証明書を使用する
SANtricity 11.8

NetApp
December 16, 2024

目次

証明書を使用する . . . 1
- コントローラのCA署名証明書の使用 . . . 1
- 管理証明書のリセット . . . 3
- インポートした証明書情報の表示 . . . 4
- クライアントとして機能するコントローラの証明書のインポート . . . 5
- 証明書失効チェックを有効にする . . . 6
- 信頼できる証明書の削除 . . . 6
- キー管理サーバでの認証にCA署名証明書を使用する . . . 7
- キー管理サーバ証明書のエクスポート . . . 9

証明書を使用する

コントローラの**CA**署名証明書の使用

コントローラとSystem Managerへのアクセスに使用されるブラウザとの間のセキュアな通信を確立するために、CA署名証明書を取得できます。

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。
- 各コントローラのIPアドレスまたはDNS名を確認しておく必要があります。

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**：コントローラの**CSR**を作成します

最初に、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）ファイルを生成する必要があります。

タスクの内容

このタスクでは、System ManagerからCSRファイルを生成する方法について説明します。CSRは、組織に関する情報、およびコントローラのIPアドレスまたはDNS名を提供します。このタスクでは、ストレージアレイにコントローラが1つある場合は1つ、コントローラが2つある場合は2つのCSRファイルが生成されます。

> 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. メニューから[設定][証明書]を選択します。
2. [Array Management]タブで、[**Complete CSR**]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--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。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。
   - 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。複数のエントリを入力する場合は、カンマで区切って指定します。
   - 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。複数のエントリを入力する場合は、カンマで区切って指定します。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。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、エラーリカバリの状況で提供されます。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。ダウンロードのフォルダの場所は、ブラウザによって異なります。

6. 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、ファイルを認証局（CA）に送信します。Eシリーズシステムでは、署名済み証明書のPEM形式（Base64 ASCIIエンコード）が必要です。PEM、.crt、.cer、または.key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。
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：コントローラの署名済み証明書をインポートする]。

手順3：コントローラの署名済み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、コントローラのファイルをインポートします。

開始する前に

- 署名済み証明書ファイルをCAから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、コントローラを識別するサーバ証明書）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。
- System Managerにアクセスす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. 選択メニュー：設定[証明書]
2. Array Management（アレイ管理）タブで、* Import（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開きます。

3. 「*参照」ボタンをクリックして、最初にルート証明書と中間証明書ファイルを選択してから、コントローラの各サーバ証明書を選択します。ルートファイルと中間ファイルは両方のコントローラで同じです。サーバ証明書のみコントローラごとに一意です。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。

   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。

管理証明書のリセット

コントローラの証明書をCA署名証明書から工場出荷時の自己署名証明書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。
- CA署名証明書を事前にインポートしておく必要があります。

タスクの内容

リセット機能は、現在のCA署名証明書ファイルを各コントローラから削除します。その後、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

コントローラで自己署名証明書が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。

インポートした証明書情報の表示

[証明書]ページでは、証明書のタイプ、発行元機関、およびストレージアレイの証明書の有効な日付範囲を確認できます。

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。

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、証明書に関する情報を表示します。

タブ	製品説明
アレイ管理	ルートファイル、中間ファイル、サーバファイルなど、各コントローラ用にインポートしたCA署名証明書に関する情報が表示されます。

タブ	製品説明
信頼性	コントローラ用にインポートしたその他すべてのタイプの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証明書--ユーザーがストレージアレイにアップロードした証明書。これには、コントローラがサーバーではなくクライアントとして機能する場合に信頼された証明書、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含まれている自己署名証明書。
キー管理	外部キー管理サーバ用にインポートしたCA署名証明書に関する情報が表示されます。

クライアントとして機能するコントローラの証明書のインポート

ネットワークサーバの信頼チェーンを検証できないためにコントローラが接続を拒否した場合は、[信頼済み]タブから証明書をインポートして、コントローラ（クライアントとして機能）がそのサーバからの通信を受け入れることができます。

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。
- 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。

タスクの内容

別のサーバ（LDAPサーバやTLSを使用するsyslogサーバなど）からコントローラへの接続を許可する場合は、[信頼済み]タブから証明書をインポート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. [信頼済み]タブで、[インポート]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。
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。

証明書失効チェックを有効にする

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。

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。
- 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。

タスクの内容

自動失効チェックは、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。

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。

   また、*Key Management*タブから失効チェックを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。

信頼できる証明書の削除

以前にインポートしたユーザがインストールした証明書を[信頼済み]タブから削除できます。

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。
- 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。

> コントローラと別のサーバ（LDAPサーバなど）の認証に使用していた証明書を、交換用の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。

タスクの内容

このタスクでは、ユーザがインストールした証明書を削除する方法について説明します。あらかじめインストールされている自己署名証明書を削除することはできません。

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。

   この表には、ストレージアレイの信頼された証明書が表示されます。
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. フィールドにと入力し `delete`、*[削除]*をクリックします。

キー管理サーバでの認証にCA署名証明書を使用する

キー管理サーバとストレージアレイコントローラの間のセキュアな通信を実現するには、適切な証明書セットを設定する必要があります。

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。

タスクの内容

コントローラとキー管理サーバ間の認証は、2つの手順で行います。

手順1：キー管理サーバを使用した認証用に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CSRを使用して、キー管理サーバが信頼する認証局（CA）から署名済みのクライアント証明書を要求する必要があります。ダウンロードしたCSRファイルを使用して、キー管理サーバからクライアント証明書を作成してダウンロードすることもできます。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Key Management Interoperability Protocol（KMIP）要求を信頼できるようにします。

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、[**Complete CSR**]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--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。

   CSRファイルがローカルシステムに保存されます。
5. キー管理サーバによって信頼されているCAから署名済みクライアント証明書を要求します。
6. クライアント証明書がある場合は、に進みます[手順2：キー管理サーバの証明書をインポートする]。

手順2：キー管理サーバの証明書をインポートする

次の手順では、ストレージアレイとキー管理サーバの間の認証用の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、キー管理サーバ証明書はサーバを検証します。コントローラのクライアント証明書ファイルとキー管理サーバのサーバ証明書ファイルの両方をロードする必要があります。

開始する前に

- 署名済みのクライアント証明書ファイル（を参照手順1：キー管理サーバを使用した認証用にCSRを作成および送信します）を用意し、そのファイルをSystem Managerにアクセスするホストにコピーしておきます。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Key Management Interoperability Protocol（KMIP）要求を信頼できるようにします。
- キー管理サーバから証明書ファイルを取得し、そのファイルをSystem Managerにアクセスするホストにコピーする必要があります。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に、キー管理サーバを検証します。キー管理サーバには、ルート証明書、中間証明書、またはサーバ証明書を使用できます。

  サーバ証明書の詳細については、キー管理サーバのドキュメントを参照してください。

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開きます。
3. Select client certificate の横にある Browse *ボタンをクリックして、ストレージアレイのコントローラ用のクライアント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. キー管理サーバのサーバ証明書の選択*の横にある*参照*ボタンをクリックして、キー管理サーバのサーバ証明書ファイルを選択します。キー管理サーバのルート証明書、中間証明書、またはサーバ証明書を選択できます。

   ダイアログボックスにファイル名が表示されます。

5. [* 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のエクスポート

キー管理サーバの証明書をローカルマシンに保存できます。

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。
- 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。

著作権に関する情報

商標に関する情報