設定
SANtricity 11.5

NetApp
February 12, 2024

目次

設定

アラート

概念

アラートの仕組み

アラートは、ストレージアレイで発生した重要なイベントについて管理者に通知します。アラートは E メール、 SNMP トラップ、 syslog を通じて送信できます。

アラートプロセスは次のように機能します。

1. 管理者がSystem Managerで、次のうち1つ以上のアラート方法を設定します。
   - 電子メール--電子メールアドレスにメッセージが送信されます。
   - *snmp *-- SNMPトラップがSNMPサーバに送信されます。
   - *syslog *--メッセージがsyslogサーバに送信される。
2. ストレージアレイのイベントモニタが問題 を検出すると、その問題 に関する情報をイベントログに書き込みます（メニュー：サポート[イベントログ]から選択できます）。これには、バッテリの障害、最適からオフラインへのコンポーネントの状態の変化、コントローラの冗長性の問題などが含まれます。
3. イベントが「アラート対象」であると判断した場合、イベントモニタは設定されているアラート方法（Eメール、SNMP、syslog）を使用して通知を送信します。重大イベントはすべて「アラート対象」とみなされるほか、一部の警告イベントと情報イベントも「アラート対象」とみなされます。

アラートの設定

アラートは、初期セットアップウィザード（Eメールアラートのみ）またはアラートページから設定できます。現在の設定を確認するには、メニューから「Settings [Alerts]」に移動します。

アラートタイルには、アラートの設定が表示されます。次のいずれかになります。

- 未設定。
- 設定：少なくとも1つのアラート方法が設定されています。どのアラート方法が設定されているかを確認するには、カーソルでタイルをポイントします。

アラート情報

アラートには次の種類の情報を含めることができます。

- ストレージアレイの名前。
- イベントログエントリに関連するイベントエラータイプ。
- イベントが発生した日時。
- イベントの短い概要 。

syslogアラートはRFC 3164のメッセージ標準に準拠します。

ストレージアレイに関連するアラートの用語を次に示します。

コンポーネント	説明
イベントモニタ	イベントモニタはストレージアレイに常駐し、バックグラウンドタスクとして実行されます。ストレージアレイで異常を検出すると、その問題に関する情報をイベントログに書き込みます。これには、バッテリの障害、最適からオフラインへのコンポーネントの状態の変化、コントローラの冗長性の問題などが含まれます。イベントが「アラート対象」であると判断した場合、イベントモニタは設定されているアラート方法（Eメール、SNMP、syslog）を使用して通知を送信します。重大イベントはすべて「アラート対象」とみなされるほか、一部の警告イベントと情報イベントも「アラート対象」とみなされます。
メールサーバ	メールサーバはEメールアラートの送受信に使用されます。サーバはSMTP（簡易メール転送プロトコル）を使用します。
SNMP	簡易ネットワーク管理プロトコル（SNMP）は、IPネットワーク上のデバイス間で情報を管理および共有するために使用されるインターネット標準プロトコルです。
SNMPトラップ	SNMPトラップは、SNMPサーバに送信される通知です。トラップには、ストレージアレイの重要な問題に関する情報が含まれています。
SNMP トラップの送信先	SNMPトラップの送信先は、SNMPサービスを実行しているサーバのIPv4またはIPv6アドレスです。
コミュニティ名	コミュニティ名は、SNMP環境内のネットワークサーバのパスワードのような役割を果たす文字列です。
MIBファイル	管理情報ベース（MIB）ファイルは、ストレージアレイ内で監視および管理されているデータを定義します。SNMPサービスアプリケーションがインストールされたサーバにコピーしてコンパイルする必要があります。このMIBファイルは、サポートサイトのSystem Managerソフトウェアで入手できます。
MIB変数	管理情報ベース（MIB）変数は、SNMP GetRequestsへの応答として、ストレージアレイ名、アレイの場所、担当者などの値を返すことができます。

コンポーネント	説明
syslog	syslogは、ネットワークデバイスがイベントメッセージをロギングサーバに送信するために使用するプロトコルです。
UDP	User Datagram Protocol（UDP）は、パケットヘッダーで送信元と送信先のポート番号を指定するトランスポートレイヤプロトコルです。

方法

Eメールアラートの管理

メールサーバとアラートの受信者を設定

Eメールアラートを設定するには、メールサーバのアドレスとアラート受信者のEメールアドレスを指定する必要があります。Eメールアドレスは20個まで指定できます。

作業を開始する前に

- メールサーバのアドレスを確認しておく必要があります。アドレスには、IPv4アドレス、IPv6アドレス、または完全修飾ドメイン名を使用できます。

  完全修飾ドメイン名を使用するには、両方のコントローラにDNSサーバを設定する必要があります。DNSサーバはハードウェアページから設定できます。

- アラート送信者として使用するEメールアドレスを確認しておく必要があります。これは、アラートメッセージの「送信元」フィールドに表示されるアドレスです。SMTPプロトコルでは送信者アドレスが必要です。ない場合はエラーになります。
- アラート受信者のEメールアドレスを確認しておく必要があります。通常、受信者には、ネットワーク管理者またはストレージ管理者のアドレスを指定します。Eメールアドレスは20個まで入力できます。

このタスクについて

このタスクでは、メールサーバの設定方法、送信者と受信者のEメールアドレスの入力方法、および[Alerts]ページから入力したすべてのEメールアドレスのテスト方法について説明します。

Eメールアラートは初期セットアップウィザードから設定することもできます。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. [**Email**]タブを選択します。

   電子メールサーバーがまだ構成されていない場合、[電子メール*]タブに[メールサーバーの構成]と表示されます。

3. ［メールサーバーの設定］を選択します。

[メールサーバーの設定*]ダイアログボックスが開きます。

4. メールサーバの情報を入力し、[保存]をクリックします。
   - メールサーバのアドレス—メールサーバの完全修飾ドメイン名'IPv4アドレス'またはIPv6アドレスを入力します

     完全修飾ドメイン名を使用するには、両方のコントローラにDNSサーバを設定する必要があります。DNSサーバはハードウェアページから設定できます。

   - 電子メール送信者のアドレス—電子メールの送信者として使用する有効な電子メールアドレスを入力しますこのアドレスは、電子メールメッセージの「送信元」フィールドに表示されます。
   - Eメールに連絡先情報を含める—アラートメッセージに送信者の連絡先情報を含めるには、このオプションを選択し、名前と電話番号を入力します。「保存」をクリックすると、電子メールアドレスが「*警告」ページの「電子メール」タブに表示されます。
5. [電子メールの追加]を選択します。

   [電子メールの追加*]ダイアログボックスが開きます。

6. アラート受信者のEメールアドレスを1つ以上入力し、*追加*をクリックします。

   電子メールアドレスは、[アラート（* Alerts *）]ページに表示されます。

7. メールアドレスが有効であることを確認するには、「すべてのメールをテスト」をクリックして、テストメッセージを受信者に送信します。

結果

Eメールアラートを設定すると、アラート対象のイベントが発生するたびにイベントモニタから指定した受信者にEメールメッセージが送信されます。

アラート用のEメールアドレスの編集

Eメールアラートを受け取る受信者のEメールアドレスを変更することができます。

作業を開始する前に

編集する電子メールアドレスは、[Alerts]ページの[Email]タブで定義する必要があります。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. [**Email**]タブを選択します。
3. [**Email Address**]テーブルで、変更するアドレスを選択し、右端にある*Edit*（鉛筆）アイコンをクリックします。

   行が編集可能なフィールドになります。

4. 新しいアドレスを入力し、保存（チェックマーク）アイコンをクリックします。

   変更をキャンセルする場合は、[キャンセル（X）]アイコンを選択します。

結果

[Alerts]ページの[Email]タブには、更新された電子メールアドレスが表示されます。

アラート用の**E**メールアドレスを追加する

Eメールアラートには受信者を20名まで追加できます。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. [**Email**]タブを選択します。
3. [電子メールの追加]を選択します。

   [電子メールの追加]ダイアログボックスが開きます。

4. 空のフィールドに新しいEメールアドレスを入力します。複数のアドレスを追加する場合は、[別の電子メールを追加]を選択して別のフィールドを開きます。
5. [追加（ Add ）] をクリックします。

結果

[Alerts]ページの[Email]タブに新しい電子メールアドレスが表示されます。

アラート用の**E**メールアドレスを削除する

Eメールアラートを受け取る受信者のEメールアドレスを削除できます。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. [**Email**]タブを選択します。
3. [**Email Address**]テーブルから、削除する電子メールアドレスを選択します。

   表の右上にある* Delete *ボタンを選択できるようになります。

4. [削除（ Delete ）] をクリックします。

   [電子メールの削除の確認*]ダイアログボックスが開きます。

5. 操作を確定し、*削除*をクリックします。

結果

このEメールアドレスにアラートが送信されなくなります。

アラート用のメールサーバを編集します

Eメールアラートに使用するメールサーバのアドレスやEメールの送信元のアドレスを変更することができます。

作業を開始する前に

変更するメールサーバのアドレスを確認しておく必要があります。アドレスには、IPv4アドレス、IPv6アドレス、または完全修飾ドメイン名を使用できます。

> 完全修飾ドメイン名を使用するには、両方のコントローラにDNSサーバを設定する必要があります。DNSサーバはハードウェアページから設定できます。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. [**Email**]タブを選択します。
3. ［メールサーバーの設定］を選択します。

   [メールサーバーの設定*]ダイアログが開きます。

4. メールサーバのアドレス、送信者情報、および連絡先情報を編集します。
   - メールサーバのアドレス—メールサーバの完全修飾ドメイン名'IPv4アドレス'またはIPv6アドレスを編集します

     > 完全修飾ドメイン名を使用するには、両方のコントローラにDNSサーバを設定する必要があります。DNSサーバはハードウェアページから設定できます。

   - 電子メール送信者のアドレス—電子メールの送信者として使用する電子メールアドレスを編集します このアドレスは、電子メールメッセージの「送信元」フィールドに表示されます。
   - 電子メールに連絡先情報を含める—送信者の連絡先情報を編集するには、このオプションを選択し、名前と電話番号を編集します。
5. [保存（ Save ）] をクリックします。

SNMPアラートの管理

SNMPアラートのコミュニティとデスティネーションを設定する

簡易ネットワーク管理プロトコル（SNMP）アラートを設定するには、ストレージアレイのイベントモニタからSNMPトラップを送信できるサーバを少なくとも1つ指定する必要があります。この設定には、サーバのコミュニティ名とIPアドレスが必要です。

作業を開始する前に

- ネットワークサーバにSNMPサービスアプリケーションが設定されている必要があります。イベントモニタからトラップメッセージを送信するためには、このサーバのネットワークアドレス（IPv4アドレスまたはIPv6アドレス）が必要です。複数のサーバを使用できます（最大10台のサーバを使用できます）。
- 印刷可能なASCII文字だけを使用したコミュニティ名が作成されている必要があります。コミュニティ名は、ネットワークサーバのパスワードのような役割を果たす文字列で、通常はネットワーク管理者が作成します。コミュニティを最大256個作成できます。
- SNMPサービスアプリケーションがインストールされたサーバに管理情報ベース（MIB）ファイルをコピーしてコンパイルしておきます。このMIBファイルは、監視および管理されるデータを定義します。

  MIBファイルがない場合は、ネットアップサポートサイトから入手できます。

  - に進みます "ネットアップサポート"。

- 「*ダウンロード」をクリックします。
- [*ソフトウェア]をクリックします。
- 管理ソフトウェア（SANtricity System Managerなど）を探し、右側の「* Go ！*」をクリックします。
- 最新バージョンの[**View & Download**（表示とダウンロード）]をクリックします。
- ページの下部にある[* Continue *（続行）]をクリックします。
- EULA に同意します。
- 下にスクロールしてSNMPトラップのMIBファイル*を探し、リンクをクリックしてファイルをダウンロードします。

このタスクについて

このタスクでは、トラップの送信先となるSNMPサーバを指定し、設定をテストする方法について説明します。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. [**SNMP**]タブを選択します。

   コミュニティがまだ設定されていない場合は、SNMPタブに「コミュニティの設定」と表示されます。

3. [コミュニティの設定]を選択します。

   コミュニティの設定*（Configure Communities *）ダイアログボックスが開きます。

4. [コミュニティ名]フィールドに、ネットワークサーバーのコミュニティストリングを1つ以上入力し、[保存*]をクリックします。

   ［アラート］ページに［トラップ送信先の追加］が表示されます。

5. 「トラップ送信先の追加」を選択します。

   [トラップ送信先の追加*]ダイアログボックスが開きます。

6. 1つ以上のトラップ送信先を入力し、関連するコミュニティ名を選択して、* Add *をクリックします。
   - トラップ送信先-- SNMPサービスを実行しているサーバーのIPv4またはIPv6アドレスを入力します
   - コミュニティ名—ドロップダウンから、このトラップの送信先のコミュニティ名を選択します。（コミュニティ名を1つだけ定義した場合は、その名前がこのフィールドにすでに表示されます）。
   - 認証失敗トラップを送信—コミュニティ名が認識されないためにSNMP要求が拒否された場合にトラップの送信先にアラートを送信するには'このオプション(チェックボックス)をオンにします[追加]をクリックすると、トラップの送信先と関連するコミュニティ名が、[警告]ページの[**SNMP**]タブに表示されます。
7. トラップが有効であることを確認するには、テーブルからトラップの送信先を選択し、*トラップの送信先のテスト*をクリックして、設定したアドレスにテストトラップを送信します。

結果

アラート対象のイベントが発生するたびに、イベントモニタからサーバにSNMPトラップが送信されます。

SNMPトラップのコミュニティ名を編集します

SNMPトラップのコミュニティ名を編集できます。また、SNMPトラップの送信先に別のコミュニティ名を関連付けることもできます。

作業を開始する前に

印刷可能なASCII文字だけを使用したコミュニティ名が作成されている必要があります。コミュニティ名は、ネットワークサーバのパスワードのような役割を果たす文字列で、ネットワーク管理者が作成します。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. [**SNMP**]タブを選択します。

   トラップの送信先とコミュニティ名が表に表示されます。

3. コミュニティ名を次のように編集します。
   - コミュニティ名を編集するには、コミュニティの設定*を選択します。新しいコミュニティ名を入力し、 Save *をクリックします。コミュニティ名には印刷可能なASCII文字のみを使用できます。
   - コミュニティ名を新しいトラップ送信先に関連付けるには、テーブルからコミュニティ名を選択し、右端の*編集*（鉛筆）アイコンをクリックします。[コミュニティ名]ドロップダウンから、SNMPトラップの送信先の新しいコミュニティ名を選択し、[保存]（チェックマーク）アイコンをクリックします。

     変更をキャンセルする場合は、[キャンセル（X）]アイコンを選択します。

結果

[**Alerts**]ページの[**SNMP**]タブには、更新されたコミュニティが表示されます。

SNMPトラップのコミュニティ名を追加します

SNMPトラップのコミュニティ名は最大で256個追加できます。

作業を開始する前に

コミュニティ名を作成する必要があります。コミュニティ名は、ネットワークサーバのパスワードのような役割を果たす文字列で、通常はネットワーク管理者が作成します。印刷可能なASCII文字だけで構成されます。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. [**SNMP**]タブを選択します。

   トラップの送信先とコミュニティ名が表に表示されます。

3. [コミュニティの設定]を選択します。

   コミュニティの設定*（Configure Communities *）ダイアログボックスが開きます。

4. [別のコミュニティを追加]を選択します。

5. 新しいコミュニティ名を入力し、* Save *をクリックします。

結果

新しいコミュニティ名は、[* Alerts]ページの[* SNMP]タブに表示されます。

SNMPトラップのコミュニティ名を削除します

SNMPトラップのコミュニティ名を削除できます。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. [**SNMP**]タブを選択します。

   トラップの送信先とコミュニティ名が[Alerts]ページに表示されます。

3. [コミュニティの設定]を選択します。

   コミュニティの設定*（Configure Communities *）ダイアログボックスが開きます。

4. 削除するコミュニティ名を選択し、右端の*削除*（X）アイコンをクリックします。

   このコミュニティ名にトラップ送信先が関連付けられている場合、*コミュニティの削除の確認*ダイアログボックスに、影響を受けるトラップ送信先アドレスが表示されます。

5. 操作を確定し、*削除*をクリックします。

結果

コミュニティ名とそれに関連付けられているトラップ送信先は、[Alerts]ページから削除されます。

SNMP MIB変数を設定します

SNMPアラートの場合、必要に応じて、SNMPトラップに表示される管理情報ベース（MIB）変数を設定できます。これらの変数で、ストレージアレイの名前、場所、および担当者を返すことができます。

作業を開始する前に

SNMPサービスアプリケーションがインストールされたサーバにMIBファイルをコピーしてコンパイルしておく必要があります。

MIBファイルがない場合は、次の方法で入手できます。

- に進みます "ネットアップサポート"。
- 「*ダウンロード」をクリックします。
- [*ソフトウェア]をクリックします。
- 管理ソフトウェア（SANtricity System Managerなど）を探し、右側の「* Go！*」をクリックします。
- 最新バージョンで* View & Download *をクリックします。
- ページの下部にある[* Continue *（続行）]をクリックします。

- EULA に同意します。
- 下にスクロールしてSNMPトラップのMIBファイル*を探し、リンクをクリックしてファイルをダウンロードします。

このタスクについて

このタスクでは、SNMPトラップのMIB変数を定義する方法について説明します。これらの変数は、SNMP GetRequestsに対する応答で次の値を返すことができます。

- *sysName*(ストレージアレイの名前)
- *sysLocation*(ストレージアレイの場所)
- *sysContact*(管理者の名前)

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. [**SNMP**]タブを選択します。
3. [Configure SNMP MIB Variables]を選択します。

   [Configure SNMP MIB Variables*]ダイアログボックスが開きます。

4. 次の値を1つ以上入力し、*保存*をクリックします。
   - **Name**-- MIB変数`*sysName*`の値。たとえば、ストレージアレイの名前を入力します。
   - 場所-- MIB変数`*sysLocation*`の値。たとえば、ストレージアレイの場所を入力します。
   - *Contact *-- MIB変数の値'*sysContact*'。たとえば、ストレージアレイを担当する管理者を入力します。

結果

これらの値はストレージアレイのアラートのSNMPトラップメッセージに表示されます。

SNMPアラートのトラップ送信先を追加します

SNMPトラップの送信に使用するサーバは最大10台まで追加できます。

作業を開始する前に

- 追加するネットワークサーバにSNMPサービスアプリケーションが設定されている必要があります。イベントモニタからトラップメッセージを送信するためには、このサーバのネットワークアドレス（IPv4アドレスまたはIPv6アドレス）が必要です。複数のサーバを使用できます（最大10台のサーバを使用できます）。
- 印刷可能なASCII文字だけを使用したコミュニティ名が作成されている必要があります。コミュニティ名は、ネットワークサーバのパスワードのような役割を果たす文字列で、通常はネットワーク管理者が作成します。コミュニティを最大256個作成できます。
- SNMPサービスアプリケーションがインストールされたサーバに管理情報ベース（MIB）ファイルをコピーしてコンパイルしておきます。このMIBファイルは、監視および管理されるデータを定義します。

  MIBファイルがない場合は、ネットアップサポートサイトから入手できます。

  - に進みます "ネットアップサポート"。

- 「*ダウンロード」をクリックします。
- [*ソフトウェア]をクリックします。
- 管理ソフトウェア（SANtricity System Managerなど）を探し、右側の「* Go ！*」をクリックします。
- 最新バージョンで* View & Download *をクリックします。
- ページの下部にある[* Continue *（続行）]をクリックします。
- EULA に同意します。
- 下にスクロールしてSNMPトラップのMIBファイル*を探し、リンクをクリックしてファイルをダウンロードします。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. [**SNMP**]タブを選択します。

   現在定義されているトラップ送信先が表に表示されます。

3. 「トラップのディスペションを追加」*を選択します。

   [トラップ送信先の追加*]ダイアログボックスが開きます。

4. 1つ以上のトラップ送信先を入力し、関連するコミュニティ名を選択して、* Add *をクリックします。
   - トラップ送信先-- SNMPサービスを実行しているサーバーのIPv4またはIPv6アドレスを入力します
   - コミュニティ名—ドロップダウンから、このトラップの送信先のコミュニティ名を選択します。（コミュニティ名を1つだけ定義した場合は、その名前がこのフィールドにすでに表示されます）。
   - 認証失敗トラップを送信—コミュニティ名が認識されないためにSNMP要求が拒否された場合にトラップの送信先にアラートを送信するには'このオプション(チェックボックス)をオンにします[追加]をクリックすると、トラップの送信先と関連するコミュニティ名が表に表示されます。
5. トラップが有効であることを確認するには、テーブルからトラップの送信先を選択し、*トラップの送信先のテスト*をクリックして、設定したアドレスにテストトラップを送信します。

結果

アラート対象のイベントが発生するたびに、イベントモニタからサーバにSNMPトラップが送信されます。

トラップ送信先を削除します

トラップ送信先のアドレスを削除して、ストレージアレイのイベントモニタからSNMPトラップが送信されないようにすることができます。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. [**SNMP**]タブを選択します。

   トラップ送信先のアドレスが表に表示されます。

3. トラップの送信先を選択し、ページ右上の*削除*をクリックします。

4. 操作を確定し、*削除*をクリックします。

   宛先アドレスが[* Alerts*（警告）]ページに表示されなくなりました。

結果

削除したトラップ送信先にストレージアレイのイベントモニタからSNMPトラップが届かなくなります。

syslogアラートの管理

アラート用のsyslogサーバを設定します

syslogアラートを設定するには、syslogサーバのアドレスとUDPポートを入力する必要があります。最大5台のsyslogサーバを指定できます。

作業を開始する前に

- syslogサーバのアドレスを確認しておく必要があります。このアドレスは、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスのいずれかで指定できます。
- syslogサーバのUDPポート番号を確認しておく必要があります。通常は514です。

このタスクについて

このタスクでは、syslogサーバのアドレスとポートを入力し、入力したアドレスをテストする方法について説明します。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. *Syslog *タブを選択します。

   syslogサーバがまだ定義されていない場合、[*Alerts]ページに[Add Syslog Servers]と表示されます。

3. [Add Syslog Servers]をクリックします。

   [Add Syslog Server*]ダイアログボックスが開きます。

4. 1つ以上のsyslogサーバ（最大5つ）の情報を入力し、* Add *をクリックします。
   - サーバーアドレス—完全修飾ドメイン名’IPv4アドレス’またはIPv6アドレスを入力します
   - UDPポート-- syslogのUDPポートは通常は514です。設定されているsyslogサーバが表に表示されます。
5. サーバーアドレスにテストアラートを送信するには、*すべてのSyslogサーバーをテスト*を選択します。

結果

アラート対象のイベントが発生するたびに、イベントモニタからsyslogサーバにアラートが送信されます。

アラート用のsyslogサーバを編集します

syslogアラートの受信に使用するサーバアドレスを編集できます。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. *Syslog *タブを選択します。
3. 表からsyslogサーバのアドレスを選択し、右端の* Edit *（鉛筆）アイコンをクリックします。

