



Unified Manager の略

SANtricity 11.6

NetApp
February 12, 2024

目次

Unified Manager の略	1
メインインターフェイス	1
管理	4
証明書と認証	44

Unified Manager の略

メインインターフェイス

Unified Managerの概要

概念

インターフェイスの概要

Unified ManagerはWebベースのインターフェイスであり、1つのビューで複数のストレージアレイを管理することができます。

メインページ

Unified Managerにログインすると、メインページが開き、* Manage-All *が表示されます。このページから、ネットワーク内で検出されたストレージアレイのリストをスクロールして、そのステータスを表示し、1つのアレイまたはアレイグループに対して処理を実行できます。

ナビゲーションサイドバー

ナビゲーションサイドバーには次の情報が表示されます。

- 管理--ネットワーク内のストレージアレイの検出、アレイのSANtricity System Managerの起動、1つのアレイから複数のアレイへの設定のインポート、アレイグループの管理を行います。設定のインポートやアレイグループの作成など、アレイに対する処理を実行するには、アレイ名の横にあるチェックボックスを選択します。各行の最後にある省略記号には'名前の変更など'1つのアレイでの操作を実行するためのインラインメニューがあります
- オペレーション--あるアレイから別のアレイへの設定のインポートなど'バッチ操作の進行状況を表示します



ストレージアレイのステータスが最適でない場合は、一部の処理は使用できません。

- 証明書管理--ブラウザとクライアント間の認証に使用する証明書を管理します
- アクセス管理-- Unified Managerインターフェイスのユーザ認証を確立します。
- サポート--テクニカルサポートのオプション、リソース、連絡先を表示します。

バナー機能

上部のバナーから、Unified Managerインターフェイスのヘルプやその他のドキュメントにアクセスできます。ログイン名の横にあるドロップダウンから管理オプションにアクセスすることもできます。

サポートされているブラウザ

SANtricity Unified Managerには、いくつかの種類のブラウザからアクセスできます。

サポートされるブラウザとバージョンを次に示します。

ブラウザ	最小バージョン
Google Chrome	47
Microsoft Internet Explorer の略	11.
Microsoft Edge の場合	EdgeHTML 12
Mozilla Firefox	31.
Safari	9.



Web Services Proxyをインストールしてブラウザから使用できるようにしておく必要があります。

Unified Managerの管理

概念

管理者パスワードによる保護

SANtricity Unified Managerには、不正なアクセスを防ぐために管理者パスワードを設定する必要があります。

管理者パスワードの設定

管理者パスワードを設定すると、偶然または悪意を持ってシステムの停止を招くコマンドを実行するユーザからソフトウェアを保護できます。管理者パスワードは、Unified Managerを初めて起動するときに設定する必要があります。

すべてのユーザで共有する管理者パスワードが1つあります。このパスワードを持つユーザは、ストレージシステムの構成を変更できます。

パスワードを入力します

1つの管理セッションでパスワードの入力を求められるのは1回のみです。デフォルトでは操作がない状態が30分続くとセッションがタイムアウトし、パスワードをもう一度入力する必要があります。必要に応じて、セッションタイムアウトを調整できます。

セッション中に別の管理クライアントから同じソフトウェアにアクセスしている別のユーザがパスワードを変更した場合は、次の設定処理や表示処理でパスワードの入力を求められます。

セキュリティ上の理由から、パスワードの入力を試行できるのは5回までとなっており、この回数を超えると、ソフトウェアは「ロックアウト」状態になります。この状態では、ソフトウェアはその後のパスワード入力を拒否します。パスワードを再度入力するには、「通常」状態にリセットされるまで10分待つ必要があります。

方法

adminパスワードを変更

SANtricity Unified Managerへのアクセスに使用する管理者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。
- 現在の管理者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。

- 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。

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. 表から* admin *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]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に対して最小文字数が設定されていない場合は、システムにアクセスするユーザにパスワードの入力を求めるチェックボックスを選択します。
6. 2つのフィールドに新しいパスワードを入力します。
7. この操作を確認するためにローカル管理者パスワードを入力し、*変更*をクリックします。

ストレージレイのパスワードを変更する

SANtricity Unified Managerでストレージレイを表示したりアクセスしたりするときに使用するパスワードを更新できます。

作業を開始する前に

- Storage 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。
- SANtricity System Managerで設定されているストレージレイの現在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

このタスクでは、Unified Managerからストレージアレイにアクセスできるようにストレージアレイの現在のパスワードを入力します。これは、System Managerでアレイのパスワードが変更されたために、Unified Managerでも変更が必要になった場合などに行います。

手順

1. [* Manage * (管理)]ページで、1つ以上のストレージ・アレイを選択します。
2. [メニュー]：[一般的でないタスク][ストレージアレイパスワードの入力]を選択します。
3. 各ストレージアレイのパスワードを入力し、*保存*をクリックします。

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 Unified 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、Unified 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。

手順

1. メニューバーで、ユーザログイン名の横にあるドロップダウン矢印を選択します。
2. 「セッションタイムアウトを有効/無効にする」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。

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*チェックボックスをオフにします。

4. [保存 (Save)]をクリックします。

管理

ストレージアレイを検出

概念

アレイの検出に関する考慮事項

SANtricity Unified Managerでストレージリソースを表示して管理するには、組織のネットワークから管理対象のストレージアレイを検出する必要があります。複数のアレイを検出することも、単一のアレイを検出することもできます。

複数のストレージアレイを検出しています

複数のアレイを検出する場合は、ネットワークIPアドレスの範囲を入力すると、その範囲の各IPアドレスへの接続がUnified Managerで個別に試行されます。到達したストレージアレイが* Discover *ページに表示され、管理ドメインに追加される可能性があります。

単一のストレージアレイを検出しています

単一のアレイを検出する場合は、ストレージアレイのいずれかのコントローラのIPアドレスを1つ入力すると、そのストレージアレイが追加されます。



Unified Managerは、あるコントローラに割り当てられている1つのIPアドレスまたは範囲内のIPアドレスのみを検出して表示します。代替のコントローラまたはそれらのコントローラに割り当てられているIPアドレスがあっても、この1つのIPアドレスまたはIPアドレス範囲に含まれていなければ、Unified Managerでは検出または表示されません。ただし、ストレージアレイを追加すると、関連付けられているすべてのIPアドレスが検出され、* Manage *ビューに表示されます。

ユーザクレデンシャル

検出プロセスでは、追加する各ストレージアレイの管理者パスワードが必要になります。

Webサービスの証明書

検出プロセスでは、検出されたストレージアレイに信頼できるソースからの証明書があるかどうかUnified Managerで確認されます。Unified Managerでは、ブラウザで確立するすべての接続に対して2種類の証明書ベースの認証を使用します。

- 信頼された証明書

Unified Managerで検出されたアレイについては、認証局が発行する信頼された証明書が追加で必要となる場合があります。

これらの証明書をインポートするには、* Import *ボタンを使用します。このアレイに前に接続したことがある場合は、一方または両方のコントローラの証明書が期限切れになっているか、失効しているか、証明書チェーンにルート証明書または中間証明書がない可能性があります。ストレージアレイの管理を開始する前に、期限切れまたは失効した証明書を差し替えるか、不足しているルート証明書または中間証明書を追加する必要があります。

- 自己署名証明書

自己署名証明書を使用することもできます。署名済みの証明書をインポートせずにアレイを検出しようとすると、Unified Managerにエラーダイアログボックスが表示されます。このダイアログボックスで自己署名証明書を承認することができます。自己署名証明書が信頼済みとしてマークされ、Unified Managerにストレージアレイが追加されます。

ストレージアレイへの接続を信頼しない場合は、Unified Managerにストレージアレイを追加する前に* Cancel *を選択し、ストレージアレイのセキュリティ証明書戦略を検証します。

方法

複数のストレージアレイを検出する

複数のアレイの検出では、管理サーバが配置されているサブネット全体からすべてのストレージアレイを検出し、検出されたアレイを管理ドメインに自動的に追加します。

このタスクについて

複数のアレイを検出するには、次の手順を実行します。

手順1：ネットワークアドレスを入力する

ローカルのサブネットワーク全体を検索するには、ネットワークアドレス範囲を入力します。到達したストレージアレイが* Discover *ページに表示され、管理ドメインに追加される可能性があります。

このタスクについて

何らかの理由で検出操作を停止する必要がある場合は、*検出の停止*をクリックします。

手順

1. [* Manage（管理）]ページで、[Add/Discover*（追加/検出*）]を選択します。

ストレージアレイの追加と検出ダイアログが表示されます。

2. [ネットワーク範囲内のすべてのストレージアレイを検出する]ラジオボタンを選択します。
3. 開始ネットワークアドレスと終了ネットワークアドレスを入力して、ローカルサブネットワーク全体を検索し、*検出の開始*をクリックします。

検出プロセスが開始されます。この検出プロセスが完了するまでに数分かかることがあります。ストレージアレイが検出されると、* Discover *ページのテーブルにデータが表示されます。



管理可能なアレイが検出されない場合は、ストレージアレイがネットワークに適切に接続されていて、割り当てられたアドレスが範囲内にあることを確認してください。「新しい検出パラメータ」をクリックして、「追加/検出」ページに戻ります。

4. 検出されたストレージアレイのリストを確認します。
5. 管理ドメインに追加するストレージアレイの横にあるチェックボックスをオンにし、[次へ]をクリックします。

管理ドメインに追加する各アレイについて、SANtricity Unified Managerでクレデンシャルのチェックが実行されます。そのアレイに関連付けられている自己署名証明書や信頼されていない証明書の解決が必要になる場合があります。

6. 「* 次へ *」をクリックして、ウィザードの次の手順に進みます。
7. に進みます [\[手順2：検出時に自己署名証明書を解決する\]](#)。

手順2：検出時に自己署名証明書を解決する

検出プロセスでは、ストレージアレイに信頼できるソースからの証明書があるかどうかを確認されます。

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。

手順

1. 次のいずれかを実行します。
 - 検出されたストレージレイへの接続を信頼する場合は、ウィザードの次のカードに進みます。自己署名証明書は信頼済みとしてマークされ、SANtricity Unified Managerにストレージレイが追加されます。
 - ストレージレイへの接続を信頼しない場合は、*キャンセル*を選択し、各ストレージレイのセキュリティ証明書戦略を検証してからUnified Managerに追加してください。
2. 「*次へ*」をクリックして、ウィザードの次の手順に進みます。
3. に進みます [\[手順3：検出時に信頼されていない証明書を解決する\]](#)。

手順3：検出時に信頼されていない証明書を解決する

信頼されていない証明書の問題は、ストレージレイからSANtricity Unified Managerへのセキュアな接続を確立しようとしたときに、接続がセキュアであることが確認できないと発生します。レイの検出プロセスでは、信頼されていない証明書を解決するために、信頼できる第三者機関が発行した認証局（CA）証明書（CA署名証明書）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。
- ストレージレイの各コントローラの証明書署名要求（.CSRファイル）を生成してCAに送信しておく必要があります。
- 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上にある必要があります。

このタスクについて

信頼された追加のCA証明書のインストールが必要になる可能性があるのは、次のいずれかに該当する場合です。

- ストレージレイを新たに追加した。
- 一方または両方の証明書の期限が切れている。
- 一方または両方の証明書が失効している。
- 一方または両方の証明書のルート証明書または中間証明書がない。

手順

1. 信頼されていない証明書を解決するストレージレイの横にあるチェックボックスを選択し、* Import * ボタンを選択します。

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。

2. Browse（参照）*をクリックして、ストレージレイ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。

3. [* 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。



信頼されていない証明書の問題が未解決のストレージアレイはUnified Managerに追加されません。

4. 「* 次へ *」をクリックして、ウィザードの次の手順に進みます。
5. に進みます [\[手順4：パスワードを入力する\]](#)。

手順4：パスワードを入力する

管理ドメインに追加するストレージアレイのパスワードを入力する必要があります。

作業を開始する前に

- ストレージアレイが正しくセットアップおよび設定されている必要があります。
- ストレージアレイのパスワードは、SANtricity システムマネージャの*アクセス管理*タイルを使用して設定する必要があります。

手順

1. SANtricity Unified Managerに追加する各ストレージアレイのパスワードを入力します。
2. *オプション：*ストレージアレイをグループに関連付けます。ドロップダウンリストから、選択したストレージアレイに関連付ける目的のグループを選択します。
3. [完了] をクリックします。

完了後

ストレージアレイが管理ドメインに追加され、指定した場合は選択したグループに関連付けられます。



Unified Managerから指定のストレージアレイへの接続が確立されるまでに数分かかることがあります。

単一のアレイを検出します

単一ストレージアレイの追加/検出オプションを使用して、ストレージアレイを手動で検出し、組織のネットワークに追加します。

作業を開始する前に

- ストレージアレイが正しくセットアップおよび設定されている必要があります。
- ストレージアレイのパスワードは、SANtricity システムマネージャのアクセス管理タイルを使用して設定する必要があります。

手順

1. [* Manage （管理）] ページで、[Add/Discover*（追加/検出*）] を選択します。
[ストレージアレイの追加/検出*] ダイアログボックスが表示されます。
2. [Discover a single storage array] オプションボタンを選択します。
3. ストレージアレイ内のいずれかのコントローラのIPアドレスを入力し、*検出の開始*をクリックします。

SANtricity Unified Managerから指定のストレージアレイへの接続に数分かかることがあります。



指定したコントローラのIPアドレスに接続できない場合、「*ストレージアレイにアクセスできません」というメッセージが表示されます。

4. プロンプトが表示されたら、自己署名証明書を解決します。

検出プロセスでは、検出されたストレージアレイに信頼できるソースからの証明書があるかどうかを確認されます。ストレージアレイのデジタル証明書が見つからない場合、承認された認証局（CA）の署名がない証明書について、セキュリティ例外を追加して解決するように求められます。

5. 信頼されていない証明書についての確認が求められたら解決し

信頼されていない証明書の問題は、ストレージアレイからSANtricity Unified Managerへのセキュアな接続を確立しようとしたときに、接続がセキュアであることが確認できないと発生します。信頼されていない証明書を解決するには、信頼できる第三者機関から発行された認証局（CA）証明書をインポートします。

