証明書と認証

SANtricity 11.6

NetApp
February 12, 2024

目次

証明書と認証

証明書管理

概念

証明書の仕組み

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

署名済み証明書

証明書を使用すると、指定されたサーバとクライアント間でのみ、Web通信が非公開かつ変更されずに暗号化された形式で送信されます。Unified Managerを使用すると、ホスト管理システムのブラウザおよび検出されたストレージ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、第三者が所有者のIDを検証し、そのデバイスが信頼できると判断したことを意味します。ストレージアレイの各コントローラには、自動生成された自己署名証明書が付属しています。自己署名証明書を引き続き使用することも、CA署名証明書を取得してコントローラとホストシステム間のよりセキュアな接続を確立することもできます。

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

署名済み証明書は、信頼できる第三者機関である認証局（CA）によって検証されます。署名済み証明書には、エンティティ（通常、サーバまたはWebサイト）の所有者に関する詳細、証明書の問題 および有効期限、エンティティの有効なドメイン、およびアルファベットと数字で構成されるデジタル署名が含まれています。

ブラウザを開いてWebアドレスを入力すると、証明書チェックプロセスがバックグラウンドで実行され、有効なCA署名証明書を含むWebサイトに接続しているかどうかが確認されます。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、鍵のアイコンとhttpsの指定が含まれています。CA署名証明書が含まれていないWebサイトに接続しようとすると、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、アプリケーションプロセス中に自分の身元を確認するための手順を実行します。登録済みの会社にEメールを送信し、会社の住所を確認して、HTTPまたはDNSの検証を実行する場合があります。アプリケーションプロセスが完了すると、ホスト管理システムにロードするデジタルファイルがCAから送信されます。通常、これらのファイルには次のような信頼チェーンが含まれます。

- ルート--階層の最上位にあるのはルート証明書です。この証明書には、他の証明書への署名に使用する秘密鍵が含まれています。ルートは特定のCA組織を識別します。すべてのネットワークデバイスで同じCAを使用する場合は、ルート証明書が1つだけ必要です。
- *Intermediate *--ルートからの分岐は中間証明書です。CAは、保護されたルート証明書とサーバ証明書の間の証明書として機能する、1つ以上の中間証明書を発行します。
- サーバー--チェーンの下部にあるサーバー証明書は、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および送信されることも保証されます。

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

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。

証明書の用語

証明書管理に関連する用語を次に示します。

期間	説明
できます	認証局（CA）は、インターネットセキュリティのためにデジタル証明書と呼ばれる電子文書を発行する信頼されたエンティティです。証明書でWebサイトの所有者を識別することにより、クライアントとサーバの間のセキュアな接続が確立されます。
CSR	証明書署名要求（CSR）は、申請者から認証局（CA）に送信されるメッセージです。CSRは、CAが証明書の問題 に必要な情報を検証します。
証明書	証明書はセキュリティ上の目的でサイトの所有者を識別するもので、攻撃者による偽装を防止します。証明書には、サイトの所有者に関する情報と、その情報について証明（署名）する信頼されたエンティティのIDが含まれます。
証明書チェーン	証明書にセキュリティレイヤを追加するファイルの階層。通常、チェーンの最上位にはルート証明書が1つ、中間証明書が1つ以上、エンティティを識別するサーバ証明書が1つ含まれます。

