証明書
SANtricity 11.8

NetApp
December 16, 2024

目次

証明書

証明書の概要

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：

- "証明書の仕組み"
- "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：

- "管理システム用のCA署名証明書の使用"
- "アレイの証明書のインポート"

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、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。

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。

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	製品説明
カリフォルニア州	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。
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が証明書を発行するため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、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。
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。
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、必要なルート証明書は1つだけです。
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、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。

期間	製品説明
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、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。
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。

管理システム用のCA署名証明書の使用

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。

> 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

1. [証明書管理]を選択します。
2. [管理]タブで、[* CSR全体*]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）。

4. 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。
5. 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。
6. [完了] をクリックします。
7. 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。

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

1. 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。

2. 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。

   - 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。

3. 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

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。

3. [**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。

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。証明書の情報が[証明書管理]ページに表示されます。

管理証明書のリセット

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

1. [設定]>[証明書]*を選択します。
2. 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。

3. 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

アレイの証明書のインポート

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

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. 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。

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。

信頼できる証明書の削除

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。

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

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。

信頼されない証明書の解決

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

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. 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。

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。

証明書の管理

証明書の表示

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

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。

証明書のエクスポート

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

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。

著作権に関する情報

商標に関する情報