



Eシリーズ

Eシリーズ コントローラ アップグレード ガイド

2019年11月 | 215-13050_2019-11_ja-jp
ng-gpso-jp-documents@netapp.com

目次

概要と要件	4
このガイドの対象者	4
アップグレード時の考慮事項	4
アップグレード時の互換性	5
Eシリーズコントローラのアップグレード	8
コントローラをアップグレードする準備	8
コントローラの取り外し	12
手順1: コントローラを取り外す	12
手順2: バッテリを取り外す	13
新しいコントローラの取り付け	14
手順1: バッテリを取り付ける	14
手順2: 新しいコントローラ キャニスターを取り付ける	15
ドライブのロック解除	16
内部セキュリティ キーの作成	17
内部キー管理を使用して1本以上のドライブがセキュリティ保護 されている場合のコントローラの交換	18
外部セキュリティ キーの作成	20
外部キー管理を使用してすべてのドライブがセキュリティ保護さ れている場合のコントローラの交換	22
コントローラのアップグレード後の処理	25
手順1: コントローラの電源をオンにする	25
手順2: コントローラとトレイのステータスを確認する	27
手順3: コントローラのソフトウェアのバージョンを確認する	27
ベンダーがLSIからNETAPPに変わった場合のボリュームの再マウント	29
AIXホストでのボリュームの再マウント	29
VMwareホストでのボリュームの再マウント	29
Windowsホストでのボリュームの再マウント	30
データ保持が不要な場合の新しいSAS-3コントローラ シェルフの 背後でのSAS-2システムの再構成	31
手順1: コントローラの電源をオフにする（データ保持なし）	31
手順2: コントローラを取り付ける（データ保持なし）	32
手順3: コントローラの電源をオンにする（データ保持なし）	32
著作権に関する情報	34
商標に関する情報	35
マニュアルの更新について	36

概要と要件

アップグレードに際しての注意事項とサポートされるアップグレードパスについて説明します。

このガイドの対象者

この手順は、通常、すべてのコントローラを別のモデルまたはプラットフォームにアップグレードするために、コントローラ ドライブトレイのすべてのコントローラを交換する場合に使用します。

そのほか、次のような状況でも使用することがあります。

- コントローラ ドライブトレイのすべてのコントローラでハードウェア障害が発生して機能しなくなった場合。
- コントローラ ドライブトレイのDual Inline Memory Module (DIMM) をアップグレードするために、同じモデルのDIMMが異なるコントローラに両方のコントローラを交換する場合。

注: この手順には、HICのアップグレードシナリオは含まれていません。HICの追加、アップグレード、交換については、Eシリーズシステムの該当する手順を参照してください。

アップグレード時の考慮事項

コントローラのアップグレードに際して注意が必要な考慮事項について説明します。

- **デュプレックスとシンプレックスのコントローラのアップグレード**
デュプレックスのコントローラ ドライブトレイの場合は、両方のコントローラを交換します。シンプレックスのコントローラ ドライブトレイの場合は、1台のコントローラを交換します。どちらの場合も、コントローラ ドライブトレイの電源をオフにする必要があります。そのため、交換が完了するまではストレージアレイのデータにアクセスできません。
- **トレイとシェルフ**
E2800またはE5700のコントローラシェルフを搭載したストレージアレイでは、一般にSANtricity System Managerを使用します。それに加え、E2800またはE5700のコントローラシェルフの管理には、SANtricity Storage ManagerのEnterprise Management Window (EMW) も使用できます。この手順で説明している他のコントローラ ドライブトレイでは、いずれもSANtricity Storage Managerを使用します。
- **コントローラのバッテリー**
新しいコントローラはバッテリーを取り付けていない状態で出荷されます。可能な場合は、古いコントローラからバッテリーを取り外し、そのバッテリーを新しいコントローラに取り付けてください。ただし、一部のコントローラのアップグレードでは、新しいコントローラと互換性がないために古いコントローラのバッテリーを使用できない場合があります。その場合は、新しいコントローラと一緒にバッテリーを注文して、これらのタスクを開始する前に準備しておく必要があります。
- **ベンダーID**
一部のコントローラのアップグレードでは、SCSI Inquiryで表示されるデータのベンダーIDがLSIからNETAPPに変わります。ベンダーIDがLSIからNETAPPに変わった場合は、Windows、VMware、およびAIXの各オペレーティングシステムでデバイスを再利用する

ための追加の手順が必要になります。このアップグレード手順で、それらの各オペレーティングシステムの対応する手順を紹介しています。

- 同期ミラーリングと非同期ミラーリング**
 ストレージ アレイの同期ミラーリングでは、プライマリ サイトとリモート サイトの間の接続としてiSCSIまたはFibre Channelのみがサポートされます。新しいコントローラのホスト インターフェイス カード（HIC）構成にiSCSI接続またはFibre Channel接続が含まれていない場合、同期ミラーリングはサポートされません。
 非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 アレイで異なるバージョンのファームウェアを実行していてもかまいません。サポートされるファームウェアの最小バージョンはSANtricityファームウェアバージョン7.84です。
- ストレージ オブジェクトの制限**
 コントローラを5x00モデルから2x00モデルに変更した場合、新しいストレージ アレイの構成では、ストレージ管理ソフトウェアでサポートされる一部のストレージ オブジェクト（ボリュームなど）の数が古い構成よりも少なくなります。古い構成でストレージ オブジェクトの制限を超えていないことを確認する必要があります。詳細については、[Netapp Hardware Universe](#)を参照してください。

新しいモデルへのアップグレード

コントローラを交換して新しいモデルにアップグレードする際は、現在のストレージ アレイにインストールされているプレミアム機能が新しいモデルではサポートされない場合があります。ことに注意してください。たとえば、E2700コントローラでは、従来のSnapshotプレミアム機能はサポートされません。

E2600コントローラをE2700コントローラに交換する際、ストレージ アレイで従来のSnapshot機能を使用していた場合は、コントローラを交換する前に、その機能を無効にして、その機能に関連付けられているすべてのボリューム（Snapshotとリポジトリ）を削除するか変換する必要があります。従来のSnapshotを更新されたSnapshot機能に変換できます。コントローラドライブトレイをアップグレードする前に、ストレージ アレイで使用しているプレミアム機能に新しいコントローラでサポートされない機能が含まれている場合は、それらの機能を無効にしてください。

アップグレード時の互換性

サポートされているアップグレード パスについて説明します。

E2x00からE2x00

- バッテリー** : 古いバッテリーを再利用します。
- ベンダーID** - 追加の手順が必要です。
- 機能のサポート** - E2700では、従来のSnapshotはサポートされません。
- SAS-2シェルフ** : E2800コントローラはSAS-2シェルフには配置できません。

E2x00からE5x00

- バッテリー** : 新しいバッテリーを注文します。
- ベンダーID** : E2600からE5500またはE5600にアップグレードする場合、またはE2700からE5400にアップグレードする場合は、追加の手順が必要です。
- 機能のサポート** : E5500またはE5600では、従来のSnapshotはサポートされません。
 iSCSI HICを搭載したE5500またはE5600では、従来のRVMはサポートされません。
 iSCSI HICを搭載したE5500またはE5600では、Data Assuranceはサポートされません。

6 | Eシリーズ コントローラ アップグレード ガイド

E5700コントローラはSAS-2シェルフには配置できません。

- **SAS-3シェルフ** : E5400、E5500、およびE5600コントローラはSAS-3シェルフには配置できません。

E5x00からE2x00

- **バッテリー** : 新しいバッテリーを注文します。
- **ベンダーID** : E5500またはE5600からE2600にアップグレードする場合、またはE5400からE2700にアップグレードする場合は、追加の手順が必要です。
- **機能のサポート** : E2700では、従来のSnapshotはサポートされません。
- **SAS-3シェルフ** : E5400、E5500、およびE5600コントローラはSAS-3シェルフには配置できません。

E5x00からE5x00

- **バッテリー** : 古いバッテリーを再利用します。
- **ベンダーID** : E5400からE5500またはE5600にアップグレードする場合は、追加の手順が必要です。
- **機能のサポート** : E5500またはE5600では、従来のSnapshotはサポートされません。
iSCSI HICを搭載したE5400またはE5500では、従来のRVMはサポートされません。
iSCSI HICを搭載したE5400またはE5500では、Data Assuranceはサポートされません。
E5700コントローラはSAS-2シェルフには配置できません。
- **SAS-3シェルフ** : E5400、E5500、およびE5600コントローラはSAS-3シェルフには配置できません。