   行が編集可能なフィールドになります。

4. サーバーアドレスとUDPポート番号を編集し、保存（チェックマーク）アイコンをクリックします。

結果

更新されたサーバアドレスが表に表示されます。

アラート用の**syslog**サーバを追加します

syslogアラート用に最大5台のサーバを追加できます。

作業を開始する前に

- syslogサーバのアドレスを確認しておく必要があります。このアドレスは、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスのいずれかで指定できます。
- syslogサーバのUDPポート番号を確認しておく必要があります。通常は514です。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. *Syslog *タブを選択します。
3. [Add Syslog Servers]を選択します。

   [Add Syslog Server*]ダイアログボックスが開きます。

4. [Add another syslog server*]を選択します。
5. syslogサーバの情報を入力し、*Add*をクリックします。

   - syslogサーバアドレス—完全修飾ドメイン名'IPv4アドレス'またはIPv6アドレスを入力します
   - UDPポート-- syslogのUDPポートは通常は514です。

   最大5台のsyslogサーバを設定できます。

結果

syslogサーバのアドレスが表に表示されます。

アラート用の**syslog**サーバを削除します

syslogサーバを削除してアラートの受信を中止することができます。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. *Syslog *タブを選択します。

3. syslogサーバのアドレスを選択し、右上の「* Remove *」をクリックします。

   [**Confirm Delete Syslog Server**]ダイアログボックスが開きます。

4. 操作を確定し、*削除*をクリックします。

結果

削除したサーバにイベントモニタからアラートが届かなくなります。

よくある質問です

アラートが無効になっている場合

ストレージアレイで発生する重要なイベントに関する通知を管理者が受信できるようにするには、アラート方法を設定する必要があります。

SANtricity System Managerで管理されるストレージアレイの場合は、アラートページからアラートを設定します。アラート通知は、Eメール、SNMPトラップ、またはsyslogメッセージを介して送信できます。また、初期セットアップウィザードからEメールアラートを設定することもできます。

SNMPまたは**syslog**のアラートを設定するにはどうすればよいですか？

Eメールアラートに加えて、アラートが簡易ネットワーク管理プロトコル（SNMP）トラップまたはsyslogメッセージで送信されるように設定できます。

SNMPまたはsyslogのアラートを設定するには、メニューの[アラート]に移動します。

アレイとアラートでタイムスタンプが異なるのはなぜですか？

ストレージアレイは、アラートの送信時にアラートを受信するターゲットサーバまたはホストのタイムゾーンに合わせて修正を行いません。代わりに、ローカル時間（GMT）を使用してアラートの記録に使用されるタイムスタンプを作成します。そのため、ストレージアレイのタイムスタンプと、アラートを受信するサーバまたはホストのタイムスタンプが一致しないことがあります。

ストレージアレイはアラートの送信時にタイムゾーンを修正しないため、アラートのタイムスタンプはGMTであり、タイムゾーンオフセットはゼロです。タイムスタンプをローカルのタイムゾーンに換算するには、GMTからのオフセットを特定し、タイムスタンプにその値を加算するか減算します。

> この問題 を回避するには、ストレージアレイコントローラにネットワークタイムプロトコル（NTP）を設定します。これにより、コントローラが常に正しい時刻に同期されます。

システム

ストレージアレイの設定

キャッシュの設定とパフォーマンス

キャッシュメモリは、ドライブメディアよりも速くアクセスできる、コントローラ上の一時的な揮発性ストレージ領域です。

キャッシュを使用すると、全体的なI/Oパフォーマンスを次のように向上させることができます。

- 読み取り用にホストから要求されたデータが以前の処理からすでにキャッシュに格納されている可能性があるため、ドライブへのアクセスが不要になります。
- 書き込みデータは最初にキャッシュに書き込まれるため、データがドライブに書き込まれるのを待つことなくアプリケーションが処理を続行できます。

デフォルトのキャッシュ設定はほとんどの環境の要件を満たしていますが、必要に応じて設定を変更できます。

ストレージアレイキャッシュの設定

ストレージアレイ内のすべてのボリュームについて、Systemページで次の値を指定できます。

- フラッシュの開始値--キャッシュフラッシュ（ディスクへの書き込み）をトリガーするキャッシュ内の書き込み前のデータの割合。指定した開始の割合の書き込み前のデータがキャッシュに格納されると、フラッシュがトリガーされます。デフォルトでは、キャッシュが80%フルに達すると、コントローラがキャッシュのフラッシュを開始します。
- キャッシュブロックサイズ--キャッシュ管理の組織単位である各キャッシュブロックの最大サイズ。キャッシュブロックサイズはデフォルトで8KiBですが、4、8、16、32KiBに設定できます。アプリケーションの一般的なI/Oサイズにキャッシュブロックサイズを設定するのが理想的です。ファイルシステムやデータベースアプリケーションでは一般に小さいサイズを使用し、大規模なデータ転送やシーケンシャルI/Oを必要とするアプリケーションには大きいサイズが適しています

ボリュームキャッシュの設定

ストレージアレイ内の個々のボリュームについて、Volumes（ボリューム）ページで次の値を指定できます（メニュー：Storage [Volumes]）。

- 読み取りキャッシュ--読み取りキャッシュは'ドライブから読み取られたデータを格納するバッファです読み取り処理の対象となるデータが以前の処理ですでにキャッシュに格納されていれば、ドライブにアクセスする必要はありません。読み取りキャッシュのデータは、フラッシュされるまで保持されます。
  - 動的キャッシュ読み取りプリフェッチ--動的キャッシュ読み取りプリフェッチにより'コントローラは'ドライブからキャッシュにデータ・ブロックを読み取っているときに'追加のシーケンシャル・データ・ブロックをキャッシュにコピーすることができますこのキャッシングにより、以降のデータ要求にキャッシュから対応できる可能性が高まります。動的キャッシュ読み取りプリフェッチは、シーケンシャルI/Oを使用するマルチメディアアプリケーションで重要ですデータがキャッシュにプリフェッチされる速度と量は、ホスト読み取りの速度と要求サイズに基づいて自動で調整されます。ランダムアクセスの場合、原因 データがキャッシュにプリフェッチされることはありません。この機能は、読み取りキャッシュが無効になっている場合は適用されません。
- 書き込みキャッシュ--書き込みキャッシュは'まだドライブに書き込まれていないホストからのデータを格納するバッファです書き込みキャッシュ内のデータは、ドライブに書き込まれるまで保持されます。書き込みキャッシュにより、I/Oパフォーマンスを向上させることができます。

データ損失の可能性-バッテリなしの書き込みキャッシュオプションを有効にし、保護用のユニバーサル電源装置がない場合、データが失われる可能性があります。また、コントローラのバッテリがない場合にWrite caching without Batteriesオプションを有効にすると、データが失われる可能性があります。

- バッテリなしの書き込みキャッシュ--バッテリなしの書き込みキャッシュ設定により、バッテリがない、故障している、完全に放電されている、またはフル充電されていない場合でも書き込みキャッシュを続行できます。バッテリなしの書き込みキャッシュを選択すると電源の喪失時にデータが失われる可能性があるため、一般には推奨されません。通常、書き込みキャッシュは、バッテリが充電されるか障害が発生したバッテリが交換されるまで、コントローラによって一時的にオフにされます。
- ミラーリングありの書き込みキャッシュ--ミラーリングありの書き込みキャッシュは'一方のコントローラのキャッシュ・メモリに書き込まれたデータがもう一方のコントローラのキャッシュ・メモリにも書き込まれたときに発生しますそのため、一方のコントローラで障害が発生した場合、もう一方のコントローラで未処理の書き込み処理をすべて完了できます。書き込みキャッシュのミラーリングは、書き込みキャッシュが有効で、2台のコントローラが配置されている場合にのみ使用できます。ミラーリングありの書き込みキャッシュは、ボリュームの作成時にデフォルトで設定されます。

自動ロードバランシングの概要

自動ロードバランシングを使用すると、負荷の変化に動的に対応してボリュームのコントローラ所有権が自動的に調整されるため、コントローラ間でワークロードが移動する際の負荷の不均衡が解消され、I/Oリソースの管理が強化されます。

各コントローラのワークロードは継続的に監視され、ホストにインストールされたマルチパスドライバとの連携により、必要に応じて自動的に負荷を分散できます。ワークロードがコントローラ間で自動的に再分散されるため、ストレージアレイの負荷の変化に合わせてボリュームのコントローラ所有権を手動で調整する必要がなくなり、ストレージ管理者の負担が軽減されます。

自動ロードバランシングを有効にすると、次の機能が実行されます。

- コントローラのリソース利用率を自動的に監視して負荷を分散します。
- ボリュームのコントローラ所有権が必要に応じて自動的に調整され、ホストとストレージアレイの間のI/O帯域幅が最適化されます。

自動ロードバランシングの有効化と無効化

自動ロードバランシングは、すべてのストレージアレイでデフォルトで有効になっています。

自動ロードバランシングは、ストレージアレイの状況に応じて無効にすることができます。たとえば、次のような場合です。

- 特定のボリュームのコントローラ所有権については、ワークロードを分散するために自動的に変更されないようにする場合。
- 高度に調整された環境で、コントローラ間の負荷分散が特定の要件を満たすように意図的に設定されている。

自動ロードバランシング機能をサポートするホストタイプ

自動ロードバランシングを有効にするのはストレージアレイレベルですが、ホストまたはホストクラスタに選択したホストタイプがこの機能の動作に直接影響します。

ストレージアレイのワークロードをコントローラ間で分散する際、自動ロードバランシング機能は、両方のコントローラからアクセスでき、自動ロードバランシング機能をサポートするホストまたはホストクラスタにのみマッピングされたボリュームの移動を試みます。

これにより、ロードバランシングプロセスによってホストがボリュームにアクセスできなくなることはありませんが、自動ロードバランシングをサポートしていないホストにマッピングされたボリュームがあると、ストレージアレイはワークロードを分散できなくなります。自動ロードバランシングがワークロードを分散するためには、マルチパスドライバがTPGSをサポートしていることと、ホストタイプが次の表に含まれていることが必要です。

ホストクラスタが自動ロードバランシングに対応しているとみなされるのは、そのグループ内のすべてのホストが自動ロードバランシングをサポートしている場合です。

自動ロードバランシングをサポートするホストタイプ	マルチパスドライバ
WindowsまたはWindowsクラスタ	MPIOとNetApp EシリーズDSM
Linux DM-MP（カーネル3.10以降）	DM-MPと'scsi_dh_aluaデバイス・ハンドラ
VMware	Native Multipathing Plugin（NMP）と'VMW_SATP_ALUA Storage Array Type'プラグイン

一部の例外を除き、自動ロードバランシングをサポートしていないホストタイプは、この機能が有効になっているかどうかに関係なく正常に動作し続けます。例外の1つがシステムのフェイルオーバーです。データパスが復旧すると、ストレージアレイはマッピングされていないボリュームまたは割り当てられていないボリュームを所有権を持つコントローラに戻しますが、自動ロードバランシングをサポートしていないホストにマッピングまたは割り当てられているボリュームは移動されません。

を参照してください "Interoperability Matrix Tool で確認してください" サポートされるマルチパスドライバ、OSレベル、コントローラドライブトレイの互換性情報については、を参照してください。

自動ロードバランシング機能とOSの互換性の確認

新しいシステムを設定（または既存のシステムを移行）する前に、自動ロードバランシング機能とOSの互換性を確認します。

1. にアクセスします "Interoperability Matrix Tool で確認してください" をクリックして解決策 を検索し、サポートを確認してください。

   Red Hat Enterprise Linux 6またはSUSE Linux Enterprise Server 11を実行しているシステムの場合は、テクニカルサポートにお問い合わせください。

2. /etc/multipath.confファイルを更新して構成します
3. 該当するベンダーおよび製品の「retain_attached_device_handler」と「detect_prio」の両方が「yes」に設定されていることを確認するか、デフォルトの設定を使用します。

デフォルトのホストオペレーティングシステムタイプ

デフォルトのホストタイプは、ホストの最初の接続時にストレージアレイで使用されます。ボリュームがアクセスされたときに、ストレージアレイのコントローラがホストのオペレーティングシステムとどのように連携するかを定義します。接続されたホストを基準にストレージアレイの動作を変更する必要がある場合は、ホストタイプを変更できます。

一般に、デフォルトのホストタイプは、ストレージアレイにホストを接続する前、または追加のホストを接続するときに変更します。

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接続するホストのオペレーティングシステムがすべて同じ場合は（同機種ホスト環境）、オペレーティングシステムに一致するホストタイプに変更します。
- ストレージアレイに接続するホストに異なるオペレーティングシステムのホストが混在している場合は（異機種ホスト環境）、ホストのオペレーティングシステムの大部分に一致するホストタイプに変更します。

  たとえば、8つの異なるホストをストレージアレイに接続し、そのうち6つでWindowsオペレーティングシステムを実行している場合は、Windowsをデフォルトのホストオペレーティングシステムタイプとして選択する必要があります。

- ほとんどの接続ホストでオペレーティングシステムが異なる場合は、ホストタイプを工場出荷時のデフォルトに変更します。

  たとえば、8つの異なるホストをストレージアレイに接続し、そのうち2つのホストがWindowsオペレーティングシステムを実行している場合、3つのホストがHP-UXオペレーティングシステムを実行しています。 さらに、別の3つのOSでLinuxオペレーティングシステムを実行している場合は、デフォルトのホストオペレーティングシステムタイプとしてFactory Defaultを選択する必要があります。

方法

ストレージアレイ名を編集します

SANtricity System Managerのタイトルバーに表示されるストレージアレイ名を変更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. **[General]**で**[*Name:]**フィールドを探します。

   ストレージアレイ名が定義されていない場合、このフィールドには「不明」と表示されます。

3. ストレージアレイ名の横にある* Edit *（鉛筆）アイコンをクリックします。

   フィールドが編集可能になります。

4. 新しい名前を入力します。

名前には、アルファベット、数字、アンダースコア（_）、ダッシュ（-）、ハッシュ記号（#）を使用できます。スペースを含めることはできません。名前の最大文字数は30文字です。名前は一意である必要があります。

5. [保存（Save *）]（チェックマーク）アイコンをクリックします。

変更せずに編集可能なフィールドを閉じるには、[キャンセル（X）]アイコンをクリックします。

結果

新しい名前がSANtricity System Managerのタイトルバーに表示されます。

ストレージアレイのロケーターライトを点灯します

キャビネット内のストレージアレイの物理的な場所を特定するために、ストレージアレイのロケーター（LED）ライトを点灯できます。

手順

1. メニューを選択します。[設定][システム]。
2. [*General]で、[*Turn on Storage Array Locator Lights]をクリックします。

ストレージアレイのロケーターライトを点灯*ダイアログボックスが開き、対応するストレージアレイのロケーターライトが点灯します。

3. ストレージアレイが物理的に配置されている場合は、ダイアログボックスに戻り、*電源オフ*を選択します。

結果

ロケーターライトが消灯してダイアログボックスが閉じます。

ストレージアレイのクロックを同期する

ネットワークタイムプロトコル（NTP）が無効な場合は、コントローラのクロックを手動で設定して、管理クライアント（SANtricity System Managerにアクセスするブラウザの実行に使用されるシステム）と同期されるようにすることができます。

このタスクについて

同期によって、イベントログ内のイベントのタイムスタンプがホストログファイルに書き込まれるタイムスタンプと一致します。同期プロセスの実行中も、コントローラを引き続き使用できます。

System ManagerでNTPが有効になっている場合は、このオプションを使用してクロックを同期しないでください。代わりに、NTPではシンプルネットワークタイムプロトコル（SNTP）を使用してクロックを自動的に同期します。

同期後に、パフォーマンス統計が失われたり精度が低下したりする可能性があります。また、スケジュールに影響が生じたり（ASUP、Snapshotなど）、ログデータ内のタイムスタンプが不正確になる可能性もあります。NTPを使用すると、この問題を回避できます。

手順

1. メニューを選択します。[設定][システム]。
2. [**General**]で'[*ストレージ・アレイ・クロックの同期化]をクリックします

   ストレージ・アレイ・クロックの同期*ダイアログ・ボックスが開きますこのダイアログには、コントローラおよび管理クライアントとして使用されているコンピュータの現在の日時が表示されます。

   シンプレックスストレージアレイの場合、表示されるコントローラは1台だけです。

3. ダイアログボックスに表示された時間が一致しない場合は、*同期化*をクリックします。

結果

同期が成功すると、イベントのタイムスタンプはイベントログとホストログで同じになります。

ストレージアレイの構成を保存します

ストレージアレイの構成情報をスクリプトファイルに保存すると、追加のストレージアレイをセットアップする際に同じ構成を使用するための時間を節約できます。

作業を開始する前に

論理構成の設定を変更する処理がストレージアレイで行われていないことを確認してください。このような処理の例としては、ボリュームの作成または削除、コントローラファームウェアのダウンロード、ホットスペアドライブの割り当てまたは変更、ボリュームグループへの容量（ドライブ）の追加などがあります。

このタスクについて

ストレージアレイの構成を保存すると、ストレージアレイの設定、ボリュームの構成、ホストの構成、またはストレージアレイに対するホストとボリュームの割り当てを含むコマンドラインインターフェイス（CLI）スクリプトが生成されます。生成されたこのCLIスクリプトを使用して、ハードウェア構成がまったく同じ別のストレージアレイに構成をレプリケートできます。

ただし、ディザスタリカバリにはこのCLIスクリプトを使用しないでください。システムをリストアするには、代わりに、手動で作成する構成データベースのバックアップファイルを使用するか、テクニカルサポートに問い合わせて最新のAutoSupportデータからこのデータを取得してください。

この操作では、次の設定は保存されません。

- バッテリの寿命です
- コントローラの時刻
- 不揮発性静的ランダムアクセスメモリ（NVSRAM）の設定
- すべてのプレミアム機能
- ストレージアレイのパスワード
- ハードウェアコンポーネントの動作ステータスと状態
- ボリュームグループの動作ステータス（最適を除く）と状態
- ミラーリング、ボリュームコピーなどのコピーサービス

アプリケーションエラーのリスク-論理構成の設定を変更する処理をストレージアレイで実行中の場合は、このオプションを使用しないでください。このような処理の例としては、ボリュームの作成または削除、コントローラファームウェアのダウンロード、ホットスペアドライブの割り当てまたは変更、ボリュームグループへの容量（ドライブ）の追加などがあります。

手順

1. メニューを選択します。[設定][システム]。
2. 「ストレージアレイ構成の保存」を選択します。
3. 保存する構成の項目を選択します。
   - ストレージアレイの設定
   - ボリューム構成
   - ホスト構成
   - ホスト/ボリューム間の割り当て

   ［ホスト/ボリューム間の割り当て］項目を選択した場合、［ボリューム構成］項目と［ホスト構成］項目もデフォルトで選択されます。また、*ボリューム構成*と*ホスト構成*を保存しないと、ホスト/ボリューム間の割り当て*を保存できません。
4. [保存（ Save ）] をクリックします。

   ファイルは'storagearray-configuration.cfgという名前でブラウザのDownloadsフォルダに保存されます

完了後

ストレージアレイの構成を別のストレージアレイにロードするには、SANtricity Unified Managerを使用します。

ストレージアレイの構成のクリア

ストレージアレイからすべてのプール、ボリュームグループ、ボリューム、ホストの定義、およびホストの割り当てを削除する場合は、設定のクリア処理を使用します。

作業を開始する前に

- ストレージアレイ構成をクリアする前に、データのバックアップを作成します。

このタスクについて

ストレージアレイ構成のクリアオプションは2つあります。

- ボリューム--通常、テスト用ストレージアレイを本番ストレージアレイとして再構成するために、ボリュームオプションを使用します。たとえば、テスト用にストレージアレイを構成し、テストが完了したらテスト構成を削除し、本番環境用にストレージアレイをセットアップする場合があります。
- ストレージ・アレイ--通常'ストレージ・アレイを別の部門またはグループに移動するには'ストレージ・アレイ・オプションを使用しますたとえば、エンジニアリング部門が新しいストレージアレイを導入することになり、現在使用しているストレージアレイを管理部門に移動する場合などです。

  ストレージアレイオプションを選択すると、追加の設定がいくつか削除されます。

	ボリューム	ストレージアレイ
プールとボリュームグループを削除します	X	X
ボリュームを削除します	X	X
ホストとホストクラスタを削除します	X	X
ホスト割り当てを削除します	X	X
ストレージアレイ名を削除します		X
ストレージアレイのキャッシュ設定をデフォルトにリセットします		X

データ損失のリスク-この処理を実行すると、ストレージアレイからすべてのデータが削除されます。（完全消去は実行されません）。 この処理は開始後にキャンセルすることはできません。この処理は、テクニカルサポートから指示があった場合にのみ実行してください。

手順

1. メニューを選択します。[設定][システム]。
2. 「ストレージアレイ構成のクリア」を選択します。
3. ドロップダウンリストで、* Volume または Storage Array *のいずれかを選択します。
4. オプション：（データではなく）設定を保存する場合は、ダイアログボックス内のリンクを使用します。
5. 処理を確定します。

結果

- 現在の構成が削除され、ストレージアレイ上の既存のデータがすべて破棄されます。
- すべてのドライブの割り当てが解除されます。

ログインバナーを設定します

ユーザがSANtricity System Managerでセッションを確立する前に表示されるログインバナーを作成できます。バナーには、注意と同意を求めるメッセージを含めることができます。

このタスクについて

作成したバナーは、ログイン画面の前にダイアログボックスに表示されます。

手順

1. メニューを選択します。[設定][システム]。
2. 「一般」セクションで、「*ログインバナーの設定」を選択します。

[ログインバナーの設定*]ダイアログボックスが開きます。

3. ログインバナーに表示するテキストを入力します。

書式設定にHTMLタグやその他のマークアップタグを使用しないでください。

4. [保存（ Save ）] をクリックします。

結果

ユーザが次回System Managerにログインすると、このテキストがダイアログボックスに表示されます。ログイン画面に進むには、*OK*をクリックする必要があります。

セッションタイムアウトの管理

非アクティブな状態が一定の時間続いたユーザセッションは切断されるよう、SANtricity System Managerでタイムアウトを設定できます。

このタスクについて

デフォルトでは、System Managerのセッションタイムアウトは30分です。この時間を調整したり、セッションタイムアウトを無効にしたりすることができます。

アレイに組み込まれているSecurity Assertion Markup Language（SAML）機能を使用してアクセス管理が設定されている場合は、ユーザのSSOセッションがその期限に達したときにセッションタイムアウトが発生する可能性があります。これは、System Managerのセッションタイムアウトより前に発生することがあります。

