Unified Manager

SANtricity 11.8

NetApp
December 16, 2024

目次

Unified Manager 6による複数のアレイの管理

メインインターフェイス

Unified Manager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。このページでは、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ステータスを表示し、単一のアレイまたはアレイの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

Unified Managerの機能には、ナビゲーションサイドバーからアクセスできます。

面積	製品説明
管理	ネットワーク内のストレージアレイを検出し、アレイのSANtricity System Managerを起動し、1つのアレイから複数のアレイに設定をインポートし、アレイグループを管理します。設定のインポートやアレイグループの作成などの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オンにします。各行の最後にある省略記号は、アレイ名の変更など、単一のアレイに対する操作のインラインメニューを提供します。
運用	アレイ間での設定のインポートなど、バッチ処理の進捗状況を表示します。 ストレージアレイのステータスが最適でない場合は、一部の処理を実行できません。
証明書管理	ブラウザとクライアントの間で認証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。

インターフェイスの設定とヘルプ

インターフェイスの右上にある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。

ユーザログインとパスワード

システムにログインしている現在のユーザがインターフェイスの右上に表示されます。

ユーザとパスワードの詳細については、次を参照してください。

- "管理者パスワード保護の設定"
- "管理者パスワードの変更"
- "ローカルユーザプロファイルのパスワードの変更"

サポートされるブラウザ

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	89
Mozilla Firefox	80
Safari	14
Microsoft Edge	90

Web Services Proxyがインストールされていて、ブラウザで使用できる必要があります。

管理者パスワード保護の設定

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。

管理者パスワードとユーザプロファイル

Unified Managerの初回起動時に、管理者パスワードを設定するように求められます。adminパスワードを持つユーザなら誰でも、ストレージアレイの設定を変更できます。

Unified Managerインターフェイスには、管理パスワードに加えて、1つ以上のロールがマッピングされた設定済みのユーザプロファイルが含まれています。詳細については、を参照してください "アクセス管理の仕組み"。

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のみです。パスワードの変更については、次を参照してください。

- "管理者パスワードの変更"
- "ローカルユーザプロファイルのパスワードの変更"

セツシヨンタイムアウト

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。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、次回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、ソフトウェアは以降のパスワード試行を拒否します。パスワードを再度入力するには、10分待ってから「通常」の状態にリセットする必要があります。

セッションタイムアウトを調整したり、セッションタイムアウトを完全に無効にしたりできます。詳細については、を参照してください "セッションタイムアウトの管理"。

管理者パスワードの変更

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。

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。

タスクの内容

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が区別されます。
- 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注意してください。
- セキュリティを強化するために、15文字以上の英数字を使用し、パスワードを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の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際に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。

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に、Unified Managerでタイムアウトを設定できます。

タスクの内容

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。

> アレイに組み込まれたSecurity Assertion Markup Language（SAML）機能を使用してアクセス管理を設定している場合、ユーザのSSOセッションが最大数に達したときにセッションタイムアウトが発生することがあります。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します。

   設定できる最小タイムアウトは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。

ストレージアレイ

検出の概要

ストレージリソースを管理するには、まずネットワーク内のストレージアレイを検出する必要があります。

アレイの検出方法

[追加/検出]ページを使用して、組織のネットワークから管理するストレージアレイを検索して追加します。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。そのためには、ネットワークIPアドレスを入力すると、Unified Managerはその範囲内の各IPアドレスへの接続を個別に試行します。

詳細：

- "アレイの検出に関する考慮事項"
- "複数のストレージアレイの検出"
- "単一のアレイの検出"

アレイの管理方法

アレイを検出したら、* Manage-All *ページに移動します。このページでは、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ステータスを表示し、単一のアレイまたはアレイのグループに対して処理を実行できます。

単一のアレイを管理する場合は、アレイを選択してSystem Managerを開くことができます。

詳細：

- "System Managerへのアクセスに関する考慮事項"
- "個 々 のストレージアレイの管理"
- "ストレージアレイのステータスの表示"

概念

アレイの検出に関する考慮事項

Unified Managerでストレージリソースを表示および管理するには、組織のネットワークで管理する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の検出

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検出ページに表示され、管理ドメインに追加されることがあります。

単一のストレージアレイの検出

単一のアレイを検出する場合は、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1つ入力すると、個 々 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て[管理]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を指定する必要があります。

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が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。

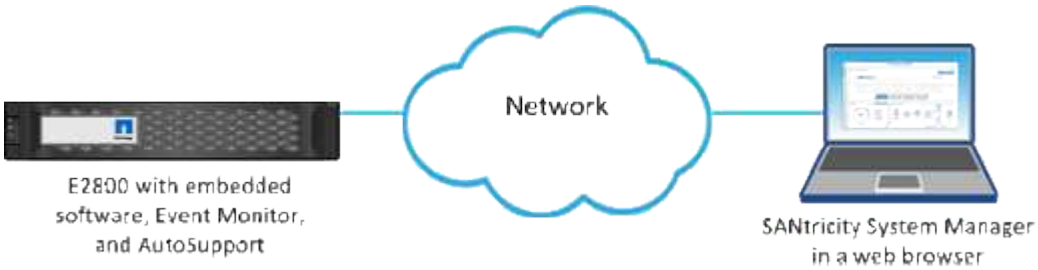
System Managerへのアクセスに関する考慮事項

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System Managerを開きます。

System Managerはコントローラに組み込まれた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。これには、アレイベースのすべての関数が含まれます。

System Managerにアクセスするには、以下を準備しておく必要があります。

- 次のいずれかのアレイモデルを参照してください。"E シリーズハードウェアの概要"
- Webブラウザを使用したネットワーク管理クライアントへのアウトオブバンド接続。



アレイの検出

複数のストレージアレイの検出

複数のアレイを検出すると、管理サーバが配置されているサブネット全体ですべてのストレージアレイが検出され、検出されたアレイが管理ドメインに自動的に追加されます。

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、System Manager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。
- 信頼されていない証明書を解決するには、認証局（CA）の信頼された証明書ファイルが必要です。証明書ファイルがローカルシステムにある必要があります。

アレイの検出は複数の手順で構成されます。

手順**1**：ネットワークアドレスを入力します

ローカル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検出ページに表示され、管理ドメインに追加されることがあります。

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. [管理] ページで、 [* 追加 / 検出 *] を選択します。

   [Add/Discover]ダイアログボックスが表示されます。

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、検出ページの表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おり、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。[新規検出パラメータ *] 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、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。

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が確認されます。

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ア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。自己署名証明書が信頼済みとしてマークされ、ストレージアレイがUnified Managerに追加されます。
- ストレージアレイへの接続を信頼しない場合は、*キャンセル*を選択し、各ストレージア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。

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は、ストレージアレイから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を確認できない場合に発生します。アレイの検出プロセスで信頼されていない証明書を解決するには、信頼できるサードパーティが発行した認証局（CA）証明書（CA署名証明書）をインポートします。

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。

- ストレージアレイを最近追加した。
- 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アレイの横にあるチェックボックスをオンにして、[インポート]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開きます。

2. Browse（参照）*をクリックして、ストレージア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。

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。

手順

1. 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を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。

終了後

ストレージアレイが管理ドメインに追加され、選択したグループ（指定されている場合）に関連付けられます。

指定したストレージアレイへのUnified Managerの接続には数分かかることがあります。

単一のアレイの検出

単一のストレージアレイを手動で検出して組織のネットワークに追加するには、[単一のストレージアレイの追加/検出]オプションを使用します。

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、System Manager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. [管理] ページで、 [* 追加 / 検出 *] を選択します。

   [Add/Discover]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。

   指定したストレージアレイへのUnified Managerの接続には数分かかることがあります。

   指定したIPアドレスでコントローラ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が確認されます。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は、認識された認証局（CA）によって署名されていない証明書を解決するためにセキュリティ例外を追加するように求められます。

5. 信頼されていない証明書があれば解決します。

   信頼されていない証明書は、ストレージアレイから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を確認できない場合に発生します。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、ストレージアレイを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「All」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。

終了後

ストレージアレイが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。

アレイの管理

ストレージアレイのステータスの表示

Unified Managerには、検出された各ストレージアレイのステータスが表示されます。

[* Manage-All*]ページに移動します。このページでは、Web Services Proxyとそのストレージアレイの間の接続のステータスを確認できます。

ステータスインジケータについては、次の表で説明します。

ステータス	を示します。
最適	ストレージアレイが最適な状態です。証明書の問題はなく、パスワードは有効です。
無効なパスワード	無効なストレージアレイパスワードが指定されました。
信頼されない証明書	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、ストレージアレイとの1つ以上の接続が信頼されていません。
要注意	ストレージアレイにユーザによる修正が必要な問題があります。
ロックダウン	ストレージアレイがロックダウン状態です。
不明	ストレージアレイに一度も接続されていません。この状況は、Web Services Proxyが起動中でまだストレージアレイに接続していない場合や、ストレージアレイがオフラインでWeb Services Proxyの起動後に一度も接続されていない場合に発生します。
オフライン	Web Services Proxyは以前にストレージアレイに接続していましたが、現在はすべての接続が失われています。

