

PKI の設定

この章では、Cisco NX-OS での公開キーインフラストラクチャ(PKI)のサポートについて説明します。PKIを使用すると、ネットワーク上で通信を安全に行うためのデジタル証明書をデバイスが入手して使用できるようになり、セキュアシェル(SSH)の管理性と拡張性も向上します。

この章は、次の項で構成されています。

- PKI の概要, on page 1
- PKIの注意事項と制約事項 (8ページ)
- PKI のデフォルト設定, on page 9
- CA の設定とデジタル証明書, on page 9
- PKIの設定の確認, on page 26
- PKIの設定例, on page 26
- PKI に関する追加情報, on page 62
- Resource Public Key Infrastructure (RPKI) $(62 \sim \checkmark)$
- RPKI 構成 (63 ページ)
- RPKI Show コマンド (65 ページ)
- ・RPKI Clear コマンド (66 ページ)
- RPKI Debug および Event History コマンド (66 ページ)

PKIの概要

ここでは、PKIについて説明します。

CAとデジタル証明書

証明機関(CA)は証明書要求を管理して、ホスト、ネットワークデバイス、ユーザなどの参加エンティティに証明書を発行します。CA は参加エンティティに対して集中型のキー管理を行います。

デジタル署名は、公開キー暗号法に基づいて、デバイスや個々のユーザをデジタル的に認証します。RSA 暗号化システムなどの公開キー暗号法では、各デバイスやユーザはキーペアを持

PKI の設定

信者の秘密キーを使用してデータを暗号化したときに作成されます。受信側は、送信側の公開 キーを使用してメッセージを復号化することで、シグニチャを検証します。このプロセスは、 受信者が送信者の公開キーのコピーを持っていて、これが本当に送信者のものであり、送信者 を騙る他人のものではないことを高い確実性を持って知っていることを基盤としています。

デジタル証明書は、デジタル署名と送信者を結び付けるものです。デジタル証明書には、名 前、シリアル番号、企業、部署または IP アドレスなど、ユーザまたはデバイスを特定する情 報を含んでいます。また、エンティティの公開キーのコピーも含んでいます。証明書に署名す る CA は、受信者が明示的に信頼する第三者機関であり、アイデンティティの正当性を立証 し、デジタル証明書を作成します。

CAのシグニチャを検証するには、受信者は、CAの公開キーを認識している必要があります。 一般的にはこのプロセスはアウトオブバンドか、インストール時に行われる操作によって処理 されます。たとえば、通常の Web ブラウザでは、デフォルトで、複数の CA の公開キーが設 定されています。

信頼モデル、トラストポイント、アイデンティティCA

PKIの信頼モデルは、設定変更が可能な複数の信頼できる CA によって階層化されています。 信頼できる CA のリストを使用して各参加デバイスを設定して、セキュリティプロトコルの交換の際に入手したピアの証明書がローカルに信頼できる CA のいずれかで発行されていた場合 には、これを認証できるようにすることができます。Cisco NX-OS ソフトウェアでは、信頼で きる CA の自己署名ルート証明書(または下位 CA の証明書チェーン)をローカルに保存して います。信頼できる CA のルート証明書(または下位 CA の場合には全体のチェーン)を安全 に入手するプロセスを、CA 認証と呼びます。

信頼できる CA について設定された情報をトラストポイントと呼び、CA 自体もトラストポイント CA と呼びます。この情報は、CA 証明書(下位 CA の場合は証明書チェーン)と証明書 取消確認情報で構成されています。

Cisco NX-OS デバイスは、トラストポイントに登録して、アイデンティティ証明書を入手し、 キーペアと関連付けることができます。このトラストポイントをアイデンティティ CA と呼び ます。

CA証明書の階層

セキュアサービスの場合、通常は複数の信頼できるCAがあります。CAは通常、すべてのホストにバンドルとしてインストールされます。NX-OSPKIインフラストラクチャは、証明書チェーンのインポートをサポートします。ただし、現在のCLIでは、一度に1つのチェーンをインストールできます。インストールするCAチェーンが複数ある場合、この手順は面倒です。これには、複数の中間CAとルートCAを含むCAバンドルをダウンロードする機能が必要です。

CAバンドルのインポート

crypto CA trustpointコマンドは、CA証明書、CRL、アイデンティティ証明書、およびキーペア を名前付きラベルにバインドします。これらの各エンティティに対応するすべてのファイル は、NX-OS certstoreディレクトリ(/isan/etc/certstore)に保存され、トラストポイントラベル でタグ付けされます。

CA証明書にアクセスするには、SSLアプリケーションは標準のNX-OS証明書ストアをポイント し、SSL初期化中にCAパスとして指定するだけです。CAがインストールされているトラスト ポイントラベルを認識する必要はありません。

クライアントがアイデンティティ証明書にバインドする必要がある場合は、トラストポイント ラベルをバインディングポイントとして使用する必要があります。

importpkcsコマンドは、トラストポイントラベルの下にCA証明書をインストールするように拡張されています。CAバンドルをインストールするようにさらに拡張できます。importコマンド 構造が変更され、pkcs7形式のCAバンドルファイルを提供するために使用されるpkcs7オプショ ンが追加されました。

Cisco NX-OS リリース 10.1(1) 以降、CA バンドルを解凍し、独自のラベルの下に各 CA チェー ンをインストールするために、pkcs7 ファイル形式がサポートされています。ラベルは、メイ ントラストポイントラベルにインデックスを追加することによって形成されます。

ー度インストールすると、バンドルへのすべてのCAチェーンの論理バインディングはありま せん。

PKCS7 形式での CA 証明書バンドルのインポート

複数の独立した証明書チェーンで構成される CA 証明書バンドルのインポートをサポートする ために、 'pkcs7' のオプションが crypto import コマンドに導入されました。

手順

	コマンドまたはアクション	目的
ステップ1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します
ステップ 2	crypto ca import <i><baselabel></baselabel></i> pksc7 <i><uri0></uri0></i> force	コマンドには2つの入力引数がありま す。Ca バンドルファイルであるソース ファイルは、 <uri0>、入力ファイルは pkcs7形式である必要があります。これ は cabundle ファイルであることを示し ます。</uri0>
		複数の証明書チェーンが cabundle から 抽出されます。このコマンドは、CA証 明書チェーンが接続された複数のトラス

	コマンドまたはアクション	目的
		トポイントを生成します。import コマン ドは、グローバルCAバンドル構成と、 生成された各トラストポイントごとの CAバンドル下位構成の、2つの構成を 生成します。
		forceオプションを指定すると、CAバンドルおよび関連するトラストポイン構成が削除され、同じバンドル名を持つ新しいCAバンドルがインポートされ、そのCAバンドルに関連する新しいトラストポイント構成が生成されます。
ステップ3	exit	設定モードを終了します。
	例: switch(config)# exit switch#	
ステップ4	(任意) show crypto ca certificates	CA 証明書を表示します。
	例 : switch# show crypto ca certificates	
ステップ5	(任意) copy running-config startup-config例:	実行コンフィギュレーションを、スター トアップ コンフィギュレーションにコ ピーします。
	switcn# copy running-config startup-config	

RSA のキーペアとアイデンティティ証明書

アイデンティティ証明書を入手するには、1つまたは複数のRSA キーペアを作成し、各RSA キーペアとCisco NX-OS デバイスが登録しようとしているトラストポイントCA を関連付けま す。Cisco NX-OS デバイスは、CA ごとにアイデンティティを1つだけ必要とします。これは CA ごとに1つのキーペアと1つのアイデンティティ証明書で構成されています。

Cisco NX-OS ソフトウェアでは、設定変更が可能なキーのサイズ(またはモジュラス)でRSA キーペアを作成できます。デフォルトのキーのサイズは 512 です。また、RSA キーペアのラ ベルも設定できます。デフォルトのキーラベルは、デバイスの完全修飾ドメイン名(FQDN) です。

トラストポイント、RSA キーペア、およびアイデンティティ証明書の関係を要約したものを 次に示します。

トラストポイントとは、Cisco NX-OS デバイスが、あらゆるアプリケーション(SSH など)のピア証明書用に信頼する特定のCAです。

- Cisco NX-OS デバイスでは、デバイス上に多くのトラストポイントを置くことができ、デバイス上のすべてのアプリケーションは、任意のトラストポイント CA によって発行されたピア証明書を信頼できます。
- トラストポイントは特定のアプリケーション用に限定されません。
- Cisco NX-OS デバイスは、トラストポイントに対応する CA に登録して、アイデンティティ 証明書を入手します。デバイスは複数のトラストポイントに登録できます。これは、各ト ラストポイントから異なるアイデンティティ証明書を入手できることを意味します。アイ デンティティ証明書は、発行する CA によって証明書に指定されている目的に応じてアプ リケーションで使用します。証明書の目的は、証明書の拡張機能として証明書に保存され ます。
- トラストポイントに登録するときには、証明を受ける RSA キーペアを指定する必要があります。このキーペアは、登録要求を作成する前に作成されていて、トラストポイントに関連付けられている必要があります。トラストポイント、キーペア、およびアイデンティティ証明書との間のアソシエーション(関連付け)は、証明書、キーペア、またはトラストポイントが削除されて明示的になくなるまで有効です。
- •アイデンティティ証明書のサブジェクト名は、Cisco NX-OS デバイスの完全修飾ドメイン 名です。
- ・デバイス上には1つまたは複数のRSAキーペアを作成でき、それぞれを1つまたは複数のトラストポイントに関連付けることができます。しかし、1つのトラストポイントに関連付けられるキーペアは1だけです。これは1つのCAからは1つのアイデンティティ証明書しか入手できないことを意味します。
- Cisco NX-OS デバイスが複数のアイデンティティ証明書を(それぞれ別の CA から)入手 する場合は、アプリケーションがピアとのセキュリティプロトコルの交換で使用する証明 書は、アプリケーション固有のものになります。
- 1つのアプリケーションに1つまたは複数のトラストポイントを指定する必要はありません。証明書の目的がアプリケーションの要件を満たしていれば、どのアプリケーションもあらゆるトラストポイントで発行されたあらゆる証明書を使用できます。
- ・あるトラストポイントから複数のアイデンティティ証明書を入手したり、あるトラストポイントに複数のキーペアを関連付ける必要はありません。ある CA はあるアイデンティティ(または名前)を1回だけ証明し、同じ名前で複数の証明書を発行することはありません。ある CA から複数のアイデンティティ証明書を入手する必要があり、またその CA が同じ名前で複数の証明書の発行を許可している場合は、同じ CA 用の別のトラストポイントを定義して、別のキーペアを関連付け、証明を受ける必要があります。

複数の信頼できる CA のサポート

Cisco NX-OS デバイスは、複数のトラストポイントを設定して、それぞれを別の CA に関連付けることにより、複数の CA を信頼できるようになります。信頼できる CA が複数あると、ピアに証明書を発行した特定の CA にデバイスを登録する必要がなくなります。代わりに、ピアが信頼する複数の信頼できる CA をデバイスに設定できます。すると、Cisco NX-OS デバイス

は設定されている信頼できる CA を使用して、ピアから受信した証明書で、ピア デバイスの ID で定義されている CA から発行されたものではないものを検証できるようになります。

PKIの登録のサポート

登録とは、SSHなどのアプリケーションに使用するデバイス用のアイデンティティ証明書を入 手するプロセスです。これは、証明書を要求するデバイスと、認証局の間で生じます。

Cisco NX-OS デバイスでは、PKI 登録プロセスを実行する際に、次の手順を取ります。

- ・デバイスでRSAの秘密キーと公開キーのペアを作成します。
- ・標準の形式で証明書要求を作成し、CAに送ります。

- Note 要求が CA で受信されたとき、CA サーバでは CA アドミニストレータが登録要求を手動で承認しなくてはならない場合があります。
 - •発行された証明書を CA から受け取ります。これは CA の秘密キーで署名されています。
 - ・デバイスの不揮発性のストレージ領域(ブートフラッシュ)に証明書を書き込みます。

カットアンドペーストによる手動での登録

Cisco NX-OS ソフトウェアでは、手動でのカットアンドペーストによる証明書の取得と登録を サポートしています。カットアンドペーストによる登録とは、証明書要求をカットアンドペー ストして、デバイスと CA 間で認証を行うことを意味します。

手動による登録プロセスでカットアンドペーストを使用するには、次の手順を実行する必要が あります。

- ・証明書登録要求を作成します。これは Cisco NX-OS デバイスで base64 でエンコードされ たテキスト形式として表示されます。
- エンコードされた証明書要求のテキストをEメールまたはWebフォームにカットアンドペーストし、CAに送ります。
- 発行された証明書(base64でエンコードされたテキスト形式)をCAからEメールまたは Webブラウザによるダウンロードで受け取ります。
- ・証明書のインポート機能を使用して、発行された証明書をデバイスにカットアンドペーストします。

複数の RSA キー ペアとアイデンティティ CA のサポート

複数のアイデンティティ CAを使用すると、デバイスが複数のトラストポイントに登録できる ようになり、その結果、別々の CA から複数のアイデンティティ証明書が発行されます。この 機能によって、Cisco NX-OS デバイスは複数のピアを持つ SSH およびアプリケーションに、これらのピアに対応する CA から発行された証明書を使用して参加できるようになります。

また複数のRSAキーペアの機能を使用すると、登録している各CAごとの別々のキーペアを デバイスで持てるようになります。これは、他のCAで指定されているキーの長さなどの要件 と競合することなく、各CAのポリシー要件に適合させることができます。デバイスでは複数 のRSAキーペアを作成して、各キーペアを別々のトラストポイントに関連付けることができ ます。したがって、トラストポイントに登録するときには、関連付けられたキーペアを証明書 要求の作成に使用します。