EF5x0からEF5x0

- **バッテリー** : 古いバッテリーを再利用します。
- **ベンダーID** : EF540からEF550またはEF560にアップグレードする場合は、追加の手順が必要です。
- **機能のサポート** : EF550 / EF560では、従来のSnapshotはサポートされません。
iSCSIを搭載したEF550 / EF560では、Data Assuranceはサポートされません。
EF570コントローラはSAS-3シェルフには配置できません。
- **SAS-3シェルフ** : EF540、EF550、およびEF560コントローラはSAS-3シェルフには配置できません。

SASエンクロージャ

E5700では、ヘッドのアップグレードにより、DE5600およびDE6600のSAS-2エンクロージャがサポートされます。SAS-2エンクロージャでE5700コントローラを利用するときは、オンボード ホスト ポートのサポートは無効になります。

SAS-2シェルフ	SAS-3シェルフ
<p>SAS-2シェルフには次のモデルがあります。</p> <ul style="list-style-type: none"> • DE1600、DE5600、およびDE6600ドライブトレイ • E5400、E5500、およびE5600コントローラドライブトレイ • EF540、EF550、およびEF560フラッシュアレイ • E2600およびE2700コントローラドライブトレイ 	<p>SAS-3シェルフには次のモデルがあります。</p> <ul style="list-style-type: none"> • E2800コントローラシェルフ • E5700コントローラシェルフ • DE212C、DE224C、およびDE460Cドライブシェルフ

SAS-2からSAS-3への投資の保護

SAS-2システムを新しいSAS-3コントローラシェルフ（E57XX / EF570 / E28XX）の背後で使用するよう再構成できます。

注意：この手順にはFPVRが必要です。FPVRの申請については、営業チームに問い合わせてください。

Eシリーズ コントローラのアップグレード

既存のコントローラを交換することでストレージ アレイをアップグレードすることができます。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、管理ソフトウェアの機能を実装します。

手順

1. [コントローラをアップグレードする準備](#) (8ページ)
コントローラをアップグレードする準備として、ドライブ セキュリティ キーを保存し、サポートデータを収集し、コントローラをオフラインにします。
2. [コントローラの取り外し](#) (12ページ)
コントローラを取り外すには、すべてのケーブルを外し、SFPトランシーバを取り外します。そのあと、コントローラ キャニスターをスライドしてコントローラ ドライブ トレイから外すことができます。
3. [新しいコントローラの取り付け](#) (14ページ)
古いコントローラを削除したあと、新しいコントローラをコントローラ ドライブ トレイに取り付けることができます。
4. [ドライブのロック解除](#) (16ページ)
E2800およびE5700のコントローラをアップグレードする場合、それらのコントローラのドライブ セキュリティ機能により、ドライブが部分的、外部、または内部でロックされた状態になります。ドライブ セキュリティ機能が有効になっている場合は、それらのドライブのロックを手動で解除する必要があります。
5. [コントローラのアップグレード後の処理](#) (25ページ)
コントローラのアップグレードが完了したら、コントローラ シェルフの電源をオンにし、コントローラのソフトウェアのバージョンを確認します。そのあと、サポートデータを収集し、運用を再開することができます。
6. [ベンダーがLSIからNETAPPに変わった場合のボリュームの再マウント](#) (29ページ)
コントローラのアップグレードでベンダーIDがLSIからNETAPPに変わった場合は、ボリュームを再マウントします。

コントローラをアップグレードする準備

コントローラをアップグレードする準備として、ドライブ セキュリティ キーを保存し、サポートデータを収集し、コントローラをオフラインにします。

手順

1. 既存のストレージ アレイのオペレーティング システム (コントローラ ファームウェア) が現在のコントローラに対応する最新のバージョンに更新されていることを確認します。

注: SANtricity OSバージョン8.50をサポートするコントローラにアップグレードする場合は、新しいコントローラを取り付けて電源をオンにしたあとに、最新バージョンのSANtricity OSと最新のNVS RAMをインストールする必要があります。このアップグレードを行わないと、ストレージ アレイを自動ロード バランシング (ALB) の対象として設定できないことがあります。
2. ドライブ セキュリティを使用している状況でコントローラを交換する場合は、次の手順を実行します。

セキュリティ タイプと状況 **手順**

- 内部キー管理、1本以上のドライブがロックされている
- a. 内部セキュリティ キー ファイルを管理クライアント (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) の既知の場所にエクスポートします。これには、`export storageArray securityKey`コマンドを使用します。セキュリティ キーに関連付けられているパス フレーズを入力し、コマンドの保存場所を指定する必要があります。このコマンドの使用方法については、『コマンドライン リファレンス』を参照してください。
 - b. 内部セキュリティ キーに関連付けられているパス フレーズを確認します。
-

- 外部キー管理、すべてのドライブがロックされている、コントローラの交換時に一時的に内部キー管理に切り替えることができる (推奨)
- 次の手順を順序どおりに実行します。
- a. **[設定] > [システム] > [セキュリティ キー管理] > [キー管理サーバ設定の表示 / 編集]**ダイアログを使用して、外部KMSのサーバアドレスとポート番号をメモします。
 - b. コントローラの交換後にストレージ 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がローカル ホストに保存されていることを確認します。証明書を保存するには、`save storageArray keyManagementCertificate`コマンドを使用します。`certificateType`パラメータを`client`に設定して1回実行し、パラメータを`server`に設定してもう1回実行してください。このコマンドの使用方法については、『コマンドライン リファレンス』を参照してください。
 - c. `disable storageArray externalKeyManagement`コマンドを実行して内部キー管理に切り替えます。
 - d. 内部セキュリティ キー ファイルを管理クライアント (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) の既知の場所にエクスポートします。これには、`export storageArray securityKey`コマンドを使用します。セキュリティ キーに関連付けられているパス フレーズを入力し、コマンドの保存場所を指定する必要があります。このコマンドの使用方法については、『コマンドライン リファレンス』を参照してください。
 - e. 内部セキュリティ キーに関連付けられているパス フレーズを確認します。
-

- 外部キー管理、すべてのドライブがロックされている、コントローラの交換時に一時的に内部キー管理に切り替えることはできない
- 次の手順を順序どおりに実行します。
- a. **[設定] > [システム] > [セキュリティ キー管理] > [キー管理サーバ設定の表示 / 編集]**ダイアログを使用して、外部KMSのサーバアドレスとポート番号をメモします。
 - b. コントローラの交換後にストレージ 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がローカル ホストに保存されていることを確認します。証明書を保存するには、`save storageArray keyManagementCertificate`コマンドを使用します。`certificateType`パラメータを`client`に設定して1回実行し、パラメータを`server`に設定してもう1回実行してください。このコマンドの使用方法については、『コマンドライン リファレンス』を参照してください。
-

セキュリティ タイプと状況	手順
---------------	----

外部キー管理、一部のドライブがロックされている	追加の手順は必要ありません。
-------------------------	----------------

3. ストレージ アレイのシリアル番号をメモします。
 - a. SANtricity Storage Managerを開きます。**[EMW]** ツリー ビューで、ストレージ アレイをダブルクリックしてSystem Managerを起動します。
 - b. System Managerで、**[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。
 - c. **[ストレージ アレイの詳細情報を表示]** まで下にスクロールして**[ストレージ アレイ プロファイル]**を選択します。
画面にレポートが表示されます。
 - d. ストレージ アレイ プロファイルからシャーシのシリアル番号を見つけるには、**[検索]** テキスト ボックスに「**シリアル番号**」と入力し、**[検索]**をクリックします。
一致するキーワードがすべて強調表示されます。すべての結果を1つずつスクロールするには、**[検索]**を繰り返しクリックします。
 - e. Chassis Serial Numberの値をメモします。
このシリアル番号は、[コントローラのアップグレード後の処理](#) (25ページ) の手順を実行する際に必要になります。
4. GUIまたはCLIのいずれかを使用して、ストレージ アレイに関するサポート データを収集します。
 - System ManagerまたはArray Management Windowで、ストレージ アレイのサポート バンドルを収集して保存します。
 - System Managerで、**[サポート]** > **[サポート センター]** > **[診断]** タブを選択します。次に、**[サポート データの収集]**を選択し、**[収集]**をクリックします。
 - Array Management Windowで、ツールバーから**[Monitor]** > **[Health]** > **[Collect Support Data Manually]**を選択します。次に、サポート バンドルの名前とシステム上の保存場所を指定します。
ブラウザのDownloadsフォルダに、support-data.7zという名前でファイルが保存されます。
シェルフにドロワーが搭載されている場合、そのシェルフの診断データはtray-componet-state-capture.7zという別の圧縮ファイルにアーカイブされます。
 - CLIで、`save storageArray supportData` コマンドを実行してストレージ アレイに関する包括的なサポート データを収集します。
注： サポート データの収集時は、ストレージ アレイのパフォーマンスに一時的に影響が及ぶことがあります。
5. ストレージ アレイと接続されているすべてのホストの間でI/O処理が発生しないようにします。
 - ストレージからホストにマッピングされたLUNに関連するすべてのプロセスを停止します。
 - ストレージからホストにマッピングされたLUNに対するアプリケーションによるデータの書き込みを停止します。