6. 「*次へ*」をクリックします。

7. *オプション：*検出されたストレージアレイをグループに関連付けます。ドロップダウンリストから、ストレージアレイに関連付ける目的のグループを選択します。

デフォルトでは、「すべて」のグループが選択されています。

8. 管理ドメインに追加するストレージアレイの管理者パスワードを入力し、* OK *をクリックします。

完了後

ストレージアレイがSANtricity Unified Managerに追加され、指定した場合は選択したグループにも追加されます。

サポートデータの自動収集が有効になっている場合は、追加したストレージアレイのサポートデータが自動的に収集されます。

を起動します

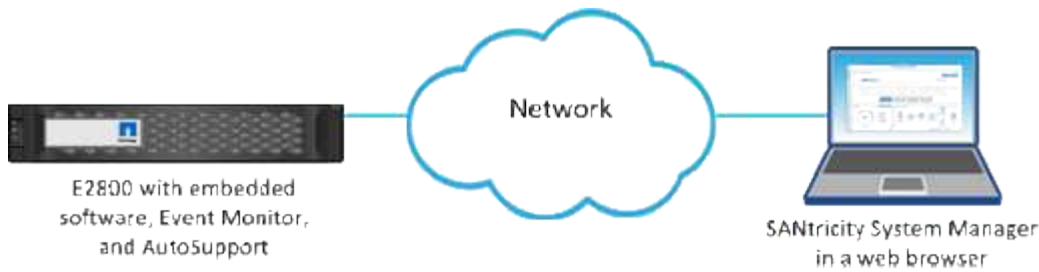
SANtricity System Managerにアクセスする際の考慮事項

ストレージアレイを設定および管理する場合は、1つ以上のストレージアレイを選択し、起動オプションを使用してSANtricity System Managerを開きます。

SANtricity System Managerは、E2800またはE5700コントローラに組み込みのアプリケーションで、イーサネット管理ポートを介してネットワークに接続されます。

SANtricity System Managerには、E2800アレイまたはE5700アレイ向けのアレイベースのすべての機能が含まれています。

SANtricity System Managerにアクセスするには、Webブラウザを使用してネットワーク管理クライアントにアウトオブバンド接続する必要があります。



個々のストレージアレイを管理します

管理操作を実行する場合は、起動オプションを使用して、1つ以上のストレージアレイのブラウザベースのSANtricity System Managerを開くことができます。

手順

1. [* Manage * (管理)] ページで、管理する1つ以上のストレージ・アレイを選択します。
2. [* 起動 *] をクリックします。

新しいウィンドウが開き、SANtricity System Managerのログインページが表示されます。

3. ユーザー名とパスワードを入力し、*ログイン*をクリックします。

設定をインポートします

概念

設定のインポートの仕組み

SANtricity Unified Managerを使用して、1つのストレージアレイから複数のストレージアレイに設定をインポートできます。設定のインポート機能は、ネットワーク内で複数のアレイを設定する必要がある場合に時間を節約するバッチ処理です。

インポートできる設定

複数のアレイにインポートできる構成は次のとおりです。

- アラート--電子メール、syslogサーバ、またはSNMPサーバを使用して、管理者に重要なイベントを送信するためのアラート方法。
- * AutoSupport *--ストレージ・アレイの状態を監視し、テクニカル・サポートに自動ディスパッチを送信する機能
- 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)を介して管理されるユーザー認証の方法。
- ストレージ構成--以下に関連する構成。
 - ボリューム (リポジトリボリュームでないシックボリュームのみ)
 - ボリュームグループとプール
 - ホットスペアドライブの割り当て
- システム設定--以下に関連する設定。

- ボリュームのメディアスキャン設定
- SSD設定
- 自動ロードバランシング（ホスト接続レポートは含まれません）

設定ワークフロー

設定をインポートするワークフローは次のとおりです。

1. ソースとして使用するストレージアレイで、SANtricity システムマネージャを使用して設定を行います。
2. ターゲットとして使用するストレージアレイで、SANtricity システムマネージャを使用して設定をバックアップします。
3. SANtricity Unified Managerの* Manage *ページに移動して、設定をインポートします。
4. [* Operations]ページで、設定のインポート操作の結果を確認します。

ストレージ構成のレプリケートに関する要件

ストレージアレイ間でストレージ構成をインポートする前に、要件およびガイドラインを確認してください。

シェルフ

- コントローラが配置されているシェルフがソースとターゲットのアレイで同一である。
- シェルフIDがソースとターゲットのアレイで同じである。
- 拡張シェルフの同一のスロットに同じドライブタイプが搭載されている必要があります（ドライブが構成で使用されている場合、未使用ドライブの場所は問題になりません）。

コントローラ

- コントローラタイプはソースとターゲットのアレイで同一である必要はない（E2800からE5700にインポートする場合など）が、RBODエンクロージャのタイプは同一である必要がある。
- ホストのDA機能を含むHICが、ソースとターゲットのアレイで同じである必要があります。
- デュプレックス構成からシンプレックス構成へのインポートはサポートされていませんが、シンプレックス構成からデュプレックス構成へのインポートは可能です。
- FDE設定はインポートプロセスに含まれない。

ステータス

- ターゲットアレイのステータスが最適である必要があります。
- ソースアレイのステータスが「最適」である必要はありません。

ストレージ

- ターゲットのボリューム容量がソースよりも大きいと、ソースとターゲットのアレイでドライブ容量が異なることがあります。（ターゲットアレイには容量の大きい新しいドライブが搭載されている場合、それらのドライブはレプリケーション処理によってボリュームに完全には構成されない可能性があります）。

- ソースアレイのディスクプールのボリュームが64TB以上の場合、ターゲットでインポートプロセスを実行できない。
- シンボリウムはインポートプロセスに含まれません。

方法

アラート設定をインポートします

ストレージアレイから別のストレージアレイにアラート設定をインポートできます。このバッチ処理により、ネットワーク内に複数のアレイを設定する必要がある場合に時間を節約できます。

作業を開始する前に

- アラートは、ソースとして使用するストレージアレイのSANtricity System Managerで設定します（メニュー：設定[アラート]）。
- ターゲットストレージアレイの既存の構成は、SANtricity システムマネージャでバックアップされます（メニュー：[設定（Settings）][システム（System）]>[ストレージアレイ構成の保存（Save Storage Array Configuration）]）。

このタスクについて

インポート処理では、Eメール、SNMP、またはsyslogのいずれかのアラートを選択できます。インポートされる設定は次のとおりです。

- ***Email alerts ***--メールサーバのアドレスとアラート受信者の電子メールアドレス。
- ***Syslogアラート***-- syslogサーバのアドレスとUDPポート。
- ***snmp alerts ***-- SNMPサーバのコミュニティ名とIPアドレス。

手順

1. [管理]ページで、[設定のインポート]をクリックします。

設定のインポート*ウィザードが開きます。

2. [設定の選択]ダイアログで、[電子メールアラート]、[* SNMPアラート*]、または[* syslogアラート*]のいずれかを選択し、[次へ]をクリックします。

ソースアレイを選択するためのダイアログボックスが開きます。

3. 「ソースの選択」ダイアログで、インポートする設定のアレイを選択し、「次へ」をクリックします。
4. [ターゲットの選択*]ダイアログで新しい設定を受信する1つまたは複数のアレイを選択します



ファームウェアが8.50未満のストレージアレイは選択できません。また、Unified Managerが通信できないアレイ（オフラインのアレイや、証明書、パスワード、ネットワークに問題があるアレイなど）は、このダイアログに表示されません。

5. [完了]をクリックします。

[オペレーション（Operations *）]ページには、インポート操作の結果が表示されます。処理が失敗した場合は、その行をクリックすると詳細を確認できます。

結果

Eメール、SNMP、またはsyslogを使用して管理者にアラートを送信するようにターゲットストレージアレイが設定されます。

AutoSupport 設定をインポートします

ストレージアレイから別のストレージアレイにAutoSupport 構成をインポートできます。このバッチ処理により、ネットワーク内に複数のアレイを設定する必要がある場合に時間を節約できます。

作業を開始する前に

- AutoSupport は、ソースとして使用するストレージアレイのSANtricity System Managerで設定します（メニュー：サポート[サポートセンター]）。
- ターゲットストレージアレイの既存の構成は、SANtricity システムマネージャでバックアップされます（メニュー：[設定（Settings）][システム（System）]>[ストレージアレイ構成の保存（Save Storage Array Configuration）]）。

このタスクについて

インポートされる設定には、個別の機能（Basic AutoSupport、AutoSupport OnDemand、Remote Diagnostics）、メンテナンス期間、配信方法、およびディスパッチスケジュール。

手順

1. [管理]ページで、[設定のインポート]をクリックします。

設定のインポート*ウィザードが開きます。

2. [設定の選択*]ダイアログで、AutoSupport]を選択し、[次へ]をクリックします。

ソースアレイを選択するためのダイアログボックスが開きます。

3. 「ソースの選択」ダイアログで、インポートする設定のアレイを選択し、「次へ」をクリックします。

4. [ターゲットの選択*]ダイアログで新しい設定を受信する1つまたは複数のアレイを選択します



ファームウェアが8.50未満のストレージアレイは選択できません。また、Unified Manager が通信できないアレイ（オフラインのアレイや、証明書、パスワード、ネットワークに問題があるアレイなど）は、このダイアログに表示されません。

5. [完了] をクリックします。

[オペレーション（Operations *）]ページには、インポート操作の結果が表示されます。処理が失敗した場合は、その行をクリックすると詳細を確認できます。

結果

ターゲットストレージアレイのAutoSupport 設定がソースアレイと同じに設定されます。

ディレクトリサービス設定をインポートします

ストレージアレイから別のストレージアレイにディレクトリサービス設定をインポート

できます。このバッチ処理により、ネットワーク内に複数のアレイを設定する必要がある場合に時間を節約できます。

作業を開始する前に

- ディレクトリサービスは、ソースとして使用するストレージアレイのSANtricity System Managerで設定します（メニュー：設定[アクセス管理]）。
- ターゲットストレージアレイの既存の構成は、SANtricity システムマネージャでバックアップされます（メニュー：[設定（Settings）][システム（System）]>[ストレージアレイ構成の保存（Save Storage Array Configuration）]）。

このタスクについて

インポートされる設定には、LDAP（Lightweight Directory Access Protocol）サーバのドメイン名とURL、およびLDAPサーバのユーザ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マッピングが含まれます。

手順

1. [管理]ページで、[設定のインポート]をクリックします。

設定のインポート*ウィザードが開きます。

2. [設定の選択*]ダイアログで、[ディレクトリサービス]を選択し、[次へ*]をクリックします。

ソースアレイを選択するためのダイアログボックスが開きます。

3. 「ソースの選択」ダイアログで、インポートする設定のアレイを選択し、「次へ」をクリックします。

4. [ターゲットの選択*]ダイアログで新しい設定を受信する1つまたは複数のアレイを選択します



ファームウェアが8.50未満のストレージアレイは選択できません。また、Unified Managerが通信できないアレイ（オフラインのアレイや、証明書、パスワード、ネットワークに問題があるアレイなど）は、このダイアログに表示されません。

5. [完了]をクリックします。

[オペレーション（Operations *）]ページには、インポート操作の結果が表示されます。処理が失敗した場合は、その行をクリックすると詳細を確認できます。

結果

ターゲットストレージアレイのディレクトリサービスがソースアレイと同じに設定されます。

システム設定をインポートします

ストレージアレイから別のストレージアレイにシステム設定をインポートできます。このバッチ処理により、ネットワーク内に複数のアレイを設定する必要がある場合に時間を節約できます。

作業を開始する前に

- ソースとして使用するストレージアレイのシステム設定をSANtricity System Managerで設定しておきます。

- ターゲットストレージレイの既存の構成は、SANtricity システムマネージャでバックアップされます（メニュー：[設定（Settings）][システム（System）]>[ストレージレイ構成の保存（Save Storage Array Configuration）]）。

このタスクについて

インポートされる設定には、ボリュームのメディアスキャン設定、コントローラのSSD設定、および自動ロードバランシングが含まれます（ホスト接続レポートは含まれません）。

手順

1. [管理]ページで、[設定のインポート]をクリックします。

設定のインポート*ウィザードが開きます。

2. [設定の選択*]ダイアログで、[システム*]を選択し、[次へ*]をクリックします。

ソースレイを選択するためのダイアログボックスが開きます。

3. 「ソースの選択」ダイアログで、インポートする設定のレイを選択し、「次へ」をクリックします。

4. [ターゲットの選択*]ダイアログで新しい設定を受信する1つまたは複数のレイを選択します



ファームウェアが8.50未満のストレージレイは選択できません。また、Unified Manager が通信できないレイ（オフラインのレイや、証明書、パスワード、ネットワークに問題があるレイなど）は、このダイアログに表示されません。

5. [完了]をクリックします。

[オペレーション（Operations *）]ページには、インポート操作の結果が表示されます。処理が失敗した場合は、その行をクリックすると詳細を確認できます。

結果

ターゲットストレージレイのシステム設定がソースレイと同じに設定されます。

ストレージ構成の設定をインポートします

ストレージレイから別のストレージレイにストレージ構成をインポートできます。このバッチ処理により、ネットワーク内に複数のレイを設定する必要がある場合に時間を節約できます。

作業を開始する前に

- ソースとして使用するストレージレイのストレージをSANtricity System Managerで設定しておきます。
- ターゲットストレージレイの既存の構成は、SANtricity システムマネージャでバックアップされます（メニュー：[設定（Settings）][システム（System）]>[ストレージレイ構成の保存（Save Storage Array Configuration）]）。
- ソースレイとターゲットレイが次の要件を満たしている必要があります。
 - コントローラが配置されているシェルフが同じである必要があります。
 - シェルフIDが同じである必要があります。
 - 拡張シェルフの同一のスロットに同じドライブタイプが搭載されている。

- RBODエンクロージャタイプが同一である。
- HICが、ホストのData Assurance機能を含めて同一である。
- ターゲットアレイのステータスが最適である必要があります。
- ターゲットアレイのボリューム容量がソースアレイよりも大きい。
- 次の制限事項を理解しておきます。
 - デュプレックス構成からシンプレックス構成へのインポートはサポートされていませんが、シンプレックス構成からデュプレックス構成へのインポートは可能です。
 - ソースアレイのディスクプールのボリュームが64TB以上の場合、ターゲットでインポートプロセスを実行できない。
 - シンボリュームはインポートプロセスに含まれません。

このタスクについて

インポートされる設定には、設定済みのボリューム（リポジトリボリュームでないシックボリュームのみ）、ボリュームグループ、プール、およびホットスペアドライブの割り当てが含まれます。