ピア証明書の検証

PKIでは、CiscoNX-OSデバイスでのピア証明書の検証機能をサポートしています。CiscoNX-OS では、SSHなどのアプリケーションのためのセキュリティ交換の際にピアから受け取った証明書を検証します。アプリケーションはピア証明書の正当性を検証します。CiscoNX-OS ソフトウェアでは、ピア証明書の検証の際に次の手順を実行します。

- ・ピア証明書がローカルの信頼できる CA のいずれかから発行されていることを確認します。
- ・ピア証明書が現在時刻において有効であること(期限切れでない)ことを確認します。
- ・ピア証明書が、発行した CA によって取り消されていないことを確認します。

取消確認については、Cisco NX-OS ソフトウェアでは証明書失効リスト(CRL)をサポートしています。トラストポイントCAではこの方法を使用して、ピア証明書が取り消されていないことを確認できます。

証明書の取消確認

Cisco NX-OS ソフトウェアでは、CA 証明書の取消のステータスを確認できます。アプリケー ションでは、指定した順序に従って取消確認メカニズムを使用できます。CRL、NDcPP:OCSP for Syslog、なし、またはこれらの方式の組み合わせを指定できます。

CRLのサポート

CAでは証明書失効リスト(CRL)を管理して、有効期限前に取り消された証明書についての 情報を提供します。CAではCRLをリポジトリで公開して、発行したすべての証明書の中にダ ウンロード用の公開 URL 情報を記載しています。ピア証明書を検証するクライアントは、発 行した CA から最新の CRL を入手して、これを使用して証明書が取り消されていないかどう かを確認できます。クライアントは、自身の信頼できるCAのすべてまたは一部のCRLをロー カルにキャッシュして、その CRL が期限切れになるまで必要に応じて使用することができま す。

Cisco NX-OS ソフトウェアでは、先にダウンロードしたトラストポイントについての CRL を 手動で設定して、これをデバイスのブートフラッシュ(cert-store)にキャッシュすることがで きます。ピア証明書の検証の際、Cisco NX-OS ソフトウェアは、CRL がすでにローカルにキャッ シュされていて、取消確認でこの CRL を使用するよう設定されている場合にだけ、発行した CA からの CRL をチェックします。それ以外の場合、Cisco NX-OS ソフトウェアでは CRL チェックを実行せず、他の取消確認方式が設定されている場合を除き、証明書は取り消されて いないと見なします。

NDcPP : syslog \mathcal{O} OCSP

Online Certificate Status Protocol (OCSP)は、ピアがこの失効情報を取得し、それを検証して証明書失効ステータスを確認する必要がある場合に、証明書失効をチェックする方法です。この方式では、クラウドを介してOCSPレスポンダに到達するピアの機能、または証明書失効情報を取得する証明書送信者のパフォーマンスによって、証明書失効ステータスが制限されます。

リモート syslog サーバが OCSP レスポンダ URL を持つ証明書を共有すると、クライアントは サーバ証明書を外部 OCSP レスポンダ (CA) サーバに送信します。CA サーバはこの証明書を 検証し、有効な証明書か失効した証明書かを確認します。この場合、クライアントは失効した 証明書リストをローカルに保持する必要はありません。

証明書と対応するキー ペアのインポートとエクスポート

CA 認証と登録のプロセスの一環として、下位 CA 証明書(または証明書チェーン)とアイデ ンティティ証明書を標準の PEM (base64) 形式でインポートできます。

トラストポイントでのアイデンティティ情報全体を、パスワードで保護される PKCS#12 標準 形式でファイルにエクスポートできます。このファイルは、後で同じデバイス(システム ク ラッシュの後など)や交換したデバイスににインポートすることができます。PKCS#12 ファイ ル内の情報は、RSA キーペア、アイデンティティ証明書、および CA 証明書(またはチェー ン)で構成されています。

PKIの注意事項と制約事項

PKIに関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS デバイスに設定できるキーペアの最大数は 16 です。
- ・Cisco NX-OS デバイスで宣言できるトラスト ポイントの最大数は 16 です。
- ・Cisco NX-OS デバイスに設定できるアイデンティティ証明書の最大数は 16 です。
- CA 証明書チェーン内の証明書の最大数は 10 です。
- ・ある CA に対して認証できるトラストポイントの最大数は 10 です。
- ・設定のロールバックでは PKI の設定はサポートしていません。
- Cisco NX-OS リリース 9.3 (5) 以降では、Cisco NX-OS ソフトウェアは NDcPP: OCSP for Syslog をサポートしています。

(注) Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

PKI のデフォルト設定

次の表に、PKI パラメータのデフォルト設定を示します。

Table 1: PKI パラメータのデフォルト値

パラメータ	デフォルト
トラスト ポイント	なし
RSA キーペア	なし
RSA キーペアのラベル	デバイスの FQDN
RSA キーペアのモジュール	512
RSA キーペアのエクスポートの可 否	イネーブル
取消確認方式	CRL

CAの設定とデジタル証明書

ここでは、Cisco NX-OS デバイス上で CA とデジタル証明書が相互に連携して動作するように するために、実行が必要な作業について説明します。

ホスト名とIPドメイン名の設定

デバイスのホスト名または IP ドメイン名をまだ設定していない場合は、設定する必要があり ます。これは、Cisco NX-OS ソフトウェアでは、アイデンティティ証明書のサブジェクトとし て完全修飾ドメイン名(FQDN)を使用するためです。また、Cisco NX-OS ソフトウェアでは、 キーの作成の際にラベルが指定されていないと、デバイスの FQDN をデフォルトのキー ラベ ルとして使用します。たとえば、DeviceA.example.com という名前の証明書は、DeviceA という デバイスのホスト名と example.com というデバイスの IP ドメイン名に基づいています。

Caution

ution 証明書を作成した後にホスト名またはIP ドメイン名を変更すると、証明書が無効になります。

9

Procedure

	Command or Action	Purpose
ステップ1	configure terminal	グローバル コンフィギュレーション
	Example:	モードを開始します。
	<pre>switch# configure terminal switch(config)#</pre>	
ステップ2	hostname hostname	デバイスのホスト名を設定します。
	Example:	
	switch(config)# hostname DeviceA	
ステップ3	ip domain-name <i>name</i> [use-vrf <i>vrf-name</i>]	デバイスのIPドメイン名を設定します。
	Example:	VRF 名が指定されていないと、このコ
	DeviceA(config)# ip domain-name	マンドではデフォルトの VRF を使用し
	example.com	ます。
ステップ4	exit	コンフィギュレーション モードを終了
	Example:	します。
	switch(config)# exit switch#	
ステップ5	(Optional) show hosts	 IP ドメイン名を表示します。
	Example:	
	switch# show hosts	
ステップ6	(Optional) copy running-config	実行コンフィギュレーションを、スター
	startup-config	トアップ コンフィギュレーションにコ
	Example:	ピーします。
	switch# copy running-config startup-config	
	1	1

RSA キーペアの生成

RSAキーペアは、アプリケーション向けのセキュリティプロトコルの交換時に、セキュリティ ペイロードの署名、暗号化、および復号化のために作成します。デバイスのための証明書を取 得する前に、RSA キーペアを作成する必要があります。

Cisco NX-OS リリース 9.3(3) 以降では、Cisco NX-OS デバイスをトラスト ポイント CA に関連 付ける前に、明示的に RSA キーペアを生成する必要があります。Cisco NX-OS リリース 9.3(3) よりも前では、使用できない場合、RSAキーペアは自動生成されます。

Procedure

I

	Command or Action	Purpose
ステップ1	<pre>configure terminal Example: switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します
ステップ 2	crypto key generate rsa [label <i>label-string</i>] [exportable] [modulus <i>size</i>] Example:	RSA キーペアを生成します。デバイス に設定できるキーペアの最大数は16で す。
	switch(config)# crypto key generate rsa exportable	ラベル文字列には、大文字と小文字を区別して、最大 64 文字の英数字で値を指定します。デフォルトのラベル文字列は、ピリオド文字(.) で区切ったホスト名と FQDN です。
		有効なモジュラスの値は 512、768、 1024、1536、および 2048 です。デフォ ルトのモジュラスのサイズは 512 です。
		Note 適切なキーのモジュラスを決定する際 には、Cisco NX-OS デバイスと CA(登 録を計画している対象)のセキュリティ ポリシーを考慮する必要があります。
		デフォルトでは、キーペアはエクスポー トできません。エクスポート可能なキー ペアだけ、PKCS#12 形式でエクスポー トできます。
		Caution キーペアのエクスポートの可否は変更 できません。
ステップ3	exit	コンフィギュレーション モードを終了
	Example: switch(config)# exit switch#	します。
ステップ4	(Optional) show crypto key mypubkey rsa Example: switch# show crypto key mypubkey rsa	作成したキーを表示します。

	Command or Action	Purpose
ステップ5	(Optional) copy running-config startup-config	実行コンフィギュレーションを、スター トアップ コンフィギュレーションにコ
	Example:	ピーします。
	switch# copy running-config startup-config	

トラストポイント CA のアソシエーションの作成

Cisco NX-OS デバイスとトラスト ポイント CA を関連付ける必要があります。

Before you begin

RSA キーペアを作成します。

Procedure

	Command or Action	Purpose
ステップ1	configure terminal	グローバル構成モードを開始します。
ステップ 2	<pre>Example: switch# configure terminal switch(config)# crypto ca trustpoint name Example: switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#</pre>	デバイスが信頼するトラストポイント CAを宣言し、トラストポイント コン フィギュレーション モードを開始しま す。
		Note 設定できるトラストポイントの最大数 は 50 です。
ステップ3	<pre>cabundle baselabel Example: switch(config-trustpoint)# cabundle test</pre>	特定のCAバンドル下でトラストポイン トをグループ化します。このコマンドの No形式を使用すると、CAバンドルか らトラストポイントが切り離されます。 このコマンドは、トラストポイントを既 存のCAバンドルに関連付けます。新し いCAバンドルは設定しません。
ステップ4	<pre>enrollment terminal Example: switch(config-trustpoint)# enrollment terminal</pre>	手動でのカットアンドペーストによる証 明書の登録をイネーブルにします。デ フォルトではイネーブルになっていま す。 Note

	Command or Action	Purpose
		Cisco NX-OS ソフトウェアでは、手動 でのカットアンドペースト方式による 証明書の登録だけをサポートしていま す。
ステップ5	<pre>rsakeypair label Example: switch(config-trustpoint)# rsakeypair</pre>	RSA キー ペアのラベルを指定して、こ のトラストポイントを登録用に関連付け ます。
	SwitchA	Note CA ごとに 1 つの RSA キー ペアだけを 指定できます。
ステップ6	<pre>exit Example: switch(config-trustpoint)# exit switch(config)#</pre>	トラストポイントコンフィギュレーショ ン モードを終了します。
ステップ 1	(Optional) show crypto ca trustpoints Example: switch(config)# show crypto ca trustpoints	トラストポイントの情報を表示します。
ステップ8	<pre>(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スター トアップ コンフィギュレーションにコ ピーします。

Related Topics

RSA キーペアの生成 (10ページ)

CAの認証

CA が Cisco NX-OS デバイスに対して認証されると、CA を信頼するプロセスの設定が完了します。まず、PEM 形式の CA の自己署名証明書を入手し、Cisco NX-OS デバイスを CA に対して認証する必要があります。この証明書には、CA の公開キーが含まれています。この CA の証明書は自己署名(CA が自身の証明書に署名したもの)であるため、CA の公開キーは、CA アドミニストレータに連絡し、CA 証明書のフィンガープリントを比較して手動で認証する必要があります。



Note 認証する CA が他の CA の下位 CA である場合、認証する CA は自己署名 CA ではありません。 その上位の CA がさらに別の CA の下位である場合もあります。最終的には自己署名 CA に到 達します。このタイプの CA 証明書を、認証する CA の CA 証明書チェーンと呼びます。この 場合は、CA 認証の際に、証明書チェーン内のすべての CA の CA 証明書の完全なリストを入 力する必要があります。CA 証明書チェーン内の証明書の最大数は 10 です。

