

IOSデバイスでのx509認証によるSSHの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[配備上の考慮事項](#)

[設定](#)

[\(オプション\) TACACS サーバーとの統合](#)

[確認](#)

[トラブルシュート](#)

[関連情報](#)

概要

このドキュメントでは、標準規格 RFC6187 に従って、IOS デバイスで x509v3 証明書を使用して SSH サーバーを設定する方法について説明します。

セキュアシェルプロトコル (SSH) は相互認証を提供します。つまり、クライアントとサーバーの両方が認証されます。従来、サーバーは認証に RSA 秘密キー/公開キーペアを使用していました。SSH クライアントは、公開キーのチェックサムを計算し、管理者に信頼できるかどうかを尋ねます。管理者は、アウトオブバンド方式でルータから公開キーをエクスポートし、値を比較する必要があります。実際には、これは面倒な方法であり、公開キーは検証なしで受け入れられることが多く、中間者攻撃の潜在的なリスクにつながります。

標準規格 RFC6187 は、Web ベースの伝送を保護するために一般的に使用される TLS (Transport Layer Security) プロトコルと同様のレベルのセキュリティおよびユーザーエクスペリエンスを提供するため、この問題に対するソリューションとなります。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- PKI インフラストラクチャ

使用するコンポーネント

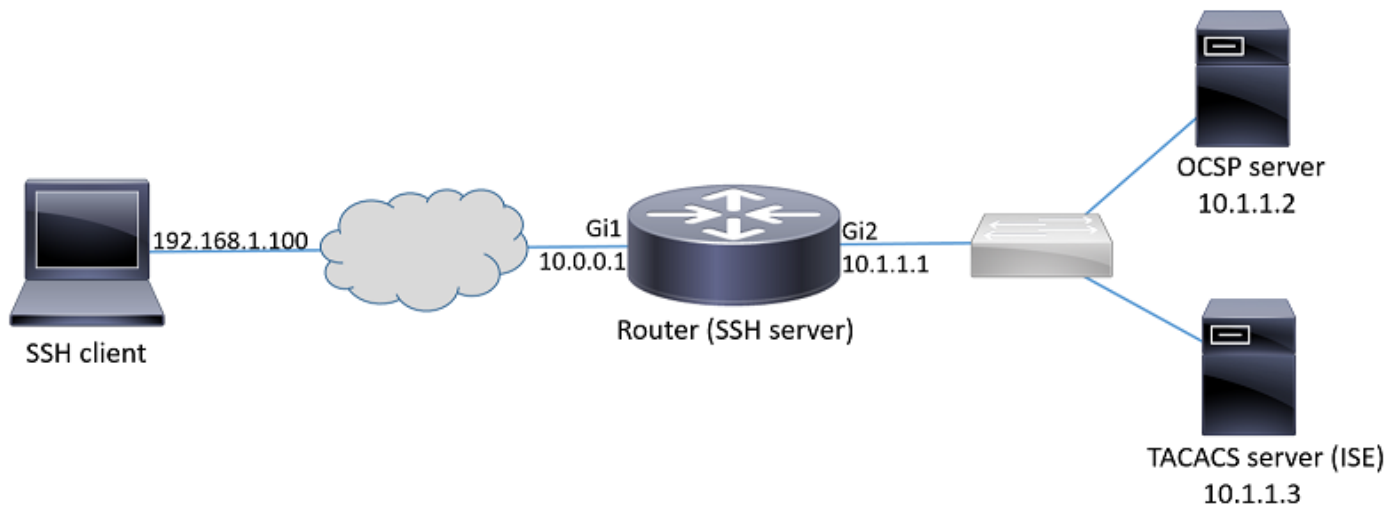
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- IOS-XE バージョン 16.6.1 を実行する CSR 1000v ルータ
- Pragma Fortress SSH クライアント
- Windows Server 2016 OCSP サーバー
- Identity Services Engine バージョン 2.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図