手順

1. [管理]ページで、[設定のインポート]をクリックします。

設定のインポート*ウィザードが開きます。

2. [設定の選択*]ダイアログで、[ストレージ構成*]を選択し、[次へ*]をクリックします。

ソースアレイを選択するためのダイアログボックスが開きます。

3. 「ソースの選択」ダイアログで、インポートする設定のアレイを選択し、「次へ」をクリックします。
4. [ターゲットの選択*]ダイアログで新しい設定を受信する1つまたは複数のアレイを選択します



ファームウェアが8.50未満のストレージアレイは選択できません。また、Unified Managerが通信できないアレイ（オフラインのアレイや、証明書、パスワード、ネットワークに問題があるアレイなど）は、このダイアログに表示されません。

5. [完了]をクリックします。

[オペレーション (Operations *)] ページには、インポート操作の結果が表示されます。処理が失敗した場合は、その行をクリックすると詳細を確認できます。

結果

ターゲットストレージアレイのストレージ構成がソースアレイと同じに設定されます。

よくある質問です

どの設定がインポートされますか？

設定のインポート機能は、1つのストレージアレイから複数のストレージアレイに構成をロードするバッチ処理です。この処理でインポートされる設定は、SANtricity System Managerでソースストレージアレイがどのように設定されているかによって異なります。

す。

複数のストレージアレイにインポートできる設定は次のとおりです。

- **Email alerts**--メールサーバのアドレスとアラート受信者の電子メールアドレスを設定します
- **Syslog** アラート-- syslogサーバのアドレスとUDPポートを含む設定。
- ***snmp alerts ***-- SNMPサーバのコミュニティ名とIPアドレスを含む設定。
- *** AutoSupport ***--個別の機能（Basic AutoSupport、AutoSupport OnDemand、Remote Diagnostics）、メンテナンス時間、配信方法、およびディスパッチスケジュール。
- **ディレクトリサービス**-- LDAP (Lightweight Directory Access Protocol)サーバのドメイン名とURL、およびLDAPサーバのユーザーグループとストレージアレイの定義済みロールとのマッピングが含まれます。
- **ストレージ構成**--ボリューム(リポジトリボリューム以外のシックボリュームのみ)、ボリュームグループ、プール、およびホットスペアドライブの割り当てが含まれます。
- **システム設定**--ボリュームのメディアスキャン設定、コントローラのSSDキャッシュ、および自動ロードバランシングが含まれます(ホスト接続レポートは含まれません)。

ストレージアレイが一部表示されないのはなぜですか？

設定のインポート処理の際、ターゲットの選択ダイアログボックスに一部のストレージアレイが表示されないことがあります。

ストレージアレイが表示されない理由は次のとおりです。

- ファームウェアのバージョンが8.50未満である。
- ストレージアレイがオフラインになっている。
- Unified Managerがそのアレイと通信できない（アレイに証明書、パスワード、ネットワークの問題がある場合など）。

グループの管理

概念

ストレージアレイグループ

一連のストレージアレイを1つのグループにまとめて物理インフラや仮想インフラを管理することができます。ストレージアレイをグループ化すると、ジョブの監視やレポートが簡単になります。

ストレージアレイグループには次の2種類があります。

- すべてのグループ

allグループはデフォルトのグループで、組織で検出されたすべてのストレージアレイが含まれます。Allグループには、メインビューからアクセスできます。

- ユーザが作成したグループ

ユーザが作成したグループには、そのグループに追加するように手動で選択したストレージレイが含まれます。ユーザが作成したグループには、メインビューからアクセスできます。

ストレージレイのステータス

SANtricity Unified Managerを開くと、各ストレージレイとの通信が確立され、各ストレージレイのステータスが表示されます。

ストレージレイのステータスおよびWebサービスプロキシとそのストレージレイ間の接続のステータスを表示できます。

ステータス	を示します
最適	ストレージレイが最適な状態です。証明書の問題はなく、パスワードが有効です。
パスワードが無効です	無効なストレージレイパスワードが指定されました。
信頼できない証明書です	HTTPS証明書が自己署名証明書でインポートされていないか、CA署名証明書でルート証明書と中間CA証明書がインポートされていないため、ストレージレイとの1つ以上の接続が信頼されていません。
要注意	ストレージレイにユーザによる修正操作が必要な問題があります。
ロックダウン	ストレージレイがロックダウン状態です。
不明です	ストレージレイに一度も接続していません。この状況は、Webサービスプロキシが起動中でまだストレージレイに接続していない場合や、ストレージレイがオフラインでWebサービスプロキシの起動後に一度も接続されていない場合に発生することがあります。
オフラインです	Web Services Proxyをストレージレイに接続しましたが、現在はすべての接続が失われています。

方法

グループを管理します

ストレージレイグループを作成します

ストレージグループを作成し、そのグループにストレージレイを追加します。ストレージグループでは、ボリュームを構成するストレージをどのドライブから提供するかを定義します。

手順

1. [* Manage * (管理)]ページで、[MENU: Manage Groups (グループの管理)][Create storage array group] (ストレージアレイグループの作成) を選択します
2. [名前]フィールドに、新しいグループの名前を入力します。
3. 新しいグループに追加するストレージアレイを選択します。
4. [作成 (Create)] をクリックします。

ストレージアレイグループを削除します

不要になった1つ以上のストレージアレイグループを削除することができます。

このタスクについて

この処理で削除されるのは、ストレージアレイグループだけです。削除したグループに関連付けられているストレージアレイには、Manage Allビューまたはそれに関連付けられているその他のグループからアクセスできます。

手順

1. [* Manage (管理)]ページで、[MENU: Manage Groups (グループの管理)][Delete storage array group] (ストレージアレイグループの削除) を選択します。
2. 削除するストレージアレイグループを1つ以上選択します。
3. [削除] をクリックします。 *

ストレージアレイグループの名前を変更します

現在の名前が適切でない場合は、ストレージアレイグループの名前を変更できます。

このタスクについて

これらのガイドラインに注意してください。

- 名前には、アルファベット、数字、アンダースコア (_) 、ハイフン (-) 、シャープ (#) を使用できます。他の文字を選択すると、エラーメッセージが表示されます。別の名前を選択するように求められます。
- 名前は30文字以内にしてください。名前の先頭と末尾のスペースはすべて削除されます。
- わかりやすい一意の名前を使用してください。
- わかりにくい名前は使用しないでください。

手順

1. メインビューで* Manage *を選択し、名前を変更するストレージ・アレイ・グループを選択します。
2. メニューを選択します。Manage Groups [Rename storage array group] (グループの名前変更) 。
3. [グループ名] フィールドに、グループの新しい名前を入力します。
4. *名前変更.*をクリックします

ストレージアレイをグループに追加します

ユーザが作成したグループにストレージアレイを追加することができます。

手順

1. メインビューで、* Manage *を選択し、ストレージ・アレイを追加するグループを選択します。
2. 選択メニュー：グループの管理[グループへのストレージアレイの追加]。
3. グループに追加するストレージアレイを選択します。
4. [* 追加]をクリックします。 *

グループからストレージアレイを削除します

管理対象のストレージアレイを特定のストレージグループで管理する必要がなくなった場合は、それらのストレージアレイをグループから削除することができます。

このタスクについて

グループからストレージアレイを削除しても、ストレージアレイ自体やそのデータには影響はありません。ストレージアレイをSANtricity System Managerで管理している場合は、引き続きブラウザを使用して管理できます。ストレージアレイをグループから誤って削除した場合は、再度追加することができます。

手順

1. [* Manage * (管理)]ページで、[MENU: Manage Groups (グループの管理)][グループからのストレージアレイの削除]を選択します。
2. 削除するストレージアレイが含まれているグループをドロップダウンから選択し、グループから削除する各ストレージアレイの横にあるチェックボックスをクリックします。
3. [削除 (Remove)]をクリックします。

SANtricity Unified Managerからのストレージアレイの削除

ストレージアレイをSANtricity Unified Managerで管理する必要がなくなった場合は、削除することができます。

このタスクについて

削除すると、そのストレージアレイにはアクセスできなくなります。ただし、ブラウザでIPアドレスまたはホスト名を直接指定すれば、削除したストレージアレイへの接続を確立できます。

ストレージアレイを削除しても、ストレージアレイ自体やそのデータには影響はありません。ストレージアレイを誤って削除した場合は、再度追加することができます。

手順

1. [* Manage * (管理)]ページを選択します。
2. 削除するストレージアレイを1つ以上選択します。
3. メニューから「Uncommon Tasks (一般的でないタスク)」を選択します。

ストレージアレイがSANtricity Unified Managerのすべてのビューから削除されます。

アップグレードセンター

概念

アップグレードの仕組み

SANtricity Unified Managerを使用して、同じタイプの複数のストレージアレイのSANtricity OSソフトウェアを新しいバージョンにアップグレードできます。

アップグレードワークフロー

以下に、ソフトウェアのアップグレードを実行するための大まかなワークフローを示します。

1. 最新のSANtricity OSソフトウェアファイルをサポートサイトからダウンロードします（サポート*ページのUnified Managerからリンクできます）。管理ホストシステム（ブラウザでUnified Managerにアクセスするホスト）にファイルを保存し、ファイルを解凍します。
2. Unified Managerで、SANtricity OSソフトウェアファイルとNVS RAMファイルをリポジトリ（ファイルが格納されているWebサービスプロキシサーバの領域）にロードします。ファイルは、メニューから追加できます。Upgrade Center [Upgrade SANtricity OS Software]またはメニューからアップグレードセンター[Manage Software Repository]。
3. リポジトリにファイルをロードしたら、アップグレードに使用するファイルを選択できます。SANtricity OSソフトウェアのアップグレードページ（メニュー：アップグレードセンター[Upgrade SANtricity OS software]）から、SANtricity OSソフトウェアファイルとNVS RAMファイルを選択します。ソフトウェアファイルを選択すると、互換性があるストレージアレイのリストがこのページに表示されます。次に、新しいソフトウェアでアップグレードするストレージアレイを選択します。（互換性のないアレイは選択できません）。
4. ソフトウェアの転送とアクティブ化をすぐに開始することも、ファイルをステージングしてあとでアクティブ化することもできます。アップグレードプロセスを実行すると、Unified Managerで次の処理が実行されます。
 - a. ストレージアレイの健全性チェックが実行され、アップグレードの完了の妨げとなる状況がないかどうかを確認されます。健全性チェックでいずれかのアレイに問題が見つかった場合は、そのアレイをスキップして他のアレイのアップグレードを続行するか、プロセス全体を停止して該当するアレイのトラブルシューティングを行うことができます。
 - b. 各コントローラにアップグレードファイルが転送されます。
 - c. コントローラが一度に1台ずつリブートされ、新しいSANtricity OSソフトウェアがアクティブ化されます。アクティブ化では、既存のSANtricity OSファイルが新しいファイルに置き換えられます。



ソフトウェアをあとでアクティブ化するように指定することもできます。

即時アップグレードまたは段階的アップグレード

アップグレードはただちにアクティブ化することも、ステージングしてあとでアクティブ化することもできます。あとでアクティブ化する理由は次のとおりです。

- * 時間帯 * —ソフトウェアのアクティブ化には時間がかかることがあるため、I/O 負荷の低い時間帯に実行できます。I/O負荷とキャッシュサイズによっては、コントローラのアップグレードに通常15~25分間かかることがあります。アクティブ化の際にはコントローラがリブートしてフェイルオーバーするため、アップグレードが完了するまではパフォーマンスが通常よりも低下する可能性があります。

- * パッケージのタイプ * — 他のストレージアレイ上のファイルをアップグレードする前に '新しいソフトウェアとファームウェアを 1 つのストレージアレイでテストすることをお勧めします

ステージング済みソフトウェアをアクティブにするには、メニューサポート[Upgrade Center]に移動し、SANtricity OSコントローラソフトウェアのアップグレードというラベルの付いた領域で[Activate (有効化)]をクリックします。

ヘルスチェック

健全性チェックはアップグレードプロセスの一環として実行されますが、開始する前に別途実行することもできます（メニュー：Upgrade Center [Pre-Upgrade Health Check]に移動）。

健全性チェックでは、ストレージシステムのすべてのコンポーネントについて、アップグレードを実行できる状態であるかがチェックされます。次の状況に該当する場合、アップグレードを実行できないことがあります

- 割り当てられたドライブで障害が発生し
- ホットスペアを使用中です
- 不完全なボリュームグループです
- 同時に実行できません
- ボリュームが見つからない
- コントローラのステータスが最適でない
- イベントログイベントが多すぎます
- 構成データベースの検証に失敗しました
- ドライブの DACstore のバージョンが古い

アップグレード時の考慮事項

SANtricity Unified Managerを使用して複数のストレージアレイをアップグレードする場合に、計画段階で確認が必要な考慮事項を以下に記載します。

現在のバージョン

検出された各ストレージアレイについて、Unified Managerの管理ページからSANtricity OSの現在のソフトウェアバージョンを表示できます。バージョンはSANtricity OSソフトウェア列に表示されます。各行のSANtricity OS のバージョンをクリックするとポップアップダイアログボックスが表示され、コントローラのファームウェアと NVSRAM の情報を確認できます。

アップグレードが必要なその他のコンポーネント

アップグレードプロセスの一環として、ホストがコントローラと正しく連携するように、ホストのマルチパス/フェイルオーバードライバやHBAドライバのアップグレードも必要になることがあります。

互換性の情報については、を参照してください "[NetApp Interoperability Matrix を参照してください](#)"。手順については、使用するオペレーティングシステムに対応したエクスプレスガイドを参照してください。エクスプレスガイドは、から入手できます "[Eシリーズドキュメントセンター](#)"。

デュアルコントローラ

ストレージアレイにコントローラが 2 台あり、マルチパスドライバがインストールされている場合は、アップグレードの実行中もストレージアレイで I/O の処理を継続できます。アップグレードの実行中は、次の処理が実行されます。

1. コントローラ A のすべての LUN がコントローラ B にフェイルオーバーされます
2. コントローラ A でアップグレードが実行されます
3. コントローラ A に LUN が戻され、コントローラ B の LUN もすべて移されます。
4. コントローラ B でアップグレードが実行されます

アップグレードの完了後、所有権のある正しいコントローラにボリュームが配置されるように、コントローラ間で手動でのボリュームの再配置が必要になることがあります。

方法

アップグレード前の健全性チェックを実行

健全性チェックはアップグレードプロセスの一環として実行されますが、開始前に別途実行することもできます。健全性チェックでは、ストレージアレイのコンポーネントについて、アップグレードを実行できる状態であるかがチェックされます。

手順

1. メインビューで * Manage * を選択し、メニューから Upgrade Center [Pre-Upgrade Health Check] を選択します。