手順

1. メニューを選択します。[設定][システム]。
2. 「一般」セクションで、「セッションタイムアウトの有効化/無効化」を選択します。

セッションタイムアウト*の有効化/無効化ダイアログボックスが開きます。

3. スピナーコントロールを使用して、時間を分単位で増減できます。

System Managerに設定できる最小のタイムアウトは15分です。

セッションタイムアウトを無効にするには、*時間の長さを設定*チェックボックスの選択を解除します。

4. [保存（ Save ）] をクリックします。

ストレージアレイのキャッシュ設定を変更します

ストレージアレイ内のすべてのボリュームでは、フラッシュおよびブロックサイズについてキャッシュメモリの設定を調整できます。

このタスクについて

キャッシュメモリは、ドライブメディアよりも速くアクセスできる、コントローラ上の一時的な揮発性ストレ

ージ領域です。キャッシュのパフォーマンスを調整するには、次の設定を調整します。

キャッシュ設定	説明
デマンドキャッシュフラッシュを開始します	キャッシュに格納された書き込み前のデータが何パーセントに達したらキャッシュフラッシュ（ディスクへの書き込み）を開始するかを指定します。デフォルトでは、書き込み前のデータが容量の80%に達するとキャッシュフラッシュが開始されます。書き込み処理が中心の環境では、この割合を高くすると、新しい書き込み要求をディスクにアクセスせずにキャッシュで処理できるため便利です。I/Oが不規則でデータのバーストがある環境では、この割合を低くして、バーストとバーストの間に頻繁にキャッシュがフラッシュされるようにすると効果的です。ただし、80%より小さいパーセントの開始パーセント値を指定すると、原因 のパフォーマンスが低下する可能性があります。
キャッシュブロックサイズ	キャッシュブロックサイズは、各キャッシュブロックの最大サイズであり、キャッシュを管理する際の単位となります。デフォルトのブロックサイズは8KiBです。System Managerでは、4、8、16、または32KiBのキャッシュブロックサイズを選択できます。使用するブロックサイズはアプリケーションによって異なり、ストレージのパフォーマンスに影響します。ファイルシステムやデータベースアプリケーションには小さいサイズが適しています。マルチメディアなどのシーケンシャルI/Oを生成するアプリケーションには、大きいサイズが適しています。

手順

1. メニューを選択します。[設定][システム]。
2. 下にスクロールして「その他の設定」を選択し、「キャッシュ設定の変更」をクリックします。

   [キャッシュ設定の変更]ダイアログボックスが開きます。

3. 次の値を調整します。
   - デマンドキャッシュフラッシュの開始—環境で使用されているI/Oに適した割合を選択します80%未満の値を選択すると、パフォーマンスが低下する可能性があります。
   - キャッシュブロックサイズ—アプリケーションに適したサイズを選択します
4. [保存（ Save ）] をクリックします。

ホスト接続レポートの設定

ホスト接続レポートを有効にすると、コントローラと設定済みのホスト間の接続をストレージアレイで常時監視して、接続が中断された場合に通知されるようにすることができます。この機能はデフォルトで有効になっています。

このタスクについて

ホスト接続のレポートを無効にすると、接続またはストレージアレイに接続されているホストに関するマルチパスドライバの問題がシステムによって監視されなくなります。

また、コントローラのリソース利用率を監視してバランスを調整する自動ロードバランシングも無効になります。

手順

1. メニューを選択します。[設定][システム]。
2. 下にスクロールして「* Additional Settings 」(その他の設定)を表示し、「* Enable / Disable Host Connectivity Reporting *」(ホスト接続レポートの有効化/無効化

   このオプションが現在有効か無効かを示すテキストがこのオプションの下に表示されます。

   確認ダイアログが開きます。
3. 続行するには、 [はい] をクリックします。

   このオプションを選択すると、機能の有効と無効を切り替えることができます。

自動ロードバランシングを設定する

自動ロードバランシング*機能を使用すると、ホストからの受信I/Oトラフィックが動的に管理され、両方のコントローラに分散されます。この機能はデフォルトで有効になっていますが、System Managerから無効にすることもできます。

このタスクについて

自動ロードバランシングを有効にすると、次の機能が実行されます。

- コントローラのリソース利用率を自動的に監視して負荷を分散します。
- ボリュームのコントローラ所有権が必要に応じて自動的に調整され、ホストとストレージアレイの間のI/O帯域幅が最適化されます。

自動ロードバランシングは、ストレージアレイの状況に応じて無効にすることができます。たとえば、次のような場合です。

- 特定のボリュームのコントローラ所有権については、ワークロードを分散するために自動的に変更されないようにする場合。
- 高度に調整された環境で、コントローラ間の負荷分散が特定の要件を満たすように意図的に設定されている。

手順

1. メニューを選択します。[設定][システム]。
2. 下にスクロールして「その他の設定」を選択し、「自動ロードバランシングの有効化/無効化」をクリックします。

   この機能が現在有効か無効かを示すテキストがこのオプションの下に表示されます。

確認ダイアログが開きます。

3. 続行するには、[はい]をクリックして確定します。

このオプションを選択すると、機能の有効と無効を切り替えることができます。

> この機能を無効から有効に切り替えると、ホスト接続レポート機能も自動的に有効になります。

デフォルトのホストタイプを変更

デフォルトのホストオペレーティングシステムの変更設定を使用して、ストレージアレイレベルでデフォルトのホストタイプを変更します。一般に、デフォルトのホストタイプは、ストレージアレイにホストを接続する前、または追加のホストを接続するときに変更します。

このタスクについて

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接続するホストのオペレーティングシステムがすべて同じ場合は（同機種ホスト環境）、オペレーティングシステムに一致するホストタイプに変更します。
- ストレージアレイに接続するホストに異なるオペレーティングシステムのホストが混在している場合は（異機種ホスト環境）、ホストのオペレーティングシステムの大部分に一致するホストタイプに変更します。

  たとえば、8つの異なるホストをストレージアレイに接続し、そのうち6つでWindowsオペレーティングシステムを実行している場合は、Windowsをデフォルトのホストオペレーティングシステムタイプとして選択する必要があります。

- ほとんどの接続ホストでオペレーティングシステムが異なる場合は、ホストタイプを工場出荷時のデフォルトに変更します。

  たとえば、8つの異なるホストをストレージアレイに接続し、そのうち2つのホストがWindowsオペレーティングシステムを実行している場合、3つのホストがHP-UXオペレーティングシステムを実行しています。 さらに、別の3つのOSでLinuxオペレーティングシステムを実行している場合は、デフォルトのホストオペレーティングシステムタイプとしてFactory Defaultを選択する必要があります。

手順

1. メニューを選択します。[設定][システム]。
2. 下にスクロールして「その他の設定」を選択し、「デフォルトのホストOSタイプの変更」をクリックします。
3. デフォルトとして使用するホストオペレーティングシステムのタイプを選択します。
4. [変更（ Change ）] をクリックします。

従来の管理インターフェイスを有効または無効にします

ストレージアレイと管理クライアントの間の通信方法である、従来の管理インターフェイス（SYMbol）を有効または無効にすることができます。デフォルトでは、従来の管理

インターフェイスは有効になっています。無効にすると、ストレージアレイと管理クライアントはより安全な通信方法（REST API over https）を使用しますが、無効にした場合、特定のツールやタスクに影響する可能性があります。

このタスクについて

この設定は処理に次のように影響します。

- * on *（デフォルト）--ミラーリング、E5700およびE5600ストレージアレイのみで動作するCLIコマンド、およびQuickConnectユーティリティやOCIアダプタなどのその他のツールに必要な設定です。
- オフ--ストレージアレイと管理クライアント間の通信の機密性を強化し、外部ツールにアクセスするために必要な設定です。ディレクトリサーバ（LDAP）を設定する際に推奨される設定です。

手順

1. メニューを選択します。[設定][システム]。
2. 下にスクロールして「その他の設定」を選択し、「*管理インターフェイスの変更」をクリックします。
3. ダイアログボックスで、*はい*をクリックして続行します。

よくある質問です

コントローラキャッシュとは何ですか？

コントローラキャッシュは、コントローラとホストの間、およびコントローラとディスクの間の2種類のI/O（入出力）処理をスムーズに行うための物理メモリスペースです。

読み取りおよび書き込みのデータ転送では、ホストとコントローラは高速な接続を介して通信します。ただし、ディスクは比較的低速なデバイスであるため、コントローラのバックエンドからディスクへの通信は低速になります。

コントローラキャッシュがデータを受信すると、コントローラはデータを保持していることをホストアプリケーションに通知します。これにより、ホストアプリケーションはI/Oがディスクに書き込まれるのを待たずに代わりに、アプリケーションは処理を続行できます。また、サーバアプリケーションはキャッシュされたデータにアクセスできるため、データにアクセスするためにディスクを読み取る必要がなくなります。

コントローラキャッシュは、ストレージアレイの全体的なパフォーマンスに次のように影響します。

- キャッシュはバッファとして機能するため、ホストとディスクのデータ転送を同期する必要がありません。
- ホストからの読み取り/書き込み処理の対象となるデータが以前の処理ですでにキャッシュに格納されていれば、ディスクにアクセスする必要はありません。
- 書き込みキャッシュを使用している場合、ホストは以前の書き込み処理がディスクに書き込まれる前に後続の書き込みコマンドを送信できます。
- キャッシュプリフェッチを有効にすると、シーケンシャルリードアクセスが最適化されます。読み取り処理ではデータがディスクから読み取られるのではなく、キャッシュ内のデータが使用される可能性が高くなります。

データ損失の可能性--バッテリなしの書き込みキャッシュ*オプションを有効にして保護用のユニバーサル電源装置を持たないと、データが失われる可能性があります。また、コントローラのバッテリがない場合に*バッテリなしの書き込みキャッシュ*オプションを有効にすると、データが失われる可能性があります。

キャッシュフラッシュとは何ですか？

キャッシュ内の書き込み前のデータの量が一定のレベルに達すると、コントローラはキャッシュされたデータを定期的にドライブに書き込みます。この書き込みプロセスは「フラッシュ」と呼ばれます。

コントローラは、デマンドベースと経過時間ベースの2つのアルゴリズムを使用してキャッシュをフラッシュします。デマンドベースのアルゴリズムは、キャッシュされたデータの量がキャッシュフラッシュしきい値を下回るまで使用されます。デフォルトでは、キャッシュの80%が使用中になるとフラッシュが開始されます。

System Managerでは、「デマンド・キャッシュ・フラッシュの開始」しきい値を、環境で使用されるI/Oのタイプに最も適した値に設定できます。書き込み操作が主な環境では'新しい書き込み要求をディスクに移動せずにキャッシュで処理できる可能性を高めるために'デマンド・キャッシュ・フラッシュの開始パーセントを高く設定する必要があります割合を高く設定すると、キャッシュフラッシュの回数が減ってキャッシュに残るデータ量が増えるため、キャッシュヒットの可能性が高まります。

I/Oが不規則な（データバーストが発生する）環境では、キャッシュフラッシュを低く設定して、データバースト間でキャッシュが頻繁にフラッシュされるようにします。さまざまな負荷を処理する多様なI/O環境や、負荷のタイプが不明な環境では、このしきい値を中間の50%に設定します。80%未満に設定した場合、ホスト読み取りに必要なデータがキャッシュにないためにパフォーマンスが低下する可能性があります。また、割合を低くすると、キャッシュレベルを維持するために必要なディスクへの書き込み回数が増えるため、システムオーバーヘッドが増大します。

経過時間ベースのアルゴリズムでは、書き込みデータがディスクにフラッシュされるまでのキャッシュでの保持期間を指定します。キャッシュフラッシュしきい値に達するまでは、経過時間ベースのアルゴリズムが使用されます。デフォルトは10秒ですが、カウントされるのは非アクティブな期間のみです。System Managerではフラッシュのタイミングを変更できません。代わりに、コマンドラインインターフェイス（CLI）でSet Storage Arrayコマンドを使用する必要があります。

データ損失の可能性--バッテリなしの書き込みキャッシュ*オプションを有効にして保護用のユニバーサル電源装置を持たないと、データが失われる可能性があります。また、コントローラのバッテリがない場合に*バッテリなしの書き込みキャッシュ*オプションを有効にすると、データが失われる可能性があります。

キャッシュブロックサイズとは何ですか？

ストレージアレイのコントローラはキャッシュを複数の「ブロック」に編成します。ブロックは、サイズが4KiB、8KiB、16KiB、または32KiBのメモリチャンクです。ストレージシステムのボリュームはすべて同じキャッシュスペースを共有するため、ボリュームで使用できるキャッシュブロックサイズは1つだけです。

キャッシュブロックは、ディスクの論理ブロックシステムで使用される512バイトブロックとは異なります。

使用するブロックサイズはアプリケーションによって異なり、ストレージのパフォーマンスに影響する可能性

があります。System Managerのデフォルトのブロックサイズは8KiBですが、4KiB、8KiB、16KiB、または32KiBに設定できます。ファイルシステムやデータベースアプリケーションには小さいサイズが適しています。大容量のデータ転送、シーケンシャルI/O、マルチメディアなどの広帯域幅を必要とするアプリケーションには、大きいサイズが適しています。

ストレージアレイのクロックを同期する必要があるのはいつですか？

System Managerと管理クライアント（ブラウザ経由でSystem Managerにアクセスするコンピュータ）で表示されるタイムスタンプが異なる場合は、ストレージアレイのコントローラクロックを手動で同期する必要があります。このタスクが必要になるのは、System ManagerでNTP（ネットワークタイムプロトコル）が有効になっていない場合だけです。

クロックを手動で同期する代わりに、NTPサーバを使用することを強く推奨します。NTPは、SNTP（Simple Network Time Protocol）を使用して自動的にクロックを外部サーバと同期します。

同期ステータスは、システムページから入手できる*ストレージアレイクロックの同期*ダイアログボックスで確認できます。ダイアログボックスに表示された時間が一致しない場合は、同期を実行します。このダイアログボックスを定期的に表示することで、コントローラクロックの時間表示が同期されているかどうかを確認できます。

ホスト接続レポートとは何ですか？

ホスト接続レポートを有効にすると、ストレージアレイはコントローラと設定されたホスト間の接続を継続的に監視し、接続が中断された場合に警告します。

ケーブルに緩み、損傷、脱落が生じた場合や、ホストに問題が生じた場合は、接続の中断が発生する可能性があります。これらの状況では、Recovery Guruメッセージが発行されることがあります。

- ホストの冗長性が失われました--どちらかのコントローラがホストと通信できない場合に開きます
- ホストタイプが正しくありません--ストレージアレイでホストタイプが正しく指定されていないと'フェイルオーバーの問題が発生する可能性があります

コントローラのリブートにかかる時間が接続タイムアウトよりも長くなる可能性がある場合は、ホスト接続レポートを無効にすることができます。この機能を無効にすると、Recovery Guruメッセージが生成されなくなります。

また、コントローラのリソース使用量を監視してバランスを調整する自動ロードバランシングも無効になります。ただし、ホスト接続レポートを再度有効にしても、自動ロードバランシング機能は自動的には有効になりません。

iSCSI 設定

概念

iSCSIの用語

ストレージアレイに関連するiSCSIの用語を次に示します。

期間	説明
CHAP	チャレンジハンドシェイク認証プロトコル（CHAP）方式では、初回のリンク確立時にターゲットとイニシエータのIDを検証します。認証は、CHAP_secret__という共有セキュリティキーに基づいて行われます。
コントローラ	コントローラは、ボード、ファームウェア、ソフトウェアで構成されます。ドライブを制御し、 System Manager の機能を実装します。
DHCP	動的ホスト構成プロトコル（DHCP）は、インターネットプロトコル（IP）ネットワークでIPアドレスなどのネットワーク設定パラメータを動的に配布するために使用されるプロトコルです。
IB	InfiniBand （ IB ）は、ハイパフォーマンスのサーバとストレージシステムの間のデータ転送用の通信標準です。
ICMP PING応答	Internet Control Message Protocol（ICMP）は、ネットワークに接続されたコンピュータのオペレーティングシステムでメッセージの送信に使用されるプロトコルです。ICMPメッセージを送信することで、ホストに到達できるかどうかや、そのホストとのパケットの送受信にどれくらいの時間がかかるかが確認されます。
IQN	iSCSI Qualified Name（IQN）は、iSCSIイニシエータまたはiSCSIターゲットの一意の名前です。
iSER	iSCSI Extensions for RDMA（iSER）は、InfiniBandやイーサネットなどのRDMAトランスポートを使用する処理用にiSCSIプロトコルを拡張したプロトコルです。
iSNS	Internet Storage Name Service（iSNS）は、TCP / IPネットワーク上のiSCSIデバイスとFibre Channelデバイスの自動検出、管理、構成が可能なプロトコルです。
MAC アドレス	メディアアクセス制御（MAC）アドレスはイーサネットで使用される識別子で、同じ物理トランスポートネットワークインターフェイス上の2つのポートを接続する別々の論理チャネルを区別します。
管理クライアント	管理クライアントは、System Managerにアクセスするためのブラウザがインストールされたコンピュータです。
MTU	Maximum Transmission Unit（MTU；最大転送単位）は、ネットワークで送信可能なパケットまたはフレームの最大サイズです。
RDMA	Remote Direct Memory Access（RDMA）は、ネットワークコンピュータ同士が、それぞれのオペレーティングシステムを介さずにメインメモリ内でデータを交換できるテクノロジです。

期間	説明
名前のない検出セッション	名前のない検出セッションのオプションが有効な場合、iSCSIイニシエータは、コントローラの情報を取得するためにターゲットIQNを指定する必要はありません。

方法

iSCSIポートを設定

コントローラにiSCSIホスト接続が搭載されている場合は、ハードウェアページまたはシステムページからiSCSIポートを設定できます。

作業を開始する前に

- コントローラにiSCSIポートが搭載されている必要があります。そうでない場合、iSCSI設定は使用できません。
- ネットワーク速度（ポートとホストの間のデータ転送率）を把握しておく必要があります。

このタスクについて

このタスクでは、ハードウェアページから iSCSI ポート設定にアクセスする方法について説明します。システムページ（メニュー：設定[システム]）から設定にアクセスすることもできます。

iSCSIの設定および機能は、ストレージアレイでiSCSIがサポートされている場合にのみ表示されます。

手順

1. 「 * ハードウェア * 」を選択します。
2. 図にドライブが表示されている場合は、 * シェルフの背面を表示 * をクリックします。

   図の表示が切り替わり、ドライブではなくコントローラが表示されます。
3. iSCSI ポートを設定するコントローラをクリックします。

   コントローラのコンテキストメニューが表示されます。
4. Configure iSCSI Port* （ iSCSI ポートの設定）を選択します。

   Configure iSCSI Ports *オプションは、System ManagerがコントローラでiSCSIポートを検出した場合にのみ表示されます。

   Configure iSCSI Ports （ iSCSI ポートの設定）ダイアログボックスが開きます。
5. ドロップダウンリストで、設定するポートを選択し、 * Next * をクリックします。
6. 構成ポートの設定を選択し、 * 次へ * をクリックします。

   すべてのポート設定を表示するには、ダイアログボックスの右側にある[詳細ポート設定を表示]リンクをクリックします。

フィールドの詳細

ポートの設定	説明
IPv4 を有効にする / IPv6 を有効にする	一方または両方のオプションを選択して、 IPv4 ネットワークと IPv6 ネットワークのサポートを有効にします。メモ：ポートへのアクセスを無効にする場合は、両方のチェックボックスをオフにします。
TCPリスニングポート（Show more port settingsをクリックすると使用可能）	必要に応じて、新しいポート番号を入力します。 リスニングポートは、コントローラがホスト iSCSI イニシエータからの iSCSI ログインをリスンするために使用する TCP ポート番号です。デフォルトのリスニングポートは 3260 です。3260 、または 49152~65535 の値を入力する必要があります。
MTUサイズ（Show more port settingsをクリックして使用可能）	必要に応じて、 Maximum Transmission Unit （ MTU ；最大伝送ユニット）の新しいサイズをバイト単位で入力します。 デフォルトの Maximum Transmission Unit （ MTU ；最大転送単位）サイズは 1500 バイト / フレームです。1500~9000 の値を入力する必要があります。
ICMP PING 応答を有効にします	Internet Control Message Protocol （ ICMP ）を有効にする場合は、このオプションを選択します。ネットワーク接続されたコンピュータのオペレーティングシステムは、このプロトコルを使用してメッセージを送信します。ICMP メッセージを送信することで、ホストに到達できるかどうかや、そのホストとのパケットの送受信にどれくらいの時間がかかるかが確認されます。

IPv4を有効にするを選択した場合は、次へをクリックするとIPv4設定を選択するダイアログボックスが開きます。IPv6を有効にするを選択した場合は、次へをクリックすると、IPv6設定を選択するためのダイアログボックスが開きます。両方のオプションを選択した場合は、最初にIPv4設定のダイアログボックスが開き、次へをクリックすると、IPv6設定のダイアログボックスが開きます。

7. IPv4 と IPv6 、またはその両方を自動または手動で設定します。すべてのポート設定を表示するには、ダイアログボックスの右側にある * Show more settings * リンクをクリックします。

フィールドの詳細

ポートの設定	説明
自動的に設定を取得します	設定を自動的に取得するには、このオプションを選択します。
静的な設定を手動で指定します	このオプションを選択した場合は、フィールドに静的アドレスを入力します。（必要に応じて、住所をカットアンドペーストしてフィールドに貼り付けることもできます）。 IPv4の場合は、ネットワークのサブネットマスクとゲートウェイも指定します。IPv6 の場合は、ルーティング可能な IP アドレスとルータの IP アドレスも指定します。
VLANサポートを有効にします（[詳細設定を表示]をクリックして使用できます）。	VLAN を有効にしてその ID を入力する場合は、このオプションを選択します。VLAN は、同じスイッチ、同じルータ、またはその両方でサポートされる他の物理 LAN （ローカルエリアネットワーク）および仮想 LAN から物理的に分離されたように動作する論理ネットワークです。
イーサネットの優先順位を有効にする（[詳細設定を表示]をクリックして使用可能）。	ネットワークアクセスの優先度を決定するパラメータを有効にする場合は、このオプションを選択します。スライダを使用して優先度を1（最も低い）から7（最も高い）の間で選択します。 共有 LAN 環境（イーサネットなど）では、多数のステーションがネットワークアクセスで競合する可能性があります。アクセスは先に行われたものから順に処理されます。2 つのステーションが同時にネットワークにアクセスしようとすると、両方のステーションがオフになり、再試行するまで待機します。スイッチイーサネットでは、 1 つのステーションだけがスイッチポートに接続されるため、このプロセスは最小限に抑えられます。

8. [完了] をクリックします。

iSCSI認証を設定

iSCSIネットワークのセキュリティを強化するために、コントローラ（ターゲット）とホスト（イニシエータ）の間に認証を設定できます。System Managerは、チャレンジハンドシェイク認証プロトコル（CHAP）方式を使用します。CHAPは初回のリンク確立時にターゲットとイニシエータのIDを検証します。認証は、CHAP_secret__という共有セキュリティキーに基づいて行われます。

作業を開始する前に

イニシエータ（iSCSIホスト）のCHAPシークレットは、ターゲット（コントローラ）のCHAPシークレットを設定する前でもあとでも設定できます。このタスクの手順を実行する前に、ホストがiSCSI接続を確立するのを待ってから、個々のホストでCHAPシークレットを設定する必要があります。接続が確立されると、iSCSI認証のダイアログボックス（このタスクで説明）にホストのIQN名とCHAPシークレットが表示され、手動で入力する必要はありません。

このタスクについて

次のいずれかの認証方法を選択できます。

- 一方向認証--コントローラがiSCSIホストの識別情報を認証できるようにするには'この設定を使用します(一方向認証)
- 双方向認証--コントローラとiSCSIホストの両方が認証(双方向認証)を実行できるようにするには'この設定を使用しますこの設定は、コントローラがiSCSIホストの識別情報を認証できるようにし、さらにiSCSIホストがコントローラの識別情報を認証できるようにすることで、二次的なセキュリティを提供します。

iSCSIの設定と機能は、ストレージアレイがiSCSIをサポートしている場合にのみ、設定ページに表示されます。

手順

1. メニューを選択します。[設定][システム]。
2. [* iSCSI settings]で、[Configure Authentication*]をクリックします。

   Configure Authentication（認証の設定）ダイアログボックスが表示され、現在設定されている方式が示されます。CHAPシークレットが設定されているホストがあるかどうかも表示されます。