個 々 のストレージアレイの管理

[起動]オプションを使用すると、管理処理を実行する場合に1つ以上のストレージアレイに対してブラウザベースのSystem Managerを開くことができます。

手順

1. [管理]ページで、管理するストレージアレイを1つ以上選択します。
2. [* 起動 *] をクリックします。

   新しいウィンドウが開き、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。

ストレージアレイのパスワードの変更

Unified Managerでストレージアレイを表示したりアクセスしたりするために使用するパスワードを更新できます。

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。
- ストレージアレイの現在のパスワード（System Managerで設定されているパスワード）を確認しておく必要があります。

タスクの内容

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. 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。

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

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

タスクの内容

削除したストレージアレイにはアクセスできません。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ることで、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、ストレージアレイやそのデータには影響しません。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。

設定のインポート

設定のインポートの概要

設定のインポート機能を使用すると、1つのアレイから複数のアレイに設定をインポートするバッチ処理を実行できます。この機能により、ネットワーク内で複数のアレイを構成する必要がある場合に時間を節約できます。

どのような設定をインポートできますか？

アラート方法、AutoSupport設定、ディレクトリサービス設定、ストレージ設定（ボリュームグループやプールなど）、およびシステム設定（自動ロードバランシングなど）をインポートできます。

詳細：

- "設定のインポートの仕組み"
- "ストレージ構成のレプリケートに関する要件"

バッチインポートの実行方法を教えてください。

ソースとして使用するストレージアレイで、System Managerを開き、必要な設定を行います。そのあと、Unified Managerの[管理]ページに移動し、1つ以上のアレイに設定をインポートします。

詳細：

- "アラート設定のインポート"
- "AutoSupport設定のインポート"
- "ディレクトリサービス設定のインポート"
- "ストレージ構成のインポート"
- "システム設定のインポート"

概念

設定のインポートの仕組み

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、ネットワーク内に複数のアレイを構成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以外の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、System Manager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、System Managerを使用して設定をバックアップします。
3. 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、要件と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がソースアレイとターゲットアレイで同一である必要があります。
- 拡張シェルフは、同じドライブタイプの同じスロットに搭載する必要があります（ドライブが構成で使用されている場合は、未使用ドライブの場所は関係ありません）。

コントローラ

- コントローラのタイプはソースアレイとターゲットアレイで異なる場合があり（E2800からE5700にインポートする場合など）、RBODエンクロージャのタイプは同じである必要があります。
- HIC（ホストのDA機能を含む）がソースアレイとターゲットアレイで同一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ません。

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かぎり、ソースアレイとターゲットアレイでドライブ容量が異なる場合があります。（ターゲットアレイには、より新しい大容量のドライブが搭載されている場合がありますが、こ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構成されません）。
- ソースアレイのディスクプールボリュームが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ません。
- シンボリュームはインポートプロセスに含まれません。

バッチインポートの使用

アラート設定のインポート

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。

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System Managerで設定します（メニュー：Settings [Alerts]）。
- ターゲットストレージアレイの既存の構成は、System Managerでバックアップされます（メニュー：[設定][システム]>[ストレージアレイ構成の保存]）。

タスクの内容

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ボックスで、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]ダイアログボックスで、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. [Select Targets]ダイアログボックスで、新しい設定を適用するアレイを1つ以上選択します。

   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、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、このダイアログボックスに表示されません。

5. [完了] をクリックします。

   [Operations]ページにインポート処理の結果が表示されます。処理に失敗した場合は、その行をクリックすると詳細が表示されます。

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した。

AutoSupport設定のインポート

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。

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（メニュー：サポート[サポートセンター]）に対してSystem Managerで設定します。
- ターゲットストレージアレイの既存の構成は、System Managerでバックアップされます（メニュー：[設定][システム]>[ストレージアレイ構成の保存]）。

タスクの内容

インポートされる設定には、個別の機能（Basic AutoSupport、AutoSupport OnDemand、および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ボックスで、「* 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]ダイアログボックスで、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. [Select Targets]ダイアログボックスで、新しい設定を適用するアレイを1つ以上選択します。

   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、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、このダイアログボックスに表示されません。

5. [完了] をクリックします。

[Operations]ページにインポート処理の結果が表示されます。処理に失敗した場合は、その行をクリックすると詳細が表示されます。

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なります。

ディレクトリサービス設定のインポート

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。

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System Managerで設定されます（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、System Managerでバックアップされます（メニュー：[設定][システム]>[ストレージアレイ構成の保存]）。

タスクの内容

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]ダイアログボックスで、[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]ダイアログボックスで、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. [Select Targets]ダイアログボックスで、新しい設定を適用するアレイを1つ以上選択します。

   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、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、このダイアログボックスに表示されません。

5. [完了] をクリックします。

   [Operations]ページにインポート処理の結果が表示されます。処理に失敗した場合は、その行をクリックすると詳細が表示されます。

結果

ターゲットストレージアレイにソースアレイと同じディレクトリサービスが設定されます。

システム設定のインポート

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。

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System Managerで設定しておきます。
- ターゲットストレージアレイの既存の構成は、System Managerでバックアップされます（メニュー：[設定][システム]>[ストレージアレイ構成の保存]）。

タスクの内容

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]ダイアログボックスで、[システム]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]ダイアログボックスで、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. [Select Targets]ダイアログボックスで、新しい設定を適用するアレイを1つ以上選択します。

   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、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、このダイアログボックスに表示されません。

5. [完了] をクリックします。

   [Operations]ページにインポート処理の結果が表示されます。処理に失敗した場合は、その行をクリックすると詳細が表示されます。

結果

ターゲットストレージアレイのシステム設定がソースアレイと同じになります。

ストレージ構成のインポート

ストレージアレイから別のストレージア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。

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アレイの既存の構成は、System Managerでバックアップされます（メニュー：[設定][システム]>[ストレージアレイ構成の保存]）。
- ソースアレイとターゲットア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。
  - 拡張シェルフには、同じドライブタイプの同じスロットが搭載されている必要があります。
  - RBODエンクロージャタイプは同一である必要があります。
  - 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の容量よりも大きい。
- 次の制限事項に注意してください。
  - 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ません。
  - シンボリュームはインポートプロセスに含まれません。

タスクの内容

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]ダイアログボックスで、[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]ダイアログボックスで、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. [Select Targets]ダイアログボックスで、新しい設定を適用するアレイを1つ以上選択します。

   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、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、このダイアログボックスに表示されません。

5. [完了] をクリックします。

   [Operations]ページにインポート処理の結果が表示されます。処理に失敗した場合は、その行をクリックすると詳細が表示されます。

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。

FAQ

どのような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、ソースストレージアレイがSystem Managerでどのように設定されているかによって異なります。

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)サーバーのドメイン名とURL、およびLDAPサーバー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実行時に、一部のストレージアレイがターゲットの選択ダイアログボックスに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です。
- システム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など）。

アレイクルウフ

グループの概要

[グループの管理]ページでは、管理しやすいように一連のストレージアレイグループを作成できます。

アレイグループとは

一連のストレージアレイをグループ化して、物理インフラと仮想インフラを管理できます。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を簡単に実行できます。

グループには次の2種類があります。

- すべてのグループ--すべてのグループがデフォルトのグループで、組織内で検出されたすべてのストレージアレイが含まれます。[すべて]グループには、メインビューからアクセスできます。
- ユーザーが作成したグループ--ユーザーが作成したグループには'手動で選択してそのグループに追加するストレージア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。

グループを設定するにはどうすればよいですか。

[Manage Groups]ページでは、グループを作成し、そのグループにアレイを追加できます。

詳細：

- "ストレージアレイグループの設定"

ストレージアレイグループの設定

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アレイを追加します。

グループの設定は、2つの手順で構成されます。

手順**1**：グループを作成する

最初にグループを作成します。ストレージグループは、ボリュームを構成するストレージを提供するドライブを定義します。

手順

1. 管理ページで、メニューからグループの管理[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。

手順**2**：ストレージアレイをグループに追加する

1つ以上のストレージアレイをユーザが作成したグループに追加できます。

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。 *

グループからのストレージアレイの削除

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から管理する必要がなくなった場合は、グループから削除できます。

タスクの内容

グループからストレージアレイを削除しても、ストレージアレイやそのデータには影響しません。ストレージアレイを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誤ってグループから削除した場合は、再度追加することができます。

手順

1. 管理ページで、メニュー：グループの管理[グループからストレージアレイを削除]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。

ストレージアレイグループの削除

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できます。

タスクの内容

この処理で削除されるのは、ストレージアレイグループのみです。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、[すべて管理]ビューまたは関連付けられているその他のグループから引き続きアクセスできます。

手順

1. 管理ページで、メニューからグループの管理[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（ Delete ）] をクリックします。

ストレージアレイグループの名前変更

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

タスクの内容

これらのガイドラインに注意してください。

- 名前に使用できる文字は、アルファベット、数字、アンダースコア（_）、ハイフン（-）、シャープ（#）です。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。
- わかりやすく覚えやすい一意のわかりやすい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