期間	説明
中間証明書	証明書チェーンのルートから1つ以上の中間証明書が分岐します。CAは、保護されたルート証明書とサーバ証明書の間の証明書として機能する、1つ以上の中間証明書を発行します。
キーストア	キーストアはホスト管理システム上のリポジトリであり、秘密鍵とそれに対応する公開鍵および証明書が格納されています。これらのキーと証明書によって、コントローラなどの独自のエンティティが識別されます。
ルート証明書	ルート証明書は、証明書チェーンの階層の最上位にあります。この証明書には、他の証明書への署名に使用する秘密鍵が含まれています。ルートは特定のCA組織を識別します。すべてのネットワークデバイスで同じCAを使用する場合は、ルート証明書が1つだけ必要です。
署名済み証明書	認証局（CA）によって検証される証明書。このデータファイルには秘密鍵が含まれており、サーバとクライアントの間でHTTPS接続を介してデータが暗号化された形式で送信されることが保証されます。また、署名済み証明書には、エンティティ（通常、サーバまたはWebサイト）の所有者に関する詳細およびアルファベットと数字で構成されるデジタル署名が含まれています。署名済み証明書は信頼チェーンを使用するため、本番環境で最もよく使用されます。「CA署名証明書」または「管理証明書」とも呼ばれます。
自己署名証明書	自己署名証明書は、エンティティの所有者によって検証されます。このデータファイルには秘密鍵が含まれており、サーバとクライアントの間でHTTPS接続を介してデータが暗号化された形式で送信されることが保証されます。また、アルファベットと数字で構成されるデジタル署名も含まれます。自己署名証明書はCA署名証明書と同じ信頼チェーンを使用しないため、テスト環境で最もよく使用されます。「事前にインストールされている」証明書とも呼ばれます。
サーバ証明書	サーバ証明書は、証明書チェーンの最下位にあります。Webサイトやその他のデバイスなど、特定のエンティティを識別します。ストレージシステムの各コントローラには個別のサーバ証明書が必要です。
信頼ストア	信頼ストアは、CAなどの信頼できるサードパーティの証明書を格納するリポジトリです。
Web Services Proxyの使用方法	Web Services Proxyは標準のHTTPSメカニズムによるアクセスを提供するプロキシで、管理者にストレージアレイの管理サービスの設定を許可します。このプロキシは、WindowsホストまたはLinuxホストにインストールできます。Unified ManagerインターフェイスにはWeb Services Proxyが付随しています。

方法

CA署名証明書を使用する

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

作業を開始する前に

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

このタスクについて

CA署名証明書の使用は、2つの手順で構成された手順 です。

手順1：CSRを作成および送信します

最初に証明書署名要求（CSR）ファイルを生成し、そのファイルをCAに送信する必要があります。

作業を開始する前に

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

このタスクについて

このタスクでは、Unified ManagerとWeb Services Proxyをホストするシステムの署名付き管理証明書を受け取るためにCAに送信するCSRファイルを生成する方法について説明します。組織に関する情報とともに、ホストシステムのIPアドレスまたはDNS名を指定する必要があります。

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

手順

1. [証明書管理]を選択します。
2. [管理（**Management**）]タブで、[CSR全体*（* Complete CSR *）]を選択します。
3. 次の情報を入力し、[次へ*]をクリックします。
   - 組織--会社または組織の正式名称。Inc.やCorp.などの接尾辞も含めて入力してください
   - 組織単位（オプション）--証明書を処理している組織の部門。
   - 市区町村--ホストシステムまたは事業の所在地である市区町村。
   - 都道府県(オプション)--ホストシステムまたは事業の所在地である都道府県。
   - 国の**ISO**コード--自国を表す2桁のISO（国際標準化機構）コード（USなど）。
4. ホストシステムに関する次の情報を入力します。
   - 共通名-- Webサービスプロキシがインストールされているホストシステムの IPアドレスまたはDNS名。このアドレスが正しいことを確認してください。ブラウザでUnified Managerにアクセスする際に入力したアドレスと正確に一致している必要があります。http：//またはhttps：//を含めないでください。
   - 代替**IP**アドレス--共通名がIPアドレスの場合は’オプションでホストシステムの追加のIPアドレスまたはエイリアスを入力できます複数指定する場合は、カンマで区切って入力します。
   - 代替**DNS**名--共通名がDNS名の場合は’ホストシステムの追加のDNS名を入力します複数指定する場合は、カンマで区切って入力します。代替DNS名がない場合は、最初のフィールドに入力したDNS名を

ここにコピーします。

5. [完了] をクリックします。

   CSRファイルがローカルシステムにダウンロードされます。ダウンロードフォルダの場所は、ブラウザによって異なります。

6. CSRファイルをCAに送信し、PEM形式またはDER形式の署名済み証明書を要求します。

完了後

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

手順2：管理証明書をインポートする

署名済み証明書を受け取ったあと、Unified Managerインターフェイスがインストールされているホストシステムの証明書チェーンをインポートします。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。
- 証明書署名要求（.CSRファイル）を生成してCAに送信しておきます。
- 信頼された証明書ファイルをCAから受け取っておきます。
- 証明書ファイルがローカルシステムにインストールされている必要があります。
- CAからチェーン証明書（たとえば、.p7bファイル）が提供された場合は、チェーンファイルを個々のファイル（ルート証明書、1つ以上の中間証明書、サーバ証明書）に展開する必要があります。Windowsのcertmgrユーティリティーを使用してファイルを展開できます(右クリックして[**menu: All Tasks[Export]**)を選択します)エクスポートが完了すると、チェーン内の証明書ファイルごとに1つのCERファイルが表示されます。