- アレイのボリュームに関連付けられているファイルシステムをすべてアンマウントします。

注: ホストI/O処理を停止する具体的な手順はホスト オペレーティング システムや構成によって異なり、ここでは説明していません。環境に応じたホストI/O処理の停止方法がわからない場合は、ホストをシャットダウンすることを検討してください。

注意：データ損失の可能性 – I/O処理の実行中にこの手順を続行すると、データが失われる場合があります。

- ストレージ アレイでミラーリング関係が確立されている場合は、セカンダリ ストレージ アレイのすべてのホストI/O処理を停止します。
- 非同期ミラーリングまたは同期ミラーリングを使用している場合は、System ManagerまたはArray Management Windowを使用して、ミラー ペアの削除とミラーリング関係の非アクティブ化を行います。
- シン ボリュームとしてホストに報告されるシンプロビジョニング ボリュームがあり、古いアレイでUNMAP機能をサポートするファームウェア（8.25以降のファームウェア）を実行している場合は、すべてのシン ボリュームでライトバック キャッシュを無効にします。
 - System Managerで、**[ストレージ]** > **[ボリューム]**を選択します。
 - いずれかのボリュームを選択し、**[さらに表示]** > **[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。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。
 - [基本]**タブを選択し、読み取りキャッシュと書き込みキャッシュの設定を変更します。
 - [保存]**をクリックします。
 - キャッシュ メモリ内のデータがディスクにフラッシュされるまで5分待ちます。
- Security Assertion Markup Language（SAML）がコントローラで有効になっている場合は、SAML認証を無効にします。
注： SAMLを有効にした場合、SANtricity System Managerで無効にすることはできません。SAMLの設定を無効にする場合は、テクニカル サポートにお問い合わせください。
- 実行中のすべての処理が完了するまで待つから、次の手順に進みます。
 - System Managerの**[ホーム]**ページで、**[実行中の処理を表示]**を選択します。
 - [実行中の処理]**ウィンドウに表示されたすべての処理が完了したことを確認してから、次の手順に進みます。
- コントローラ ドライブ トレイの電源をオフにします。
 コントローラ ドライブ トレイのすべてのLEDが消灯するまで待ちます。
- コントローラ ドライブ トレイに接続されている各ドライブ トレイの電源をオフにします。
 すべてのドライブがスピン ダウンするまで2分間待ちます。

次のタスク

[コントローラの取り外し](#)（12ページ）に進みます。

コントローラの取り外し

コントローラを取り外すには、すべてのケーブルを外し、SFPトランシーバを取り外します。そのあと、コントローラ キャニスターをスライドしてコントローラ ドライブ トレイから外すことができます。

タスク概要

デュプレックスのコントローラ ドライブ トレイのコントローラをアップグレードする場合は、同じ手順を繰り返して2台目のコントローラ キャニスターを取り外します。

手順

1. **手順1: コントローラを取り外す** (12ページ)
新しいコントローラ キャニスターにアップグレードできるように、コントローラ キャニスターを取り外します。すべてのケーブルを外し、SFPトランシーバを取り外す必要があります。その後、コントローラ キャニスターをスライドしてコントローラ シェルフから外すことができます。
2. **手順2: バッテリを取り外す** (13ページ)
バッテリーを取り外します。これは、古いコントローラ キャニスターのバッテリーを新しいコントローラ キャニスターで使用する場合にのみ行います。

手順1: コントローラを取り外す

新しいコントローラ キャニスターにアップグレードできるように、コントローラ キャニスターを取り外します。すべてのケーブルを外し、SFPトランシーバを取り外す必要があります。そのあと、コントローラ キャニスターをスライドしてコントローラ シェルフから外すことができます。

開始する前に

- コントローラ キャニスターに接続する各ケーブルを識別するためのラベルを用意しておく必要があります。

手順

1. ESDリストバンドを装着するか、静電気防止処置を施します。
2. 古いコントローラ キャニスターに接続された各ケーブルにラベルを付けます。HICの構成によっては、コントローラ キャニスターの交換後に一部のケーブルを再接続できる場合があります。
3. 古いコントローラ キャニスターからすべてのインターフェイス ケーブルとイーサネット ケーブルを外します。

光ファイバ ケーブルがある場合は、2つのリリース レバーを使ってコントローラ キャニスターを途中まで取り外した状態にできます。それらのリリース レバーを開いた状態にすれば、光ファイバ ケーブルのリリース タブを押し下げるのが簡単になります。

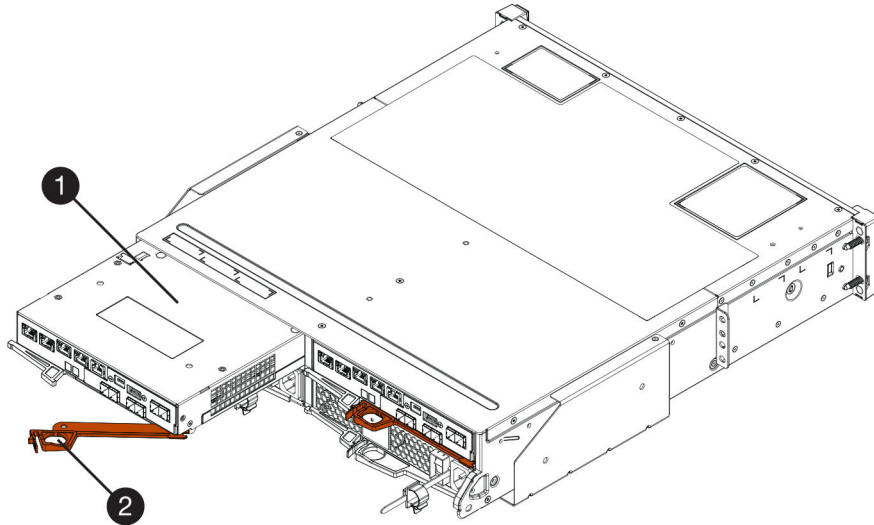
注意：パフォーマンスの低下を防ぐためにも、ケーブルをねじったり、折り曲げたり、はさんだり、踏みつけたりしないでください。

4. 古いコントローラ キャニスターにFibre Channel HICまたはInfiniBand HICが搭載されている場合は、Small Form-factor Pluggable (SFP+) トランシーバ (Fibre Channel) またはQuad SFP (QSFP+) トランシーバ (InfiniBand) をHICから取り外し、再利用する場合のために保管しておきます。

5. コントローラAを取り外します。

- a. リリースハンドルのロックを解除して外側に回転させ、コントローラ キャニスターを外します。
- b. リリースハンドルを両手でつかみ、コントローラ キャニスターをコントローラ ドライブトレイから引き出します。

次の図は、コントローラ モデルのリリースハンドルの一般的な場所の例を示したものです。リリースハンドルは、コントローラ シェルフとコントローラ ドライブトレイで似た構成になっています。



① コントローラ キャニスター ② カム ハンドル

6. コントローラ ドライブトレイの近くの静電気防止処置を施した平らな場所に、古いコントローラ キャニスターをリリースレバーを上にして置きます。コントローラ キャニスターの上部カバーを外せる状態にしておいてください。
7. (オプション) デュプレックスのコントローラ ドライブトレイのコントローラをアップグレードする場合は、同じ手順を繰り返して2台目のコントローラ キャニスターを取り外します。

次のタスク

古いコントローラから取り外したバッテリーを新しいコントローラで使用する場合は、[手順 2: バッテリーを取り外す](#) (13ページ) に進みます。それ以外の場合は、[新しいコントローラの取り付け](#) (14ページ) に進みます。