Before you begin

CA とのアソシエーションを作成します。 CA 証明書または CA 証明書チェーンを入手します。

Procedure

	Command or Action	Purpose
ステップ1	configure terminal	グローバル コンフィギュレーション
	Example:	モードを開始します
	switch# configure terminal switch(config)#	
ステップ2	crypto ca authenticate name pemfile uri0	CAの証明書をカットアンドペーストす
ステップ 2	crypto ca authenticate name pemfile uri0 Example: switch (config) # crypto ca authenticate admin-ca input (cut & paste) CA certificate (chain) in PEM format; end the input with a line containing only END OF INPUT : BEGIN CERTIFICATE MICH_COCY_MERGLEUISA/CREENING/ENDERGENING KEMBUSSASISIGERARAWIDERZEJANJOSSICAERMEATAL MEMERINQUENIXUMAABEJARMACTCUHERDIGAERAAAII (MKQ12/2842/HBMASICHERZEJARMACTCUHERDIGAERAAAII (MKQ12/2842/HBMASICHERZEJARMACTCUHERDIGAERAAAII (MKQ12/2842/HBMASICHERZEJARMACTCUHERDIGAERAAAII (MKQ12/2842/HBMASICHERZEJARMACTCUHERDIGAERAAAII (MKQ12/2842/HBMASICHERZEJARMACTCUHERDIGAERAAAII (MKQ12/2842/HBMASICHERZEJARMACTCUHERDIGAERAAAII (MKQ12/2842/HBMASICHERZEJARMACTCUHERDIGAERAAII (MKQ12/2842/HBMASICHERZEJARMACTCUHERDIGAERAAII (MKQ12/2842/HBMASICHERZEJARMACTCUHERDIGAERAAII (MKQ12/2842/HBMASICHERZEJARMACTCUHERDIGAERAAII (MKQ12/2842/HBMASICHERZEJARMACTCUHERDIGAERAAII (MKQ12/2842/HBMASICHERZEJARMACTCUHERDIGAERAAII (MKQ12/2842/HBMASICHERZEJARAAII (MKQ12/2842/HBMASICHERZEJAI	CA の証明書をカットアンドペーストす るようプロンプトが表示されます。CA を宣言したときに使用した名前と同じ名 前を使用します。 また、CAチェーンを検証し、指定され たトラストポイントに直接接続します。 あるCAに対して認証できるトラストポ イントの最大数は10です。 Note 下位CAの認証の場合、Cisco NX-OS ソ フトウェアでは、自己署名 CA に到達 する CA 証明書の完全なチェーンが必 要になります。これは証明書の検証や PKCS#12 形式でのエクスポートに CA チェーンが必要になるためです。
	BUACHAGUGEES91wHGQCQNLapghAFCDEyyt/WC2sF92 NBG7E00N66zex0EOEfG1Vs6mXp1//w== END CERTIFICATE END OF INPUT Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12 Do you accept this certificate? [yes/no]: yes	

	Command or Action	Purpose
ステップ3	exit	コンフィギュレーション モードを終了
	Example:	します。
	switch(config)# exit switch#	
ステップ4	(Optional) show crypto ca trustpoints	トラストポイントCAの情報を表示しま
	Example:	す。
	switch# show crypto ca trustpoints	
ステップ5	(Optional) copy running-config startup-config	実行コンフィギュレーションを、スター トアップ コンフィギュレーションにコ
	Example:	ピーします。
	switch# copy running-config startup-config	

Related Topics

トラストポイント CA のアソシエーションの作成 (12 ページ)

証明書取消確認方法の設定

クライアント(SSHユーザなど)とのセキュリティ交換の際に、Cisco NX-OS デバイスは、クライアントから送られたピア証明書の検証を実行します。検証プロセスには、証明書の取消状況の確認が含まれます。

CAからダウンロードしたCRLを確認するよう、デバイスに設定できます。CRLのダウンロードとローカルでの確認では、ネットワーク上にトラフィックは発生しません。しかし、証明書がダウンロードとダウンロードの中間で取り消され、デバイス側ではその取り消しに気付かない場合も考えられます。

Before you begin

CA を認証します。

CRL チェックを使用する場合は、CRL が設定済みであることを確認します。

Procedure

	Command or Action	Purpose
ステップ1	configure terminal	グローバル構成モードを開始します。
	Example:	
	<pre>switch# configure terminal switch(config)#</pre>	

	Command or Action	Purpose
ステップ2	<pre>crypto ca trustpoint name Example: switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#</pre>	トラストポイントCAを指定し、トラス トポイント コンフィギュレーション モードを開始します。
ステップ3	<pre>revocation-check {crl [none] none} Example: switch(config-trustpoint)# revocation-check none</pre>	 証明書取消確認方法を設定します。デ フォルトの方式は crl. です。 Cisco NX-OS ソフトウェアでは、指定し た順序に従って証明書取消方式を使用し ます。
ステップ4	<pre>exit Example: switch(config-trustpoint)# exit switch(config)#</pre>	トラストポイントコンフィギュレーショ ン モードを終了します。
ステップ5	(Optional) show crypto ca trustpoints Example: switch(config)# show crypto ca trustpoints	トラストポイントCAの情報を表示しま す。
ステップ6	<pre>(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スター トアップ コンフィギュレーションにコ ピーします。

Related Topics

CA の認証 (13 ページ) CRL の設定 (22 ページ)

証明書要求の作成

使用する各デバイスの RSA キーペア用に、対応するトラストポイント CA からアイデンティ ティ証明書を入手するために、要求を作成する必要があります。その後、表示された要求を CA 宛の E メールまたは Web サイトのフォームにカットアンドペーストします。

Before you begin

CA とのアソシエーションを作成します。

CA 証明書または CA 証明書チェーンを入手します。

Procedure

	Command or Action	Purpose
ステップ1	configure terminal	グローバル構成モードを開始します。
	Example:	
	switch# configure terminal	
	switch(config)#	
ステップ2	crypto ca enroll name	認証したCAに対する証明書要求を作成
	Example:	します。
	<pre>switch(config)# crypto ca enroll admin-ca Create the certificate request Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it. Password:nbv123 The subject name in the certificate will be: DeviceA.cisco.com Include the switch serial number in the option.</pre>	Note チャレンジパスワードを記憶しておい てください。このパスワードは設定と 一緒に保存されません。証明書を取り 消す必要がある場合には、このパスワー ドを入力する必要があります。
	<pre>the subject name? [yes/no]: no Include an IP address in the subject name [yes/no]: yes ip address:172.22.31.162 The certificate request will be displayed BEGIN CERTIFICATE REQUEST MIRGCROROACHERGAILEANRANNAMINESJENIJS5120xg28UQX KZINCHQHERGGAMEANGAMEANIAINCTSJENIJS5120xg28UQX KZINCHQHERGGAMEANGAMEANIAINCTSJENIJS5120xg28UQX KZINCHQHERGGAMEANGAMEANIAINCTSJENIJS5120xg28UQX VANDAANAANAANIZALAJENNAMINESJENIJS5122HWALAUX VANDAANAANAANIZALAJENNAMINESJENIJS5122HWALAUX KZINCHQHERGGAMEANIAINCHSSJENIJS5122HWALAUX KZINCHQHERGGAMEANIAINCHSSJENIJS5122HWALAUX KZINCHQHERGGAMEANIAINCHSSJENIJS5122HWALAUX KZINCHQHERGGAMEANIAINCHSSJENIJS5122HWALAUX KZINCHQHERGGAMEANIAINCHSSJENIJS5122HWALAUX KZINCHQHERGGAMEANIAINCHSSJENIJS5122HWALAUX KZINCHQHERGGAMEANIAUNINENCHJIGNIZAUSARAMUMIJ 823NDNAKWAMWANUTENCHJIGNIZAUSARAMUMUM END CERTIFICATE REQUEST</pre>	
ステップ3	exit	トラストポイントコンフィギュレーショ
	Example:	ンモードを終了します。
	<pre>switch(config-trustpoint)# exit switch(config)#</pre>	
ステップ4	(Optional) show crypto ca certificates	CA 証明書を表示します。
	Example:	
	switch(config)# show crypto ca certificates	

	Command or Action	Purpose
ステップ5	(Optional) copy running-config startup-config	実行コンフィギュレーションを、スター トアップ コンフィギュレーションにコ
	Example:	ピーします。
	switch(config)# copy running-config startup-config	

Related Topics

トラストポイント CA のアソシエーションの作成 (12 ページ)

アイデンティティ証明書のインストール

アイデンティティ証明書は、CAからEメールまたはWebブラウザ経由でbase64でエンコードされたテキスト形式で受信できます。CAから入手したアイデンティティ証明書を、エンコードされたテキストをカットアンドペーストしてインストールする必要があります。

Before you begin

CAとのアソシエーションを作成します。

CA 証明書または CA 証明書チェーンを入手します。

Procedure

	Command or Action	Purpose
ステップ1	configure terminal	グローバル構成モードを開始します。
	Example:	
	<pre>switch# configure terminal switch(config)#</pre>	
ステップ2	crypto ca import name certificate	admin-caという名前のCAに対するアイ
	Example:	デンティティ証明書をカットアンドペー
	switch (config) # crypto ca import admin-ca certificate input (cut & paste) certificate in PEM format: BEGIN CERTIFICATE MIEAUCAGAMEGICCOQAANACAREACIONOPQEAUEAEAEA (GSESDSQEARAWIDERZEJANJSSSSCACAENPAYIAKORWARM VQEMILXUXAR282542BJMFACUUDWDD9ZIRVAAUEOMQ22 288278BJMFASID5DHN53522532CAEBJMFAYIAKORWARM VQEMILXUXAR282542BJMFACUUDWDD9ZIRVAAUEOMQ22 288278BJMFASID5DHN5352553264300000000000000000000000000000000000	ストするよう、プロンプトが表示されま す。 デバイスに設定できるアイデンティティ 証明書の最大数は 16 です。

	Command or Action	Purpose
	PANAQYEANDAY JOETHERALLEAMANOCRAMITZIESMACALLEAMQA mTATENE JAFANCHI (ZEESEIMARIA GAMINIC SAMITALEAMACA (MARIA LyAZIMA QAYEMA BAGA (MARIA GAMINICAL (MARIA) LyAXAZIMA QAYEMA (MARIA) LYAXAZIMA (MARIA) AGEE JEMAGGA (JEEZCHI JAHAN (MARIA) AGEE JEMAGGA (JEEZCHI JAHAN) AGEE JEMAGGA (JEEZCHI JAHAN) AGEE JEMAGGA (JEEZCHI JAHAN) ANARTANIA GAMINICANA (JAHAN) ANARTANIA GAMINICANA (JAHAN) ANARTANIA GAMINICANA (JAHAN) ANARTANIA GAMINICANA (JAHAN) ANARTANIA GAMINICANA (JAHAN) ANARTANIA GAMINICANA (JAHAN) ANARTANIA (JAHAN	
ステップ3	exit Example: switch(config)# exit switch#	設定モードを終了します。
ステップ4	(Optional) show crypto ca certificates Example: switch# show crypto ca certificates	CA 証明書を表示します。
ステップ5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スター トアップ コンフィギュレーションにコ ピーします。

Related Topics

トラストポイント CA のアソシエーションの作成 (12 ページ)

トラストポイントの設定がリブート後も維持されていることの確認

トラストポイントの設定が、Cisco NX-OS デバイスのリブート後も維持されていることを確認 できます。

トラストポイントの設定は、通常の Cisco NX-OS デバイスの設定であり、スタートアップコ ンフィギュレーションに確実にコピーした場合にだけ、システムのリブート後も維持されま す。トラストポイント設定をスタートアップコンフィギュレーションにコピーしておけば、 トラストポイントに関連する証明書、キーペア、および CRL が自動的に保持されます。逆 に、トラストポイントがスタートアップコンフィギュレーションにコピーされていないと、 証明書、キーペア、および関連 CRL は保持されません。リブート後に、対応するトラストポ イント設定が必要になるからです。設定した証明書、キーペア、および CRL を確実に保持す るために、必ず、実行コンフィギュレーションをスタートアップコンフィギュレーションにコ ピーしてください。また、証明書またはキーペアを削除した後は実行コンフィギュレーション を保存して、削除が永続的に反映されるようにしてください。

トラストポイントに関連付けられた証明書と CRL は、そのトラストポイントがすでにスター トアップコンフィギュレーションに保存されていれば、インポートした時点で(つまりスター トアップ コンフィギュレーションにコピーしなくても)維持されるようになります。 パスワードで保護したアイデンティティ証明書のバックアップを作成して、これを外部のサー バに保存することを推奨します。



Note コンフィギュレーションを外部サーバにコピーすると、証明書およびキーペアも保存されま す。

Related Topics

PKCS 12 形式でのアイデンティティ情報のエクスポート (20ページ)

PKCS 12 形式でのアイデンティティ情報のエクスポート

アイデンティティ証明書を、トラストポイントのRSAキーペアやCA証明書(または下位CAの場合はチェーン全体)と一緒にPKCS#12ファイルにバックアップ目的でエクスポートすることができます。デバイスのシステムクラッシュからの復元の際や、スーパーバイザモジュールの交換の際には、証明書やRSAキーペアをインポートすることができます。

Note エクスポートの URL を指定するときに使用できるのは、bootflash:*filename* という形式だけです。

Before you begin

CA を認証します。

アイデンティティ証明書をインストールします。

Procedure

	Command or Action	Purpose
ステップ1	configure terminal	グローバル コンフィギュレーション
	Example:	モードを開始します
	<pre>switch# configure terminal switch(config)#</pre>	
ステップ2	crypto ca export name pkcs12	アイデンティティ証明書と、トラストポ
	bootflash:filename password	イントCAの対応するキーペアとCA証
	Example:	明書をエクスポートします。パスワード
	<pre>switch(config)# crypto ca export admin-ca pkcs12 bootflash:adminid.p12 nbv123</pre>	には、大文字と小文字を区別して、最大 128 文字の英数字で値を指定します。
ステップ3	exit	コンフィギュレーション モードを終了
	Example:	します。

Command or Action		Purpose
switch(config)# exi switch#	t	
ステップ4 copy booflash:filename /]filename	e scheme : //server/ [url	PKCS#12 形式のファイルをリモート サーバにコピーします。
Example: switch# copy bootfl. tftp:adminid.pl2	ash:adminid.p12	<i>scheme</i> 引数に対しては、 tftp: 、 ftp: 、 scp: 、または sftp: を入力できます。 <i>server</i> 引数は、リモートサーバのアドレ スまたは名前であり、 <i>url</i> 引数はリモー トサーバにあるソースファイルへのパ スです。 <i>server、url</i> 、および <i>filename</i> の各引数 は、大文字小文字を区別して入力しま す。