3. 次のいずれかを選択します。
   - 認証なし--コントローラがiSCSIホストのIDを認証しないようにするには'このオプションを選択して'完了*をクリックしますダイアログボックスが閉じ、設定が完了します。
   - 一方向認証--コントローラがiSCSIホストのIDを認証できるようにするには'このオプションを選択して'次へをクリックします*ターゲットCHAPの構成ダイアログ・ボックスを表示します
   - 双方向認証--コントローラとiSCSIホストの両方が認証を実行できるようにするには'このオプションを選択して'次へ*をクリックし'ターゲットCHAPの構成ダイアログ・ボックスを表示します
4. 一方向認証または双方向認証について、コントローラ（ターゲット）のCHAPシークレットを入力または確認します。CHAPシークレットは、12~57文字の印刷可能なASCII文字で指定する必要があります。

   コントローラのCHAPシークレットがすでに設定されている場合は、フィールド内の文字は表示されません。必要に応じて、既存の文字を置き換えることができます（新しい文字はマスクされません）。

5. 次のいずれかを実行します。
   - 一方向認証を設定する場合は、*完了*をクリックします。ダイアログボックスが閉じ、設定が完了します。
   - _2Way _authenticationを設定する場合は、* Next *をクリックしてConfigure Initiator CHAPダイアログボックスを表示します。
6. 双方向認証について、任意のiSCSIホスト（イニシエータ）のCHAPシークレット（12~57文字の印刷可能

なASCII文字）を入力または確認します。特定のホストに双方向認証を設定しない場合は、「* Initiator CHAP Secret *」フィールドを空白のままにします。

ホストのCHAPシークレットがすでに設定されている場合は、フィールド内の文字は表示されません。必要に応じて、既存の文字を置き換えることができます（新しい文字はマスクされません）。

7. [完了] をクリックします。

結果

認証なしを指定した場合を除き、iSCSIログインシーケンス中にコントローラとiSCSIホストの間で認証が行われます。

iSCSI検出設定を有効にします

iSCSIネットワーク内のストレージデバイスの検出に関連する設定を有効にすることができます。ターゲット検出設定では、Internet Storage Name Service（iSNS）プロトコルを使用してストレージアレイのiSCSI情報を登録し、名前のない検出セッションを許可するかどうかを設定できます

作業を開始する前に

iSNSサーバで静的IPアドレスが使用されている場合は、そのアドレスをiSNSの登録に使用できる必要があります。IPv4とIPv6の両方がサポートされています。

このタスクについて

iSCSI検出に関連する次の設定を有効にすることができます。

- * iSNSサーバによるターゲットの登録を有効にする*--有効にすると'ストレージ・アレイはiSNSサーバからiSCSI Qualified Name（IQN）とポート情報を登録しますこの設定は、イニシエータがiSNSサーバからIQNとポート情報を取得できるように、iSNS検出を許可します。
- 名前のない検出セッションを有効にする--名前のない検出セッションを有効にすると'イニシエータ（iSCSIホスト）は'検出タイプ接続のログインシーケンス中にターゲットのIQN（コントローラ）を指定する必要はありません無効な場合、ホストはIQNを指定してコントローラへの検出セッションを確立する必要があります。ただし、通常の（I/Oベアリング）セッションでは常にターゲットIQNが必要です。この設定を無効にすると、権限のないiSCSIホストがIPアドレスのみを使用してコントローラに接続することを防止できます。

iSCSIの設定と機能は、ストレージアレイがiSCSIをサポートしている場合にのみ、設定ページに表示されます。

手順

1. メニューを選択します。[設定][システム]。
2. [* iSCSI settings]で、[*ターゲット検出設定の表示/編集]をクリックします。

   [* Target Discovery Settings*（ターゲット検出設定*）]ダイアログボックスが表示されます。[Enable iSNS server…]フィールドの下に、コントローラがすでに登録されているかどうかを示すダイアログボックスが表示されます。

3. コントローラを登録するには、[iSNSサーバーを有効にしてターゲットを登録する*]を選択し、次のいずれ

かを選択します。

- * DHCPサーバから自動的に設定を取得*--動的ホスト構成プロトコル(DHCP)サーバを使用してiSNSサーバを設定する場合は'このオプションを選択しますこのオプションを使用する場合は、コントローラのすべてのiSCSIポートでDHCPを使用するように設定する必要があります。必要に応じて、コントローラのiSCSIポートの設定を更新して、このオプションを有効にします。

> DHCPサーバでiSNSサーバのアドレスを指定するには、オプション43の「ベンダー固有の情報」を使用するようにDHCPサーバを設定する必要があります。 このオプションでは、iSNSサーバのIPv4アドレスをデータバイト0xa-0xd（10-13）に含める必要があります。

- 静的な設定を手動で指定-- iSNSサーバの静的IPアドレスを入力する場合は'このオプションを選択します（必要に応じて、住所をカットアンドペーストしてフィールドに貼り付けることもできます）。 フィールドに、IPv4アドレスまたはIPv6アドレスを入力します。両方を設定した場合は、IPv4がデフォルトです。また、TCPリスニングポートを入力します（デフォルトの3205を使用するか、49152~65535の値を入力）。

4. ストレージアレイを名前のない検出セッションの対象にするには、*名前のない検出セッションを有効にする*を選択します。
   - 有効にすると、iSCSIイニシエータは、コントローラの情報を取得するためにターゲットIQNを指定する必要はありません。
   - 無効にすると、イニシエータがターゲットIQNを指定しないかぎり、検出セッションは実行されません。名前のない検出セッションを無効にすると、セキュリティが向上します。
5. [保存（ Save ）] をクリックします。

結果

System Managerがコントローラをi SNSサーバに登録しようとする間、進捗状況バーが表示されます。この処理には最大5分かかることがあります。

iSCSI統計パッケージを表示します

ストレージアレイへのiSCSI接続に関するデータを表示できます。

このタスクについて

System Managerには、次のタイプのiSCSI統計が表示されます。統計はすべて読み取り専用で、設定することはできません。

- イーサネット**MAC**統計--メディアアクセス制御(MAC)の統計情報を提供します。MACは、物理アドレスまたはMACアドレスと呼ばれるアドレス指定メカニズムも提供します。MACアドレスは、各ネットワークアダプタに割り当てられている一意のアドレスです。MACアドレスは、サブネットワーク内のデスティネーションへのデータパケットの配信に役立ちます。
- イーサネット**TCP/IP**統計-- iSCSIデバイスのTCP (Transmission Control Protocol)とIP (Internet Protocol)のTCP/IPの統計情報を提供しますTCPを使用すると、ネットワークホスト上のアプリケーションが相互に接続を作成し、パケットでデータを交換できます。IPは、パケット交換インターネットワークを介してデータを通信するデータ指向プロトコルです。IPv4統計とIPv6統計は個別に表示されます。
- ローカル・ターゲット/イニシエータ（プロトコル）統計：ストレージ・メディアへのブロック・レベルのアクセスを提供するiSCSIターゲットの統計情報を表示します非同期ミラーリング処理でイニシエータとして使用される場合は'ストレージ・アレイのiSCSI統計情報を表示します
- **DCBX**の運用状態統計--さまざまなData Center Bridging Exchange（DCBX）機能の運用状態を表示しま

す。

- *LLDP TLV statistics *-- Link Layer Discovery Protocol (LLDP) Type Length Value (TLTLV)統計を表示します。
- **DCBX TLV**統計-- Data Center Bridging（DCB）環境内のストレージアレイのホストポートを識別する情報が表示されます。この情報は、識別や機能のためにネットワークピアと共有されます。

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

手順

1. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
2. [View iSCSI Statistics Packages]を選択します。
3. タブをクリックして、さまざまな統計を表示します。
4. ベースラインを設定するには、*新しいベースラインを設定*をクリックします。

   ベースラインを設定すると、統計を収集するための新しい開始ポイントが設定されます。すべてのiSCSI統計に同じベースラインが使用されます。

iSCSIセッションを終了します

不要になったiSCSIセッションを終了できます。iSCSIセッションは、非同期ミラー関係にあるホストまたはリモートストレージアレイとの間で確立できます。

このタスクについて

iSCSIセッションを終了する理由としては、次のようなものが考えられます。

- 不正アクセス-- iSCSIイニシエータがログオンされていて、アクセスできない場合は、iSCSIセッションを終了して、iSCSIイニシエータをストレージアレイから強制的に切断できます。認証方法を「なし」にしたため、iSCSIイニシエータがログオンした可能性があります。
- システムダウンタイム--ストレージアレイを停止する必要があり'iSCSIイニシエータがまだログオンしている場合は'iSCSIセッションを終了してiSCSIイニシエータをストレージアレイから切断できます

手順

1. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
2. 「* iSCSIセッションの表示/終了*」を選択します。

   現在のiSCSIセッションのリストが表示されます。

3. 終了するセッションを選択します
4. [セッションの終了]をクリックし、操作を実行することを確認します。

iSCSI セッションを表示します

ストレージアレイへのiSCSI接続に関する詳細情報を表示できます。iSCSIセッションは、非同期ミラー関係にあるホストまたはリモートストレージアレイとの間で確立でき

ます。

手順

1. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
2. 「* iSCSIセッションの表示/終了*」を選択します。

   現在のiSCSIセッションのリストが表示されます。

3. 特定のiSCSIセッションに関する追加情報 を表示するには、セッションを選択し、*詳細の表示*をクリックします。

フィールドの詳細

項目	説明
セッション識別子（SSID）	iSCSIイニシエータとiSCSIターゲット間のセッションを識別する16進数の文字列。SSIDは、ISIDとTPGTで構成されます。
イニシエータセッションID（ISID）	セッション識別子のイニシエータの部分。イニシエータはログイン時にISIDを指定します。
ターゲットポータルグループ	iSCSIターゲット。
ターゲットポータルグループタグ（TPGT）	セッション識別子のターゲットの部分。iSCSIターゲットポータルグループの16ビットの数値識別子。
イニシエータのiSCSI名	世界規模で一意なイニシエータの名前。
イニシエータのiSCSIラベル	System Managerで設定されたユーザラベル。
イニシエータのiSCSIエイリアス	iSCSIノードにも関連付けることができる名前。エイリアスを使用すると、組織がユーザにわかりやすい文字列をiSCSI名に関連付けることができます。ただし、エイリアスはiSCSI名に代わるものではありません。イニシエータのiSCSIエイリアスは、System Managerではなく、ホストでのみ設定できます
ホスト	ストレージアレイに入出力を送信するサーバ。
接続ID（CID）	イニシエータとターゲット間のセッション内における接続の一意の名前。イニシエータがこのIDを生成し、ログイン要求の際にターゲットに提供します。接続IDは、接続を閉じるログアウト時にも表示されます。
イーサネットポート識別子	接続に関連付けられているコントローラポート。
イニシエータのIPアドレス	イニシエータのIPアドレス。
ネゴシエーション済みのログインパラメータ	iSCSIセッションのログイン時に処理されるパラメータ。
認証方式	iSCSIネットワークへのアクセスを必要とするユーザを認証する手法。有効な値は* chap および None *です。

項目	説明
ヘッダーダイジェスト方式	iSCSIセッションに有効なヘッダー値を表示する手法。HeaderDigestおよびDataDigestには、* None または CRC32C を使用できます。両方のデフォルト値は None *です。
データダイジェスト方式	iSCSIセッションに有効なデータ値を表示する手法。HeaderDigestおよびDataDigestには、* None または CRC32C を使用できます。両方のデフォルト値は None *です。
最大接続数	iSCSIセッションに許可される接続の最大数。1~4を接続の最大数として指定できます。デフォルト値は* 1 *です。
ターゲットエイリアス	ターゲットに関連付けられているラベル。
イニシエータのエイリアス	イニシエータに関連付けられているラベル。
ターゲットのIPアドレス	iSCSIセッションのターゲットのIPアドレス。DNS名はサポートされません。
初期R2T	最初の転送準備完了ステータス。ステータスは「* Yes 」または「 No *」のいずれかになります。
最大バースト長	このiSCSIセッションの最大SCSIペイロード（バイト）。512~262、144（256KB）を最大バースト長として指定できます。デフォルト値は* 262,144（256KB）*です。
第1バースト長	このiSCSIセッションの未承諾データのSCSIペイロード（バイト単位）。512~131、072（128KB）を第1バースト長として指定できます。デフォルト値は*65,536（64KB）*です。
デフォルトの待機時間	接続の終了または接続のリセット後に接続を試行するまでの最小秒数。0~3600をデフォルトの待機時間の値として指定できます。デフォルトは* 2 *です。
デフォルトの保持時間です	接続の終了または接続のリセット後も接続が可能な最大秒数。0~3600をデフォルトの保持時間として指定できます。デフォルト値は*20*です。
最大未処理R2T	このiSCSIセッションの未処理の「準備が完了した転送」の最大数。1~16を未処理の「準備が完了した転送」の最大値として指定できます。デフォルトは* 1 *です。
エラーリカバリレベル	このiSCSIセッションのエラーリカバリのレベル。エラーリカバリレベルの値は常に* 0 *に設定されています。

項目	説明
受信データ最大セグメント長	イニシエータまたはターゲットがペイロードデータユニット（PDU）で受信できる最大データ量。
ターゲット名	ターゲットの正式名（エイリアスではありません）。iqn形式のターゲット名です。
イニシエータ名	イニシエータの正式名（エイリアスではありません）。iqn形式または_eui_formatを使用するイニシエータ名です。

4. レポートをファイルに保存するには、*保存*をクリックします。

   ブラウザのDownloadsフォルダに'iscsi-session-connections.txt'というファイル名でファイルが保存されます

iSER over InfiniBandポートを設定します

コントローラにiSER over InfiniBandポートが搭載されている場合は、ホストとのネットワーク接続を設定できます。構成設定は、[ハードウェア]ページまたは[システム]ページから使用できます。

作業を開始する前に

- コントローラにiSER over InfiniBandポートが搭載されている必要があります。そうでないと、System ManagerでiSER over InfiniBand設定を使用できません。
- ホスト接続のIPアドレスを確認しておく必要があります。

このタスクについて

iSER over InfiniBand構成には、* Hardware ページまたはメニューからアクセスできます：**Settings [System]**。このタスクでは、**[*Hardware**]ページからポートを設定する方法について説明します。

> iSER over InfiniBandの設定と機能は、ストレージアレイのコントローラにiSER over InfiniBandポートが搭載されている場合にのみ表示されます。

手順

1. 「 * ハードウェア * 」を選択します。
2. 図にドライブが表示されている場合は、 * シェルフの背面を表示 * をクリックします。

   図の表示が切り替わり、ドライブではなくコントローラが表示されます。

3. iSER over InfiniBandポートを設定するコントローラをクリックします。

   コントローラのコンテキストメニューが表示されます。

4. iSER over InfiniBandポートの設定*を選択します。

   Configure iSER over InfiniBand ports（iSER over InfiniBandポートの設定）ダイアログボックスが開きま

す。

5. ドロップダウンリストで設定するHICポートを選択し、ホストのIPアドレスを入力します。
6. [**Configure**] をクリックします。
7. 設定を完了したら、* Yes *をクリックしてiSER over InfiniBandポートをリセットします。

iSER over InfiniBandの統計を表示します

ストレージアレイのコントローラにiSER over InfiniBandポートが搭載されている場合は、ホスト接続に関するデータを表示できます。

このタスクについて

System Managerには、次のタイプのiSER over InfiniBand統計が表示されます。統計はすべて読み取り専用で、設定することはできません。

- ローカルターゲット（プロトコル）統計- iSER over InfiniBandターゲットの統計を提供し、ストレージメディアへのブロックレベルのアクセスが表示されます。
- * iSER over InfiniBandインターフェイス統計*- InfiniBandインターフェイス上のすべてのiSERポートの統計が提供され、各スイッチポートに関連付けられているパフォーマンス統計とリンクエラー情報が含まれます。

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

iSER over InfiniBand統計には、System（システム）ページ（メニュー：Settings（システム））またはSupport（サポート）ページからアクセスできます。ここでは、Supportページから統計情報にアクセスする方法について説明します。

手順

1. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
2. View iSER over InfiniBand Statistics *を選択します。
3. タブをクリックして、さまざまな統計を表示します。
4. ベースラインを設定するには、*新しいベースラインを設定*をクリックします。

   ベースラインを設定すると、統計を収集するための新しい開始ポイントが設定されます。すべてのiSER over InfiniBand統計に同じベースラインが使用されます。

よくある質問です

iSNSサーバを登録に使用するとどうなりますか？

Internet Storage Name Service（iSNS）サーバの情報を使用する場合は、iSNSサーバを照会してターゲット（コントローラ）から情報を取得するようにホスト（イニシエータ）を設定できます。

この登録により、コントローラのiSCSI Qualified Name（IQN）とポート情報がiSNSサーバに提供され、イニシエータ（iSCSIホスト）とターゲット（コントローラ）間の照会が可能になります。

iSCSIではどの登録方法が自動的にサポートされますか。

iSCSIの実装では、Internet Storage Name Service（iSNS）検出方式またはSend Targetsコマンドの使用がサポートされます。

iSNS方式では、イニシエータ（iSCSIホスト）とターゲット（コントローラ）の間でiSNS検出を実行できます。ターゲットコントローラを登録して、コントローラのiSCSI修飾名（IQN）とポート情報をiSNSサーバに提供します。

iSNSを設定しない場合、iSCSIホストはiSCSI検出セッション中にSend Targetsコマンドを送信します。これに応答して、コントローラからポート情報（ターゲットIQN、ポートIPアドレス、リスニングポート、ターゲットポートグループなど）が返されます。iSNSを使用する場合は、ホストイニシエータがiSNSサーバからターゲットIPを取得できるため、この検出方式は必要ありません。

iSER over InfiniBand統計には何が表示されますか？

View iSER over InfiniBand Statistics *ダイアログボックスには、ローカルターゲット（プロトコル）統計とiSER over InfiniBand（IB）インターフェイス統計が表示されます。統計はすべて読み取り専用で、設定することはできません。

- ローカルターゲット（プロトコル）統計- iSER over InfiniBandターゲットの統計を提供し、ストレージメディアへのブロックレベルのアクセスが表示されます。
- * iSER over InfiniBandインターフェイス統計*- InfiniBandインターフェイス上のすべてのiSER over InfiniBandポートの統計が提供され、各スイッチポートに関連付けられているパフォーマンス統計とリンクエラー情報が含まれます。

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

iSER over InfiniBandを設定または診断するためにほかに必要な作業は何ですか？

次の表に、iSER over InfiniBandセッションの設定と管理に使用するSystem Managerの機能を示します。

> iSER over InfiniBandを設定できるのは、ストレージアレイのコントローラにiSER over InfiniBandホスト管理ポートが搭載されている場合のみです。

iSER over InfiniBandを設定して診断します

アクション	場所
iSER over InfiniBandポートを設定します	1. 「 * ハードウェア * 」を選択します。 2. Show back of shelf*を選択します。 3. コントローラを選択します。 4. iSER over InfiniBandポートの設定*を選択します。 または 1. メニューを選択します。[設定][システム]。 2. 下にスクロールして* iSER over InfiniBand setting*を選択し、* iSER over InfiniBandポートの設定*を選択します。
iSER over InfiniBandの統計を表示します	1. メニューを選択します。[設定][システム]。 2. 下にスクロールして* iSER over InfiniBand settings を表示し、 View iSER over InfiniBand Statistics *を選択します。

システム：**NVMe**設定

概念

NVMe の概要

一部のコントローラには、NVMe（Non-Volatile Memory Express）over InfiniBandファブリックまたはNVMe over RoCE（RDMA over Converged Ethernet）ファブリックを実装するためのポートが搭載されています。NVMeを使用すると、ホストとストレージアレイの間でハイパフォーマンスな通信が可能になります。

NVMeとは

*NVM _*は「不揮発性メモリ」を表し、多くのタイプのストレージデバイスで使用されている永続的メモリです。*_NVM*（NVM Express）は、NVMデバイスとのハイパフォーマンスなマルチキュー通信に特化して設計された、標準インターフェイスまたはプロトコルです。

NVMe over Fabricsとは

_NVMe over Fabrics（NVMe-oF）_は、NVMeメッセージベースのコマンドおよびデータをホストコンピュータとストレージの間でネットワーク経由で転送できるようにするテクノロジ仕様です。SANtricity OS 11.40リリース以降では、NVMeストレージアレイ（a_subsystem _）に、InfiniBandファブリックまたはRDMAファブリックを使用するホストからアクセスできます。NVMeコマンドは、ホスト側とサブシステム側の両方のトランスポート抽象化レイヤで有効化され、カプセル化されます。これにより、ハイパフォーマンスなNVMeインターフェイスのエンドツーエンドがホストからストレージへ拡張され、コマンドセットが標準化、簡易化されます。

NVMe-oFストレージは、ローカルのブロックストレージデバイスとしてホストに提示されます。ボリューム（a_namespac_）は、他のブロックストレージデバイスと同様にファイルシステムにマウントできます。必要に応じて、REST API、SMcli、またはSANtricity System Managerを使用してストレージをプロビジョニン

グできます。

NVMe Qualified Name（NQN）とは

NVMe Qualified Name（NQN）は、リモートストレージターゲットを識別するために使用します。ストレージアレイのNVMe Qualified Nameは常にサブシステムによって割り当てられ、変更はできません。NVMe Qualified Nameはアレイ全体で1つです。NVMe Qualified Nameは最大223文字です。iSCSI Qualified Nameと比較してみてください。

ネームスペースおよびネームスペースIDとは何ですか。

ネームスペースはSCSIの論理ユニットに相当し、アレイ内のボリュームに関連付けられています。ネームスペースID（NSID）は、SCSIの論理ユニット番号（LUN）に相当します。NSIDはネームスペースの作成時に作成し、1~255の値を設定できます。

NVMeコントローラとは

ホストのイニシエータからストレージシステムのターゲットへのパスを表すSCSI I_T Nexusと同様に、ホスト接続プロセスで作成されるNVMeコントローラは、ストレージアレイ内のネームスペースとホストの間のアクセスパスを提供します。NVMeコントローラはホストのNQNとホストポート識別子によって一意に識別されます。NVMeコントローラを関連付けることができるのは単一のホストのみですが、NVMeコントローラは複数のネームスペースにアクセスできます。

SANtricity System Managerを使用して、どのホストがどのネームスペースにアクセスできるかを設定し、ホストのネームスペースIDを設定します。その後、NVMeコントローラが作成されると、NVMeコントローラからアクセス可能なネームスペースIDのリストが作成され、許可される接続の設定に使用されます。

NVMeの用語

ストレージアレイに関連するNVMeの用語を次に示します。

期間	説明
InfiniBandの略	InfiniBand （ IB ）は、ハイパフォーマンスのサーバとストレージシステムの間のデータ転送用の通信標準です。
ネームスペース	ネームスペースは、ブロックアクセス用にフォーマットされたNVMストレージです。SCSIの論理ユニットに相当し、ストレージアレイではボリュームに関連します。
ネームスペースID	ネームスペースIDは、NVMeコントローラのネームスペースの一意の識別子です。1~255の値を設定できます。SCSIの論理ユニット番号（LUN）に相当します。
NQN	NVMe Qualified Name（NQN）は、リモートストレージターゲット（ストレージアレイ）を識別するために使用します。
NVM	非揮発性メモリ（NVM）は、多くのタイプのストレージデバイスで使用されている永続的メモリです。