手順2: バッテリーを取り外す

バッテリーを取り外します。これは、古いコントローラ キャニスターのバッテリーを新しいコントローラ キャニスターで使用する場合にのみ行います。

手順

1. 古いコントローラ キャニスターの上部カバーの両方のラッチ ボタンを押し下げながら、上部カバーをキャニスターの背面方向にスライドします。

2. コントローラ ドライブトレイのモデルに応じて、次のいずれかの方法で古いバッテリーを外します。
 - E2600コントローラ ドライブトレイまたはE2700コントローラ ドライブトレイの場合は、バッテリーをコントローラ キャニスターに固定している取り付けネジを外します。
 - E5400コントローラ ドライブトレイ、EF540コントローラ ドライブトレイ、E5500コントローラ ドライブトレイ、EF550コントローラ ドライブトレイ、E5600コントローラ ドライブトレイ、またはEF560コントローラ ドライブトレイの場合は、バッテリーをコントローラ キャニスターに固定しているタブを外します。
3. バッテリーを古いコントローラ キャニスターの背面方向にスライドして取り外します。

次のタスク

[新しいコントローラの取り付け](#) (14ページ) に進みます。

新しいコントローラの取り付け

古いコントローラを削除したあと、新しいコントローラをコントローラ ドライブトレイに取り付けることができます。

タスク概要

デュプレックスのコントローラ ドライブトレイのコントローラをアップグレードする場合は、同じ手順を繰り返して2台目のコントローラ キャニスターを取り付けます。

手順

1. [手順1: バッテリーを取り付ける](#) (14ページ)
元のコントローラ キャニスターから取り外したバッテリー、または注文した新しいバッテリーを取り付けます。
2. [手順2: 新しいコントローラ キャニスターを取り付ける](#) (15ページ)
新しいコントローラ キャニスターをコントローラ シェルフに取り付けます。

手順1: バッテリーを取り付ける

元のコントローラ キャニスターから取り外したバッテリー、または注文した新しいバッテリーを取り付けます。

開始する前に

- 元のコントローラ キャニスターから取り外したバッテリー、または注文した新しいバッテリーを用意しておきます。
- 新しいコントローラ キャニスターを用意しておきます。

タスク概要

コントローラ ドライブトレイの各コントローラについて、次の手順を実行します。

手順

1. 新しいコントローラ キャニスターを開封し、取り外し可能なカバーを上にして、静電気防止処置を施した平らな場所に置きます。
2. カバーのボタンを押し下げながらスライドし、カバーを取り外します。

3. バッテリーのスロットが手前になるようにコントローラ キャニスターの向きを変えます。
4. コントローラのモデルに応じて、次のいずれかを実行します。
 - E2600またはE2700コントローラ モデル：
 - a. バッテリー回路基板を新しいコントローラ キャニスターの前面方向にスライドして挿入します。
 - b. 取り付けネジを締めて、バッテリー回路基板を新しいコントローラ キャニスターのカードに固定します。
 - c. カチッという音がして上部ラッチ カバーが固定されるまで上部カバーを前方にスライドして、新しいコントローラ キャニスターに上部カバーを再度取り付けます。カチッという音がしてラッチが固定されると、ラッチの下部がシャーシの金属製のスロットに収まります。
 - 他のコントローラ モデル：
 - a. バッテリーを新しいコントローラ キャニスターに挿入します。
バッテリーが新しいキャニスターの壁面のリベットの下の位置にくるまでスライドします。
 - b. 固定用ハンドルを45度傾けて、バッテリー下部のコネクタをキャニスターのコネクタに合わせます。
 - c. カチッという音がするまでバッテリーを下に押し、固定用ハンドルを上動かしてコントローラ バッテリーをコントローラ キャニスターに固定します。
注意：E5XXコントローラ ドライブトレイにコントローラ バッテリーが正しく装着されていることを確認するには、一度引き出してから再度挿入します。カチッという音がして収まり、固定用ハンドルを小刻みに動かしても直立した状態から動かなければ、正しい位置に固定されています。
 - d. カチッという音がして上部ラッチ カバーが固定されるまで上部カバーを前方にスライドして、新しいコントローラ キャニスターに上部カバーを再度取り付けます。カチッという音がしてラッチが固定されると、ラッチの下部がシャーシの金属製のスロットに収まります。
5. コントローラ キャニスターを裏返し、バッテリーが正しく取り付けられていることを確認します。

次のタスク

[手順2: 新しいコントローラ キャニスターを取り付ける](#) (15ページ) に進みます。

手順2: 新しいコントローラ キャニスターを取り付ける

新しいコントローラ キャニスターをコントローラ シェルフに取り付けます。

手順

1. 新しいコントローラ キャニスターをスライドしてコントローラ ドライブトレイに最後まで押し込みます。リリースレバーをコントローラ キャニスターの中心側に回転させて、所定の位置に固定します。
2. 新しいコントローラ キャニスターにFibre Channel HICまたはInfiniBand HICが搭載されている場合は、SFP+トランシーバ (Fibre Channel) またはQSFP+トランシーバ (InfiniBand) をコントローラ キャニスターに取り付けます。

アップグレードに関係するHICによっては、古いコントローラ キャニスターから取り外したSFP+トランシーバまたはQSFP+トランシーバを再利用できる場合があります。

3. コントローラ ドライブ トレイとドライブ トレイの間のすべてのケーブルを再接続します。

ドライブのケーブル接続構成が古いコントローラと同じ場合は、ケーブルに付けておいたラベルを使用して正しく再接続できます。

注：以前のモデルからE2700コントローラにアップグレードする場合は、ドライブのケーブル接続構成が古いコントローラで使用されている構成と異なる可能性があります。

次のタスク

[コントローラのアップグレード後の処理](#) (25ページ) に進みます。

ドライブのロック解除

E2800およびE5700のコントローラをアップグレードする場合、それらのコントローラのドライブ セキュリティ機能により、ドライブが部分的、外部、または内部でロックされた状態になります。ドライブ セキュリティ機能が有効になっている場合は、それらのドライブのロックを手動で解除する必要があります。

操作

- [内部セキュリティ キーの作成](#) (17ページ)
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。
- [内部キー管理を使用して1本以上のドライブがセキュリティ保護されている場合のコントローラの交換](#) (18ページ)
デュアルコントローラ システムの両方のコントローラまたはシンプレックス システムの1台のコントローラを交換する際、内部セキュリティ キーを使用してストレージ アレイの1本以上のドライブがロックされている場合は、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、ドライブへのアクセスのロックを解除できます。
- [外部セキュリティ キーの作成](#) (20ページ)
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。
- [外部キー管理を使用してすべてのドライブがセキュリティ保護されている場合のコントローラの交換](#) (22ページ)
デュアルコントローラ システムの両方のコントローラまたはシンプレックス システムの1台のコントローラを交換する際、外部セキュリティ キーを使用してストレージ アレイのすべてのドライブがロックされている場合は、ドライブへのアクセスのロックを解除するために外部キー管理サーバとの通信を再確立する必要があります。

内部セキュリティ キーの作成

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。

タスク概要

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。

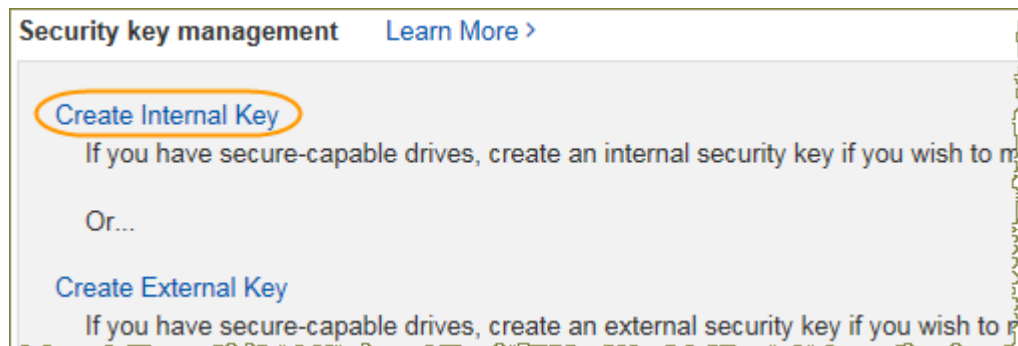
注：ドライブ セキュリティのパス フレーズは、ストレージ アレイの管理者パスワードとは別のものです。

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。

注：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。

手順

1. [設定]>[システム]を選択します。
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、[セキュリティ キーを作成]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** - デフォルトの値(コントローラ ファームウェアで生成されたストレージ アレイ名とタイムスタンプ) をそのまま使用することも、独自の値を入力することもできます。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。

注：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、確認のためにもう一度入力します。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）。