Related Topics

```
RSA キー ペアの生成 (10 ページ)
CA の認証 (13 ページ)
アイデンティティ証明書のインストール (18 ページ)
```

PKCS 12 フォーマットで ID 情報のインポート

デバイスのシステム クラッシュからの復元の際や、スーパーバイザ モジュールの交換の際には、証明書や RSA キー ペアをインポートすることができます。



Note インポートの URL を指定するときに使用できるのは、bbootflash:*filename* fという形式だけです。

Before you begin

CA 認証によってトラストポイントに関連付けられている RSA キー ペアがないこと、および トラストポイントに関連付けられている CA がないことを確認して、トラストポイントが空で あるようにします。

Procedure

	Command or Action	Purpose
ステップ1	<pre>copy scheme:// server/[url /]filename bootflash:filename</pre>	PKCS#12 形式のファイルをリモート サーバからコピーします。
	Example:	

	Command or Action	Purpose
	switch# copy tftp:adminid.p12 bootflash:adminid.p12	<i>scheme</i> 引数に対しては、 tftp: 、 ftp: 、 scp: 、または sftp: を入力できます。 <i>server</i> 引数は、リモートサーバのアドレ スまたは名前であり、 <i>url</i> 引数はリモー トサーバにあるソースファイルへのパ スです。 <i>server、url、</i> および <i>filename</i> の各引数 は、大文字小文字を区別して入力しま す。
ステップ2	<pre>configure terminal Example: switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します
ステップ 3	<pre>crypto ca import name [pksc12] bootflash:filename Example: switch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.p12 nbv123</pre>	アイデンティティ証明書と、トラストポ イントCAの対応するキーペアとCA証 明書をインポートします。
ステップ4	<pre>exit Example: switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ5	(Optional) show crypto ca certificates Example: switch# show crypto ca certificates	CA 証明書を表示します。
ステップ6	<pre>(Optional) copy running-config startup-config Example: switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スター トアップ コンフィギュレーションにコ ピーします。

CRLの設定

トラストポイントからダウンロードした CRL を手動で設定することができます。Cisco NX-OS ソフトウェアでは、CRL をデバイスのブートフラッシュ(cert-store)にキャッシュします。ピ ア証明書の検証の際、Cisco NX-OS ソフトウェアが発行した CA からの CRL をチェックするの は、CRL をデバイスにダウンロードしていて、この CRL を使用する証明書取消確認を設定し ている場合だけです。

Before you begin

証明書取消確認がイネーブルになっていることを確認します。

Procedure

	Command or Action	Purpose
ステップ1	<pre>copy scheme:[//server/[url /]]filename bootflash:filename</pre>	リモート サーバから CRL をダウンロー ドします。
	Example:	<i>scheme</i> 引数に対しては、 tftp: 、 ftp: 、
	switch# copy tftp:adminca.crl bootflash:adminca.crl	scp: 、または sftp: を入力できます。 <i>server</i> 引数は、リモートサーバのアドレ スまたは名前であり、 <i>url</i> 引数はリモー トサーバにあるソース ファイルへのパ スです。
		<i>server、url、</i> および <i>filename</i> の各引数 は、大文字小文字を区別して入力しま す。
ステップ2	configure terminal	グローバル コンフィギュレーション
	Example:	モードを開始します
	<pre>switch# configure terminal switch(config)#</pre>	
ステップ 3	crypto ca crl request name bootflash:filename	ファイルで指定されている CRL を設定 するか、現在の CRL と置き換えます。
	Example:	
	<pre>switch(config)# crypto ca crl request admin-ca bootflash:adminca.crl</pre>	
ステップ4	exit	コンフィギュレーション モードを終了
	Example: switch(config)# exit switch#	します。
ステップ5	(Optional) show crypto ca crl name	CA の CRL 情報を表示します。
	Example: switch# show crypto ca crl admin-ca	
ステップ6	(Optional) copy running-config startup-config	実行コンフィギュレーションを、スター トアップ コンフィギュレーションにコ
	Example:	ピーします。
	switch# copy running-config startup-config	

CAの設定からの証明書の削除

トラストポイントに設定されているアイデンティティ証明書やCA証明書を削除できます。最 初にアイデンティティ証明書を削除し、その後でCA証明書を削除します。アイデンティティ 証明書を削除した後で、RSA キーペアとトラストポイントの関連付けを解除できます。証明 書の削除は、期限切れになった証明書や取り消された証明書、破損した(あるいは破損したと 思われる)キーペア、現在は信頼されていない CA を削除するために必要です。

Procedure

	Command or Action	Purpose
ステップ1	configure terminal	グローバル構成モードを開始します。
	<pre>Example: switch# configure terminal switch(config)#</pre>	
ステップ2	<pre>crypto ca trustpoint name Example: switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#</pre>	トラストポイントCAを指定し、トラス トポイント コンフィギュレーション モードを開始します。
ステップ3	<pre>delete ca-certificate Example: switch(config-trustpoint)# delete ca-certificate</pre>	CA証明書または証明書チェーンを削除 します。
ステップ4	<pre>delete certificate [force] Example: switch(config-trustpoint)# delete certificate</pre>	アイデンティティ証明書を削除します。 削除しようとしているアイデンティティ 証明書が証明書チェーン内の最後の証明 書である場合や、デバイス内の唯一のア イデンティティ証明書である場合は、 force オプションを使用する必要があり ます。この要件は、証明書チェーン内の 最後の証明書や唯一のアイデンティティ 証明書を誤って削除してしまい、アプリ ケーション (SSH など) で使用する証 明書がなくなってしまうことを防ぐため に設けられています。
ステップ5	<pre>exit Example: switch(config-trustpoint)# exit switch(config)#</pre>	トラストポイントコンフィギュレーショ ン モードを終了します。

	Command or Action	Purpose
ステップ6	(Optional) show crypto ca certificates [<i>name</i>]	CA の証明書情報を表示します。
	Example:	
	switch(config)# show crypto ca certificates admin-ca	
ステップ 1	(Optional) copy running-config startup-config	実行コンフィギュレーションを、スター トアップ コンフィギュレーションにコ
	Example:	ピーします。
	switch(config)# copy running-config startup-config	

Cisco NX-OSデバイスからの RSA キーペアの削除

RSAキーペアが何らかの理由で破損し、現在は使用されてないと見られるときには、そのRSA キーペアを Cisco NX-OS デバイスから削除することができます。



Note

デバイスから RSA キーペアを削除した後、CA アドミニストレータに、その CA にあるこのデバイスの証明書を取り消すよう依頼します。その証明書を最初に要求したときに作成したチャレンジパスワードを入力する必要があります。

Procedure

	Command or Action	Purpose
ステップ1	configure terminal	グローバル コンフィギュレーション
	Example:	モードを開始します
	<pre>switch# configure terminal switch(config)#</pre>	
ステップ2	crypto key zeroize rsa label	RSA キーペアを削除します。
	Example:	
	switch(config)# crypto key zeroize rsa MyKey	
ステップ3	exit	コンフィギュレーション モードを終了
	Example:	します。
	switch(config)# exit switch#	
ステップ4	(Optional) show crypto key mypubkey rsa	RSA キーペアの設定を表示します。
	Example:	
	switch# show crypto key mypubkey rsa	

	Command or Action	Purpose
ステップ5	(Optional) copy running-config startup-config	実行コンフィギュレーションを、スター トアップ コンフィギュレーションにコ
	Example:	ピーします。
	switch# copy running-config startup-config	

Related Topics

証明書要求の作成 (16ページ)

PKIの設定の確認

PKI 設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show crypto key mypubkey rsa	Cisco NX-OS デバイスで作成 された RSA 公開キーの情報を 表示します。
show crypto ca certificates	CAとアイデンティティ証明書 についての情報を表示しま す。
show crypto ca crl	CA の CRL についての情報を 表示します。
show crypto ca trustpoints	CA トラストポイントについて の情報を表示します。

PKIの設定例

ここでは、Microsoft Windows Certificate サーバを使用して Cisco NX-OS デバイスで証明書と CRL を設定する作業の例について説明します。



Note デジタル証明書の作成には、どのようなタイプのサーバでも使用できます。Microsoft Windows Certificate サーバに限られることはありません。

Cisco NX-OS デバイスでの証明書の設定

Cisco NX-OS デバイスで証明書を設定するには、次の手順に従ってください。

Procedure

- ステップ1 デバイスの FQDN を設定します。 switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. switch(config)# hostname Device-1 Device-1(config)#
- **ステップ2** デバイスの DNS ドメイン名を設定します。

Device-1(config) # ip domain-name cisco.com

ステップ3 トラストポイントを作成します。

Device-1(config)# crypto ca trustpoint myCA Device-1(config-trustpoint)# exit Device-1(config)# show crypto ca trustpoints trustpoint: myCA; key: revokation methods: crl

ステップ4 このデバイス用の RSA キー ペアを作成します。

Device-1(config)# crypto key generate rsa label myKey exportable modulus 1024
Device-1(config)# show crypto key mypubkey rsa
key label: myKey
key size: 1024
exportable: yes

ステップ5 RSA キーペアとトラストポイントを関連付けます。

Device-1(config)# crypto ca trustpoint myCA Device-1(config-trustpoint)# rsakeypair myKey Device-1(config-trustpoint)# exit Device-1(config)# show crypto ca trustpoints trustpoint: myCA; key: myKey revokation methods: crl

- **ステップ6** Microsoft Certificate Service の Web インターフェイスから CA をダウンロードします。
- **ステップ7** トラストポイントに登録する CA を認証します。

Device-1(config)# crypto ca authenticate myCA input (cut & paste) CA certificate (chain) in PEM format; end the input with a line containing only END OF INPUT : -----BEGIN CERTIFICATE-----

MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRI1jK0ZejANBgkqhkiG9w0BAQUFADCB kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAk10 MRIwEAYDVQQIEw1LYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE ChMFQ21zY28xEzARBgNVBAsTCm51dHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN AQkBFhFhbWFuZGt1QGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3J1MQ4wDAYDVQQKEwVDaXNjbzETMBEG A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHz1uNccNM87ypyzwuoSNZXOMpeRXXI

```
OzyBAgiXT2ASFuUOwQ1iDM8r0/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU20yRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6qLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
----END CERTIFICATE----
END OF INPUT
Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
Do you accept this certificate? [yes/no]:y
Device-1(config) # show crypto ca certificates
Trustpoint: myCA
CA certificate 0:
subject= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/
L=Bangalore/O=Yourcompany/OU=netstorage/CN=Aparna CA
issuer= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/
L=Bangalore/O=Yourcompany/OU=netstorage/CN=Aparna CA
serial=0560D289ACB419944F4912258CAD197A
notBefore=May 3 22:46:37 2005 GMT
```

```
ステップ8 トラストポイントに登録するために使用する証明書要求を作成します。
```

MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12

notAfter=May 3 22:55:17 2007 GMT

purposes: sslserver sslclient ike

```
Device-1(config) # crypto ca enroll myCA
Create the certificate request ..
 Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.
  Password: nbv123
 The subject name in the certificate will be: Device-1.cisco.com
 Include the switch serial number in the subject name? [yes/no]: no
 Include an IP address in the subject name [yes/no]: yes
ip address: 10.10.1.1
The certificate request will be displayed ...
----BEGIN CERTIFICATE REQUEST----
MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ
DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
----END CERTIFICATE REQUEST----
```

ステップ9 Microsoft Certificate Service の Web インターフェイスからアイデンティティ証明書を要求しま す。

ステップ10 アイデンティティ証明書をインポートします。

Device-1(config)# crypto ca import myCA certificate input (cut & paste) certificate in PEM format: ----BEGIN CERTIFICATE-----MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAk1OMRIwEAYD

VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ21z Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZ1Z2FzLTEu Y21zY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBqQC/GNVACdjQu41C dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47 glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWefgrR bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3J1MQ4w DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh cm5hIENBghAFYNKJrLQZ1E9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6 Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmE1MjBDQS5jcmwwMKAuoCyGKmZpbGU6 $\verb"Ly9cXHnzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH"$ AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3N1LTA4L0N1cnRFbnJvbGwvc3N1 LTA4X0Fw YXJuYSUy MENBLmNy dDA9BggrBgeFBQcwAoYxZmlsZTovL1xcc3N1LTA4 $\tt XENlcnRFbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF$ ${\tt AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw} \\$ E36cIZu4WsExREqxbTk8ycx7V5o= ----END CERTIFICATE-----

Device-1(config)# **exit** Device-1#

ステップ11 証明書の設定を確認します。ステップ12 証明書の設定をスタートアップ コンフィギュレーションに保存します。

Related Topics

CA 証明書のダウンロード (29 ページ) アイデンティティ証明書の要求 (35 ページ)

CA 証明書のダウンロード

Microsoft Certificate Service の Web インターフェイスから CA 証明書をダウンロードする手順 は、次のとおりです。

Procedure

ステップ1 Microsoft Certificate Services の Web インターフェイスから、[Retrieve the CA certificate or certificate revocation task] をクリックし、[Next] をクリックします。

Microsoft Certificate Services -- Aparna CA

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other s will be able to securely identify yourself to other people over the web, sign your e-mail mes depending upon the type of certificate you request.