手順

1. [証明書管理]を選択します。
2. [管理（ Management）]タブで、[インポート（ Import）]を選択します。

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

3. [**Browse**](参照)をクリックして、最初にルートファイルと中間ファイルを選択し、次にサーバー証明書を選択します。

   ファイル名がダイアログボックスに表示されます。

4. [* インポート *] をクリックします。

結果

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

管理証明書をリセットします

管理証明書を工場出荷時の自己署名証明書の状態に戻すことができます。

作業を開始する前に

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

このタスクについて

このタスクでは、WebサービスプロキシとSANtricity Unified Managerがインストールされているホストシステムから現在の管理証明書を削除します。証明書をリセットすると、ホストシステムでは自己署名証明書が再び使用されるようになります。

手順

1. [証明書管理]を選択します。
2. [管理（ Management）]タブで、[リセット（ Reset）]を選択します。

   [管理証明書のリセットの確認]ダイアログボックスが開きます。

3. フィールドに「reset」と入力し、「* Reset *」をクリックします。

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

結果

システムでサーバの自己署名証明書が再び使用されるようになります。そのため、セッションの自己署名証明書を手動で承認するように求められます。

アレイの証明書をインポートします

必要に応じて、SANtricity Unified Managerをホストするシステムで認証できるように、ストレージアレイの証明書をインポートすることができます。証明書には、認証局（CA）が署名した証明書と自己署名の証明書があります。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。
- 信頼された証明書をインポートする場合は、SANtricity System Managerを使用してストレージアレイのコントローラの証明書をインポートする必要があります。

手順

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

   このページには、ストレージ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。

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

   表示を制限するには、[*次の証明書を表示…]フィルタリングフィールドを使用するか、いずれかの列見出

しをクリックして証明書の行をソートします。

4. ダイアログボックスで証明書を選択し、*インポート*をクリックします。

   証明書がアップロードされて検証されます。

証明書を表示します

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

作業を開始する前に

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

手順

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

証明書をエクスポートします

証明書をエクスポートして詳細を確認することができます。

作業を開始する前に

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

手順

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

5. 証明書ビューアアプリケーションでファイルを開きます。

信頼された証明書を削除する

期限切れになった証明書など、不要になった証明書を削除することができます。

作業を開始する前に

古い証明書を削除する前に、新しい証明書をインポートしてください。

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

手順

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

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

   [信頼された証明書の削除の確認]ダイアログボックスが開きます。

4. 削除を確認し、* Delete *をクリックします。

   証明書がテーブルから削除されます。

信頼されていない証明書を

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

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。
- CA署名証明書をインポートする場合は、次の点に注意してください。
  - ストレージ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上にある必要があります。

このタスクについて

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

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

手順

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

   このページには、ストレージ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。

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

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

4. ダイアログボックスで証明書を選択し、*インポート*をクリックします。

   証明書がアップロードされて検証されます。

アクセス管理

概念

アクセス管理の仕組み

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

設定ワークフロー

アクセス管理の設定は次のように行います。

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

   初めてのログインでは'ユーザ名adminが自動的に表示され'変更することはできませんadminユーザは'システムのすべての機能にフル・アクセスできます初回ログイン時にパスワードを設定する必要があります。

2. ユーザインターフェイスでアクセス管理に移動します。事前に設定されているローカルユーザロールが表示されます。これらのロールはRBAC（ロールベースアクセス制御）機能の実装です。
3. 管理者は、次の認証方式を1つ以上設定します。
   - ローカルユーザーの役割-- 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に必要な設定はありません。

- ディレクトリサービス-- LDAP (Lightweight Directory Access Protocol)サーバとディレクトリサービス(MicrosoftのActive Directoryなど)を介して認証を管理します管理者がLDAPサーバに接続し、ローカルユーザロールにLDAPユーザをマッピングします。