配備上の考慮事項

- 1 つの この機能を利用するには、RFC6187 互換 SSH クライアントが必要です。
- この機能は、IOS バージョン 15.5(2)T および IOS-XE バージョン 15.5(2)S に実装されています。
- SSH クライアントおよびサーバーは、サポートされている認証メカニズムをネゴシエートします。デバイスで以前にサポートされていたすべての認証メカニズムは、スムーズな移行を保証するために、x509 ベース認証メカニズムと同時に実行できます。
- 管理者は、サーバーのみ、クライアントのみ、または両方に対して x509 ベース認証方式を使用できます。
- IOS サーバーは、クライアントから提示された証明書が失効していないかどうかを検証できます。そのために、接続のたびに、失効した証明書のデータベースが参照されます。これにより、証明書の秘密キーが漏洩した場合や特定のユーザーのアクセス権を失効させる必要がある場合に、他のデバイスを再設定することなくアクセス権を失効させることができます。
- 失効チェックはオプションですが、漏洩したログイン情報に基づいてアクセスを拒否する機能を導入することを強くお勧めします。もう一つのオプションは、外部の

TACACS (Terminal Access Controller Access-Control System) または RADIUS サーバーで証明書から取得したユーザー名の認証を実行することです。証明書が漏洩した場合は、外部サーバーでアカウントを無効にして、その証明書を使用したアクセスを防ぐことができます。

- ユーザーの認証は、外部サーバーで実行することも、スキップする (有効な証明書を持つすべてのユーザーがデバイスへのアクセス権を持つと見なされます) こともできます。この例では、簡単にするために前者の方法を使用します。
- 相手側の認証データを正常に検証するために、クライアントとサーバーは、共通の認証局 (CA) を信頼するだけで済みます。つまり、ルータ証明書に署名した CA の証明書を、クライアントデバイスの信頼できる証明書ストアにインストールするだけで済みます。
- 証明書は、相手側のアイデンティティに関する情報を提供します (一般に、共通名とサブジェクト代替名がこの目的に使用されます)。クライアントは、管理者によって入力として提供されたサーバーのホスト名または IP アドレス名を、提示された証明書で使用可能なアイデンティティデータと比較する必要があります。これにより、中間者攻撃やその他のなりすまし攻撃の可能性が大幅に制限されます。

設定

AAA パラメータを設定します。基本的なシナリオ (外部認可サーバーなし) では、証明書から取得したユーザー名の許可はスキップできます。

```
aaa new-model
aaa authorization network CERT none
```

CA 証明書とルータ証明書 (オプション) を保持するトラストポイントを設定します。

```
crypto pki trustpoint SSH
enrollment mode ra
enrollment url http://10.1.1.2:80/CertSrv/mscep/mscep.dll
serial-number
ip-address 10.0.0.1
subject-name cn=10.0.0.1
revocation-check ocsp
ocsp url http://10.1.1.2/ocsp
rsa-keypair SSH 2048
authorization list CERT
! The username has to be fetched from the certificate for accounting and authorization purposes.
Multiple options are available.
authorization username subjectname commonname
```

ヒント : OCSP サーバーに到達できない場合、管理者は、**revocation-check ocsp** 設定を使用してすべてのアクセスを拒否するか **revocation-check ocsp none** を使用して失効チェックなしでアクセスを許可する (非推奨) かを選択できます。

SSH トンネルネゴシエーション中に使用される、許可された認証メカニズムを設定します。

```
! Algorithms used to authenticate server
```

```
ip ssh server algorithm hostkey x509v3-ssh-rsa ssh-rsa

! Acceptable algorithms used to authenticate the client
ip ssh server algorithm authentication publickey password keyboard

! Acceptable pubkey-based algorithms used to authenticate the client
ip ssh server algorithm publickey x509v3-ssh-rsa ssh-rsa
```

認証プロセスで正しい証明書を使用するように SSH サーバーを設定します。

```
ip ssh server certificate profile
! Certificate used by server
server
trustpoint sign SSH

! CA used to authenticate client certificates
user
trustpoint verify SSH
```

(オプション) TACACS サーバーとの統合

ユーザー名が証明書から取得されると、IOS は、TACACS サーバーに対してそのユーザー名の許可を実行できます。これは、TACACS サーバーがデバイス管理用にすでに展開されている場合に特に役立ちます。

