セキュリティキーの設定

SANtricity 11.8

NetApp
December 16, 2024

目次

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。

著作権に関する情報

商標に関する情報