[Pre-Upgrade Health Check] ダイアログ・ボックスが開き、検出されたすべてのストレージ・システムが一覧表示されます

2. 必要に応じて、ストレージシステムのリストをフィルタまたはソートして、状態が現在「最適」でないすべてのシステムを確認します。
3. 健全性チェックを実行するストレージシステムのチェックボックスを選択します。
4. [スタート] ボタンをクリックします。

健全性チェックの実行中、ダイアログボックスに進捗状況が表示されます。

5. 健全性チェックが完了したら、各行の右側にある省略記号 (...) をクリックして、詳細情報を表示したり他のタスクを実行したりできます。



健全性チェックでいずれかのアレイに問題が見つかった場合は、そのアレイをスキップして他のアレイのアップグレードを続行するか、プロセス全体を停止して該当するアレイのトラブルシューティングを行うことができます。

SANtricity OSをアップグレードします

ストレージアレイのソフトウェアとNVSRAMをアップグレードして、最新の機能とバグ修正をすべて適用します。コントローラNVSRAMは、コントローラのデフォルトの設定を指定するコントローラファイルです。

作業を開始する前に

- 最新のSANtricity OSファイルは、SANtricity WebサービスプロキシとUnified Managerが実行されているホストシステムにあります。
- ソフトウェアのアップグレードをすぐにアクティブ化するかあとでアクティブ化するかを決めます。

あとでアクティブ化する理由は次のとおりです。

- * 時間帯 * — ソフトウェアのアクティブ化には時間がかかることがあるため、I/O 負荷の低い時間帯に実行できます。アクティブ化の際にはコントローラがフェイルオーバーするため、アップグレードが完了するまではパフォーマンスが通常よりも低下する可能性があります。
- * パッケージのタイプ * -- 他のストレージアレイのファイルをアップグレードする前に '新しい OS ソフトウェア' を 1 つのストレージアレイでテストすることをお勧めします



- データ損失のリスク、ストレージアレイの損傷のリスク * — アップグレードの実行中にストレージアレイを変更しないでください。ストレージアレイの電源は切らないでください。

手順

1. ストレージアレイにコントローラが 1 台しかない場合やマルチパスドライバがインストールされていない場合は、アプリケーションエラーを回避するためにストレージアレイへの I/O アクティビティを停止します。ストレージアレイにコントローラが 2 台あり、マルチパスドライバがインストールされている場合は、I/O アクティビティを停止する必要はありません。
2. メイン・ビューから * Manage * を選択し、アップグレードするストレージ・アレイを1つ以上選択します。
3. メニューからアップグレードセンター [Upgrade SANtricity OS Software] を選択します。

SANtricity OS ソフトウェアのアップグレードページが表示されます。

4. サポートサイトからローカルマシンに最新のSANtricity OSソフトウェアパッケージをダウンロードします。
 - a. [新しいファイルをソフトウェアリポジトリに追加する *] をクリックします。
 - b. 最新の * SANtricity OS ダウンロード * を検索するためのリンクをクリックします。
 - c. [Download Latest Release] リンクをクリックします。
 - d. 以降の手順に従って、SANtricity OS ファイルと NVSRAM ファイルをローカルマシンにダウンロードします。



バージョン 8.42 以降のデジタル署名されたファームウェアが必要です。署名のないファームウェアをダウンロードしようとする、エラーが表示されてダウンロードが中止されます。

5. コントローラのアップグレードに使用する OS ソフトウェアファイルと NVSRAM ファイルを選択します。
 - a. [Select a SANtricity OS software file*] ドロップダウンから、ローカルマシンにダウンロードした OS ファイルを選択します。

使用可能なファイルが複数ある場合は、日付が新しい順にファイルがソートされます。



ソフトウェアリポジトリには、Web サービスプロキシに関連付けられているすべてのソフトウェアファイルが表示されます。使用するファイルが表示されない場合は、リンク * ソフトウェアリポジトリに新しいファイルを追加 * をクリックして、追加する OS ファイルが保存されている場所を参照します。

- a. Select an NVSRAM file * ドロップダウンから、使用するコントローラファイルを選択します。

ファイルが複数ある場合は、日付が新しい順にファイルがソートされます。

6. [Compatible Storage Array] テーブルで ' 選択した OS ソフトウェア・ファイルと互換性のあるストレージ・アレイを確認し ' アップグレードするアレイを選択します

- [管理] ビューで選択したストレージ・アレイおよび選択したファームウェア・ファイルと互換性のあるストレージ・アレイは ' デフォルトで [互換性のあるストレージ・アレイ] テーブルで選択されています
- 選択したファームウェアファイルで更新できないストレージアレイは、ステータス * incompatible * と表示される互換性があるストレージアレイテーブルで選択できません。

7. オプション：*ソフトウェアファイルをアクティブ化せずにストレージアレイに転送するには、OSソフトウェアをストレージアレイに転送し、ステージング済みとしてマークし、後でアクティブ化*チェックボックスをオンにします。

8. [スタート] ボタンをクリックします。

9. すぐにアクティブ化するかあとでアクティブ化するかに応じて、次のいずれかを実行します。

- 「 * transfer * 」と入力して、アップグレード対象として選択したアレイの OS ソフトウェアのバージョンを転送することを確認し、「 * Transfer * 」をクリックします。

転送されたソフトウェアをアクティブにするには、メニューから [Upgrade Center] [Activate Staged OS Software] を選択します。

- アップグレード対象として選択したアレイ上の OS ソフトウェアのバージョンを転送してアクティブ化することを確認するには、* upgrade * と入力し、* Upgrade * をクリックします。

アップグレード対象として選択した各ストレージアレイにソフトウェアファイルが転送され、ストレージアレイがリブートされてファイルがアクティブ化されます。

アップグレード処理では次の処理が実行されます。

- アップグレードプロセスの一環として、アップグレード前の健全性チェックが実行されます。アップグレード前の健全性チェックでは、ストレージアレイのすべてのコンポーネントについて、アップグレードを実行できる状態であるかがチェックされます。
- いずれかの健全性チェックでストレージアレイに問題が見つかった場合、アップグレードが停止します。省略符号 (...) をクリックして * ログを保存 * を選択すると、エラーを確認できます。ヘルスチェックエラーを無視するように選択し、* Continue * をクリックしてアップグレードを続行することもできます。
- アップグレード前の健全性チェックのあとに、アップグレード処理をキャンセルすることができます。

10. *オプション：*アップグレードが完了したら、省略記号 (...) をクリックし、*ログの保存*を選択すると、特定のストレージ・アレイのアップグレード内容のリストが表示されます。

ブラウザの Downloads フォルダに 'upgrade_log-<date>.json ` という名前でファイルが保存されます

ステージング済みOSソフトウェアをアクティブ化します

ソフトウェアファイルはただちにアクティブ化することも、都合のいいタイミングでアクティブ化することもできます。この手順では、ソフトウェアファイルをあとでアクティブ化するように選択した場合を想定しています。

このタスクについて

ファームウェアファイルは、アクティブ化せずに転送できます。あとでアクティブ化する理由は次のとおりです。

- *** 時間帯 ***—ソフトウェアのアクティブ化には時間がかかることがあるため、I/O 負荷の低い時間帯に実行できます。アクティブ化の際にはコントローラがリブートしてフェイルオーバーするため、アップグレードが完了するまではパフォーマンスが通常よりも低下する可能性があります。
- *** パッケージのタイプ ***—他のストレージアレイ上のファイルをアップグレードする前に '新しいソフトウェアとファームウェアを 1 つのストレージアレイでテストすることをお勧めします



起動後にアクティブ化プロセスを停止することはできません。

手順

1. メインビューで、*** Manage ***（管理）を選択します。必要に応じて、ステータス列をクリックしてページ上部の「OS Upgrade (waiting activation)」というステータスのすべてのストレージアレイをソートします。
2. ソフトウェアをアクティブ化するストレージアレイを 1 つ以上選択し、メニューから [Upgrade Center] [Activate Staged OS Software] を選択します。

アップグレード処理では次の処理が実行されます。

- アップグレード前の健全性チェックは、アクティブ化プロセスの一環として実行されます。アップグレード前の健全性チェックでは、ストレージアレイのすべてのコンポーネントについて、アクティブ化を実行できる状態であるかがチェックされます。
 - いずれかの健全性チェックでストレージアレイに問題が見つかった場合、アクティブ化は停止します。省略符号 (...) をクリックして *** ログを保存 *** を選択すると、エラーを確認できます。ヘルスチェックエラーを無視して、[*** Continue (続行) ***] をクリックしてアクティブ化を続行することもできます。
 - アップグレード前の健全性チェックのあとに、アクティブ化処理をキャンセルすることができます。アップグレード前の健全性チェックが正常に完了すると、アクティブ化が実行されます。アクティブ化にかかる時間は、ストレージアレイの構成とアクティブ化しているコンポーネントによって異なります。
3. *** オプション :** *** アクティブ化が完了すると、省略記号 (...) をクリックし、「ログを保存」を選択することにより、特定のストレージアレイに対してアクティブ化された内容のリストが表示されます。**

ブラウザの Downloads フォルダに 'activate_log-<date>.json という名前でファイルが保存されます

ソフトウェアリポジトリを管理します

ソフトウェアリポジトリには、Web サービスプロキシに関連付けられているすべてのソフトウェアファイルが表示されます。使用するファイルが表示されない場合は、ソフトウェアリポジトリの管理オプションを使用して、WebサービスプロキシとUnified

Managerが実行されているホストシステムに1つ以上のSANtricity OSファイルをインポートできます。ソフトウェアリポジトリにあるSANtricity OSファイルを削除することもできます。

作業を開始する前に

- SANtricity OSファイルを追加する場合は、ローカルシステム上にOSファイルがあることを確認します。

手順

1. メインビューから* Manage *を選択し、メニューからUpgrade Center [Manage Software Repository]を選択します。

[ソフトウェアリポジトリの管理]ダイアログが表示されます。

2. 次のいずれかを実行します。

オプション	これをしなさい...
インポート	<p>a. [インポート.]をクリックします</p> <p>b. [*参照]をクリックし、追加するOSファイルが保存されている場所に移動します。</p> <p>OSファイルのファイル名は「N2800-830000-000.dlp」のようになります。</p> <p>c. 追加するOSファイルを1つ以上選択し、*インポート*をクリックします。</p>
削除	<p>a. ソフトウェアリポジトリから削除するOSファイルを1つ以上選択します。</p> <p>b. [削除 (Delete)]をクリックします。</p>

インポートを選択した場合は、ファイルがアップロードされて検証されます。削除を選択した場合は、ファイルがソフトウェアリポジトリから削除されます。

ステージング済みOSソフトウェアをクリアします

保留中のバージョンがあとで誤ってアクティブ化されないように、ステージング済みのOSソフトウェアを削除することができます。ステージング済みOSソフトウェアを削除しても、ストレージレイで実行されている現在のバージョンには影響しません。

手順

1. メインビューから* Manage *を選択し、メニュー：Upgrade Center（アップグレードセンター）[Clear Staged OS Software]（ステージング済みOSソフトウェアのクリア）を選択します。

Clear Staged OS Software（ステージング済みOSソフトウェアのクリア）ダイアログボックスが開き、検出されたすべてのストレージシステムの中に保留中のソフトウェアまたはNVSRAMが表示されます。

2. 必要に応じて、ストレージシステムのリストをフィルタまたはソートして、ソフトウェアがステージング

済みのすべてのシステムを確認します。

3. 保留中のソフトウェアをクリアするストレージシステムのチェックボックスを選択します。
4. [クリア]をクリックします。

処理のステータスがダイアログボックスに表示されます。

ミラーリング

概念

ミラーリングの概要

Unified ManagerにはSANtricity ミラーリング機能の設定オプションが用意されており、管理者は2つのストレージレイ間でデータをレプリケートしてデータを保護できます。



この機能は、EF600またはEF300ストレージシステムでは使用できません。

ミラーリングのタイプ

SANtricity アプリケーションには、非同期と同期の2種類のミラーリングがあります。

非同期ミラーリングでは、データボリュームをオンデマンドで、またはスケジュールに基づいてコピーします。これにより、データの破損や損失が原因で発生するダウンタイムを回避または最小限に抑えることができます。非同期ミラーリングでは、特定の時点におけるプライマリボリュームの状態がキャプチャされ、前回のイメージキャプチャ以降に変更されたデータだけがコピーされます。プライマリサイトはただちに更新でき、セカンダリサイトは帯域幅に余裕があれば更新できます。情報はキャッシュされ、あとでネットワークリソースが利用可能になったときに送信されます。このタイプのミラーリングは、バックアップやアーカイブなどの定期的なプロセスに最適です。

同期ミラーリングでは、データボリュームをリアルタイムでレプリケートして、継続的な可用性を確保します。目的は、2つのストレージレイのいずれかで災害が発生した場合に重要なデータのコピーを確保しておくことで、データ損失ゼロの目標復旧時点（RPO）を達成することです。プライマリボリュームに書き込みが行われるたびにセカンダリボリュームにも書き込みが行われるため、どの時点においてもコピーは本番環境のデータと同一です。プライマリボリュームで行われた変更でセカンダリボリュームが更新されるまで、ホストは書き込みが成功したという確認応答を受信しません。このタイプのミラーリングは、ディザスタリカバリなどのビジネス継続性の確保に最適です。

ミラーリングのタイプの違い

次の表に、2種類のミラーリングの主な違いを示します。

属性	非同期	同期
レプリケーション方法	ポイントインタイム-ミラーリングはオンデマンドで、またはユーザー定義のスケジュールに従って自動的に実行されます。	連続—ミラーリングは継続して自動的に実行され、ホストに書き込みがあるたびにデータがコピーされます。

属性	非同期	同期
距離 (Distance)	アレイ間の長距離をサポートします。通常、この距離は、ネットワークとチャネル拡張テクノロジーの機能によってのみ制限されます。	アレイ間の距離は短い距離に制限されています。レイテンシおよびアプリケーションパフォーマンスの要件を満たすために、通常はローカルストレージアレイから約10km (6.2マイル) 以内の距離にする必要があります。
通信方法	標準のIPまたはFibre Channelネットワーク。	Fibre Channelネットワークのみ。
ボリュームタイプ	標準またはシン。	標準のみ。