注：IOS SSH サーバーは、現時点では、認証方式チェーンをサポートしていません。これは、証明書を使用してユーザーを認証する場合に、TACACS サーバーをパスワード認証に使用できないことを意味します。このサーバーは、許可にのみ使用できます。

TACACS サーバーを設定します。

```
tacacs server ISE
address ipv4 10.1.1.3
key cisco123
```

TACACS サーバーを使用するように許可リストを設定します。

```
aaa authorization network ISE group tacacs+
```

1. ISE (Identity Services Engine) を設定します。設定例については、次の資料を参照してください。

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200208-Configure-ISE-2-0-IOS-TACACS-Authentic.html>

2. TACACS プロファイルを設定します。許可を成功させるには、[ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [TACACSプロファイル (TACACS Profiles)] > [追加 (Add)] に移動して、追加パラメータの **cert-application=all** を設定する必要があります。

Common Tasks

Common Task Type

<input checked="" type="checkbox"/> Default Privilege	<input type="text" value="15"/>	(Select 0 to 15)
<input checked="" type="checkbox"/> Maximum Privilege	<input type="text" value="15"/>	(Select 0 to 15)
<input type="checkbox"/> Access Control List	<input type="text"/>	
<input type="checkbox"/> Auto Command	<input type="text"/>	
<input type="checkbox"/> No Escape	<input type="text"/>	(Select true or false)
<input type="checkbox"/> Timeout	<input type="text"/>	Minutes (0-9999)
<input type="checkbox"/> Idle Time	<input type="text"/>	Minutes (0-9999)

Custom Attributes

[+ Add](#) [Trash](#) [Edit](#)

<input type="checkbox"/>	Type	Name	Value
<input type="checkbox"/>	MANDATORY	cert-application	all

3. ポリシーセットを設定するには、[ワークセンター (Work Centers)] > [デバイス管理 (Device Administration)] > [デバイス管理ポリシーセット (Device Admin Policy Sets)] > [追加 (Add)] に移動します。

▼ Authentication Policy

<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols : Default Device Admin	and use : All_User_ID_Stores
-------------------------------------	----------------------------	--	------------------------------

▼ Authorization Policy

▼ Exceptions (1)

Local Exceptions

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	Certificate auth	if network admins	then Select Profile(s)	permit_lvl_15

確認

```
show ip ssh
SSH Enabled - version 1.99
```

```
Authentication methods:publickey,password,keyboard-interactive
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
--- output truncated ----
```

```
show users
```

```
Line User Host(s) Idle Location
1 vty 0 admin1 idle 00:02:37 192.168.1.100
```

