

Configurando o SSH com autenticação x509 em dispositivos de IOS

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Considerações de desenvolvimento](#)

[Configurações](#)

[Integração \(opcional\) com servidor de TACACS](#)

[Verificar](#)

[Troubleshooting](#)

[Informação relacionada](#)

Introdução

Este documento descreve como configurar o servidor de SSH com uso dos Certificados x509v3 em dispositivos de IOS de acordo com o RFC6187 padrão.

O protocolo secure shell (SSH) fornece a autenticação mútua, isto é ambo cliente e servidor é autenticado. Tradicionalmente, o server usa o keypair privado e público RSA para a autenticação. O cliente SSH computa a soma de verificação da chave pública e pergunta ao administrador se se confia. O administrador deve exportar a chave pública do roteador com uso do método out-of-band e comparar os valores. Na prática, este é um método incômodo e a chave pública é aceita frequentemente sem verificação, que conduz ao risco potencial de ataques que envolva pessoas.

O padrão do RFC6187 é uma solução a este interesse porque fornece a experiência similar do nível de segurança e do usuário ao protocolo TLS (Transport Layer Security) de uso geral para proteger transmissões com base na Web.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Infraestrutura PKI

[Componentes Utilizados](#)

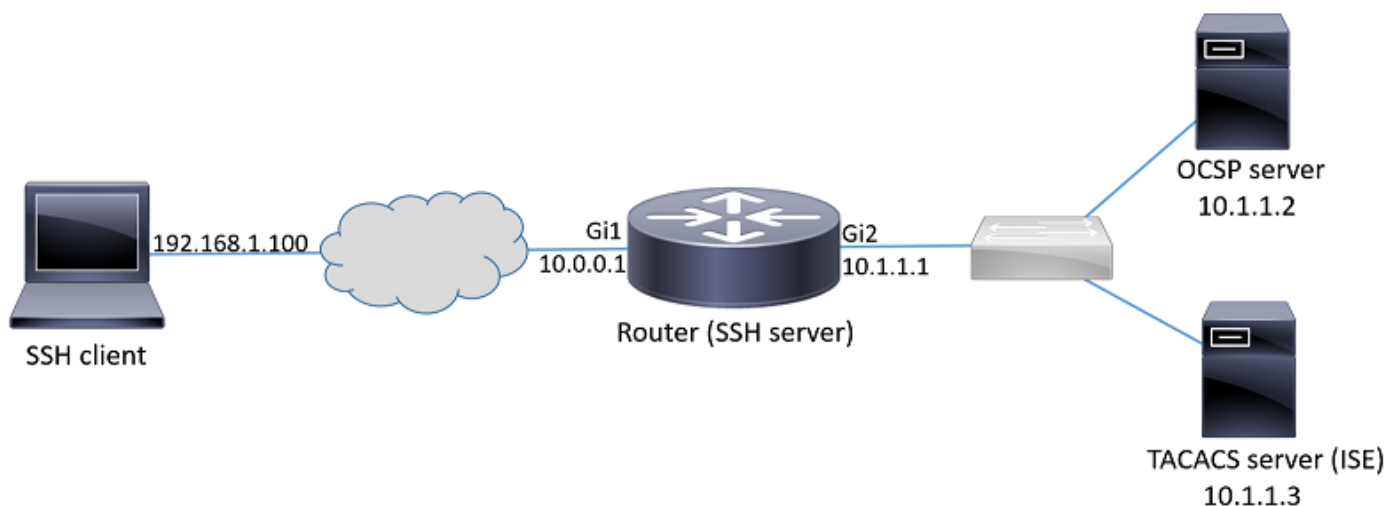
As informações neste documento são baseadas nestas versões de software e hardware:

- 1000v Router CSR que executa a versão 16.6.1 IOS-XE
- Cliente SSH da fortaleza do Pragma
- Server de Windows Server 2016 OCSP
- Versão 2.1 do Identity Services Engine

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Configurar

Diagrama de Rede



Considerações de desenvolvimento

- Um cliente SSH RFC6187-compatible é necessário para aproveitar-se da característica.
- A característica foi executada na Versão do IOS 15.5(2)T e na versão 15.5(2)S IOS-XE.
- O cliente SSH e o server negociam mecanismos da autenticação apoiados. Todos os mecanismos do authentication apoiados previamente no dispositivo podem continuar a ser executado simultaneamente com mecanismos da autenticação x509-based a fim assegurar a transição fácil.
- O administrador pode escolher usar o método de autenticação x509-based para o server somente, o cliente somente ou ambos.
- O servidor de IOS pode verificar se o certificado apresentado pelo cliente não é revogado. A fim fazer isso, o base de dados de Certificados revogados é consultado em cima de cada conexão. Isto permite a revogação do acesso sem a necessidade de reconfigurar outros dispositivos, caso que, se a chave privada do certificado é comprometida ou se o acesso para um usuário específico precisa de ser revogado.

