイはワークロードを分散できなくなります。自動ロードバランシングがワークロードを分散するためには、マルチパスドライバがTPGSをサポートしていることと、ホストタイプが次の表に含まれていることが必要です。

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	マルチパスドライバ
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
VMware	Native Multipathing Plugin（NMP）と'VMW_SATP_ALUA Storage Array Type'プラグイン

一部の例外を除き、自動ロードバランシングをサポートしていないホストタイプは、この機能が有効になっているかどうかに関係なく正常に動作し続けます。例外の1つがシステムのフェイルオーバーです。データパスが復旧すると、ストレージアレイはマッピングされていないボリュームまたは割り当てられていないボリュームを所有権を持つコントローラに戻しますが、自動ロードバランシングをサポートしていないホストにマッピングまたは割り当てられているボリュームは移動されません。

を参照してください "Interoperability Matrix Tool で確認してください" サポートされるマルチパスドライバ、OSレベル、コントローラドライブトレイの互換性情報については、を参照してください。

自動ロードバランシング機能と**OS**の互換性の確認

新しいシステムを設定（または既存のシステムを移行）する前に、自動ロードバランシング機能とOSの互換性を確認します。

1. にアクセスします "Interoperability Matrix Tool で確認してください" をクリックして解決策 を検索し、サポートを確認してください。

   Red Hat Enterprise Linux 6またはSUSE Linux Enterprise Server 11を実行しているシステムの場合は、テクニカルサポートにお問い合わせください。

2. /etc/multipath.confファイルを更新して構成します
3. 該当するベンダーおよび製品の「retain_attached_device_handler」と「detect_prio」の両方が「yes」に設定されていることを確認するか、デフォルトの設定を使用します。

デフォルトのホストオペレーティングシステムタイプ

デフォルトのホストタイプは、ホストの最初の接続時にストレージアレイで使用されます。ボリュームがアクセスされたときに、ストレージアレイのコントローラがホストのオペレーティングシステムとどのように連携するかを定義します。接続されたホストを基準にストレージアレイの動作を変更する必要がある場合は、ホストタイプを変更できます。

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

次のガイドラインに注意してください。

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

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

- ほとんどの接続ホストでオペレーティングシステムが異なる場合は、ホストタイプを工場出荷時のデフォルトに変更します。

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

方法

ストレージアレイ名を編集します

SANtricity System Managerのタイトルバーに表示されるストレージアレイ名を変更することができます。

手順

1. メニューを選択します。[設定][システム]。
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、このフィールドには「不明」と表示されます。

3. ストレージアレイ名の横にある* Edit *（鉛筆）アイコンをクリックします。

   フィールドが編集可能になります。

4. 新しい名前を入力します。

   名前には、アルファベット、数字、アンダースコア（_）、ダッシュ（-）、ハッシュ記号（#）を使用できます。スペースを含めることはできません。名前の最大文字数は30文字です。名前は一意である必要があります。

5. [保存（Save *）]（チェックマーク）アイコンをクリックします。

   変更せずに編集可能なフィールドを閉じるには、[キャンセル（X）]アイコンをクリックします。

結果

新しい名前がSANtricity System Managerのタイトルバーに表示されます。

ストレージアレイのロケーターライトを点灯します

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. メニューを選択します。[設定][システム]。
2. [*General]で、[*Turn on Storage Array Locator Lights]をクリックします。

   ストレージアレイのロケーターライトを点灯*ダイアログボックスが開き、対応するストレージアレイのロケーターライトが点灯します。

3. ストレージアレイが物理的に配置されている場合は、ダイアログボックスに戻り、*電源オフ*を選択します。

結果

ロケーターライトが消灯してダイアログボックスが閉じます。

ストレージアレイのクロックを同期する

ネットワークタイムプロトコル（NTP）が無効な場合は、コントローラのクロックを手動で設定して、管理クライアント（SANtricity System Managerにアクセスするブラウザの実行に使用されるシステム）と同期されるようにすることができます。

このタスクについて

同期によって、イベントログ内のイベントのタイムスタンプがホストログファイルに書き込まれるタイムスタンプと一致します。同期プロセスの実行中も、コントローラを引き続き使用できます。

System ManagerでNTPが有効になっている場合は、このオプションを使用してクロックを同期しないでください。代わりに、NTPではシンプルネットワークタイムプロトコル（SNTP）を使用してクロックを自動的に同期します。

同期後に、パフォーマンス統計が失われたり精度が低下したりする可能性があります。また、スケジュールに影響が生じたり（ASUP、Snapshotなど）、ログデータ内のタイムスタンプが不正確になる可能性もあります。NTPを使用すると、この問題を回避できます。

手順

1. メニューを選択します。[設定][システム]。
2. [**General**]で'[*ストレージ・アレイ・クロックの同期化]をクリックします

   ストレージ・アレイ・クロックの同期*ダイアログ・ボックスが開きますこのダイアログには、コントローラおよび管理クライアントとして使用されているコンピュータの現在の日時が表示されます。

   シンプレックスストレージアレイの場合、表示されるコントローラは1台だけです。

3. ダイアログボックスに表示された時間が一致しない場合は、*同期化*をクリックします。

結果

同期が成功すると、イベントのタイムスタンプはイベントログとホストログで同じになります。

ストレージアレイの構成を保存します

ストレージアレイの構成情報をスクリプトファイルに保存すると、追加のストレージアレイをセットアップする際に同じ構成を使用するための時間を節約できます。

作業を開始する前に

論理構成の設定を変更する処理がストレージアレイで行われていないことを確認してください。このような処理の例としては、ボリュームの作成または削除、コントローラファームウェアのダウンロード、ホットスペアドライブの割り当てまたは変更、ボリュームグループへの容量（ドライブ）の追加などがあります。

このタスクについて

ストレージアレイの構成を保存すると、ストレージアレイの設定、ボリュームの構成、ホストの構成、またはストレージアレイに対するホストとボリュームの割り当てを含むコマンドラインインターフェイス（CLI）スクリプトが生成されます。生成されたこのCLIスクリプトを使用して、ハードウェア構成がまったく同じ別のストレージアレイに構成をレプリケートできます。

ただし、ディザスタリカバリにはこのCLIスクリプトを使用しないでください。システムをリストアするには、代わりに、手動で作成する構成データベースのバックアップファイルを使用するか、テクニカルサポートに問い合わせて最新のAutoSupportデータからこのデータを取得してください。

この操作では、次の設定は保存されません。

- バッテリの寿命です
- コントローラの時刻
- 不揮発性静的ランダムアクセスメモリ（NVSRAM）の設定

- すべてのプレミアム機能
- ストレージアレイのパスワード
- ハードウェアコンポーネントの動作ステータスと状態
- ボリュームグループの動作ステータス（最適を除く）と状態
- ミラーリング、ボリュームコピーなどのコピーサービス

> アプリケーションエラーのリスク-論理構成の設定を変更する処理をストレージアレイで実行中の場合は、このオプションを使用しないでください。このような処理の例としては、ボリュームの作成または削除、コントローラファームウェアのダウンロード、ホットスペアドライブの割り当てまたは変更、ボリュームグループへの容量（ドライブ）の追加などがあります。

手順

1. メニューを選択します。[設定][システム]。
2. 「ストレージアレイ構成の保存」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

   > ［ホスト/ボリューム間の割り当て］項目を選択した場合、［ボリューム構成］項目と［ホスト構成］項目もデフォルトで選択されます。また、*ボリューム構成*と*ホスト構成*を保存しないと、ホスト/ボリューム間の割り当て*を保存できません。
4. [保存（ Save ）] をクリックします。

   ファイルは'storagearray-configuration.cfgという名前でブラウザのDownloadsフォルダに保存されます

完了後

ストレージアレイの構成を別のストレージアレイにロードするには、SANtricity Unified Managerを使用します。

ストレージアレイの構成のクリア

ストレージアレイからすべてのプール、ボリュームグループ、ボリューム、ホストの定義、およびホストの割り当てを削除する場合は、設定のクリア処理を使用します。

作業を開始する前に

- ストレージアレイ構成をクリアする前に、データのバックアップを作成します。

このタスクについて

ストレージアレイ構成のクリアオプションは2つあります。

- ボリューム--通常、テスト用ストレージアレイを本番ストレージアレイとして再構成するために、ボリュ

ームオプションを使用します。たとえば、テスト用にストレージアレイを構成し、テストが完了したらテスト構成を削除し、本番環境用にストレージアレイをセットアップする場合があります。

- ストレージ・アレイ--通常'ストレージ・アレイを別の部門またはグループに移動するには'ストレージ・アレイ・オプションを使用しますたとえば、エンジニアリング部門が新しいストレージアレイを導入することになり、現在使用しているストレージアレイを管理部門に移動する場合などです。

  ストレージアレイオプションを選択すると、追加の設定がいくつか削除されます。

	ボリューム	ストレージアレイ
プールとボリュームグループを削除します	X	X
ボリュームを削除します	X	X
ホストとホストクラスタを削除します	X	X
ホスト割り当てを削除します	X	X
ストレージアレイ名を削除します		X
ストレージアレイのキャッシュ設定をデフォルトにリセットします		X

データ損失のリスク-この処理を実行すると、ストレージアレイからすべてのデータが削除されます。（完全消去は実行されません）。 この処理は開始後にキャンセルすることはできません。この処理は、テクニカルサポートから指示があった場合にのみ実行してください。

手順

1. メニューを選択します。[設定][システム]。
2. 「ストレージアレイ構成のクリア」を選択します。
3. ドロップダウンリストで、* Volume または Storage Array *のいずれかを選択します。
4. オプション：（データではなく）設定を保存する場合は、ダイアログボックス内のリンクを使用します。
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。

ログインバナーを設定します

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

ます。

このタスクについて

作成したバナーは、ログイン画面の前にダイアログボックスに表示されます。

手順

1. メニューを選択します。[設定][システム]。
2. 「一般」セクションで、「*ログインバナーの設定」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。

   書式設定にHTMLタグやその他のマークアップタグを使用しないでください。

4. [保存（ Save ）] をクリックします。

結果

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

セッションタイムアウトの管理

非アクティブな状態が一定の時間続いたユーザセッションは切断されるよう、SANtricity System Managerでタイムアウトを設定できます。

このタスクについて

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

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

手順

1. メニューを選択します。[設定][システム]。
2. 「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. スピナーコントロールを使用して、時間を分単位で増減できます。

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

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

4. [保存（ Save ）] をクリックします。

ストレージアレイのキャッシュ設定を変更します

ストレージアレイ内のすべてのボリュームでは、フラッシュおよびブロックサイズについてキャッシュメモリの設定を調整できます。

このタスクについて

キャッシュメモリは、ドライブメディアよりも速くアクセスできる、コントローラ上の一時的な揮発性ストレージ領域です。キャッシュのパフォーマンスを調整するには、次の設定を調整します。

キャッシュ設定	説明
デマンドキャッシュフラッシュを開始します	キャッシュに格納された書き込み前のデータが何パーセントに達したらキャッシュフラッシュ（ディスクへの書き込み）を開始するかを指定します。デフォルトでは、書き込み前のデータが容量の80%に達するとキャッシュフラッシュが開始されます。書き込み処理が中心の環境では、この割合を高くすると、新しい書き込み要求をディスクにアクセスせずにキャッシュで処理できるため便利です。I/Oが不規則でデータのバーストがある環境では、この割合を低くして、バーストとバーストの間に頻繁にキャッシュがフラッシュされるようにすると効果的です。ただし、80%より小さいパーセントの開始パーセント値を指定すると、原因 のパフォーマンスが低下する可能性があります。
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、各キャッシュブロックの最大サイズであり、キャッシュを管理する際の単位となります。デフォルトのブロックサイズは8KiBです。System Managerでは、4、8、16、または32KiBのキャッシュブロックサイズを選択できます。使用するブロックサイズはアプリケーションによって異なり、ストレージのパフォーマンスに影響します。ファイルシステムやデータベースアプリケーションには小さいサイズが適しています。マルチメディアなどのシーケンシャルI/Oを生成するアプリケーションには、大きいサイズが適しています。