アップグレード

アップグレードセンターの概要

アップグレードセンターでは、複数のストレージアレイのSANtricity OSソフトウェアとNVSRAMのアップグレードを管理できます。

アップグレードの仕組み

最新のOSソフトウェアをダウンロードしてから、1つ以上のアレイをアップグレードします。

アップグレードワークフロー

次の手順では、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NVSRAMファイルをリポジトリ（Webサービスプロキシサーバのファイルが格納されている領域）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 SANtricity OS Software]または[Upgrade Center]>[Manage Software Repository]から選択します。
3. ファイルがリポジトリにロードされたら、アップグレードで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NVSRAM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に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. その後、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、後でアクティブ化するためにファイルをステージング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を妨げる可能性のある状況がないかどうかが確認されます。いずれかのアレイが健全性チェックで不合格になった場合は、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合格しなかった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. アップグレードファイルを各コントローラに転送します。
   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が完了するまでに通常15~25分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。

健全性チェック

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かどうかがチェックされます。アップグレードを実行できない状況は次のとおりです。

- 割り当て済みドライブで障害が発生
- ホットスペアを使用中です
- ボリュームグループに不備がある
- 同時に実行できない処理
- 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の数が多すぎる
- 構成データベースの検証エラー
- 古いバージョンのDACstoreを搭載したドライブ

アップグレードするときは、どのような点に注意する必要がありますか？

複数のストレージアレイをアップグレードする前に、計画の一環として重要な考慮事項を確認してください。

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ソフトウェアの列に表示されます。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できるように、ホストのマルチパス/フェイルオーバードライバまたはHBAドライバのアップグレードも必要になる場合があります。

互換性については、を参照して "NetAppのInteroperability Matrix"ください。手順については、使用してい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 "E シリーズおよび SANtricity に関するドキュメント"ます。

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の処理を続行できます。アップグレード中に、次のプロセスが実行されます。

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が自身のLUNとコントローラBのすべてのLUNをテイクバックします。
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。

ソフトウェアとファームウェアのアップグレード

アップグレード前の健常性チェックを実行

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、開始前に個別に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かどう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。

   [アップグレード前の健全性チェック]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一覧が表示されます。

2. 必要に応じて、ストレージシステムをリストでフィルタまたはソートして、現在最適状態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は、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、その他のタスクを実行したりできます。

> いずれかのアレイが健全性チェックで不合格になった場合は、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合格しなかった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のアップグレード

1つ以上のストレージアレイを最新のソフトウェアとNVSRAMで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

デフォルト設定を指定するコントローラファイルです。

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の Unified Managerが実行されているホストシステムにあります。
- ソフトウェアアップグレードを今すぐアクティブ化するかあとでアクティブ化するかを決めておきます。

  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

システムを11.80.x以降にアップグレードするには、SANtricity OS 11.70.5が実行されている必要があります。

タスクの内容

```
[NOTE]
====
データ損失またはストレージアレイの破損のリスク-
アップグレードの実行中はストレージアレイを変更しないでください。ストレージアレイへの電源を維持します。

====
.手順
. ストレージアレイにコントローラが
1台しかない場合、またはマルチパスドライバを使用していない場合は、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。
. 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。
. 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。
+
[Upgrade SANtricity OS software]ページが表示されます。

. 最新のSANtricity OSソフトウェアパッケージを
NetAppサポートサイトからローカルマシンにダウンロードします。
+
.. [ 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。
.. 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。
.. [Download Latest Release] リンクをクリックします。
.. 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。

+
[NOTE]
====
バージョン8.42以降では、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と、エラーが表示されてダウンロードが中止されます。

====
. 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。
+
.. [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。

+
[NOTE]
====
ソフトウェアリポジトリには、Web Services
Proxy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。

====
.. 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。

. [互換性があるストレージアレイ]の表で、選択した
OSソフトウェアファイルと互換性が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。
+
** [互換性があるストレージアレイ]の表では、[管理
]ビューで選択したストレージアレイのうち、選択したファームウェアファイルと互換性があるストレージアレイがデフォルトで選択されます。
** 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。

. *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。
. [スタート] ボタンをクリックします。
. 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、リブートが開始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。

+
**
アップグレード前の健常性チェックは、アップグレードプロセスの一環として実行されます。アップグレード前の健常性チェックでは、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かどうかがチェックされます。
** ストレージアレイの健全性チェックに失敗すると、アップグレードは停止します。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常性チェックのあとに、アップグレード処理をキャンセルできます。

. *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フォルダにという名前でファイルが保存されます `upgrade_log-<date>.json`。

[[IDefb87482c18d4dd8872d3ee8c930e648]]
= ステージング済みOSソフトウェアのアクティブ化

```
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
ソフトウェアファイルはすぐにアクティブ化することも、都合の良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ことを前提としています。

.タスクの内容
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


```
[NOTE]
====
```
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
. メインビューで、* Manage *（管理）を選択します。必要に応じて、ページ上部の[ステータス]列をクリックしてソートし、ステータスが「OSアップグレード（アクティブ化待ち）」のすべてのストレージアレイを表示します。
. 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常性チェックは、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常性チェックでは、ストレージアレイのすべてのコンポーネントについて、アクティブ化を続行できるかどうかがチェックされます。
** ストレージアレイの健全性チェックに失敗すると、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常性チェックのあとにアクティブ化処理をキャンセルできます。アップグレード前の健常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するコンポーネントによって異なります。

. *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フォルダにという名前でファイルが保存されます `activate_log-<date>.json`。

[[IDd0a8d664558c459907fb3f27eaa5cc8e]]
= ソフトウェアリポジトリの管理
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ソフトウェアリポジトリには、Web Services
Proxy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。

.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
. 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。
+
[Manage Software Repository]ダイアログボックスが表示されます。

. 次のいずれかを実行します。

+
[cols="25h,~"]
|===
| オプション | これをしなさい…

a|
インポート
a|
.. [*インポート.*]をクリックします
.. [*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。
+
OSファイルのファイル名は、のようになり `N2800-830000-000.dlp`ます。

.. 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。

a|
削除
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。
.. [削除（ Delete ）] をクリックします。

|===

.結果
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。[Delete]を選択すると、ファイルがソフトウェアリポジトリから削除されます。

[[ID3b3d15cb8170528e2259d79a6688de07]]
= ステージング済みOSソフトウェアのクリア
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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、ストレージアレ

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
. 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。
+
[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、保留中のソフトウェアまたはNVSRAMがあるストレージシステムが検出されたすべてのリストが表示されます。

.
必要に応じて、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表示できるように、リストでストレージシステムをフィルタまたはソートします。
. 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。
. [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。

:leveloffset: -1

:leveloffset: -1

= ミラーリング

:leveloffset: +1

[[IDc932de422716fe626d2320cd4c5ff61c]]
= ミラーリングの概要
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ミラーリング機能を使用して、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でデータを非同期または同期的にレプリケートします。

[NOTE]
====

同期ミラーリングは、EF600またはEF300ストレージシステムでは使用できません。

====

== ミラーリングとは

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、データボリュームがオンデマンドまたはスケジュールに基づいてコピーされるため、データの破損や損失が原因で発生するダウンタイムを最小限または回避できます。同期ミラーリングでは、データボリュームがリアルタイムでレプリケートされるため、継続的な可用性が確保されます。

詳細：

* xref:{relative_path}mirroring-overview.html["ミラーリングの仕組み"]
* xref:{relative_path}mirroring-terminology.html["ミラーリングに関する用語"]

== ミラーリングの設定方法

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。

詳細：

* xref:{relative_path}mirroring-configuration-workflow.html["ミラーリングの設定ワークフロー"]
* xref:{relative_path}requirements-for-using-mirroring.html["ミラーリングを使用するための要件"]
* xref:{relative_path}create-asynchronous-mirrored-pair-um.html["非同期ミラーペアの作成"]
* xref:{relative_path}create-synchronous-mirrored-pair-um.html["同期ミラーペアの作成"]