トラブルシューティング

次のデバッグは、成功したセッションを追跡するために使用されています。

```
debug ip ssh detail
debug crypto pki transactions
debug crypto pki messages
debug crypto pki validation
```

```
Aug 21 20:07:08.717: SSH0: starting SSH control process
! Server identifies itself
Aug 21 20:07:08.717: SSH0: sent protocol version id SSH-1.99-Cisco-1.25
! Client identifies itself
Aug 21 20:07:08.771: SSH0: protocol version id is - SSH-2.0-Pragma FortressCL 5.0.10.766
Aug 21 20:07:08.771: SSH2 0: kexinit sent: kex algo = diffie-hellman-group-exchange-sha1,diffie-
hellman-group14-sha1
```

```
! Authentication algorithms supported by server
Aug 21 20:07:08.771: SSH2 0: kexinit sent: hostkey algo = x509v3-ssh-rsa,ssh-rsa
Aug 21 20:07:08.772: SSH2 0: kexinit sent: encryption algo = aes128-ctr,aes192-ctr,aes256-ctr
Aug 21 20:07:08.772: SSH2 0: kexinit sent: mac algo = hmac-sha2-256,hmac-sha2-512,hmac-
sha1,hmac-sha1-96
Aug 21 20:07:08.772: SSH2 0: SSH2_MSG_KEXINIT sent
Aug 21 20:07:08.915: SSH2 0: SSH2_MSG_KEXINIT received
Aug 21 20:07:08.916: SSH2 0: kex: client->server enc:aes256-ctr mac:hmac-sha1
Aug 21 20:07:08.916: SSH2 0: kex: server->client enc:aes256-ctr mac:hmac-sha1
```

```
! Client chooses authentication algorithm
Aug 21 20:07:08.916: SSH2 0: Using hostkey algo = x509v3-ssh-rsa
Aug 21 20:07:08.916: SSH2 0: Using kex_algo = diffie-hellman-group-exchange-sha1
Aug 21 20:07:08.917: SSH2 0: Modulus size established : 4096 bits
Aug 21 20:07:08.976: SSH2 0: expecting SSH2_MSG_KEX_DH_GEX_INIT
Aug 21 20:07:09.141: SSH2 0: SSH2_MSG_KEXDH_INIT received
```

```
! Server sends certificate associated with trustpoint "SSH"
Aug 21 20:07:09.208: SSH2 0: Sending Server certificate associated with PKI trustpoint "SSH"
Aug 21 20:07:09.208: CRYPTO_PKI: (A003C) Session started - identity selected (SSH)
Aug 21 20:07:09.208: SSH2 0: Got 2 certificate(s) on certificate chain
Aug 21 20:07:09.208: CRYPTO_PKI: Rcvd request to end PKI session A003C.
Aug 21 20:07:09.208: CRYPTO_PKI: PKI session A003C has ended. Freeing all resources.
Aug 21 20:07:09.209: CRYPTO_PKI: unlocked trustpoint SSH, refcount is 0
Aug 21 20:07:09.276: SSH2: kex_derive_keys complete
Aug 21 20:07:09.276: SSH2 0: SSH2_MSG_NEWKEYS sent
Aug 21 20:07:09.276: SSH2 0: waiting for SSH2_MSG_NEWKEYS
Aug 21 20:07:16.927: SSH2 0: SSH2_MSG_NEWKEYS received
Aug 21 20:07:17.177: SSH2 0: Authentications that can continue = publickey,password,keyboard-
interactive
Aug 21 20:07:17.225: SSH2 0: Using method = none
Aug 21 20:07:17.226: SSH2 0: Authentications that can continue = publickey,password,keyboard-
interactive
Aug 21 20:07:32.305: SSH2 0: Using method = publickey
```

```
! Client sends certificate
Aug 21 20:07:32.305: SSH2 0: Received publickey algo = x509v3-ssh-rsa
Aug 21 20:07:32.305: SSH2 0: Verifying certificate for user 'admin1' in
SSH2_MSG_USERAUTH_REQUEST
Aug 21 20:07:32.305: SSH2 0: Verifying certificate for user 'admin1'
Aug 21 20:07:32.306: SSH2 0: Received a chain of 2 certificate
Aug 21 20:07:32.308: SSH2 0: Received 0 ocsdp-response
Aug 21 20:07:32.308: SSH2 0: Starting PKI session for certificate verification
Aug 21 20:07:32.308: CRYPTO_PKI: (A003D) Session started - identity not specified
Aug 21 20:07:32.309: CRYPTO_PKI: (A003D) Adding peer certificate
Aug 21 20:07:32.310: CRYPTO_PKI: found UPN as admin1@example.com
Aug 21 20:07:32.310: CRYPTO_PKI: Added x509 peer certificate - (1016) bytes
Aug 21 20:07:32.310: CRYPTO_PKI: (A003D) Adding peer certificate
Aug 21 20:07:32.310: CRYPTO_PKI: Added x509 peer certificate - (879) bytes
Aug 21 20:07:32.311: CRYPTO_PKI: ip-ext-val: IP extension validation not required
Aug 21 20:07:32.311: CRYPTO_PKI: create new ca_req_context type PKI_VERIFY_CHAIN_CONTEXT,ident
31
Aug 21 20:07:32.312: CRYPTO_PKI: (A003D)validation path has 1 certs

Aug 21 20:07:32.312: CRYPTO_PKI: (A003D) Check for identical certs
Aug 21 20:07:32.312: CRYPTO_PKI : (A003D) Validating non-trusted cert
Aug 21 20:07:32.312: CRYPTO_PKI: (A003D) Create a list of suitable trustpoints
Aug 21 20:07:32.312: CRYPTO_PKI: Found a issuer match
Aug 21 20:07:32.312: CRYPTO_PKI: (A003D) Suitable trustpoints are: SSH,
Aug 21 20:07:32.313: CRYPTO_PKI: (A003D) Attempting to validate certificate using SSH policy
Aug 21 20:07:32.313: CRYPTO_PKI: (A003D) Using SSH to validate certificate
Aug 21 20:07:32.313: CRYPTO_PKI: Added 1 certs to trusted chain.
Aug 21 20:07:32.314: CRYPTO_PKI: Prepare session revocation service providers
Aug 21 20:07:32.314: CRYPTO_PKI: Deleting cached key having key id 30
Aug 21 20:07:32.314: CRYPTO_PKI: Attempting to insert the peer's public key into cache
Aug 21 20:07:32.314: CRYPTO_PKI:Peer's public inserted successfully with key id 31
Aug 21 20:07:32.315: CRYPTO_PKI: Expiring peer's cached key with key id 31
Aug 21 20:07:32.315: CRYPTO_PKI: (A003D) Certificate is verified

! Revocation status is checked
Aug 21 20:07:32.315: CRYPTO_PKI: (A003D) Checking certificate revocation
Aug 21 20:07:32.315: OCSP: (A003D) Process OCSP_VALIDATE message
Aug 21 20:07:32.315: CRYPTO_PKI: (A003D)Starting OCSP revocation check
Aug 21 20:07:32.316: CRYPTO_PKI: OCSP server URL is http://10.1.1.2/ocsp
Aug 21 20:07:32.316: CRYPTO_PKI: no responder matching this URL; create one!
Aug 21 20:07:32.316: OCSP: (A003D)OCSP Get Response command
Aug 21 20:07:32.317: CRYPTO_PKI: http connection opened
Aug 21 20:07:32.317: CRYPTO_PKI: OCSP send header size 132
Aug 21 20:07:32.317: CRYPTO_PKI: sending POST /ocsp HTTP/1.0
Host: 10.1.1.2
User-Agent: RSA-Cert-C/2.0
Content-type: application/ocsp-request
Content-length: 312

Aug 21 20:07:32.317: CRYPTO_PKI: OCSP send data size 312
Aug 21 20:07:32.322: OCSP: (A003D)OCSP Parse HTTP Response command
Aug 21 20:07:32.322: OCSP: (A003D)OCSP Validate DER Response command
Aug 21 20:07:32.322: CRYPTO_PKI: OCSP response status - successful.
Aug 21 20:07:32.323: CRYPTO_PKI: Decoding OCSP Response
Aug 21 20:07:32.323: CRYPTO_PKI: OCSP decoded status is GOOD.
Aug 21 20:07:32.323: CRYPTO_PKI: Verifying OCSP Response
Aug 21 20:07:32.325: CRYPTO_PKI: Added 11 certs to trusted chain.
Aug 21 20:07:32.325: ../VIEW_ROOT/cisco.comp/pki_ssl/src/ca/provider/revoke/ocsp/ocsputil.c(547)
: E_NOT_FOUND : no matching entry found
Aug 21 20:07:32.325: ../VIEW_ROOT/cisco.comp/pki_ssl/src/ca/provider/revoke/ocsp/ocsputil.c(547)
: E_NOT_FOUND : no matching entry found
Aug 21 20:07:32.326: CRYPTO_PKI: (A003D) Validating OCSP responder certificate
Aug 21 20:07:32.327: CRYPTO_PKI: OCSP Responder cert doesn't need rev check
```