手順

1. メニューを選択します。[設定][システム]。
2. 下にスクロールして「その他の設定」を選択し、「キャッシュ設定の変更」をクリックします。

   [キャッシュ設定の変更]ダイアログボックスが開きます。

3. 次の値を調整します。
   - デマンドキャッシュフラッシュの開始—環境で使用されているI/Oに適した割合を選択します80%未満の値を選択すると、パフォーマンスが低下する可能性があります。

◦ キャッシュブロックサイズ—アプリケーションに適したサイズを選択します

4. [保存（ Save ）] をクリックします。

ホスト接続レポートの設定

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

このタスクについて

ホスト接続のレポートを無効にすると、接続またはストレージアレイに接続されているホストに関するマルチパスドライバの問題がシステムによって監視されなくなります。

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

手順

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

   このオプションが現在有効か無効かを示すテキストがこのオプションの下に表示されます。

   確認ダイアログが開きます。

3. 続行するには、 [はい] をクリックします。

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

自動ロードバランシングを設定する

自動ロードバランシング*機能を使用すると、ホストからの受信I/Oトラフィックが動的に管理され、両方のコントローラに分散されます。この機能はデフォルトで有効になっていますが、System Managerから無効にすることもできます。

このタスクについて

自動ロードバランシングを有効にすると、次の機能が実行されます。

- コントローラのリソース利用率を自動的に監視して負荷を分散します。
- ボリュームのコントローラ所有権が必要に応じて自動的に調整され、ホストとストレージアレイの間のI/O帯域幅が最適化されます。

自動ロードバランシングは、ストレージアレイの状況に応じて無効にすることができます。たとえば、次のような場合です。

- 特定のボリュームのコントローラ所有権については、ワークロードを分散するために自動的に変更されないようにする場合。

- 高度に調整された環境で、コントローラ間の負荷分散が特定の要件を満たすように意図的に設定されている。

手順

1. メニューを選択します。[設定][システム]。
2. 下にスクロールして「その他の設定」を選択し、「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。

   確認ダイアログが開きます。
3. 続行するには、[はい]をクリックして確定します。

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

   この機能を無効から有効に切り替えると、ホスト接続レポート機能も自動的に有効になります。

デフォルトのホストタイプを変更

デフォルトのホストオペレーティングシステムの変更設定を使用して、ストレージアレイレベルでデフォルトのホストタイプを変更します。一般に、デフォルトのホストタイプは、ストレージアレイにホストを接続する前、または追加のホストを接続するときに変更します。

このタスクについて

次のガイドラインに注意してください。

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

  たとえば、8つの異なるホストをストレージアレイに接続し、そのうち6つでWindowsオペレーティングシステムを実行している場合は、Windowsをデフォルトのホストオペレーティングシステムタイプとして選択する必要があります。
- ほとんどの接続ホストでオペレーティングシステムが異なる場合は、ホストタイプを工場出荷時のデフォルトに変更します。

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

手順

1. メニューを選択します。[設定][システム]。

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

従来の管理インターフェイスを有効または無効にします

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。デフォルトでは、従来の管理インターフェイスは有効になっています。無効にすると、ストレージアレイと管理クライアントはより安全な通信方法（REST API over https）を使用しますが、無効にした場合、特定のツールやタスクに影響する可能性があります。

このタスクについて

この設定は処理に次のように影響します。

- * on *（デフォルト）--ミラーリング、E5700およびE5600ストレージアレイのみで動作するCLIコマンド、およびQuickConnectユーティリティやOCIアダプタなどのその他のツールに必要な設定です。
- オフ--ストレージアレイと管理クライアント間の通信の機密性を強化し、外部ツールにアクセスするために必要な設定です。ディレクトリサーバ（LDAP）を設定する際に推奨される設定です。

手順

1. メニューを選択します。[設定][システム]。
2. 下にスクロールして「その他の設定」を選択し、「*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、*はい*をクリックして続行します。

よくある質問です

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。ただし、ディスクは比較的低速なデバイスであるため、コントローラのバックエンドからディスクへの通信は低速になります。

コントローラキャッシュがデータを受信すると、コントローラはデータを保持していることをホストアプリケーションに通知します。これにより、ホストアプリケーションはI/Oがディスクに書き込まれるのを待たずに代わりに、アプリケーションは処理を続行できます。また、サーバアプリケーションはキャッシュされたデータにアクセスできるため、データにアクセスするためにディスクを読み取る必要がなくなります。

コントローラキャッシュは、ストレージアレイの全体的なパフォーマンスに次のように影響します。

- キャッシュはバッファとして機能するため、ホストとディスクのデータ転送を同期する必要がありません。
- ホストからの読み取り/書き込み処理の対象となるデータが以前の処理ですでにキャッシュに格納されてい

れば、ディスクにアクセスする必要はありません。

- 書き込みキャッシュを使用している場合、ホストは以前の書き込み処理がディスクに書き込まれる前に後続の書き込みコマンドを送信できます。
- キャッシュプリフェッチを有効にすると、シーケンシャルリードアクセスが最適化されます。読み取り処理ではデータがディスクから読み取られるのではなく、キャッシュ内のデータが使用される可能性が高くなります。

> データ損失の可能性--バッテリなしの書き込みキャッシュ*オプションを有効にして保護用のユニバーサル電源装置を持たないと、データが失われる可能性があります。また、コントローラのバッテリがない場合に*バッテリなしの書き込みキャッシュ*オプションを有効にすると、データが失われる可能性があります。

キャッシュ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下回るまで使用されます。デフォルトでは、キャッシュの80%が使用中になるとフラッシュが開始されます。

System Managerでは、「デマンド・キャッシュ・フラッシュの開始」しきい値を、環境で使用されるI/Oのタイプに最も適した値に設定できます。書き込み操作が主な環境では'新しい書き込み要求をディスクに移動せずにキャッシュで処理できる可能性を高めるために'デマンド・キャッシュ・フラッシュの開始パーセントを高く設定する必要があります割合を高く設定すると、キャッシュフラッシュの回数が減ってキャッシュに残るデータ量が増えるため、キャッシュヒットの可能性が高まります。

I/Oが不規則な（データバーストが発生する）環境では、キャッシュフラッシュを低く設定して、データバースト間でキャッシュが頻繁にフラッシュされるようにします。さまざまな負荷を処理する多様なI/O環境や、負荷のタイプが不明な環境では、このしきい値を中間の50%に設定します。80%未満に設定した場合、ホスト読み取りに必要なデータがキャッシュにないためにパフォーマンスが低下する可能性があります。また、割合を低くすると、キャッシュレベルを維持するために必要なディスクへの書き込み回数が増えるため、システムオーバーヘッドが増大します。

経過時間ベースのアルゴリズムでは、書き込みデータがディスクにフラッシュされるまでのキャッシュでの保持期間を指定します。キャッシュフラッシュしきい値に達するまでは、経過時間ベースのアルゴリズムが使用されます。デフォルトは10秒ですが、カウントされるのは非アクティブな期間のみです。System Managerではフラッシュのタイミングを変更できません。代わりに、コマンドラインインターフェイス（CLI）でSet Storage Arrayコマンドを使用する必要があります。

> データ損失の可能性--バッテリなしの書き込みキャッシュ*オプションを有効にして保護用のユニバーサル電源装置を持たないと、データが失われる可能性があります。また、コントローラのバッテリがない場合に*バッテリなしの書き込みキャッシュ*オプションを有効にすると、データが失われる可能性があります。

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複数の「ブロック」に編成します。ブロックは、サイズが4KiB、8KiB、16KiB、または32KiBのメモリチャンクです。ストレー

ジシステムのボリュームはすべて同じキャッシュスペースを共有するため、ボリュームで使用できるキャッシュブロックサイズは1つだけです。

キャッシュブロックは、ディスクの論理ブロックシステムで使用される512バイトブロックとは異なります。

使用するブロックサイズはアプリケーションによって異なり、ストレージのパフォーマンスに影響する可能性があります。System Managerのデフォルトのブロックサイズは8KiBですが、4KiB、8KiB、16KiB、または32KiBに設定できます。ファイルシステムやデータベースアプリケーションには小さいサイズが適しています。大容量のデータ転送、シーケンシャルI/O、マルチメディアなどの広帯域幅を必要とするアプリケーションには、大きいサイズが適しています。

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？

System Managerと管理クライアント（ブラウザ経由でSystem Managerにアクセスするコンピュータ）で表示されるタイムスタンプが異なる場合は、ストレージアレイのコントローラクロックを手動で同期する必要があります。このタスクが必要になるのは、System ManagerでNTP（ネットワークタイムプロトコル）が有効になっていない場合だけです。

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入手できる*ストレージアレイクロックの同期*ダイアログボックスで確認できます。ダイアログボックスに表示された時間が一致しない場合は、同期を実行します。このダイアログボックスを定期的に表示することで、コントローラクロックの時間表示が同期されているかどうかを確認できます。

ホスト接続レポートとは何ですか？

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

ケーブルに緩み、損傷、脱落が生じた場合や、ホストに問題が生じた場合は、接続の中断が発生する可能性があります。これらの状況では、Recovery Guruメッセージが発行されることがあります。

- ホストの冗長性が失われました--どちらかのコントローラがホストと通信できない場合に開きます
- ホストタイプが正しくありません--ストレージアレイでホストタイプが正しく指定されていないと'フェイルオーバーの問題が発生する可能性があります

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

また、コントローラのリソース使用量を監視してバランスを調整する自動ロードバランシングも無効になります。ただし、ホスト接続レポートを再度有効にしても、自動ロードバランシング機能は自動的には有効になりません。

iSCSI 設定

概念

iSCSIの用語

ストレージアレイに関連するiSCSIの用語を次に示します。

期間	説明
CHAP	チャレンジハンドシェイク認証プロトコル（CHAP）方式では、初回のリンク確立時にターゲットとイニシエータのIDを検証します。認証は、CHAP_secret__という共有セキュリティキーに基づいて行われます。
コントローラ	コントローラは、ボード、ファームウェア、ソフトウェアで構成されます。ドライブを制御し、 System Manager の機能を実装します。
DHCP	動的ホスト構成プロトコル（DHCP）は、インターネットプロトコル（IP）ネットワークでIPアドレスなどのネットワーク設定パラメータを動的に配布するために使用されるプロトコルです。
IB	InfiniBand （ IB ）は、ハイパフォーマンスのサーバとストレージシステムの間のデータ転送用の通信標準です。
ICMP PING応答	Internet Control Message Protocol（ICMP）は、ネットワークに接続されたコンピュータのオペレーティングシステムでメッセージの送信に使用されるプロトコルです。ICMPメッセージを送信することで、ホストに到達できるかどうかや、そのホストとのパケットの送受信にどれくらいの時間がかかるかが確認されます。
IQN	iSCSI Qualified Name（IQN）は、iSCSIイニシエータまたはiSCSIターゲットの一意の名前です。
iSER	iSCSI Extensions for RDMA（iSER）は、InfiniBandやイーサネットなどのRDMAトランスポートを使用する処理用にiSCSIプロトコルを拡張したプロトコルです。
iSNS	Internet Storage Name Service（iSNS）は、TCP / IPネットワーク上のiSCSIデバイスとFibre Channelデバイスの自動検出、管理、構成が可能なプロトコルです。
MAC アドレス	メディアアクセス制御（MAC）アドレスはイーサネットで使用される識別子で、同じ物理トランスポートネットワークインターフェイス上の2つのポートを接続する別々の論理チャネルを区別します。
管理クライアント	管理クライアントは、System Managerにアクセスするためのブラウザがインストールされたコンピュータです。