= 概念

:leveloffset: +1

[[ID6f5565d1479440cab9089cf06f8597c5]]
= ミラーリングの仕組み

```
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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つのストレージア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。

[NOTE]
====
同期ミラーリングは、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、データボリュームがオンデマンドまたはスケジュールに基づいてコピーされるため、データの破損や損失が原因で発生するダウンタイムを最小限または回避できます。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の許す限り更新できます。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ると送信されます。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、データボリュームがリアルタイムでレプリケートされるため、継続的な可用性が確保されます。目的は、2つのストレージア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、コピーは常に本番環境のデータと同じです。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ことを示す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目的に最適です。



== 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。

[cols="1a,1a,1a"]
|===
| 属性 | 非同期 | 同期
```

```
 a|
```
レプリケーション方法
```
 a|
```
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。
```
 a|
```
continuous --ミラーリングは自動的に継続的に実行され
'ホストの書き込みごとにデータがコピーされます

```
 a|
```
距離
```
 a|
```
アレイ間の長距離をサポートします。通常、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。
```
 a|
```
アレイ間の距離は短くしてください。レイテンシと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。

```
 a|
```
通信方法
```
 a|
```
標準のIPまたはFibre Channelネットワーク。
```
 a|
```
Fibre Channelネットワークのみ。

```
 a|
```
ボリュームタイプ
```
 a|
```
標準またはシン。
```
 a|
```
標準のみ。

```
|===
```

```
[[IDe4b35b813de58f9ea45fb16c13ba0198]]
```
= ミラーリングの設定ワークフロー

```
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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。

. Unified Managerで初期設定を実行します。
+
.. 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。
..
ミラー整合性グループを作成または選択します。ミラー整合性グループは、ローカルアレイ上のプライマリボリュームとリモートアレイ上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、実行する同期方法（手動またはスケジュール）を指定します。
..
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。
..
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。
..
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。


. 初期同期の進捗状況を確認します。
+
.. Unified Managerで、ローカルアレイのSystem Managerを起動します。
.. 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。


. 必要に応じて、System Managerで後続のデータ転送の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だけ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。
+
[NOTE]
====
非同期レプリケーションは定期的に行われるため、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。

. Unified Managerで初期設定を実行します。
+
.. 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。
.. 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。
.. 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。
.. 同期と再同期の優先度を選択します。
..
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。

. 初期同期の進捗状況を確認します。
+
.. Unified Managerで、ローカルアレイのSystem Managerを起動します。
.. 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、通常の処理を通じて同期状態が維持されます。新しいブロックと変更されたブロックだけ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。

. 必要に応じて、System Managerで同期設定を変更できます。
+
[NOTE]
====
同期レプリケーションは継続的であるため、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機能を提供する必要があります。

====

```
[[ID3dc652f6e4954eda1853e1bb06d4b1af]]
= ミラーリングに関する用語
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
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。

```
[cols="25h,~"]
|===
| 期間 | 製品説明


 a|
```
ローカルストレージアレイ
```
 a|
```
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。

```
 a|
```
ミラー整合性グループ
```
 a|
```
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、整合性のあるリカバリポイントが維持されます。

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。

```
 a|
```
ミラーペア
```
 a|
```
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。

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。書き込み処理は最初にプライマリボリュームに対して実行され、次に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は、同じ同期設定が共有されます。

a|
プライマリボリューム
a|
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。

a|
リモートストレージアレイ
a|
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。

a|
リザーブ容量
a|
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。

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。

a|
セカンダリボリューム
a|
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。

a|
同期
a|
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。同期は、通信の中断後に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場合にも実行されます。通信リンクの動作が再開されると、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。

|===

```
[[ID559d2c73943347841fb3331625453072]]
= ミラーリングを使用するための要件
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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。



== Unified Manager

* 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にストレージアレイの有効な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。




== ストレージアレイ

[NOTE]
====
同期ミラーリングはEF600またはEF300ストレージアレイでは使用できません。

====
* 2つのストレージアレイが必要です。
* 各ストレージアレイに2台のコントローラが必要です。
* Unified Managerで2つのストレージアレイが検出されている必要があります。
*
プライマリアレイとセカンダリアレイの両方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、ネットワークに接続されている必要があります。
* ストレージア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OSバージョンを実行できます）。
* ローカルとリモートのストレージア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ア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。

* ストレージア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。このポートでのI/O要求は、ミラーリング処理の対象となるコントローラからのみ許可されます。
*
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は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

[NOTE]

====
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。
+

NOTE: EF600およびEF300コントローラでは、非同期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のプロトコル、トレイレベル、セグメントサイズ、セキュリティタイプ、およびRAIDレベルが同じである必要があります。対応していない非同期ミラーペアは、使用可能なボリュームのリストに表示されません。

* セカンダリボリュームは、プライマリボリュームと同じサイズ以上である必要があります。
* 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、作成された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。
*
非同期ミラーリングの場合、プライマリボリュームとセカンダリボリュームのドライブセキュリティ機能が同じである必要があります。
+
** プライマリボリュームがFIPSに対応している場合、セカンダリボリュームはFIPSに対応している必要があります。
** プライマリボリュームがFDEに対応している場合、セカンダリボリュームはFDEに対応している必要があります。
**
プライマリボリュームでドライブセキュリティを使用していない場合、セカンダリボリュームでドライブセキュリティを使用していない必要があります。

== 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ア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。

:leveloffset: -1

= ミラーリングの設定

```
:leveloffset: +1


[[ID59f302dac40f9e20583e9a54b2bf5276]]
= 非同期ミラーペアの作成
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
非同期ミラーリングを設定するには、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を含むミラーペアを作成します。

.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にストレージアレイの有効な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、ストレージアレイおよびボリュームに関する次の要件も満たしている必要があります。

* 各ストレージアレイに2台のコントローラが必要です。
* Unified Managerで2つのストレージアレイが検出されている必要があります。
*
プライマリアレイとセカンダリアレイの両方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、ネットワークに接続されている必要があります。
* ストレージア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OSバージョンを実行できます）。
* ローカルとリモートのストレージア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ア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アレイを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。
* セカンダリボリュームは、プライマリボリュームと同じサイズ以上である必要があります。
```

.タスクの内容
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ます。

== 手順1：ミラー整合性グループを作成または選択する

この手順では、新しい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、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必要な再同期方法（手動または自動）を指定します。

.手順
. [* 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。
. 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。

. 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。

+
.. 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。
..
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上のデータに最も近い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、アンダースコア（_）、ダッシュ（-）、ハッシュ記号（#）だけです。最大文字数は30文字で、スペースは使用できません。
..
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。
+
[NOTE]
====
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。

====
.. 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、同期間隔が30分に設定され、同期プロセスが午後4時に開始される場合、次のプロセスは午後4時30分に開始されます。

. . 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。
*** 自動同期では、3つのアラート方法を設定できます。
1つは、特定の時間内に同期が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制限時間を超えた場合、もう1つはリザーブ容量が特定のしきい値（残りの容量の割合で定義）に近づいている場合です。

. [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。

+
[NOTE]
====
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

この手順では、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。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したボリュームには、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
. 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。
. 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、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。
+
*** ミラーペアを長期間保持する場合。
*** 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。

. [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

この手順では、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。リモートストレージア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アレイのミラー整合性グループに追加したボリュームには、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
.
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。
. 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、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。
+
*** ミラーペアを長期間保持する場合。
*** 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。

. 「* 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アレイとリモートストレージアレイの間の初期同期を開始します。
*
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にミラーペア用のリザーブ容量を作成します。

NOTE:
ミラーリングしているボリュームがシンボリュームの場合、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のあるデータ量が削減されます。

[[ID80ef80528b56691e77df8a49457c771e]]
= 同期ミラーペアの作成
:allow-uri-read:

```
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
同期ミラーリングを設定するには、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を含むミラーペアを作成します。

[NOTE]
====
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。

====
.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にストレージアレイの有効な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、ストレージアレイおよびボリュームに関する次の要件も満たしている必要があります。

* ミラーリングに使用する2つのストレージアレイがUnified
Managerで検出されている必要があります。
* 各ストレージアレイに2台のコントローラが必要です。
*
プライマリアレイとセカンダリアレイの両方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、ネットワークに接続されている必要があります。
* ストレージア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
OSバージョンを実行できます）。
* ローカルとリモートのストレージア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アレイを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。
* 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。シンボリュームや
Snapshotボリュームを使用することはできません。
* 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ボリュームを使用することはできません。
*
```

セカンダリボリュームには、プライマリボリュームと同じサイズ以上のサイズを指定する必要があります。

.タスクの内容
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ます。

== 手順1：プライマリボリュームを選択する

この手順では、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。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。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
. [* 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。
. 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。

.
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。
. [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

この手順では、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。リモートストレージア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
.
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。
+
[NOTE]
====
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。

====

+
**
ストレージアレイは、それぞれのストレージアレイ名で表示されます。ストレージア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アレイがリストにない場合は、Unified Managerでそのストレージアレイが検出されていることを確認してください。

.
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。
+
[NOTE]
====
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。

====
. [次へ]*をクリックし、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

このステップでは、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。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
. スライダ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。

+
このダイアログで設定した優先度は、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
+
同期優先度を最低に設定すると、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、ストレージアレイのI/Oアクティビティに影響する可能性があります。

. リモートストレージア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。このオプションは、データをリカバリするための最良の機会を提供します。
** *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。

. 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アレイとリモートストレージアレイの間の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での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。

.終了後

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。

:leveloffset: -1

= FAQ

:leveloffset: +1

[[ID7a1bfd48e6c5cd10360a88ed2b1f8f52]]
= 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？
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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にストレージアレイの有効な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、ストレージアレイに関する次の要件も満たしている必要があります。

* Unified Managerで2つのストレージアレイが検出されている必要があります。
* 各ストレージアレイに2台のコントローラが必要です。
*
プライマリアレイとセカンダリアレイの両方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、ネットワークに接続されている必要があります。
* ストレージア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OSバージョンを実行できます）。
* ローカルとリモートのストレージア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アレイを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。

[NOTE]
====
同期ミラーリングは、EF600またはEF300ストレージシステムでは使用できません。

====

[[ID687588a2f2ca0d8a597af23f26ab43db]]
= 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？
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ミラーペアを作成する前に、次のガイドラインに従ってください。

* 2つのストレージアレイが必要です。
* 各ストレージアレイに2台のコントローラが必要です。
* Unified Managerで2つのストレージアレイが検出されている必要があります。
*
プライマリアレイとセカンダリアレイの両方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、ネットワークに接続されている必要があります。
* ストレージア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OSバージョンを実行できます）。
* ローカルとリモートのストレージア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ア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。

[NOTE]
====
同期ミラーリングは、EF600またはEF300ストレージシステムでは使用できません。

====

