



証明書を使用する SANtricity 11.7

NetApp
February 12, 2024

目次

証明書を使用する	1
コントローラのCA署名証明書を使用する	1
管理証明書をリセットします	4
インポートされた証明書の情報を表示	4
クライアントとして機能するコントローラの証明書をインポートする	5
証明書失効チェックを有効にします	6
信頼された証明書を削除する	7
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をエクスポートする	9

証明書を使用する

コントローラのCA署名証明書を使用する

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。

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。
- 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。

このタスクについて

CA署名証明書の使用は、3つの手順で構成される手順です。

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。

このタスクについて

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、組織に関する情報とコントローラのIPアドレスまたはDNS名のいずれかを提供します。このタスクでは、ストレージレイにコントローラが1つあり、CSRファイルが2つある場合は1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、に進むこともできます [手順2：CSRファイルを送信します](#)。

手順

1. メニューから[設定][証明書]を選択します。
2. [Array Management]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名の先頭にワイルドカードを使用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。DNS名の先頭にワイルドカードを使用することはできません。ストレージ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. に進みます [手順2：CSRファイルを送信します](#)。

手順2：CSRファイルを送信します

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ています。

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、別のCSRファイルを再生成しないでください。* CSRを生成するたびに、システムは秘密鍵と公開鍵のペアを作成します。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から返された署名済み証明書については、を参照してください [\[手順3：コントローラの署名済み証明書をインポートする\]](#)。

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

署名済み証明書を認証局（CA）から受け取ったあと、コントローラのファイルをインポートします。

作業を開始する前に

- 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（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、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。ウィンドウを使用できます。certmgr ファイルを解凍するユーティリティ(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エンコーディングが推奨されます。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。
- 証明書ファイルをSystem Managerにアクセスするホストシステムに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表示されます。

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。

管理証明書をリセットします

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。

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。
- 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。

このタスクについて

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. を入力します reset をクリックし、*[リセット]*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

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。

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、ストレージアレイの証明書タイプ、発行元、および有効な証明書の日付範囲を確認できます。

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. 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。

タブをクリックする	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。
高い信頼性	<p>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。</p> <ul style="list-style-type: none"> • 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をインポートする

コントローラが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できます。このタブでは、コントローラ（クライアントとして動作）がそのサーバからの通信を受け入れることができます。

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。
- 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

別のサーバがコントローラ（LDAPサーバやTLSを使用するsyslogサーバなど）に接続できるようにするには、[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。

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。

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

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レスポンドのアドレス*]フィールドに、OCSPレスポンドサーバの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レイが接続しようとする時、接続は拒否され、イベントがログに記録されます。

信頼された証明書を削除する

以前に[信頼済み]タブからインポートした、ユーザーがインストールした証明書を削除できます。

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。



コントローラとLDAPサーバなどの別のサーバの認証に使用している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。

ストレージ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. を入力します delete フィールドで、*[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レイコントローラのためのセキュアな通信を確立するためには、適切な証明書セットを設定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

コントローラとキー管理サーバ間の認証は、2段階の手順です。

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、キー管理サーバで信頼されている

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および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、キー管理サーバが自身のKey Management Interoperability Protocol（KMIP）要求を信頼できるように、ストレージレイのコントローラを検証します。

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。

CSRファイルがローカルシステムに保存されます。

5. キー管理サーバで信頼されているCAから署名済みの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

次の手順として、ストレージレイとキー管理サーバ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ストレージ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。

作業を開始する前に

- 署名済みのクライアント証明書ファイルがある（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](#)）をクリックし、System Managerにアクセスするホストにファイルをコピーしておきます。クライアント証明書は、キー管理サーバが自身のKey Management Interoperability Protocol（KMIP）要求を信頼できるように、ストレージレイのコントローラを検証します。
- 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表示されます。

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。

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェア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权を有し、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权については、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、<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。