ドライブセキュリティ

SANtricity software

NetApp
August 22, 2025

目次

ドライブセキュリティ

ドライブセキュリティの概要

[セキュリティキー管理]ページで、ドライブセキュリティとキー管理を設定できます。

ドライブセキュリティとは

_Drive Security_は、セキュリティ有効ドライブをストレージアレイから取り外したときに、そのドライブ上のデータへの不正アクセスを防止する機能です。対応するドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。FDEドライブまたはFIPSドライブをアレイから物理的に取り外した場合は、別のアレイに取り付けるまで動作できません。別のアレイに取り付けると、正しいセキュリティキーを指定するまでドライブはセキュリティロック状態になります。a_security key_は、ストレージアレイ内のこれらのタイプのドライブおよびコントローラで共有される文字列です。

詳細：

- "ドライブセキュリティ機能の仕組み"
- "セキュリティキー管理の仕組み"
- "ドライブセキュリティの用語"

キー管理の設定方法

ドライブセキュリティを実装するには、アレイにFDEドライブまたはFIPSドライブを取り付ける必要があります。これらのドライブのキー管理を設定するには、メニューから次のいずれかを選択します。Settings [System > Security key management]コントローラの永続的メモリから内部キーを作成するか、キー管理サーバから外部キーを作成できます。最後に、ボリューム設定で[セキュリティ対応]を選択して、プールおよびボリュームグループのドライブセキュリティを有効にします。

詳細：

- "内部セキュリティキーの作成"
- "外部セキュリティキーの作成"
- "プールの手動作成"
- "ボリュームグループの作成"

ドライブのロックを解除する方法を教えてください。

キー管理を設定したあとにセキュリティ有効ドライブをストレージアレイ間で移動した場合、ドライブ上の暗号化データにアクセスできるようにするには、セキュリティキーを新しいストレージアレイに再割り当てする必要があります。

詳細：

- "内部キー管理の使用時のドライブのロック解除"
- "外部キー管理の使用時のドライブのロック解除"

関連情報

キー管理に関連するタスクの詳細については、以下を参照してください。

- "キー管理サーバでの認証にCA署名証明書を使用する"
- "セキュリティキーのバックアップ"

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。

これらのドライブをドライブセキュリティ機能と組み合わせて使用すると、データにアクセスするためのセキュリティキーが必要になります。ドライブをアレイから物理的に取り外した場合、別のアレイに取り付けるまでドライブは動作しません。別のアレイに取り付けると、正しいセキュリティキーを指定するまでセキュリティロック状態になります。

ドライブセキュリティの実装方法

ドライブセキュリティを実装するには、次の手順を実行します。

1. ストレージアレイにセキュリティ対応のFDEドライブまたはFIPSドライブを取り付けます（FIPSのサポートが必要なドライブには、FIPSドライブのみを使用します。ボリュームグループまたはプールにFIPSドライブとFDEドライブが混在している場合、すべてのドライブがFDEドライブとして扱われます。また、FIPSのみのボリュームグループまたはプールでFDEドライブを追加したりスペアとして使用したりすることはできません）。
2. セキュリティキーを作成します。セキュリティキーは、読み取り/書き込みアクセス用にコントローラとドライブで共有される文字列です。コントローラの永続的メモリから内部キーを作成するか、キー管理サーバから外部キーを作成できます。外部キー管理の場合は、キー管理サーバとの間で認証を確立する必要があります。
3. プールおよびボリュームグループに対してドライブセキュリティを有効にします。
   - プールまたはボリュームグループを作成します（受験者テーブルの「Secure Capable 」列で「 Yes」を検索してください）。
   - 新しいボリュームを作成するときにプールまたはボリュームグループを選択します（Pool and volume group Candidatesテーブルで、「* SecureCapable 」の横の「 Yes」*を探します）。

ドライブレベルでのドライブセキュリティの動作

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

ドライブセキュリティ機能は、セキュリティ対応ドライブを使用して保護を強化します。これらのドライブのボリュームグループまたはプールをドライブセキュリティの対象として選択すると、ドライブはセキュリティキーを探してからデータへのアクセスを許可します。プールおよびボリュームグループのドライブセキュリテ