```
[[ID5e9f58868117fdc0ef115fce3373ebf1]]
= この割合を変更するのはなぜですか？
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
非同期ミラーリング処理用のリザーブ容量は、通常は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。




[[IDbacb5d2b12dcccef833506702e37012b]]
= リザーブ容量の候補が複数表示されるのはなぜですか？
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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ボリュームが複数ある場合は、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、推奨される候補のリストを更新できます。選択に基づいて最適な候補が表示されます。




[[IDe35ac4de892d3511be68b24dfaddbc5b]]
= ボリュームが一部表示されないのはなぜですか？
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
```

```
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
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、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。

```
NOTE: EF600および
EF300コントローラでは、非同期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のプロトコル、トレイレベル、セグメントサイズ、セキュリティタイプ、およびRAIDレベルが同じである必要があります。対応していない非同期ミラーペアは、使用可能なボリュームのリストに表示されません。


[[IDb9f6c295a2b86f467ce0b3bde2e716a4]]
= リモートストレージアレイのボリュームが一部表示されないのはなぜですか？
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
リモートストレージア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を使用できない可能性があります。

* 標準以外のボリューム（Snapshotボリュームなど）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の場合、シンボリューム属性がプライマリボリュームとセカンダリボリュームで一致しません。

* 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。

*
非同期ミラーリングの場合、プライマリボリュームとセカンダリボリュームのドライブセキュリティ機能が同じである必要があります。
+
** プライマリボリュームがFIPSに対応している場合、セカンダリボリュームはFIPSに対応している必要があります。
** プライマリボリュームがFDEに対応している場合、セカンダリボリュームはFDEに対応している必要があります。
**
プライマリボリュームでドライブセキュリティを使用していない場合、セカンダリボリュームでドライブセキュリティを使用していない必要があります。

[[IDa07e3666b91c442c4b67556b1689d529]]
= 同期優先度は同期速度にどのような影響を与えますか？
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
同期優先度は、システムパフォーマンスに対する同期アクティビティに割り当てる処理時間を定義します。

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。

次のプライオリティレートを使用できます。

* 最低
* 低
* 中
* 高
* 最高

優先度が最低の場合はシステムパフォーマンスがサポートされますが、再同期にかかる時間は長くなります。最も優先度が高い場合は再同期がサポートされますが、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、優先度の大まかな違いを示しています。

