セキュリティキーの管理

SANtricity 11.5

NetApp
February 12, 2024

目次

セキュリティキーの管理

概念

ドライブセキュリティ機能の仕組み

ドライブセキュリティは、 Full Disk Encryption （ FDE ）ドライブまたは連邦情報処理標準（ FIPS ）ドライブを使用してセキュリティを強化するストレージアレイの機能です。これらのドライブにドライブセキュリティ機能を使用すると、データにアクセスするためのセキュリティキーが必要になります。ドライブをアレイから物理的に取り外した場合、別のアレイに取り付けるまでは動作しなくなり、取り付けた時点で正しいセキュリティキーが提供されるまではセキュリティロック状態になります。

ドライブセキュリティを実装する方法

ドライブセキュリティを実装するには、次の手順を実行します。

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

ドライブレベルでのドライブセキュリティの動作

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

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

ストレージアレイレベルでのドライブセキュリティの動作

ドライブセキュリティ機能を使用する場合、セキュリティ有効ドライブとストレージアレイのコントローラで

共有されるセキュリティキーを作成します。ドライブの電源をオフにしてオンにするたびに、コントローラによってセキュリティキーが適用されるまでセキュリティ有効ドライブはセキュリティロック状態になります。

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

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

ボリュームレベルでのドライブセキュリティの動作

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

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

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

ドライブの電源をオフにしてオンにするたびに、コントローラによってセキュリティキーが適用されるまでセキュリティ有効ドライブはセキュリティロック状態になります。セキュリティ有効ドライブをストレージアレイから取り外すと、ドライブのデータはロックされます。ドライブを別のストレージアレイに再度取り付けると、データに再びアクセスできるようになる前にセキュリティキーが検索されます。データのロックを解除するには、元のセキュリティキーを適用する必要があります。

セキュリティキーは次のいずれかの方法で作成および管理できます。

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

内部キー管理

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

1. ストレージアレイにセキュリティ対応ドライブを取り付けます。対応するドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。
2. ドライブセキュリティ機能が有効になっていることを確認します。ドライブセキュリティ機能を有効にする手順については、必要に応じてストレージベンダーに問い合わせてください。
3. 識別子とパスフレーズを定義して、内部セキュリティキーを作成します。識別子は、セキュリティキーに関連付けられる文字列で、コントローラとキーに関連付けられたすべてのドライブに格納されます。パスフレーズは、バックアップ用にセキュリティキーを暗号化するために使用されます。内部キーを作成するには、メニューに移動します。[システム]、[セキュリティキー管理]、[内部キーの作成]の順に選択します。

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

外部キー管理

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

1. ストレージアレイにセキュリティ対応ドライブを取り付けます。対応するドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。
2. ドライブセキュリティ機能が有効になっていることを確認します。ドライブセキュリティ機能を有効にする手順については、必要に応じてストレージベンダーに問い合わせてください。
3. ストレージアレイとキー管理サーバの間の認証用に、クライアントの証明書署名要求（CSR）を生成してダウンロードします。メニューに移動します。Settings [証明書]、[キー管理]、[CSRの作成]の順に選択します。
4. ダウンロードしたCSRファイルを使用して、キー管理サーバからクライアント証明書を作成してダウンロードします。
5. クライアント証明書とキー管理サーバの証明書のコピーがローカルホストにあることを確認します。
6. キー管理サーバのIPアドレスとKMIP通信に使用するポート番号を定義して、外部キーを作成します。このプロセスでは、証明書ファイルもロードします。外部キーを作成するには、メニューに移動します。[設定]、[システム]、[セキュリティキー管理]、[外部キーの作成]の順に選択します。

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

ドライブセキュリティの用語

ストレージアレイに関連するドライブセキュリティの用語を次に示します。

期間	説明
ドライブセキュリティ機能	ドライブセキュリティは、 Full Disk Encryption （ FDE ）ドライブまたは連邦情報処理標準（ FIPS ）ドライブを使用してセキュリティを強化するストレージアレイの機能です。これらのドライブにドライブセキュリティ機能を使用すると、データにアクセスするためのセキュリティキーが必要になります。ドライブをアレイから物理的に取り外した場合、別のアレイに取り付けるまでは動作しなくなり、取り付けた時点で正しいセキュリティキーが提供されるまではセキュリティロック状態になります。
FDEドライブ	Full Disk Encryption（FDE）ドライブは、ハードウェアレベルでディスクドライブの暗号化を実行します。ハードドライブに搭載されたASICチップにより、書き込み時にデータが暗号化され、読み取り時に復号化されます。
FIPSドライブ	FIPSドライブは、連邦情報処理標準（FIPS）140-2レベル2に準拠しています。基本的な概念はFDEドライブと同じですが、米国政府の基準に従って強力な暗号化アルゴリズムと暗号化方式を実装しています。FIPSドライブにはFDEドライブよりも高度なセキュリティ基準が採用されています。
管理クライアント	System Managerにアクセスするためのブラウザを含むローカルシステム（コンピュータやタブレットなど）。
パスフレーズ	パスフレーズは、バックアップ用にセキュリティキーを暗号化するために使用されます。ドライブの移行やヘッドの交換でバックアップされているセキュリティキーをインポートしたときは、セキュリティキーの暗号化に使用したものと同じパスフレーズを指定する必要があります。パスフレーズは8~32文字で指定できます。 ドライブセキュリティのパスフレーズは、ストレージアレイの管理者パスワードとは無関係です。