ィはいつでも有効にでき、ドライブ上の既存データには影響しません。ただし、ドライブセキュリティを無効にするには、ドライブ上のすべてのデータを消去する必要があります。

ストレージアレイレベルでのドライブセキュリティの動作

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

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

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

ボリュームレベルでのドライブセキュリティの動作

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

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

- ボリュームグループとプールはセキュリティ対応ドライブだけで構成されている必要があります。（FIPSのサポートが必要なドライブには、FIPSドライブのみを使用します。ボリュームグループまたはプールにFIPSドライブとFDEドライブが混在している場合、すべてのドライブがFDEドライブとして扱われます。また、FIPSのみのボリュームグループまたはプールでFDEドライブを追加したりスペアとして使用したりすることはできません）。
- ボリュームグループとプールの状態が最適I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用のセキュリティキーが必要です。セキュリティキーは、ストレージアレイ内のこれらのタイプのドライブとコントローラで共有される文字列です。

ドライブの電源をオフにしてオンにするたびに、コントローラがセキュリティキーを適用するまでセキュリティ有効ドライブはセキュリティロック状態になります。セキュリティ有効ドライブをストレージアレイから取り外すと、ドライブのデータはロックされます。ドライブを別のストレージアレイに取り付け直すと、データへのアクセスを再開する前にセキュリティキーが検索されます。データのロックを解除するには、元のセキュリティキーを適用する必要があります。

セキュリティキーは、次のいずれかの方法で作成および管理できます。

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

内部キー管理

内部キーは、コントローラの永続的メモリ上のアクセス不能な場所に保持され、「非表示」になります。内部キー管理を実装するには、次の手順を実行します。

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お問い合わせください。
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た文字列で、コントローラとキーに関連付けられたすべてのドライブに格納されます。パスフレーズは、バックアップ用にセキュリティキーを暗号化するために使用します。内部キーを作成するには、メニューに移動します。[システム]、[セキュリティキー管理]、[内部キーの作成]の順に選択します。

セキュリティキーは、コントローラのアクセスできない非表示の場所に格納されます。その後、セキュリティ有効のボリュームグループまたはプールを作成したり、既存のボリュームグループおよびプールでセキュリティを有効にしたりできます。

外部キー管理

外部キーは、Key Management Interoperability Protocol（KMIP）を使用して別のキー管理サーバに保持されます。外部キー管理を実装するには、次の手順を実行します。

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お問い合わせください。
3. 署名済みのクライアント証明書ファイルを取得します。クライアント証明書は、キー管理サーバがストレージアレイのKMIP要求を信頼できるように、ストレージアレイのコントローラを検証します。
   a. まず、クライアント証明書署名要求（CSR）を生成してダウンロードします。メニューに移動します。Settings [証明書]、[キー管理]、[CSRの作成]の順に選択します。
   b. 次に、キー管理サーバによって信頼されているCAから署名済みクライアント証明書を要求します。（CSRファイルを使用して、キー管理サーバからクライアント証明書を作成およびダウンロードすることもできます）。
   c. クライアント証明書ファイルが作成されたら、そのファイルをSystem Managerにアクセスするホストにコピーします。
4. キー管理サーバから証明書ファイルを取得し、そのファイルをSystem Managerにアクセスするホストにコピーします。キー管理サーバ証明書は、ストレージアレイがサーバのIPアドレスを信頼できるように、キー管理サーバを検証します。キー管理サーバには、ルート証明書、中間証明書、またはサーバ証明書を使用できます。
5. キー管理サーバのIPアドレスとKMIP通信に使用するポート番号を定義して、外部キーを作成します。このプロセスでは、証明書ファイルもロードします。外部キーを作成するには、メニューに移動します。[設定]、[システム]、[セキュリティキー管理]、[外部キーの作成]の順に選択します。

