



セキュリティキーを管理します

SANtricity 11.7

NetApp
February 12, 2024

目次

セキュリティキーを管理します	1
セキュリティキーを変更する	1
外部キー管理から内部キー管理に切り替えます	2
キー管理サーバの設定を編集します	3
セキュリティキーをバックアップする	3
セキュリティキーを検証する	4
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	4
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	6

セキュリティキーを管理します

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ます、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。

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。

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。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。

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。

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. [参照]*をクリックし、キーファイル（例：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。

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

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。
- 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

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](#)"。

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

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"。

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

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

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

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

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

商標に関する情報

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