期間	説明
セキュリティ対応ドライブ	セキュリティ対応ドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。これらのドライブでは、書き込み時にデータが暗号化され、読み取り時に復号化されます。ドライブセキュリティ機能を使用したセキュリティの強化に使用できるため、これらのドライブはsecured_capable_とみなされます。これらのドライブを使用するボリュームグループやプールでドライブセキュリティ機能を有効にすると、ドライブはsecure-_enabled_になります。
セキュリティ有効ドライブ	セキュリティ有効ドライブは、ドライブセキュリティ機能で使用されます。ドライブセキュリティ機能を有効にし、かつsecured_caped_drivesのプールまたはボリュームグループにドライブセキュリティを適用すると、ドライブはsecure*enable*になります。読み取りおよび書き込みアクセスは、正しいセキュリティキーが設定されたコントローラからしか実行できません。この追加のセキュリティ機能により、ストレージアレイから物理的に取り外されたドライブ上のデータへの不正アクセスを防止できます。
セキュリティキー	セキュリティキーは、ストレージアレイのセキュリティ有効ドライブとコントローラで共有される文字列です。ドライブの電源をオフにしてオンにするたびに、コントローラによってセキュリティキーが適用されるまでセキュリティ有効ドライブはセキュリティロック状態になります。セキュリティ有効ドライブをストレージアレイから取り外すと、ドライブのデータはロックされます。ドライブを別のストレージアレイに再度取り付けると、データに再びアクセスできるようになる前にセキュリティキーが検索されます。データのロックを解除するには、元のセキュリティキーを適用する必要があります。セキュリティキーは次のいずれかの方法で作成および管理できます。 • 内部キー管理—セキュリティキーをコントローラの永続的メモリに作成して保管します • 外部キー管理—セキュリティキーを外部キー管理サーバに作成して保管します
セキュリティキー識別子	セキュリティキー識別子は、セキュリティキーの作成時にセキュリティキーに関連付けられる文字列です。この識別子は、コントローラとセキュリティキーに関連付けられたすべてのドライブに格納されます。

方法

内部セキュリティキーを作成します

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

作業を開始する前に

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

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

このタスクについて

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

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

手順

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

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

3. 次のフィールドに情報を入力します。

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

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

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

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

4. [作成（ Create ）] をクリックします。

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

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

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

結果

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

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

完了後

セキュリティキーを検証して、キーファイルが破損していないことを確認します。

外部セキュリティキーを作成します

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

作業を開始する前に

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

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

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

このタスクについて

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

手順

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

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

   [外部セキュリティキーの作成*]ダイアログボックスが開きます。

3. [キーサーバへの接続]で、次のフィールドに情報を入力します。
   - キー管理サーバのアドレス-キー管理に使用するサーバの完全修飾ドメイン名またはIPアドレス（IPv4またはIPv6）を入力します。
   - キー管理ポート番号-- Key Management Interoperability Protocol (KMIP)通信に使用するポート番号を入力しますキー管理サーバの通信に使用される最も一般的なポート番号は5696です。
   - クライアント証明書の選択—最初の参照ボタンをクリックして'ストレージアレイのコントローラの証明書ファイルを選択します
   - キー管理サーバのサーバ証明書を選択します-- 2番目の参照ボタンをクリックして'キー管理サーバの証明書ファイルを選択します
4. 「 * 次へ * 」をクリックします。
5. [**Create/Backup Key**](キーの作成/バックアップ)*で、次のフィールドに情報を入力します。
   - パスフレーズを定義/パスフレーズを再入力—パスフレーズを入力して確認します8~32文字で指定し、以下の文字をそれぞれ1文字以上含める必要があります。
     - 大文字のアルファベット（1文字以上）。パスフレーズでは大文字と小文字が区別されることに注意してください。
     - 数字（1文字以上）。
     - 英数字以外の、！、*、@などの文字（1文字以上）。