4. Unified Managerのログインクレデンシャルをユーザに割り当てます。
5. ユーザが自身のクレデンシャルを入力してシステムにログインします。ログイン時には、次のバックグラウンドタスクが実行されます。
   - ユーザ名とパスワードをユーザアカウントと照合して認証します。
   - 割り当てられたロールに基づいてユーザの権限が決まります。
   - ユーザインターフェイスの機能にユーザがアクセスできるようにします。
   - 上部のバナーにユーザ名が表示されます。

Unified Managerで使用できる機能

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

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

使用できない機能は、ユーザインターフェイスではグレー表示されるか、非表示になります。

アクセス管理の用語

SANtricity Unified Managerに関連するアクセス管理の用語を次に示します。

期間	説明
Active Directory	Active Directory（AD）は、Windowsドメインネットワーク用のLDAPを使用するMicrosoftのディレクトリサービスです。
結合	バインド処理は、ディレクトリサーバに対するクライアントの認証に使用されます。通常はアカウントとパスワードのクレデンシャルが必要ですが、匿名のバインド処理が可能なサーバもあります。
できます	認証局（CA）は、インターネットセキュリティのためにデジタル証明書と呼ばれる電子文書を発行する信頼されたエンティティです。証明書でWebサイトの所有者を識別することにより、クライアントとサーバの間のセキュアな接続が確立されます。
証明書	証明書はセキュリティ上の目的でサイトの所有者を識別するもので、攻撃者による偽装を防止します。証明書には、サイトの所有者に関する情報と、その情報について証明（署名）する信頼されたエンティティのIDが含まれます。

期間	説明
LDAP	Lightweight Directory Access Protocol（LDAP）は、分散型のディレクトリ情報サービスへのアクセスと管理に使用されるアプリケーションプロトコルです。このプロトコルを使用すると、さまざまなアプリケーションやサービスがLDAPサーバに接続してユーザを検証できます。
RBAC	ロールベースアクセス制御（RBAC）は、コンピュータやネットワークリソースへのアクセスを個々のユーザのロールに基づいて制御する手法です。Unified Managerには事前定義されたロールがあります
SSO	シングルサインオン（SSO）は、1組のログインクレデンシャルで複数のアプリケーションにアクセスできるようにする認証サービスです。
Web Services Proxyの使用方法	Web Services Proxyは標準のHTTPSメカニズムによるアクセスを提供するプロキシで、管理者にストレージアレイの管理サービスの設定を許可します。このプロキシは、WindowsホストまたはLinuxホストにインストールできます。Unified ManagerインターフェイスはWeb Services Proxyで使用できます。

マッピングされたロールの権限

ロールベースアクセス制御（RBAC）機能には、1つ以上のロールがマッピングされた事前定義済みのユーザが含まれています。各ロールには、SANtricity Unified Managerのタスクにアクセスするための権限が含まれています。

これらのロールにより、次のタスクへのアクセスが可能になります。

- * Storage admin *--アレイ上のストレージ・オブジェクトへの読み取り/書き込みのフル・アクセスを提供しますが’セキュリティ構成へのアクセスはありません
- * Security admin *--アクセス管理と証明書管理のセキュリティ設定へのアクセス。
- * Support admin *--ストレージ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。

ローカルユーザロールを使用したアクセス管理

管理者は、SANtricity Unified Managerに組み込みのロールベースアクセス制御（RBAC）機能を使用できます。これらの機能のことを「ローカルユーザロール」と呼びます。

設定ワークフロー

ローカルユーザロールはシステムで事前に設定されています。認証にローカルユーザロールを使用する場合、管理者は次の操作を行うことができます。

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

   adminユーザは’システムのすべての機能にフル・アクセスできます

2. ユーザプロファイルを確認します。ユーザプロファイルは事前に定義されており、変更することはできません。
3. *オプション：*管理者が各ユーザプロファイルに新しいパスワードを割り当てます。
4. ユーザは各自に割り当てられたクレデンシャルでシステムにログインします。

管理

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

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

ディレクトリサービスを使用したアクセス管理

LDAP（Lightweight Directory Access Protocol）サーバとディレクトリサービス（MicrosoftのActive Directoryなど）を使用して認証を管理することができます。

設定ワークフロー

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

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

   adminユーザは’システムのすべての機能にフル・アクセスできます

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

管理

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

- ディレクトリサーバを追加します。

- ディレクトリサーバの設定を編集します。
- LDAPユーザをローカルユーザロールにマッピングする。
- ディレクトリサーバを削除する。
- パスワードを変更します。
- パスワードの最小文字数を設定する。
- パスワードなしでのログインをユーザに許可します。