入力したクレデンシャルを使用して、システムがキー管理サーバに接続されます。その後、セキュリティ有効

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

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	製品説明
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。これらのドライブをドライブセキュリティ機能と組み合わせて使用すると、データにアクセスするためのセキュリティキーが必要になります。ドライブをアレイから物理的に取り外した場合、別のアレイに取り付けるまでドライブは動作しません。別のアレイに取り付けると、正しいセキュリティキーを指定するまでセキュリティロック状態になります。
FDEトライフ	Full Disk Encryption（FDE）ドライブは、ハードウェアレベルでディスクドライブの暗号化を実行します。ハードドライブには、書き込み時にデータを暗号化し、読み取り時に復号化するASICチップが搭載されています。
FIPSトライフ	FIPSドライブは、連邦情報処理標準（FIPS）140-2レベル2に準拠しています。基本的な概念はFDEドライブと同じですが、米国政府の基準に従って強力な暗号化アルゴリズムと暗号化方式を実装しています。FIPSドライブにはFDEドライブよりも高度なセキュリティ基準が採用されています。
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）。
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します。ドライブの移行またはヘッドの交換によってバックアップされたセキュリティキーをインポートする場合は、セキュリティキーの暗号化に使用したパスフレーズを指定する必要があります。パスフレーズは8~32文字で指定できます。 ドライブセキュリティのパスフレーズは、ストレージアレイの管理者パスワードとは別のものです。
セキュリティ対応ドライブ	セキュリティ対応ドライブには、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。

期間	製品説明
セキュリティ有効ドライブ	セキュリティ有効ドライブは、ドライブセキュリティ機能で使用されます。ドライブセキュリティ機能を有効にし、かつsecured_caped_drivesのプールまたはボリュームグループにドライブセキュリティを適用すると、ドライブはsecure*enable*になります。読み取り/書き込みアクセスは、正しいセキュリティキーが設定されたコントローラからのみ実行できます。この追加のセキュリティ機能により、ストレージアレイから物理的に取り外されたドライブ上のデータへの不正アクセスを防止できます。
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、コントローラがセキュリティキーを適用するまでセキュリティ有効ドライブはセキュリティロック状態になります。セキュリティ有効ドライブをストレージアレイから取り外すと、ドライブのデータはロックされます。ドライブを別のストレージアレイに取り付け直すと、データへのアクセスを再開する前にセキュリティキーが検索されます。データのロックを解除するには、元のセキュリティキーを適用する必要があります。セキュリティキーは、次のいずれかの方法で作成および管理できます。 • 内部キー管理—セキュリティキーをコントローラの永続的メモリに作成して保持します。 • 外部キー管理—セキュリティキーを外部キー管理サーバに作成して保管します。
セキュリティキー識別子	セキュリティキー識別子は、キーの作成時にセキュリティキーに関連付けられる文字列です。識別子は、コントローラとセキュリティキーに関連付けられたすべてのドライブに格納されます。

セキュリティキーの設定

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には、ストレージアレイのコントローラとセキュリティ対応ドライブで共有される内部セキュリティキーを作成します。内部キーは、コントローラの永続的メモリに保持されます。

開始する前に

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

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

タスクの内容

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

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

手順

1. メニューを選択します。[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)をそのまま使用するか'独自の値を入力することができます入力できる文字数は最大189文字です。使用できるのは英数字のみで、スペース、句読点、記号は使用できません。

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

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

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

4. [作成（ Create ）] をクリックします。

   セキュリティキーは、コントローラのアクセスできない場所に格納されています。実際のキーと一緒に、ブラウザからダウンロードされる暗号化されたキーファイルがあります。

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

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および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再度オンにすると、すべてのセキュリティ有効ドライブがセキュリティロック状態に変わります。この状態のデータには、ドライブの初期化時にコントローラが正しいセキュリティキーを適用するまでアクセスできません。第三者がロックされたドライブを物理的に取り外して別のシステムに取り付けた場合でも、データへの不正アクセスを防止することができます。

終了後

セキュリティキーを検証して、キーファイルが破損していないことを確認する必要があります。

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、キー管理サーバとストレージアレイのセキュリティ対応ドライブで共有される外部キーを作成する必要があります。