Aug 21 20:07:32.328: CRYPTO_PKI: response signed by a delegated responder
Aug 21 20:07:32.328: CRYPTO_PKI: OCSP Response is verified
Aug 21 20:07:32.328: CRYPTO_PKI: (A003D) OCSP revocation check is complete 0
Aug 21 20:07:32.328: OCSP: destroying OCSP trans element
Aug 21 20:07:32.328: CRYPTO_PKI: Revocation check is complete, 0
Aug 21 20:07:32.328: CRYPTO_PKI: Revocation status = 0
Aug 21 20:07:32.328: CRYPTO_PKI: Remove session revocation service providers
Aug 21 20:07:32.329: CRYPTO_PKI: Remove session revocation service providers
Aug 21 20:07:32.329: CRYPTO_PKI: (A003D) Certificate validated
Aug 21 20:07:32.329: CRYPTO_PKI: Populate AAA auth data
Aug 21 20:07:32.329: CRYPTO_PKI: Selected AAA username: 'admin1'
Aug 21 20:07:32.329: CRYPTO_PKI: Anticipate checking AAA list: 'CERT'
Aug 21 20:07:32.329: CRYPTO_PKI: Checking AAA authorization
Aug 21 20:07:32.329: CRYPTO_PKI_AAA: checking AAA authorization (CERT, admin1, <all>)
Aug 21 20:07:32.329: CRYPTO_PKI_AAA: pre-authorization chain validation status (0x400)
Aug 21 20:07:32.329: CRYPTO_PKI_AAA: post-authorization chain validation status (0x400)
Aug 21 20:07:32.329: CRYPTO_PKI: (A003D)chain cert was anchored to trustpoint SSH, and chain validation result was: CRYPTO_VALID_CERT
Aug 21 20:07:32.329: CRYPTO_PKI: destroying ca_req_context type PKI_VERIFY_CHAIN_CONTEXT,ident 31, ref count 1
Aug 21 20:07:32.330: CRYPTO_PKI: ca_req_context released
Aug 21 20:07:32.330: CRYPTO_PKI: (A003D) Validation TP is SSH
Aug 21 20:07:32.330: CRYPTO_PKI: (A003D) Certificate validation succeeded
Aug 21 20:07:32.330: CRYPTO_PKI: Rcvd request to end PKI session A003D.
Aug 21 20:07:32.330: CRYPTO_PKI: PKI session A003D has ended. Freeing all resources.
Aug 21 20:07:32.395: SSH2 0: Verifying certificate for user 'admin1'
Aug 21 20:07:32.395: SSH2 0: Received a chain of 2 certificate
Aug 21 20:07:32.396: SSH2 0: Received 0 ocsf-response
Aug 21 20:07:32.396: SSH2 0: Starting PKI session for certificate verification
Aug 21 20:07:32.396: CRYPTO_PKI: (A003E) Session started - identity not specified
Aug 21 20:07:32.396: CRYPTO_PKI: (A003E) Adding peer certificate
Aug 21 20:07:32.397: CRYPTO_PKI: found UPN as admin1@example.com
Aug 21 20:07:32.397: CRYPTO_PKI: Added x509 peer certificate - (1016) bytes
Aug 21 20:07:32.397: CRYPTO_PKI: (A003E) Adding peer certificate
Aug 21 20:07:32.398: CRYPTO_PKI: Added x509 peer certificate - (879) bytes
Aug 21 20:07:32.398: CRYPTO_PKI: ip-ext-val: IP extension validation not required
Aug 21 20:07:32.400: CRYPTO_PKI: create new ca_req_context type PKI_VERIFY_CHAIN_CONTEXT,ident 32
Aug 21 20:07:32.400: CRYPTO_PKI: (A003E)validation path has 1 certs