SANtricity アプリケーションにおけるミラーリングの仕組みの詳細については、System Managerのオンラインヘルプを参照してください。

ミラーリングの設定ワークフロー

Unified Managerで非同期ミラーリングまたは同期ミラーリングを設定し、System Managerを使用して同期を管理します。

非同期ミラーリングのワークフロー

非同期ミラーリングのワークフローは次のとおりです。

1. Unified Managerで初期設定を実行します。
 - a. データ転送元としてローカルストレージアレイを選択します。
 - b. ミラー整合性グループを作成するか、既存のミラー整合性グループを選択します。ミラー整合性グループは、ローカルアレイのプライマリボリュームとリモートアレイのセカンダリボリュームのコンテナです。プライマリボリュームとセカンダリボリュームは「ミラーペア」と呼ばれます。ミラー整合性グループを初めて作成する場合は、手動同期とスケジュールされた同期のどちらを実行するかを指定します。
 - c. ローカルストレージアレイからプライマリボリュームを選択し、リザーブ容量を確認します。リザーブ容量は、コピー処理に使用される物理割り当て容量です。
 - d. 転送先としてリモートストレージアレイを選択し、セカンダリボリュームを選択して、リザーブ容量を確認します。
 - e. プライマリボリュームからセカンダリボリュームへの初回のデータ転送を開始します。ボリュームサイズによっては、この初回転送に数時間かかることがあります。
2. 初期同期の進捗状況を確認します。
 - a. Unified Managerで、ローカルアレイのSystem Managerを起動します。
 - b. System Managerで、ミラーリング処理のステータスを確認します。ミラーリングが完了すると、ミラーペアのステータスは「最適」になります。
3. *オプション：*以降のデータ転送については、System Managerでスケジュールを再設定したり、手動で実

行したりできます。新しいブロックと変更されたブロックのみがプライマリボリュームからセカンダリボリュームに転送されます。



非同期レプリケーションは定期的に行われるため、システムでは変更されたブロックを統合してネットワーク帯域幅を節約できます。書き込みスループットと書き込みレイテンシへの影響は最小限に抑えられます。

同期ミラーリングのワークフロー

同期ミラーリングのワークフローは次のとおりです。

1. Unified Managerで初期設定を実行します。
 - a. データ転送元としてローカルストレージアレイを選択します。
 - b. ローカルストレージアレイからプライマリボリュームを選択します。
 - c. データ転送先としてリモートストレージアレイを選択し、セカンダリボリュームを選択します。
 - d. 同期と再同期の優先度を選択します。
 - e. プライマリボリュームからセカンダリボリュームへの初回のデータ転送を開始します。ボリュームサイズによっては、この初回転送に数時間かかることがあります。
2. 初期同期の進捗状況を確認します。
 - a. Unified Managerで、ローカルアレイのSystem Managerを起動します。
 - b. System Managerで、ミラーリング処理のステータスを確認します。ミラーリングが完了すると、ミラーペアのステータスは「最適」になります。2つのアレイは、通常の動作を行って同期を維持しようとし、新しいブロックと変更されたブロックのみがプライマリボリュームからセカンダリボリュームに転送されます。
3. オプション： System Managerで同期設定を変更できます。



同期レプリケーションは継続的に行われるため、2つのサイト間のレプリケーションリンクで十分な帯域幅を確保する必要があります。

ミラーリングに関する用語

ストレージアレイに関連するミラーリングの用語を次に示します。

期間	説明
ローカルストレージアレイ	ローカルストレージアレイは、操作の対象となるストレージアレイです。

期間	説明
ミラー整合性グループ	<p>ミラー整合性グループは、1つ以上のミラーペアのコンテナです。非同期ミラーリング処理では、ミラー整合性グループを作成する必要があります。グループ内のすべてのミラーペアが同時に再同期されるため、一貫したリカバリポイントが維持されます。</p> <p>同期ミラーリングではミラー整合性グループを使用しません。</p>
ミラーペア	<p>ミラーペアは、プライマリボリュームとセカンダリボリュームの2つのボリュームで構成されます。</p> <p>非同期ミラーリングでは、ミラーペアは常にミラー整合性グループに属します。書き込み処理はまずプライマリボリュームに対して実行され、その後セカンダリボリュームにレプリケートされます。ミラー整合性グループ内の各ミラーペアで同じ同期設定が共有されます。</p>
プライマリボリューム	ミラーペアのプライマリボリュームは、ミラーリングするソースボリュームです。
リモートストレージアレイ	通常、リモートストレージアレイはセカンダリサイトとして指定され、セカンダリサイトにはミラーリング構成のデータのレプリカが格納されます。
リザーブ容量	<p>リザーブ容量は、コピーサービス処理やストレージオブジェクトに使用される物理割り当て容量です。ホストから直接読み取ることはできません。</p> <p>ミラーリングの動作状態を維持するために必要な情報をコントローラが永続的に保存できるようにするには、これらのボリュームが必要です。これらのボリュームには、差分ログやcopy-on-writeデータなどの情報が格納されます。</p>
セカンダリボリューム	ミラーペアのセカンダリボリュームは、通常はセカンダリサイトに配置され、データのレプリカが格納されます。
同期	同期は、ローカルストレージアレイとリモートストレージアレイの間の初期同期で実行されます。また、通信が中断されてプライマリボリュームとセカンダリボリュームが同期されていない状態になったときにも実行されます。通信リンクが再確立されると、レプリケートされていないデータがセカンダリボリュームのストレージアレイに同期されます。

ミラーリングを設定する場合は、次の要件に注意してください。

SANtricity Unified Manager の略

- Web Services Proxyサービスが実行されている必要があります。
- Unified ManagerがHTTPS接続経由でローカルホストで実行されている必要があります。
- Unified Managerにストレージレイの有効なSSL証明書が表示されている必要があります。Unified Managerのメニューから「Certificate Management」に移動し、自己署名証明書を受け入れるか、独自のセキュリティ証明書をインストールできます。

ストレージレイ



EF600ストレージレイではミラーリングを使用できません。

- 2つのストレージレイが必要です。
- 各ストレージレイに2台のコントローラが必要です。
- Unified Managerで2つのストレージレイが検出されている必要があります。
- プライマリレイとセカンダリレイの各コントローラにイーサネット管理ポートが設定されていて、各コントローラがネットワークに接続されている必要があります。
- ストレージレイに必要なファームウェアの最小バージョンは7.84です（それぞれ異なるバージョンのOSを実行できます）。
- ローカルとリモートのストレージレイのパスワードを確認しておく必要があります。
- ミラーリングするプライマリボリューム以上のセカンダリボリュームを作成するには、リモートストレージレイに十分な空き容量が必要です。
- 非同期ミラーリングはFibre Channel（FC）またはiSCSIホストポートを搭載したコントローラでサポートされますが、同期ミラーリングはFCホストポートを搭載したコントローラでのみサポートされます。

接続要件

FCインターフェイスでのミラーリング（非同期または同期）には次の要件が適用されます。

- ストレージレイの各コントローラでは、最も番号が大きいFCホストポートがミラーリング処理の専用ポートとして使用されます。
- ベースのFCポートとホストインターフェイスカード（HIC）のFCポートの両方があるコントローラでは、HICの最も番号が大きいポートが使用されます。専用ポートにログオンしたホストはログアウトされ、ホストログイン要求は許可されません。このポートでは、ミラーリング処理の対象となるコントローラからのI/O要求のみが許可されます。
- 専用のミラーリングポートは、ディレクトリサービスとネームサービスのインターフェイスをサポートするFCファブリック環境に接続されている必要があります。特に、FC-ALおよびポイントツーポイントミラー関係が確立されたコントローラ間の接続オプションとしてサポートされないことに注意してください。

iSCSIインターフェイスでのミラーリング（非同期のみ）には次の要件が適用されます。

- FCとは異なり、iSCSIでは専用のポートを必要としません。iSCSI環境で非同期ミラーリングを使用する場合、ストレージアレイのどのフロントエンドiSCSIポートも非同期ミラーリング専用にする必要はありません。これらのポートは、非同期ミラーリングのトラフィックとホスト/アレイ間のI/O接続で共有されます。
- コントローラはリモートストレージシステムのリストを管理しており、iSCSIイニシエータはこのリストを使用してセッションの確立を試みます。iSCSI接続の確立に成功した最初のポートは、そのリモートストレージアレイとの以降のすべての通信に使用されます。通信に失敗すると、使用可能なすべてのポートを使用して新しいセッションの確立が試行されます。
- iSCSIポートは、アレイレベルでポート単位で設定します。設定メッセージおよびデータ転送用のコントローラ間通信では、次の設定を含むグローバル設定が使用されます。
 - VLAN：ローカルシステムとリモートシステムが通信するためには、両方のシステムでVLAN設定が同じである必要があります
 - iSCSIリスニングポート
 - ジャンボフレーム
 - イーサネットの優先順位



コントローラ間のiSCSI通信には、管理イーサネットポートではなくホスト接続ポートを使用する必要があります。

ミラーボリュームの候補

- ミラーペアのプライマリボリュームとセカンダリボリュームでは、RAIDレベル、キャッシングパラメータ、およびセグメントサイズが異なる場合があります。
- セカンダリボリュームには、プライマリボリュームと同等以上のサイズが必要です。
- ボリュームに設定できるミラー関係は1つだけです。
- 同期ミラーペアの場合、プライマリボリュームとセカンダリボリュームは標準ボリュームである必要があります。シンボリュームやSnapshotボリュームは使用できません。
- 同期ミラーリングの場合、特定のストレージアレイでサポートされるボリュームの数に制限があります。ストレージアレイに設定されているボリュームの数がサポートされている制限よりも少ないことを確認してください。同期ミラーリングがアクティブな場合は、作成済みの2つのリザーブ容量ボリュームがボリュームの制限に含まれます。

リザーブ容量

非同期ミラーリングの場合：

- コントローラのリセットおよびその他の一時的な中断からリカバリするための書き込み情報をログに記録するには、ミラーペアのプライマリボリュームとセカンダリボリュームにリザーブ容量ボリュームが必要です。
- ミラーペアのプライマリボリュームとセカンダリボリュームには追加のリザーブ容量が必要であるため、ミラー関係にある両方のストレージアレイに空き容量が確保されていることを確認してください。

同期ミラーリングの場合：

- コントローラのリセットおよびその他の一時的な中断からリカバリするための書き込み情報をログに記録するには、プライマリボリュームとセカンダリボリュームにリザーブ容量が必要です。

- 同期ミラーリングがアクティブ化されると、リザーブ容量ボリュームが自動的に作成されます。ミラーペアのプライマリボリュームとセカンダリボリュームにはリザーブ容量が必要であるため、同期ミラー関係にある両方のストレージレイに十分な空き容量が確保されていることを確認してください。

ドライブセキュリティ機能

- セキュリティ対応ドライブを使用する場合、プライマリボリュームとセカンダリボリュームのセキュリティ設定に互換性がある必要があります。この制限は強制的には適用されないため、自分で確認する必要があります。
- セキュリティ対応ドライブを使用する場合、プライマリボリュームとセカンダリボリュームで同じタイプのドライブを使用する必要があります。この制限は強制的には適用されないため、自分で確認する必要があります。
- Data Assurance (DA) を使用する場合、プライマリボリュームとセカンダリボリュームでDA設定を同じにする必要があります。

方法

非同期ミラーペアを作成する

非同期ミラーリングを設定するには、ローカルレイのプライマリボリュームとリモートレイのセカンダリボリュームを含むミラーペアを作成します。



この機能は、EF600またはEF300ストレージシステムでは使用できません。

作業を開始する前に

ミラーペアを作成する前に、Unified Managerに関する次の要件を満たしている必要があります。

- Web Services Proxyサービスが実行されている必要があります。
- Unified ManagerがHTTPS接続経由でローカルホストで実行されている必要があります。
- Unified Managerにストレージレイの有効なSSL証明書が表示されている必要があります。Unified Managerのメニューから「Certificate Management」に移動し、自己署名証明書を受け入れるか、独自のセキュリティ証明書をインストールできます。

また、ストレージレイに関する次の要件を満たしていることも確認してください。

- 各ストレージレイに2台のコントローラが必要です。
- Unified Managerで2つのストレージレイが検出されている必要があります。
- プライマリレイとセカンダリレイの各コントローラにイーサネット管理ポートが設定されていて、各コントローラがネットワークに接続されている必要があります。
- ストレージレイに必要なファームウェアの最小バージョンは7.84です（それぞれ異なるバージョンのOSを実行できます）。
- ローカルとリモートのストレージレイのパスワードを確認しておく必要があります。
- ミラーリングするプライマリボリューム以上のセカンダリボリュームを作成するには、リモートストレージレイに十分な空き容量が必要です。
- ローカルとリモートのストレージレイをFibre ChannelファブリックまたはiSCSIインターフェイスを介して接続します。

- ・ 非同期ミラー関係で使用するプライマリボリュームとセカンダリボリュームの両方を作成しておきます。

このタスクについて

非同期ミラーペアを作成するプロセスは複数の手順で構成される手順 です。

手順1：ミラー整合性グループを作成または選択します

新しいミラー整合性グループを作成するか、既存のグループを選択できます。

作業を開始する前に

- ・ 新しいミラー整合性グループを作成するには、Unified Managerでローカルストレージアレイとリモートストレージアレイが検出されている必要があります。

このタスクについて

ミラー整合性グループは、プライマリボリュームとセカンダリボリューム（ミラーペア）のコンテナであり、グループ内のすべてのペアに対して必要な再同期方法（手動または自動）を指定します。

手順

1. [* Manage *（管理）] ページで、ソースに使用するローカルストレージアレイを選択します。
2. メニューを選択します。アクション[非同期ミラーペアの作成]。

非同期ミラーペアの作成ウィザードが開きます。

3. 既存のミラー整合性グループを選択するか、新規に作成します。

既存のグループを選択するには、「既存のミラー整合グループ」が選択されていることを確認してから、表からグループを選択してください。整合性グループには複数のミラーペアを含めることができます。

新しいグループを作成するには、次の手順を実行します。

- a. 新しいミラー整合性グループを選択*し、*次へ*をクリックします。
- b. 2つのストレージアレイ間でミラーリングするボリュームのデータを表す、一意の名前を入力します。名前に使用できる文字は、アルファベット、数字、およびアンダースコア（_）、ダッシュ（-）、ハッシュ記号（#）のみです。最大文字数は30文字で、スペースは使用できません。
- c. ローカルストレージアレイとの間でミラー関係を確立するリモートストレージアレイを選択します。