開始する前に

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

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

- ドライブセキュリティ機能が有効になっている必要があります。そうしないと、このタスクの実行中に[セキュリティキーを作成できません]ダイアログボックスが開きます。ドライブセキュリティ機能を有効にする手順については、必要に応じてストレージベンダーにお問い合わせください。
- ストレージアレイのコントローラ用の署名済みクライアント証明書ファイルがあり、そのファイルをSystem Managerにアクセスするホストにコピーしておきます。クライアント証明書はストレージアレイのコントローラを検証し、キー管理サーバがKey Management Interoperability Protocol（KMIP）要求を信頼できるようにします。
- キー管理サーバから証明書ファイルを取得し、そのファイルをSystem Managerにアクセスするホストにコピーする必要があります。キー管理サーバ証明書は、ストレージアレイがサーバのIPアドレスを信頼できるように、キー管理サーバを検証します。キー管理サーバには、ルート証明書、中間証明書、またはサーバ証明書を使用できます。

  サーバ証明書の詳細については、キー管理サーバのドキュメントを参照してください。

タスクの内容

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

手順

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。

   現在内部キー管理が設定されている場合は、外部キー管理に切り替えるかどうかを確認するダイアログボックスが開きます。

[外部セキュリティキーの作成]ダイアログボックスが開きます。

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-- KMIP通信に使用するポート番号を入力しますキー管理サーバの通信に使用される最も一般的なポート番号は5696です。

     *オプション：*バックアップ・キー・サーバを構成する場合は、*キー・サーバの追加*をクリックし、そのサーバの情報を入力します。プライマリキーサーバに到達できない場合は、2番目のキーサーバが使用されます。各キーサーバが同じキーデータベースにアクセスできることを確認します。アクセスできないと、アレイはエラーを投稿し、バックアップサーバを使用できません。

     一度に使用されるキーサーバは1つだけです。ストレージアレイがプライマリキーサーバに到達できない場合、アレイはバックアップキーサーバに接続します。両方のサーバ間でパリティを維持する必要があることに注意してください。そうしないと、エラーが発生する可能性があります。

   - クライアント証明書の選択--最初の*参照*ボタンをクリックして、ストレージアレイのコントローラの証明書ファイルを選択します。
   - キー管理サーバのサーバ証明書を選択-- 2番目の*参照*ボタンをクリックして、キー管理サーバの証明書ファイルを選択します。キー管理サーバのルート証明書、中間証明書、またはサーバ証明書を選択できます。

4. 「 * 次へ * 」をクリックします。
5. 「キーの作成/バックアップ」では、セキュリティ上の理由からバックアップ・キーを作成できます。

   - （推奨）バックアップキーを作成する場合は、チェックボックスを選択したまま、パスフレーズを入力して確認します。値は8~32文字で、次の文字をそれぞれ含める必要があります。
     - 大文字のアルファベット（1文字以上）。パスフレーズでは大文字と小文字が区別されることに注意してください。
     - 数字（1文字以上）。
     - !、*、@などの英数字以外の文字（1文字以上）。

     後で使用するために、必ず入力を記録しておいてください。セキュリティ有効ドライブをストレージアレイから移動する必要がある場合は、ドライブデータのロックを解除するためにパスフレーズが必要です。

   +

   - バックアップキーを作成しない場合は、チェックボックスを選択解除します。

     外部キーサーバへのアクセスが失われ、バックアップキーがないと、ドライブを別のストレージアレイに移行するとドライブ上のデータにアクセスできなくなることに注意してください。このオプションは、System Managerでバックアップキーを作成する唯一の方法です。

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。

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

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。

   ページには、次のメッセージと外部キー管理用のリンクが表示されます。

   ```
   Current key management method: External
   ```

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および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再度オンにすると、すべてのセキュリティ有効ドライブがセキュリティロック状態に変わります。この状態のデータには、ドライブの初期化時にコントローラが正しいセキュリティキーを適用するまでアクセスできません。第三者がロックされたドライブを物理的に取り外して別のシステムに取り付けた場合でも、データへの不正アクセスを防止することができます。

終了後

セキュリティキーを検証して、キーファイルが破損していないことを確認する必要があります。

セキュリティキーを管理します。

セキュリティキーの変更

セキュリティキーはいつでも新しいキーに置き換えることができます。社内でセキュリティ侵害の可能性があり、権限のない担当者がドライブデータにアクセスできないようにする場合は、セキュリティキーの変更が必要になることがあります。