重要: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. [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。

注: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. キーの識別子とパス フレーズ、およびダウンロードされたキー ファイルの場所をメモし、[閉じる]をクリックします。

タスクの結果

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。

注: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。

次のタスク

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。

内部キー管理を使用して1本以上のドライブがセキュリティ保護されている場合のコントローラの交換

デュアルコントローラ システムの両方のコントローラまたはシンプレックス システムの1台のコントローラを交換する際、内部セキュリティ キーを使用してストレージ アレイの1本以上のドライブがロックされている場合は、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、ドライブへのアクセスのロックを解除できます。

開始する前に

注:内部キー管理でセキュリティ保護されたドライブが混在している状況でコントローラを交換したあとに、デジタル表示ディスプレイにロックダウン コード_{L5}が表示される場合は、テクニカル サポートにお問い合わせください。

- ストレージ アレイでロックされているドライブについて、セキュリティ キー識別子とパスフレーズを確認しておく必要があります。

注：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。

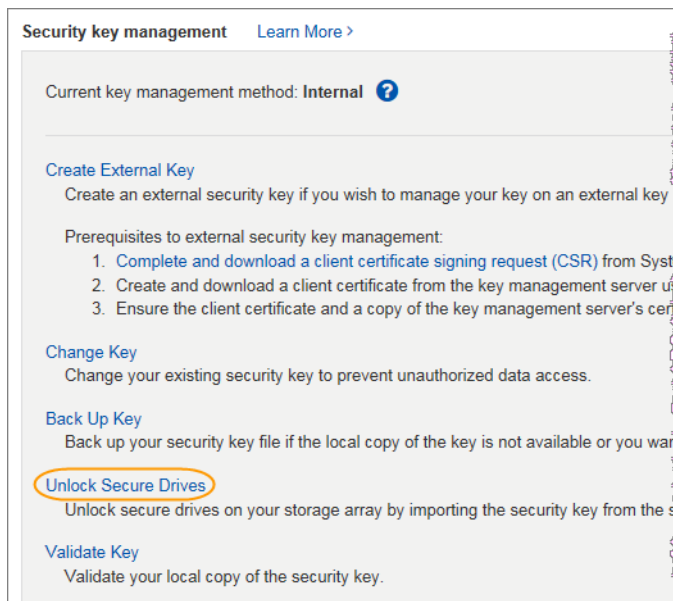
- セキュリティ キー ファイルは管理クライアント（System Managerへのアクセスに使用するブラウザを備えたシステム）にあります。
- コントローラの交換前にアレイで使用していた元のセキュリティ キーをインポートする前に、新しい交換用コントローラで新しい内部セキュリティ キーを作成しておく必要があります。

タスク概要

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、ドロップダウン リストでセキュリティ キー識別子を選択してから、キーのパス フレーズを入力します。

手順

1. [ストレージ アレイ]メニューから[セキュリティ]>[ドライブ セキュリティ]>[キー管理 証明書のインポート]を選択して、[コントローラをアップグレードする準備](#)（8ページ）で保存したセキュリティ キーをインポートします。
 - ストレージ アレイにセキュリティ保護されたドライブのみが含まれていた場合（セキュリティ保護されていないドライブが含まれていない場合）は、コントローラが自動的にリブートしてインポート処理が実行されます。すべてのコントローラがブートするまで待ちます。コントローラのブートが完了すると、対応するアイコンが Enterprise Management Window（EMW）に表示されます。
2. [設定]>[システム]を選択します。
3. [セキュリティ キー管理]の下にある[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。

4. 最初のフィールドのドロップダウン リスト（右端の矢印をクリック）で、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 キー識別子を選択します。

識別子を選択すると、関連付けられているドライブの情報がフィールドの下に表示され、**[参照]**ボタンが使用可能な状態になります。ドライブは、シェルフ番号、ドロワー番号、およびベイ番号で識別されます。

5. **[参照]**をクリックし、識別子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 ファイルがフィールドの下に表示されます。

6. 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。

7. **[ロック解除]**をクリックします。

ロック解除処理が成功すると、ダイアログ ボックスに次のメッセージが表示されます。

関連付けられているセキュア ドライブのロックが解除されました。

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。

8. 開始時点でストレージ アレイにセキュリティ保護されたドライブとセキュリティ保護されていないドライブが混在していた場合は、セキュリティ保護されていたドライブをネイティブ状態に設定します。

- a. SMcliで`set drives=(trayID1,[drawerID1,]slotID1 ... trayIDn,[drawerIDn,]slotIDn) nativeState`コマンドを実行します。

指定するドライブは、コントローラの交換の開始時点でセキュリティ保護されていたドライブです。

- b. SANtricity System Managerを使用してすべてのコントローラをリセットします。

- c. すべてのコントローラがブートするまで待ちます。コントローラのブートが完了すると、EMWに表示されます。

外部セキュリティ キーの作成

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。

注：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 ベンダーにお問い合わせください。
- 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、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証明します。

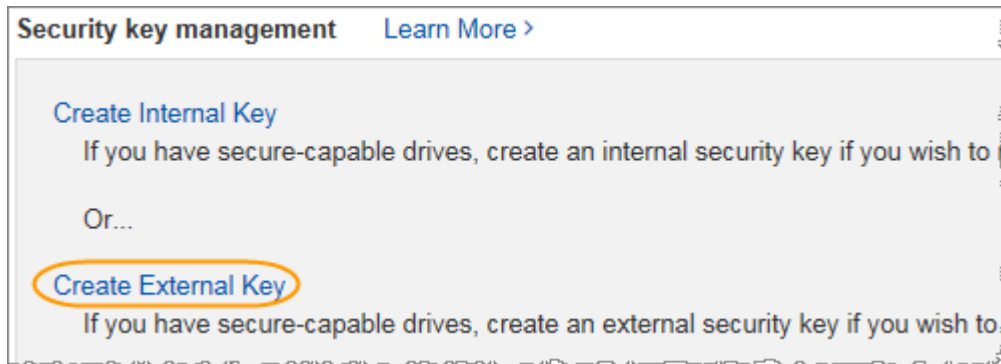
タスク概要

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. [設定]>[システム]を選択します。
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。

注：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. [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）の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を選択** - 1つ目の[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の証明書ファイルを選択します。
 - **キー管理サーバのサーバ証明書を選択** - 2つ目の[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. [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、確認のためにもう一度入力します。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）。

重要: 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パス フレーズが必要になります。

6. **[終了]**をクリックします。

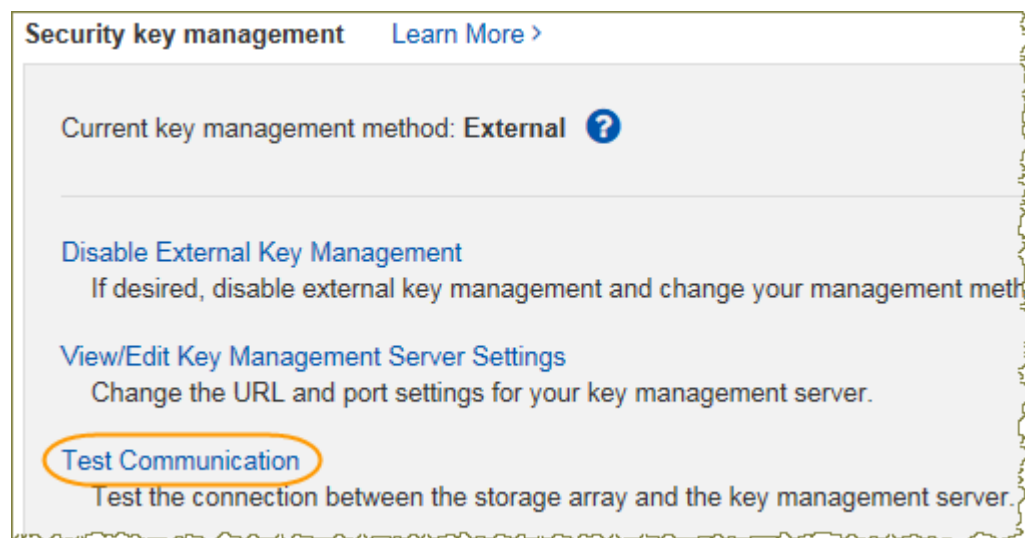
入力したクレデンシャルを使用して、システムがキー管理サーバに接続されます。その後、セキュリティ キーのコピーがローカル システムに格納されます。

注：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 ファイルの場所をメモし、**[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に関連したリンクが表示されます。