```
[cols="45h,~"]
|===
| 完全同期の優先度 | 最高の同期速度と比較した経過時間


 a|
最低
 a|
最高プライオリティレートの約8倍の長さになります。



 a|
低
 a|
最高プライオリティレートの約6倍の長さになります。



 a|
中
 a|
最高プライオリティレートの約3.5倍の長さになります。



 a|
高
 a|
最高プライオリティレートの約2倍の時間がかかります。

|===
```

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。

[[ID13dd9eaf9744477367df9821945bdcde]]
= 手動同期ポリシーの使用が推奨されるのはなぜですか。
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

:leveloffset: -1

:leveloffset: -1

= 証明書

:leveloffset: +1

[[IDe29cbc73b9e466f44f98e4736bf805e2]]
= 証明書の概要
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
証明書管理では、証明書署名要求（CSR）の作成、証明書のインポート、および既存の証明書の管理を行うことができます。

== 証明書とは

_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し、インターネット上のセキュアな通信を実現するデジタルファイルです。証明書には2種類あります。A_Signed certificate_is validated by a Certificate Authority（CA；認証局）とa_self-signed certificate_is validated by the entity of the entity instead of a third party。

詳細：

* xref:{relative_path}how-certificates-work-unified.html["証明書の仕組み"]
* xref:{relative_path}certificate-terminology-unified.html["証明書の用語"]

== 証明書を設定する方法を教えてください。

[証明書管理]では、Unified Managerをホストする管理ステーションの証明書を設定できます。また、アレイのコントローラの証明書をインポートすることもできます。

詳細：

* xref:{relative_path}use-ca-signed-certificate-um.html["管理システム用のCA署名証明書の使用"]
* xref:{relative_path}import-array-certificates-unified.html["アレイの証明書のインポート"]

= 概念

:leveloffset: +1

[[ID28dc866e9f79dc56fa8eccaf910d9be5]]
= 証明書の仕組み
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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、Web通信が、指定されたサーバとクライアントの間でのみ、非公開かつ変更されずに暗号化された形式で送信されることが保証されます。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ア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、誰かが所有者のIDを検証し、自分のデバイスが信頼できると判断したことを意味します。ストレージアレイには、自動生成された自己署名証明書が各コントローラに付属しています。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の間のよりセキュアな接続を確立することもできます。

[NOTE]
====
CA署名証明書はセキュリティ保護に優れていますが（中間者攻撃を防止するなど）、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、自己署名証明書は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（通常はサーバまたはWebサイト）の所有者に関する詳細、証明書の発行日と有効期限、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ます。

ブラウザを開いてWebアドレスを入力すると、証明書の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が確認されます。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、南京錠のアイコンとhttpsの指定が含まれます。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と、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、申請プロセス中にユーザー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、CAからホスト管理システムにロードするデジタルファイルが送信されます。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、必要なルート証明書は1つだけです。
* *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ー証明書は、
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ー証明書です。ストレージア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

ストレージア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されて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が含まれている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す。

== 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と、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と、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。

[[ID3270e5aa501d1f4b528b472e8ebc5a7b]]

= 証明書の用語
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
証明書管理に関連する用語を次に示します。

[cols="25h,~"]
|===
| 期間 | 製品説明

a|
カリフォルニア州
a|
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ドキュメント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。

a|
CSR
a|
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が証明書を発行するために必要な情報を検証します。

a|
証明書
a|
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、この情報を証明（署名）する信頼されたエンティティのIDが含まれています。

a|
証明書チェーン
a|
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、チェーンには階層の最上位にある1つのルート証明書、1つ以上の中間証明書、およびエンティティを識別するサーバ証明書が含まれます。

a|
中間証明書
a|
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。

a|
キーストア
a|
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。

a|
ルート証明書
a|
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、必要なルート証明書は1つだけです。

a|
署名済み証明書
a|
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、HTTPS接続を介してサーバとクライアントの間でデータが暗号化された形式で送信されるようにします。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。

a|
自己署名証明書
a|
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、HTTPS接続を介してサーバとクライアントの間でデータが暗号化された形式で送信されるようにします。また、文字と数字で構成されるデジタル署名も含まれています。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。

a|
サーバ証明書
a|
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。

a|
信頼ストア
a|
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。

|===

:leveloffset: -1

[[ID99583ab724c14dc43db7714457d7c99e]]
= 管理システム用のCA署名証明書の使用
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

.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、証明書機能は表示されません。

.タスクの内容
CA署名証明書の使用は、3つの手順で構成されます。

== 手順1：CSRファイルを作成します

最初に証明書署名要求（CSR）ファイルを生成して、組織とWeb Services ProxyとUnified Managerがインストールされているホストシステムを特定する必要があります。

[NOTE]
====
または、OpenSSLなどのツールを使用してCSRファイルを生成し、に進みます<<手順2：CSRファイルを送信する>>。

====
.手順
. [証明書管理]を選択します。
. [管理]タブで、[* CSR全体*]を選択します。
. 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.などのサフィックスを含めます。
** *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）。

. Web Services Proxyがインストールされている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://.は含めないでください。DNS名の1文字目をワイルドカードにすることはできません。
** *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。DNS名の1文字目をワイルドカードにすることはできません。

. ホスト情報が正しいことを確認します。そうでない場合、CAから返された証明書はインポートしようとしたときに失敗します。
. [完了] をクリックします。
. にアクセスします。

== 手順2：CSRファイルを送信する

証明書署名要求（CSR）ファイルを作成したら、そのファイルを認証局（CA）に送信して、Unified ManagerとWeb Services
Proxyをホストするシステムの署名済み管理証明書を受け取ります。

NOTE: Eシリーズシステムには、署名済み証明書用のPEM形式（Base64
ASCIIエンコード）が必要です。これには、.pem、.crt、.cer、.keyのいずれかのファイルタイプが含まれます。

.手順
. ダウンロードしたCSRファイルの場所を確認します。
+
ダウンロードのフォルダの場所は、ブラウザによって異なります。

. CSRファイルをCA（VerisignやDigiCertなど）に送信し、
PEM形式の署名付き証明書を要求します。
+
[CAUTION]
====
* CSRファイルをCAに送信した後は、別のCSRファイルを再生成しないでください。
*CSRを生成すると、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、秘密鍵はシステムの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インポートすると、秘密鍵と公開鍵の両方が元のペアになります。キーが一致しないと署名済み証明書は機能せず、CAに新しい証明書を要求する必要があります。

====
. CAから署名済み証明書が返されたら、に進みます<<手順3：管理証明書をインポートする>>。

== 手順3：管理証明書をインポートする

認証局（CA）から署名済み証明書を受け取ったら、Web Services Proxy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に証明書をインポートします。

.開始する前に
* CAから署名済み証明書を受け取っておきます。これらのファイルには、ルート証明書、
1つ以上の中間証明書、およびサーバ証明書が含まれます。
* CAからチェーン証明書ファイル（
.p7bファイルなど）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ユーティリティを使用してファイルを展開でき `certmgr`ます

(右クリックしてメニューを選択します:すべてのタスク[エクスポート])。Base-64エンコードを推奨します。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。
* Web Services Proxyを実行しているホストシステムに証明書ファイルをコピーしておきます。

.手順
. [証明書管理]を選択します。
. [管理（Management）]タブで、[*インポート（* Import）]を選択する
+
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開きます。

.
[*Browse*]をクリックして、最初にルート証明書ファイルと中間証明書ファイルを選択し、次にサーバ証明書を選択します。外部ツールからCSRを生成した場合は、CSRと一緒に作成された秘密鍵ファイルもインポートする必要があります。
+
ファイル名がダイアログボックスに表示されます。

. [* 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。証明書の情報が[証明書管理]ページに表示されます。

[[IDbe7f3d496c294050813ba8eee3a051eb]]
= 管理証明書のリセット
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

.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、証明書機能は表示されません。

.タスクの内容
このタスクでは、Web Services Proxyと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使用されるようになります。

.手順
. [設定]>[証明書]*を選択します。
. [アレイ管理]*タブを選択し、*[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。

. フィールドにと入力し `reset`、*[リセット]*をクリックします。
+
ブラウザの更新後、ブラウザによって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、そのサイトがHTTP Strict Transport Securityを使用していると報告されることがあります。この状態は、自己署名証明書に切り替えたときに発生します。宛先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、ブラウザから閲覧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。その結果、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るプロンプトが表示されます。

= アレイ証明書を使用する

:leveloffset: +1

[[ID90666f44e3f607b214642991502447c4]]
= アレイの証明書のインポート
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
必要に応じて、Unified Managerをホストするシステムで認証できるように、ストレージアレイの証明書をインポートできます。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。

.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、System Managerを使用してストレージアレイ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
. [証明書管理]を選択します。
. [*Trusted*]タブを選択します。
+
このページには、ストレージア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。

. 次のいずれかのメニューを選択します。Import [Certificates] CA certificate or menu：Import [Self-Signed storage array certificates]。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。

. 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。

[[IDc14d26ffe172f0d915dbd6779354ede0]]
= 信頼できる証明書の削除
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

.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。

[CAUTION]
====
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を共有す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ることに注意してください。

====
.手順

. [証明書管理]を選択します。
. [*Trusted*]タブを選択します。
. 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。
+
[NOTE]
====
* 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。

. 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。

[[ID117723ccbfa1572e010cf99339779133]]
= 信頼されない証明書の解決
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
信頼されていない証明書は、ストレージアレイから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を確認できない場合に発生します。

[証明書]ページで信頼されていない証明書を解決するには、ストレージアレイの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が発行した認証局（CA）証明書をインポートします。

.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、次の手順を実行します。
+
** ストレージア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にあることを確認します。

.タスクの内容
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。

* ストレージアレイを最近追加した。
* 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
. [証明書管理]を選択します。
. [*Trusted*]タブを選択します。
+
このページには、ストレージア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。

. 次のいずれかのメニューを選択します。Import [Certificates] CA certificate or menu：Import [Self-Signed storage array certificates]。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。

. 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。

:leveloffset: -1

= 証明書の管理

:leveloffset: +1

[[ID0fdd731be7081d42c47858621bdddf69]]
= 証明書の表示
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
証明書の概要情報を表示できます。これには、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）が含まれます。

.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、証明書機能は表示されません。

.手順
. [証明書管理]を選択します。
. 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。

. 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。

[[ID7dbb82f215de9b3802dbc5eba3836c5b]]
= 証明書のエクスポート
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

.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
. [証明書管理]を選択します。
. 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。

. 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。
. [* Export*]をクリックし、証明書ファイルを保存します。
. 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。

:leveloffset: -1

:leveloffset: -1

= アクセス管理

:leveloffset: +1

[[ID46f4c3f8232650bcf75967b7ba0cde67]]
= アクセス管理の概要
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセス管理は、Unified Managerでユーザ認証を設定する方法の1つです。

== どのような認証方式を使用できますか。

次の認証方式を使用できます。

* *ローカルユーザーの役割*--
RBAC（役割ベースのアクセス制御）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。
* *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
* *saml *-- 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。

詳細：

* xref:{relative_path}how-access-management-works-unified.html["アクセス管理の仕組み"]
* xref:{relative_path}access-management-terminology-unified.html["アクセス管理の用語"]
* xref:{relative_path}permissions-for-mapped-roles-unified.html["マッピングされたロールの権限"]
* xref:{relative_path}access-management-with-saml.html["SAML"]

== アクセス管理を設定するにはどうすればよいですか？

SANtricityソフトウェアは、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。LDAPを使用する場合は、[アクセス管理]ページで設定できます。

詳細：

* xref:{relative_path}access-management-with-local-user-roles-unified.html["ローカルユーザロールを使用したアクセス管理"]
* xref:{relative_path}access-management-with-directory-services-unified.html["ディレクトリサービスを使用したアクセス管理"]
* xref:{relative_path}configure-saml.html["SAMLの設定"]

= 概念

:leveloffset: +1

[[IDcbda7abe8496c1ca55b8217c142bff92]]
= アクセス管理の仕組み
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/

```
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
アクセス管理を使用してUnified Managerでユーザ認証を確立します。



== 設定ワークフロー

アクセス管理の設定は次のように機能します。

. 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。
+
[NOTE]
====
初回ログイン時は、ユーザ名が `admin`自動的に表示され、変更することはできません。
`admin`ユーザには、システム内のすべての機能へのフルアクセス権が付与されます。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。

====
.
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。
. 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*--
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、設定は必要ありません。
** *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、LDAPユーザをローカルユーザロールにマッピングします。
** *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。