Select a task:

- Retrieve the CA certificate or certificate revocation list
- C Request a certificate
- C Check on a pending certificate

ステップ2 表示されたリストから、ダウンロードする CA 証明書ファイルを選択します。[Base 64 encoded] をクリックし、[Download CA certificate] をクリックします。

Microsoft Certificate Services -- Aparna CA

Retrieve The CA Certificate Or Certificate Revocation List

Install this CA certification path to allow your computer to trust certificates issued from t

It is not necessary to manually install the CA certification path if you request and install a CA certification path will be installed for you automatically.

Choose file to download:

CA Certificate: Current [Aparna CA]

○ DER encoded or ● Base 64 encoded

Download CA certificate

Download CA certification path

Download latest certificate revocation list

ステップ3 [File Download] ダイアログボックスにある [Open] をクリックします。



I

ステップ4	[Certificate] ダイアログボックスにある [Copy to File] をクリックし、[OK] をクリックします。

<i>Microsoft</i> Certificate Services Apama CA		
Retrieve The CA Certificate Or Certi	ficate Revocation List	
Install this CA certification path to allow	General Details Certification	Path
It is not necessary to manually install th CA certification path will be installed fc	Show: <a>All>	•
Choose file to download:	Field	Value V3
CA Certificate: Current [Aparna CA]	Serial number Signature algorithm Issuer	0560 D289 ACB4 1994 4F4 sha1RSA Aparna CA, netstorage, C
© DER encoded or 《	Valid to	04 Mei 2007 4:25:17 Aparna CA, netstorage, C
<u>Download CA certifica</u> <u>Download CA certifica</u>		RSA (512 Bits)
<u>Download latest certific</u>		
		Edit Properties

r

ステップ5 [Certificate Export Wizard] ダイアログボックスから [Base-64 encoded X.509 (CER)] を選択し、 [Next] をクリックします。

	Certificate	
Install this CA certification path to allow	General Details	Certification Path
It is not necessary to manually install th CA certification path will be installed fc	Show: <a>All>	Certificate Evnort Wizard
Choose file to download: CA Certificate: Current [Aparna CA]	Version Serial numbe Signature alç	Export File Format Certificates can be exported in a variety
© DER encoded or (<u>Download CA certifica</u> <u>Download CA certifica</u> Download latest certific	Valid from Valid from Subject	Select the format you want to use: © DER encoded binary X.509 (.CEF © Base-64 encoded X.509 (.CER) © Cryptographic Message Syntax S
		 Personal Information Exchange - Include all certificates in the Enable strong protection (rec
		Delete the private <u>k</u> ey if the

- **ステップ6** [Certificate Export Wizard] ダイアログボックスにある [File name:] テキスト ボックスに保存する ファイル名を入力し、[Next] をクリックします。
- **ステップ7** [Certificate Export Wizard] ダイアログボックスで、[Finish] をクリックします。

ステップ8 Microsoft Windows の type コマンドを入力して、Base-64 (PEM) 形式で保存されている CA 証 明書を表示します。

D:\testcerts>type_aparnaCA.cer BEGIN_CERTIFICATE MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRI1jK0ZejANBgkqhkiG9w0BAQUFAD kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRZUBjaXNjby5jb20xCzAJBgNUBAYTAk MRIwEAYDUQQIEw1LYXJuYXRha2ExEjAQBgNUBAcTCUJhbmdhbG9yZTEOMAwGA1 ChMFQ21zY28xEzARBgNUBAsTCm51dHN0b3JhZ2UxEjAQBgNUBAMTCUFwYXJuYS QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhv AQkBFhFhbWFuZGt1QGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNUBAGTCU cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3J1MQ4wDAYDUQQKEwUDaXNjbzETMB A1UECxMKbmU0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhv AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHz1uNccNM87ypyzwuoSNZX0MpeRX
BAMCAcYwDwYDUROTAQH/BAUwAwEB/zAdBgNUHQ4EFgQUJyjyRoMbrCNMRU2OyR GgsWbHEwawYDUROfBGQwYjAuoCygKoYoaHROcDovL3NzZSOwOC9DZXJORW5yb2 LØFwYXJuYSUyMENBLmNybDAwoC6gLIYqZm1sZTovL1xcc3N1LTA4XEN1cnRFbn bGxcQXBhcm5hJTIwQOEuY3JsMBAGCSsGAQQBgjcUAQQDAgEAMA0GCSqGSIb3DQ BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9 NBG7E0oN66zex0E0EfG1Vs6mXv1//w==
BAMCAcYwDwYDUROTAQH/BAUwAwEB/zAdBgNUHQ4EFgQUJyjyRoMbrCNMRU2OyR GgsWbHEwawYDUROfBGQwYjAuoCygKoYoaHROcDovL3NzZSOwOC9DZXJORW5yb2 LØFwYXJuYSUyMENBLmNybDAwoC6gLIYqZm1sZTovL1xcc3N1LTA4XEN1cnRFbn bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcUAQQDAgEAMA0GCSqGSIb3DQ BQUAA0EAHv6UQ+8nE399Tww+KaGrØg0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9 NBG7E0oN66zex0EOEfG1Vs6mXp1//w== END_CERTIFICATE

アイデンティティ証明書の要求

PKCS#12 証明書署名要求(CSR)を使用して Microsoft Certificate サーバにアイデンティティ証明書を要求するには、次の手順に従ってください。

Procedure

ステップ1 Microsoft Certificate Services の Web インターフェイスから、[証明書の要求 (Request a certificate)]をクリックし、[次へ (Next)]をクリックします。

Microsoft Certificate Services -- Aparna CA

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other s will be able to securely identify yourself to other people over the web, sign your e-mail mes depending upon the type of certificate you request.

Select a task:

- C Retrieve the CA certificate or certificate revocation list
- Request a certificate
- C Check on a pending certificate

ステップ2	[詳細な要求	(Advanced request)]をクリックし、	[次へ	(Next)]をクリッ	ヮします。
-------	--------	--------------------	----------	-----	--------	-------	-------

Microsoft Certificate Services -- Aparna CA

Choose Request Type

Please select the type of request you would like to make:

O User certificate request:



Advanced request

ステップ3 [Base64エンコード済み PKCS#10 を使用する証明書要求または base64 エンコード済み PKCS#7 ファイルを使用する更新要求を送信する (Submit a certificate request using a base64 encoded PKCS#10 file or a renewal request using a base64 encoded PKCS#7 file)] をクリックし、[次へ

(Next)]をクリックします。

Microsoft Certificat	te Services Apari	na CA		
Advanced Cert	ificate Requests	5		
You can request certification auth	a certificate for y ority (CA) will det	ourself, another u ermine the certifi	ser, or a computer cates that you can	using one of the foll obtain.
O Submit a cer	rtificate request to	o this CA using a	form.	
Submit a cer	rtificate request u	sing a base64 er	ncoded PKCS #10	file or a renewal rec
C Request a ce You must have	ertificate for a sm an enrollment agen	art card on beha t certificate to subm	f of another user us it a request for another	sing the Smart Card r <i>user.</i>

ステップ4 [保存済みの要求 (Saved Request)]テキストボックスに、base64のPKCS#10証明書要求をペーストし、[次へ (Next)]をクリックします。証明書要求が Cisco NX-OS デバイスのコンソール

からコピーされます。

Microsoft Certificate Services -- Aparna CA

Submit A Saved Request

Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request server) into the request field to submit the request to the certification authority (CA).

Saved Request:

ステップ5 CAアドミニストレータから証明書が発行されるまで、1~2日間待ちます。

Microsoft Certificate Services -- Aparna CA

Certificate Pending

Your certificate request has been received. However, you must wait for an administrator to

Please return to this web site in a day or two to retrieve your certificate.

Note: You must return with this web browser within 10 days to retrieve your certificate

I

ステップ6 CA アドミニストレータが証明書要求を承認するのを確認します。

Tree	Request ID	Binary Request	Request Disposition Message	Request S
📴 Certification Authority (Local)	116	BEGIN NE	Taken Under Submission	11/12/200 All Tasks
Revoked Certificates				Refresh
Pending Requests			_	Help
Environment Failed Requests				

ステップ7 Microsoft Certificate Services の Web インターフェイスから、[保留中の証明書をチェックする (Check on a pending certificate)]をクリックし、[次へ(Next)]をクリックします。

Microsoft Certificate Services -- Aparna CA

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other s will be able to securely identify yourself to other people over the web, sign your e-mail mes depending upon the type of certificate you request.

Select a task:

- C Retrieve the CA certificate or certificate revocation list
- C Request a certificate
- Check on a pending certificate

ステップ8 チェックする証明書要求を選択して、[次へ (Next)]をクリックします。

Microsoft Certificate Services -- Aparna CA

Check On A Pending Certificate Request

Please select the certificate request you want to check:

Saved-Request Certificate (12 Nopember 2005 20:30:22)

ステップ9 [Base 64 エンコード済み(Base 64 encoded)]をクリックして、[CA 証明書のダウンロード (Download CA certificate)]をクリックします。

Microsoft Certificate Services -- Apama CA
Certificate Issued
The certificate you requested was issued to you.
© DER encoded or © Base 64 encoded
Download CA certificate
Download CA certification path

ステップ10 [ファイルのダウンロード(File Download)]ダイアログボックスで、[開く (Open)]をクリックします。

 ○ DER encoded or ● Base 6 ▶ Download CA certificate Download CA certification path Some files can harm your computer. If the file inf looks suspicious, or you do not fully trust the sou save this file. ■ File name: certnew.cer ■ File type: Security Certificate ■ From: 10.76.45.108 ● This type of file could harm your computer in malicious code. ■ Would you like to open the file or save it to your ■ Den Save Cancel ■ Always ask before opening this type of file 	ODER encoded or ⊙Base	6 File Dow	nioad		
Image: Download CA certification path Image: Security Certificate Save this file. File name: certnew.cer File type: Security Certificate From: 10.76.45.108 Image: Comparison of the could harm your computer in the malicious code. Would you like to open the file or save it to your Image: Download CA certification path File name: certnew.cer File type: Security Certificate From: 10.76.45.108 Image: Certnew.cer Security Certificate From: 10.76.45.108 Image: Certnew.cer Security Certificate Image: Certnew.cer Security Certificate From: 10.76.45.108 Image: Certnew.cer Security Certificate Image: Certnew.cer Security Certificate	Download CA certificate	9	Some files can h	iarm your compute	er. If the file info
File name: certnew.cer File type: Security Certificate From: 10.76.45.108 Image: Computer of the could harm your computer in the stype of file could harm your computer in the stype of the could you like to open the file or save it to your Image: Open Save Image: Cancel Image: Always ask before opening this type of file	bownload CA certification path		looks suspicious save this file.	, or you do not ful	lly trust the sou
File type: Security Certificate From: 10.76.45.108		-	File name:	certnew.cer	
From: 10.76.45.108			File type:	Security Certifica	ite
This type of file could harm your computer i malicious code. Would you like to open the file or save it to your <u>Open</u> <u>Save</u> Cancel Mays ask before opening this type of file			From:	10.76.45.108	
Would you like to open the file or save it to your □pen Save Cancel ✓ Always ask before opening this type of file			A This type of malicious co	í file could harm y ode.	our computer if
Always ask before opening this type of file			Would you like to	o open the file or : Save	save it to your
			Always ask t	pefore opening thi	is type of file

ステップ11 [Certificate] ボックスで、[Details] タブをクリックし、[Copy to File...] をクリックします。. [証 明書のエクスポート ダイアログ (Certificate Export Dialog)] ボックスで、[Base-64 エンコード 済み X.509 (.CER) (Base-64 encoded X.509 (.CER))] をクリックし、[次へ (Next)] をクリッ

General Decais Certification	n Path	b-
Show: <a>All>	•	
Field	Value	
Serial number Signature algorithm Issuer Valid from Valid to Subject Public key	0A33 8EA1 0000 0000 0074 sha1R5A Aparna CA, netstorage, Cisco 12 Nopember 2005 8:32:40 12 Nopember 2006 8:42:40 Vegas-1.cisco.com R5A (1024 Bits)	
	Edit Properties	Select the format you want C DER encoded binary
		C Cryptographic Messa
		C <u>P</u> ersonal Information Include all certific Enable strong pr
		I_ Delete the privat

ステップ12 [証明書エクスポートウィザード (Certificate Export Wizard)]ダイアログボックスにある[ファ イル名: (File name:)]テキストボックスに保存するファイル名を入力し、[次へ (Next)]を



Microsoft Certificate Services - Microsoft Internet Explorer provided by Cisco Systems, Inc. ? × General Details Certification Path b- 🗿 🖸 - 🗐 A • Show: <All> Field ٠ Value Version ٧3 💳 Serial number 0A33 8EA1 0000 0000 0074 💳 Signature algorithm sha1RSA EIssuer Aparna CA, netstorage, Cisco... 💳 Valid from 12 Nopember 2005 8:32:40 💳 Valid to 12 Nopember 2006 8:42:40 E Subject Vegas-1.cisco.com 🖻 Public key RSA (1024 Bits) • Certificate Export Wizard Completin Wizard You have succes wizard. Edit Properties... Copy to F You have specifi File Name Export Keys Include all cert File Format •

ステップ13 [完了 (Finish)]をクリックします。

ステップ14 Microsoft Windows の **type** コマンドを入力して、アイデンティティ証明書を Base-64 でエンコードされた形式で表示します。