現在のキー管理方法：外部

8. **[通信のテスト]**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。

タスクの結果

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。

注：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。

次のタスク

- 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。

外部キー管理を使用してすべてのドライブがセキュリティ保護されている場合のコントローラの交換

デュアルコントローラ システムの両方のコントローラまたはシンプレックス システムの1台のコントローラを交換する際、外部セキュリティ キーを使用してストレージ アレイのす

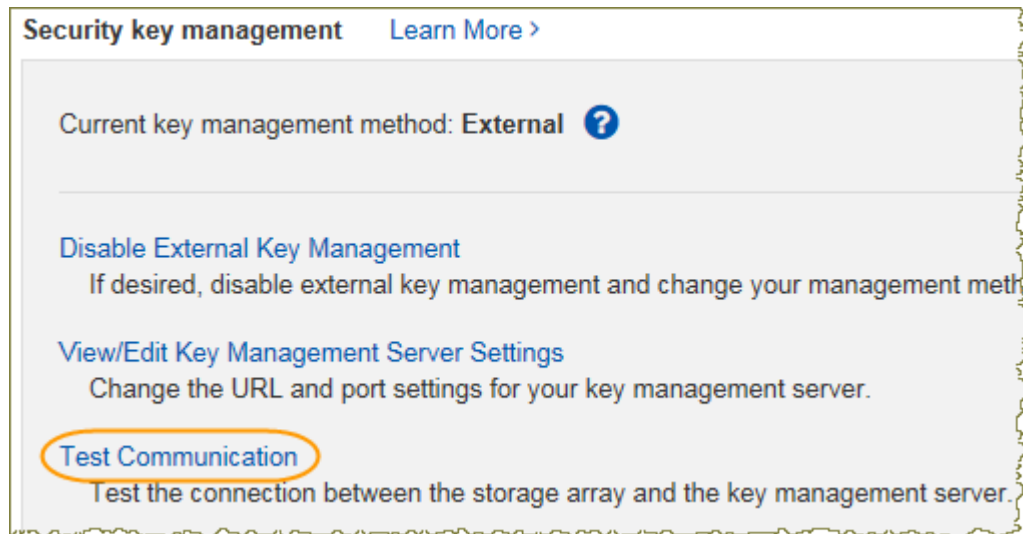
すべてのドライブがロックされている場合は、ドライブへのアクセスのロックを解除するために外部キー管理サーバとの通信を再確立する必要があります。

開始する前に

- 外部KMSとコントローラの両方が同じサブネットにあることを確認します。
- [コントローラをアップグレードする準備](#) (8ページ) の手順に従って、外部KMSのサーバアドレスとポート番号をメモしておきます。
- [コントローラをアップグレードする準備](#) (8ページ) の手順に従って、クライアント証明書とサーバ証明書を取得してローカルホストに保存しておきます。これらの証明書は、ストレージアレイとキー管理サーバの相互認証に必要です。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証明します。
- 外部セキュリティキーに関連付けられているパスフレーズを確認しておきます。

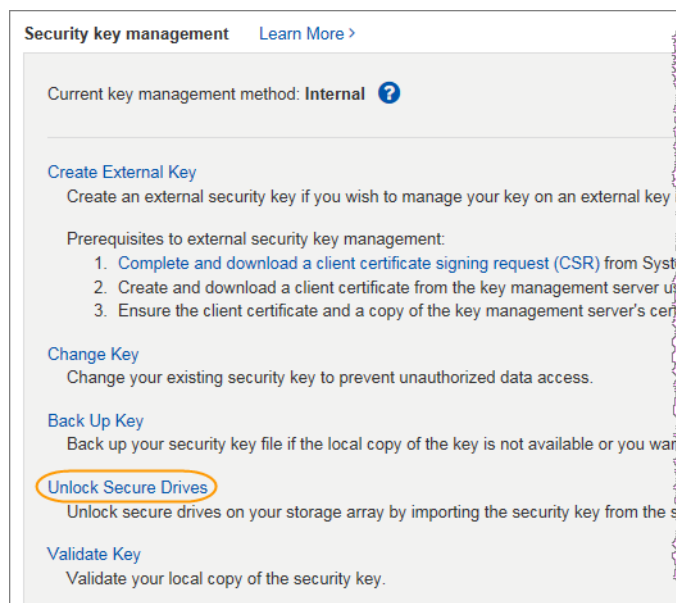
手順

1. **[設定] > [システム]**を選択します。
2. **[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) の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を選択** - 1つ目の**[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の証明書ファイルを選択します。
 - **キー管理サーバのサーバ証明書を選択** - 2つ目の**[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。
3. **[次へ]**をクリックします。
4. **[終了]**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。
注: 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. ダウンロードしたキーファイルの場所をメモし、**[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に関連したリンクが表示されます。
 現在のキー管理方法: 外部
6. **[通信のテスト]**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。

7. [設定] > [システム]を選択します。
8. [セキュリティ キー管理]の下にある[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。

9. 最初のフィールドのドロップダウン リスト（右端の矢印をクリック）で、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 キー識別子を選択します。

識別子を選択すると、関連付けられているドライブの情報がフィールドの下に表示され、[参照]ボタンが使用可能な状態になります。ドライブは、シェルフ番号、ドロワー番号、およびベイ番号で識別されます。

10. [参照]をクリックし、識別子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 ファイルがフィールドの下に表示されます。
11. 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。

12. [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、「関連付けられているセキュアドライブのロックが解除されました」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。

タスクの結果

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。

コントローラのアップグレード後の処理

コントローラのアップグレードが完了したら、コントローラ シェルフの電源をオンにし、コントローラのソフトウェアのバージョンを確認します。そのあと、サポート データを収集し、運用を再開することができます。

タスク概要

デュプレックスのコントローラ ドライブ トレイのコントローラをアップグレードする場合は、同じ手順を繰り返して2台目のコントローラのアップグレードを実行します。

手順

1. [手順1: コントローラの電源をオンにする](#) (25ページ)
コントローラ シェルフの電源をオンにし、正しく動作していることを確認する必要があります。
2. [手順2: コントローラとトレイのステータスを確認する](#) (27ページ)
LEDとストレージ管理ソフトウェアを使用して、コントローラとトレイのステータスを確認できます。
3. [手順3: コントローラのソフトウェアのバージョンを確認する](#) (27ページ)
新しいコントローラが正しいオペレーティング システム(コントローラ ファームウェア)とNVSRAMで動作していることを確認する必要があります。

手順1: コントローラの電源をオンにする

コントローラ シェルフの電源をオンにし、正しく動作していることを確認する必要があります。

手順

1. コントローラ ドライブ トレイに接続された各ドライブ トレイの背面にある電源スイッチをオンにします。
2. ドライブがスピン アップするまで2分待ちます。
3. コントローラ ドライブ トレイの背面にある電源スイッチをオンにします。
4. 電源投入プロセスが完了するまで3分待ちます。
5. E2800コントローラまたはE5700コントローラを交換する場合は、ドライブ セキュリティの状況に応じて次のいずれかの手順に進みます。

コントローラの交換の種類	手順および前提条件
いずれのドライブもセキュリティ保護されていない、外部キー管理でも内部キー管理でもない	終了後 (26ページ) に進みます。

コントローラの交換の種類	手順および前提条件
セキュリティ保護されたドライブとセキュリティ保護されていないドライブが混在している、内部キー管理	<p>内部セキュリティ キーを作成してから、そのセキュリティ キーを手動でインポートしてセキュリティ保護されたドライブのロックを解除する必要があります。ドライブのロックが解除されると、ドライブにアクセスできるようになります。</p> <p>a. 内部セキュリティ キーの作成 (17ページ)</p> <p>b. 内部キー管理を使用して1本以上のドライブがセキュリティ保護されている場合のコントローラの交換 (18ページ)</p>
すべてのドライブがセキュリティ保護されている、内部キー管理	内部キー管理を使用して1本以上のドライブがセキュリティ保護されている場合のコントローラの交換 (18ページ)
セキュリティ保護されたドライブとセキュリティ保護されていないドライブが混在している、外部キー管理	<p>終了後 (26ページ) に進みます。</p> <p>注意： コントローラの交換の完了後、コントローラが自動的に外部キー管理サーバと再同期され、ドライブのロックが解除されてアクセス可能になります。</p> <p>注： 内部キー管理でセキュリティ保護されたドライブが混在している状況でコントローラを交換したあとに、デジタル表示ディスプレイにロックダウン コードL5が表示される場合は、テクニカルサポートにお問い合わせください。</p>
すべてのドライブがセキュリティ保護されている、外部キー管理、コントローラの交換時に一時的に内部キー管理に切り替えている	<p>最初に、内部キー管理の手順を使用して、セキュリティ保護されたドライブのロックを解除する必要があります。ドライブのロックを解除したあと、ストレージ アレイに対する新しい外部セキュリティ キーを作成して外部キー管理に戻します。</p> <p>a. 内部キー管理を使用して1本以上のドライブがセキュリティ保護されている場合のコントローラの交換 (18ページ)</p> <p>b. 外部セキュリティ キーの作成 (20ページ)</p>
すべてのドライブがセキュリティ保護されている、外部キー管理、コントローラの交換時に一時的に内部キー管理に切り替えていない	外部キー管理を使用してすべてのドライブがセキュリティ保護されている場合のコントローラの交換 (22ページ)