. 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。
.
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。ログイン中、システムは次のバックグラウンドタスクを実行します。
+
** ユーザアカウントに対してユーザ名とパスワードを認証します。
```

** 割り当てられたロールに基づいてユーザの権限を決定します。
** 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で使用できる機能

機能にアクセスできるかどうかは、ユーザに割り当てられたロールによって異なります。ロールには次のようなものがあります。

* * 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。

使用できない機能は淡色表示されるか、ユーザインターフェイスに表示されません。

[[IDef8b908c7a6ff4692fe527b9fbc719f8]]
= アクセス管理の用語
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Unified Managerに関連するアクセス管理の用語を次に示します。

[cols="25h,~"]
|===
| 期間 | 製品説明

a|
Active Directory

a|
Active Directory（AD）は、Windowsドメインネットワーク用にLDAPを使用するMicrosoftのディレクトリサービスです。

a|
バインド
a|
バインド操作は、ディレクトリサーバに対してクライアントを認証するために使用されます。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。

a|
カリフォルニア州
a|
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ドキュメント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。

a|
証明書
a|
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、この情報を証明（署名）する信頼されたエンティティのIDが含まれています。

a|
LDAP
a|
Lightweight Directory Access Protocol（LDAP）は、分散されたディレクトリ情報サービスにアクセスして管理するための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をLDAPサーバに接続してユーザを検証できます。

a|
RBAC
a|
ロールベースアクセス制御（RBAC）は、個 々

のユーザのロールに基づいてコンピュータリソースまたはネットワークリソースへのアクセスを制御する方法です。Unified Managerには事前定義されたロールがあります

 a|
SAML
 a|
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では多要素認証が可能で、ユーザはIDを証明するために2つ以上の項目（パスワードやフィンガープリントなど）を指定する必要があります。ストレージアレイに組み込まれているSAML機能は、アイデンティティのアサーション、認証、および許可に関してSAML2.0に準拠しています。

 a|
SSO
 a|
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。

 a|
Web Services Proxy
 a|
Web Services Proxyは標準の
HTTPSメカニズムを介したアクセスを提供し、管理者がストレージアレイの管理サービスを設定できるようにします。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。

|===

[[ID102c42f1301a0fc7a001a0020f69878a]]
= マッピングされたロールの権限
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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されたユーザが含まれます。各ロールには、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。

各ロールは、次のタスクへのアクセスをユーザに提供します。

* * 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。

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。

[[ID39f8a00218d9f8f6b80d44539ee903a6]]
= ローカルユーザロールを使用したアクセス管理
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
管理者は、Unified Managerで適用されるロールベースアクセス制御（
RBAC）機能を使用できます。これらの機能は、「ローカルユーザロール」と呼ばれます。

== 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には、管理者は次の操作を実行します。

. 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。
+
[NOTE]
====
 `admin`ユーザには、システム内のすべての機能へのフルアクセス権が付与されます。

====
.

管理者が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、変更できません。
. 必要に応じて、管理者は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。
. 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。
* ユーザがパスワードなしでログインできるようにします。

[[ID47461a1a3c5b5b30ca32c7606eff5fbc]]
= ディレクトリサービスを使用したアクセス管理
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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、設定は次のように機能します。

. 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。
+
[NOTE]
====
 `admin`ユーザには、システム内のすべての機能へのフルアクセス権が付与されます。

====
. LDAPサーバの設定を入力します。設定には、ドメイン名、

URL、バインドアカウント情報が含まれます。
. 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は、LDAPサーバとWeb Services Proxyがインストールされているホスト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。
.
サーバ接続が確立されると、管理者は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定義されており、変更することはできません。
. LDAPサーバとWeb Services Proxyの間の接続をテストします。
. ユーザは、自分に割り当てられた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します。
* ディレクトリサーバを削除します。
* 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。
* ユーザがパスワードなしでログインできるようにします。

[[ID3a69d138577698d76e34434d82eda6e3]]
= SAMLを使用したアクセス管理
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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機能します。

. 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。
+
[NOTE]
====
この `admin`ユーザには、System
Managerのすべての機能に対するフルアクセスが付与されます。

====
. 管理者は、[アクセス管理]の下の[*SAML *]タブに移動します。
. 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、Unified
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。
. サービスプロバイダと
IdPの間に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。通信を設定するために、管理者はUnified
Managerを使用して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。次に、IdPシステムからメタデータファイルをIdPにインポートします。
+
[NOTE]
====
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。

====
. 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。そのためには、管理者はUnified
Managerを使用してマッピングを作成します。
. IdP URLへのSSOログインをテストします。このテストでは、ストレージアレイと
IdPが通信できることを確認します。
+
[CAUTION]
====
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。

====
. Unified Managerで、ストレージアレイのSAMLを有効にします。
. 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する
* サービスプロバイダファイルのエクスポート

== アクセス制限

SAMLが有効な場合、ユーザは従来のStorage Managerインターフェイスからそのアレイのストレージを検出または管理できません。

また、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たログイン

:leveloffset: -1

= ローカルユーザロールを使用する

:leveloffset: +1

[[IDaba8ea594b7aaa19d6dba13bd01e3d63]]
= ローカルユーザロールの表示
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
[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、Unified Managerの Webサービスプロキシで適用されるロールベースアクセス制御（RBAC）の一部です。

.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。

.タスクの内容
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のみです。

.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。

[[IDdb7e0c5300b1947829c549e1cc159465]]
= ローカルユーザプロファイルのパスワードの変更
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

.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。

.タスクの内容
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（[設定の表示/編集]）以上にする必要があります。
* パスワードは大文字と小文字が区別されます。
*
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注意してください。
* セキュリティを強化するために、
15文字以上の英数字を使用し、パスワードを頻繁に変更してください。

.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。

. [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。

.
ローカルユーザパスワードの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際に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。

[[ID1efabd95bf91ec53cc8587946402cdc7]]
= ローカルユーザのパスワード設定の変更

```
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
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に必要な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。

.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。

.タスクの内容
ローカルユーザパスワードの最小文字数を設定する際は、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文字に設定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に対してパスワードの最小文字数を設定するには、[Require all local user passwords to be at least]チェックボックスをオンにし、スピンボックスで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にする必要があります。

. [保存（ Save ）] をクリックします。

:leveloffset: -1

= ディレクトリサービスを使用する

:leveloffset: +1

[[ID7ba621ca443d028fbcb7d7d968347a18]]
= ディレクトリサーバの追加
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセス管理用の認証を設定するには、LDAPサーバと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。次に、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。

.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をローカルマシンにインストールする必要があります。

.タスクの内容
ディレクトリサーバの追加は、2つの手順で行います。最初にドメイン名と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は、認証用のCA証明書もアップロードする必要があります（標準の署名機関によって署名されている場合）。バインドアカウントのクレデンシャルがある場合は、ユーザ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
. アクセス管理*を選択します。
. [*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。

. [*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
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 製品説明

 a|
構成設定

 a|
ドメイン
 a|
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。

 a|
サーバURL
 a|
LDAPサーバにアクセスするためのURLをの形式で入力し `ldap[s]://*host*:*port*`ます。

 a|
証明書のアップロード（オプション）
 a|

NOTE: このフィールドは、上記の[Server URL]フィールドで
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。

 a|

バインドアカウント（オプション）

a|
LDAPサーバに対する検索クエリおよびグループ内の検索に使用する読み取り専用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」の場合は、などの値を入力します `CN=bindacct,CN=Users,DC=cpoc,DC=local`。

a|
バインドパスワード（オプション）

a|
NOTE: このフィールドは、バインドアカウントを入力すると表示されます。

バインドアカウントのパスワードを入力します。

a|
追加する前にサーバ接続をテストする

a|
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選択してテストに失敗した場合、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。

a|
権限の設定

a|
検索ベースDN

a|
ユーザを検索するLDAPコンテキストを入力します。通常はの形式で入力します `CN=Users, DC=cpoc, DC=local`。

a|
ユーザ名属性

a|
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`。

a|
グループ属性
a|
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`。

|===
====
. [*役割マッピング*（Role Mapping *）]タブをクリックします。
. 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
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 製品説明

a|
マッピング

a|
グループDN
a|
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。正規表現がサポートされています。正規表現パターンに含まれていない場合は、これらの特殊な正規表現文字をバックスラッシュ（\）でエスケープする必要があります。\.[]{}()<>*+-=!?^$|

a|
役割
a|
フィールド内をクリックし、グループDNにマッピングするローカルユーザロールを1つ選択します。このグループに含めるロールをそれぞれ個別に選択する必要があります。MonitorロールはSANtricity Unified
Managerにログインするため必要なロールであり、他のロールと一緒に指定する必要があります。各ロールの権限は次のとおりです。

** * 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。

|===
====
+

NOTE: Monitorロールは、管理者を含むすべてのユーザに必要です。

. 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。
. マッピングが終了したら、*追加*をクリックします。
+
システムによって検証が実行され、ストレージアレイとLDAPサーバが通信できるかどうかが確認されます。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。

[[IDd7c67b0aefccde036cb52ab2e204a10b]]
= ディレクトリサーバの設定とロールマッピングの編集
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセス管理でディレクトリサーバをすでに設定している場合は、その設定をいつでも変更できます。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。

.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を定義する必要があります。

.手順
. アクセス管理*を選択します。
. [*ディレクトリサービス*]タブを選択します。
. 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。
. 「*表示/設定の編集*」を選択します。
+
[ディレクトリサーバーの設定]ダイアログボックスが開きます。

. サーバー設定*タブで、必要な設定を変更します。
+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 製品説明

a|
構成設定

a|
ドメイン
a|
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。

a|
サーバURL
a|
LDAPサーバにアクセスするためのURL（の形式） `ldap[s]://host:port`。

a|
バインドアカウント（オプション）
a|
LDAPサーバに対する検索クエリおよびグループ内の検索に使用する読み取り専用ユーザアカウント。

a|
バインドパスワード（オプション）
a|
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すると表示されます）。

a|
保存する前にサーバ接続をテストする
a|
システムがLDAPサーバ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選択してテストに失敗した場合、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。