- A verificação da revogação é opcional, mas é altamente recomendado ter a possibilidade para negar o acesso baseado em credenciais comprometidas. Uma outra opção é a executar a autorização para o username buscado do certificado no Terminal Access Controller Access Control System externo (TACACS) ou no servidor Radius. Caso que o certificado é comprometido, a conta pode ser desabilitada no servidor interno para impedir o acesso com uso desse certificado.
- A autorização dos usuários pode ser executada pelo servidor interno ou pode ser saltada (todos os usuários com um certificado válido suposto para ter privilégios ao dispositivo de acesso). O método anterior é usado neste exemplo para simplificar.
- A fim verificar com sucesso os dados de autenticação do outro partido, a necessidade do cliente e servidor somente de confiar um Certificate Authority (CA) comum. Isto significa que somente o certificado de CA que assinou o certificado de roteador precisa de ser instalado na loja do certificado confiável do dispositivo do cliente.
- O certificado fornece a informação sobre a identidade do outro partido (o Common Name e o nome alternativo sujeito são usados tipicamente para essa finalidade). O cliente deve comparar o hostname ou o nome do endereço IP de Um ou Mais Servidores Cisco ICM NT do server que foi fornecido como a entrada pelo administrador com os dados da identidade disponíveis no certificado apresentado. Limita severamente os oportnities de ataques homem-em--médios ou outros da personificação.

Configurações

Configurar parâmetros AAA. Em um cenário básico (sem servidor de autorização externo), a autorização para o username buscado do certificado pode ser saltada.

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

Configurar um ponto confiável que guarde o certificado de CA e opcionalmente o certificado de roteador.

```
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 oosp
oosp url http://10.1.1.2/oosp
rsaakeypair 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
```

Tip: Caso que o server OOSP é inacessível, o administrador pode escolher recusar todo o acesso usando a configuração do **oosp da revogação-verificação** ou permitir o acesso sem

verificação da revogação usando o **ocsp da revogação-verificação nenhuns** (não recomendado).

Configure permitiu os mecanismos da autenticação usados durante a negociação do túnel SSH.

```
! Alorithms 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
```

Configurar o servidor de SSH para usar Certificados corretos no processo de autenticação.

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

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

Integração (opcional) com servidor de TACACS

Depois que o username é buscado do certificado, os IO podem executar a autorização para esse servidor de TACACS do aginst username. Isto é especialmente útil se o servidor de TACACS é distribuído já para a administração do dispositivo.

Note: O servidor IOS SSH atualmente não apoia o encadeamento do método de autenticação. Isto significa que se os Certificados são usados para autenticar o usuário, o servidor de TACACS não pode ser usado para a autenticação de senha. Pode somente ser usado para a autorização.

Configurar o servidor de TACACS.

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

Configurar a lista da autorização para usar o servidor de TACACS.

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

1. Configurar ISE (Identity Services Engine). O exemplo de configuração pode ser encontrado em:

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

2. Configurar o perfil TACACS. O **cert-application=all** adicional do parâmetro precisa de ser configurado para que a autorização suceda, navega aos **elementos dos centros de trabalho > da administração > da política do dispositivo > aos resultados > ao > Add dos perfis TACACS**.

Common Tasks

Common Task Type

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

Custom Attributes

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

3. A fim configurar a política para ajustar-se, navegue aos **centros de trabalho > ao > Add dos grupos da política Admin da administração do dispositivo > do dispositivo**.

▼ **Authentication Policy**

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 <i>Select Profile(s)</i>	permit_lvl_15

Verificar

```
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
```

Troubleshooting

Estes debugam são usados para seguir a sessão bem-sucedida:

```
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 oosp-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

Caso que o certificado para o admin1 foi revogado:

```
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
```

Informação relacionada

- **Manual de configuração PKI:**
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mt-book.html
- **TACACS no exemplo de configuração ISE:**
<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200208-Configure-ISE-2-0-IOI-TACACS-Authentic.html>
- [Suporte Técnico e Documentação - Cisco Systems](#)