手順

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する--(内部セキュリティキーのみ)デフォルトの値（コントローラ ファームウェアで生成されたストレージ アレイ名とタイムスタンプ）をそのまま使用するか、独自の値を入力します。入力できる文字数は最大189文字です。使用できるのは英数字のみで、スペース、句読

点、記号は使用できません。

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

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

4. 外部セキュリティキーの場合、新しいセキュリティキーの作成時に古いセキュリティキーを削除するには、ダイアログの下部にある[Delete current security key…]チェックボックスを選択します。

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

5. [変更（ Change ）] をクリックします。

   前のキーは新しいセキュリティキーで上書きされ、無効になります。

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

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

終了後

セキュリティキーを検証して、キーファイルが破損していないことを確認する必要があります。

外部キー管理から内部キー管理への切り替え

ドライブセキュリティの管理方法を外部キーサーバからストレージアレイで使用される内部方式に変更できます。以前に外部キー管理用に定義したセキュリティキーが、内部キー管理に使用されます。

タスクの内容

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

手順

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。

   [外部キー管理の無効化]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。値は8~32文字で、次の文字をそれぞれ含める必要があります。

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

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

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。

終了後

セキュリティキーを検証して、キーファイルが破損していないことを確認する必要があります。

キー管理サーバ設定の編集

外部キー管理を設定している場合は、キー管理サーバの設定をいつでも表示および編集できます。

手順

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。
   - キー管理ポート番号-- Key Management Interoperability Protocol (KMIP)通信に使用するポート番号を入力します

     オプション： Add Key Server*をクリックすると、別のキーサーバを含めることができます。

4. [保存（ Save ）] をクリックします。

セキュリティキーのバックアップ

セキュリティキーを作成または変更したら、元のキーファイルが破損した場合に備えて、キーファイルのバックアップコピーを作成できます。

タスクの内容

このタスクでは、以前に作成したセキュリティキーをバックアップする方法について説明します。この手順では、バックアップ用の新しいパスフレーズを作成します。このパスフレーズは、元のキーの作成時または最後の変更時に使用されたパスフレーズと一致する必要はありません。このパスフレーズは、作成するバックアップにのみ適用されます。

手順

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。

   値は8~32文字で、次の文字をそれぞれ含める必要があります。

   - 大文字（1文字以上）
   - 数字（1文字以上）
   - 英数字以外の文字（！、*、@など）（1文字以上）

   後で使用するためには、必ず入力を記録してください。このセキュリティキーのバックアップにアクセスするには、パスフレーズが必要です。

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。

終了後

バックアップセキュリティキーを検証する必要があります。

セキュリティキーの検証

セキュリティキーを検証して、セキュリティキーが破損していないこと、およびパスフレーズが正しいことを確認できます。

タスクの内容

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

手順

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. [参照]*をクリックし、キーファイル（など）を選択します `drivesecurity.slk`。
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。

   検証の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される手順に従います。

内部キー管理の使用時のドライブのロック解除

内部キー管理を設定したあとにセキュリティ有効ドライブをストレージアレイ間で移動した場合、ドライブ上の暗号化されたデータにアクセスできるようにするには、セキュリティキーを新しいストレージアレイに再割り当てする必要があります。

開始する前に

- ソースアレイ（ドライブを取り外すアレイ）で、ボリュームグループをエクスポートし、ドライブを取り外しておきます。ターゲットアレイにドライブを取り付け直しておきます。

  > エクスポート/インポート機能はSystem Managerユーザインターフェイスではサポートされていません。ボリュームグループを別のストレージアレイにエクスポート/インポートするには、コマンドラインインターフェイス（CLI）を使用する必要があります。

  ボリュームグループの移行の詳細な手順については、を参照して "NetAppナレッジベース"ください。System Managerで管理している新しいアレイや従来型システムのアレイについては、該当する手順に従ってください。