リモートストレージアレイがパスワードで保護されている場合は、パスワードの入力を求められます。

- d. ミラーペアの同期を手動で行うか自動で行うかを選択します。
 - 手動--このオプションは、グループ内のすべてのミラーペアの同期を手動で開始する場合に選択します。再同期をあとで実行する場合は、プライマリストレージアレイのSystem Managerを起動して、メニューから「Storage [Asynchronous Mirroring]」に移動し、「Mirror Consistency Groups *」タブでグループを選択して、メニューから「More [Manually resynchronize]」を選択する必要があります。
 - 自動--前回の更新の開始から次の更新の開始までの間隔を*分*、時間、または*日*で選択します。たとえば、同期間隔を30分に設定し、同期プロセスを午後4時に開始すると、次のプロセスは午後4時30分に開始されます

e. 必要なアラート設定を選択します。

- 手動同期の場合は、アラートを受信するときのしきい値（残りの容量の割合によって定義）を指定します。
- 自動同期の場合は、次の3つのアラート方法を設定できます。同期が特定の時間内に完了していない場合、リモートアレイのリカバリポイントデータが特定の期限よりも古くなった場合、およびリザーブ容量が特定のしきい値（残りの容量の割合によって定義）に近づいている場合。

4. [次へ]を選択し、に進みます [\[手順2：プライマリボリュームを選択する\]](#)。

新しいミラー整合性グループを定義した場合は、Unified Managerによって、最初にローカルストレージアレイに、続いてリモートストレージアレイにミラー整合性グループが作成されます。各アレイのSystem Managerを起動すると、ミラー整合性グループを表示および管理できます。



Unified Managerによるミラー整合性グループの作成がローカルストレージアレイで成功したあと、リモートストレージアレイで失敗した場合は、ローカルストレージアレイからミラー整合性グループが自動的に削除されます。Unified Managerによるミラー整合性グループの削除でエラーが発生した場合は、手動で削除する必要があります。

手順2：プライマリボリュームを選択する

ミラー関係で使用するプライマリボリュームを選択し、リザーブ容量を割り当てます。

作業を開始する前に

- 非同期ミラー関係で使用するプライマリボリュームをローカルストレージアレイに作成しておく必要があります。

このタスクについて

ローカルストレージアレイのプライマリボリュームを選択すると、そのミラーペアに対応するすべてのボリュームのリストが表示されます。使用できないボリュームはリストに表示されません。

ローカルストレージアレイのミラー整合性グループに追加するボリュームには、ミラー関係のプライマリロールが割り当てられます。

手順

1. 対応するボリュームのリストからプライマリボリュームとして使用するボリュームを選択し、* Next *をクリックしてリザーブ容量を割り当てます。
2. 対応する候補のリストから、プライマリボリュームのリザーブ容量を選択します。

次のガイドラインに注意してください。

- リザーブ容量のデフォルト設定はベースボリュームの容量の20%であり、通常はこの容量で十分です。割合を変更する場合は、[候補の更新]をクリックします。
- 必要な容量は、プライマリボリュームに対するI/O書き込みの頻度とサイズ、およびその容量を維持する必要がある期間によって異なります。
- 一般に、次のいずれかまたは両方に該当する場合は、リザーブ容量を大きくします。
 - ミラーペアを長期にわたって維持する場合。
 - 大量のI/Oアクティビティにより、プライマリボリュームのデータブロックの大部分で変更が発生する場合。プライマリボリュームに対する一般的なI/Oアクティビティを判断するには、過去のパ

パフォーマンスデータやその他のオペレーティングシステムユーティリティを使用します。

3. [次へ]を選択し、に進みます [\[手順3：セカンダリボリュームを選択する\]](#)。

手順3：セカンダリボリュームを選択する

ミラー関係で使用するセカンダリボリュームを選択し、リザーブ容量を割り当てます。

作業を開始する前に

- 非同期ミラー関係で使用するセカンダリボリュームをリモートストレージレイに作成しておく必要があります。
- セカンダリボリュームには、プライマリボリュームと同等以上のサイズが必要です。

このタスクについて

リモートストレージレイのセカンダリボリュームを選択すると、そのミラーペアに対応するすべてのボリュームのリストが表示されます。使用できないボリュームはリストに表示されません。

リモートストレージレイのミラー整合性グループに追加するボリュームには、ミラー関係のセカンダリロールが割り当てられます。

手順

1. 対応するボリュームのリストから、ミラーペアのセカンダリボリュームとして使用するボリュームを選択し、* Next *をクリックしてリザーブ容量を割り当てます。
2. 対応する候補のリストから、セカンダリボリュームのリザーブ容量を選択します。

次のガイドラインに注意してください。

- リザーブ容量のデフォルト設定はベースボリュームの容量の20%であり、通常はこの容量で十分です。割合を変更する場合は、[候補の更新]をクリックします。
 - 必要な容量は、プライマリボリュームに対するI/O書き込みの頻度とサイズ、およびその容量を維持する必要がある期間によって異なります。
 - 一般に、次のいずれかまたは両方に該当する場合は、リザーブ容量を大きくします。
 - ミラーペアを長期にわたって維持する場合。
 - 大量のI/Oアクティビティにより、プライマリボリュームのデータブロックの大部分で変更が発生する場合。プライマリボリュームに対する一般的なI/Oアクティビティを判断するには、過去のパフォーマンスデータやその他のオペレーティングシステムユーティリティを使用します。
3. 「* Finish *」を選択して、非同期ミラーリングのシーケンスを完了します。

結果

Unified Managerは次の処理を実行します。

- ローカルストレージレイとリモートストレージレイの間で初期同期を開始します。
- ミラーリングしているボリュームがシンボルボリュームの場合、初期同期では、プロビジョニングされたブロック（レポート容量ではなく割り当て容量）のみがセカンダリボリュームに転送されます。これにより、初期同期を完了するために転送する必要があるデータの量が削減されます。
- ローカルストレージレイとリモートストレージレイにミラーペア用のリザーブ容量を作成します。

同期ミラーリングを設定するには、ローカルレイのプライマリボリュームとリモートレイのセカンダリボリュームを含むミラーペアを作成します。



この機能は、EF600またはEF300ストレージシステムでは使用できません。

作業を開始する前に

ミラーペアを作成する前に、Unified Managerに関する次の要件を満たしている必要があります。

- Web Services Proxyサービスが実行されている必要があります。
- Unified ManagerがHTTPS接続経由でローカルホストで実行されている必要があります。
- Unified Managerにストレージレイの有効なSSL証明書が表示されている必要があります。Unified Managerのメニューから「Certificate Management」に移動し、自己署名証明書を受け入れるか、独自のセキュリティ証明書をインストールできます。

また、ストレージレイに関する次の要件を満たしていることも確認してください。

- ミラーリングに使用する2つのストレージレイがUnified Managerで検出されている必要があります。
- 各ストレージレイに2台のコントローラが必要です。
- プライマリレイとセカンダリレイの各コントローラにイーサネット管理ポートが設定されていて、各コントローラがネットワークに接続されている必要があります。
- ストレージレイに必要なファームウェアの最小バージョンは7.84です（それぞれ異なるバージョンのOSを実行できます）。
- ローカルとリモートのストレージレイのパスワードを確認しておく必要があります。
- ローカルとリモートのストレージレイをFibre Channelファブリックを介して接続します。
- 同期ミラー関係で使用するプライマリボリュームとセカンダリボリュームの両方を作成しておきます。

このタスクについて

同期ミラーペアを作成するプロセスは複数の手順で構成される手順です。

手順1：プライマリボリュームを選択します

同期ミラー関係で使用するプライマリボリュームを選択します。

作業を開始する前に

- 同期ミラー関係で使用するプライマリボリュームを作成しておく必要があります。
- プライマリボリュームは標準ボリュームである必要があります。シンボリックボリュームやSnapshotボリュームは使用できません。

このタスクについて

ローカルストレージレイのプライマリボリュームを選択すると、そのミラーペアに対応するすべてのボリュームのリストが表示されます。使用できないボリュームはリストに表示されません。

選択するボリュームには、ミラー関係のプライマリロールが割り当てられます。

手順

1. [* Manage * (管理)]ページで、ソースに使用するローカルストレージレイを選択します。
2. メニューを選択します。アクション[同期ミラーペアの作成]。

同期ミラーペアの作成ウィザードが開きます。

3. 対応するボリュームのリストから、ミラーのプライマリボリュームとして使用するボリュームを選択します。
4. [次へ]を選択し、に進みます [\[手順2：セカンダリボリュームを選択する\]](#)。

手順2：セカンダリボリュームを選択する

ミラー関係で使用するセカンダリボリュームを選択します。

作業を開始する前に

- 同期ミラー関係で使用するセカンダリボリュームを作成しておく必要があります。
- セカンダリボリュームは標準ボリュームである必要があります。シンボリックボリュームやSnapshotボリュームは使用できません。
- セカンダリボリュームには、プライマリボリュームと同等以上のサイズが必要です。

このタスクについて

リモートストレージレイのセカンダリボリュームを選択すると、そのミラーペアに対応するすべてのボリュームのリストが表示されます。使用できないボリュームはリストに表示されません。

選択するボリュームには、ミラー関係のセカンダリロールが割り当てられます。

手順

1. ローカルストレージレイとの間でミラー関係を確立するリモートストレージレイを選択します。



リモートストレージレイがパスワードで保護されている場合は、パスワードの入力を求められます。

- ストレージレイは、対応するストレージレイ名別に表示されます。ストレージレイに名前を付けていない場合は、「unnamed」と表示されます。
- 使用するストレージレイがリストにない場合は、Unified Managerでそのストレージレイが検出されていることを確認してください。

2. 対応するボリュームのリストから、ミラーのセカンダリボリュームとして使用するボリュームを選択します。



選択したセカンダリボリュームの容量がプライマリボリュームよりも大きい場合、使用可能な容量はプライマリボリュームのサイズまでに制限されます。

3. 「次へ」をクリックして、に進みます [\[手順3：同期設定を選択します\]](#)。

手順3：同期設定を選択します

通信中断後のデータの同期方法を決定する設定を選択します。

このタスクについて

通信が中断した場合に、プライマリボリュームの所有コントローラがセカンダリボリュームとの間でデータを再同期する優先度を設定できます。また、再同期ポリシーとして、手動または自動のどちらかを選択する必要があります。

手順

1. スライダーバーを使用して同期優先度を設定します。

同期優先度は、I/O要求の処理と比較して、初期同期および通信中断後の再同期処理を完了するためにどの程度のシステムリソースが使用されるかを決定するものです。

このダイアログ環境で設定した優先度。プライマリボリュームとセカンダリボリュームの両方に適用されます。プライマリボリュームの速度は、あとからSystem Managerでメニューを選択して変更できます。Storage [Synchronous Mirroring > More > Edit Settings]を選択します。

同期優先度は5段階で設定できます。

- 最低
- 低
- 中
- 高
- 最高-同期優先度が最低に設定されている場合はI/Oアクティビティが優先され、再同期処理にかかる時間が長くなります。同期優先度が最高に設定されている場合は再同期処理が優先されますが、ストレージレイのI/Oアクティビティに影響する可能性があります。

2. リモートストレージレイのミラーペアの再同期を手動で行うか自動で行うかを選択します。

- 手動（推奨オプション）-ミラーペアとの通信が回復したあとに同期を手動で再開する場合に選択します。このオプションを選択すると、最適なタイミングでデータをリカバリできます。
- 自動--ミラーペアとの通信が回復した後、再同期を自動的に開始する場合に選択します。同期を手動で再開するには、System Managerでメニューから「Storage [Synchronous Mirroring]（ストレージ同期ミラーリング）」を選択し、テーブルでミラーペアを強調表示して、「* More」（詳細）で「Resume *」（続行）を選択します。

3. 完了*をクリックして、同期ミラーリングを完了します。

結果

ミラーリングがアクティブ化されると、システムは次の処理を実行します。

- ローカルストレージレイとリモートストレージレイの間に初期同期を開始します。
- 同期優先度と再同期ポリシーを設定します。
- コントローラのHICで最も大きい番号のポートをデータ送信のミラーリング用に予約します。

このポートで受信したI/O要求は、ミラーペアに含まれるセカンダリボリュームのリモートの優先コントローラ所有者からのみ承認されます。（プライマリボリュームにおける予約が許可されます）。

- コントローラごとに1つずつ、リザーブ容量用ボリュームを2つ作成します。これは、コントローラのリセットおよびその他の一時的な中断からリカバリするための書き込み情報のロギングに使用されます。

各ボリュームの容量は128MiBです。ただし、ボリュームがプールに配置されている場合は、ボリューム

ごとに4GiBが予約されます。

完了後

System Managerに移動して、メニューHome（View Operations in Progress）を選択し、同期ミラーリング処理の進捗状況を表示します。この処理には時間がかかることがあり、システムのパフォーマンスに影響する可能性があります。

よくある質問です

ミラー整合性グループを作成するときは、どのような点に注意する必要がありますか？

ミラー整合性グループを作成する際は、次のガイドラインに従ってください。

Unified Managerに関する次の要件を満たしている必要があります。

- Web Services Proxyサービスが実行されている必要があります。
- Unified ManagerがHTTPS接続経由でローカルホストで実行されている必要があります。
- Unified Managerにストレージレイの有効なSSL証明書が表示されている必要があります。Unified Managerのメニューから「Certificate Management」に移動し、自己署名証明書を受け入れるか、独自のセキュリティ証明書をインストールできます。

また、ストレージレイに関する次の要件を満たしていることも確認してください。

- Unified Managerで2つのストレージレイが検出されている必要があります。
- 各ストレージレイに2台のコントローラが必要です。
- プライマリレイとセカンダリアレイの各コントローラにイーサネット管理ポートが設定されていて、各コントローラがネットワークに接続されている必要があります。
- ストレージレイに必要なファームウェアの最小バージョンは7.84です（それぞれ異なるバージョンのOSを実行できます）。
- ローカルとリモートのストレージレイのパスワードを確認しておく必要があります。
- ローカルとリモートのストレージレイをFibre ChannelファブリックまたはiSCSIインターフェイスを介して接続します。



この機能は、EF600またはEF300ストレージシステムでは使用できません。

ミラーペアを作成するときは、どのような点に注意する必要がありますか？

ミラーペアを作成する際は、次のガイドラインに従ってください。

- 2つのストレージレイが必要です。
- 各ストレージレイに2台のコントローラが必要です。
- Unified Managerで2つのストレージレイが検出されている必要があります。
- プライマリレイとセカンダリアレイの各コントローラにイーサネット管理ポートが設定されていて、各コントローラがネットワークに接続されている必要があります。
- ストレージレイに必要なファームウェアの最小バージョンは7.84です（それぞれ異なるバージョン

