



ドライブセキュリティ SANtricity software

NetApp
November 03, 2025

目次

ドライブセキュリティ	1
SANtricity System Managerのドライブセキュリティについて学ぶ	1
ドライブセキュリティとは何ですか？	1
キー管理を設定するにはどうすればよいですか？	1
ドライブのロックを解除する方法	1
関連情報	2
概念	2
SANtricity System Managerのドライブセキュリティ機能の仕組み	2
SANtricity System Manager におけるセキュリティ キー管理の仕組み	3
SANtricity ソフトウェアのドライブ セキュリティ用語について学習します	5
セキュリティキーを設定する	6
SANtricity System Managerで内部セキュリティキーを作成する	6
SANtricity System Managerで外部セキュリティキーを作成する	8
セキュリティキーを管理します	10
SANtricity System Managerでセキュリティキーを変更する	10
SANtricity System Managerで外部キー管理から内部キー管理に切り替える	11
SANtricity System Managerでキー管理サーバーの設定を編集する	12
SANtricity System Managerでセキュリティキーをバックアップする	13
SANtricity System Managerでセキュリティキーを検証する	13
SANtricity System Manager の内部キー管理を使用しているときにドライブのロックを解除する	14
SANtricity System Managerで外部キー管理を使用しているときにドライブのロックを解除する	16
SANtricity System Manager のストレージ ドライブ セキュリティに関する FAQ	18
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？	18
パスフレーズを定義する必要があるのはなぜですか？	19
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。	19
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？	19
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？	20
読み取り/書き込みアクセスとは何ですか？	20
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？	21
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？	21

ドライブセキュリティ

SANtricity System Managerのドライブセキュリティについて学ぶ

ドライブセキュリティとキー管理は、セキュリティキー管理のページで設定できます。

ドライブセキュリティとは何ですか？

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

詳細はこちら。

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

キー管理を設定するにはどうすればよいですか？

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

詳細はこちら。

- ["内部セキュリティキーを作成します"](#)
- ["外部セキュリティキーを作成します"](#)
- ["プールを手動で作成する"](#)
- ["ボリュームグループを作成します"](#)

ドライブのロックを解除する方法

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

詳細はこちら。

- ["内部キー管理を使用する場合は、ドライブのロックを解除します"](#)

- "外部キー管理を使用する場合は、ドライブのロックを解除します"

関連情報

キー管理に関連するタスクの詳細：

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

概念

SANtricity System Managerの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、取り付けられ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レイから取り外して別のストレージ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ペアとして使用したりすることはできません）。
- ボリュームグループとプールの状態が最適である必要があります。

SANtricity System Manager におけるセキュリティ キー管理の仕組み

ドライブセキュリティ機能を実装する場合、セキュリティ有効ドライブ（FIPSまたはFDE）には、データアクセスのためにセキュリティキーが必要です。セキュリティキーは、ストレージ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レイに再度取り付けると、データに再びアクセスできるようになる前にセキュリティキーが検索されます。データのロックを解除するには、元のセキュリティキーを適用する必要があります。

セキュリティキーは次のいずれかの方法で作成および管理できます。

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

内部キー管理

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

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

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

外部キー管理

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

1. ストレージ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KMIP要求を信頼できるよう、ストレージ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、キー管理サーバで信頼されているCAから署名済みのクライアント証明書を要求します。(CSRファイルを使用してキー管理サーバからクライアント証明書を作成およびダウンロードすることもできます)。
 - c. クライアント証明書ファイルを作成したら、System Managerにアクセスしているホストにそのファイルをコピーします。
 - d. また、秘密鍵と公開鍵のペアを使用して、外部で証明書署名要求を生成することもできます。
4. キー管理サーバから証明書ファイルを取得し、System Managerにアクセスしているホストにそのファイルをコピーします。キー管理サーバ証明書は、ストレージレイがサーバのIPアドレスを信頼できるよう、キー管理サーバを検証します。キー管理サーバには、ルート証明書、中間証明書、またはサーバ証明書を使用できます。
5. 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。

SANtricity ソフトウェアのドライブ セキュリティ用語について学習します

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、取り付けられ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)。
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。

期間	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secureenable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。
セキュリティキー	<p>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。</p> <ul style="list-style-type: none"> • 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。