期間	説明
MTU	Maximum Transmission Unit（MTU；最大転送単位）は、ネットワークで送信可能なパケットまたはフレームの最大サイズです。
RDMA	Remote Direct Memory Access（RDMA）は、ネットワークコンピュータ同士が、それぞれのオペレーティングシステムを介さずにメインメモリ内でデータを交換できるテクノロジです。
名前のない検出セッション	名前のない検出セッションのオプションが有効な場合、iSCSIイニシエータは、コントローラの情報を取得するためにターゲットIQNを指定する必要はありません。

方法

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またはシステムページからiSCSIポートを設定できます。

作業を開始する前に

- コントローラにiSCSIポートが搭載されている必要があります。そうでない場合、iSCSI設定は使用できません。
- ネットワーク速度（ポートとホストの間のデータ転送率）を把握しておく必要があります。

このタスクについて

このタスクでは、ハードウェアページから iSCSI ポート設定にアクセスする方法について説明します。システムページ（メニュー：設定[システム]）から設定にアクセスすることもできます。

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. 図にドライブが表示されている場合は、 * シェルフの背面を表示 * をクリックします。

   図の表示が切り替わり、ドライブではなくコントローラが表示されます。
3. 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 Port* （ iSCSI ポートの設定）を選択します。

   Configure iSCSI Ports *オプションは、System ManagerがコントローラでiSCSIポートを検出した場合にのみ表示されます。

Configure iSCSI Ports （ iSCSI ポートの設定）ダイアログボックスが開きます。

5. ドロップダウンリストで、設定するポートを選択し、 * Next * をクリックします。
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[詳細ポート設定を表示]リンクをクリックします。

   フィールドの詳細

ポートの設定	説明
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。メモ：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オフにします。
TCPリスニングポート（Show more port settingsをクリックすると使用可能）	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（Show more port settingsをクリックして使用可能）	必要に応じて、 Maximum Transmission Unit （ MTU ；最大伝送ユニット）の新しいサイズをバイト単位で入力します。 デフォルトの Maximum Transmission Unit （ MTU ；最大転送単位）サイズは 1500 バイト / フレームです。1500~9000 の値を入力する必要があります。
ICMP PING 応答を有効にします	Internet Control Message Protocol （ ICMP ）を有効にする場合は、このオプションを選択します。ネットワーク接続されたコンピュータのオペレーティングシステムは、このプロトコルを使用してメッセージを送信します。ICMP メッセージを送信することで、ホストに到達できるかどうかや、そのホストとのパケットの送受信にどれくらいの時間がかかるかが確認されます。

   IPv4を有効にするを選択した場合は、次へをクリックするとIPv4設定を選択するダイアログボックスが開きます。IPv6を有効にするを選択した場合は、次へをクリックすると、IPv6設定を選択するためのダイアログボックスが開きます。両方のオプションを選択した場合は、最初にIPv4設定のダイアログボックスが開き、次へをクリックすると、IPv6設定のダイアログボックスが開きます。

7. IPv4 と IPv6 、またはその両方を自動または手動で設定します。すべてのポート設定を表示するには、ダイアログボックスの右側にある * Show more settings * リンクをクリックします。

   フィールドの詳細

ポートの設定	説明
自動的に設定を取得します	設定を自動的に取得するには、このオプションを選択します。
静的な設定を手動で指定します	このオプションを選択した場合は、フィールドに静的アドレスを入力します。（必要に応じて、住所をカットアンドペーストしてフィールドに貼り付けることもできます）。 IPv4の場合は、ネットワークのサブネットマスクとゲートウェイも指定します。IPv6 の場合は、ルーティング可能な IP アドレスとルータの IP アドレスも指定します。
VLANサポートを有効にします（[詳細設定を表示]をクリックして使用できます）。	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（[詳細設定を表示]をクリックして使用可能）。	ネットワークアクセスの優先度を決定するパラメータを有効にする場合は、このオプションを選択します。スライダを使用して優先度を1（最も低い）から7（最も高い）の間で選択します。 共有 LAN 環境（イーサネットなど）では、多数のステーションがネットワークアクセスで競合する可能性があります。アクセスは先に行われたものから順に処理されます。2 つのステーションが同時にネットワークにアクセスしようとすると、両方のステーションがオフになり、再試行するまで待機します。スイッチイーサネットでは、 1 つのステーションだけがスイッチポートに接続されるため、このプロセスは最小限に抑えられます。

8. [完了] をクリックします。

iSCSI認証を設定

iSCSIネットワークのセキュリティを強化するために、コントローラ（ターゲット）とホスト（イニシエータ）の間に認証を設定できます。System Managerは、チャレンジハンドシェイク認証プロトコル（CHAP）方式を使用します。CHAPは初回のリンク確立時に

ターゲットとイニシエータのIDを検証します。認証は、CHAP_secret__という共有セキュリティキーに基づいて行われます。

作業を開始する前に

イニシエータ（iSCSIホスト）のCHAPシークレットは、ターゲット（コントローラ）のCHAPシークレットを設定する前でもあとでも設定できます。このタスクの手順を実行する前に、ホストが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。

このタスクについて

次のいずれかの認証方法を選択できます。

- 一方向認証--コントローラがiSCSIホストの識別情報を認証できるようにするには'この設定を使用します(一方向認証)
- 双方向認証--コントローラとiSCSIホストの両方が認証(双方向認証)を実行できるようにするには'この設定を使用しますこの設定は、コントローラがiSCSIホストの識別情報を認証できるようにし、さらにiSCSIホストがコントローラの識別情報を認証できるようにすることで、二次的なセキュリティを提供します。

iSCSIの設定と機能は、ストレージアレイがiSCSIをサポートしている場合にのみ、設定ページに表示されます。

手順

1. メニューを選択します。[設定][システム]。
2. [* iSCSI settings]で、[Configure Authentication*]をクリックします。

   Configure Authentication（認証の設定）ダイアログボックスが表示され、現在設定されている方式が示されます。CHAPシークレットが設定されているホストがあるかどうかも表示されます。

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には'このオプションを選択して'完了*をクリックしますダイアログボックスが閉じ、設定が完了します。
   - 一方向認証--コントローラがiSCSIホストのIDを認証できるようにするには'このオプションを選択して'次へをクリックします*ターゲットCHAPの構成ダイアログ・ボックスを表示します
   - 双方向認証--コントローラとiSCSIホストの両方が認証を実行できるようにするには'このオプションを選択して'次へ*をクリックし'ターゲットCHAPの構成ダイアログ・ボックスを表示します
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、既存の文字を置き換えることができます（新しい文字はマスクされません）。

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。

◦ _2Way _authenticationを設定する場合は、* Next *をクリックしてConfigure Initiator CHAPダイアログボックスを表示します。

6. 双方向認証について、任意のiSCSIホスト（イニシエータ）のCHAPシークレット（12~57文字の印刷可能なASCII文字）を入力または確認します。特定のホストに双方向認証を設定しない場合は、「* Initiator CHAP Secret *」フィールドを空白のままにします。

ホストのCHAPシークレットがすでに設定されている場合は、フィールド内の文字は表示されません。必要に応じて、既存の文字を置き換えることができます（新しい文字はマスクされません）。

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。

iSCSI検出設定を有効にします

iSCSIネットワーク内のストレージデバイスの検出に関連する設定を有効にすることができます。ターゲット検出設定では、Internet Storage Name Service（iSNS）プロトコルを使用してストレージアレイのiSCSI情報を登録し、名前のない検出セッションを許可するかどうかを設定できます

作業を開始する前に

iSNSサーバで静的IPアドレスが使用されている場合は、そのアドレスをiSNSの登録に使用できる必要があります。IPv4とIPv6の両方がサポートされています。

このタスクについて

iSCSI検出に関連する次の設定を有効にすることができます。

- * iSNSサーバによるターゲットの登録を有効にする*--有効にすると'ストレージ・アレイはiSNSサーバからiSCSI Qualified Name（IQN）とポート情報を登録しますこの設定は、イニシエータがiSNSサーバからIQNとポート情報を取得できるように、iSNS検出を許可します。
- 名前のない検出セッションを有効にする--名前のない検出セッションを有効にすると'イニシエータ（iSCSIホスト）は'検出タイプ接続のログインシーケンス中にターゲットのIQN（コントローラ）を指定する必要はありません無効な場合、ホストはIQNを指定してコントローラへの検出セッションを確立する必要があります。ただし、通常の（I/Oベアリング）セッションでは常にターゲットIQNが必要です。この設定を無効にすると、権限のないiSCSIホストがIPアドレスのみを使用してコントローラに接続することを防止できます。

iSCSIの設定と機能は、ストレージアレイがiSCSIをサポートしている場合にのみ、設定ページに表示されます。

手順

1. メニューを選択します。[設定][システム]。
2. [* iSCSI settings]で、[*ターゲット検出設定の表示/編集]をクリックします。

   [* Target Discovery Settings*（ターゲット検出設定*）]ダイアログボックスが表示されます。[Enable iSNS

server…]フィールドの下に、コントローラがすでに登録されているかどうかを示すダイアログボックスが表示されます。

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サーバから自動的に設定を取得*--動的ホスト構成プロトコル(DHCP)サーバを使用してiSNSサーバを設定する場合は'このオプションを選択しますこのオプションを使用する場合は、コントローラのすべてのiSCSIポートでDHCPを使用するように設定する必要があります。必要に応じて、コントローラのiSCSIポートの設定を更新して、このオプションを有効にします。

     DHCPサーバでiSNSサーバのアドレスを指定するには、オプション43の「ベンダー固有の情報」を使用するようにDHCPサーバを設定する必要があります。 このオプションでは、iSNSサーバのIPv4アドレスをデータバイト0xa-0xd（10-13）に含める必要があります。

   - 静的な設定を手動で指定-- iSNSサーバの静的IPアドレスを入力する場合は'このオプションを選択します（必要に応じて、住所をカットアンドペーストしてフィールドに貼り付けることもできます）。 フィールドに、IPv4アドレスまたはIPv6アドレスを入力します。両方を設定した場合は、IPv4がデフォルトです。また、TCPリスニングポートを入力します（デフォルトの3205を使用するか、49152~65535の値を入力）。
4. ストレージアレイを名前のない検出セッションの対象にするには、*名前のない検出セッションを有効にする*を選択します。
   - 有効にすると、iSCSIイニシエータは、コントローラの情報を取得するためにターゲットIQNを指定する必要はありません。
   - 無効にすると、イニシエータがターゲットIQNを指定しないかぎり、検出セッションは実行されません。名前のない検出セッションを無効にすると、セキュリティが向上します。
5. [保存（ Save ）] をクリックします。

結果

System Managerがコントローラをi SNSサーバに登録しようとする間、進捗状況バーが表示されます。この処理には最大5分かかることがあります。

iSCSI統計パッケージを表示します

ストレージアレイへのiSCSI接続に関するデータを表示できます。

このタスクについて

System Managerには、次のタイプのiSCSI統計が表示されます。統計はすべて読み取り専用で、設定することはできません。

- イーサネット**MAC**統計--メディアアクセス制御(MAC)の統計情報を提供します。MACは、物理アドレスまたはMACアドレスと呼ばれるアドレス指定メカニズムも提供します。MACアドレスは、各ネットワークアダプタに割り当てられている一意のアドレスです。MACアドレスは、サブネットワーク内のデスティネーションへのデータパケットの配信に役立ちます。
- イーサネット**TCP/IP**統計-- iSCSIデバイスのTCP (Transmission Control Protocol)とIP (Internet Protocol)のTCP/IPの統計情報を提供しますTCPを使用すると、ネットワークホスト上のアプリケーションが相互に接続を作成し、パケットでデータを交換できます。IPは、パケット交換インターネットワークを介してデータを通信するデータ指向プロトコルです。IPv4統計とIPv6統計は個別に表示されます。