Aug 21 20:07:32.400: CRYPTO_PKI: (A003E) Check for identical certs
Aug 21 20:07:32.400: CRYPTO_PKI : (A003E) Validating non-trusted cert
Aug 21 20:07:32.401: CRYPTO_PKI: (A003E) Create a list of suitable trustpoints
Aug 21 20:07:32.401: CRYPTO_PKI: Found a issuer match
Aug 21 20:07:32.401: CRYPTO_PKI: (A003E) Suitable trustpoints are: SSH,
Aug 21 20:07:32.401: CRYPTO_PKI: (A003E) Attempting to validate certificate using SSH policy
Aug 21 20:07:32.401: CRYPTO_PKI: (A003E) Using SSH to validate certificate
Aug 21 20:07:32.402: CRYPTO_PKI: Added 1 certs to trusted chain.
Aug 21 20:07:32.402: CRYPTO_PKI: Prepare session revocation service providers
Aug 21 20:07:32.402: CRYPTO_PKI: Deleting cached key having key id 31
Aug 21 20:07:32.403: CRYPTO_PKI: Attempting to insert the peer's public key into cache
Aug 21 20:07:32.403: CRYPTO_PKI:Peer's public inserted successfully with key id 32
Aug 21 20:07:32.404: CRYPTO_PKI: Expiring peer's cached key with key id 32
Aug 21 20:07:32.404: CRYPTO_PKI: (A003E) Certificate is verified
Aug 21 20:07:32.404: CRYPTO_PKI: (A003E) Checking certificate revocation
Aug 21 20:07:32.404: OCSP: (A003E) Process OCSP_VALIDATE message
Aug 21 20:07:32.404: CRYPTO_PKI: (A003E)Starting OCSP revocation check
Aug 21 20:07:32.405: CRYPTO_PKI: OCSP server URL is http://10.1.1.2/ocsp
Aug 21 20:07:32.405: CRYPTO_PKI: no responder matching this URL; create one!
Aug 21 20:07:32.405: OCSP: (A003E)OCSP Get Response command
Aug 21 20:07:32.406: CRYPTO_PKI: http connection opened
Aug 21 20:07:32.406: CRYPTO_PKI: OCSP send header size 132
Aug 21 20:07:32.406: CRYPTO_PKI: sending POST /ocsp HTTP/1.0
Host: 10.1.1.2