のOSを実行できます)。

- ローカルとリモートのストレージレイのパスワードを確認しておく必要があります。
- ミラーリングするプライマリボリューム以上のセカンダリボリュームを作成するには、リモートストレージレイに十分な空き容量が必要です。
- 非同期ミラーリングはFibre Channel (FC) またはiSCSIホストポートを搭載したコントローラでサポートされますが、同期ミラーリングはFCホストポートを搭載したコントローラでのみサポートされます。



この機能は、EF600またはEF300ストレージシステムでは使用できません。

この割合を変更するのはどのような場合ですか？

非同期ミラーリング処理用のリザーブ容量は、一般にベースボリュームの20%です。通常はこの容量で十分です。

必要な容量は、ベースボリュームに対するI/O書き込みの頻度とサイズ、およびストレージオブジェクトのコピーサービス処理を使用する期間によって異なります。一般に、次のいずれかまたは両方に該当する場合は、リザーブ容量の割合を大きくします。

- 特定のストレージオブジェクトのコピーサービス処理の期間が非常に長い場合。
- 大量のI/Oアクティビティにより、ベースボリュームのデータブロックの大部分で変更が発生する場合。ベースボリュームに対する一般的なI/Oアクティビティを判断するには、過去のパフォーマンスデータやその他のオペレーティングシステムユーティリティを使用します。

リザーブ容量の候補が複数表示されるのはなぜですか？

プールまたはボリュームグループ内にストレージオブジェクトに対して選択した容量の割合を満たす複数のボリュームがある場合は、複数の候補が表示されます。

ベースボリューム上でコピーサービス処理用にリザーブする物理ドライブスペースの割合を変更すると、推奨される候補の一覧が更新されます。選択内容に基づいて最適な候補が表示されます。

ボリュームが一部表示されないのはなぜですか？

ミラーペアのプライマリボリュームを選択すると、対応するすべてのボリュームのリストが表示されます。

使用できないボリュームはリストに表示されません。次のいずれかの理由で、ボリュームが対象外になっている可能性があります。

- 最適状態でない。
- すでにミラー関係に参加している。
- 同期ミラーリングの場合、ミラーペアのプライマリボリュームとセカンダリボリュームは標準ボリュームである必要があります。シンボリュームやSnapshotボリュームは使用できません。
- 非同期ミラーリングの場合は、シンボリュームで自動拡張が有効になっている必要があります。

リモートストレージレイのボリュームが一部表示されないのはなぜですか？

リモートストレージレイ上のセカンダリボリュームを選択すると、そのミラーペアに対応するすべてのボリュームのリストが表示されます。

使用できないボリュームはリストに表示されません。次のいずれかの理由で、ボリュームが対象外になっている可能性があります。

- ボリュームが、Snapshotボリュームなどの標準以外のボリュームである。
- 最適状態でない。
- すでにミラー関係に参加している。
- 非同期ミラーリングでは、プライマリボリュームとセカンダリボリュームの間のシンボル属性が一致しません。
- Data Assurance (DA) を使用する場合、プライマリボリュームとセカンダリボリュームでDA設定を同じにする必要があります。
 - プライマリボリュームでDAを有効にする場合、セカンダリボリュームでもDAを有効にする必要があります。
 - プライマリボリュームでDAを有効にしない場合、セカンダリボリュームでもDAを無効にする必要があります。

同期優先度は同期速度にどのような影響を与えますか？

同期優先度は、同期アクティビティに割り当てられる処理時間をシステムパフォーマンスと比較して決定します。

プライマリボリュームのコントローラ所有者は、この処理をバックグラウンドで実行します。同時にコントローラ所有者は、プライマリボリュームへのローカルのI/O書き込みと、対応するセカンダリボリュームへのリモートの書き込みを処理します。再同期には、I/Oアクティビティに使用されるはずのコントローラの処理リソースが使用されるため、再同期がホストアプリケーションのパフォーマンスに影響する可能性があります。

同期優先度に応じた所要時間や、同期優先度がシステムパフォーマンスに与える影響を特定する際には、次のガイドラインに注意してください。

優先度は次のとおりです。

- 最低
- 低
- 中
- 高
- 最高

最低ではシステムパフォーマンスが優先されますが、再同期化に時間がかかります。最高では再同期化が優先されますが、システムパフォーマンスが低下する可能性があります。

これらのガイドラインは、各優先度の大きな違いを示しています。

完全同期の優先度	最高の同期速度と比較した経過時間
最低	最高の優先度であれば、約8倍の時間を要します。
低	最高の優先度であれば、約6回。
中	最高の優先度であれば、約3倍から半分。
高	優先度が最高の場合は、約2倍です。

同期の所要時間には、ボリュームサイズとホストのI/O速度が影響します。

手動同期ポリシーの使用が推奨されるのはなぜですか？

手動再同期が推奨されるのは、データがリカバリされる可能性が最も高い方法で再同期プロセスを管理できるためです。

自動再同期ポリシーを使用していて、再同期中に通信が中断する問題が発生した場合は、セカンダリボリューム上のデータが一時的に破損する可能性があります。再同期が完了すると、データは修正されます。

証明書と認証

証明書管理

概念

証明書の仕組み

証明書は、Webサイトやサーバなどのオンラインエンティティを識別するデジタルファイルで、インターネット上のセキュアな通信を実現します。

署名済み証明書

証明書を使用すると、指定されたサーバとクライアント間でのみ、Web通信が非公開かつ変更されずに暗号化された形式で送信されます。Unified Managerを使用すると、ホスト管理システムのブラウザおよび検出されたストレージレイのコントローラの証明書を管理できます。

証明書には信頼できる認証局が署名した証明書と自己署名の証明書があります。「署名」とは、第三者が所有者のIDを検証し、そのデバイスが信頼できると判断したことを意味します。ストレージレイの各コントローラには、自動生成された自己署名証明書が付属しています。自己署名証明書を引き続き使用することも、CA署名証明書を取得してコントローラとホストシステム間のよりセキュアな接続を確立することもできます。



CA署名証明書はセキュリティ保護を強化しますが（中間者攻撃を阻止するなど）、大規模なネットワークの場合はコストがかかる可能性があります。一方、自己署名証明書の方が安全性は低くなりますが、無料です。したがって、自己署名証明書は本番環境ではなく内部テスト環境で最もよく使用されます。

署名済み証明書は、信頼できる第三者機関である認証局（CA）によって検証されます。署名済み証明書に

は、エンティティ（通常、サーバまたはWebサイト）の所有者に関する詳細、証明書の問題 および有効期限、エンティティの有効なドメイン、およびアルファベットと数字で構成されるデジタル署名が含まれています。

ブラウザを開いてWebアドレスを入力すると、証明書チェックプロセスがバックグラウンドで実行され、有効なCA署名証明書を含むWebサイトに接続しているかどうかを確認されます。通常、署名済み証明書で保護されたサイトのアドレスには、鍵のアイコンとhttpsの指定が含まれています。CA署名証明書が含まれていないWebサイトに接続しようとする、サイトがセキュアでないことを示す警告がブラウザに表示されます。

CAは、アプリケーションプロセス中に自分の身元を確認するための手順を実行します。登録済みの会社にEメールを送信し、会社の住所を確認して、HTTPまたはDNSの検証を実行する場合があります。アプリケーションプロセスが完了すると、ホスト管理システムにロードするデジタルファイルがCAから送信されます。通常、これらのファイルには次のような信頼チェーンが含まれます。

- ルート--階層の最上位にあるのはルート証明書です。この証明書には、他の証明書への署名に使用する秘密鍵が含まれています。ルートは特定のCA組織を識別します。すべてのネットワークデバイスで同じCAを使用する場合は、ルート証明書が1つだけ必要です。
- *Intermediate *-ルートからの分岐は中間証明書です。CAは、保護されたルート証明書とサーバ証明書の間の証明書として機能する、1つ以上の中間証明書を発行します。
- サーバー--チェーンの下部にあるサーバ証明書は、Webサイトやその他のデバイスなど、特定のエンティティを識別するサーバ証明書です。ストレージレイの各コントローラには個別のサーバ証明書が必要です。

自己署名証明書

ストレージレイの各コントローラには、自己署名証明書が事前にインストールされています。自己署名証明書はCA署名証明書と似ていますが、第三者ではなくエンティティの所有者によって検証される点が異なります。CA署名証明書と同様に、自己署名証明書には独自の秘密鍵が含まれており、サーバとクライアントの間のHTTPS接続を介してデータが暗号化および送信されることも保証されます。

自己署名証明書はブラウザでは「信頼されている」ものではありません。自己署名証明書のみを含むWebサイトに接続しようとするたびに、ブラウザに警告メッセージが表示されます。Webサイトに進むには、警告メッセージ内のリンクをクリックする必要があります。これにより、基本的には自己署名証明書が受け入れられません。

Unified Managerの証明書

Unified Managerインターフェイスは、ホストシステムにWeb Services Proxyとともにインストールされます。ブラウザを開いてUnified Managerに接続しようとする、ホストが信頼できるソースであるかどうかを確認するためにデジタル証明書がチェックされます。ブラウザでサーバのCA署名証明書が見つからない場合は、警告メッセージが表示されます。そこからWebサイトにアクセスして、そのセッションの自己署名証明書を受け入れることができます。または、CAから署名入りのデジタル証明書を取得して、警告メッセージが表示されないようにすることもできます。

コントローラの証明書

Unified Managerセッション中に、CA署名証明書のないコントローラにアクセスしようとする、追加のセキュリティメッセージが表示されることがあります。この場合、自己署名証明書を永続的に信頼するか、コントローラのCA署名証明書をインポートして、Web Services Proxyサーバがこれらのコントローラから受信するクライアント要求を認証できるようにすることができます。

証明書管理に関連する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。
証明書チェーン	証明書にセキュリティレイヤを追加するファイルの階層。通常、チェーンの最上位にはルート証明書が1つ、中間証明書が1つ以上、エンティティを識別するサーバ証明書が1つ含まれます。
中間証明書	証明書チェーンのルートから1つ以上の中間証明書が分岐します。CAは、保護されたルート証明書とサーバ証明書の間の証明書として機能する、1つ以上の中間証明書を発行します。
キーストア	キーストアはホスト管理システム上のリポジトリであり、秘密鍵とそれに対応する公開鍵および証明書が格納されています。これらのキーと証明書によって、コントローラなどの独自のエンティティが識別されます。
ルート証明書	ルート証明書は、証明書チェーンの階層の最上位にあります。この証明書には、他の証明書への署名に使用する秘密鍵が含まれています。ルートは特定のCA組織を識別します。すべてのネットワークデバイスで同じCAを使用する場合は、ルート証明書が1つだけ必要です。
署名済み証明書	認証局（CA）によって検証される証明書。このデータファイルには秘密鍵が含まれており、サーバとクライアントの間でHTTPS接続を介してデータが暗号化された形式で送信されることが保証されます。また、署名済み証明書には、エンティティ（通常、サーバまたはWebサイト）の所有者に関する詳細およびアルファベットと数字で構成されるデジタル署名が含まれています。署名済み証明書は信頼チェーンを使用するため、本番環境で最もよく使用されます。「CA署名証明書」または「管理証明書」とも呼ばれます。
自己署名証明書	自己署名証明書は、エンティティの所有者によって検証されます。このデータファイルには秘密鍵が含まれており、サーバとクライアントの間でHTTPS接続を介してデータが暗号化された形式で送信されることが保証されます。また、アルファベットと数字で構成されるデジタル署名も含まれます。自己署名証明書はCA署名証明書と同じ信頼チェーンを使用しないため、テスト環境で最もよく使用されます。「事前にインストールされている」証明書とも呼ばれます。

期間	説明
サーバ証明書	サーバ証明書は、証明書チェーンの最下位にあります。Webサイトやその他のデバイスなど、特定のエンティティを識別します。ストレージシステムの各コントローラには個別のサーバ証明書が必要です。
信頼ストア	信頼ストアは、CAなどの信頼できるサードパーティの証明書を格納するリポジトリです。
Web Services Proxyの使用方法	Web Services Proxyは標準のHTTPSメカニズムによるアクセスを提供するプロキシで、管理者にストレージレイの管理サービスの設定を許可します。このプロキシは、WindowsホストまたはLinuxホストにインストールできます。Unified ManagerインターフェイスにはWeb Services Proxyが付随しています。

方法

CA署名証明書を使用する

Unified Managerをホストする管理システムへのセキュアなアクセスを確立するために、CA署名証明書を取得して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。

このタスクについて

CA署名証明書の使用は、2つの手順で構成された手順 です。

手順1：CSRを作成および送信します

最初に証明書署名要求（CSR） ファイルを生成し、そのファイルをCAに送信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、Unified ManagerとWeb Services Proxyをホストするシステム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、ホストシステムのIPアドレスまたはDNS名を指定する必要があります。



CAに送信したあとで新しいCSRを生成しないでください。CSRの生成時に、システムでは秘密鍵と公開鍵のペアが作成されます。公開鍵はCSRの一部であり、秘密鍵はキーストアに保持されます。署名済み証明書を受け取ってキーストアにインポートすると、システムでは秘密鍵と公開鍵の両方が元のペアになります。そのため、CSRをCAに送信したあとで新しいCSRを生成しないでください。新しいキーを生成すると、コントローラではCAから受け取った証明書が機能しくなくなります。

手順

1. [証明書管理]を選択します。
2. [管理 (Management)]タブで、[CSR全体* (* Complete CSR *)]を選択します。
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--ホストシステム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)--ホストシステム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) 。
4. ホストシステムに関する次の情報を入力します。
 - 共通名-- WebサービスプロキシがインストールされているホストシステムのIPアドレスまたはDNS名。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Unified 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。http://またはhttps://を含めないでください。
 - 代替IPアドレス--共通名がIPアドレスの場合は'オプションでホストシステムの追加のIPアドレスまたはエイリアスを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。
 - 代替DNS名--共通名がDNS名の場合は'ホストシステムの追加の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。
5. [完了] をクリックします。

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。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、PEM形式またはDER形式の署名済み証明書を要求します。

完了後

CAから証明書ファイルが返されるまで待ってから、に進みます **"手順2：管理証明書をインポートする"**。

手順2：管理証明書をインポートする

署名済み証明書を受け取ったあと、Unified Managerインターフェイスがインストールされているホストシステムの証明書チェーン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。
- 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。
- CAからチェーン証明書 (たとえば、.p7bファイル) が提供された場合は、チェーンファイルを個々のファイル (ルート証明書、1つ以上の中間証明書、サーバ証明書) に展開する必要があります。Windowsのcertmgrユーティリティーを使用してファイルを展開できます(右クリックして[**menu: All Tasks[Export]**]を選択します)エクスポートが完了すると、チェーン内の証明書ファイルごとに1つのCERファイルが表示されます。