- ローカル・ターゲット/イニシエータ（プロトコル）統計：ストレージ・メディアへのブロック・レベルのアクセスを提供するiSCSIターゲットの統計情報を表示します非同期ミラーリング処理でイニシエータとして使用される場合は'ストレージ・アレイのiSCSI統計情報を表示します
- **DCBX**の運用状態統計--さまざまなData Center Bridging Exchange（DCBX）機能の運用状態を表示します。
- *LLDP TLV statistics *-- Link Layer Discovery Protocol (LLDP) Type Length Value (TLTLV)統計を表示します。
- **DCBX TLV**統計-- Data Center Bridging（DCB）環境内のストレージアレイのホストポートを識別する情報が表示されます。この情報は、識別や機能のためにネットワークピアと共有されます。

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

手順

1. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
2. [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. ベースラインを設定するには、*新しいベースラインを設定*をクリックします。

   ベースラインを設定すると、統計を収集するための新しい開始ポイントが設定されます。すべてのiSCSI統計に同じベースラインが使用されます。

iSCSIセッションを終了します

不要になったiSCSIセッションを終了できます。iSCSIセッションは、非同期ミラー関係にあるホストまたはリモートストレージアレイとの間で確立できます。

このタスクについて

iSCSIセッションを終了する理由としては、次のようなものが考えられます。

- 不正アクセス-- iSCSIイニシエータがログオンされていて、アクセスできない場合は、iSCSIセッションを終了して、iSCSIイニシエータをストレージアレイから強制的に切断できます。認証方法を「なし」にしたため、iSCSIイニシエータがログオンした可能性があります。
- システムダウンタイム--ストレージアレイを停止する必要があり'iSCSIイニシエータがまだログオンしている場合は'iSCSIセッションを終了してiSCSIイニシエータをストレージアレイから切断できます

手順

1. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
2. 「* iSCSIセッションの表示/終了*」を選択します。

   現在のiSCSIセッションのリストが表示されます。

3. 終了するセッションを選択します
4. [セッションの終了]をクリックし、操作を実行することを確認します。

iSCSI セッションを表示します

ストレージアレイへのiSCSI接続に関する詳細情報を表示できます。iSCSIセッションは、非同期ミラー関係にあるホストまたはリモートストレージアレイとの間で確立できます。

手順

1. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
2. 「* iSCSIセッションの表示/終了*」を選択します。

   現在のiSCSIセッションのリストが表示されます。

3. 特定のiSCSIセッションに関する追加情報 を表示するには、セッションを選択し、*詳細の表示*をクリックします。

フィールドの詳細

項目	説明
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ができる名前。エイリアスを使用すると、組織がユーザにわかりやすい文字列をiSCSI名に関連付けることができます。ただし、エイリアスはiSCSI名に代わるものではありません。イニシエータのiSCSIエイリアスは、System Managerではなく、ホストでのみ設定できます
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時にも表示されます。
イーサネットポート識別子	接続に関連付けられているコントローラポート。
イニシエータの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必要とするユーザを認証する手法。有効な値は* chap および None *です。

項目	説明
ヘッダーダイジェスト方式	iSCSIセッションに有効なヘッダー値を表示する手法。HeaderDigestおよびDataDigestには、* None または CRC32C を使用できます。両方のデフォルト値は None *です。
データダイジェスト方式	iSCSIセッションに有効なデータ値を表示する手法。HeaderDigestおよびDataDigestには、* None または CRC32C を使用できます。両方のデフォルト値は None *です。
最大接続数	iSCSIセッションに許可される接続の最大数。1~4を接続の最大数として指定できます。デフォルト値は* 1 *です。
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。
イニシエータのエイリアス	イニシエータに関連付けられているラベル。
ターゲットの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	最初の転送準備完了ステータス。ステータスは「* Yes 」または「 No *」のいずれかになります。
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）。512~262、144（256KB）を最大バースト長として指定できます。デフォルト値は* 262,144（256KB）*です。
第1バースト長	このiSCSIセッションの未承諾データのSCSIペイロード（バイト単位）。512~131、072（128KB）を第1バースト長として指定できます。デフォルト値は*65,536（64KB）*です。
デフォルトの待機時間	接続の終了または接続のリセット後に接続を試行するまでの最小秒数。0~3600をデフォルトの待機時間の値として指定できます。デフォルトは* 2 *です。
デフォルトの保持時間です	接続の終了または接続のリセット後も接続が可能な最大秒数。0~3600をデフォルトの保持時間として指定できます。デフォルト値は*20*です。
最大未処理R2T	このiSCSIセッションの未処理の「準備が完了した転送」の最大数。1~16を未処理の「準備が完了した転送」の最大値として指定できます。デフォルトは* 1 *です。
エラーリカバリレベル	このiSCSIセッションのエラーリカバリのレベル。エラーリカバリレベルの値は常に* 0 *に設定されています。

項目	説明
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。
ターゲット名	ターゲットの正式名（エイリアスではありません）。iqn形式のターゲット名です。
イニシエータ名	イニシエータの正式名（エイリアスではありません）。iqn形式または_eui_formatを使用するイニシエータ名です。

4. レポートをファイルに保存するには、*保存*をクリックします。

   ブラウザのDownloadsフォルダに'iscsi-session-connections.txt'というファイル名でファイルが保存されます

iSER over InfiniBandポートを設定します

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。構成設定は、[ハードウェア]ページまたは[システム]ページから使用できます。

作業を開始する前に

- コントローラにiSER over InfiniBandポートが搭載されている必要があります。そうでないと、System ManagerでiSER over InfiniBand設定を使用できません。
- ホスト接続のIPアドレスを確認しておく必要があります。

このタスクについて

iSER over InfiniBand構成には、* Hardware ページまたはメニューからアクセスできます：**Settings [System]**。このタスクでは、**[*Hardware**]ページからポートを設定する方法について説明します。

> iSER 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iSER 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. 図にドライブが表示されている場合は、 * シェルフの背面を表示 * をクリックします。

   図の表示が切り替わり、ドライブではなくコントローラが表示されます。

3. 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. iSER over InfiniBandポートの設定*を選択します。

   Configure iSER over InfiniBand ports（iSER over InfiniBandポートの設定）ダイアログボックスが開きま

す。

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、* Yes *をクリックしてiSER over InfiniBandポートをリセットします。

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。

このタスクについて

System Managerには、次のタイプのiSER over InfiniBand統計が表示されます。統計はすべて読み取り専用で、設定することはできません。

- ローカルターゲット（プロトコル）統計- iSER over InfiniBandターゲットの統計を提供し、ストレージメディアへのブロックレベルのアクセスが表示されます。
- * iSER over InfiniBandインターフェイス統計*- InfiniBandインターフェイス上のすべてのiSERポートの統計が提供され、各スイッチポートに関連付けられているパフォーマンス統計とリンクエラー情報が含まれます。

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

iSER over InfiniBand統計には、System（システム）ページ（メニュー：Settings（システム））またはSupport（サポート）ページからアクセスできます。ここでは、Supportページから統計情報にアクセスする方法について説明します。

手順

1. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
2. 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. ベースラインを設定するには、*新しいベースラインを設定*をクリックします。

   ベースラインを設定すると、統計を収集するための新しい開始ポイントが設定されます。すべてのiSER over InfiniBand統計に同じベースラインが使用されます。

よくある質問です

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）から情報を取得するようにホスト（イニシエータ）を設定できます。

この登録により、コントローラのiSCSI Qualified Name（IQN）とポート情報がiSNSサーバに提供され、イニ

シエータ（iSCSIホスト）とターゲット（コントローラ）間の照会が可能になります。

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、iSCSIホストはiSCSI検出セッション中にSend Targetsコマンドを送信します。これに応答して、コントローラからポート情報（ターゲットIQN、ポートIPアドレス、リスニングポート、ターゲットポートグループなど）が返されます。iSNSを使用する場合は、ホストイニシエータがiSNSサーバからターゲットIPを取得できるため、この検出方式は必要ありません。

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。統計はすべて読み取り専用で、設定することはできません。

- ローカルターゲット（プロトコル）統計- iSER over InfiniBandターゲットの統計を提供し、ストレージメディアへのブロックレベルのアクセスが表示されます。
- * iSER over InfiniBandインターフェイス統計*- InfiniBandインターフェイス上のすべてのiSER over InfiniBandポートの統計が提供され、各スイッチポートに関連付けられているパフォーマンス統計とリンクエラー情報が含まれます。

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

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？

次の表に、iSER over InfiniBandセッションの設定と管理に使用するSystem Managerの機能を示します。

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。

iSER over InfiniBandを設定して診断します

アクション	場所
iSER over InfiniBandポートを設定します	1. 「 * ハードウェア * 」を選択します。 2. Show back of shelf*を選択します。 3. コントローラを選択します。 4. iSER over InfiniBandポートの設定*を選択します。 または 1. メニューを選択します。[設定][システム]。 2. 下にスクロールして* iSER over InfiniBand setting*を選択し、* iSER over InfiniBandポートの設定*を選択します。
iSER over InfiniBandの統計を表示します	1. メニューを選択します。[設定][システム]。 2. 下にスクロールして* iSER over InfiniBand settings を表示し、 View iSER over InfiniBand Statistics *を選択します。

システム：NVMe設定

概念

NVMe の概要

一部のコントローラには、NVMe（Non-Volatile Memory Express）over InfiniBandファブリックまたはNVMe over RoCE（RDMA over Converged Ethernet）ファブリックを実装するためのポートが搭載されています。NVMeを使用すると、ホストとストレージアレイの間でハイパフォーマンスな通信が可能になります。

NVMeとは

*NVM _*は「不揮発性メモリ」を表し、多くのタイプのストレージデバイスで使用されている永続的メモリです。*_NVM*（NVM Express）は、NVMデバイスとのハイパフォーマンスなマルチキュー通信に特化して設計された、標準インターフェイスまたはプロトコルです。

NVMe over Fabricsとは

_NVMe over Fabrics（NVMe-oF）_は、NVMeメッセージベースのコマンドおよびデータをホストコンピュータとストレージの間でネットワーク経由で転送できるようにするテクノロジ仕様です。SANtricity OS 11.40リリース以降では、NVMeストレージアレイ（a_subsystem _）に、InfiniBandファブリックまたはRDMAファブリックを使用するホストからアクセスできます。NVMeコマンドは、ホスト側とサブシステム側の両方のトランスポート抽象化レイヤで有効化され、カプセル化されます。これにより、ハイパフォーマンスなNVMeインターフェイスのエンドツーエンドがホストからストレージへ拡張され、コマンドセットが標準化、簡易化されます。

NVMe-oFストレージは、ローカルのブロックストレージデバイスとしてホストに提示されます。ボリューム（a_namespac_）は、他のブロックストレージデバイスと同様にファイルシステムにマウントできます。必要に応じて、REST API、SMcli、またはSANtricity System Managerを使用してストレージをプロビジョニン

グできます。

NVMe Qualified Name（NQN）とは

NVMe Qualified Name（NQN）は、リモートストレージターゲットを識別するために使用します。ストレージアレイのNVMe Qualified Nameは常にサブシステムによって割り当てられ、変更はできません。NVMe Qualified Nameはアレイ全体で1つです。NVMe Qualified Nameは最大223文字です。iSCSI Qualified Nameと比較してみてください。

ネームスペースおよびネームスペースIDとは何ですか。

ネームスペースはSCSIの論理ユニットに相当し、アレイ内のボリュームに関連付けられています。ネームスペースID（NSID）は、SCSIの論理ユニット番号（LUN）に相当します。NSIDはネームスペースの作成時に作成し、1~255の値を設定できます。