方法

ローカルユーザロールを表示します

[ローカルユーザーの役割]タブでは、ユーザーとデフォルトの役割とのマッピングを表示できます。これらのマッピングは、SANtricity Unified ManagerのWebサービスプロキシで適用されるRBAC（ロールベースアクセス制御）の一部です。

作業を開始する前に

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

このタスクについて

ユーザとマッピングは変更できません。変更できるのはパスワードだけです。

手順

1. アクセス管理*を選択します。
2. [ローカルユーザー役割*（Local User Roles *）]タブを選択します。

   表にユーザが表示されます。

   - **admin**--システム内のすべての機能にアクセスできるスーパー管理者。このユーザにはすべてのロールが含まれています
   - * storage *--すべてのストレージ・プロビジョニングを担当する管理者。このユーザには、Storage Admin、Support Admin、Monitorのロールが含まれています。
   - * security *--アクセス管理や証明書管理など、セキュリティ設定を担当するユーザー。このユーザには、Security AdminとMonitorのロールが含まれています。
   - * support *--ハードウェアリソース、障害データ、ファームウェアアップグレードを担当するユーザー。このユーザには、Support AdminとMonitorのロールが含まれています。
   - *monitor *--システムへの読み取り専用アクセス権を持つユーザー。このユーザにはMonitorロールのみが含まれています。
   - * rw *（読み取り/書き込み）-このユーザには、Storage Admin、Support Admin、Monitorのロールが含まれています。
   - * ro *（読み取り専用）--このユーザーには、Monitorロールのみが含まれています。

パスワードを変更します

アクセス管理で各ユーザのユーザパスワードを変更できます。

作業を開始する前に

- Root Adminの権限が割り当てられたローカル管理者としてログインする必要があります。
- ローカル管理者のパスワードを確認しておく必要があります。

このタスクについて

パスワードを選択する際は、次のガイドラインに注意してください。

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

手順

1. アクセス管理*を選択します。
2. [ローカルユーザー役割*（Local User Roles *）]タブを選択します。
3. 表からユーザを選択します。

   [パスワードの変更*]ボタンが使用可能になります。

4. [パスワードの変更 *] を選択します。

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

5. ローカルユーザパスワードに対して最小文字数が設定されていない場合は、システムにアクセスするユーザにパスワードの入力を求めるチェックボックスを選択できます。
6. 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。
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。

結果

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

ローカルユーザパスワードの設定を変更します

すべての新規または更新されるローカルユーザパスワードの最小文字数を設定できます。また、ローカルユーザがパスワードを入力せずにシステムにアクセスできるようにすることもできます。

作業を開始する前に

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

このタスクについて

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

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

手順

1. アクセス管理*を選択します。
2. [ローカルユーザー役割*（Local User Roles *）]タブを選択します。
3. 「表示/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。

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

     新しいローカルユーザパスワードは、現在の設定以上の長さにする必要があります。

5. [保存（ Save ）] をクリックします。

ディレクトリサーバを追加します

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

作業を開始する前に

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

このタスクについて

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

手順

1. アクセス管理*を選択します。
2. [ディレクトリサービス]タブで、[ディレクトリサーバーの追加]を選択します。

   [ディレクトリサーバーの追加*]ダイアログボックスが開きます。

3. [サーバー設定]タブで、LDAPサーバーの資格情報を入力します。

フィールドの詳細

設定	説明
構成設定	ドメイン
LDAPサーバのドメイン名を入力します。ドメインを複数入力する場合は、カンマで区切って入力します。ドメイン名は、ログイン（*username@domain*）で、認証するディレクトリサーバを指定するために使用されます。	サーバURL
LDAPサーバにアクセスするためのURLを'ldap[s]:///*host:port*'の形式で入力します	証明書のアップロード（オプション）
このフィールドは、上記のサーバURLフィールドにLDAPSプロトコルが指定されている場合にのみ表示されます。 [**Browse**]をクリックして、アップロードするCA証明書を選択します。これは、LDAPサーバの認証に使用される信頼された証明書または証明書チェーンです。	バインドアカウント（オプション）