- ドライブセキュリティ機能が有効になっている必要があります。そうしないと、このタスクの実行中に[セキュリティキーを作成できません]ダイアログボックスが開きます。ドライブセキュリティ機能を有効にする手順については、必要に応じてストレージベンダーにお問い合わせください。
- ロックを解除するドライブに関連付けられているセキュリティキーを確認しておく必要があります。
- セキュリティキーファイルは管理クライアント（System Managerへのアクセスに使用するブラウザを備えたシステム）にあります。別のシステムで管理されているストレージアレイにドライブを移動する場合は、その管理クライアントにセキュリティキーファイルを移動する必要があります。

タスクの内容

内部キー管理を使用する場合、セキュリティキーはストレージアレイにローカルに格納されます。セキュリティキーは、読み取り/書き込みアクセス用にコントローラとドライブで共有される文字列です。ドライブをアレイから物理的に取り外して別のドライブに取り付けた場合、正しいセキュリティキーを指定するまでドライブは動作しません。

コントローラの永続的メモリから内部キーを作成するか、キー管理サーバから外部キーを作成できます。ここでは、_INTERNAL _KEY管理を使用する場合のデータのロック解除について説明します。外部キー管理を使用した場合は、を参照してください"外部キー管理の使用時のドライブのロック解除"。コントローラのアップグレードを実行し、すべてのコントローラを最新のハードウェアに交換する場合は、のEシリーズおよびSANtricityドキュメントセンターに記載されている手順に従う必要があります。"ドライブのロック解除"

セキュリティ有効ドライブを別のアレイに取り付けると、そのアレイでドライブが検出され、「要対応」状態となって「セキュリティ キーが必要です」というステータスが表示されます。ドライブ データのロックを解除するには、セキュリティ キー ファイルを選択し、キーのパス フレーズを入力します（このパスフレーズはストレージアレイの管理者パスワードとは異なります）。

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

手順

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表に表示されます。

3. *オプション：ドライブ番号にカーソルを合わせると、ドライブの場所（シェルフ番号とベイ番号）が表示されます。
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、ダイアログボックスに「The associated secure drives have been unlocked」と表示されます。

結果

すべてのドライブがロックされてロックが解除されると、ストレージアレイ内の各コントローラがリブートされます。ただし、ターゲットストレージアレイ内にロック解除されたドライブがすでにある場合、コントローラはリブートされません。

終了後

デスティネーションアレイ（新しくドライブを取り付けたアレイ）で、ボリュームグループをインポートできるようになりました。

エクスポート/インポート機能はSystem Managerユーザインターフェイスではサポートされていません。ボリュームグループを別のストレージアレイにエクスポート/インポートするには、コマンドラインインターフェイス（CLI）を使用する必要があります。

ボリュームグループの移行の詳細な手順については、を参照して "NetAppナレッジベース"ください。

外部キー管理の使用時のドライブのロック解除

外部キー管理を設定したあとにセキュリティ有効ドライブをストレージアレイ間で移動した場合、ドライブ上の暗号化されたデータにアクセスできるようにするには、セキュリティキーを新しいストレージアレイに再割り当てする必要があります。

開始する前に

- ソースアレイ（ドライブを取り外すアレイ）で、ボリュームグループをエクスポートし、ドライブを取り外しておきます。ターゲットアレイにドライブを取り付け直しておきます。

  エクスポート/インポート機能はSystem Managerユーザインターフェイスではサポートされていません。ボリュームグループを別のストレージアレイにエクスポート/インポートするには、コマンドラインインターフェイス（CLI）を使用する必要があります。

  ボリュームグループの移行の詳細な手順については、を参照して "NetAppナレッジベース"ください。System Managerで管理している新しいアレイや従来型システムのアレイについては、該当する手順に従ってください。