User-Agent: RSA-Cert-C/2.0
Content-type: application/ocsp-request
Content-length: 312

Aug 21 20:07:32.406: CRYPTO_PKI: OCSP send data size 312
Aug 21 20:07:32.409: OCSP: (A003E)OCSP Parse HTTP Response command
Aug 21 20:07:32.410: OCSP: (A003E)OCSP Validate DER Response command
Aug 21 20:07:32.410: CRYPTO_PKI: OCSP response status - successful.
Aug 21 20:07:32.410: CRYPTO_PKI: Decoding OCSP Response
Aug 21 20:07:32.411: CRYPTO_PKI: OCSP decoded status is GOOD.
Aug 21 20:07:32.411: CRYPTO_PKI: Verifying OCSP Response
Aug 21 20:07:32.413: CRYPTO_PKI: Added 11 certs to trusted chain.
Aug 21 20:07:32.413: ../VIEW_ROOT/cisco.comp/pki_ssl/src/ca/provider/revoke/ocsp/ocsputil.c(547)
: E_NOT_FOUND : no matching entry found
Aug 21 20:07:32.413: ../VIEW_ROOT/cisco.comp/pki_ssl/src/ca/provider/revoke/ocsp/ocsputil.c(547)
: E_NOT_FOUND : no matching entry found
Aug 21 20:07:32.414: CRYPTO_PKI: (A003E) Validating OCSP responder certificate
Aug 21 20:07:32.415: CRYPTO_PKI: OCSP Responder cert doesn't need rev check
Aug 21 20:07:32.415: CRYPTO_PKI: response signed by a delegated responder
Aug 21 20:07:32.416: CRYPTO_PKI: OCSP Response is verified
Aug 21 20:07:32.416: CRYPTO_PKI: (A003E) OCSP revocation check is complete 0
Aug 21 20:07:32.416: OCSP: destroying OCSP trans element
Aug 21 20:07:32.416: CRYPTO_PKI: Revocation check is complete, 0
Aug 21 20:07:32.416: CRYPTO_PKI: Revocation status = 0
Aug 21 20:07:32.416: CRYPTO_PKI: Remove session revocation service providers
Aug 21 20:07:32.416: CRYPTO_PKI: Remove session revocation service providers
Aug 21 20:07:32.416: CRYPTO_PKI: (A003E) Certificate validated
Aug 21 20:07:32.417: CRYPTO_PKI: Populate AAA auth data
Aug 21 20:07:32.417: CRYPTO_PKI: Selected AAA username: 'admin1'
Aug 21 20:07:32.417: CRYPTO_PKI: Anticipate checking AAA list: 'CERT'
Aug 21 20:07:32.417: CRYPTO_PKI: Checking AAA authorization
Aug 21 20:07:32.417: CRYPTO_PKI_AAA: checking AAA authorization (CERT, admin1, <all>)
Aug 21 20:07:32.417: CRYPTO_PKI_AAA: pre-authorization chain validation status (0x400)
Aug 21 20:07:32.417: CRYPTO_PKI_AAA: post-authorization chain validation status (0x400)
Aug 21 20:07:32.417: CRYPTO_PKI: (A003E)chain cert was anchored to trustpoint SSH, and chain
validation result was: CRYPTO_VALID_CERT
Aug 21 20:07:32.417: CRYPTO_PKI: destroying ca_req_context type PKI_VERIFY_CHAIN_CONTEXT,ident
32, ref count 1
Aug 21 20:07:32.417: CRYPTO_PKI: ca_req_context released
Aug 21 20:07:32.417: CRYPTO_PKI: (A003E) Validation TP is SSH
Aug 21 20:07:32.417: CRYPTO_PKI: (A003E) Certificate validation succeeded
Aug 21 20:07:32.418: CRYPTO_PKI: Rcvd request to end PKI session A003E.
Aug 21 20:07:32.418: CRYPTO_PKI: PKI session A003E has ended. Freeing all resources.
Aug 21 20:07:32.418: SSH2 0: Verifying signature for user 'admin1' in SSH2_MSG_USERAUTH_REQUEST
Aug 21 20:07:32.418: SSH2 0: Received a chain of 2 certificate
Aug 21 20:07:32.418: SSH2 0: Received 0 ocsp-response
Aug 21 20:07:32.418: CRYPTO_PKI: found UPN as admin1@example.com