次のタスク

[手順2: コントローラのステータスを確認する](#) (27ページ) に進みます。

手順2: コントローラとトレイのステータスを確認する

LEDとストレージ管理ソフトウェアを使用して、コントローラとトレイのステータスを確認できます。

手順

1. コントローラAのLEDを参照して、正しくブートしていることを確認します。
リブート中はホスト リンク保守操作必要LEDが緑色に点灯します。
コントローラのリブートが完了すると、デジタル表示ディスプレイに2台目のコントローラのデジタル表示ディスプレイと同じトレイIDが表示されます。
2. コントローラ ドライブ トレイのいずれかの保守操作必要LEDが点灯している場合やコントローラ保守操作必要LEDが点灯している場合は、次の手順を実行します。
 - a. コントローラ キャニスターが正しく取り付けられていること、およびすべてのケーブルが正しく装着されていることを確認します。
 - b. コントローラ ドライブ トレイの保守操作必要LEDとコントローラ保守操作必要LEDをもう一度確認します。
3. デュプレックス構成の場合は、コントローラBについて手順1と手順2を繰り返します。
4. LEDとストレージ管理ソフトウェアを使用して、ストレージ アレイのすべてのトレイのステータスを確認します。

次のタスク

[手順3: コントローラのソフトウェアのバージョンを確認する](#) (27ページ) に進みます。

手順3: コントローラのソフトウェアのバージョンを確認する

新しいコントローラが正しいオペレーティング システム (コントローラ ファームウェア) とNVSRAMで動作していることを確認する必要があります。

手順

1. 次のいずれかを実行します。
 - SANtricity 11.30およびコントローラ ファームウェア8.30をサポートしないコントローラへのアップグレードの場合は、新しいコントローラで実行されているバージョンが元のコントローラで最後に実行していたバージョンと一致していることを確認します。これは、通常は古いコントローラでサポートされている最新のリリースになります。必要に応じて、新しいコントローラに適切なバージョンをインストールします。
 - SANtricity 11.30およびコントローラ ファームウェア8.30を実行するコントローラへのアップグレードの場合は、新しいコントローラの電源をオンにしたあとに最新のNVSRAMをダウンロードしてインストールします。
2. コントローラのアップグレードでプロトコルが変更になる場合 (Fibre ChannelからiSCSIなど)、ストレージ アレイに対して定義されたホストがすでにあるときは、新しいホストポートをホストに関連付けます。
 - a. System Managerで、**[ストレージ] > [ホスト]**を選択します。
 - b. ポートに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。
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。

- c. **[ホスト ポート]**タブをクリックします。

ダイアログ ボックスに現在のホスト ポート識別子が表示されます。

- d. 各ホストに関連付けられているホスト ポート識別子の情報を更新するには、古いホストアダプタのホスト ポートIDを新しいホストアダプタの新しいホスト ポートIDに置き換えます。
- e. 各ホストについて手順dを繰り返します。
- f. **[保存]**をクリックします。

互換性があるハードウェアについては、[NetApp Interoperability Matrix](#)および[NetApp Hardware Universe](#)を参照してください。

3. ヘッド交換の準備でライトバック キャッシュを無効にしていた場合は、すべてのボリュームで有効にします。
4. ヘッド交換の準備でSAMLを無効にしていた場合は、交換用コントローラで有効にします。
 - a. System Managerで、**[SAML]** タブを選択し、**[SAML の有効化]** リンクを選択します。
[SAML の有効化の確認]ダイアログが開きます。
 - b. 「enable」と入力し、**[有効化]** をクリックします。
 - c. 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。
5. GUIまたはCLIのいずれかを使用して、ストレージ アレイに関するサポート データを収集します。
 - System ManagerまたはArray Management Windowで、ストレージ アレイのサポートバンドルを収集して保存します。
 - System Managerで、**[サポート]** > **[サポート センター]** > **[診断]**タブを選択します。次に、**[サポート データの収集]**を選択し、**[収集]**をクリックします。
 - Array Management Windowで、ツールバーから**[Monitor]** > **[Health]** > **[Collect Support Data Manually]**を選択します。次に、サポートバンドルの名前とシステム上の保存場所を指定します。

ブラウザのDownloadsフォルダに、support-data.7zという名前でファイルが保存されます。

シェルフにドロワーが搭載されている場合、そのシェルフの診断データはtray-componet-state-capture.7zという別の圧縮ファイルにアーカイブされます。

- CLIで、`save storageArray supportData` コマンドを実行してストレージ アレイに関する包括的なサポート データを収集します。

注： サポートデータの収集時は、ストレージ アレイのパフォーマンスに一時的に影響が及ぶことがあります。

6. ストレージ アレイの構成の変更をネットアップ テクニカル サポートに連絡します。
 - a. [コントローラをアップグレードする準備](#) (8ページ) でメモしておいたコントローラ ドライブ トレイのシリアル番号を用意します。
 - b. ネットアップ サポート サイト (mysupport.netapp.com/eservice/assistant) にログインします。
 - c. **[Category 1]**のドロップダウン リストで**[Product Registration]**を選択します。

- d. **[Comments]**テキスト ボックスに次のテキストを入力します。*serial number*をコントローラ ドライブ トレイのシリアル番号に置き換えてください。

Please create alert against Serial Number: *serial number*. The alert name should be "E-Series Upgrade". The alert text should read as follows:

"Attention: The controllers in this system have been upgraded from the original configuration. Verify the controller configuration before ordering replacement controllers and notify dispatch that the system has been upgraded."

- e. フォームの下部にある**[Submit]**ボタンをクリックします。

次のタスク

コントローラのアップグレードでベンダーIDがLSIからNETAPPに変わった場合は、[ベンダーがLSIからNETAPPに変わった場合のボリュームの再マウント](#) (29ページ) に進みます。それ以外の場合は、これでコントローラのアップグレードは完了になり、通常の運用を再開できます。

ベンダーがLSIからNETAPPに変わった場合のボリュームの再マウント

コントローラのアップグレードでベンダーIDがLSIからNETAPPに変わった場合は、ボリュームを再マウントします。

操作

- [AIXホストでのボリュームの再マウント](#) (29ページ)
コントローラの交換後、ストレージ アレイの新しいボリュームに加えて、元のボリュームも使用停止のボリュームとして表示されることがあります。
- [VMwareホストでのボリュームの再マウント](#) (29ページ)
コントローラのアップグレード後にVMwareホストで発生する可能性がある問題に対処します。
- [Windowsホストでのボリュームの再マウント](#) (30ページ)
Windowsホストでボリュームを再マウントして、接続されたホストがアップグレード後のストレージ アレイにあるボリュームでI/O処理を実行できるように構成します。

AIXホストでのボリュームの再マウント

コントローラの交換後、ストレージ アレイの新しいボリュームに加えて、元のボリュームも使用停止のボリュームとして表示されることがあります。

手順

1. 使用停止のボリュームが表示される場合は、`cfgmgr`コマンドを実行します。

VMwareホストでのボリュームの再マウント

コントローラのアップグレード後にVMwareホストで発生する可能性がある問題に対処します。

タスク概要

コントローラを交換したあと、次のような状況になることがあります。

- ストレージ アレイのボリュームの新しいパスに加えて、元のパスも稼働していないパスとして表示される。
- ストレージ アレイのボリュームのリストで、ベンダーIDがLSIのままになる。これは、ボリュームが最初にLSIのルールで要求されたために、ボリュームがオンラインに戻ったあとも同じLSIのルールが使用される場合に発生することがあります。
- LSIからNETAPPへの変更が表示名に反映されない。これは、初回検出後に表示名が「free test」になったことが原因で発生することがあります。この場合は、手動で表示名を変更できます。