C:\WINNT\system32\cmd.exe
D:\testcerts>type myID.cer BEGIN CERTIFICATE MIIEADCCA6qgAwIBAgIKCj00oQAAAAAAADDANBgkqhkiG9w0BAQUFADCBkDEgMB4G CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20kCzAJBgNUBAYTAk10MRIwEAYD VQQIEw1LYXJuYXRha2ExEjAQBgNUBACTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ21z Y28xEzARBgNUBAsTCD51dHN0b3JhZ2UxEjAQBgNUBAMTCUFwYXJuYSBDQTAeFw0w NTExMTIWZA9NDBaFw0wNjExMTIWZEyNDBaMBwxGjAYBgNUBAMTEVZ1Z2FzLTEu Y21zY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C dq1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2U0iyeCYE8ylncWyw5E08rJ47 g1xr42/s19IRIb/8udU/cj9jSfKK56koa7xWYAu8rDf28jMCnIM4W1aY/q2q4Gb x7RifdU06uFqFZEgs17/E1ash9LxLwIDAQABo41CEzCCAg8wJQYDUR0RAQH/BBsw GYIRUmUNYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDUR00BBYEFKCLi+2sspWefgrR bhWm1Uyo9jngMIHMBgNUHSMEgcQwgcGAFCco8kaDG6wjTEUNjskYUBoLFmxxoYGW PIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZG11QGNpc2NvLmNvbTELMAkGA1UE BhMCSU4xEjAQBgNUBAgTCUthcm5hdGFYTESMBAGA1UEBxMJQmFuZ2Fsb3J1MQ4w DAYDUQQKEwUDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh cm5hIENBghAFYNKJrLQZIE9JEiWMrR16MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6 Ly9c2UtMDgvQ2UydEUucm9sbC9BcGFybmEIMjBDQSjcmwMKAuoCyGKmZpbGU6 Ly9c2UtMDgvQ2UydEUucm9sbC9BcGFybmEIMjBDQSjcmwMKAuoCyGKmZpbGU6 Ly9c2UtMDgvQ2UydEUucm9sbC9BcGFybmEIMjBDQSjcmwMKAuoCyGKmZpbGU6 Ly9c2UtMDgvQ2UydEUucm9sbC9BcGFybmEIMjBDQSjcmwMKAuoCyGKmZpbGU6 Ly9c2UtMDgvQ2UydEUucm9sbC9BcGFybmEIMjBDQSjcmwMKAuoCyGKmZpbGU6 Ly9c2UtMDgvQ2UydEUucm9sbC9BcGFybmEIMjBDQSjcmwMKAuoCyGKmZpbGU6 Ly9c2UtMDgvQ2UydEUucm9sbC9BcGFybmEIMjBDQSjcmwMKAuoCyGKmZpbGU6 Ly9c2UtMDgvQ2UydEUucm9sbC9BcGFybmEIMjBDQSjcmwMKAuoCyGKmZpbGU6 Ly9c2UtMDgvQ2UydEUucm9sbC9BcGFybmEIMjBDQSjcmwMKAuoCyGKmZpbGU6 Ly9c2UtMDgvQ2UydEUucm9sbC9BcGFybmEIMjBDQSjcmwMKAuoCyGKmZpbGU6 Ly9c2UtMDgvQ2UydEUucm9sbC9BcGFybmEIMjBDQSjcmwMKAuoCyGKmZpbGU6 Ly9c2UtMDgvQ2UydEUucm9sbC9BcGFybmEIMjBDQSjcmwMKAuOCyGKmZpbGU6 Ly9c2UtMDgvQ2UydEUucm9sbC9BcGFybmEIMjBDQSjcmwMKAuOCyGKmZpbGU6 Ly9c2UtMDgvQ2UydEUucm9sbC9BcGFybmEIMjBDQAYZm1sZTovL1xcc3N1LTA4 XEN1cnRFbnJvbGxcc3N1LTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF AANBADbGBGsbe7GNLh9xe0TWBNbm24U69ZSuDDcOcUZUUTgrpnTqVP
D:\testcerts>

Related Topics

証明書要求の作成 (16 ページ)Cisco NX-OS デバイスでの証明書の設定 (26 ページ)

証明書の取り消し

Microsoft CA 管理者プログラムを使用して証明書を取り消す手順は、次のとおりです。

Procedure

ステップ1 [Certification Authority] ツリーから、[Issued Certificates] フォルダをクリックします。リストから、取り消す証明書を右クリックします。

I

Certification Authority (Local) Aparna CA Revoked Certificates Seg 92 Pending Requests Failed Requests 93 94 99 91 10 10	ascab Re SS SS SS SS SS SS SS SS SS SS SS SS SS	Quester Name E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS	j j j 5 B	EGIN CERTI EGIN CERTI	Serial Number 786263d00000000000 7862643d000000000 7862643d000000000 7c327818000000000 7c3278270000000000 7c3278370000000000 7c3278470000000000 7c3278470000000000 7c3278470000000000 7c3278470000000000 7c3278470000000000 7c3278470000000000 1c1013cf0000000000 1c10d1910000000000 2b4eb3670000000000 458b6b4300000000000000000000000000000000000
Certification Authority (Local) Aparna CA Revoked Certificates Issued Certificates Pending Requests Failed Requests 99 10 11 11	55 55 55 55 55 55 55 1 55 2 55 3 55 5 55 5 55 5 55 5 55	E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS	5B 5B 5B 5B 5B 5B 5B 5B 5B 5B 5B	EGIN CERTI EGIN CERTI	78626300000000000000000000000000000000000
Aparna CA 90 Revoked Certificates 91 Issued Certificates 92 Pending Requests 93 Failed Requests 94 99 91 10 910 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 11 11	55 55 55 55 55 55 55 5 5 5 5 5 5 5 5 5	E-U8/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS	5B 5B 5B 5B 5B 5B 5B 5B 5B 5B 5B	EGIN CERTI EGIN CERTI	786264300000000000000000000000000000000000
Revoked Certificates 99 Subscription of the second	55 55 55 55 55 55 1 55 2 55 3 55 4 55 5 55 5 55 5 55	E-U8/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS	5B 5B 5B 5B 5B 5B 5B 5B 5B 5B	EGIN CERTI EGIN CERTI	7c32781800000000000000000 7c3278270000000000 7c3278370000000000 7c3278470000000000 7ca48c220000000000 021a9d1a0000000000 1c1013cf0000000000 1c10d1910000000000 2b4eb3670000000000 458b6b4300000000000000000000000000000000000
Issued Certificates 192 Pending Requests 100 Failed Requests 100 10 100 10 100 100 100	55 55 55 55 55 0 55 1 55 2 55 3 55 5 55 5 55 5 55	E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS	5B 5B 5B 5B 5B 5B 5B 5B 5B	EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI	7c327818000000000 7c3278270000000000 7c3278370000000000 7c3278470000000000 021a9d1a0000000000 1c1013cf00000000000 1c10d1910000000000 2b4eb3670000000000 458b6b4300000000000000000000000000000000000
■ Pending Requests ■ 93 ■ Failed Requests ■ 94 ■ 95 ■ 98 ● 98 ■ 99 ■ 10 ■ 10 ■ 10 ■ 10 ■ 10 ■ 10 ■ 10 ■ 10 ■ 10 ■ 10 ■ 10 ■ 10 ■ 10 ■ 10 ■ 10 ■ 10 ■ 10 ■ 10 ■ 10 ■ 10 ■ 11 ■ 11	55 55 55 0 55 1 55 2 55 3 55 4 55 5 55 5 55	E-U8(IUSR_SS E-08(IUSR_SS E-08(IUSR_SS E-08(IUSR_SS E-08(IUSR_SS E-08(IUSR_SS E-08(IUSR_SS E-08(IUSR_SS E-08(IUSR_SS E-08(IUSR_SS E-08(IUSR_SS	5B 5B 5B 5B 5B 5B 5B 5B 5B	EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI	7c3278270000000000 7c3278370000000000 7c3278470000000000 021a9d1a0000000000 1c1013cf00000000000 1c10d1910000000000 2b4eb3670000000000 458b6b4300000000000000000000000000000000000
Falled Requests 194 195 199 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 11 11 11 11	55 55 0 55 1 55 2 55 3 55 4 55 5 55 5 55	E-U8/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS E-08/IUSR_SS	5B 5B 5B 5B 5B 5B 5B 5B	EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI	7c3278370000000000 7c3278470000000000 021a9d1a0000000000 1c1013cf00000000000 1c10d1910000000000 2b4eb3670000000000 458b6b4300000000000000000000000000000000000
295 299 2910 29	55 55 0 55 1 55 2 55 3 55 4 55 5 55 5 55	E-U8\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS	5B 5B 5B 5B 5B 5B 5B	EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI	7c3278470000000000 7ca48c220000000000 021a9d1a0000000000 1c1013cf00000000000 1c10d1910000000000 2b4eb3670000000000 458b6b430000000000 4eb5b327000000000000000000000000000000000000
10 10 10 10 10 10 10 10 10 10	55 55 0 55 2 55 3 55 4 55 5 55 5 55 5 55	E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS	5B 5B 5B 5B 5B 5B	EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI	7ca48c2200000000000000000000000000000000000
299 2010 2	55 0 55 1 55 2 55 3 55 4 55 5 55 5 55	E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS	5E 5E 5E 5E 5E 5E	EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI	021a9d1a000000000 1c1013cf0000000000 1c10d1910000000000 2b4eb3670000000000 458b6b430000000000 4eb5b327000000000000000000000000000000000000
10 10 10 10 10 10 10 10 10 10	0 SS 1 SS 2 SS 3 SS 4 SS 5 SS 5 SS	E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS	5B 5B 5B 5B 5B	EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI	1c1013cr0000000000 1c10d191000000000 2b4eb367000000000 458b6b43000000000 4eb5b3270000000000
10 10 10 10 10 10 10 10 10 10	1 55 2 55 3 55 4 55 5 55 5 55	E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS	5B 5B 5B 5B	EGIN CERTI EGIN CERTI EGIN CERTI EGIN CERTI	1c10d1910000000000 2b4eb3670000000000 458b6b43000000000 4eb5b3270000000000
10 10 10 10 10 10 10 10 10 10	2 SS 3 SS 4 SS 5 SS 5 SS	E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS	5В 5В 5В	EGIN CERTI EGIN CERTI EGIN CERTI	2b4eb3670000000000 458b6b430000000000 4eb5b32700000000000
10 10 10 10 10 10 10 10 10 10	3 SS 4 SS 5 SS 6 SS	E-08\IUSR_SS E-08\IUSR_SS E-08\IUSR_SS	5B 5B	EGIN CERTI EGIN CERTI	458b6b430000000000 4eb5b3270000000000
10 10 10 10 10 10 10 10 11 11 11	4 SS 5 SS 6 SS	E-08\IUSR_SS E-08\IUSR_SS	5B	EGIN CERTI	4eb5b3270000000000
10 10 10 10 10 10 11 11 11 11	5 SS 6 SS	E-08\IUSR_SS	-		
10 10 10 10 10 11 11 11	6 SS		рВ	EGIN CERTI	4f6008410000000000
10 10 10 10 11 11 11	-	E-08\IUSR_SS	БВ	EGIN CERTI	4fdf956400000000000
10 10 11 11 11	7 SS	E-08\IUSR_SS	5В	EGIN CERTI	5f3e8c960000000000
10 11 11 11	8 SS	E-08\IUSR_SS	5В	EGIN CERTI	5f413d200000000000
11 11 11	9 SS	E-08\IUSR_SS	5B	EGIN CERTI	17b22de8000000000
See 11	0 SS	E-08\IUSR_SS	5В	EGIN CERTI	17b30676000000000
	1 SS	E-08\IUSR_SS	5В	EGIN CERTI	11ea38060000000000
11	2 SS	E-08\IUSR_SS	5В	EGIN CERTI	170bea8b000000000
11	3 SS	E-08\IUSR_SS	5В	EGIN CERTI	4aafff2e00000000007
11	4 SS	E-08\IUSR_SS	5В	EGIN CERTI	78cc6e6c0000000000
E 11	5 SS	E-08\IUSR_SS	5В	EGIN CERTI	78e34161000000000
11	6 SS	E-08 ¹ TUSR SS	iB	EGIN CERTI	0a338ea1000000000
		Oper	n		

ステップ2 [All Tasks] > [Revoke Certificate] の順に選択します。

📴 Certification Authority				
📙 Action View 🗍 🖨 🔿 🗈 🖪	1 🔮 🖫	B		
Tree	Request ID	Requester Name	Binary Certificate	Serial Number
Certification Authority (Local)	89	SSE-08\IUSR_SS	BEGIN CERTI	786263d00000000
🗄 🕼 Aparna CA	90	SSE-08\IUSR_SS	BEGIN CERTI	7862643d0000000
Revoked Certificates	91	SSE-08\IUSR_SS	BEGIN CERTI	786264d90000000
	92	SSE-08\IUSR_SS	BEGIN CERTI	7c3278180000000
Pending Requests	93	SSE-08\IUSR_SS	BEGIN CERTI	7c3278270000000
Failed Requests	94	SSE-08\IUSR_SS	BEGIN CERTI	7c3278370000000
	95	SSE-08\IUSR_SS	BEGIN CERTI	7c3278470000000
	98 👔		DECIN CEDIT	
	99	Lertificate Revocatio		비스իօօ
	100	Are you sure you want	to revoke the selected	certificate(s)? 000
	101			000
	102	You may specify a reas	on for this revocation.	poor
	103	Reason code:		poor
	104	Unspecified	•	poor
	105	1		1000
	106		Yes	No 000
	107			000
	108	SSE-08\IUSR_SS	BEGIN CERTI	5F413d2000000000
	109	SSE-08\IUSR_SS	BEGIN CERTI	17b22de80000000
	110	SSE-08\IUSR_SS	BEGIN CERTI	17b306760000000
	111	SSE-08\IUSR_SS	BEGIN CERTI	11ea38060000000
	112	SSE-08\IUSR_SS	BEGIN CERTI	170bea8b0000000
	113	SSE-08\IUSR_SS	BEGIN CERTI	4aafff2e00000000
	114	SSE-08\IUSR_SS	BEGIN CERTI	78cc6e6c00000000
	115	SSE-08\IUSR_SS	BEGIN CERTI	78e341610000000
	116	SSE-08\IUSR_SS	BEGIN CERTI	0a338ea10000000
	•			
	500 00	N		