- ドライブセキュリティ機能が有効になっている必要があります。そうしないと、このタスクの実行中に[セキュリティキーを作成できません]ダイアログボックスが開きます。ドライブセキュリティ機能を有効にする手順については、必要に応じてストレージベンダーにお問い合わせください。
- キー管理サーバのIPアドレスとポート番号を確認しておく必要があります。
- ストレージアレイのコントローラ用の署名済みクライアント証明書ファイルがあり、そのファイルをSystem Managerにアクセスするホストにコピーしておきます。クライアント証明書はストレージアレイのコントローラを検証し、キー管理サーバがKey Management Interoperability Protocol（KMIP）要求を信頼できるようにします。
- キー管理サーバから証明書ファイルを取得し、そのファイルをSystem Managerにアクセスするホストにコピーする必要があります。キー管理サーバ証明書は、ストレージアレイがサーバのIPアドレスを信頼できるように、キー管理サーバを検証します。キー管理サーバには、ルート証明書、中間証明書、またはサーバ証明書を使用できます。

サーバ証明書の詳細については、キー管理サーバのドキュメントを参照してください。

タスクの内容

外部キー管理を使用する場合、セキュリティキーは外部のサーバに格納され、セキュリティキーを保護するように設計されています。セキュリティキーは、読み取り/書き込みアクセス用にコントローラとドライブで共有される文字列です。ドライブをアレイから物理的に取り外して別のドライブに取り付けた場合、正しいセキュリティキーを指定するまでドライブは動作しません。

コントローラの永続的メモリから内部キーを作成するか、キー管理サーバから外部キーを作成できます。ここでは、_external_key管理を使用する場合のデータのロック解除について説明します。内部キー管理を使用した場合は、を参照してください"内部キー管理の使用時のドライブのロック解除"。コントローラのアップグレードを実行し、すべてのコントローラを最新のハードウェアに交換する場合は、のEシリーズおよびSANtricityドキュメントセンターに記載されている手順に従う必要があります。"ドライブのロック解除"

セキュリティ有効ドライブを別のアレイに取り付けると、そのアレイでドライブが検出され、「要対応」状態となって「セキュリティ キーが必要です」というステータスが表示されます。ドライブ データのロックを解除するには、セキュリティ キー ファイルをインポートし、キーのパス フレーズを入力します（このパスフレーズはストレージアレイの管理者パスワードとは異なります）。その際に、外部キー管理サーバを使用するようにストレージ アレイを設定すると、セキュリティ キーにアクセスできるようになります。ストレージアレイに接続してセキュリティキーを取得するためには、サーバの連絡先情報を指定する必要があります。

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

手順

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。
3. 必要な接続情報と証明書をウィザードに入力します。
4. ［通信のテスト］をクリックして、外部キー管理サーバへのアクセスを確認します。
5. [セキュアドライブのロック解除]を選択します。

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

6. *オプション：ドライブ番号にカーソルを合わせると、ドライブの場所（シェルフ番号とベイ番号）が表示されます。
7. [*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。

8. このキーファイルに関連付けられているパスフレーズを入力します。

   入力した文字はマスクされます。

9. [ロック解除]をクリックします。

   ロック解除処理が成功すると、ダイアログボックスに「The associated secure drives have been unlocked」と表示されます。

結果

すべてのドライブがロックされてロックが解除されると、ストレージアレイ内の各コントローラがリブートされます。ただし、ターゲットストレージアレイ内にロック解除されたドライブがすでにある場合、コントローラはリブートされません。

終了後

デスティネーションアレイ（新しくドライブを取り付けたアレイ）で、ボリュームグループをインポートできるようになりました。

エクスポート/インポート機能はSystem Managerユーザインターフェイスではサポートされていません。ボリュームグループを別のストレージアレイにエクスポート/インポートするには、コマンドラインインターフェイス（CLI）を使用する必要があります。

ボリュームグループの移行の詳細な手順については、を参照して "NetAppナレッジベース"ください。

FAQ

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で共有されます。セキュリティ有効ドライブをストレージアレイから取り外すと、セキュリティキーによってデータが不正アクセスから保護されます。

セキュリティキーは、次のいずれかの方法で作成および管理できます。

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

内部キー管理

内部キーは、コントローラの永続的メモリ上のアクセス不能な場所に保持され、「非表示」になります。内部セキュリティキーを作成する前に、次の作業を実行する必要があります。

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お問い合わせください。

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

外部キー管理

外部キーは、Key Management Interoperability Protocol（KMIP）を使用して別のキー管理サーバに保持されます。外部セキュリティキーを作成する前に、次の作業を実行する必要があります。