期間	説明
NVMe	Non-Volatile Memory Express（NVMe）は、SSDドライブなどのフラッシュベースのストレージデバイス向けに設計されたインターフェイスです。以前の論理デバイスインターフェイスに比べ、I/Oオーバーヘッドが少なく、パフォーマンスも向上しています。
NVMe-oF	Non-Volatile Memory Express over Fabrics（NVMe-oF）は、NVMeコマンドとデータをホストとストレージ間でネットワーク経由で転送するための仕様です。
NVMeコントローラ	NVMeコントローラはホストの接続プロセス中に作成されます。ホストとストレージアレイ内のネームスペースの間のアクセスパスを提供します。
NVMeキューです	NVMeインターフェイス経由でのコマンドやメッセージの受け渡しに使用されるキューです。
NVMe サブシステム	NVMeホストに接続されているストレージアレイです。
RDMA	Remote Direct Memory Access（RDMA）を使用すると、ネットワークインターフェイスカード（NIC）ハードウェアに転送プロトコルを実装することで、サーバとの間でより直接的なデータ移動を実現できます。
RoCE	RDMA over Converged Ethernet （ RoCE ）は、イーサネットネットワークを介したリモートダイレクトメモリアクセス（ RDMA ）を可能にするネットワークプロトコルです。
SSD の場合	ソリッドステートディスク（ SSD ）は、ソリッドステートメモリ（フラッシュ）を使用してデータを永続的に格納するデータストレージデバイスです。SSDは従来のハードドライブをエミュレートしたものであり、ハードドライブと同じインターフェイスで利用できます。

方法

NVMe over InfiniBandポートを設定する

コントローラにNVMe over InfiniBand接続が搭載されている場合は、ハードウェアページまたはシステムページでNVMeポートを設定できます。

作業を開始する前に

- コントローラにNVMe over InfiniBandホストポートが搭載されている必要があります。そうでないと、System ManagerでNVMe over InfiniBand設定を使用できません。
- ホスト接続のIPアドレスを確認しておく必要があります。

このタスクについて

NVMe over InfiniBand構成には、* Hardware ページまたはメニューからアクセスできます：**Settings [System]**。このタスクでは、**[*Hardware**]ページからポートを設定する方法について説明します。

NVMe over InfiniBandの設定と機能は、ストレージアレイのコントローラにNVMe over InfiniBandポートが搭載されている場合にのみ表示されます。

手順

1. 「 * ハードウェア * 」を選択します。
2. 図にドライブが表示されている場合は、 * シェルフの背面を表示 * をクリックします。

   図の表示が切り替わり、ドライブではなくコントローラが表示されます。

3. NVMe over InfiniBandポートを設定するコントローラをクリックします。

   コントローラのコンテキストメニューが表示されます。

4. Configure NVMe over InfiniBand ports] を選択します。

   Configure NVMe over InfiniBand Ports * （ NVMe over InfiniBand ポートの設定 * ）ダイアログボックスが開きます。

5. ドロップダウンリストで設定するHICポートを選択し、ホストのIPアドレスを入力します。
6. [**Configure**] をクリックします。
7. 設定を完了したら、「* Yes」をクリックしてNVMe over InfiniBandポートをリセットします。

NVMe over RoCEポートを設定します

コントローラにNVMe over RoCE（RDMA over Converged Ethernet）用の接続が含まれている場合は、ハードウェアページまたはシステムページからNVMeポートを設定できます。

作業を開始する前に

- コントローラにNVMe over RoCEホストポートが搭載されている必要があります。そうでないと、System ManagerでNVMe over RoCE設定を使用できません。
- ホスト接続のIPアドレスを確認しておく必要があります。

このタスクについて

NVMe over RoCE 構成には、 * Hardware * ページまたはメニューからアクセスできます： Settings [System] 。このタスクでは、 Hardware ページからポートを設定する方法について説明します。

NVMe over RoCE の設定と機能は、ストレージアレイのコントローラに NVMe over RoCE ポートが搭載されている場合にのみ表示されます。

手順

1. 「 * ハードウェア * 」を選択します。
2. 図にドライブが表示されている場合は、 * シェルフの背面を表示 * をクリックします。

   図の表示が切り替わり、ドライブではなくコントローラが表示されます。

3. NVMe over RoCE ポートを設定するコントローラをクリックします。

コントローラのコンテキストメニューが表示されます。

4. NVMe over RoCE ポートの設定 * を選択します。

   Configure NVMe over RoCE Ports（NVMe over RoCEポートの設定）ダイアログボックスが開きます。

5. ドロップダウンリストで、設定するHICポートを選択します。
6. 「 * 次へ * 」をクリックします。

   すべてのポート設定を表示するには、ダイアログボックスの右側にある * Show more port settings * リンクをクリックします。

   フィールドの詳細

ポートの設定	説明
イーサネットポート速度の設定	ポートのSFPの速度と同じ速度を選択します。
IPv4 を有効にする / IPv6 を有効にする	一方または両方のオプションを選択して、 IPv4 ネットワークと IPv6 ネットワークのサポートを有効にします。 ポートへのアクセスを無効にする場合は、両方のチェックボックスを選択解除します。
MTUサイズ（Show more port settingsをクリックして使用可能）	必要に応じて、 Maximum Transmission Unit （ MTU ；最大伝送ユニット）の新しいサイズをバイト単位で入力します。 デフォルトの Maximum Transmission Unit （ MTU ；最大転送単位）サイズは 1500 バイト / フレームです。1500~9000 の値を入力する必要があります。

   IPv4を有効にするを選択した場合は、次へをクリックするとIPv4設定を選択するダイアログボックスが開きます。IPv6を有効にするを選択した場合は、次へをクリックすると、IPv6設定を選択するためのダイアログボックスが開きます。両方のオプションを選択した場合は、最初にIPv4設定のダイアログボックスが開き、次へをクリックすると、IPv6設定のダイアログボックスが開きます。

7. IPv4 と IPv6 、またはその両方を自動または手動で設定します。

フィールドの詳細

ポートの設定	説明
自動的に設定を取得します	設定を自動的に取得するには、このオプションを選択します。
静的な設定を手動で指定します	このオプションを選択した場合は、フィールドに静的アドレスを入力します。（必要に応じて、住所をカットアンドペーストしてフィールドに貼り付けることもできます）。 IPv4の場合は、ネットワークのサブネットマスクとゲートウェイも指定します。IPv6 の場合は、ルーティング可能な IP アドレスとルータの IP アドレスも指定します。

8. [完了] をクリックします。

NVMe over Fabricsの統計を表示します

ストレージアレイへのNVMe over Fabrics接続に関するデータを表示できます。

このタスクについて

System Managerには、次のタイプのNVMe over Fabrics統計が表示されます。統計はすべて読み取り専用で、設定することはできません。

- * nvmeサブシステム統計*--タイムアウトや接続エラーなど、NVMeコントローラの統計が表示されます。
- *rdma Interface statistics *--送受信されたパケット情報を含むRDMAインタフェースの統計情報を提供します。

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

NVMe over Fabrics統計には、システムページ（メニュー：設定[システム]）またはサポートページからアクセスできます。ここでは、Supportページから統計情報にアクセスする方法について説明します。

手順

1. メニューを選択します。Support（サポートセンター）> Diagnostics（診断）タブ。
2. View NVMe over Fabrics Statistics *を選択します。
3. ベースラインを設定するには、*新しいベースラインを設定*をクリックします。

   ベースラインを設定すると、統計を収集するための新しい開始ポイントが設定されます。すべてのNVMe統計に同じベースラインが使用されます。

よくある質問です

NVMe over InfiniBand統計には何が表示されますか？

View NVMe over Fabrics Statistics *ダイアログボックスには、NVMeサブシステムとNVMe over InfiniBandインターフェイスの統計が表示されます。統計はすべて読み取り専用で、設定することはできません。

- * nvmeサブシステム統計*- NVMeコントローラとそのキューの統計が表示されます。NVMeコントローラは、ストレージアレイ内のネームスペースとホストの間のアクセスパスを提供します。NVMeサブシステム統計では、接続障害、リセット、シャットダウンなどの項目を確認できます。これらの統計の詳細については、[表見出しの凡例を表示する*]をクリックしてください。
- * rdma Interface statistics **-- RDMA**インターフェイス上のすべての**NVMe over Fabrics**ポートの統計を提供します。各スイッチポートに関連付けられているパフォーマンス統計とリンクエラー情報が含まれます。統計の詳細については、**[**表見出しの凡例を表示する]をクリックしてください。

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

NVMe over Fabrics統計には何が表示されますか？

View NVMe over Fabrics Statistics *ダイアログボックスには、NVMeサブシステムとNVMe over RoCEインターフェイスの統計が表示されます。統計はすべて読み取り専用で、設定することはできません。

- * nvmeサブシステム統計*- NVMeコントローラとそのキューの統計が表示されます。NVMeコントローラは、ストレージアレイ内のネームスペースとホストの間のアクセスパスを提供します。NVMeサブシステム統計では、接続障害、リセット、シャットダウンなどの項目を確認できます。これらの統計の詳細については、[表見出しの凡例を表示する*]をクリックしてください。
- * rdma Interface statistics **-- RDMA**インターフェイス上のすべての**NVMe over Fabrics**ポートの統計を提供します。各スイッチポートに関連付けられているパフォーマンス統計とリンクエラー情報が含まれます。統計の詳細については、**[**表見出しの凡例を表示する]をクリックしてください。

これらの統計はそれぞれ、統計の生データまたはベースライン統計として表示できます。統計の生データは、コントローラの起動以降に収集されたすべての統計です。ベースライン統計は、ベースライン時間の設定以降に収集されたポイントインタイムの統計です。

NVMe over InfiniBandを設定または診断するためにほかに必要な作業は何ですか？

次の表に、NVMe over InfiniBandセッションの設定と管理に使用するSystem Managerの機能を示します。

NVMe over InfiniBandを設定できるのは、ストレージアレイのコントローラにNVMe over InfiniBandポートが搭載されている場合のみです。

NVMe over InfiniBandを設定して診断します

アクション	場所
NVMe over InfiniBandポートを設定する	1. 「 * ハードウェア * 」を選択します。 2. Show back of shelf*を選択します。 3. コントローラを選択します。 4. Configure NVMe over InfiniBand ports] を選択します。 または 1. メニューを選択します。[設定][システム]。 2. 下にスクロールして* NVMe over InfiniBand settings を表示し、 Configure NVMe over InfiniBand ports *を選択します。
NVMe over InfiniBandの統計を表示します	1. メニューを選択します。[設定][システム]。 2. 下にスクロールして* NVMe over InfiniBand settings を表示し、 View NVMe over Fabrics Statistics *を選択します。

NVMe over RoCEを設定または診断するためにほかに必要な作業は何ですか？

NVMe over RoCEの設定と管理は、ハードウェアと設定のページで実行できます。

NVMe over RoCEを設定できるのは、ストレージアレイのコントローラにNVMe over RoCEポートが搭載されている場合のみです。

NVMe over RoCEを設定して診断します

アクション	場所
NVMe over RoCEポートを設定します	1. 「 * ハードウェア * 」を選択します。 2. Show back of shelf*を選択します。 3. コントローラを選択します。 4. NVMe over RoCE ポートの設定 * を選択します。 または 1. メニューを選択します。[設定][システム]。 2. 下にスクロールして* NVMe over RoCE settings （**NVMe over RoCE**設定）に進み、* Configure NVMe over RoCE Ports （**NVMe over RoCE**ポートの設定）を選択します。
NVMe over Fabricsの統計を表示します	1. メニューを選択します。[設定][システム]。 2. 下にスクロールして* NVMe over RoCE settings を表示し、 View NVMe over Fabrics Statistics *を選択します。

アドオン機能

概念

アドオン機能の仕組み

アドオンは、System Managerの標準構成には含まれていない機能で、有効にするにはキーが必要です。アドオン機能には、単一のプレミアム機能と、バンドルされた機能パックがあります。

以下に、プレミアム機能または機能パックを有効にする手順の概要を示します。

1. 次の情報を入手します。
   - シャーシのシリアル番号と機能有効識別子。機能をインストールするストレージアレイを識別します。これらはSystem Managerにあります。
   - Feature Activation Code。機能購入時にサポートサイトから入手できます。
2. ストレージプロバイダに問い合わせるか、Premium Feature Activationサイトにアクセスして、機能キーを取得します。シャーシのシリアル番号、機能有効識別子、およびFeature Activation Codeを指定します。
3. System Managerで、機能キーファイルを使用してプレミアム機能または機能パックを有効にします。

アドオン機能に関する用語

ストレージアレイに関連するアドオン機能の用語を次に示します。

期間	説明
機能有効識別子	機能有効識別子は、特定のストレージアレイを識別する一意の文字列です。プレミアム機能を取得した場合、この識別子によって機能が特定のストレージアレイにのみ関連付けられます。この文字列は、[システム]ページの[アドオン]の下に表示されます。
機能キーファイル	機能キーファイルは、プレミアム機能や機能パックのロックを解除して有効にするためのファイルです。
機能パック	機能パックは、ストレージアレイの属性を変更する（プロトコルをFibre ChannelからiSCSIに変更するなど）バンドルです。機能パックを有効にするには特別なキーが必要です。
プレミアム機能	プレミアム機能は追加オプションであり、有効にするにはキーが必要です。標準構成のSystem Managerには含まれていません。

方法

機能キーファイルを取得します

ストレージアレイでプレミアム機能または機能パックを有効にするには、まず機能キーファイルを取得する必要があります。キーは1つのストレージアレイにのみ関連付けられます。

このタスクについて

このタスクでは、機能の必要な情報を収集し、機能キーファイルの要求を送信する方法について説明します。必要な情報は次のとおりです。

- シャーシのシリアル番号
- 機能有効識別子
- Feature Activation Code （機能アクティベーションコード）

手順

1. System Managerで、シャーシのシリアル番号を確認して記録します。このシリアル番号は、サポートセンターのタイルにマウスを合わせると表示されます。
2. System Manager で、機能有効識別子を確認します。[設定]、[システム]の順に移動し、下にスクロールして*アドオン*を表示します。機能有効識別子*を探します。機能有効識別子の番号を記録します。
3. Feature Activation Codeを確認して記録します。機能パックの場合、このアクティベーションコードは、変換を実行するための適切な手順に記載されています。

   ネットアップの手順説明にはからアクセスできます "NetApp Eシリーズシステムのドキュメントセンター"。

   プレミアム機能の場合は、サポートサイトから次の手順でアクティベーションコードにアクセスできます。

   a. にログインします "ネットアップサポート"。
   b. [製品の管理]>[ソフトウェアライセンス]メニューに移動します。
   c. ストレージアレイシャーシのシリアル番号を入力し、* Go *をクリックします。
   d. [**License Key**]列で、Feature Activation Codeを探します。
   e. 必要な機能のFeature Activation Codeを記録します。
4. シャーシのシリアル番号、Feature Activation Code、機能有効識別子を記載したEメールまたはテキストドキュメントをストレージサプライヤに送信して、機能キーファイルをリクエストします。

   に進むこともできます "ネットアップライセンスのアクティブ化：ストレージアレイプレミアム機能のアクティブ化" 機能または機能パックを入手するために必要な情報を入力します。（このサイトの手順はプレミアム機能用であり、機能パック用ではありません）。

完了後

機能キーファイルを取得したら、プレミアム機能または機能パックを有効にすることができます。

プレミアム機能を有効にします

プレミアム機能は追加オプションであり、有効にするにはキーが必要です。

作業を開始する前に

- 機能キーを入手しておきます。キーについては、必要に応じてテクニカルサポートにお問い合わせください。
- 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備えたシステム）上にキーファイルをロードしておきます。

このタスクについて

このタスクでは、System Managerを使用してプレミアム機能を有効にする方法について説明します。

プレミアム機能を無効にする場合は、コマンドラインインターフェイス（CLI）でDisable Storage Array Featureコマンド（disable storageArray (featurePack|feature=featureAttributeList)）を使用する必要があります。

手順

1. メニューを選択します。[設定][システム]。
2. 「アドオン」で、「プレミアム機能を有効にする」を選択します。

   プレミアム機能を有効にするダイアログボックスが開きます。

3. **[Browse]**(参照)をクリックし、キーファイルを選択します。

   ファイル名がダイアログボックスに表示されます。

4. **[Enable]** をクリックします。

機能パックを有効にします

機能パックは、ストレージアレイの属性を変更する（プロトコルをFibre ChannelからiSCSIに変更するなど）バンドルです。機能パックを有効にするには特別なキーが必要です。

作業を開始する前に

- 適切な手順に従って変換を実行し、新しいストレージアレイ属性に合わせてシステムを準備しておきます。

  変換手順については、を参照してください "NetApp Eシリーズシステムのドキュメントセンター"。

- ストレージアレイがオフラインであり、ホストやアプリケーションからのアクセスがないことを確認します。
- すべてのデータがバックアップされます。
- 機能パックファイルを入手しておきます。

  機能パックファイルは管理クライアント（System Managerにアクセスするためのブラウザを備えたシス

テム）上にロードされます。

システムを停止するメンテナンス時間をスケジュールして、ホストとコントローラの間のすべてのI/O処理を停止する必要があります。また、変更が完了するまではストレージアレイのデータにアクセスできないことに注意してください。

このタスクについて

このタスクでは、System Managerを使用して機能パックを有効にする方法について説明します。完了したら、ストレージアレイを再起動する必要があります。

手順

1. メニューを選択します。[設定][システム]。
2. [* アドオン *] で、 [* 機能パックの変更 *] を選択します。
3. [**Browse**](参照)をクリックし、キーファイルを選択します。

   ファイル名がダイアログボックスに表示されます。
4. フィールドに「 * CHANGE * 」と入力します。
5. [変更（ Change ）] をクリックします。

   機能パックの移行が開始され、コントローラがリブートします。I/Oアクティビティをなくすために、書き込み前のキャッシュデータが削除されます。両方のコントローラが自動的にリブートし、新しい機能パックが有効になります。リブートが完了すると、ストレージアレイは応答可能な状態に戻ります。

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l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）。

期間	説明
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。
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。

期間	説明
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。

アクセス管理

概念

アクセス管理の仕組み

アクセス管理は、SANtricity System Managerでユーザ認証を確立する手段の1つです。ユーザは割り当てられたクレデンシャルを使用してシステムにログインする必要があります。

アクセス管理の設定およびユーザ認証は次のように行います。

1. Security Adminの権限を含むユーザプロファイルでSystem Managerにログインします。

   > 初めてのログインでは'ユーザ名adminが自動的に表示され'変更することはできませんadmin ユーザは'システムのすべての機能にフル・アクセスできます

2. ユーザインターフェイスでアクセス管理に移動します。ストレージアレイはローカルユーザロールを使用するように事前に設定されています。これはロールベースアクセス制御（RBAC）機能の実装です。
3. 管理者は、次の認証方式を1つ以上設定します。
   - ローカルユーザーの役割--ストレージアレイに適用されるRBAC機能を使用して認証を管理しますローカルユーザロールには、事前定義されたユーザプロファイルと、特定のアクセス権限を持つロールが含まれます。管理者は、これらのローカルユーザロールを単一の認証方式として使用することも、ディレクトリサービスと組み合わせて使用することもできます。ユーザのパスワードを設定する以外に必要な設定はありません。
   - ディレクトリサービス-- LDAP (Lightweight Directory Access Protocol)サーバとディレクトリサービス(MicrosoftのActive Directoryなど)を介して認証を管理します管理者がLDAPサーバに接続し、ストレージアレイに組み込まれているローカルユーザロールにLDAPユーザをマッピングします。
   - *saml *-- Security Assertion Markup Language（SAML）2.0を使用してアイデンティティプロバイダ（IdP）を介して認証を管理します。管理者がIdPシステムとストレージアレイの間の通信を確立し、ストレージアレイに組み込まれているローカルユーザロールにIdPユーザをマッピングします。
4. ユーザにSystem Managerのログインクレデンシャルを渡します。
5. ユーザが自身のクレデンシャルを入力してシステムにログインします。

   > 認証がSAMLとシングルサインオン（SSO）で管理されている場合は、System Managerのログインダイアログが省略されることがあります。

   ログイン時には、次のバックグラウンドタスクが実行されます。
   - ユーザ名とパスワードをユーザアカウントと照合して認証します。
   - 割り当てられたロールに基づいてユーザの権限が決まります。
   - ユーザインターフェイスのタスクにユーザがアクセスできるようになります。
   - インターフェイスの右上にユーザ名が表示されます。

System Managerで実行できるタスク

タスクへのアクセス権は、ユーザに割り当てられている次のロールによって異なります。

- * Storage admin *--ストレージ・オブジェクト（ボリュームやディスク・プールなど）への読み取り/書き込みのフル・アクセス。セキュリティ構成へのアクセスはありません。
- * Security admin *--アクセス管理、証明書管理、監査ログ管理のセキュリティ構成へのアクセス、および従来の管理インターフェイス（SYMbol）のオン/オフの切り替え機能。
- * Support admin *--ストレージアレイのすべてのハードウェアリソース、障害データ、MELイベント、およびコントローラファームウェアアップグレードへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
- *Monitor *--すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

使用できないタスクは、ユーザインターフェイスではグレー表示されるか、非表示になります。たとえば、Monitorロールを持つユーザは、ボリュームに関するすべての情報を表示できますが、そのボリュームを変更するための機能にはアクセスできません。[サービスのコピー]や[ワークロードへの追加]などの機能のタブはグレー表示され、[設定の表示/編集]のみが使用できます。

SANtricity Storage Managerへのユーザアクセス

ローカルユーザロールとディレクトリサービスが設定されている場合は、Enterprise Management Window（EMW）で次のいずれかの機能を実行する前に、クレデンシャルを入力する必要があります。

- ストレージアレイの名前を変更しています
- コントローラファームウェアをアップグレード中です
- ストレージアレイ構成をロードしています
- スクリプトを実行する
- 未使用のセッションがタイムアウトしたときにアクティブな処理を実行しようとしています

ストレージアレイにSAMLが設定されている場合、ユーザはEMWを使用してそのアレイのストレージを検出または管理することはできません。

アクセス管理の用語

ストレージアレイに関連するアクセス管理の用語を次に示します。

期間	説明
Active Directory	Active Directory（AD）は、Windowsドメインネットワーク用のLDAPを使用するMicrosoftのディレクトリサービスです。
結合	バインド処理は、ディレクトリサーバに対するクライアントの認証に使用されます。通常はアカウントとパスワードのクレデンシャルが必要ですが、匿名のバインド処理が可能なサーバもあります。