ステップ3 [Reason code] ドロップダウン リストから取り消しの理由を選択し、[Yes] をクリックします。

📴 Certification Authority				
<u>Action</u> ⊻iew	• 🖻 🕼 🖩	}∣ 😫		
Tree	Request ID	Requester Name	Binary Certificate	Serial Number
Certification Authority (Local)	15	SSE-08\IUSR_SS	BEGIN CERTI	5dae53cd00000000000
🖻 🕅 Aparna CA	16	SSE-08\IUSR_SS	BEGIN CERTI	5db140d30000000000
Revoked Certificates	17	SSE-08\IUSR_SS	BEGIN CERTI	5e2d7c1b0000000000
	18	SSE-08\IUSR_SS	BEGIN CERTI	16db4f8f00000000001
Pending Requests	19	SSE-08\IUSR_SS	BEGIN CERTI	261c39240000000000
Failed Requests	20	SSE-08\IUSR_SS	BEGIN CERTI	262b52020000000000
	21	SSE-08\IUSR_SS	BEGIN CERTI	2634c7f200000000000
	22	SSE-08\IUSR_SS	BEGIN CERTI	2635b00000000000000
	23	SSE-08\IUSR_SS	BEGIN CERTI	264850400000000000
	24	SSE-08\IUSR_SS	BEGIN CERTI	2a2763570000000000
	25	SSE-08\IUSR_SS	BEGIN CERTI	3f88cbf700000000001
	26	SSE-08\IUSR_SS	BEGIN CERTI	6e4b5f5f00000000000
	27	SSE-08\IUSR_SS	BEGIN CERTI	725689d80000000000
	28	SSE-08\IUSR_SS	BEGIN CERTI	735a88780000000000
	29	SSE-08\IUSR_SS	BEGIN CERTI	148511c70000000000
	30	SSE-08\IUSR_SS	BEGIN CERTI	14a717010000000000
	31	SSE-08\IUSR_SS	BEGIN CERTI	14fc45b500000000000
	32	SSE-08\IUSR_SS	BEGIN CERTI	486ce80b0000000002
	33	SSE-08\IUSR_SS	BEGIN CERTI	4ca4a3aa0000000002
	47	SSE-08\IUSR_SS	BEGIN CERTI	1aa55c8e00000000002
	63	SSE-08\IUSR_SS	BEGIN CERTI	3f0845dd0000000003
	66	SSE-08\IUSR_SS	BEGIN CERTI	3f619b7e00000000004
	82	SSE-08\IUSR_SS	BEGIN CERTI	6313c4630000000000
	96	SSE-08\IUSR_SS	BEGIN CERTI	7c3861e30000000000
	97	SSE-08\IUSR_SS	BEGIN CERTI	7c6ee3510000000000
	116	SSE-08\IUSR_SS	BEGIN CERTI	0a338ea10000000007
			1	
l				
1				

ステップ4 [Revoked Certificates] フォルダをクリックして、証明書の取り消しを表示および確認します。

CRLの作成と公開

Microsoft CA 管理者プログラムを使用して CRL を作成および公開する手順は、次のとおりです。

Procedure

ステップ1 [Certification Authority]の画面から、[Action]>[All Tasks]>[Publish]の順に選択します。

ě	Action View	⇔ ⇒ 🗈	💽 😭 🛃	₽ 😫		
ł	All Tasks 💦 🕨	Publish	Request ID	Requester Name	Binary Certificate	Serial Number
	Refresh	ty (Local)	- 🔯 15	SSE-08\IUSR_SS	BEGIN CERTI	5dae53cd0000000
	Export List	cy (Localy	16	SSE-08\IUSR_SS	BEGIN CERTI	5db140d3000000
		rtificates	17	SSE-08\IUSR_SS	BEGIN CERTI	5e2d7c1b0000000
	Properties	ficates	18	SSE-08\IUSR_SS	BEGIN CERTI	16db4f8f0000000
	Help	quests	19	SSE-08\IUSR_SS	BEGIN CERTI	261c3924000000
ļ	Falled Red	uests	20	SSE-08\IUSR_SS	BEGIN CERTI	262b5202000000
			21	SSE-08\IUSR_SS	BEGIN CERTI	2634c7f20000000
			22	SSE-08\IUSR_SS	BEGIN CERTI	263560000000000
			23	SSE-08\IUSR_SS	BEGIN CERTI	26485040000000
			24	SSE-08\IUSR_SS	BEGIN CERTI	2a276357000000
			25	SSE-08\IUSR_SS	BEGIN CERTI	3f88cbf70000000
			26	SSE-08\IUSR_SS	BEGIN CERTI	6e4b5f5f00000000
			27	SSE-08\IUSR_SS	BEGIN CERTI	725b89d8000000
			28	SSE-08\IUSR_SS	BEGIN CERTI	735a8878000000
			29	SSE-08\IUSR_SS	BEGIN CERTI	148511c7000000
			30	SSE-08\IUSR_SS	BEGIN CERTI	14a71701000000
			31	SSE-08\IUSR_SS	BEGIN CERTI	14fc45b50000000
			32	SSE-08\IUSR_SS	BEGIN CERTI	486ce80b000000
			33	SSE-08\IUSR_SS	BEGIN CERTI	4ca4a3aa0000000
			47	SSE-08\IUSR_SS	BEGIN CERTI	1aa55c8e0000000
			63	SSE-08\IUSR_SS	BEGIN CERTI	3f0845dd0000000
			100 66	SSE-08\IUSR_SS	BEGIN CERTI	3f619b7e0000000
			82	SSE-08\IUSR_SS	BEGIN CERTI	6313c463000000
			96	SSE-08\IUSR_SS	BEGIN CERTI	7c3861e30000000
			97	SSE-08\IUSR_SS	BEGIN CERTI	7c6ee3510000000
			116	SSE-08\IUSR_SS	BEGIN CERTI	0a338ea10000000

ステップ2 [Certificate Revocation List] ダイアログボックスで、[Yes] をクリックして最新の CRL を公開します。

Tree	Request ID	Requester Name	Binary Certificate	Serial Number
Certification Authority (Local)	- 🔯 15	SSE-08\IUSR_SS	BEGIN CERTI	5dae53cd00000000
	16	SSE-08\IUSR_SS	BEGIN CERTI	5db140d300000000
Revoked Certificates	17	SSE-08\IUSR_SS	BEGIN CERTI	5e2d7c1b00000000
Issued Certificates	18	SSE-08\IUSR_SS	BEGIN CERTI	16db4f8f00000000
Pending Requests	19	SSE-08\IUSR_SS	BEGIN CERTI	261c39240000000
Failed Requests	20	SSE-08\IUSR_SS	BEGIN CERTI	262b52020000000
	21	SSE-08\IUSR_SS	BEGIN CERTI	2634c7f200000000
	22	SSE-08\IUSR_SS	BEGIN CERTI	2635b00000000000
	23	SSE-08\IUSR_SS	BEGIN CERTI	264850400000000
	Revocation List	CRL is still valid and ca	n be used by clients. A	ire you sure you want
	The last published	CRL is still valid and ca	n be used by clients. A	re you sure you want
	The last published	CRL is still valid and ca Yes SSE-08\IUSR_SS	n be used by clients. A	re you sure you want
	The last published	CRL is still valid and ca Yes SSE-08\IUSR_SS SSE-08\IUSR_SS	n be used by clients. A s NoBEGIN CERTI PECIN CERTI	re you sure you want] 14fc45b5000000000 486ce80b00000000
	The last published	CRL is still valid and ca Yes SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS	n be used by clients. A	re you sure you want 14fc45b500000000 486ce80b0000000 4ca4a3aa00000000
	The last published	CRL is still valid and ca Yes SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS	n be used by clients. A	re you sure you want 14fc45b500000000 486ce80b0000000 4ca4a3aa00000000 1aa55c8e00000000
	The last published	CRL is still valid and ca Yes SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS	n be used by clients. A	re you sure you want 14fc45b5000000000 486ce80b0000000 4ca4a3aa00000000 1aa55c8e00000000 3f0845dd00000000
	Revocation List The last published	CRL is still valid and ca Yes SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS	n be used by clients. A	re you sure you want 14fc45b500000000 486ce80b0000000 4ca4a3aa00000000 1aa55c8e00000000 3f0845dd00000000 3f619b7e00000000 6313c46300000000
	Revocation List The last published	CRL is still valid and ca Yes SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS	n be used by clients. A No NoBEGIN CERTIBEGIN CERTIBEGIN CERTIBEGIN CERTIBEGIN CERTIBEGIN CERTIBEGIN CERTIBEGIN CERTIBEGIN CERTI	re you sure you want 14fc45b5000000000 486ce80b0000000 4ca4a3aa00000000 1aa55c8e00000000 3f0845dd00000000 3f619b7e00000000 6313c46300000000 7c3861e300000000
	Revocation List The last published	CRL is still valid and ca Yes SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS	n be used by clients. A No BEGIN CERTI BEGIN CERTI BEGIN CERTI BEGIN CERTI BEGIN CERTI BEGIN CERTI BEGIN CERTI BEGIN CERTI	re you sure you want 14fc45b5000000000 486ce80b0000000 4ca4a3aa00000000 1aa55c8e00000000 3f619b7e00000000 3f619b7e00000000 7c3861e300000000 7c6ee35100000000
	Revocation List The last published	CRL is still valid and ca Yes SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS SSE-08\IUSR_SS	n be used by clients. A	re you sure you want 14fc45b500000000 486ce80b0000000 4ca4a3aa0000000 1aa55c8e0000000 3f0845dd0000000 3f619b7e00000000 6313c4630000000 7c3861e30000000 0a338ea10000000

CRLのダウンロード

Microsoft 社の CA の Web サイトから CRL をダウンロードする手順は、次のとおりです。

Procedure

ステップ1 Microsoft Certificate Services の Web インターフェイスから、[Retrieve the CA certificate or certificate revocation list] をクリックし、[Next] をクリックします。

Microsoft Certificate Services -- Aparna CA

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or othe will be able to securely identify yourself to other people over the web, sign your e-mail r depending upon the type of certificate you request.

Select a task:

- Retrieve the CA certificate or certificate revocation list
- C Request a certificate
- C Check on a pending certificate

I

I

ステップ2 [Download latest certificate revocation list] をクリックします。

Microsoft Certificate Services Aparna CA
Retrieve The CA Certificate Or Certificate Revocation List
Install this CA certification path to allow your computer to trust certificates issued from thi
It is not necessary to manually install the CA certification path if you request and install a CA certification path will be installed for you automatically.
Choose file to download:
CA Certificate: Current [Aparna CA]
C DER encoded or
Download CA certificate
Download CA certification path
Download latest certificate revocation list

ステップ3 [File Download] ダイアログボックスで、[Save] をクリックします。

Microsoft Certificate Services Aparna CA		
Retrieve The CA Certificate Or Certificate Revo	ocation List	
leatell this CA contification path to allow your compu	top to the contificato	
nstail this CA certification path to allow your compl	iter to trust certificate	es issuea from i
t is not necessary to manually install the CA ^{File Dow}	nload	
CA certification path will be installed for you	C (l	
	looks suspicious, or you do	omputer. If the file info not fully trust the sour
hoose file to download:	save this file.	
CA Certificate: Current [Aparna CA]	File name: certorl.orl	
	File type: Certificate	Revocation List
	From: 10.76.45.1	08
ODER encoded or • Ba		
Deumland CA partificate		
Download CA certification a	Would you like to open the	file or save it to your c
Download latest certificate r	<u>Upen</u> <u>Save</u>	e Cancel
	🔽 Al <u>w</u> ays ask before open	ing this type of file

I

Microsoft Certificate Services Aparna CA			
Retrieve The CA Certificate Or Certificate	Revocation I	_ist	
Install this CA certification path to allow your c	omputer to tru	st certificates	s issued from this
It is not necessary to manually install the CA c CA certification path will be installed for you a	File Download Save As		
Choose file to download:	Save jn	: 🔁 testcerts	
CA Certificate: Current [Aparna CA]			
⊂DER encoded or ⊛Base			
Download CA certificate	Desktop		
Download CA certification pa			
	documents		
	Mu Computer		
		J	
	My Network P	File <u>n</u> ame:	aparnaCA.crl
		Save as <u>t</u> ype:	Certificate Revocati



Related Topics

証明書取消確認方法の設定(15ページ)

CRLのインポート

CRL を CA に対応するトラストポイントにインポートする手順は、次のとおりです。

Procedure

ステップ1 CRL ファイルを Cisco NX-OS デバイスのブートフラッシュにコピーします。

Device-1# copy tftp:apranaCA.crl bootflash:aparnaCA.crl

ステップ2 CRL を設定します。

Device-1# configure terminal

```
Device-1(config) # crypto ca crl request myCA bootflash:aparnaCA.crl
Device-1(config) #
```