手順

1. 各ホストで再スキャンを実行します。
2. このサブシステムに対するすべてのホストI/O処理を停止します。
3. ネットアップのルールでボリュームを再利用します。
 - a. `esxcli storage core device list` コマンドを実行します。コマンドの出力を確認し、名前が `aa.xxxx` の形式のボリュームを特定します。
 - b. `do esxcli storage core claiming reclaim -d naa.xxxxxx` コマンドを実行して、ベンダーIDをLSIからNETAPPに変更します。

Windowsホストでのボリュームの再マウント

Windowsホストでボリュームを再マウントして、接続されたホストがアップグレード後のストレージ アレイにあるボリュームでI/O処理を実行できるように構成します。

手順

1. [デバイス マネージャー]で、[非表示デバイスの表示]を選択します。
2. [デバイス マネージャー]に表示されたNETAPP SCSIディスク デバイスのそれぞれについて、エントリを右クリックして[アンインストール]を選択します。

Windowsのダイアログ ボックスでホストのリブートが必要であることを示すメッセージが表示される場合は、ハードウェアのスキャンとリブートに進む前に、すべてのボリュームのアンインストールを完了します。
3. [デバイス マネージャー]で右クリックし、[ハードウェア変更のスキャン]を選択します。
4. ホストをリブートします。

データ保持が不要な場合の新しいSAS-3コントローラシェルフの背後でのSAS-2システムの再構成

データを保持する必要がなければ、承認済みSAS-2アレイ（E2700、E5500 / EF5500、E5600 / EF560）のコントローラシェルフをドライブシェルフに変換し、そのシェルフとそれに関連する承認済みSAS-2ドライブシェルフ（DE1600、DE5600、DE6600）を新しい承認済みSAS-3アレイ（E2800、E5700 / EF570）および承認済みSAS-3ドライブシェルフ（DE212C、DE224C、DE460C）の背後に配置できます。

タスク概要

この手順は複雑であるため、実行にあたっては次のことに注意してください。

- この手順にはFPVRが必要です。FPVRの申請については、ネットアッププロフェッショナルサービスにお問い合わせください。

注：FPVRを取得せずにこの手順を実行すると、ドライブ障害が発生し、コントローラがロックダウンする可能性があります。
- データをバックアップできる場合は、ネットアッププロフェッショナルサービスの支援なしで実行できます。
- データをバックアップできない場合は、ネットアッププロフェッショナルサービスに支援を要請してください。
- 両方のアレイについて、手順の準備が完了していることを確認します。
 - **既存のアレイ：**SANtricity OS 8.25以降を搭載した既存のアレイの電源をオンにしておきます。
 - **新しいアレイ：**新しいアレイを開封し、電源はオフにしておきます。
- ドライブシェルフに変換するSAS-2コントローラシェルフのシリアル番号をメモします。

手順

1. **手順1: コントローラの電源をオフにする（データ保持なし）**（31ページ）
コントローラの電源をオフにする前に、すべての処理をシャットダウンする必要があります。
2. **手順2: コントローラを取り付ける（データ保持なし）**（32ページ）
シャットダウンが完了したら、アレイのコントローラを交換できます。
3. **手順3: コントローラの電源をオンにする（データ保持なし）**（32ページ）
取り付けが完了したら、コントローラの電源をオンにし、構成の変更をネットアップテクニカルサポートに送信します。

手順1: コントローラの電源をオフにする（データ保持なし）

コントローラの電源をオフにする前に、すべての処理をシャットダウンする必要があります。

手順

1. 既存のSAS-2アレイにまだアクセス可能な場合は、すべてのボリュームグループを削除し、両方のコントローラの電源をオフにして、すべてのケーブルを外します。

2. ドライブ シェルフに変換するSAS-2コントローラ シェルフのシリアル番号をメモします。
3. 既存のアレイでドライブ セキュリティを使用している場合は、セキュリティ キーを利用できることを確認します。

次のタスク

手順2: コントローラの電源をオフにする（データ保持なし）（32ページ）に進みます。

手順2: コントローラを取り付ける（データ保持なし）

シャットダウンが完了したら、アレイのコントローラを交換できます。

手順

1. IOMまたはESMを搭載した既存のアレイの両方のコントローラを交換します。
2. 可能な場合は、既存のアレイから取り外したホスト ケーブルとネットワーク ケーブルを新しいアレイのコントローラに接続します。

注: 新しいアレイのホスト接続によっては、別のケーブルが必要になることがあります。

3. 新しいアレイのコントローラ背後でドライブ シェルフをケーブル接続します。

既存のコントローラ ドライブ トレイとそれに接続されたドライブ トレイをドライブ シェルフとして新しいアレイのコントローラにケーブル接続できるようになります。

注: SAS-2からSAS-3への接続には、SAS HDからminiSASへのケーブルが必要です。特定のコントローラおよび拡張シェルフ構成の詳細なケーブル接続情報については、『[E-Series Hardware Cabling Guide](#)』を参照してください。

次のタスク

手順3: コントローラの電源をオンにする（データ保持なし）（32ページ）に進みます。

手順3: コントローラの電源をオンにする（データ保持なし）

取り付けが完了したら、コントローラの電源をオンにし、構成の変更をネットアップ テクニカル サポートに送信します。

手順

1. 新しいアレイとそれに接続されたドライブ シェルフの電源をオンにします。
2. [SANtricity Quick Connect](#)ユーティリティをインストールして、管理ポートとIPアドレスを設定します。
3. 既存のアレイでドライブ セキュリティを使用していた場合は、セキュリティ キーをインポートします。
4. この手順を実行する前に既存のアレイからボリューム グループを削除できなかった場合は、すべての外部ドライブをネイティブとして扱うように設定する必要があります。ドライブをネイティブに設定する方法の詳細については、SANtricityのオンライン ヘルプを参照してください。
5. 構成の変更をネットアップ テクニカル サポートに送信します。

- a. 手順2でメモしておいた古いコントローラ ドライブ トレイのシリアル番号を用意します。
- b. ネットアップ サポート サイト (mysupport.netapp.com/eservice/assistant) にログインします。
- c. **[Give Us Feedback]**ページの**[Category 1]**のドロップダウン リストで、**[Installed products]**を選択します。
- d. **[Give Us Feedback]**ページの**[Category 2]**のドロップダウン リストで、**[Decommission request]**を選択します。
- e. **[Comments]**テキスト ボックスに次のテキストを入力します。*serial number*をコントローラ ドライブ トレイのシリアル番号に置き換えてください。

Please decommission this serial number as the entitlement has been moved to another serial number in the system. Please reference this in the SN notes.

- f. **[Submit]**を選択します。

タスクの結果

SAS-2からSAS-3への構成の変更がネットアップ テクニカル サポートに送信されます。

著作権に関する情報

Copyright © 2019 NetApp, Inc. All rights reserved. Printed in the U.S.A.

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。

ここに記載されている「データ」は商用品目（FAR 2.101で定義）に該当し、その所有権はネットアップに帰属します。米国政府は、データが提供される際の米国政府との契約に関連し、かつ当該契約が適用される範囲においてのみ「データ」を使用するための、非独占的、譲渡不可、サブライセンス不可、世界共通の限定的な取り消し不可のライセンスを保有します。ここに記載されている場合を除き、書面によるネットアップの事前の許可なく、「データ」を使用、開示、複製、変更、実行、または表示することは禁止されています。米国国防総省のライセンス権限は、DFARS 252.227-7015 (b) 項に規定されている権限に制限されます。

商標に関する情報

NetApp、NetAppのロゴ、ネットアップの商標一覧のページに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。

<http://www.netapp.com/jp/legal/netapptmlist.aspx>

マニュアルの更新について

弊社では、マニュアルの品質を向上していくため、皆様からのフィードバックをお寄せいただく専用のEメール アドレスを用意しています。また、GA/FCS版の製品マニュアルの初回リリース時や既存マニュアルへの重要な変更があった場合にご案内させていただくTwitter アカウントもあります。

本マニュアルの改善についてご提案がある場合は、次のアドレスまでコメントをEメールでお送りください。

ng-gpso-jp-documents@netapp.com

その際、担当部署で適切に対応させていただくため、製品名、バージョン、オペレーティング システム、弊社営業担当者または代理店の情報を必ず入れてください。

GA/FCS版の製品マニュアルの初回リリース時や既存マニュアルへの重要な変更があった場合のご案内を希望される場合は、Twitterアカウント@NetAppDocをフォローしてください。