期間	説明
できます	認証局（CA）は、インターネットセキュリティのためにデジタル証明書と呼ばれる電子文書を発行する信頼されたエンティティです。証明書でWebサイトの所有者を識別することにより、クライアントとサーバの間のセキュアな接続が確立されます。
証明書	証明書はセキュリティ上の目的でサイトの所有者を識別するもので、攻撃者による偽装を防止します。証明書には、サイトの所有者に関する情報と、その情報について証明（署名）する信頼されたエンティティのIDが含まれます。
IdP	アイデンティティプロバイダ（IdP）は、ユーザにクレデンシャルを要求して認証されたユーザかどうかを確認するために使用される外部のシステムです。多要素認証にも対応し、Active Directoryなどの任意のユーザデータベースを使用するように設定できます。IdPの保守はセキュリティチームが行います。
LDAP	Lightweight Directory Access Protocol（LDAP）は、分散型のディレクトリ情報サービスへのアクセスと管理に使用されるアプリケーションプロトコルです。このプロトコルを使用すると、さまざまなアプリケーションやサービスがLDAPサーバに接続してユーザを検証できます。
RBAC	ロールベースアクセス制御（RBAC）は、コンピュータやネットワークリソースへのアクセスを個々のユーザのロールに基づいて制御する手法です。ストレージアレイにはRBACが適用され、事前定義されたロールが用意されています。
SAML	Security Assertion Markup Language（SAML）は、2つのエンティティ間の認証と許可に使用されるXMLベースの標準規格です。SAMLは、ユーザの認証時に複数の項目（パスワードとフィンガープリントなど）を求める多要素認証に対応しています。ストレージアレイに組み込みのSAML機能は、SAML2.0のアイデンティティアサーション、認証、および許可に準拠しています。
SP	サービスプロバイダ（SP）は、ユーザの認証とアクセスを制御するシステムです。アクセス管理にSAMLを設定すると、ストレージアレイがアイデンティティプロバイダに認証を要求するサービスプロバイダとして機能します。

期間	説明
SSO	シングルサインオン（SSO）は、1組のログインクレデンシャルで複数のアプリケーションにアクセスできるようにする認証サービスです。

マッピングされたロールの権限

ストレージアレイに組み込みのロールベースアクセス制御（RBAC）機能には、1つ以上のロールがマッピングされた事前定義済みのユーザプロファイルが含まれています。各ロールには、SANtricity System Managerのタスクにアクセスするための権限が含まれています。

ユーザプロファイルとマッピングされたロールには、どちらかのSystem Managerのユーザインターフェイスで設定（Access Management >ローカルユーザロール）のメニューからアクセスできます。

これらのロールにより、次のタスクへのアクセスが可能になります。

- * Storage admin *--ストレージ・オブジェクト（ボリュームやディスク・プールなど）への読み取り/書き込みのフル・アクセス。セキュリティ構成へのアクセスはありません。
- * Security admin *--アクセス管理、証明書管理、監査ログ管理のセキュリティ構成へのアクセス、および従来の管理インターフェイス（SYMbol）のオン/オフの切り替え機能。
- * Support admin *--ストレージアレイのすべてのハードウェアリソース、障害データ、MELイベント、およびコントローラファームウェアアップグレードへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
- *Monitor *--すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

ユーザに特定のタスクに対する権限がない場合、そのタスクはグレー表示されるか、ユーザインターフェイスに表示されません。

ローカルユーザロールを使用したアクセス管理

管理者は、ストレージアレイに組み込みのロールベースアクセス制御（RBAC）機能をアクセス管理に使用できます。これらの機能のことを「ローカルユーザロール」と呼びます。

設定ワークフロー

ローカルユーザロールはストレージアレイに事前に設定されています。認証にローカルユーザロールを使用する場合、管理者は次の操作を行うことができます。

1. Security Adminの権限を含むユーザプロファイルでSANtricity System Managerにログインします。

   adminユーザは'システムのすべての機能にフル・アクセスできます

2. ユーザプロファイルを確認します。ユーザプロファイルは事前に定義されており、変更することはできません。

3. 必要に応じて、各ユーザプロファイルに新しいパスワードを割り当てます。
4. ユーザは各自に割り当てられたクレデンシャルでシステムにログインします。

管理

認証にローカルユーザロールのみを使用する場合、管理者は次の管理タスクを実行できます。

- パスワードを変更します。
- パスワードの最小文字数を設定する。
- パスワードなしでのログインをユーザに許可します。

ディレクトリサービスを使用したアクセス管理

管理者は、LDAP（Lightweight Directory Access Protocol）サーバとディレクトリサービス（MicrosoftのActive Directoryなど）をアクセス管理に使用できます。

設定ワークフロー

ネットワークでLDAPサーバとディレクトリサービスが使用されている場合、設定は次のようになります。

1. Security Adminの権限を含むユーザプロファイルでSANtricity System Managerにログインします。

   adminユーザは'システムのすべての機能にフル・アクセスできます

2. LDAPサーバの設定を入力します。これには、ドメイン名、URL、バインドアカウント情報が含まれます。
3. LDAPサーバでセキュアなプロトコル（LDAPS）を使用している場合、LDAPサーバとストレージアレイの間の認証に使用する認証局（CA）証明書チェーンをアップロードします。
4. サーバ接続が確立されたら、ユーザグループをストレージアレイのロールにマッピングします。これらのロールは事前に定義されており、変更できません。
5. LDAPサーバとストレージアレイの間の接続をテストします。
6. ユーザは各自に割り当てられたLDAP /ディレクトリサービスのクレデンシャルを使用してシステムにログインします。

管理

認証にディレクトリサービスを使用する場合、管理者は次の管理タスクを実行できます。

- ディレクトリサーバを追加します。
- ディレクトリサーバの設定を編集します。
- LDAPユーザをローカルユーザロールにマッピングする。
- ディレクトリサーバを削除する。

SAMLを使用したアクセス管理

管理者は、アレイに組み込みのSecurity Assertion Markup Language（SAML）2.0の機能

をアクセス管理に使用できます。

設定ワークフロー

SAMLの設定は次のように行います。

1. Security Adminの権限を含むユーザプロファイルでSystem Managerにログインします。

   adminユーザはSystem Managerのすべての機能にフル・アクセスできます

2. 管理者は、[アクセス管理]の下の[*SAML *]タブに移動します。
3. アイデンティティプロバイダ（IdP）との通信を設定します。IdPは、ユーザにクレデンシャルを要求して認証されたユーザかどうかを確認するための外部システムです。ストレージアレイとの通信を設定するには、IdPシステムからIdPメタデータファイルをダウンロードし、System Managerを使用してそのファイルをストレージアレイにアップロードします。
4. サービスプロバイダとIdP間の信頼関係を確立します。サービスプロバイダはユーザ権限を制御します。このケースでは、ストレージアレイ内のコントローラがサービスプロバイダの役割を果たします。通信を設定するには、System Managerを使用して、各コントローラのサービスプロバイダメタデータファイルをエクスポートします。その後、IdPシステムからそれらのメタデータファイルをIdPにインポートします。

   また、認証時に名前IDを返す機能がIdPでサポートされていることを確認しておく必要があります。

5. ストレージアレイのロールをIdPで定義されているユーザ属性にマッピングします。これを行うには、管理者はSystem Managerを使用してマッピングを作成します。
6. IdP URLへのSSOログインをテストします。このテストで、ストレージアレイとIdPが通信できることを確認します。

   SAMLを有効にすると、ユーザインターフェイスで無効にしたり、IdP設定を編集したりすることはできなくなります。SAMLの設定を無効にしたり編集したりする必要がある場合は、テクニカルサポートにお問い合わせください。

7. System Managerから、ストレージアレイのSAMLを有効にします。
8. ユーザが自身のSSOクレデンシャルを使用してシステムにログインします。

管理

認証にSAMLを使用している場合、管理者は次の管理タスクを実行できます。

- 新しいロールマッピングを変更または作成します
- サービスプロバイダファイルをエクスポート

アクセス制限

SAMLが有効な場合、次のクライアントはストレージアレイのサービスとリソースにアクセスできません。

- Enterprise Management Window（EMW）

- コマンドラインインターフェイス（ CLI ）
- ソフトウェア開発キット（SDK）クライアント
- インバンドクライアント
- HTTPベーシック認証REST APIクライアント
- 標準のREST APIエンドポイントを使用してログインします

方法

ローカルユーザロールを表示します

[ローカルユーザーの役割]タブでは、ユーザープロファイルとデフォルトの役割のマッピングを表示できます。これらのマッピングは、ストレージアレイに適用されたロールベースアクセス制御（RBAC）の一部です。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。

このタスクについて

ユーザプロファイルとマッピングは変更できません。変更できるのはパスワードだけです。

手順

1. メニューを選択します。Settings [Access Management]。
2. [ローカルユーザー役割*（Local User Roles *）]タブを選択します。

   ユーザプロファイルが表に表示されます。

   - * Root admin *(admin)--システム内のすべての機能にアクセスできるスーパー管理者。このユーザプロファイルにはすべてのロールが含まれています。
   - * Storage admin *（storage）--すべてのストレージプロビジョニングを担当する管理者。このユーザプロファイルには、Storage Admin、Support Admin、Monitorの各ロールが含まれています。
   - * Security admin *（security）--アクセス管理、証明書管理、セキュリティ有効ドライブ機能など、セキュリティ構成を担当するユーザー。このユーザプロファイルには、Security AdminとMonitorの各ロールが含まれています。
   - * Support admin*(support)--ハードウェアリソース’障害データ’ファームウェアのアップグレードを担当するユーザーこのユーザプロファイルには、Support AdminとMonitorの各ロールが含まれています。
   - **Monitor**(モニタ)--システムへの読み取り専用アクセス権を持つユーザ。このユーザプロファイルには、Monitorロールのみが含まれています。

パスワードを変更します

アクセス管理で各ユーザプロファイルのユーザパスワードを変更できます。

作業を開始する前に

- Root Adminの権限が割り当てられたローカル管理者としてログインする必要があります。

- ローカル管理者のパスワードを確認しておく必要があります。

このタスクについて

パスワードを選択する際は、次のガイドラインに注意してください。

- 新しいローカルユーザパスワードは、最小パスワードの現在の設定（[表示/編集の設定]）以上である必要があります。
- パスワードは大文字と小文字を区別します。
- パスワードの末尾のスペースは削除されません。パスワードにスペースが含まれている場合は、スペースを含めるようにしてください。
- セキュリティを強化するために、パスワードには15文字以上の英数字を使用し、頻繁に変更してください。

System Managerでパスワードを変更すると、コマンドラインインターフェイス（CLI）のパスワードも変更されます。また、パスワードは、ユーザのアクティブなセッションを終了するために原因 を変更します。

手順

1. メニューを選選択します。Settings [Access Management]。
2. [ローカルユーザー役割*（Local User Roles *）]タブを選択します。
3. 表からユーザを選択します。

   [パスワードの変更*]ボタンが使用可能になります。

4. [パスワードの変更 *] を選択します。

   パスワードの変更*（Change Password *）ダイアログボックスが開きます。

5. ローカルユーザパスワードの最低文字数が設定されていない場合は、選択したユーザがパスワードを入力しないとストレージアレイにアクセスできないようにするオプションのチェックボックスをオンにし、そのユーザの新しいパスワードを入力します。
6. ローカル管理者パスワードを入力し、* Change *をクリックします。

結果

ユーザが現在ログインしている場合、パスワードを変更するとユーザのアクティブなセッションが終了します。

ローカルユーザパスワードの設定を変更します

ストレージアレイで新規または更新されるローカルユーザパスワードの最小文字数を設定できます。また、ローカルユーザがパスワードを入力せずにストレージアレイにアクセスできるようにすることもできます。

作業を開始する前に

- Root Adminの権限が割り当てられたローカル管理者としてログインする必要があります。

このタスクについて

ローカルユーザパスワードの最小文字数を設定する際には、次のガイドラインに注意してください。

- 設定を変更しても既存のローカルユーザパスワードには影響しません。
- ローカルユーザパスワードの最小文字数は、0~30文字にする必要があります。
- 新しいローカルユーザパスワードは、現在の最小文字数の設定以上にする必要があります。
- ローカルユーザがパスワードを入力せずにストレージアレイにアクセスできるようにする場合は、パスワードの最小文字数を設定しないでください。

手順

1. メニューを選択します。Settings [Access Management]。
2. [ローカルユーザー役割*（Local User Roles *）]タブを選択します。
3. 「表示/設定の編集」ボタンを選択します。

   [ローカルユーザーパスワードの設定*]ダイアログボックスが開きます。

4. 次のいずれかを実行します。
   - ローカルユーザがパスワードを入力せずにストレージアレイにアクセスできるようにするには、「すべてのローカルユーザパスワードを少なくとも必要とする」チェックボックスをオフにします。
   - すべてのローカルユーザパスワードの最小文字数を設定するには、「すべてのローカルユーザパスワードを少なくとも必要とする」チェックボックスをオンにしてから、スピンボックスを使用してすべてのローカルユーザパスワードの最小文字数を設定します。

     新しいローカルユーザパスワードは、現在の設定以上の長さにする必要があります。
5. [保存（ Save ）] をクリックします。

ディレクトリサーバを追加します

アクセス管理用に認証を設定するには、ストレージアレイとLDAPサーバの間の通信を確立し、LDAPユーザグループをアレイの事前定義されたロールにマッピングします。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- ユーザグループがディレクトリサービスに定義されている必要があります。
- LDAPサーバのクレデンシャルを確認しておく必要があります。ドメイン名とサーバのURLのほか、必要に応じてバインドアカウントのユーザ名とパスワードも指定できます。
- セキュアなプロトコルを使用するLDAPSサーバの場合は、LDAPサーバの証明書チェーンがローカルマシンにインストールされている必要があります。

このタスクについて

ディレクトリサーバの追加は、2つのステップで行います。まず、ドメイン名とURLを入力します。サーバでセキュアなプロトコルを使用している場合、認証に使用するCA証明書が標準の署名機関によって署名されていない場合、その証明書もアップロードする必要があります。バインドアカウントのクレデンシャルがある場合は、そのアカウント名とパスワードも入力できます。次に、LDAPサーバのユーザグループをストレージアレイの事前定義されたロールにマッピングします。

手順 でLDAPサーバを追加すると、従来の管理インターフェイスは無効になります。従来の管理インターフェイス（SYMbol）は、ストレージアレイと管理クライアントの間の通信に使用される方法です。無効にすると、ストレージアレイと管理クライアントはより安全な通信方法（HTTPS経由のREST API）を使用します。

手順

1. メニューを選択します。Settings [Access Management]。
2. [ディレクトリサービス]タブで、[ディレクトリサーバーの追加]を選択します。

   [ディレクトリサーバーの追加*]ダイアログボックスが開きます。

3. [サーバー設定]タブで、LDAPサーバーの資格情報を入力します。

フィールドの詳細

設定	説明
構成設定	ドメイン
LDAPサーバのドメイン名を入力します。ドメインを複数入力する場合は、カンマで区切って入力します。ドメイン名は、ログイン（*username@domain*）で、認証するディレクトリサーバを指定するために使用されます。	サーバURL
LDAPサーバにアクセスするためのURLを'ldap[s]://*host:port*'の形式で入力します	証明書のアップロード（オプション）
このフィールドは、上記のサーバURLフィールドにLDAPSプロトコルが指定されている場合にのみ表示されます。 [**Browse**]をクリックして、アップロードするCA証明書を選択します。これは、LDAPサーバの認証に使用される信頼された証明書または証明書チェーンです。	バインドアカウント（オプション）
LDAPサーバに対する検索クエリやグループ内の検索で使用する読み取り専用のユーザアカウントを入力します。アカウント名はLDAPタイプの形式で入力します。たとえば、バインドユーザの名前が「bindacct」であれば、「CN=bindacct、CN=Users、DC=cpoc、DC=local」などと入力します。	バインドパスワード（オプション）
このフィールドは、上記のバインドアカウントを入力した場合に表示されます。 バインドアカウントのパスワードを入力します。	追加する前にサーバ接続をテストします

設定	説明
入力したLDAPサーバの設定でストレージアレイと通信できるかどうかを確認するには、このチェックボックスを選択します。このテストは、ダイアログボックスの下部にある*追加*（* Add *）をクリックした後に実行されます。このチェックボックスをオンにした場合、テストに失敗すると設定は追加されません。設定を追加するには、エラーを解決するか、チェックボックスを選択解除してテストをスキップする必要があります。	権限の設定
検索ベースDN	ユーザーを検索するLDAPコンテキストを入力します通常は'CN=Users'DC=copc'DC=local'の形式で入力します
ユーザー名属性	認証用のユーザIDにバインドされた属性を入力します。例:「sAMAccountName」。
グループ属性	グループとロールのマッピングに使用される、ユーザの一連のグループ属性を入力します。例: memberOf, managedObjects`

4. [ロールマッピング]タブをクリックします。
5. 事前定義されたロールにLDAPグループを割り当てます。1つのグループに複数のロールを割り当てることができます。

   フィールドの詳細

設定	説明
マッピング	グループDN
マッピングするLDAPユーザグループの識別名（DN）を指定します。	ロール

   Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールがないユーザの場合、System Managerは正常に動作しません。

6. 必要に応じて、*別のマッピングを追加*をクリックして、グループとロールのマッピングをさらに入力します。
7. マッピングが終了したら、*追加*をクリックします。

   ストレージアレイとLDAPサーバが通信できるかどうかの検証がシステムによって実行されます。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で入力したクレデンシャルを確認し、必要に応じて

情報を再入力します。

ディレクトリサーバ設定とロールマッピングを編集します

アクセス管理でディレクトリサーバを設定済みの場合は、いつでも設定を変更できます。設定には、サーバ接続情報とグループとロールのマッピングが含まれます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- ディレクトリサーバが定義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。Settings [Access Management]。
2. [ディレクトリサービス]タブを選択します。
3. 複数のサーバが定義されている場合は、編集するサーバを表から選択します。
4. 「表示/設定の編集」を選択します。

   [ディレクトリサーバー設定]ダイアログボックスが開きます。

5. サーバー設定*タブで、必要な設定を変更します。

設定	説明
構成設定	ドメイン
LDAPサーバのドメイン名。ドメインを複数入力する場合は、カンマで区切って入力します。ドメイン名は、ログイン（*username@domain*）で、認証するディレクトリサーバを指定するために使用されます。	サーバURL
LDAPサーバにアクセスするためのURL。形式は「ldap[s]：//*host*：*port*」です。	バインドアカウント（オプション）
LDAPサーバに対する検索クエリやグループ内の検索で使用する読み取り専用のユーザアカウント。	バインドパスワード（オプション）
バインドアカウントのパスワード（このフィールドはバインドアカウントを入力した場合に表示されます）。	保存する前にサーバ接続をテストします

設定	説明
ストレージアレイがLDAPサーバの設定と通信できることを確認します。テストは、ダイアログボックスの下部にある「保存」をクリックすると実行されます。このチェックボックスをオンにした場合、テストに失敗すると設定は変更されません。設定を編集するには、エラーを解決するか、チェックボックスを選択解除してテストをスキップする必要があります。	権限の設定
検索ベースDN	ユーザを検索するLDAPコンテキスト。通常は「CN=Users」、DC=copc、DC=local」の形式で入力します。
ユーザー名属性	認証用のユーザIDにバインドされた属性。例: 「sAMAccountName」。
グループ属性	グループとロールのマッピングに使用される、ユーザのグループ属性のリスト。例: memberOf, managedObjects`

6. [役割マッピング]タブで、目的のマッピングを変更します。

設定	説明
マッピング	グループDN
マッピングするLDAPユーザグループのドメイン名。	ロール

Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールがないユーザの場合、System Managerは正常に動作しません。

7. 必要に応じて、*別のマッピングを追加*をクリックして、グループとロールのマッピングをさらに入力します。
8. [保存（ Save ）] をクリックします。

結果

このタスクを完了すると、アクティブなユーザセッションはすべて終了します。現在のユーザセッションのみが保持されます。

ディレクトリサーバを削除します

ディレクトリサーバとストレージアレイ間の接続を解除するために、アクセス管理ページからサーバ情報を削除できます。このタスクは、新しいサーバを設定して古いサーバを削除する場合などに実行します。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。

このタスクについて

このタスクを完了すると、アクティブなユーザセッションはすべて終了します。現在のユーザセッションのみが保持されます。

手順

1. メニューを選択します。Settings [Access Management]。
2. [ディレクトリサービス]タブを選択します。
3. リストから、削除するディレクトリサーバを選択します。
4. [削除（ Remove ）] をクリックします。

   [ディレクトリサーバーの削除*]ダイアログボックスが開きます。

5. フィールドに「remove」と入力し、「* Remove *」をクリックします。

   ディレクトリサーバの構成設定、権限設定、およびロールのマッピングが削除されます。ユーザは、このサーバからのクレデンシャルを使用してログインできなくなります。

SAMLを設定する

アクセス管理の認証を設定する場合、ストレージアレイに組み込みのSecurity Assertion Markup Language（SAML）機能を使用することができます。この設定により、アイデンティティプロバイダとストレージプロバイダの間の接続が確立されます。

このタスクについて

アイデンティティプロバイダ（IdP）は、ユーザにクレデンシャルを要求して認証されたユーザかどうかを確認するために使用される外部のシステムです。多要素認証にも対応し、Active Directoryなどの任意のユーザデータベースを使用するように設定できます。IdPの保守はセキュリティチームが行います。サービスプロバイダ（SP）は、ユーザの認証とアクセスを制御するシステムです。アクセス管理にSAMLを設定すると、ストレージアレイがアイデンティティプロバイダに認証を要求するサービスプロバイダとして機能します。IdPとストレージアレイの間の接続を確立するには、この2つのエンティティ間でメタデータファイルを共有します。その後、IdPのユーザエンティティをストレージアレイのロールにマッピングします。最後に、接続とSSOログインをテストしたうえでSAMLを有効にします。

- SAMLとディレクトリサービス*。認証方式としてディレクトリサービスを使用するように設定されている状況でSAMLを有効にした場合、System ManagerではSAMLがディレクトリサービスよりも優先されます。あとでSAMLを無効にすると、元の設定に戻ってディレクトリサービスが使用されます。

- SAMLを編集および無効化しています。* SAMLを有効にすると、ユーザインターフェイスで無効にすることはできず、IdP設定を編集することもできません。SAMLの設定を無効にしたり編集したりする必要がある場合は、テクニカルサポートにお問い合わせください。

SAML認証の設定は複数の手順からなる手順 です。

- 手順1：IdPのメタデータファイルをアップロードする
- 手順2：サービスプロバイダのファイルをエクスポートする
- 手順3：ロールをマッピングする
- 手順4：SSOログインをテストする
- 手順5：SAMLを有効にする

手順**1**：**IdP**のメタデータファイルをアップロードする

ストレージアレイにIdPの接続情報を提供するには、System ManagerにIdPのメタデータをインポートします。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- IdP管理者がIdPシステムの設定を完了している必要があります。
- IdP管理者が、認証時に名前IDを返す機能がIdPでサポートされていることを確認しておく必要があります。
- IdPサーバとコントローラのクロックを同期しておきます（NTPサーバを使用するかコントローラのクロックの設定を調整します）。
- IdPのメタデータファイルをIdPシステムからダウンロードし、System Managerへのアクセスに使用するローカルシステムで使用できるようにしておきます。

このタスクについて

このタスクでは、IdPのメタデータファイルをSystem Managerにアップロードします。このメタデータは、IdPシステムが認証要求を正しいURLにリダイレクトし、受信した応答を検証するために必要です。コントローラが2台ある場合でも、アップロードするメタデータファイルはストレージアレイに対して1つだけです。

