証明書
SANtricity 11.5

NetApp
February 12, 2024

目次

証明書

概念

CA証明書の仕組み

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

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

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

信頼できる認証局のデジタル証明書を使用するには、次の手順が必要です。

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

証明書の用語

ストレージアレイに関連する証明書の用語を次に示します。

期間	説明
できます	認証局（CA）は、インターネットセキュリティのためにデジタル証明書と呼ばれる電子文書を発行する信頼されたエンティティです。証明書でWebサイトの所有者を識別することにより、クライアントとサーバの間のセキュアな接続が確立されます。
CSR	証明書署名要求（CSR）は、申請者から認証局（CA）に送信されるメッセージです。CSRは、CAが証明書の問題 に必要な情報を検証します。

期間	説明
証明書	証明書はセキュリティ上の目的でサイトの所有者を識別するもので、攻撃者による偽装を防止します。証明書には、サイトの所有者に関する情報と、その情報について証明（署名）する信頼されたエンティティのIDが含まれます。
クライアント証明書	セキュリティキー管理のために、クライアント証明書はストレージアレイのコントローラを検証し、キー管理サーバがコントローラのIPアドレスを信頼できるようにします。
キー管理サーバ証明書	セキュリティキー管理のために、キー管理サーバ証明書はサーバを検証し、ストレージアレイがサーバのIPアドレスを信頼できるようにします。
管理証明書	管理証明書は、認証局（CA）によって承認され、Webアプリケーションへのセキュアなアクセスを許可します。「署名済み証明書」とも呼ばれます。
OCSPサーバ	Online Certificate Status Protocol（OCSP）サーバは、スケジュールされた有効期限の前に認証局（CA）が証明書を失効させたかどうかを確認し、証明書が失効している場合はユーザがサーバにアクセスできないようにします。
自己署名証明書	自己署名証明書はコントローラに事前にロードされています。サイト接続が自己署名されている場合、Webアプリケーションに進む前に警告メッセージが表示されます。
信頼された証明書	認証局（CA）が発行した信頼された証明書は、証明書階層の最上位にある既知の証明書です。「ルート証明書」とも呼ばれます。

方法

コントローラの**CA**証明書署名要求（**CSR**）を作成します

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

作業を開始する前に

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

このタスクについて

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

手順

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

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

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

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

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

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

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

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

6. .CSRファイルをCAに送信します。

完了後

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

コントローラの信頼された証明書をインポートする

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

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。
- 証明書署名要求（.CSRファイル）を生成してCAに送信しておきます。
- 信頼された証明書ファイルをCAから受け取っておきます。
- 証明書ファイルがローカルシステムにインストールされている必要があります。

このタスクについて

このタスクでは、ストレージアレイのコントローラ用に信頼された証明書をアップロードする方法について説明します。

手順

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

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

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

   ダイアログボックスにファイル名が表示されます。

4. [* インポート *] をクリックします。

結果

ファイルがアップロードされて検証されます。

完了後

管理証明書をインポートします。

コントローラの管理証明書をインポートします

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

作業を開始する前に

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

このタスクについて

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

手順

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

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

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

   ファイル名がダイアログボックスに表示されます。

4. [* インポート *] をクリックします。

   ファイルがアップロードされて検証されます。

結果

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

インポートされた証明書の情報を表示

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

作業を開始する前に

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

このタスクについて

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

手順

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

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

信頼された証明書を削除する

ユーザがインポートした証明書を削除することができます。

作業を開始する前に

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

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

このタスクについて

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

手順

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

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

   [信頼された証明書の削除の確認]ダイアログボックスが開きます。

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

管理証明書をリセットします

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

作業を開始する前に

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

このタスクについて

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

手順

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

   [管理証明書のリセットの確認]ダイアログボックスが開きます。

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

結果

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

キーサーバの**CA**証明書署名要求（**CSR**）を実行します

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

作業を開始する前に

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

このタスクについて

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

手順

1. メニューから[設定][証明書]を選択します。
2. [キー管理]タブで、[* CSR全体*]を選択します。
3. 次の情報を入力します。

- 共通名--証明書ファイルに表示されるストレージアレイ名など、このCSRを識別する名前。
- 組織--会社または組織の正式名称。Inc.やCorp.などの接尾辞も含めて入力してください
- 組織単位（オプション）--証明書を処理している組織の部門。
- 市区町村--組織の所在地である市区町村。
- 都道府県(オプション)--組織の所在地である都道府県。
- 国の**ISO**コード--組織の所在地である米国などの2桁のISO（国際標準化機構）コード。

4. [* ダウンロード] をクリックします。
5. .CSRファイルをCAに送信します。

完了後

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

キー管理サーバ証明書をインポート

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

作業を開始する前に

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

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

- キー管理サーバ証明書が必要です。

> キー管理サーバ証明書は、ストレージアレイがサーバのIPアドレスを信頼できるように、サーバを検証します。キー管理サーバ証明書を取得するには、キー管理サーバから生成する必要があります。

このタスクについて

このタスクでは、ストレージアレイコントローラとキー管理サーバの間の認証用に証明書ファイルをアップロードする方法について説明します。

手順

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

証明書ファイルをインポートするためのダイアログボックスが表示されます。

3. ファイルを選択するには、*参照*ボタンをクリックします。

   ダイアログボックスにファイル名が表示されます。

4. [* インポート *] をクリックします。

   ファイルがアップロードされて検証されます。

キー管理サーバ証明書をエクスポートする

キー管理サーバ用の証明書をローカルマシンに保存できます。

作業を開始する前に

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

手順

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

   [保存（Save）]ダイアログボックスが開きます。

4. ファイル名を入力し、*保存*をクリックします。

証明書失効チェックを有効にします

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

作業を開始する前に

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

このタスクについて

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

手順

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

   失効チェックは、[キー管理]タブから有効にすることもできます。

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

結果

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

よくある質問です

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

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

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

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

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

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

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

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

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

キー管理サーバ証明書は、ストレージアレイがサーバのIPアドレスを信頼できるよう、キー管理サーバを検証します。キー管理サーバ証明書を取得するには、キー管理サーバから生成する必要があります。

証明書失効チェックについて、どのような点に注意する必要がありますか？

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

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

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

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

失効チェックが有効になるのはどのタイプのサーバですか？

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

著作権に関する情報

商標に関する情報