a|
権限の設定

a|
検索ベースDN
a|
ユーザを検索するLDAPコンテキスト。通常はの形式です。 `CN=Users, DC=cpoc, DC=local`

a|
ユーザ名属性
a|
認証用のユーザIDにバインドされた属性。例：
`sAMAccountName`。

a|
グループ属性
a|
ユーザのグループ属性のリスト。グループとロールのマッピングに使用されます。例：
`memberOf, managedObjects`。

|===

```
====
. [*役割マッピング*]タブで、目的のマッピングを変更します。
+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 製品説明


 a|
*マッピング*


 a|
グループDN
 a|
マッピングするLDAPユーザグループのドメイン名。正規表現がサポートされています。これらの特殊正規表現文字が正規表現パターンに含まれていない場合は、バックスラッシュ（\）でエスケープする必要があります。

\.[]{}()<>*+-=！？^$|


 a|
役割
 a|
グループDNにマッピングするロール。このグループに含めるロールをそれぞれ個別に選択する必要があります。MonitorロールはSANtricity Unified Managerにログインするため必要なロールであり、他のロールと一緒に指定する必要があります。ロールには次のものがあります。

** * 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。


|===
```

```
====
+

NOTE: Monitorロールは、管理者を含むすべてのユーザに必要です。

. 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。
. [ 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。現在のユーザーセッションのみが保持されます。



[[IDc0251ddc7acce1772ef25e00c4000cd5]]
= ディレクトリサーバの削除
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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]ページで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たあとに古いサーバを削除する場合に実行できます。

.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。

.タスクの内容
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。現在のユーザーセッションのみが保持されます。

.手順
. アクセス管理*を選択します。
. [*ディレクトリサービス*]タブを選択します。
. リストから、削除するディレクトリサーバを選択します。
. [ 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。

. フィールドにと入力し `remove`、*[削除]*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。

:leveloffset: -1

= SAMLを使用

:leveloffset: +1

[[ID7897fae080fffbd7bf18e12d5d5af22e]]
= SAMLの設定
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセス管理用の認証を設定するには、ストレージアレイに組み込みのSecurity Assertion Markup Language（
SAML）機能を使用できます。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。

.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。
* ストレージアレイのコントローラの
IPアドレスまたはドメイン名を確認しておく必要があります。
* 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が同期されていることを確認しておきます（
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、Unified
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。

.タスクの内容

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。多要素認証を提供し、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IdPを設定できます。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が設定されている場合、ストレージアレイは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。次に、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。

[NOTE]
====
* 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設定している場合にSAMLを有効にすると、Unified ManagerではSAMLがディレクトリサービスよりも優先されます。SAMLをあとで無効にすると、ディレクトリサービスの設定は以前の設定に戻ります。

====
[CAUTION]
====
*編集と無効化。*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。

====
SAML認証の設定は複数の手順で構成されます。

== 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、Unified ManagerにIdPメタデータをインポートします。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。

.手順
. メニューを選択します。Settings [Access Management]。
. SAML *タブを選択します。
+
設定手順の概要が表示されます。

. 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。
+
[Import Identity Provider File]ダイアログボックスが開きます。

. 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。

. [* 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には、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。このメタデータは、IdPがコントローラとの信頼関係を確立し、許可要求を処理するために必要です。このファイルには、IdPがサービスプロバイダと通信できるように、コントローラのドメイン名やIPアドレスなどの情報が含まれています。

.手順
. [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]ダイアログボックスが開きます。

. 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。
+
「*Export」をクリックすると、サービスプロバイダの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。ファイルが保存されている場所をメモします。

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

Unified Managerへのアクセスをユーザに許可するには、IdPユーザの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。

.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Unified Managerにインポートします。

* 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が、信頼関係のIdPシステムにインポートされている。

.手順
. 「mapping Unified Manager * roles」のリンクをクリックします。
+
ロールマッピング(Role Mapping)ダイアログボックスが開きます

. 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
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 製品説明

a|
マッピング

a|
ユーザ属性
a|
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。

a|
属性値
a|
マッピングするグループの属性値を指定します。正規表現がサポートされています。(`\`正規表現パターンに含まれていない特殊な正規表現文字は、バックスラッシュでエスケープする必要があります。\.[]{}()<>*+-=!?^$|

a|
役割
a|
フィールド内をクリックし、属性にマッピングするストレージアレイのロールを1つ選択します。含めるロールをそれぞれ個別に選択する必要があります。Monitorロールは Unified Managerにログインするために必要な他のロールと一緒に指定する必要があります。少なくとも1つ

のグループにはSecurity Adminロールも必要です。

各ロールの権限は次のとおりです。

** * 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。

|===
====
+
[NOTE]
====
Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールが割り当てられていないユーザのUnified Managerは正しく動作しません。

====
. 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。
+
[NOTE]
====
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。

====
. 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。

.開始する前に

* IdPのメタデータファイルをUnified Managerにインポートします。
* 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が、信頼関係の
IdPシステムにインポートされている。

.手順
. [Test SSO Login*]リンクを選択します。
+
SSOクレデンシャルを入力するためのダイアログボックスが開きます。

. 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は、ダイアログボックスが開きます。

. 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かった場合は、エラーメッセージと詳細情報が表示されます。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アドレスが正しい。

== 手順5：SAMLを有効にする

最後に、ユーザ認証用のSAMLの設定を完了します。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、前の手順で説明しています。

.開始する前に
* IdPのメタデータファイルをUnified Managerにインポートします。
* 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が、信頼関係の
IdPシステムにインポートされている。
* 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。

[CAUTION]
====
*編集と無効化。*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。

====
.手順
. [* SAML *]タブで、[* SAMLを有効にする]リンクを選択します。
+
[SAMLの有効化の確認]ダイアログボックスが開きます。

. と入力し `enable`、*[有効化]*をクリックします。
. SSOログインテスト用の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。

[[ID0e0949e46c0e798eb608a7c8751faf7a]]
= SAMLロールマッピングの変更
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
アクセス管理用にSAMLを設定している場合は、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の間のロールマッピングを変更できます。

.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
. メニューを選択します。Settings [Access Management]。
. SAML *タブを選択します。
. [*役割のマッピング*]を選択します。
+
ロールマッピング(Role Mapping)ダイアログボックスが開きます

. 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。
+
[CAUTION]
====
SAMLが有効になっている間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、Unified Managerにアクセスできなくなります。

====
+
.フィールドの詳細
[%collapsible]
====
[cols="25h,~"]
|===
| 設定 | 製品説明

 a|
マッピング

 a|
ユーザ属性
 a|
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。

 a|
属性値
 a|
マッピングするグループの属性値を指定します。

 a|
役割
 a|
フィールド内をクリックし、属性にマッピングするストレージアレイのロールを1つ選択します。このグループに含めるロールをそれぞれ個別に選択する必要があります。Monitorロールは Unified Managerにログインするために必要な他のロールと一緒に指定する必要があります。少なくとも1つのグループにSecurity
Adminロールを割り当てる必要があります。各ロールの権限は次のとおりです。

** * 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。

|===
====
+

NOTE: Monitorロールは、管理者を含むすべてのユーザに必要です。
Monitorロールが割り当てられていないユーザのUnified Managerは正しく動作しません。

. 必要に応じて、* 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。
. [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。現在のユーザーセッションのみが保持されます。

[[ID07b6aaf334cfa34916b0ae417667d0a5]]
= SAMLサービスプロバイダファイルのエクスポート
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
必要に応じて、ストレージアレイのサービスプロバイダメタデータをエクスポートし、その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できます。

.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。

.タスクの内容
このタスクでは、コントローラからメタデータ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信頼関係を確立し、認証要求を処理するために必要です。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
. メニューを選択します。Settings [Access Management]。
. SAML *タブを選択します。
. 「*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]ダイアログボックスが開きます。

. [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。
+
[NOTE]
====
ドメイン名フィールドは読み取り専用です。

====
+
ファイルが保存されている場所をメモします。

. ローカルシステムで、エクスポートした
XML形式のサービスプロバイダメタデータファイルを探します。
.
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、コントローラ情報を手動で入力することもできます。
. [* 閉じる *] をクリックします。

:leveloffset: -1

= FAQ

:leveloffset: +1

[[IDd570e40b61a2ad52272750f67f0e2592]]
= ログインできないのはなぜですか？

```
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
ログイン時にエラーが表示された場合は、次の原因を確認してください。

ログインエラーは、次のいずれかの理由で発生する可能性があります。

* 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。
* Privilegesが不十分です。
* ログインに何度も失敗したため、ロックアウトモードがトリガーされました。
10分待ってから再ログインしてください。
* SAML認証が有効になりました。ブラウザの表示を更新してログインします。




[[IDdc7cc639c10528d2246aeaf1b536248e]]
= 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？
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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をローカルマシンにインストールする必要があります。




[[IDecf017413500378c8f73b7a374a78ef8]]
=
ストレージアレイのロールに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？
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]
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。

[NOTE]
====
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。

* 管理者がディレクトリサービスでユーザーグループを定義しました。
* 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。

== 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。
*
マッピングするグループの属性値がわかっている必要があります。正規表現がサポートされています。（`\`正規表現パターンに含まれていない特殊な正規表現文字は、バックスラッシュでエスケープする必要があります）。
+
[listing]

```
\.[]{}()<>*+-=!?^$|
----
* Monitorロールは、管理者を含むすべてのユーザに必要です。
Monitorロールが割り当てられていないユーザのUnified Managerは正しく動作しません。



[[ID2fd71270ddc31aef2686b5ec0df545af]]
= SAMLを設定して有効にするときは、どのような点に注意する必要がありますか？
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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

開始する前に、次のこと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きます。
* 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が同期されていることを確認しておきます（
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、Unified
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いることを確認してください。

* 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。（SAMLを有効にする前にSSOログインのテストも実行されます）。
* 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またはディレクトリサービス）が自動的にリストアされます。
* 現在ユーザ認証用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が設定されている場合、次のクライアントはストレージアレイ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たログイン

[[IDb42ad0bece338ecf63c01d6aa8106d6b]]
= ローカルユーザとは何ですか？
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ローカルユーザはシステムに事前に定義されており、特定の権限が含まれています。

ローカルユーザは次のとおりです。

* *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。

:leveloffset: -1

:leveloffset: -1

:leveloffset: -1

:leveloffset: -1

<<<
著作権に関する情報

の使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

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

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

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

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

商標に関する情報

NetApp、NetAppのロゴ、link:http://www.netapp.com/TM[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。