手順

1. メニューを選択します。Settings [Access Management]。
2. SAML *タブを選択します。

   設定手順の概要が表示されます。

3. アイデンティティプロバイダ（IdP）ファイルのインポート*リンクをクリックします。

   [アイデンティティプロバイダファイルのインポート]ダイアログが開きます。

4. Browse *をクリックして、ローカルシステムにコピーしたIdPメタデータファイルを選択してアップロードします。

   ファイルを選択すると、IdPのエンティティIDが表示されます。

5. [* インポート *] をクリックします。

手順**2**：サービスプロバイダのファイルをエクスポートする

IdPとストレージアレイの間の信頼関係を確立するために、サービスプロバイダのメタデータをIdPにインポートします。

作業を開始する前に

- ストレージアレイの各コントローラのIPアドレスまたはドメイン名を確認しておきます。

このタスクについて

このタスクでは、コントローラからメタデータ（コントローラごとに1ファイル）をエクスポートします。このメタデータは、IdPがコントローラとの間の信頼関係を確立し、許可要求を処理するために必要になります。このファイルには、コントローラのドメイン名やIPアドレスなど、IdPがサービスプロバイダと通信するために必要な情報が含まれています。

手順

1. [サービスプロバイダファイルのエクスポート*]リンクをクリックします。

   サービスプロバイダファイルのエクスポート*ダイアログが開きます。

2. コントローラのIPアドレスまたはDNS名を[コントローラ**A** *]フィールドに入力し、**[***エクスポート**]**をクリックしてメタデータファイルをローカルシステムに保存します。ストレージアレイにコントローラが**2**台ある場合は、**2**台目のコントローラの Controller B *フィールドでこの手順を繰り返します。

   Export（エクスポート）をクリックすると、サービスプロバイダメタデータがローカルシステムにダウンロードされます。ファイルの保存先をメモします。

3. ローカルシステムで、エクスポートしたサービスプロバイダのメタデータファイルを探します。

   コントローラごとにXML形式のファイルが1つあります。

4. IdPサーバで、サービスプロバイダのメタデータファイルをインポートして信頼関係を確立します。ファイルを直接インポートすることも、ファイルからコントローラの情報を手動で入力することもできます。

手順**3**：ロールをマッピングする

System Managerに対する許可とアクセスをユーザに提供するには、IdPユーザ属性とグループメンバーシップをストレージアレイの事前定義されたロールにマッピングする必要があります。

作業を開始する前に

- IdP管理者が、IdPシステムでユーザ属性とグループメンバーシップを設定しておく必要があります。
- IdPのメタデータファイルをSystem Managerにインポートしておきます。
- 各コントローラのサービスプロバイダメタデータファイルをIdPシステムにインポートして信頼関係を確立しておきます。

このタスクについて

このタスクでは、System Managerを使用してIdPグループをローカルユーザロールにマッピングします。

手順

1. System Managerのロールをマッピングするためのリンクをクリックします。

   [役割マッピング（* Role Mapping *）]ダイアログボックスが開きます。

2. IdPユーザの属性とグループを事前定義されたロールに割り当てます。1つのグループに複数のロールを割り当てることができます。

   フィールドの詳細

設定	説明
マッピング	ユーザー属性
マッピングするSAMLグループの属性（「member of」など）を指定します。	属性値
マッピングするグループの属性値を指定します。	ロール

   Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールがないユーザの場合、System Managerは正常に動作しません。

3. 必要に応じて、*別のマッピングを追加*をクリックして、グループとロールのマッピングをさらに入力します。

   ロールのマッピングは、SAMLを有効にしたあとに変更できます。

4. マッピングが終了したら、*保存*をクリックします。

手順**4**：**SSO**ログインをテストする

IdPシステムとストレージアレイが通信できることを確認するために、必要に応じてSSOログインをテストできます。このテストは、SAMLを有効にする最後の手順でも実行します。

作業を開始する前に

- IdPのメタデータファイルをSystem Managerにインポートしておきます。
- 各コントローラのサービスプロバイダメタデータファイルをIdPシステムにインポートして信頼関係を確立しておきます。

手順

1. [Test SSO Login*]リンクを選択します。

   SSOクレデンシャルの入力を求めるダイアログが表示されます。

2. Security AdminとMonitorの両方の権限を持つユーザのログインクレデンシャルを入力します。

ログインのテスト中にダイアログが開きます。

3. テストに成功したことを示すメッセージを確認します。テストに成功した場合は、SAMLを有効にする次の手順に進みます。

   テストが正常に完了しない場合は、エラーメッセージに詳細が表示されます。次の点を確認してください。

   - ユーザがSecurity AdminとMonitorの権限を持つグループに属していること。
   - アップロードしたIdPサーバのメタデータが正しいこと。
   - SPメタデータファイル内のコントローラのアドレスが正しいこと。

手順**5**：**SAML**を有効にする

最後の手順として、SAMLユーザ認証を有効にします。

作業を開始する前に

- IdPのメタデータファイルをSystem Managerにインポートしておきます。
- 各コントローラのサービスプロバイダメタデータファイルをIdPシステムにインポートして信頼関係を確立しておきます。
- 少なくともMonitorロールとSecurity Adminロールを1つずつマッピングしておきます。

このタスクについて

このタスクでは、ユーザ認証のSAMLの設定を終了する方法について説明します。このプロセスでは、SSOログインのテストも求められます。SSOログインのテストプロセスについては、前の手順で説明したとおりです。

- SAMLを編集および無効化しています。* SAMLを有効にすると、ユーザインターフェイスで無効にすることはできず、IdP設定を編集することもできません。SAMLの設定を無効にしたり編集したりする必要がある場合は、テクニカルサポートにお問い合わせください。

手順

1. [* SAML **]**タブで、**[** SAMLを有効にする]リンクを選択します。

   [*Confirm Enable SAML *]ダイアログが開きます。

2. 「enable」と入力し、「* Enable」をクリックします。
3. SSOログインのテスト用にユーザクレデンシャルを入力します。

結果

SAMLが有効になると、アクティブなセッションはすべて終了され、SAMLを使用したユーザの認証が開始されます。

SAMLのロールマッピングを変更する

アクセス管理にSAMLを設定している場合、IdPグループとストレージアレイの事前定義されたロールとの間のロールマッピングを変更できます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- IdP管理者が、IdPシステムでユーザ属性とグループメンバーシップを設定しておく必要があります。
- SAMLを設定して有効にします。

手順

1. メニューを選択します。Settings [Access Management]。
2. SAML *タブを選択します。
3. [役割のマッピング]を選択します。

   [役割マッピング（* Role Mapping *）]ダイアログボックスが開きます。

4. IdPユーザの属性とグループを事前定義されたロールに割り当てます。1つのグループに複数のロールを割り当てることができます。

   SAMLが有効になっているときは権限を削除しないように注意してください。削除すると、System Managerにアクセスできなくなります。

   フィールドの詳細

設定	説明
マッピング	ユーザー属性
マッピングするSAMLグループの属性（「member of」など）を指定します。	属性値
マッピングするグループの属性値を指定します。	ロール

   Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールがないユーザの場合、System Managerは正常に動作しません。

5. オプション： Add another mapping *をクリックして、グループとロールのマッピングをさらに入力します。
6. [保存（ Save ）] をクリックします。

結果

このタスクを完了すると、アクティブなユーザセッションはすべて終了します。現在のユーザセッションのみが保持されます。

SAMLサービスプロバイダファイルをエクスポートする

必要に応じて、ストレージアレイのサービスプロバイダのメタデータをエクスポートし

て、ファイルをアイデンティティプロバイダ（IdP）システムに再インポートすることができます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- SAMLを設定して有効にします。

このタスクについて

このタスクでは、コントローラからメタデータ（コントローラごとに1ファイル）をエクスポートします。このメタデータは、IdPがコントローラとの間の信頼関係を確立し、認証要求を処理するために必要になります。このファイルには、コントローラのドメイン名やIPアドレスなど、IdPで要求の送信に使用できる情報が含まれています。

手順

1. メニューを選択します。Settings [Access Management]。
2. SAML *タブを選択します。
3. 「書き出し」を選択します。

   サービスプロバイダファイルのエクスポート*ダイアログが開きます。

4. 各コントローラについて、* Export（エクスポート）*をクリックしてメタデータファイルをローカルシステムに保存します。

   各コントローラのドメイン名フィールドは読み取り専用です。

   ファイルの保存先をメモします。

5. ローカルシステムで、エクスポートしたサービスプロバイダのメタデータファイルを探します。

   コントローラごとにXML形式のファイルが1つあります。

6. IdPサーバから、サービスプロバイダのメタデータファイルをインポートします。ファイルを直接インポートすることも、ファイルからコントローラの情報を手動で入力することもできます。
7. [* 閉じる *] をクリックします。

監査ログアクティビティを表示します

Security Admin権限を持つユーザは、監査ログを表示して、ユーザによる操作、認証エラー、無効なログインの試行、およびユーザセッションの期間を監視できます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。

手順

1. メニューを選択します。Settings [Access Management]。

2. [監査ログ]タブを選択します。

   *監査ログ*アクティビティは表形式で表示されます。この表には、次の情報列が含まれます。

   - 日付/時刻--ストレージアレイがイベントを検出した日時（GMT）のタイムスタンプ
   - ユーザー名--イベントに関連付けられたユーザー名。ストレージアレイに対して認証されていない操作が実行された場合は、「N/A」と表示されます。内部プロキシまたはその他のメカニズムによって、認証されていないアクションがトリガーされることがあります。
   - ステータスコード--操作のHTTPステータスコード(200、400など)およびイベントに関連する説明テキスト。
   - **URL**アクセス--完全なURL (ホストを含む)とクエリ文字列。
   - クライアント**IP**アドレス--イベントに関連付けられたクライアントのIPアドレス。
   - **Source**--イベントに関連付けられたロギングソース。System Manager、CLI、Webサービス、またはサポートシェルがあります。

3. [監査ログ]ページの選択項目を使用して、イベントを表示および管理します。

選択の詳細

選択（**Selection**）	説明
イベントを表示する期間を選択…	表示されるイベントを日付範囲（過去24時間、過去7日間、過去30日間、またはカスタムの日付範囲）で限定します。
フィルタ	表示されるイベントをフィールドに入力した文字で限定します。単語の完全一致には引用符("")を使用し、1つ以上の単語を返すには「」または「」を入力します。単語を省略するにはダッシュ(--)を入力します。
更新	最新のイベントにページを更新するには、「更新」を選択します。
設定の表示/編集	［表示/設定の編集］を選択すると、ログに記録するフルログポリシーとアクションのレベルを指定できるダイアログボックスが開きます。
イベントを削除します	「削除」を選択すると、ページから古いイベントを削除できるダイアログボックスが開きます。
列の表示/非表示を切り替えます	[列を表示/非表示（* Show/Hide * Column）]アイコンをクリックします をクリックして、表に表示する列を追加で選択します。その他の列には、次のもの • メソッド-- HTTPメソッド(POST、GET、削除など)。 • **CLI**コマンド実行-- Secure CLI要求に対して実行されるCLIコマンド(文法)。 • **CLI**戻りステータス-- CLIステータスコードまたはクライアントからの入力ファイルの要求。 • *SYMBOL手順 *--実行されたSYMBOL手順 。 • *SSH Event Type *-- Secure Shell (SSH)イベントのタイプ(ログイン、ログアウト、login_failなど) • *SSHセッションPID *-- SSHセッションのプロセスID番号。 • **SSH**セッション期間--ユーザーがログインした秒数
列フィルタを切り替えます	[切り替え*（Toggle *）]アイコンをクリックします をクリックすると、各列のフィルタリングフィールドが開きます。表示されるイベントを特定の文字で限定するには、列フィールドにその文字を入力します。フィルタリングフィールドを閉じるには、アイコンをもう一度クリックします。
変更を元に戻します	[元に戻す（Undo）]アイコンをクリックします をクリックすると、テーブルがデフォルトの設定に戻ります。
エクスポート（Export）	[**Export**]をクリックして、テーブルデータをカンマ区切り値（CSV）ファイルに保存します。

監査ログポリシーを定義する

上書きポリシーや監査ログに記録するイベントのタイプを変更することができます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。

このタスクについて

このタスクでは、監査ログの設定を変更する方法について説明します。古いイベントの上書きに関するポリシーや記録するイベントタイプに関するポリシーなどが含まれます。

手順

1. メニューを選択します。Settings [Access Management]。
2. [監査ログ]タブを選択します。
3. 「表示/設定の編集」を選択します。

   [**Audit Log Settings (**監査ログ設定)]ダイアログボックスが開きます。

4. 上書きポリシーや記録するイベントのタイプを変更します。

フィールドの詳細

設定	説明
上書きポリシー	最大容量に達したときに古いイベントを上書きするポリシーを指定します。 • 監査ログがいっぱいになったらイベントを古いものから上書きする-監査ログが50、000レコードに達したときに古いイベントを上書きします。 • 監査ログのイベントを手動で削除する必要があります-イベントが自動的に削除されないように指定します。設定した割合に達した場合、しきい値の警告が表示されます。イベントは手動で削除する必要があります。 上書きポリシーを無効にした場合、監査ログのエントリが上限に達すると、Security Adminの権限がないユーザによるSystem Managerへのアクセスは拒否されます。Security Adminの権限がないユーザが再びシステムにアクセスできるようにするには、Security Adminロールが割り当てられているユーザが古いイベントレコードを削除する必要があります。 上書きポリシーは、監査ログをsyslogサーバにアーカイブするように設定されている場合は適用されません。
ログに記録するアクションのレベル	ログに記録するイベントのタイプを指定します。 • 変更イベントのみを記録する--ユーザーの操作によってシステムに変更が発生するイベントのみを記録します • すべての変更イベントと読み取り専用イベントを記録する--情報の読み取りまたはダウンロードを伴うユーザー操作を含むすべてのイベントを記録します

5. [保存（ Save ）] をクリックします。

監査ログからイベントを削除します

監査ログの古いイベントをクリアすることができます。これにより、イベントの検索が容易になります。削除時に古いイベントをCSV（カンマ区切り値）ファイルに保存することもできます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。

このタスクについて

このタスクでは、監査ログから古いイベントを削除する方法について説明します。

手順

1. メニューを選択します。Settings [Access Management]。
2. [監査ログ]タブを選択します。
3. 「 * 削除」を選択します。

   [監査ログの削除]ダイアログボックスが開きます。

4. 削除する古いイベントの数を選択または入力します。
5. 削除したイベントをCSVファイルにエクスポートする場合は、チェックボックスを選択したままにします（推奨）。次の手順で*削除*をクリックすると、ファイル名と場所の入力を求められます。イベントをCSVファイルに保存しない場合は、チェックボックスをクリックして選択を解除します。
6. [削除（ Delete ）] をクリックします。

   確認のダイアログボックスが開きます。

7. フィールドに「delete」と入力し、「* Delete *」をクリックします。

   最も古いイベントは監査ログページから削除されます。

監査ログ用の**syslog**サーバを設定します

監査ログを外部のsyslogサーバにアーカイブする場合は、そのサーバとストレージアレイの間の通信を設定できます。接続が確立されると、監査ログは自動的にsyslogサーバに保存されます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- syslogサーバのアドレス、プロトコル、およびポート番号を確認しておく必要があります。サーバアドレスは、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスのいずれかで指定できます。
- サーバがセキュアなプロトコル（TLSなど）を使用している場合は、ローカルシステムに認証局（CA）証明書が配置されている必要があります。CA証明書がWebサイトの所有者を識別することにより、サーバとクライアントの間のセキュアな接続が確立さ

手順

1. メニューを選択します。Settings [Access Management]。
2. 監査ログ*タブで、* syslogサーバーの設定*を選択します。

   [Configure Syslog Servers]ダイアログボックスが開きます。

3. [追加（ Add ）] をクリックします。

   [Add Syslog Server*]ダイアログボックスが開きます。

4. サーバーの情報を入力し、*追加*をクリックします。
   - サーバアドレス—完全修飾ドメイン名'IPv4アドレス'またはIPv6アドレスを入力します
   - Protocol --ドロップダウンリストからプロトコル(TLS、UDP、TCPなど)を選択します。
   - 証明書のアップロード（オプション）-- TLSプロトコルを選択し、署名済みCA証明書をまだアップロードしていない場合は、参照をクリックして証明書ファイルをアップロードします。監査ログは、信頼された証明書がないとsyslogサーバにアーカイブされません。

     あとで証明書が無効になると、TLSハンドシェイクは失敗します。その結果、監査ログにエラーメッセージが記録され、syslogサーバにメッセージが送信されなくなります。この問題 を解決するには、syslogサーバで証明書を修正してから、メニューの[設定]、[監査ログ]、[syslogサーバの設定]、[すべてテスト]の順に選択します。

   - ポート-- syslog受信機のポート番号を入力します[Add]をクリックすると、[Configure Syslog Servers]*ダイアログボックスが開き、設定したsyslogサーバがページに表示されます。
5. ストレージアレイとのサーバ接続をテストするには、「*すべてテスト」を選択します。

結果

設定が完了すると、以降すべての監査ログがsyslogサーバに送信されるようになります。以前のログは転送されません。

監査ログレコード用の**syslog**サーバ設定の編集

監査ログのアーカイブに使用するsyslogサーバの設定を変更したり、サーバ用の新しい認証局（CA）証明書をアップロードしたりできます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- syslogサーバのアドレス、プロトコル、およびポート番号を確認しておく必要があります。サーバアドレスは、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスのいずれかで指定できます。
- 新しいCA証明書をアップロードする場合は、ローカルシステムに証明書がある必要があります。

手順

1. メニューを選択します。Settings [Access Management]。
2. 監査ログ*タブで、* syslogサーバーの設定*を選択します。

設定されているsyslogサーバがページに表示されます。

3. サーバ情報を編集するには、サーバ名の右側にある* Edit *（鉛筆）アイコンを選択し、次のフィールドで必要な変更を行います。
   - サーバーアドレス—完全修飾ドメイン名'IPv4アドレス'またはIPv6アドレスを入力します
   - Protocol --ドロップダウンリストからプロトコル(TLS、UDP、TCPなど)を選択します。
   - ポート-- syslog受信機のポート番号を入力します
4. （UDPまたはTCPから）プロトコルをセキュアTLSプロトコルに変更した場合は、[**Import Trusted Certificate**]をクリックしてCA証明書をアップロードします。
5. ストレージアレイとの新しい接続をテストするには、「*すべてテスト」を選択します。

結果

設定が完了すると、以降すべての監査ログがsyslogサーバに送信されるようになります。以前のログは転送されません。

よくある質問です

ログインできないのはなぜですか？

System Managerにログインする際にエラーが表示される場合は、次の問題がないか確認してください。

System Managerのログインエラーは、次のいずれかが原因の可能性があります。

- 入力したユーザ名またはパスワードが正しくありません。
- 必要な権限がありません。
- ディレクトリサーバ（設定されている場合）が使用できない可能性があります。その場合は、ローカルユーザロールでログインしてみてください。
- ログインが複数回失敗したために、ロックアウトモードがトリガーされました。10分待ってから再度ログインしてください。
- ロックアウト状態がトリガーされ、監査ログがいっぱいになった可能性があります。アクセス管理に移動し、監査ログから古いイベントを削除します。
- SAML認証が有効になりました。ログインするには、ブラウザをリフレッシュしてください。

ミラーリングタスク用のリモートストレージアレイでログインエラーが発生する場合は、次のいずれかが原因の可能性があります。

- 入力したパスワードが正しくありません。
- ログインが複数回失敗したために、ロックアウトモードがトリガーされました。10分待ってから再度ログインしてください。
- コントローラで使用されているクライアント接続が最大数に達している。複数のユーザまたはクライアントをチェックしてください。

ディレクトリサーバを追加するときは、どのような点に注意する必要がありますか？

アクセス管理でディレクトリサーバを追加する前に、次の要件を満たしていることを確認してください。

- ユーザグループがディレクトリサービスに定義されている必要があります。
- LDAPサーバのクレデンシャルを確認しておく必要があります。ドメイン名とサーバのURLのほか、必要に応じてバインドアカウントのユーザ名とパスワードも指定できます。
- セキュアなプロトコルを使用するLDAPSサーバの場合は、LDAPサーバの証明書チェーンがローカルマシンにインストールされている必要があります。

ストレージアレイのロールをマッピングするときは、どのような点に注意する必要がありますか？

グループをロールにマッピングする前に、次のガイドラインを確認してください。

ストレージアレイに搭載されたロールベースアクセス制御（RBAC）機能には次のロールがあります。

- * Storage admin *--ストレージ・オブジェクト（ボリュームやディスク・プールなど）への読み取り/書き込みのフル・アクセス。セキュリティ構成へのアクセスはありません。
- * Security admin *--アクセス管理、証明書管理、監査ログ管理のセキュリティ構成へのアクセス、および従来の管理インターフェイス（SYMbol）のオン/オフの切り替え機能。
- * Support admin *--ストレージアレイのすべてのハードウェアリソース、障害データ、MELイベント、およびコントローラファームウェアアップグレードへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
- *Monitor *--すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

ディレクトリサービス

LDAP（Lightweight Directory Access Protocol）サーバとディレクトリサービスを使用する場合は、次の点を確認してください。

- ディレクトリサービスでユーザグループを定義しておきます。
- LDAPユーザグループのグループドメイン名を確認しておきます。
- Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールがないユーザの場合、System Managerは正常に動作しません。

SAML

ストレージアレイに組み込みのSecurity Assertion Markup Language（SAML）機能を使用する場合は、次の点を確認してください。

- アイデンティティプロバイダ（IdP）管理者が、IdPシステムでユーザ属性とグループメンバーシップを設定しておく必要があります。
- グループメンバーシップ名を確認しておきます。
- Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールがないユーザの場合、System Managerは正常に動作しません。

この変更の影響を受ける外部管理ツールはどれですか。

管理インターフェイスを切り替える、認証方式にSAMLを使用する、などの特定の変更をSystem Managerで行うと、一部の外部ツールや機能が使用できなくなることがあります。

管理インターフェイス

SANtricity SMI-S ProviderやOnCommand Insight （OCI）などの従来の管理インターフェイス（SYMbol）と直接通信するツールは、レガシー管理インターフェイスの設定が有効になっていないかぎり機能しません。この設定が無効な場合、従来のCLIコマンドを使用したりミラーリング処理を実行したりすることはできません。

詳細については、テクニカルサポートにお問い合わせください。

SAML 認証

SAMLが有効な場合、次のクライアントはストレージアレイのサービスとリソースにアクセスできません。

- Enterprise Management Window（EMW）
- コマンドラインインターフェイス（ CLI ）
- ソフトウェア開発キット（SDK）クライアント
- インバンドクライアント
- HTTPベーシック認証REST APIクライアント
- 標準のREST APIエンドポイントを使用してログインします

詳細については、テクニカルサポートにお問い合わせください。

SAMLを設定および有効にするときは、どのような点に注意する必要がありますか？

認証のためにSecurity Assertion Markup Language（SAML）の機能を設定して有効にする前に、次の要件を満たしていることを確認し、SAMLの制限事項を理解しておきます。

要件

作業を開始する前に、次の点を確認してください。

- ネットワークにアイデンティティプロバイダ（IdP）を設定しておきます。IdPは、ユーザにクレデンシャルを要求して認証されたユーザかどうかを確認するための外部システムです。IdPの保守はセキュリティチームが行います。
- IdP管理者が、IdPシステムでユーザ属性とユーザグループを設定しておく必要があります。
- IdP管理者が、認証時に名前IDを返す機能がIdPでサポートされていることを確認しておく必要があります。
- IdPサーバとコントローラのクロックを同期しておきます（NTPサーバを使用するかコントローラのクロックの設定を調整します）。
- IdPのメタデータファイルをIdPシステムからダウンロードし、System Managerへのアクセスに使用する