手順

1. [証明書管理]を選択します。
2. [管理（ Management）]タブで、[インポート（ Import）]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. **[Browse]**(参照)をクリックして、最初にルートファイルと中間ファイルを選択し、次にサーバー証明書を選択します。

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。

結果

ファイルがアップロードされて検証されます。証明書の情報は、証明書の管理ページに表示されます。

管理証明書をリセットします

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。

このタスクについて

このタスクでは、WebサービスプロキシとSANtricity Unified Managerがインストールされているホストシステムから現在の管理証明書を削除します。証明書をリセットすると、ホストシステム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. [証明書管理]を選択します。
2. [管理（ Management）]タブで、[リセット（ Reset）]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。

ブラウザをリフレッシュすると、デスティネーションサイトへのアクセスがブロックされ、サイトでHTTP Strict Transport Securityが使用されていると報告されることがあります。この状況は、自己署名証明書に切り替えると発生します。デスティネーションへのアクセスをブロックしている状態をクリアするには、ブラウザから参照データをクリアする必要があります。

結果

システムでサーバの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。

アレイの証明書をインポートします

必要に応じて、SANtricity Unified Managerをホストするシステムで認証できるように、

ストレージレイの証明書をインポートすることができます。証明書には、認証局（CA）が署名した証明書と自己署名の証明書があります。

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。
- 信頼された証明書をインポートする場合は、SANtricity System Managerを使用してストレージレイのコントローラの証明書をインポートする必要があります。

手順

1. [証明書管理]を選択します。
2. [Trusted]タブを選択します。

このページには、ストレージレイについて報告されたすべての証明書が表示されます。

3. CA証明書をインポートするには* MENU：Import を選択し、自己署名証明書をインポートするには MENU：Import [Self-Signed storage array certificates]*を選択します。

表示を制限するには、[*次の証明書を表示...]フィルタリングフィールドを使用するか、いずれかの列見出しをクリックして証明書の行をソートします。

4. ダイアログボックスで証明書を選択し、*インポート*をクリックします。

証明書がアップロードされて検証されます。

証明書を表示します

証明書を使用している組織、証明書を発行した機関、有効期間、フィンガープリント（一意の識別子）など、証明書の概要情報を表示できます。

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。

手順

1. [証明書管理]を選択します。
2. 次のいずれかのタブを選択します。
 - 管理-- Webサービスプロキシをホストするシステムの証明書を表示します。管理証明書には、自己署名の証明書と認証局（CA）によって承認された証明書があります。この証明書によって、Unified Managerへのセキュアなアクセスが許可されます
 - * Trusted *-- Unified ManagerがストレージレイやLDAPサーバなどのその他のリモートサーバにアクセスできる証明書を表示します。認証局（CA）から発行された証明書と自己署名の証明書が含まれます。
3. 証明書の詳細を表示するには、その行を選択し、行の最後にある省略記号を選択して、*表示*または*エクスポート*をクリックします。

証明書をエクスポートします

証明書をエクスポートして詳細を確認することができます。

作業を開始する前に

エクスポートしたファイルを開くには、証明書ビューアアプリケーションが必要です。

手順

1. [証明書管理]を選択します。
2. 次のいずれかのタブを選択します。
 - 管理-- Webサービスプロキシをホストするシステムの証明書を表示します。管理証明書には、自己署名の証明書と認証局（CA）によって承認された証明書があります。この証明書によって、Unified Managerへのセキュアなアクセスが許可されます
 - * Trusted *-- Unified ManagerがストレージアレイやLDAPサーバなどのその他のリモートサーバにアクセスできる証明書を表示します。認証局（CA）から発行された証明書と自己署名の証明書が含まれます。
3. 証明書をページから選択し、行の最後にある省略記号をクリックします。
4. [* Export*]をクリックし、証明書ファイルを保存します。
5. 証明書ビューアアプリケーションでファイルを開きます。

信頼された証明書を削除する

期限切れになった証明書など、不要になっ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

古い証明書を削除する前に、新しい証明書をインポートしてください。



ルート証明書または中間証明書を削除すると、同じ証明書ファイルが共有されている可能性があるため、複数のストレージアレイに影響する可能性があります。

手順

1. [証明書管理]を選択します。
2. [Trusted]タブを選択します。
3. テーブルで1つ以上の証明書を選択し、*削除*をクリックします。



◦ Delete *機能は、プリインストールされている証明書では使用できません。

[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。

4. 削除を確認し、* Delete *をクリックします。

証明書がテーブルから削除されます。

信頼されていない証明書を

信頼されていない証明書の問題は、ストレージレイからSANtricity Unified Managerへのセキュアな接続を確立しようとしたときに、接続がセキュアであることが確認できないと発生します。証明書ページでは、信頼されていない証明書を解決するために、ストレージレイから自己署名証明書をインポートするか、信頼できる第三者機関から発行された認証局（CA）証明書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。
- CA署名証明書をインポートする場合は、次の点に注意してください。
 - ストレージレイの各コントローラの証明書署名要求（CSRファイル）を生成してCAに送信しておく必要があります。
 - 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上にある必要があります。

このタスクについて

信頼された追加のCA証明書のインストールが必要になる可能性があるのは、次のいずれかに該当する場合です。

- ストレージレイを新たに追加した。
- 一方または両方の証明書の期限が切れている。
- 一方または両方の証明書が失効している。
- 一方または両方の証明書のルート証明書または中間証明書がない。

手順

1. [証明書管理]を選択します。
2. [Trusted]タブを選択します。

このページには、ストレージレイについて報告されたすべての証明書が表示されます。

3. いずれかの*メニューを選択します。Import [Certificates]*。CA証明書または*メニューをインポートするには：[自己署名ストレージレイ証明書]をインポートして自己署名証明書をインポートします。

表示を制限するには、[*次の証明書を表示...]フィルタリングフィールドを使用するか、いずれかの列見出しをクリックして証明書の行をソートします。

4. ダイアログボックスで証明書を選択し、*インポート*をクリックします。

証明書がアップロードされて検証されます。

アクセス管理

概念

アクセス管理を使用してSANtricity Unified Managerでのユーザ認証を確立する。

設定ワークフロー

アクセス管理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ィールでUnified 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・アクセスできます初回ログイン時にパスワードを設定する必要があります。

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。事前に設定されているローカルユーザロールが表示されます。これらのロールはRBAC（ロールベースアクセス制御）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。
 - ローカルユーザの役割-- 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、ローカルユーザロールにLDAPユーザをマッピングします。
4. Unified Managerのログインクレデンシャルをユーザに割り当てます。
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。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機能にユーザがアクセスできるようにします。
 - 上部のバナーにユーザ名が表示されます。

Unified Managerで利用できる機能

機能へのアクセスは、ユーザに割り当てられたロールによって次のように異なります。

- * Storage admin *--アレイ上のストレージ・オブジェクトへの読み取り/書き込みのフル・アクセスを提供しますがセキュリティ構成へのアクセスはありません
- * Security admin *--アクセス管理と証明書管理のセキュリティ設定へのアクセス。
- * Support admin *--ストレージアレイ上のすべてのハードウェアリソース、障害データ、およびMELイベントへのアクセス。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。

使用できない機能は、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。

SANtricity Unified Manager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。
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。
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。Unified Managerには事前定義されたロールがあります
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。
Web Services Proxyの使用 方法	Web Services Proxyは標準のHTTPSメカニズムによるアクセスを提供するプロキシで、管理者にストレージレイの管理サービスの設定を許可します。このプロキシは、WindowsホストまたはLinuxホストにインストールできます。Unified ManagerインターフェイスはWeb Services Proxyで使用できます。

マッピングされたロールの権限

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が含まれています。各ロールには、SANtricity Unified 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。

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 *--アレイ上のストレージ・オブジェクトへの読み取り/書き込みのフル・アクセスを提供しますがセキュリティ構成へのアクセスはありません

- * Security admin *--アクセス管理と証明書管理のセキュリティ設定へのアクセス。
- * Support admin *--ストレージレイ上のすべてのハードウェアリソース、障害データ、およびMELイベントへのアクセス。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。セキュリティ設定へのアクセスはありません。

ユーザに特定の機能に対する権限がない場合、その機能は選択できないか、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、SANtricity Unified Managerに組み込みのロールベースアクセス制御（RBAC）機能を使用できます。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システムで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Unified 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. *オプション：*管理者が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

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）を使用して認証を管理することができます。

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 Unified 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サーバとホストシステム（Webサービスプロキシがインストールされているシステム）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、ユーザグループをローカルユーザ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Webサービスプロキシ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。
- 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。

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、ユーザーとデフォルトの役割とのマッピングを表示できます。これらのマッピングは、SANtricity Unified ManagerのWebサービスプロキシで適用されるRBAC（ロールベースアクセス制御）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. アクセス管理*を選択します。
2. [ローカルユーザー役割*（Local User Roles *）]タブを選択します。

表にユーザが表示されます。

- **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。このユーザにはすべてのロールが含まれています
- *** 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。このユーザには、Storage Admin、Support Admin、Monitorのロールが含まれています。
- *** security ***--アクセス管理や証明書管理など、セキュリティ設定を担当するユーザー。このユーザには、Security AdminとMonitorのロールが含まれています。
- *** support ***--ハードウェアリソース、障害データ、ファームウェアアップグレードを担当するユーザー。このユーザには、Support AdminとMonitorのロールが含まれています。
- *** monitor ***--システムへの読み取り専用アクセス権を持つユーザー。このユーザにはMonitorロールのみが含まれています。
- *** rw ***（読み取り/書き込み） -このユーザには、Storage Admin、Support Admin、Monitorのロールが含まれています。
- *** ro ***（読み取り専用） --このユーザーには、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。

手順

1. アクセス管理*を選択します。
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。

- ローカルユーザパスワードに対して最小文字数が設定されていない場合は、システムにアクセスするユーザにパスワードの入力を求めるチェックボックスを選択できます。
- 選択したユーザの新しいパスワードを2つのフィールドに入力します。
- この操作を確認するためにローカル管理者パスワードを入力し、*変更*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

すべての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システム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システム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

- アクセス管理*を選択します。
- [ローカルユーザー役割* (Local User Roles *)]タブを選択します。
- 「表示/設定の編集」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。

- 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system_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最低必要とする」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選択し、スピンド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

アクセス管理用の認証を設定するには、LDAPサーバとSANtricity Unified ManagerのWebサービスプロキシを実行するホストの間の通信を確立します。その後、LDAPユーザグループをローカルユーザ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ローカルユーザロールにマッピングします。

手順

1. アクセス管理*を選択します。
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（ <i>username@domain</i> ）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' <i>ldap[s]://host:port</i> 'の形式で入力します	証明書のアップロード（オプション）
<div data-bbox="245 1157 302 1209" data-label="Image"></div> <div data-bbox="358 947 480 1419" data-label="Text"> <p>このフィールドは、上記のサーバURLフィールドにLDAP Sプロトコルが指定されている場合にのみ表示されます。</p> </div> <div data-bbox="212 1472 513 1734" data-label="Text"> <p>[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。</p> </div>	バインドアカウント（オプション）

設定	説明
<p>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。</p>	<p>バインドパスワード（オプション）</p>
<div data-bbox="245 821 302 877">  </div> <div data-bbox="358 699 477 1003"> <p>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。</p> </div> <p>バインドアカウントのパスワードを入力します。</p>	<p>追加する前にサーバ接続をテストします</p>
<p>入力したLDAPサーバの設定でシステム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。</p>	<p>権限の設定</p>

設定	説明
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ユーザーグループの識別名 (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。

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ィー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. アクセス管理*を選択します。
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 (<i>username@domain</i>) 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「 <i>ldap[s]://host:port</i> 」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
システムがLDAPサーバの設定と通信できることを確認します。[保存 (Save)] をクリックすると、テストが実行されます。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。

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Webサービスプロキシの間の接続を解除するには、アクセス管理

ページからサーバ情報を削除します。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ィー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. アクセス管理*を選択します。
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。

よくある質問です

ログインできないのはなぜですか？

SANtricity Unified 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。

Unified 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。

ミラーリングタスク用のリモートストレージ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、一定の要件を満たす必要があります。

- ・ 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、ガイドラインを確認してください。

RBAC（ロールベースアクセス制御）機能には次のロールがあります。

- ・ * Storage admin *--アレイ上のストレージ・オブジェクトへの読み取り/書き込みのフル・アクセスを提供しますがセキュリティ構成へのアクセスはありません
- ・ * Security admin *--アクセス管理と証明書管理のセキュリティ設定へのアクセス。
- ・ * Support admin *--ストレージアレイ上のすべてのハードウェアリソース、障害データ、およびMELイベントへのアクセス。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。



Monitorロールは、管理者を含むすべてのユーザに必要です。

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。

ローカルユーザとは何ですか？

ローカルユーザは、システムに事前に定義されたユーザで、特定の権限が含まれていません。

ローカルユーザの例を次に示します。

- ・ **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。このユーザにはすべてのロールが含まれています初回ログイン時にパスワードを設定する必要があります。
- ・ * 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。このユーザには、Storage Admin、Support Admin、Monitorのロールが含まれています。このアカウントは、パスワードが設定されるまで無効になります。

- *** security ***--アクセス管理や証明書管理など、セキュリティ設定を担当するユーザー。このユーザには、Security AdminとMonitorのロールが含まれています。このアカウントは、パスワードが設定されるまで無効になります。
- *** support ***--ハードウェアリソース、障害データ、ファームウェアアップグレードを担当するユーザー。このユーザには、Support AdminとMonitorのロールが含まれています。このアカウントは、パスワードが設定されるまで無効になります。
- *** monitor ***--システムへの読み取り専用アクセス権を持つユーザー。このユーザにはMonitorロールのみが含まれています。このアカウントは、パスワードが設定されるまで無効になります。
- *** rw ***（読み取り/書き込み）-このユーザには、Storage Admin、Support Admin、Monitorのロールが含まれています。このアカウントは、パスワードが設定されるまで無効になります。
- *** ro ***（読み取り専用）--このユーザーには、Monitorロールのみが含まれています。このアカウントは、パスワードが設定されるまで無効になります。

著作権に関する情報

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

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

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

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

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

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

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

商標に関する情報

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