! Certificate status verified successfully
Aug 21 20:07:32.419: SSH2 0: Client Signature verification PASSED
Aug 21 20:07:32.419: SSH2 0: Certificate authentication passed for user 'admin1'
Aug 21 20:07:32.419: SSH2 0: authentication successful for admin1
Aug 21 20:07:32.470: SSH2 0: channel open request
Aug 21 20:07:32.521: SSH2 0: pty-req request
Aug 21 20:07:32.521: SSH2 0: setting TTY - requested: height 25, width 80; set: height 25, width
80
Aug 21 20:07:32.570: SSH2 0: shell request
Aug 21 20:07:32.570: SSH2 0: shell message received
Aug 21 20:07:32.570: SSH2 0: starting shell for vty
Aug 21 20:07:32.631: SSH2 0: channel window adjust message received 8

admin1 の証明書が失効している場合 :

```
Aug 21 19:39:52.081: CRYPTO_PKI: OCSP Response is verified
Aug 21 19:39:52.081: CRYPTO_PKI: (A0024) OCSP revocation check is complete 0
Aug 21 19:39:52.082: OCSP: destroying OCSP trans element
Aug 21 19:39:52.082: CRYPTO_PKI: Revocation check is complete, 0
Aug 21 19:39:52.082: CRYPTO_PKI: Revocation status = 1
Aug 21 19:39:52.082: CRYPTO_PKI: Remove session revocation service providers
Aug 21 19:39:52.082: CRYPTO_PKI: Remove session revocation service providers
Aug 21 19:39:52.082: CRYPTO_PKI: (A0024) Certificate revoked
Aug 21 19:39:52.082: %PKI-3-CERTIFICATE_REVOKED: Certificate chain validation has failed. The
certificate (SN: 750000001B78DA4CC0078DEC0700000000001B) is revoked
Aug 21 19:39:52.082: CRYPTO_PKI: (A0024)chain cert was anchored to trustpoint Unknown, and chain
validation result was: CRYPTO_CERT_REVOKED
Aug 21 19:39:52.082: CRYPTO_PKI: destroying ca_req_context type PKI_VERIFY_CHAIN_CONTEXT,ident
18, ref count 1
Aug 21 19:39:52.082: CRYPTO_PKI: ca_req_context released
Aug 21 19:39:52.083: CRYPTO_PKI: (A0024) Certificate validation failed
```

関連情報

- PKI 設定ガイド :

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mt-book.html

- ISE での TACACS の設定例 :

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200208-Configure-ISE-2-0-IOI-TACACS-Authentic.html>

- [テクニカル サポートとドキュメント – Cisco Systems](#)