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お問い合わせください。

3. 署名済みのクライアント証明書ファイルを取得します。クライアント証明書は、キー管理サーバがストレージアレイのKMIP要求を信頼できるように、ストレージアレイのコントローラを検証します。

   a. まず、クライアント証明書署名要求（CSR）を生成してダウンロードします。メニューに移動します。Settings [証明書]、[キー管理]、[CSRの作成]の順に選択します。

   b. 次に、キー管理サーバによって信頼されているCAから署名済みクライアント証明書を要求します。（ダウンロードしたCSRファイルを使用して、キー管理サーバからクライアント証明書を作成およびダウンロードすることもできます）。

   c. クライアント証明書ファイルが作成されたら、そのファイルをSystem Managerにアクセスするホストにコピーします。

4. キー管理サーバから証明書ファイルを取得し、そのファイルをSystem Managerにアクセスするホストにコピーします。キー管理サーバ証明書は、ストレージアレイがサーバのIPアドレスを信頼できるように、キー管理サーバを検証します。キー管理サーバには、ルート証明書、中間証明書、またはサーバ証明書を使用できます。

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

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

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

セキュリティキー識別子、関連付けられているパスフレーズ、およびセキュリティキーファイルが保存されているローカルホスト上の場所を必ず記録してください。

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？

バックアップがない状態で元のセキュリティキーが破損した場合、ドライブ上のデータをストレージアレイ間で移行すると、ドライブ上のデータにアクセスできなくなります。

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

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

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

- バックアップ用の新しいパスフレーズを作成します。このパスフレーズは、元のキーの作成時または最後の変更時に使用されたパスフレーズと一致する必要はありません。このパスフレーズは、作成するバックアップにのみ適用されます。

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

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

セキュアドライブのロックを解除するときは、どのような点に注意する必要がありますか？

セキュリティ有効ドライブのデータのロックを解除するには、ドライブのセキュリティキーをインポートする必要があります。

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

- ストレージアレイにすでにセキュリティキーが設定されている必要があります。移行したドライブのキーがターゲットストレージアレイに変更されます。
- 移行するドライブについて、セキュリティキー識別子とセキュリティキーファイルに対応するパスフレーズを確認しておく必要があります。
- セキュリティキーファイルが管理クライアント（System Managerへのアクセスに使用するブラウザを備えたシステム）にある必要があります。
- ロックされたNVMeドライブをリセットする場合は、ドライブのセキュリティIDを入力する必要があります。セキュリティIDを確認するには、ドライブを取り外す必要があります。ドライブのラベルに記載されたPSID（最大32文字）を確認してください。処理を開始する前に、ドライブが再取り付けされていることを確認してください。

読み取り/書き込みアクセスとは何ですか？

[ドライブ設定]ウィンドウには、ドライブセキュリティ属性に関する情報が表示されます。「読み取り/書き込みアクセス」は、ドライブのデータがロックされているかどうかを表示する属性の1つです。

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

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？

セキュリティキーを作成したら、キーファイルを検証して破損していないことを確認する必要があります。

検証に失敗した場合は、次の手順を実行します。

- セキュリティキー識別子がコントローラ上の識別子と一致しない場合は、正しいセキュリティキーファイルを探して検証をやり直してください。
- コントローラが検証用のセキュリティキーを復号化できない場合は、パスフレーズが正しく入力されていない可能性があります。パスフレーズを再確認し、必要に応じて再入力してから、もう一度検証を実行してください。エラーメッセージが再び表示される場合は、キーファイルのバックアップ（存在する場合）を選択して検証を再試行してください。
- それでもセキュリティキーを検証できない場合は、元のファイルが破損している可能性があります。キーの新しいバックアップを作成し、そのコピーを検証してください。

内部セキュリティキー管理と外部セキュリティキー管理の違いは何ですか。

ドライブセキュリティ機能を実装している場合は、内部セキュリティキーまたは外部セキュリティキーを使用して、セキュリティ有効ドライブがストレージアレイから取り外されたときにデータをロックダウンできます。

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。

著作権に関する情報

商標に関する情報