NVMeコントローラとは

ホストのイニシエータからストレージシステムのターゲットへのパスを表すSCSI I_T Nexusと同様に、ホスト接続プロセスで作成されるNVMeコントローラは、ストレージアレイ内のネームスペースとホストの間のアクセスパスを提供します。NVMeコントローラはホストのNQNとホストポート識別子によって一意に識別されます。NVMeコントローラを関連付けることができるのは単一のホストのみですが、NVMeコントローラは複数のネームスペースにアクセスできます。

SANtricity System Managerを使用して、どのホストがどのネームスペースにアクセスできるかを設定し、ホストのネームスペースIDを設定します。その後、NVMeコントローラが作成されると、NVMeコントローラからアクセス可能なネームスペースIDのリストが作成され、許可される接続の設定に使用されます。

NVMeの用語

ストレージアレイに関連するNVMeの用語を次に示します。

期間	説明
InfiniBandの略	InfiniBand （ IB ）は、ハイパフォーマンスのサーバとストレージシステムの間のデータ転送用の通信標準です。
ネームスペース	ネームスペースは、ブロックアクセス用にフォーマットされたNVMストレージです。SCSIの論理ユニットに相当し、ストレージアレイではボリュームに関連します。
ネームスペースID	ネームスペースIDは、NVMeコントローラのネームスペースの一意の識別子です。1~255の値を設定できます。SCSIの論理ユニット番号（LUN）に相当します。
NQN	NVMe Qualified Name（NQN）は、リモートストレージターゲット（ストレージアレイ）を識別するために使用します。
NVM	非揮発性メモリ（NVM）は、多くのタイプのストレージデバイスで使用されている永続的メモリです。

期間	説明
NVMe	Non-Volatile Memory Express（NVMe）は、SSDドライブなどのフラッシュベースのストレージデバイス向けに設計されたインターフェイスです。以前の論理デバイスインターフェイスに比べ、I/Oオーバーヘッドが少なく、パフォーマンスも向上しています。
NVMe-oF	Non-Volatile Memory Express over Fabrics（NVMe-oF）は、NVMeコマンドとデータをホストとストレージ間でネットワーク経由で転送するための仕様です。
NVMeコントローラ	NVMeコントローラはホストの接続プロセス中に作成されます。ホストとストレージアレイ内のネームスペースの間のアクセスパスを提供します。
NVMeキューです	NVMeインターフェイス経由でのコマンドやメッセージの受け渡しに使用されるキューです。
NVMe サブシステム	NVMeホストに接続されているストレージアレイです。
RDMA	Remote Direct Memory Access（RDMA）を使用すると、ネットワークインターフェイスカード（NIC）ハードウェアに転送プロトコルを実装することで、サーバとの間でより直接的なデータ移動を実現できます。
RoCE	RDMA over Converged Ethernet （ RoCE ）は、イーサネットネットワークを介したリモートダイレクトメモリアクセス（ RDMA ）を可能にするネットワークプロトコルです。
SSD の場合	ソリッドステートディスク（ SSD ）は、ソリッドステートメモリ（フラッシュ）を使用してデータを永続的に格納するデータストレージデバイスです。SSD は従来のハードドライブをエミュレートしたものであり、ハードドライブと同じインターフェイスで利用できます。

方法

NVMe over InfiniBandポートを設定する

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またはシステムページでNVMeポートを設定できます。

作業を開始する前に

- コントローラにNVMe over InfiniBandホストポートが搭載されている必要があります。そうでないと、System ManagerでNVMe over InfiniBand設定を使用できません。
- ホスト接続のIPアドレスを確認しておく必要があります。

このタスクについて

NVMe over InfiniBand構成には、* Hardware ページまたはメニューからアクセスできます：**Settings [System]**。このタスクでは、**[*Hardware**]ページからポートを設定する方法について説明します。

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. 図にドライブが表示されている場合は、 * シェルフの背面を表示 * をクリックします。

   図の表示が切り替わり、ドライブではなくコントローラが表示されます。
3. 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. Configure NVMe over InfiniBand ports] を選択します。

   Configure NVMe over InfiniBand Ports * （ NVMe over InfiniBand ポートの設定 * ）ダイアログボックスが開きます。
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、「* Yes」をクリックしてNVMe over InfiniBandポートをリセットします。

NVMe over RoCEポートを設定します

コントローラにNVMe over RoCE（RDMA over Converged Ethernet）用の接続が含まれている場合は、ハードウェアページまたはシステムページからNVMeポートを設定できます。

作業を開始する前に

- コントローラにNVMe over RoCEホストポートが搭載されている必要があります。そうでないと、System ManagerでNVMe over RoCE設定を使用できません。
- ホスト接続のIPアドレスを確認しておく必要があります。

このタスクについて

NVMe over RoCE 構成には、 * Hardware * ページまたはメニューからアクセスできます： Settings [System] 。このタスクでは、 Hardware ページからポートを設定する方法について説明します。

NVMe over RoCE 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 RoCE 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. 図にドライブが表示されている場合は、 * シェルフの背面を表示 * をクリックします。

   図の表示が切り替わり、ドライブではなくコントローラが表示されます。
3. 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 ポートの設定 * を選択します。

   Configure NVMe over RoCE Ports（NVMe over RoCEポートの設定）ダイアログボックスが開きます。

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. 「 * 次へ * 」をクリックします。

   すべてのポート設定を表示するには、ダイアログボックスの右側にある * Show more port settings * リンクをクリックします。

   フィールドの詳細

ポートの設定	説明
イーサネットポート速度の設定	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（Show more port settingsをクリックして使用可能）	必要に応じて、 Maximum Transmission Unit （ MTU ；最大伝送ユニット）の新しいサイズをバイト単位で入力します。 デフォルトの Maximum Transmission Unit （ MTU ；最大転送単位）サイズは 1500 バイト / フレームです。1500~9000 の値を入力する必要があります。

   IPv4を有効にするを選択した場合は、次へをクリックするとIPv4設定を選択するダイアログボックスが開きます。IPv6を有効にするを選択した場合は、次へをクリックすると、IPv6設定を選択するためのダイアログボックスが開きます。両方のオプションを選択した場合は、最初にIPv4設定のダイアログボックスが開き、次へをクリックすると、IPv6設定のダイアログボックスが開きます。

7. IPv4 と IPv6 、またはその両方を自動または手動で設定します。

フィールドの詳細

ポートの設定	説明
自動的に設定を取得します	設定を自動的に取得するには、このオプションを選択します。
静的な設定を手動で指定します	このオプションを選択した場合は、フィールドに静的アドレスを入力します。（必要に応じて、住所をカットアンドペーストしてフィールドに貼り付けることもできます）。 IPv4の場合は、ネットワークのサブネットマスクとゲートウェイも指定します。IPv6 の場合は、ルーティング可能な IP アドレスとルータの IP アドレスも指定します。

8. [完了] をクリックします。

NVMe over Fabricsの統計を表示します

ストレージアレイへのNVMe over Fabrics接続に関するデータを表示できます。

このタスクについて

System Managerには、次のタイプのNVMe over Fabrics統計が表示されます。統計はすべて読み取り専用で、設定することはできません。

- * nvmeサブシステム統計*--タイムアウトや接続エラーなど、NVMeコントローラの統計が表示されます。
- *rdma Interface statistics *--送受信されたパケット情報を含むRDMAインタフェースの統計情報を提供します。

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。

NVMe over Fabrics統計には、システムページ（メニュー：設定[システム]）またはサポートページからアクセスできます。ここでは、Supportページから統計情報にアクセスする方法について説明します。

手順

1. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
2. View NVMe over Fabrics Statistics *を選択します。
3. ベースラインを設定するには、*新しいベースラインを設定*をクリックします。

   ベースラインを設定すると、統計を収集するための新しい開始ポイントが設定されます。すべてのNVMe統計に同じベースラインが使用されます。

よくある質問です

NVMe over InfiniBand統計には何が表示されますか？

View NVMe over Fabrics Statistics *ダイアログボックスには、NVMeサブシステムとNVMe over InfiniBandインターフェイスの統計が表示されます。統計はすべて読み取り専用で、設定することはできません。

- * nvmeサブシステム統計*- NVMeコントローラとそのキューの統計が表示されます。NVMeコントローラは、ストレージアレイ内のネームスペースとホストの間のアクセスパスを提供します。NVMeサブシステム統計では、接続障害、リセット、シャットダウンなどの項目を確認できます。これらの統計の詳細については、[表見出しの凡例を表示する*]をクリックしてください。
- * rdma Interface statistics **-- RDMA**インターフェイス上のすべての**NVMe over Fabrics**ポートの統計を提供します。各スイッチポートに関連付けられているパフォーマンス統計とリンクエラー情報が含まれます。統計の詳細については、**[**表見出しの凡例を表示する]をクリックしてください。

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

NVMe over Fabrics統計には何が表示されますか？

View NVMe over Fabrics Statistics *ダイアログボックスには、NVMeサブシステムとNVMe over RoCEインターフェイスの統計が表示されます。統計はすべて読み取り専用で、設定することはできません。

- * nvmeサブシステム統計*- NVMeコントローラとそのキューの統計が表示されます。NVMeコントローラは、ストレージアレイ内のネームスペースとホストの間のアクセスパスを提供します。NVMeサブシステム統計では、接続障害、リセット、シャットダウンなどの項目を確認できます。これらの統計の詳細については、[表見出しの凡例を表示する*]をクリックしてください。
- * rdma Interface statistics **-- RDMA**インターフェイス上のすべての**NVMe over Fabrics**ポートの統計を提供します。各スイッチポートに関連付けられているパフォーマンス統計とリンクエラー情報が含まれます。統計の詳細については、**[**表見出しの凡例を表示する]をクリックしてください。

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

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？

次の表に、NVMe over InfiniBandセッションの設定と管理に使用するSystem Managerの機能を示します。

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。

NVMe over InfiniBandを設定して診断します

アクション	場所
NVMe over InfiniBandポートを設定する	1. 「 * ハードウェア * 」を選択します。 2. Show back of shelf*を選択します。 3. コントローラを選択します。 4. Configure NVMe over InfiniBand ports] を選択します。 または 1. メニューを選択します。[設定][システム]。 2. 下にスクロールして* NVMe over InfiniBand settings を表示し、 Configure NVMe over InfiniBand ports *を選択します。
NVMe over InfiniBandの統計を表示します	1. メニューを選択します。[設定][システム]。 2. 下にスクロールして* NVMe over InfiniBand settings を表示し、 View NVMe over Fabrics Statistics *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、ハードウェアと設定のページで実行できます。

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。

NVMe over RoCEを設定して診断します

アクション	場所
NVMe over RoCEポートを設定します	1. 「 * ハードウェア * 」を選択します。 2. Show back of shelf*を選択します。 3. コントローラを選択します。 4. NVMe over RoCE ポートの設定 * を選択します。 または 1. メニューを選択します。[設定][システム]。 2. 下にスクロールして* NVMe over RoCE settings （**NVMe over RoCE**設定）に進み、* Configure NVMe over RoCE Ports （**NVMe over RoCE**ポートの設定）を選択します。
NVMe over Fabricsの統計を表示します	1. メニューを選択します。[設定][システム]。 2. 下にスクロールして* NVMe over RoCE settings を表示し、 View NVMe over Fabrics Statistics *を選択します。

アドオン機能

概念

アドオン機能の仕組み

アドオンは、System Managerの標準構成には含まれていない機能で、有効にするにはキーが必要です。アドオン機能には、単一のプレミアム機能と、バンドルされた機能パックがあります。

以下に、プレミアム機能または機能パックを有効にする手順の概要を示します。

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にあります。
   - Feature Activation Code。機能購入時にサポートサイトから入手できます。
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、機能有効識別子、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。

アドオン機能に関する用語

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	説明
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]の下に表示されます。
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。