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

6. [完了] をクリックします。

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

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

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

   次のメッセージと外部キー管理へのリンクが表示されます。

現在のキー管理方法:外部

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

   テスト結果がダイアログボックスに表示されます。

結果

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

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

完了後

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

セキュリティキーを変更する

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

作業を開始する前に

セキュリティキーがすでに存在している必要があります。

このタスクについて

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

手順

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

   [セキュリティキーの変更*]ダイアログボックスが開きます。

3. 次のフィールドに情報を入力します。

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

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

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

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

4. [変更（ Change ）] をクリックします。

   前のキーが新しいセキュリティキーで上書きされ、無効になります。

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

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

完了後

セキュリティキーを検証して、キーファイルが破損していないことを確認します。

外部キー管理から内部キー管理に切り替えます

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

作業を開始する前に

外部キーが作成されている必要があります。

このタスクについて

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

手順

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

   [外部キー管理を無効にする]ダイアログボックスが開きます。

3. 「パスフレーズを定義/パスフレーズを再入力」で、キーのバックアップに使用するパスフレーズを入力して確認します。8~32文字で指定し、以下の文字をそれぞれ1文字以上含める必要があります。
   - 大文字のアルファベット（1文字以上）。パスフレーズでは大文字と小文字が区別されることに注意し

てください。

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

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

4. [**Disable**] をクリックします。

   バックアップキーがローカルホストにダウンロードされます。

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

結果

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

完了後

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

キー管理サーバの設定を編集します

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

作業を開始する前に

外部キー管理が設定されている必要があります。

手順

1. メニューを選択します。[設定][システム]。
2. セキュリティキー管理*で、*キー管理サーバ設定の表示/編集*を選択します。
3. 次のフィールドの情報を編集します。
   - キー管理サーバのアドレス-キー管理に使用するサーバの完全修飾ドメイン名またはIPアドレス（IPv4またはIPv6）を入力します。
   - KMIPポート番号-- Key Management Interoperability Protocol (KMIP)通信に使用するポート番号を入力します
4. [保存（ Save ）] をクリックします。

セキュリティキーをバックアップする

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

作業を開始する前に

- セキュリティキーがすでに存在している必要があります。

このタスクについて

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

手順

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

   [セキュリティキーのバックアップ*]ダイアログボックスが開きます。

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

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

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

   あとで使用できるように、エントリを記録しておいてください。このセキュリティキーのバックアップにアクセスするには、パスフレーズが必要です。

4. [バックアップ]をクリックします。

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

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

5. パスフレーズを安全な場所に記録し、*閉じる*をクリックします。

完了後

バックアップセキュリティキーを検証する必要があります。

セキュリティキーを検証する

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

作業を開始する前に

セキュリティキーが作成されている必要があります。

このタスクについて

このタスクでは、以前に作成したセキュリティキーを検証する方法について説明します。これは、キーファイルが破損していないこと、およびパスフレーズが正しいことを確認するための重要な手順です。これにより、

セキュリティ有効ドライブをストレージアレイ間で移動する場合に、あとからドライブデータにアクセスできます。

手順

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

   [セキュリティキーの検証*]ダイアログボックスが開きます。

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

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

5. [*Validate]をクリックします。

   検証結果がダイアログボックスに表示されます。

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

セキュリティキーを使用してドライブのロックを解除します

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

作業を開始する前に

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

このタスクについて

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

パスフレーズはストレージアレイの管理者パスワードとは異なります。

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

新しく取り付けたドライブのキーがターゲットストレージアレイのセキュリティキーに変更されます。

手順

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

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

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

   選択したキーファイルがダイアログボックスに表示されます。

5. このキーファイルに関連付けられているパスフレーズを入力します。

   入力した文字はマスクされます。

6. [ロック解除]をクリックします。

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

結果

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

よくある質問です

セキュリティキーを作成するときは、どのような点に注意する必要がありますか？

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

セキュリティキーは次のいずれかの方法で作成および管理できます。

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

内部セキュリティキーを作成する前に、次の作業を行う必要があります。

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

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

外部セキュリティキーを作成する前に、次の作業を行う必要があります。

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

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

パスフレーズを定義する必要があるのはなぜですか？

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

セキュリティキー情報を記録することが重要なのはなぜですか。

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

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

セキュリティキーをバックアップするときは、どのような点に注意する必要がありますか？

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

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

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

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

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

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

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

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

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

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

- （ドライブの移動先となる）ターゲットストレージアレイにすでにセキュリティキーがあることが必要です。移行されたドライブのキーはターゲットストレージアレイのキーに変更されます。
- 移行するドライブについて、セキュリティキー識別子とセキュリティキーファイルに対応するパスフレーズを確認しておきます。
- セキュリティキーファイルは管理クライアント（System Managerへのアクセスに使用するブラウザを備えたシステム）にあります。

読み取り/書き込みアクセスとは何ですか？

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

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

セキュリティキーを検証するときは、どのような点に注意する必要がありますか？

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

検証が失敗した場合は、次の手順を実行します。

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

内部セキュリティキー管理と外部セキュリティキー管理の違いは何ですか？

ドライブセキュリティ*機能を実装している場合、ストレージアレイからセキュリティ有効ドライブを取り外すと、内部セキュリティキーまたは外部セキュリティキーを使用してデータをロックダウンできます。

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

著作権に関する情報

商標に関する情報