セキュリティキーを設定する

SANtricity System Managerで内部セキュリティキーを作成する

ドライブセキュリティ機能を使用するために、ストレージアレイのコントローラとセキュリティ対応ドライブで共有される内部セキュリティキーを作成できます。内部キーは、コントローラの永続的メモリに保持されます。

作業を開始する前に

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

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。

SANtricity System Managerで外部セキュリティキーを作成する

キー管理サーバでドライブセキュリティ機能を使用するには、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必要です。このファイルをSystem Managerにアクセスするホストにコピーしておきます。クライアント証明書は、キー管理サーバが自身のKey Management Interoperability Protocol (KMIP) 要求を信頼できるよう、ストレージアレイのコントローラを検証します。
- キー管理サーバから証明書ファイルを取得し、そのファイルをSystem Managerにアクセスするホストにコピーする必要があります。キー管理サーバ証明書は、ストレージアレイがサーバのIPアドレスを信頼できるよう、キー管理サーバを検証します。キー管理サーバには、ルート証明書、中間証明書、またはサーバ証明書を使用できます。



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

このタスクについて

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

手順

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

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



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

- クライアント証明書の選択--最初の*参照*ボタンをクリックして、ストレージアレイのコントローラの証明書ファイルを選択します。
- 秘密鍵ファイルの選択-必要に応じて、2番目の*[参照]*ボタンをクリックして、ストレージアレイのコントローラ用の秘密鍵ファイルを選択します。
- キー管理サーバのサーバ証明書を選択-- 3番目の*[参照]*ボタンをクリックして、キー管理サーバの証明書ファイルを選択します。キー管理サーバのルート証明書、中間証明書、またはサーバ証明書を選択できます。

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

+

- バックアップキーを作成しない場合は、チェックボックスを選択解除します。



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

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管理します

SANtricity System Managerでセキュリティキーを変更する

セキュリティキーは、いつでも新しいキーに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る、ドライブデータへの不正アクセスを防ぎたい場合は、セキュリティキーの変更が必要になることがあります。

手順

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)。

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



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。

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。

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。

SANtricity System Managerで外部キー管理から内部キー管理に切り替える

ドライブセキュリティの管理方法を外部キーサーバからストレージレイで使用される内部の方法に変更することができます。以前に外部キー管理用に定義されたセキュリティキーが内部キー管理に使用されます。

このタスクについて

このタスクでは、外部キー管理を無効にして、新しいバックアップコピーをローカルホストにダウンロードします。既存のキーは引き続きドライブセキュリティに使用されますが、ストレージ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. 「パスワードを定義/パスワードを再入力」で、キーのバックアップに使用するパスワード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）。パスワード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ワードが必要になります。

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、パスワード、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。

SANtricity System Managerでキー管理サーバーの設定を編集する

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

手順

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。

SANtricity System Managerでセキュリティキーをバックアップする

セキュリティキーの作成後または変更後に、元のキーが破損した場合に備えてキーファイルのバックアップコピーを作成することができます。

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）



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。

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。

SANtricity System Managerで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。

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。

SANtricity System Manager の内部キー管理を使用しているときにドライブのロックを解除する

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

作業を開始する前に

- ソースレイ（ドライブを削除するレイ）でボリュームグループをエクスポートし、ドライブを削除しておきます。ターゲット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レイにエクスポート/インポートするには、コマンドラインインターフェイス（CLI）を使用する必要があります。

ボリュームグループの移行手順の詳細については、を参照してください ["ネットアップナレッジベース"](#)。System Managerで管理されている新しいレイや従来型システムの場合は、該当する手順に従ってください。

- ドライブセキュリティ機能を有効にする必要があります。そうしないと、このタスクの実行中に[セキュリティキーを作成できません]ダイアログボックスが開きます。ドライブセキュリティ機能を有効にする手順については、必要に応じてストレージベンダーに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レイにドライブを移動する場合は、その管理クライアントにセキュリティキーファイルを移動する必要があります。

このタスクについて

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



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

セキュリティ有効ドライブを別のアレイに再インストールすると、そのアレイでドライブが検出され、「Needs Attention」状態と「Security Key Needed」ステータスが表示されます。ドライブデータのロックを解除するには、セキュリティキーファイルを選択し、キーのパスフレーズを入力します。（このパスフレーズはストレージアレイの管理者パスワードとは異なります）。