方法

機能キーファイルを取得します

ストレージアレイでプレミアム機能または機能パックを有効にするには、まず機能キーファイルを取得する必要があります。キーは1つのストレージアレイにのみ関連付けられます。

このタスクについて

このタスクでは、機能の必要な情報を収集し、機能キーファイルの要求を送信する方法について説明します。必要な情報は次のとおりです。

- シャーシのシリアル番号
- 機能有効識別子
- Feature Activation Code （機能アクティベーションコード）

手順

1. System Managerで、シャーシのシリアル番号を確認して記録します。このシリアル番号は、サポートセンターのタイルにマウスを合わせると表示されます。
2. System Manager で、機能有効識別子を確認します。[設定]、[システム]の順に移動し、下にスクロールして*アドオン*を表示します。機能有効識別子*を探します。機能有効識別子の番号を記録します。
3. Feature Activation Codeを確認して記録します。機能パックの場合、このアクティベーションコードは、変換を実行するための適切な手順に記載されています。

   ネットアップの手順説明にはからアクセスできます "NetApp Eシリーズシステムのドキュメントセンター"。

   プレミアム機能の場合は、サポートサイトから次の手順でアクティベーションコードにアクセスできます。

   a. にログインします "ネットアップサポート"。
   b. [製品の管理]>[ソフトウェアライセンス]メニューに移動します。
   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. [**License Key**]列で、Feature Activation Codeを探します。
   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、Feature Activation Code、機能有効識別子を記載したEメールまたはテキストドキュメントをストレージサプライヤに送信して、機能キーファイルをリクエストします。

   に進むこともできます "ネットアップライセンスのアクティブ化：ストレージアレイプレミアム機能のアクティブ化" 機能または機能パックを入手するために必要な情報を入力します。（このサイトの手順はプレミアム機能用であり、機能パック用ではありません）。

完了後

機能キーファイルを取得したら、プレミアム機能または機能パックを有効にすることができます。

プレミアム機能を有効にします

プレミアム機能は追加オプションであり、有効にするにはキーが必要です。

作業を開始する前に

- 機能キーを入手しておきます。キーについては、必要に応じてテクニカルサポートにお問い合わせください。
- 管理クライアント（System Managerにアクセスするためのブラウザを備えたシステム）上にキーファイルをロードしておきます。

このタスクについて

このタスクでは、System Managerを使用してプレミアム機能を有効にする方法について説明します。

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. メニューを選択します。[設定][システム]。
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。

   プレミアム機能を有効にするダイアログボックスが開きます。
3. [**Browse**](参照)をクリックし、キーファイルを選択します。

   ファイル名がダイアログボックスに表示されます。
4. [**Enable**] をクリックします。

機能パックを有効にします

機能パックは、ストレージアレイの属性を変更する（プロトコルをFibre ChannelからiSCSIに変更するなど）バンドルです。機能パックを有効にするには特別なキーが必要です。

作業を開始する前に

- 適切な手順に従って変換を実行し、新しいストレージアレイ属性に合わせてシステムを準備しておきます。

変換手順については、を参照してください "NetApp Eシリーズシステムのドキュメントセンター"。

- ストレージアレイがオフラインであり、ホストやアプリケーションからのアクセスがないことを確認します。
- すべてのデータがバックアップされます。
- 機能パックファイルを入手しておきます。

  機能パックファイルは管理クライアント（System Managerにアクセスするためのブラウザを備えたシス

テム）上にロードされます。

システムを停止するメンテナンス時間をスケジュールして、ホストとコントローラの間のすべてのI/O処理を停止する必要があります。また、変更が完了するまではストレージアレイのデータにアクセスできないことに注意してください。

このタスクについて

このタスクでは、System Managerを使用して機能パックを有効にする方法について説明します。完了したら、ストレージアレイを再起動する必要があります。

手順

1. メニューを選択します。[設定][システム]。
2. [* アドオン *] で、 [* 機能パックの変更 *] を選択します。
3. [**Browse**](参照)をクリックし、キーファイルを選択します。

   ファイル名がダイアログボックスに表示されます。
4. フィールドに「 * CHANGE * 」と入力します。
5. [変更（ Change ）] をクリックします。

   機能パックの移行が開始され、コントローラがリブートします。I/Oアクティビティをなくすために、書き込み前のキャッシュデータが削除されます。両方のコントローラが自動的にリブートし、新しい機能パックが有効になります。リブートが完了すると、ストレージアレイは応答可能な状態に戻ります。

セキュリティキーの管理

概念

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ためのセキュリティキーが必要になります。ドライブをアレイから物理的に取り外した場合、別のアレイに取り付けるまでは動作しなくなり、取り付けた時点で正しいセキュリティキーが提供されるまではセキュリティロック状態になります。

ドライブセキュリティを実装する方法

ドライブセキュリティを実装するには、次の手順を実行します。

1. ストレージアレイにセキュリティ対応のFDEドライブまたはFIPSドライブを取り付けます（FIPSのサポートが必要なドライブには、FIPSドライブのみを使用します。ボリュームグループまたはプールにFIPSドライブとFDEドライブが混在している場合、すべてのドライブがFDEドライブとして扱われます。また、FIPSドライブのみを含むボリュームグループまたはプールでは、FDEドライブを追加したりスペアとして使用したりすることはできません）。

2. セキュリティキーを作成します。セキュリティキーは、読み取り/書き込みアクセス用にコントローラとドライブで共有される文字列です。コントローラの永続的メモリから内部キーを作成するか、キー管理サーバから外部キーを作成することができます。外部キー管理の場合、キー管理サーバとの間に認証を確立する必要があります。
3. プールおよびボリュームグループに対してドライブセキュリティを有効にします。
   - プールまたはボリュームグループを作成します（受験者テーブルの「Secure Capable 」列で「 Yes」を検索してください）。
   - 新しいボリュームを作成するときにプールまたはボリュームグループを選択します（Pool and volume group Candidatesテーブルで、「* SecureCapable 」の横の「 Yes」*を探します）。

ドライブレベルでのドライブセキュリティの動作

セキュリティ対応ドライブであるFDEまたはFIPSでは、書き込み時にデータが暗号化され、読み取り時に復号化されます。この暗号化と復号化は、パフォーマンスやユーザのワークフローには影響しません。ドライブごとに固有の暗号化キーがあり、このキーをドライブから転送することはできません。

ドライブセキュリティ機能は、セキュリティ対応ドライブを使用して保護を強化します。ドライブセキュリティでこれらのドライブ上のボリュームグループまたはプールを選択すると、ドライブはセキュリティキーを確認してからデータへのアクセスを許可します。プールおよびボリュームグループのドライブセキュリティはいつでも有効にすることができ、ドライブ上の既存データへの影響はありません。ただし、ドライブセキュリティを無効にするときは、ドライブ上のすべてのデータを消去する必要があります。

ストレージアレイレベルでのドライブセキュリティの動作

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

セキュリティ有効ドライブをストレージアレイから取り外して別のストレージアレイに取り付けると、ドライブはセキュリティロック状態になります。再配置したドライブは、データに再びアクセスできるようにする前にセキュリティキーを探します。データのロックを解除するには、ソースストレージアレイからセキュリティキーを適用します。再配置したドライブのロック解除が成功すると、以降はターゲットストレージアレイにすでに格納されているセキュリティキーが使用されるため、インポートしたセキュリティキーファイルは不要になります。

内部でキーを管理する場合、実際のセキュリティキーはコントローラ上のアクセスできない場所に格納されます。人間が判読できる形式ではなく、ユーザがアクセスすることもできません。

ボリュームレベルでのドライブセキュリティの動作

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

セキュリティ有効のボリュームグループおよびプールを作成する際は、次のガイドラインに注意してください。

- ボリュームグループとプールはセキュリティ対応ドライブだけで構成されている必要があります。（FIPSのサポートが必要なドライブには、FIPSドライブのみを使用します。ボリュームグループまたはプールにFIPSドライブとFDEドライブが混在している場合、すべてのドライブがFDEドライブとして扱われます。また、FIPSドライブのみを含むボリュームグループまたはプールでは、FDEドライブを追加したりス

ペアとして使用したりすることはできません）。

- ボリュームグループとプールの状態が最適lである必要があります。

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になります。セキュリティ有効ドライブをストレージアレイから取り外すと、ドライブのデータはロックされます。ドライブを別のストレージアレイに再度取り付けると、データに再びアクセスできるようになる前にセキュリティキーが検索されます。データのロックを解除するには、元のセキュリティキーを適用する必要があります。

セキュリティキーは次のいずれかの方法で作成および管理できます。

- コントローラの永続的メモリ上での内部キー管理。
- 外部キー管理サーバでの外部キー管理

内部キー管理

内部キーは、コントローラの永続的メモリに保持されます。内部キー管理を実装するには、次の手順を実行します。

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. 識別子とパスフレーズを定義して、内部セキュリティキーを作成します。識別子は、セキュリティキーに関連付けられる文字列で、コントローラとキーに関連付けられたすべてのドライブに格納されます。パスフレーズは、バックアップ用にセキュリティキーを暗号化するために使用されます。内部キーを作成するには、メニューに移動します。[システム]、[セキュリティキー管理]、[内部キーの作成]の順に選択します。

セキュリティキーは、コントローラ上のアクセスできない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. ストレージアレイとキー管理サーバの間の認証用に、クライアントの証明書署名要求（CSR）を生成してダウンロードします。メニューに移動します。Settings [証明書]、[キー管理]、[CSRの作成]の順に選択します。
4. 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します。
5. クライアント証明書とキー管理サーバの証明書のコピーがローカルホストにあることを確認します。
6. キー管理サーバのIPアドレスとKMIP通信に使用するポート番号を定義して、外部キーを作成します。このプロセスでは、証明書ファイルもロードします。外部キーを作成するには、メニューに移動します。[設定]、[システム]、[セキュリティキー管理]、[外部キーの作成]の順に選択します。

入力したクレデンシャルを使用して、システムがキー管理サーバに接続されます。これで、セキュリティ有効のボリュームグループまたはプールを作成したり、既存のボリュームグループまたはプールでセキュリティを有効にしたりできます。

ドライブセキュリティの用語

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	説明
ドライブセキュリティ機能	ドライブセキュリティは、 Full Disk Encryption （ FDE ）ドライブまたは連邦情報処理標準（ FIPS ）ドライブを使用してセキュリティを強化するストレージアレイの機能です。これらのドライブにドライブセキュリティ機能を使用すると、データにアクセスするためのセキュリティキーが必要になります。ドライブをアレイから物理的に取り外した場合、別のアレイに取り付けるまでは動作しなくなり、取り付けた時点で正しいセキュリティキーが提供されるまではセキュリティロック状態になります。
FDEドライブ	Full Disk Encryption（FDE）ドライブは、ハードウェアレベルでディスクドライブの暗号化を実行します。ハードドライブに搭載されたASICチップにより、書き込み時にデータが暗号化され、読み取り時に復号化されます。
FIPSドライブ	FIPSドライブは、連邦情報処理標準（FIPS）140-2レベル2に準拠しています。基本的な概念はFDEドライブと同じですが、米国政府の基準に従って強力な暗号化アルゴリズムと暗号化方式を実装しています。FIPSドライブにはFDEドライブよりも高度なセキュリティ基準が採用されています。
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含むローカルシステム（コンピュータやタブレットなど）。

期間	説明
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無関係です。
セキュリティ対応ドライブ	セキュリティ対応ドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。これらのドライブでは、書き込み時にデータが暗号化され、読み取り時に復号化されます。ドライブセキュリティ機能を使用したセキュリティの強化に使用できるため、これらのドライブはsecured_capable_とみなされます。これらのドライブを使用するボリュームグループやプールでドライブセキュリティ機能を有効にすると、ドライブはsecure-_enabled_になります。
セキュリティ有効ドライブ	セキュリティ有効ドライブは、ドライブセキュリティ機能で使用されます。ドライブセキュリティ機能を有効にし、かつsecured_caped_drivesのプールまたはボリュームグループにドライブセキュリティを適用すると、ドライブはsecure*enable*になります。読み取りおよび書き込みアクセスは、正しいセキュリティキーが設定されたコントローラからしか実行できません。この追加のセキュリティ機能により、ストレージアレイから物理的に取り外されたドライブ上のデータへの不正アクセスを防止できます。