ステップ3 CRL の内容を表示します。

```
Device-1(config) # show crypto ca crl myCA
Trustpoint: myCA
CRL:
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: shalWithRSAEncryption
       Issuer: /emailAddress=admin@yourcompany.com/C=IN/ST=Karnatak
Yourcompany/OU=netstorage/CN=Aparna CA
       Last Update: Nov 12 04:36:04 2005 GMT
       Next Update: Nov 19 16:56:04 2005 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
            keyid:27:28:F2:46:83:1B:AC:23:4C:45:4D:8E:C9:18:50:1
            1.3.6.1.4.1.311.21.1:
                . . .
Revoked Certificates:
    Serial Number: 611B09A10000000002
       Revocation Date: Aug 16 21:52:19 2005 GMT
Serial Number: 4CDE464E00000000003
       Revocation Date: Aug 16 21:52:29 2005 GMT
    Serial Number: 4CFC2B420000000004
       Revocation Date: Aug 16 21:52:41 2005 GMT
    Serial Number: 6C699EC200000000005
        Revocation Date: Aug 16 21:52:52 2005 GMT
    Serial Number: 6CCF7DDC0000000000
       Revocation Date: Jun 8 00:12:04 2005 GMT
    Serial Number: 70CC4FFF00000000007
       Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 4D9B11160000000008
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 52A8023000000000009
        Revocation Date: Jun 27 23:47:06 2005 GMT
        CRL entry extensions:
           X509v3 CRL Reason Code:
           CA Compromise
Serial Number: 5349AD46000000000A
        Revocation Date: Jun 27 23:47:22 2005 GMT
        CRL entry extensions:
           X509v3 CRL Reason Code:
           CA Compromise
Serial Number: 53BD173C000000000B
        Revocation Date: Jul 4 18:04:01 2005 GMT
        CRL entry extensions:
           X509v3 CRL Reason Code:
           Certificate Hold
Serial Number: 591E7ACE0000000000C
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5D3FD52E000000000D
        Revocation Date: Jun 29 22:07:25 2005 GMT
        CRL entry extensions:
           X509v3 CRL Reason Code:
           Key Compromise
Serial Number: 5DAB77130000000000
```

Revocation Date: Jul 14 00:33:56 2005 GMT Serial Number: 5DAE53CD000000000F Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 5DB140D30000000000 Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 5E2D7C1B0000000011 Revocation Date: Jul 6 21:12:10 2005 GMT CRL entry extensions: X509v3 CRL Reason Code: Cessation Of Operation Serial Number: 16DB4F8F00000000012 Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 261C39240000000013 Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 262B52020000000014 Revocation Date: Jul 14 00:33:10 2005 GMT Serial Number: 2634C7F20000000015 Revocation Date: Jul 14 00:32:45 2005 GMT Serial Number: 2635B00000000000016 Revocation Date: Jul 14 00:31:51 2005 GMT Serial Number: 2648504000000000017 Revocation Date: Jul 14 00:32:25 2005 GMT Serial Number: 2A2763570000000018 Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 3F88CBF700000000019 Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 6E4B5F5F000000001A Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 725B89D8000000001B Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 735A88780000000001C Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 148511C70000000001D Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 14A71701000000001E Revocation Date: Aug 16 21:53:15 2005 GMT Serial Number: 14FC45B5000000001F Revocation Date: Aug 17 18:30:42 2005 GMT Serial Number: 486CE80B00000000020 Revocation Date: Aug 17 18:30:43 2005 GMT Serial Number: 4CA4A3AA00000000021 Revocation Date: Aug 17 18:30:43 2005 GMT Serial Number: 1AA55C8E000000002F Revocation Date: Sep 5 17:07:06 2005 GMT Serial Number: 3F0845DD000000003F Revocation Date: Sep 8 20:24:32 2005 GMT Serial Number: 3F619B7E00000000042 Revocation Date: Sep 8 21:40:48 2005 GMT Serial Number: 6313C4630000000052 Revocation Date: Sep 19 17:37:18 2005 GMT Serial Number: 7C3861E300000000000 Revocation Date: Sep 20 17:52:56 2005 GMT Serial Number: 7C6EE35100000000061 Revocation Date: Sep 20 18:52:30 2005 GMT Serial Number: 0A338EA100000000074 <-- Revoked identity certificate Revocation Date: Nov 12 04:34:42 2005 GMT Signature Algorithm: shalWithRSAEncryption Ob:cb:dd:43:0a:b8:62:1e:80:95:06:6f:4d:ab:0c:d8:8e:32: 44:8e:a7:94:97:af:02:b9:a6:9c:14:fd:eb:90:cf:18:c9:96: 29:bb:57:37:d9:1f:d5:bd:4e:9a:4b:18:2b:00:2f:d2:6e:c1: 1a:9f:1a:49:b7:9c:58:24:d7:72

Note

.

取り消されたデバイスのアイデンティティ証明書(シリアル番号は0A338EA100000000074) が最後に表示されています。

PKIに関する追加情報

ここでは、PKIの実装に関する追加情報について説明します。

PKIの関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	Cisco NX-OS ライセンス ガイド
VRF コンフィギュレーショ ン	『 <i>Cisco Nexus 9000</i> シリーズ <i>NX-OS</i> ユニキャスト ルーティング 設定ガイド』

PKIの標準規格

1-----

	タイト ル
この機能でサポートされる新規の標準または変更された標準はありません。また、	—
既存の標準のサポートは変更されていません。	

Resource Public Key Infrastructure (RPKI)

RPKIは、BGP(インターネット)プレフィックスを認証済みの送信元AS番号にマッピングす る情報を含む、グローバルに配布されたデータベースです。BGPパスの送信元 AS を検証する ために、BGP を実行しているルータは、RPKI に接続できます。

RPKI-Cache-to-Router 接続は多対多にすることができ、1つの RPKI キャッシュは複数のルー ターに origin-AS 検証データを提供でき、1 つのルーターは複数の RPKI キャッシュに接続でき ます。ルーターは RPKI キャッシュに接続して情報をダウンロードし、BGP がインターネット ルーティング テーブルの発信元 AS 番号を検証するために使用できる特別な RPKI データベー スを構築します。

RPKI データベースは、BGP が接続するさまざまな RPKI キャッシュから集約された Route-Origin-Attestation (ROA) オブジェクトのセットです。ROA オブジェクトは、BGP プレ フィックスブロックと、そのブロックの発信を許可されたAS番号との間のマッピングを提供 します。

RPKI 構成

RPKI 構成は次のように分類されます。

- RPKI キャッシュに接続するためのコマンド。
- ・受信プレフィックスに RPKI 検証状態をマークするためのコマンド。
- •BGP ベストパス計算で RPKI 検証状態を使用するためのコマンド。
- route-map を使用して特定の検証状態を持つプレフィックスを削除または操作するための コマンド。

RPKI キャッシュに接続するためのコマンド

RPKI キャッシュ構成は、router-bgp サブモードの新しい rpki-cache サブモードで行います。こ れは、デフォルトの VRF での BGP ピアの構成に似ています。サブモードに入るには、「rpki cache <IP address>」コマンドを使用します。サブモードに入ると、RPKI キャッシュのさまざ まなパラメータを構成できます。

```
router bgp 100
 rpki cache 147.28.0.11
   description
                      A description to identify the cache
                      Shutdown the cache
    shutdown
    transport tcp port Transport port on which cache is listening
   vrf
                      Vrf in which RPKI cache is reachable
   refresh-interval
                      Specify periodic wait time between cache poll attempts
   retry-interval
                      Specify wait time before retrying failed serial or reset query
   expiry-interval
                      Specify how long to use current data while unable to perform
successful query
```



(注) トランスポート TCP ポートが明示的に構成されていない限り、BGP は RPKI-RTR ポート 323 で RPKI キャッシュへ接続します。

明示的に設定されていない限り、すべての間隔は、データ PDU の末尾の RPKI キャッシュに よって提案されたとおりに決定されます。

受信プレフィックスを RPKI 検証状態でマークするためのコマンド

RPKI プレフィックス検証処理の動作を制御するためのノブがあります。これらのノブは、ア ドレスファミリレベルで構成できます。

• origin-as validate: アドレスファミリレベルで構成すると、ROA データベースに対する eBGP パス検証が有効になります。デフォルトでは無効になっています。



- (注) このコマンドは、iBGPパスには関係ありません。iBGPパスは、 ROA データベースに対して検証されません。iBGPパスでパス検 証状態をマークする唯一の方法は、BGPプレフィックス発信元検 証状態拡張コミュニティを受信することであり、コマンドを構成 せずにデフォルトで実行されます。
 - origin-as validate signal ibgp: アドレスファミリレベルで構成すると、BGP プレフィックス発信元検証状態拡張コミュニティを介した検証状態の iBGP シグナリングが有効になります。

BGP 最適パス計算で RPKI 検証状態を使用するためのコマンド

RPKI プレフィックス検証処理の動作を制御するためのコマンドがあります。これらのコマンドは、アドレスファミリレベルで構成できます。

- bestpath origin-as use-validity:アドレスファミリレベルで構成することで、BGPベストパス処理でのパスのプリファレンスに影響するBGPパスの有効性状態を有効にします。
 デフォルトでは無効になっています。
- bestpath origin-as allow invalid: アドレスファミリレベルで構成することで、すべての「無効な」パスが BGP 最適パス計算のために考慮されるようにします(best-path origin-as 検証が設定されている場合、そのようなパスはどれも最適パス候補ではありません)。デフォルトでは無効になっています。

route-mapを使用して特定の検証状態を持つプレフィックスを削除また は操作するためのコマンド

以下は、ルートマップを使用して特定の検証状態を持つプレフィックスを削除または操作する ためのコマンドです。

route-map sample1 permit 10
match rpki {not-found | invalid | valid}

match rpki コマンドのパラメータは次のとおりです。

- not-found: この origin-AS は RPKI データベースでは不明です。
- invalid: RPKI データベース内の無効な origin-AS です。

valid: RPKI データベース内の有効な origin-AS です。

この match 句は、インバウンド ルートマップにのみ関連します。

iBGP で学習されたパスの場合、更新の入力 BGP プレフィックス発信元検証状態拡張コミュニ ティが、このルートマップ句と比較されます。 eBGP 学習パスの場合、ROA データベースルックアップによって取得された検証状態が、この ルートマップ句と比較されます。

検証状態が無効であるとマークされたプレフィックスは、BGPでの最適パスの計算に考慮され ないため、無効になりますが、管理者は、システムメモリを節約するために、そのようなプレ フィックスを完全に削除するように決定する場合があります。この目的には、次のインバウン ドルートマップが推奨されます。

route-map sample deny 10 match rpki invalid route-map sample permit 20

RPKI Show コマンド

RPKI 構成情報を表示するには、次のいずれかのタスクを行います。

コマンド	目的
show bgp rpki summary	RPKI キャッシュの数を含む RPKI 統計情報の 概要を表示します。
show bgp rpki table {ipv4 ipv6} {IP address/masklength}	現在の RPKI ROA データベースに関する情報 を表示します。オプションを指定しなかった 場合、コマンドは IPv4 ROA データベースを表 示します。IPv6 オプション(show bgp rpki table ipv6)を指定すると、このコマンドは IPv6 ROA データベースを表示します。(接続の問題な どにより)一時的にダウンしているキャッシュ から受信した ROA は(*)で表示されます。 キャッシュセッションがそのキャッシュのパー ジ時間内に確立されない場合、これらの ROA は RPKI データベースから削除されます。 table show コマンドの後に ROA プレフィック スブロックが指定されている場合(たとえば、 show bgp rpki table 67.21.36.0/24 max 24)、そ の特定の ROA エントリが詳細に表示されます (ROA が存在する場合)。 (注) 1 つの ROA(IP アドレス/最小-最大)は、複 数のオリジン AS を持つことができ、複数の キャッシュからソースを取得できます。

コマンド	目的
show bgp rpki cache {IP address}	構成されているすべてのキャッシュとそのパ ラメータ(show bgp summary など)の要約リ ストを表示します。
	前のコマンドでキャッシュ IP アドレスが指定 されている場合、そのキャッシュの詳細情報 が表示されます。
<pre>show bgp {ipv4 unicast ipv6 unicast} origin-as validity-state {valid invalid unknown}</pre>	BGP ピアに関する情報を表示します。このコ マンドには、パス (validation_state) に基づい てBGP テーブル出力をフィルタリングする新 しいオプションがあります。このコマンドで 有効性状態(有効、無効、または不明)を指 定すると、BGP テーブルから関連情報がフィ ルタリングされ、その有効性状態に一致する BGP パスのみが表示されます。

RPKI Clear コマンド

以下は RPKI Clear コマンドです。

clear bgp rpki cache * - このコマンドは、構成されているすべての RPKI キャッシュのトランスポート セッションをリセットし、すべてのキャッシュから受信したすべての IPv4 および IPv6 ROA の RPKI データベースを即座に消去します。

RPKI Debug および Event History コマンド

以下は、RPKI Debug および Event History コマンドです。

- debug bgp rpki このコマンドは、プレフィックス検証を除くすべての RPKI 関連操作のデバッグをオンにします。これには、RPKI キャッシュ接続、RPKI キャッシュのプロトコルステートマシン、ROAの挿入や削除などの RPKI データベース イベントなどのデバッグイベントが含まれます。
- sh bgp event-history rpki このコマンドは、RPKI に関する高レベルの情報をダンプします。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては 、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている 場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容につい ては米国サイトのドキュメントを参照ください。