設定	説明
LDAPサーバに対する検索クエリやグループ内の検索で使用する読み取り専用のユーザアカウントを入力します。アカウント名はLDAPタイプの形式で入力します。たとえば、バインドユーザの名前が「bindacct」であれば、「CN=bindacct、CN=Users、DC=cpoc、DC=local」などと入力します。	バインドパスワード（オプション）
このフィールドは、バインドアカウントを入力した場合に表示されます。 バインドアカウントのパスワードを入力します。	追加する前にサーバ接続をテストします
入力したLDAPサーバの設定でシステムと通信できるかどうかを確認するには、このチェックボックスを選択します。このテストは、ダイアログボックスの下部にある*追加*（* Add *）をクリックした後に実行されます。このチェックボックスをオンにした場合、テストに失敗すると設定は追加されません。設定を追加するには、エラーを解決するか、チェックボックスを選択解除してテストをスキップする必要があります。	権限の設定

設定	説明
検索ベースDN	ユーザーを検索するLDAPコンテキストを入力します通常は'CN=Users'DC=copc'DC=local'の形式で入力します
ユーザー名属性	認証用のユーザIDにバインドされた属性を入力します。例:「sAMAccountName」。
グループ属性	グループとロールのマッピングに使用される、ユーザの一連のグループ属性を入力します。例: memberOf, managedObjects`

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

   フィールドの詳細

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

   Monitorロールは、管理者を含むすべてのユーザに必要です。

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

   ストレージアレイとLDAPサーバが通信できるかどうかの検証がシステムによって実行されます。エラーメッセージが表示された場合は、ダイアログボックスで入力したクレデンシャルを確認し、必要に応じて情報を再入力します。

ディレクトリサーバ設定とロールマッピングを編集します

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

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- ディレクトリサーバが定義されている必要があります。

手順

1. アクセス管理*を選択します。
2. [ディレクトリサービス]タブを選択します。
3. 複数のサーバが定義されている場合は、編集するサーバを表から選択します。
4. 「表示/設定の編集」を選択します。

   [ディレクトリサーバー設定]ダイアログボックスが開きます。

5. サーバー設定*タブで、必要な設定を変更します。

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

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

6. [役割マッピング]タブで、目的のマッピングを変更します。

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

Monitorロールは、管理者を含むすべてのユーザに必要です。

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

結果

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

ディレクトリサーバを削除します

ディレクトリサーバとWebサービスプロキシの間の接続を解除するには、アクセス管理

ページからサーバ情報を削除します。このタスクは、新しいサーバを設定して古いサーバを削除する場合などに実行します。

作業を開始する前に

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

このタスクについて

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

手順

1. アクセス管理*を選択します。
2. [ディレクトリサービス]タブを選択します。
3. リストから、削除するディレクトリサーバを選択します。
4. [削除（ Remove ）] をクリックします。

   [ディレクトリサーバーの削除*]ダイアログボックスが開きます。

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

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

よくある質問です

ログインできないのはなぜですか？

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

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

- 入力したユーザ名またはパスワードが正しくありません。
- 必要な権限がありません。
- ディレクトリサーバ（設定されている場合）が使用できない可能性があります。その場合は、ローカルユーザロールでログインしてみてください。
- ログインが複数回失敗したために、ロックアウトモードがトリガーされました。10分待ってから再度ログインしてください。

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

- 入力したパスワードが正しくありません。
- ログインが複数回失敗したために、ロックアウトモードがトリガーされました。10分待ってから再度ログインしてください。

- コントローラで使用されているクライアント接続が最大数に達している。複数のユーザまたはクライアントをチェックしてください。

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

アクセス管理でディレクトリサーバを追加する前に、一定の要件を満たす必要があります。

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

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

グループをロールにマッピングする前に、ガイドラインを確認してください。

RBAC（ロールベースアクセス制御）機能には次のロールがあります。

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

> Monitorロールは、管理者を含むすべてのユーザに必要です。

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

- ディレクトリサービスでユーザグループを定義しておきます。
- LDAPユーザグループのグループドメイン名を確認しておきます。

ローカルユーザとは何ですか？

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

ローカルユーザの例を次に示します。

- **admin**--システム内のすべての機能にアクセスできるスーパー管理者。このユーザにはすべてのロールが含まれています初回ログイン時にパスワードを設定する必要があります。
- * storage *--すべてのストレージ・プロビジョニングを担当する管理者。このユーザには、Storage Admin、Support Admin、Monitorのロールが含まれています。このアカウントは、パスワードが設定され

るまで無効になります。

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