期間	説明
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になります。セキュリティ有効ドライブをストレージアレイから取り外すと、ドライブのデータはロックされます。ドライブを別のストレージアレイに再度取り付けると、データに再びアクセスできるようになる前にセキュリティキーが検索されます。データのロックを解除するには、元のセキュリティキーを適用する必要があります。セキュリティキーは次のいずれかの方法で作成および管理できます。 • 内部キー管理—セキュリティキーをコントローラの永続的メモリに作成して保管します • 外部キー管理—セキュリティキーを外部キー管理サーバに作成して保管します
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セキュリティキーに関連付けられる文字列です。この識別子は、コントローラとセキュリティキーに関連付けられたすべてのドライブに格納されます。

方法

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。

作業を開始する前に

- ストレージアレイにセキュリティ対応ドライブが搭載されている必要があります。対応するドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。
- ドライブセキュリティ機能を有効にする必要があります。それ以外の場合は、このタスクの実行中に[セキュリティキーを作成できません*]ダイアログボックスが開きます。ドライブセキュリティ機能を有効にする手順については、必要に応じてストレージベンダーに問い合わせてください。

ストレージアレイにFDEドライブとFIPSドライブの両方が搭載されている場合、すべてのドライブで同じセキュリティキーが共有されます。

このタスクについて

このタスクでは、内部セキュリティキーに関連付ける識別子とパスフレーズを定義します。

ドライブセキュリティのパスフレーズは、ストレージアレイの管理者パスワードとは無関係です。

手順

1. メニューを選択します。[設定][システム]。
2. セキュリティキー管理*で、*内部キーの作成*を選択します。

   まだセキュリティキーを生成していない場合は、[セキュリティキーの作成*]ダイアログボックスが開きます。

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—デフォルト値(コントローラファームウェアによって生成されたストレージアレイ名とタイムスタンプ)を受け入れるか'独自の値を入力できます入力できる文字数は最大189文字です。使用できるのは英数字のみで、スペース、句読点、記号は使用できません。

     入力した文字列の前後に追加の文字が自動的に生成されて付加されます。文字が追加されることで識別子が一意であることが保証されます。

   - パスフレーズを定義/パスフレーズを再入力—パスフレーズを入力して確認します8~32文字で指定し、以下の文字をそれぞれ1文字以上含める必要があります。
     - 大文字のアルファベット（1文字以上）。パスフレーズでは大文字と小文字が区別されることに注意してください。
     - 数字（1文字以上）。
     - 英数字以外の、！、*、@などの文字（1文字以上）。

   あとで使用できるように、エントリを記録しておいてください。セキュリティ有効ドライブをストレージアレイから移動する必要がある場合、ドライブデータのロックを解除するために識別子とパスフレーズが必要になります。

4. [作成（ Create ）] をクリックします。

   セキュリティキーは、コントローラ上のアクセスできない場所に格納されます。実際のキーとともに、ブラウザからダウンロードされた暗号化されたキーファイルも格納されます。

   ダウンロードファイルのパスは、ブラウザのデフォルトのダウンロード先によって異なる場合があります。

5. キー識別子、パスフレーズ、ダウンロードしたキーファイルの場所を記録し、*閉じる*をクリックします。

結果

これで、セキュリティ有効のボリュームグループまたはプールを作成したり、既存のボリュームグループまたはプールでセキュリティを有効にしたりできます。

ドライブの電源をオフにしてオンにするたびに、すべてのセキュリティ有効ドライブがセキュリティロック状態になります。この状態のドライブのデータには、ドライブの初期化時にコントローラによって正しいセキュリティキーが適用されるまでアクセスできません。第三者がロックされたドライブを物理的に取り外して別のシステムに取り付けた場合でも、データへの不正アクセスを防止することができます。

完了後

セキュリティキーを検証して、キーファイルが破損していないことを確認します。

外部セキュリティキーを作成します

キー管理サーバでドライブセキュリティ機能を使用するには、キー管理サーバとストレージアレイのセキュリティ対応ドライブで共有する外部キーを作成する必要があります。

作業を開始する前に

- アレイにセキュリティ対応ドライブが搭載されている必要があります。対応するドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。

  ストレージアレイにFDEドライブとFIPSドライブの両方が搭載されている場合、すべてのドライブで同じセキュリティキーが共有されます。

- ドライブセキュリティ機能を有効にする必要があります。それ以外の場合は、このタスクの実行中に[セキュリティキーを作成できません*]ダイアログボックスが開きます。ドライブセキュリティ機能を有効にする手順については、必要に応じてストレージベンダーに問い合わせてください。
- ストレージアレイとキー管理サーバが相互に認証できるように、クライアント証明書とサーバ証明書をローカルホストに用意します。クライアント証明書はコントローラを、サーバ証明書はキー管理サーバを検証します。

このタスクについて

このタスクでは、キー管理サーバのIPアドレスと使用するポート番号を定義し、外部キー管理に使用する証明書をロードします。

手順

1. メニューを選択します。[設定][システム]。
2. セキュリティキー管理*で、*外部キーの作成*を選択します。

   内部キー管理が現在設定されている場合は、外部キー管理に切り替えるかどうかの確認を求めるダイアログボックスが表示されます。

   [外部セキュリティキーの作成*]ダイアログボックスが開きます。

3. [キーサーバへの接続]で、次のフィールドに情報を入力します。
   - キー管理サーバのアドレス-キー管理に使用するサーバの完全修飾ドメイン名またはIPアドレス（IPv4またはIPv6）を入力します。
   - キー管理ポート番号-- Key Management Interoperability Protocol (KMIP)通信に使用するポート番号を入力しますキー管理サーバの通信に使用される最も一般的なポート番号は5696です。

- クライアント証明書の選択—最初の参照ボタンをクリックして'ストレージアレイのコントローラの証明書ファイルを選択します
- キー管理サーバのサーバ証明書を選択します-- 2番目の参照ボタンをクリックして'キー管理サーバの証明書ファイルを選択します

4. 「 * 次へ * 」をクリックします。
5. [**Create/Backup Key**](キーの作成/バックアップ)*で、次のフィールドに情報を入力します。
   - パスフレーズを定義/パスフレーズを再入力—パスフレーズを入力して確認します8~32文字で指定し、以下の文字をそれぞれ1文字以上含める必要があります。
     - 大文字のアルファベット（1文字以上）。パスフレーズでは大文字と小文字が区別されることに注意してください。
     - 数字（1文字以上）。
     - 英数字以外の、！、*、@などの文字（1文字以上）。

   あとで使用できるように、エントリを記録しておいてください。セキュリティ有効ドライブをストレージアレイから移動する必要がある場合、ドライブデータのロックを解除するためにパスフレーズが必要になります。

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よっ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、*閉じる*をクリックします。

   次のメッセージと外部キー管理へのリンクが表示されます。

   現在のキー管理方法:外部

8. 「* Test Communication *」を選択して、ストレージアレイとキー管理サーバの間の接続をテストします。

   テスト結果がダイアログボックスに表示されます。

結果

外部キー管理を有効にすると、セキュリティ有効のボリュームグループまたはプールを作成したり、既存のボリュームグループまたはプールでセキュリティを有効にしたりできます。

ドライブの電源をオフにしてオンにするたびに、すべてのセキュリティ有効ドライブがセキュリティロック状態になります。この状態のドライブのデータには、ドライブの初期化時にコントローラによって正しいセキュリティキーが適用されるまでアクセスできません。第三者がロックされたドライブを物理的に取り外して別のシステムに取り付けた場合でも、データへの不正アクセスを防止することができます。

完了後

- セキュリティキーを検証して、キーファイルが破損していないことを確認します。

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置き換えることができます。社内でセキュリティ侵害の可能性があり、ドライブのデータへの不正アクセスを防ぎたい場合は、セキュリティキーの変更が必要になることがあります。

作業を開始する前に

セキュリティキーがすでに存在している必要があります。

このタスクについて

このタスクでは、セキュリティキーを変更し、新しいセキュリティキーに置き換える方法について説明します。この処理が完了すると、古いキーは無効になります。

手順

1. メニューを選択します。[設定][システム]。
2. 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--(内部セキュリティキーの場合のみ) デフォルト値（コントローラファームウェアで生成されたストレージアレイ名とタイムスタンプ）をそのまま使用するか、独自の値を入力します。入力できる文字数は最大189文字です。使用できるのは英数字のみで、スペース、句読点、記号は使用できません。

     入力した文字列の前後に追加の文字が自動的に生成されて付加されます。文字が追加されることで識別子が一意であることが保証されます。

   - パスフレーズを定義/パスフレーズを再入力—これらの各フィールドにパスフレーズを入力します8~32文字で指定し、以下の文字をそれぞれ1文字以上含める必要があります。
     - 大文字のアルファベット（1文字以上）。パスフレーズでは大文字と小文字が区別されることに注意してください。
     - 数字（1文字以上）。
     - 英数字以外の、！、*、@などの文字（1文字以上）。

     この値はあとで使用するため必ずメモしておいてください。セキュリティ有効ドライブをストレージアレイから移動する必要がある場合、ドライブデータのロックを解除するために識別子とパスフレーズが必要になります。

4. [変更（ Change ）] をクリックします。

   前のキーが新しいセキュリティキーで上書きされ、無効になります。

   ダウンロードファイルのパスは、ブラウザのデフォルトのダウンロード先によって異なる場合があります。

5. キー識別子、パスフレーズ、ダウンロードしたキーファイルの場所を記録し、*閉じる*をクリックします。

完了後

セキュリティキーを検証して、キーファイルが破損していないことを確認します。

外部キー管理から内部キー管理に切り替えます

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。

作業を開始する前に

外部キーが作成されている必要があります。

このタスクについて

このタスクでは、外部キー管理を無効にして、新しいバックアップコピーをローカルホストにダウンロードします。既存のキーは引き続きドライブセキュリティに使用されますが、ストレージアレイで内部的に管理されます。

手順

1. メニューを選択します。[設定][システム]。
2. [セキュリティキー管理]で、[外部キー管理を無効にする]を選択します。

   [外部キー管理を無効にする]ダイアログボックスが開きます。

3. 「パスフレーズを定義/パスフレーズを再入力」で、キーのバックアップに使用するパスフレーズを入力して確認します。8~32文字で指定し、以下の文字をそれぞれ1文字以上含める必要があります。

   - 大文字のアルファベット（1文字以上）。パスフレーズでは大文字と小文字が区別されることに注意してください。
   - 数字（1文字以上）。
   - 英数字以外の、！、*、@などの文字（1文字以上）。

   

   _後で使用するために、必ずエントリを記録しておいてください。セキュリティ有効ドライブをストレージアレイから移動する必要がある場合、ドライブデータのロックを解除するために識別子とパスフレーズが必要になります。

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、ダウンロードしたキーファイルの場所を記録し、*閉じる*をクリックします。

結果

ドライブセキュリティがストレージアレイを使用して内部的に管理されるようになりました。

完了後

- セキュリティキーを検証して、キーファイルが破損していないことを確認します。

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している場合、キー管理サーバの設定をいつでも表示および編集することができます。

作業を開始する前に

外部キー管理が設定されている必要があります。

手順

1. メニューを選択します。[設定][システム]。
2. セキュリティキー管理*で、*キー管理サーバ設定の表示/編集*を選択します。
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。
   - KMIP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
4. [保存（ Save ）] をクリックします。