ローカルシステムで使用できるようにしておきます。

- ストレージアレイの各コントローラのIPアドレスまたはドメイン名を確認しておきます。

制限事項

上記の要件に加えて、次の制限事項を理解しておく必要があります。

- SAMLを有効にすると、ユーザインターフェイスで無効にしたり、IdP設定を編集したりすることはできなくなります。SAMLの設定を無効にしたり編集したりする必要がある場合は、テクニカルサポートにお問い合わせください。最後の設定手順でSAMLを有効にする前に、SSOログインをテストすることを推奨します。（SSOログインテストはSAMLが有効になる前にシステムでも実行されます）。
- あとでSAMLを無効にすると、以前の設定（ローカルユーザロール、ディレクトリサービス、またはその両方）が自動的にリストアされます。
- 現在ユーザ認証にディレクトリサービスが設定されている場合は、SAMLによって上書きされます。
- SAMLを設定すると、次のクライアントがストレージアレイリソースにアクセスできなくなります。
  - Enterprise Management Window（EMW）
  - コマンドラインインターフェイス（ CLI ）
  - ソフトウェア開発キット（SDK）クライアント
  - インバンドクライアント
  - HTTPベーシック認証REST APIクライアント
  - 標準のREST APIエンドポイントを使用してログインします

監査ログにはどのようなタイプのイベントが記録されますか？

監査ログには、変更イベント、または変更イベントと読み取り専用イベントの両方を記録できます。

ポリシー設定に応じて、次のタイプのイベントが表示されます。

- 変更イベント--ストレージのプロビジョニングなど、システムへの変更を含む、System Manager内からのユーザーアクション。
- 変更イベントおよび読み取り専用イベント--システムへの変更を伴うユーザー操作、およびボリューム割り当ての表示やダウンロードなどの情報を含むイベント。

syslogサーバを設定するときは、どのような点に注意する必要がありますか？

監査ログは外部syslogサーバにアーカイブできます。

syslogサーバを設定する際は、次のガイドラインに注意してください。

- サーバのアドレス、プロトコル、ポート番号を確認しておきます。サーバアドレスは、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスのいずれかで指定できます。
- サーバがセキュアなプロトコル（TLSなど）を使用している場合は、ローカルシステムに認証局（CA）証明書が配置されている必要があります。CA証明書がWebサイトの所有者を識別することにより、サーバとクライアントの間のセキュアな接続が確立さ

- 設定が完了すると、以降すべての監査ログがsyslogサーバに送信されるようになります。以前のログは転送されません。
- *Overwrite Policy*設定（View/Edit Settingsで利用可能）は、ログがsyslogサーバ設定でどのように管理されるかに影響しません。
- 監査ログは、RFC 5424のメッセージ形式に従います。

syslogサーバが監査ログを受信しなくなりました。どうすればよいですか？

syslogサーバにTLSプロトコルを設定している場合、何らかの理由で証明書が無効になるとサーバはメッセージを受信できなくなります。無効な証明書に関するエラーメッセージが監査ログに記録されます。

この問題 を解決するには、syslogサーバの証明書を修正する必要があります。有効な証明書チェーンが確立されたら、メニューに移動します。Settings [Audit Log]> Configure Syslog Servers > Test All]。

証明書

概念

CA証明書の仕組み

認証局（CA）は、インターネットセキュリティのためにデジタル証明書と呼ばれる電子文書を発行する信頼されたエンティティです。証明書でWebサイトの所有者を識別することにより、クライアントとサーバの間のセキュアな接続が確立されます。

ブラウザを開いてコントローラの管理ポート経由でSystem Managerに接続しようとすると、ストレージアレイのコントローラが信頼できるソースであるかどうかが確認されます。コントローラのデジタル証明書が見つからない場合、ブラウザは認識された権限で署名されていないことを警告し、続行するかどうかを確認するメッセージを表示します。このアラートが表示されないようにするには、署名入りのデジタル証明書をCAから取得する必要があります。

ドライブセキュリティ機能を持つ外部キー管理サーバを使用している場合は、そのサーバとコントローラの間の認証用の証明書を作成することもでき、また、ストレージアレイの自己署名証明書を使用することもできます。

信頼できる認証局のデジタル証明書を使用するには、次の手順が必要です。

1. メニュー「Settings [Certificates]」に移動します。ユーザーログインにはSecurity Admin権限が含まれている必要があります。含まれていない場合、* Certificates *がページに表示されません。
2. コントローラごと、またはキー管理サーバ用に、証明書署名要求（CSR）を作成します。
3. CSRファイルをCAに送信し、証明書が送信されるまで待ちます。
4. 信頼できる（中間およびルート）証明書をCAからインポートします。これらの証明書は、CA階層の信頼ポイントを確立します。
5. 各コントローラまたはキー管理サーバの署名入りの管理証明書をインポートします。

ストレージアレイに関連する証明書の用語を次に示します。

期間	説明
できます	認証局（CA）は、インターネットセキュリティのためにデジタル証明書と呼ばれる電子文書を発行する信頼されたエンティティです。証明書でWebサイトの所有者を識別することにより、クライアントとサーバの間のセキュアな接続が確立されます。
CSR	証明書署名要求（CSR）は、申請者から認証局（CA）に送信されるメッセージです。CSRは、CAが証明書の問題 に必要な情報を検証します。
証明書	証明書はセキュリティ上の目的でサイトの所有者を識別するもので、攻撃者による偽装を防止します。証明書には、サイトの所有者に関する情報と、その情報について証明（署名）する信頼されたエンティティのIDが含まれます。
クライアント証明書	セキュリティキー管理のために、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、キー管理サーバがコントローラのIPアドレスを信頼できるようにします。
キー管理サーバ証明書	セキュリティキー管理のために、キー管理サーバ証明書はサーバを検証し、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します。
管理証明書	管理証明書は、認証局（CA）によって承認され、Webアプリケーションへのセキュアなアクセスを許可します。「署名済み証明書」とも呼ばれます。
OCSPサーバ	Online Certificate Status Protocol（OCSP）サーバは、スケジュールされた有効期限の前に認証局（CA）が証明書を失効させたかどうかを確認し、証明書が失効している場合はユーザがサーバにアクセスできないようにします。
自己署名証明書	自己署名証明書はコントローラに事前にロードされています。サイト接続が自己署名されている場合、Webアプリケーションに進む前に警告メッセージが表示されます。

期間	説明
信頼された証明書	認証局（CA）が発行した信頼された証明書は、証明書階層の最上位にある既知の証明書です。「ルート証明書」とも呼ばれます。

方法

コントローラの**CA**証明書署名要求（**CSR**）を作成します

ストレージアレイのコントローラの認証局（CA）証明書を受け取るには、まずストレージアレイ内のコントローラごとに証明書署名要求（CSR）ファイルを生成する必要があります。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。

このタスクについて

このタスクでは、コントローラの署名付き管理証明書を受け取るためにCAに送信する.CSRファイル（証明書署名要求）を生成する方法について説明します。組織に関する情報とともに、コントローラのIPアドレスまたはDNS名を指定する必要があります。このタスクでは、ストレージアレイにコントローラが1つしかない場合は.CSRファイルが1つ、コントローラが2つある場合は2つ生成されます。

手順

1. メニューから[設定][証明書]を選択します。
2. [アレイ管理]タブで、[* CSR全体*]を選択します。

   2台目のコントローラの自己署名証明書を受け入れるよう求めるダイアログボックスが表示された場合は、*自己署名証明書を受け入れる*をクリックして続行します。

3. 次の情報を入力し、[次へ*]をクリックします。
   - 組織--会社または組織の正式名称。Inc.やCorp.などの接尾辞も含めて入力してください
   - 組織単位（オプション）--証明書を処理している組織の部門。
   - 市区町村--ストレージアレイまたは事業の所在地である市区町村。
   - 都道府県（オプション）-ストレージアレイまたは事業の所在地である都道府県。
   - 国の**ISO**コード--自国を表す2桁のISO（国際標準化機構）コード（USなど）。

   一部のフィールドには、コントローラのIPアドレスなどの適切な情報があらかじめ入力されています。事前入力された値は、明らかな間違いでないかぎり変更しないでください。たとえば、CSRをまだ作成していない場合、コントローラのIPアドレスは「localhost」に設定されます。 この場合は、「localhost」をコントローラのDNS名またはIPアドレスに変更する必要があります。

4. ストレージアレイ内のコントローラAに関する次の情報を確認または入力します。

- コントローラ**A**の共通名--コントローラAのIPアドレスまたはDNS名がデフォルトで表示されますこのアドレスが正しいことを確認してください。ブラウザでSystem Managerにアクセスする際に入力したアドレスと正確に一致している必要があります。
- コントローラ**A**の代替**IP**アドレス-共通名がIPアドレスの場合は、コントローラAの追加のIPアドレスまたはエイリアスをオプションで入力できます複数指定する場合は、カンマで区切って入力します。
- コントローラ**A**の代替**DNS**名--共通名がDNS名の場合は、コントローラAの追加のDNS名を入力します複数指定する場合は、カンマで区切って入力します。代替DNS名がない場合は、最初のフィールドに入力したDNS名をここにコピーします。ストレージアレイにコントローラが1台しかない場合は、「完了」ボタンを使用できます。ストレージアレイにコントローラが2台ある場合は、* Next *ボタンを使用できます。

> CSR要求を最初に作成するときは、[この手順をスキップ]リンクをクリックしないでください。このリンクは、エラーからリカバリする場合に使用します。CSR要求が一方のコントローラで失敗し、もう一方のコントローラで失敗することがあります。このリンクを使用すると、コントローラAでCSRがすでに定義されている場合はその作成をスキップし、コントローラBでCSRを再作成する次の手順に進むことができます

5. コントローラが1台しかない場合は、[完了]をクリックします。コントローラが2台ある場合は、[次へ]をクリックしてコントローラBの情報を入力し（上記と同じ）、[完了]をクリックします。

   シングルコントローラの場合は、1つの.CSRファイルがローカルシステムにダウンロードされます。デュアルコントローラの場合は、2つの.CSRファイルがダウンロードされます。ダウンロードフォルダの場所は、ブラウザによって異なります。

6. .CSRファイルをCAに送信します。

完了後

デジタル証明書を受け取ったら、CAから送られてきた該当する証明書ファイルをインポートします。

コントローラの信頼された証明書をインポートする

認証局（CA）からデジタル証明書を受け取ったら、コントローラの証明書チェーン（中間およびルート）をインポートできます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。
- 証明書署名要求（.CSRファイル）を生成してCAに送信しておきます。
- 信頼された証明書ファイルをCAから受け取っておきます。
- 証明書ファイルがローカルシステムにインストール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、ストレージアレイのコントローラ用に信頼された証明書をアップロードする方法について説明します。

手順

1. メニューから[設定][証明書]を選択します。
2. [**Trusted**]タブで、[**Import**]を選択します。

信頼された証明書ファイルをインポートするためのダイアログボックスが表示されます。

3. Browse（参照）*をクリックして、コントローラの証明書ファイルを選択します。

   ダイアログボックスにファイル名が表示されます。

4. [* インポート *] をクリックします。

結果

ファイルがアップロードされて検証されます。

完了後

管理証明書をインポートします。

コントローラの管理証明書をインポートします

信頼された証明書チェーンをインポートしたら、ストレージアレイ内の各コントローラの管理（署名済み）証明書ファイルをインポートします。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。
- 信頼された証明書がインポートされている。
- 各コントローラの管理証明書ファイルがCAから返されている必要があります。
- 管理証明書ファイルがローカルシステム上にある必要があります。

このタスクについて

このタスクでは、コントローラ認証用に管理証明書ファイルをアップロードする方法について説明します。

手順

1. メニューから[設定][証明書]を選択します。
2. [* Array Management*（アレイ管理*）]タブで、[* Import*（インポート*）]を選択し

   証明書ファイルをインポートするためのダイアログボックスが表示されます。

3. [**Browse**]をクリックして、コントローラAのファイルを選択しますコントローラが2台ある場合は、2番目の* Browse *ボタンをクリックして、コントローラBのファイルを選択します

   ファイル名がダイアログボックスに表示されます。

4. [* インポート *] をクリックします。

   ファイルがアップロードされて検証されます。

結果

セッションは自動的に終了します。証明書を有効にするには、再度ログインする必要があります。再度ログインすると、新しいCA署名証明書がセッションに使用されます。

インポートされた証明書の情報を表示

[証明書]ページでは、証明書の種類、発行機関、および以前にインポートした証明書の有効な日付範囲を表示できます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。

このタスクについて

このタスクでは、ユーザがインストールした証明書または事前にインストールされた証明書の情報を表示する方法について説明します。

手順

1. メニューから[設定][証明書]を選択します。
2. いずれかのタブを選択して、コントローラの管理証明書、信頼された証明書、およびキー管理サーバの証明書に関する情報を表示します。

タブをクリックする	説明
アレイ管理	コントローラ用にインポートしたすべてのサーバ証明書に関する情報が表示されます。
高い信頼性	コントローラ用にインポートしたすべての信頼された（ルート）証明書に関する情報が表示されます。[Show certificates that are …]の下のフィルタフィールドを使用して、ユーザがインストールした証明書または事前にインストールされた証明書を表示します。 • ユーザーがインストールしたもの。ユーザがストレージアレイにアップロードした証明書（信頼された証明書、LDAPS証明書、アイデンティティフェデレーション証明書が含まれます）。 • プリインストール。ストレージアレイに付属の証明書。
キー管理	外部キー管理サーバ用にインポートしたすべての管理（署名済み）証明書に関する情報が表示されます。

信頼された証明書を削除する

ユーザがインポートした証明書を削除することができます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。
- 信頼された証明書を新しいバージョンに更新する場合は、古い証明書を削除する前に更新された証明書をインポートする必要があります。

ストレージアレイの管理証明書またはLDAPサーバの認証に使用していた証明書を新しい証明書をインポートする前に削除すると、システムにアクセスできなくなることがあります。

このタスクについて

このタスクでは、ユーザがインポートした証明書を削除する方法について説明します。事前定義された証明書は削除できません。

手順

1. メニューから[設定][証明書]を選択します。
2. [**Trusted**]タブを選択します。

   ストレージアレイの信頼された証明書が表に表示されます。
3. 削除する証明書を表から選択します。
4. [メニュー]、[一般的ではないタスク]、[削除]の順にクリック

   [信頼された証明書の削除の確認]ダイアログボックスが開きます。
5. フィールドに「delete」と入力し、「* Delete *」をクリックします。

管理証明書をリセットします

ストレージアレイの管理証明書を工場出荷時の自己署名証明書の状態に戻すことができます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。
- 証明書をインポートしておく必要があります。

このタスクについて

ストレージアレイにある管理証明書をリセットすると、現在の管理証明書が各コントローラから削除されます。証明書のリセット後、コントローラでは自己署名証明書が再び使用されるようになります。

手順

1. メニューから[設定][証明書]を選択します。
2. [* Array Management*（アレイ管理）]タブで、[* Reset*（リセット）]を選択します。

   [管理証明書のリセットの確認]ダイアログボックスが開きます。
3. フィールドに「reset」と入力し、「* Reset *」をクリックします。

結果

ブラウザをリフレッシュすると、コントローラでは自己署名証明書が再び使用されるようになります。そのため、セッションの自己署名証明書を手動で承認するように求められます。

キーサーバの**CA**証明書署名要求（**CSR**）を実行します

キー管理サーバの認証局（CA）証明書を受け取るには、まず証明書署名要求（CSR）ファイルを生成する必要があります。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。

このタスクについて

このタスクでは、キー管理サーバの署名済み証明書を受け取るためにCAに送信する.CSRファイル（証明書署名要求）を生成する方法について説明します。このタスクでは、組織に関する情報を指定する必要があります。

手順

1. メニューから[設定][証明書]を選択します。
2. [キー管理]タブで、[* CSR全体*]を選択します。
3. 次の情報を入力します。
   - 共通名--証明書ファイルに表示されるストレージアレイ名など、このCSRを識別する名前。
   - 組織--会社または組織の正式名称。Inc.やCorp.などの接尾辞も含めて入力してください
   - 組織単位（オプション）--証明書を処理している組織の部門。
   - 市区町村--組織の所在地である市区町村。
   - 都道府県**(**オプション**)**--組織の所在地である都道府県。
   - 国の**ISO**コード--組織の所在地である米国などの2桁のISO（国際標準化機構）コード。
4. [* ダウンロード] をクリックします。
5. .CSRファイルをCAに送信します。

完了後

キー管理サーバからクライアント証明書とサーバ証明書を取得したら、ストレージアレイコントローラで認証するためにそれらの証明書をインポートします。

キー管理サーバ証明書をインポート

外部キー管理のために、ストレージアレイとキー管理サーバが互いに信頼関係を確立できるように、2つのエンティティの間の認証用に証明書をインポートします。証明書には2種類あります。クライアント証明書はコントローラを検証し、キー管理サーバ証明書はサーバを検証します。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。
- ストレージアレイでクライアント証明書を使用できる必要があります。

クライアント証明書は、キー管理サーバがコントローラのIPアドレスを信頼できるよう、ストレージアレイのコントローラを検証します。クライアント証明書を取得するには、ストレージアレイのCSRを作成して、キー管理サーバにアップロードする必要があります。サーバから、クライアント証明書を生成します。

- キー管理サーバ証明書が必要です。

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、サーバを検証します。キー管理サーバ証明書を取得するには、キー管理サーバから生成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、ストレージアレイコントローラとキー管理サーバの間の認証用に証明書ファイルをアップロードする方法について説明します。

手順

1. メニューから[設定][証明書]を選択します。
2. [キー管理]タブで、[インポート]を選択します。

   証明書ファイルをインポートするためのダイアログボックスが表示されます。
3. ファイルを選択するには、*参照*ボタンをクリックします。

   ダイアログボックスにファイル名が表示されます。
4. [* インポート *] をクリックします。

   ファイルがアップロードされて検証されます。

キー管理サーバ証明書をエクスポートする

キー管理サーバ用の証明書をローカルマシンに保存できます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。
- 証明書をインポートしておく必要があります。

手順

1. メニューから[設定][証明書]を選択します。
2. [キー管理（Key Management *）]タブを選択します。
3. 表からエクスポートする証明書を選択し、* Export *（エクスポート）をクリックします。

   [保存（Save）]ダイアログボックスが開きます。
4. ファイル名を入力し、*保存*をクリックします。

証明書失効チェックを有効にします

失効した証明書の自動チェックを有効にして、Online Certificate Status Protocol（OCSP）サーバがユーザによるセキュアでない接続をブロックするようにすることができます。自動失効チェックは、認証局（CA）が発行した証明書に問題がある場合や、秘密鍵が漏えいした場合に役立ちます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。
- 両方のコントローラにDNSサーバが設定されている必要があります。これにより、OCSPサーバの完全修飾ドメイン名が使用できるようになります。このタスクはハードウェアページから実行できます。
- 独自のOCSPサーバを指定する場合は、そのサーバのURLを確認しておく必要があります。

このタスクについて

このタスクでは、OCSPサーバを設定するか、証明書ファイルに指定されているサーバを使用することができます。OCSPサーバは、スケジュールされた有効期限よりも前にCAによって失効された証明書がないかを判断し、証明書が失効している場合は、ユーザによるサイトへのアクセスをブロックします。

手順

1. メニューから[設定][証明書]を選択します。
2. [**Trusted**]タブを選択します。

   失効チェックは、[キー管理]タブから有効にすることもできます。

3. [一般的でないタスク]をクリックし、ドロップダウンメニューから[失効チェックを有効にする*]を選択します。
4. 「失効チェックを有効にする」を選択して、チェックボックスにチェックマークが表示され、ダイアログボックスに追加のフィールドが表示されるようにします。
5. [* OCSPレスポンダのアドレス*]フィールドに、OCSPレスポンダサーバのURLをオプションで入力できます。アドレスを入力しない場合は、証明書ファイルで指定されているOCSPサーバのURLが使用されます。
6. [アドレスのテスト*]をクリックして、指定したURLへの接続をシステムがオープンできることを確認します。
7. [保存（ Save ）] をクリックします。

結果

証明書が失効しているサーバにストレージアレイが接続しようとすると、接続は拒否され、イベントがログに記録されます。

よくある質問です

Cannot Access Other Controllerダイアログボックスが表示されるのはなぜですか。

CA証明書に関連する特定の処理（証明書のインポートなど）を実行すると、2台目のコントローラの自己署名証明書を受け入れるよう求めるダイアログボックスが表示される

ことがあります。

2台のコントローラを搭載したストレージアレイ（デュプレックス構成）では、SANtricity System Managerが2台目のコントローラと通信できない場合、または処理の特定の段階でブラウザが証明書を受け入れられない場合に、このダイアログボックスが表示されることがあります。

このダイアログボックスが表示された場合は、[自己署名証明書を承認する]をクリックして続行します。パスワードの入力を求めるダイアログボックスが表示された場合は、System Managerへのアクセスに使用する管理者パスワードを入力します。

このダイアログボックスが再び表示され、証明書のタスクを完了できない場合は、次のいずれかの手順を実行してください。

- 別のブラウザを使用してこのコントローラにアクセスし、証明書を受け入れて続行します。
- System Managerを使用して2台目のコントローラにアクセスし、自己署名証明書を受け入れてから、1台目のコントローラに戻って続行します。

System Managerにアップロードする必要がある証明書を確認するにはどうすればよいですか？

外部キー管理では、ストレージアレイとキー管理サーバが互いに信頼関係を確立できるように、2つのエンティティの間の認証用に2種類の証明書をインポートします。

クライアント証明書は、キー管理サーバがコントローラのIPアドレスを信頼できるよう、ストレージアレイのコントローラを検証します。クライアント証明書を取得するには、ストレージアレイのCSRを作成して、キー管理サーバにアップロードする必要があります。サーバから、クライアント証明書を生成し、System Managerを使用してインポートします。

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、キー管理サーバを検証します。キー管理サーバ証明書を取得するには、キー管理サーバから生成する必要があります。

証明書失効チェックについて、どのような点に注意する必要がありますか？

System Managerでは、証明書失効リスト（CRL）をアップロードする代わりに、Online Certificate Status Protocol（OCSP）サーバを使用して失効した証明書をチェックできます。

失効した証明書は信頼しないようにしてください。証明書が失効する理由はいくつかあります。たとえば、認証局（CA）から証明書が適切に発行されていない、秘密鍵が不正に使用された、特定されたエンティティがポリシーの要件を満たしていない、などの場合です。

System ManagerでOCSPサーバへの接続を確立すると、ストレージアレイは、AutoSupport サーバ、外部キー管理サーバ（EKMS）、Lightweight Directory Access Protocol over SSL（LDAPS）サーバ、またはsyslogサーバに接続するたびに失効チェックを実行します。ストレージアレイは、これらのサーバの証明書の検証を試行して、証明書が失効していないことを確認します。その証明書について、サーバから「good」、「revoked」「unknown」のいずれかの値が返されます。証明書が失効している場合や、アレイがOCSPサーバにアクセスできない場合は、接続が拒否されます。

System ManagerまたはコマンドラインインターフェイスCLI）で指定したOCSPレスポンダアドレスは、証明書ファイル内のOCSPアドレスよりも優先されます。

失効チェックが有効になるのはどのタイプのサーバですか？

ストレージアレイは、AutoSupport サーバ、外部キー管理サーバ（EKMS
）、Lightweight Directory Access Protocol over SSL（LDAPS）サーバ、またはsyslogサーバに接続するたびに失効チェックを実行します。

著作権に関する情報

商標に関する情報