新しいストレージアレイに取り付けられている他のセキュリティ有効ドライブでは、インポートするセキュリティキーとは別のセキュリティキーが使用される場合があります。インポートプロセスでは、取り付けるドライブのデータのロック解除にのみ古いセキュリティキーが使用されます。ロック解除プロセスが成功すると、新しく取り付けられ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. *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、「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ポートされます。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、コントローラはリポートされません。

完了後

デスティネーションアレイ（新しく設置したドライブがあるアレイ）でボリュームグループをインポートできるようにになりました。



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手順の詳細については、を参照してください "[ネットアップナレッジベース](#)"。

SANtricity System Managerで外部キー管理を使用しているときにドライブのロックを解除する

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

作業を開始する前に

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



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

ボリュームグループの移行手順の詳細については、を参照してください "[ネットアップナレッジベース](#)"。System Managerで管理されている新しいアレイや従来型システムの場合は、該当する手順に従ってください。

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



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

このタスクについて

外部キー管理を使用する場合、セキュリティキーは、安全なセキュリティキー用に設計されたサーバの外部に格納されます。セキュリティキーは、読み取り/書き込みアクセス用にコントローラとドライブで共有される文字列です。ドライブをアレイから物理的に取り外して別のドライブに取り付けると、正しいセキュリティキ

ーを指定しないかぎり動作しません。



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

セキュリティ有効ドライブを別のアレイに再インストールすると、そのアレイでドライブが検出され、「Needs Attention」状態と「Security Key Needed」ステータスが表示されます。ドライブデータのロックを解除するには、セキュリティキーファイルをインポートし、キーのパスフレーズを入力します。（このパスフレーズはストレージアレイの管理者パスワードとは異なります）。このプロセスでは、外部キー管理サーバを使用するようにストレージアレイを設定すると、セキュアキーにアクセスできるようになります。ストレージアレイがセキュリティキーに接続して取得するためには、サーバの連絡先情報を指定する必要があります。

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

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、「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レイ内の一部のドライブがすでにロック解除されている場合、コントローラはリブートされません。

完了後

デスティネーションレイ（新しく設置したドライブがあるレイ）でボリュームグループをインポートできるようにしました。



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レイにエクスポート/インポートするには、コマンドラインインターフェイス（CLI）を使用する必要があります。

ボリュームグループの移行手順の詳細については、を参照してください "[ネットアップナレッジベース](#)"。

SANtricity System Manager のストレージ ドライブ セキュリティに関する FAQ

この FAQ は、質問に対する簡単な回答を探している場合に役立ちます。

セキュリティキーを作成するときは、どのような点に注意する必要がありますか？

セキュリティキーは、ストレージ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レイから取り外すと、セキュリティキーによってデータが不正アクセスから保護されます。

セキュリティキーは次のいずれかの方法で作成および管理できます。

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

内部キー管理

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

1. ストレージ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。

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

外部キー管理

外部キーは、Key Management Interoperability Protocol (KMIP) を使用して別のキー管理サーバに保持されま

す。外部セキュリティキーを作成する前に、次の作業を行う必要があります。

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、キー管理サーバで信頼されているCAから署名済みのクライアント証明書を要求します。(ダウンロードしたCSRファイルを使用して、キー管理サーバからクライアント証明書を作成およびダウンロードすることもできます)。
 - c. クライアント証明書ファイルを作成したら、System Managerにアクセスしているホストにそのファイルをコピーします。
4. キー管理サーバから証明書ファイルを取得し、System Managerにアクセスしているホストにそのファイルをコピーします。キー管理サーバ証明書は、ストレージアレイがサーバのIPアドレスを信頼できるように、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。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？

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。

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

読み取り/書き込みアクセスとは何ですか？

Drive Settings（ドライブ設定）ウィンドウには、Drive Security（ドライブセキュリティ）属性に関する情報が表示されます。「読み取り/書き込みアクセス」は、ドライブのデータがロックされている場合に表示される属性の1つです。

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

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レイから取り外されたときにデータをロックダウンすることができます。

セキュリティキーは、ストレージ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

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。