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。

作業を開始する前に

- セキュリティキーがすでに存在している必要があります。

このタスクについて

このタスクでは、以前に作成したセキュリティキーをバックアップする方法について説明します。この手順では、バックアップ用の新しいパスフレーズを作成します。このパスフレーズは、元のキーの作成時または最後の変更時に使用されたパスフレーズと同じである必要はありません。このパスフレーズは、作成するバックアップにのみ適用されます。

手順

1. メニューを選択します。[設定][システム]。
2. セキュリティキー管理*で、*バックアップキー*を選択します。

   [セキュリティキーのバックアップ*]ダイアログボックスが開きます。

3. [パスフレーズを定義/パスフレーズを再入力]フィールドに、このバックアップのパスフレーズを入力して確認します。

   8~32文字で指定し、以下の文字をそれぞれ1文字以上含める必要があります。

   - 大文字のアルファベット（1文字以上）

- 数字（1文字以上）
- アルファベット以外の文字（！、*、@など）（1文字以上）

> あとで使用できるように、エントリを記録しておいてください。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. [バックアップ]をクリックします。

   セキュリティキーのバックアップがローカルホストにダウンロードされ、[**Confirm/Record Security Key Backup**]ダイアログボックスが開きます。

> 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、*閉じる*をクリックします。

完了後

バックアップセキュリティキーを検証する必要があります。

セキュリティキーを検証する

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。

作業を開始する前に

セキュリティキーが作成されている必要があります。

このタスクについて

このタスクでは、以前に作成したセキュリティキーを検証する方法について説明します。これは、キーファイルが破損していないこと、およびパスフレーズが正しいことを確認するための重要な手順です。これにより、セキュリティ有効ドライブをストレージアレイ間で移動する場合に、あとからドライブデータにアクセスできます。

手順

1. メニューを選択します。[設定][システム]。
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**](参照)をクリックし’キーファイル(たとえば’drives] ecsecurity.slk`)を選択します
4. 選択したキーに関連付けられているパスフレーズを入力します。

   有効なキーファイルとパスフレーズを選択すると、*検証*ボタンが使用可能になります。

5. [*Validate]をクリックします。

   検証結果がダイアログボックスに表示されます。

6. 結果に「セキュリティキーの検証に成功しました」と表示された場合は、*閉じる*をクリックします。エラーメッセージが表示された場合は、ダイアログボックスに表示される推奨手順に従います。

セキュリティキーを使用してドライブのロックを解除します

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は、適切なセキュリティキーを新しいストレージアレイにインポートする必要があります。キーをインポートすると、ドライブ上のデータのロックが解除されます。

作業を開始する前に

- （ドライブの移動先となる）ターゲットストレージアレイでセキュリティキーが設定済みである必要があります。移行されたドライブのキーはターゲットストレージアレイのキーに変更されます。
- ロックを解除するドライブに関連付けられているセキュリティキーを把握しておく必要があります。
- セキュリティキーファイルは管理クライアント（System Managerへのアクセスに使用するブラウザを備えたシステム）にあります。別のシステムで管理されるストレージアレイにドライブを移動する場合は、その管理クライアントにセキュリティキーファイルを移動する必要があります。

このタスクについて

このタスクでは、あるストレージアレイから取り外されて別のストレージアレイに再度取り付けられたセキュリティ有効ドライブ内のデータのロックを解除する方法について説明します。アレイでドライブが検出されると、再配置されたこれらのドライブに対して「Needs Attention」状態と「Security Key Needed」ステータスが表示されます。ドライブのセキュリティキーをストレージアレイにインポートすることで、ドライブデータのロックを解除できます。このプロセスでは、セキュリティキーファイルを選択して、キーのパスフレーズを入力します。

パスフレーズはストレージアレイの管理者パスワードとは異なります。

新しいストレージアレイに取り付けられている他のセキュリティ有効ドライブでは、インポートするセキュリティキーとは別のセキュリティキーが使用される場合があります。インポートプロセスでは、取り付けるドライブのデータのロック解除にのみ古いセキュリティキーが使用されます。ロック解除プロセスが成功すると、新しく取り付けたドライブのキーがターゲットストレージアレイのセキュリティキーに変更されます。

手順

1. メニューを選択します。[設定][システム]。
2. セキュリティキー管理*で、*セキュアドライブのロック解除*を選択します。

   [セキュアドライブのロック解除*]ダイアログボックスが開きます。セキュリティキーを必要とするドライブがテーブルに表示されます。

3. 必要に応じて、ドライブの場所（シェルフ番号およびベイ番号）を確認するドライブ番号にカーソルを合わせます。
4. [*参照]をクリックし、ロックを解除するドライブに対応するセキュリティキーファイルを選択します。

   選択したキーファイルがダイアログボックスに表示されます。

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. [ロック解除]をクリックします。

   ロック解除処理が成功すると、「The associated secure drives have been unlocked」というメッセージを示すダイアログボックスが表示されます。

結果

すべてのドライブがロックされたあとでロック解除されると、ストレージアレイ内の各コントローラがリブートされます。ただし、ターゲットストレージアレイ内の一部のドライブがすでにロック解除されている場合、コントローラはリブートされません。

よくある質問です

セキュリティキーを作成するときは、どのような点に注意する必要がありますか？

セキュリティキーは、ストレージアレイ内のコントローラとセキュリティ有効ドライブによって共有されます。セキュリティ有効ドライブをストレージアレイから取り外すと、セキュリティキーによってデータが不正アクセスから保護されます。

セキュリティキーは次のいずれかの方法で作成および管理できます。

- コントローラの永続的メモリ上での内部キー管理。
- 外部キー管理サーバでの外部キー管理

内部セキュリティキーを作成する前に、次の作業を行う必要があります。

1. ストレージアレイにセキュリティ対応ドライブを取り付けます。対応するドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。
2. ドライブセキュリティ機能が有効になっていることを確認します。ドライブセキュリティ機能を有効にする手順については、必要に応じてストレージベンダーに問い合わせてください。

識別子とパスフレーズを定義して、内部セキュリティキーを作成します。識別子は、セキュリティキーに関連付けられる文字列で、コントローラとキーに関連付けられたすべてのドライブに格納されます。パスフレーズは、バックアップ用にセキュリティキーを暗号化するために使用されます。作成したセキュリティキーは、コントローラ上のアクセスできない場所に格納されます。これで、セキュリティ有効のボリュームグループまたはプールを作成したり、既存のボリュームグループまたはプールでセキュリティを有効にしたりできます。

外部セキュリティキーを作成する前に、次の作業を行う必要があります。

1. ストレージアレイにセキュリティ対応ドライブを取り付けます。対応するドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。
2. ドライブセキュリティ機能が有効になっていることを確認します。ドライブセキュリティ機能を有効にする手順については、必要に応じてストレージベンダーに問い合わせてください。
3. ストレージアレイとキー管理サーバの間の認証用に、クライアントの証明書署名要求（CSR）を生成してダウンロードします。メニューに移動します。Settings [証明書]、[キー管理]、[CSRの作成]の順に選択します。
4. 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します。
5. クライアント証明書とキー管理サーバの証明書のコピーがローカルホストにあることを確認します。

キー管理サーバのIPアドレスとKMIP通信に使用するポート番号を定義して、外部キーを作成します。このプロセスでは、証明書ファイルもロードします。作成が完了すると、入力したクレデンシャルを使用してキー管理サーバに接続されます。これで、セキュリティ有効のボリュームグループまたはプールを作成したり、既存のボリュームグループまたはプールでセキュリティを有効にしたりできます。

パスフレーズを定義する必要があるのはなぜですか？

パスフレーズは、ローカルの管理クライアントに格納されているセキュリティキーファイルの暗号化と復号化に使用されます。パスフレーズがないとセキュリティキーを復号化できず、セキュリティ有効ドライブが別のストレージアレイに再設置された場合、データのロック解除にセキュリティキーを使用できません。

セキュリティキー情報を記録することが重要なのはなぜですか。

セキュリティキー情報が失われてバックアップがない場合、セキュリティ有効ドライブの再配置時やコントローラのアップグレード時にデータが失われる可能性があります。ドライブ上のデータのロックを解除するには、セキュリティキーが必要です。

セキュリティキー識別子、関連付けられているパスフレーズ、およびセキュリティキーファイルが保存されていたローカルホスト上の場所を書き留めておいてください。

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態で元のセキュリティキーが破損すると、ドライブ上のデータがストレージアレイ間で移行される場合に、そのデータにアクセスできなくなります。

セキュリティキーをバックアップする際は、次のガイドラインに注意してください。

- 元のキーファイルのセキュリティキー識別子とパスフレーズを確認しておきます。

  識別子を使用するのは内部キーのみです。識別子を作成すると、追加の文字が自動的に生成され、識別子の文字列の両端に追加されます。文字が追加されることで識別子が一意であることが保証されます。

- バックアップ用の新しいパスフレーズを作成します。このパスフレーズは、元のキーの作成時または最後の変更時に使用されたパスフレーズと同じである必要はありません。このパスフレーズは、作成するバックアップにのみ適用されます。

  ドライブセキュリティのパスフレーズをストレージアレイの管理者パスワードと混同しないでください。ドライブセキュリティのパスフレーズは、セキュリティキーのバックアップを保護します。管理者パスワードは、ストレージアレイ全体を不正アクセスから保護します。

- バックアップセキュリティキーファイルが管理クライアントにダウンロードされます。ダウンロードファイルのパスは、ブラウザのデフォルトのダウンロード先によって異なる場合があります。セキュリティキー情報の格納場所を記録しておいてください。

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？

新しいストレージアレイに移動したセキュリティ有効ドライブのデータロックを解除するには、ドライブのセキュリティキーをインポートする必要があります。

セキュリティ有効ドライブのロックを解除する際は、次のガイドラインに注意してください。

- （ドライブの移動先となる）ターゲット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、セキュリティキー識別子とセキュリティキーファイルに対応するパスフレーズを確認しておきます。
- セキュリティキーファイルは管理クライアント（System Managerへのアクセスに使用するブラウザを備えたシステム）にあります。

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含まれています。「読み取り/書き込みアクセス」は、ドライブのデータがロックされている場合に表示される属性の1つです。

ドライブセキュリティ*属性を表示するには、ハードウェアページに移動します。ドライブを選択し、*設定の表示*をクリックして、*詳細設定を表示*をクリックします。ドライブのロックが解除されている場合、ページの下部にある「読み取り/書き込みアクセス可能」属性の値は「*はい」です。読み取り/書き込みアクセス可能属性の値は*いいえ、ドライブがロックされている場合は無効なセキュリティキー*です。セキュリティキーをインポートすることで、セキュアドライブのロックを解除できます（メニュー：[設定][システム]>[セキュアドライブのロック解除]に進みます）。

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、次の手順を実行します。

- セキュリティキー識別子がコントローラ上の識別子と一致しない場合は、正しいセキュリティキーファイルを探して検証をやり直してください。
- コントローラが検証用のセキュリティキーを復号化できない場合は、パスフレーズが正しく入力されていない可能性があります。パスフレーズを再度確認し、必要に応じて再入力してから検証をやり直してください。エラーメッセージが再び表示される場合は、キーファイルのバックアップを選択し（使用可能な場合）、検証をやり直してください。
- それでもセキュリティキーを検証できない場合は、元のファイルが破損している可能性があります。キーの新しいバックアップを作成し、そのコピーを検証してください。

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、ストレージアレイからセキュリティ有効ドライブを取り外すと、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データをロックダウンできます。

セキュリティキーは、ストレージアレイのセキュリティ有効ドライブとコントローラで共有される文字列です。内部キーは、コントローラの永続的メモリに保持されます。外部キーは、Key Management Interoperability Protocol（KMIP）を使用して別のキー管理サーバに保持されます。