配置与x509验证的SSH在IOS设备

目录

简介

本文描述如何配置有使用的SSH服务器x509v3在IOS设备的证书符合标准的RFC6187。
安全套接协议(SSH)提供相互验证，即两客户端和服务器验证。传统上，服务器使用RSA私有和公共密钥对验证。如果它是委托， SSH客户端计算公共密钥校验和并且要求管理员。管理员应该导出从路由器的公共密钥有使用的带外方法和比较值。实际上，这是一个笨重方法，并且公共密钥经常接受，不用验证，导致中间人攻击潜伏风险。
RFC6187标准是解决方案对此注意事项作为它提供相似的安全级别和用户体验给常用TLS (传输层安全)的协议保护基于Web的发射。

先决条件

要求

Cisco 建议您了解以下主题：

- PKI基础设施

使用的组件

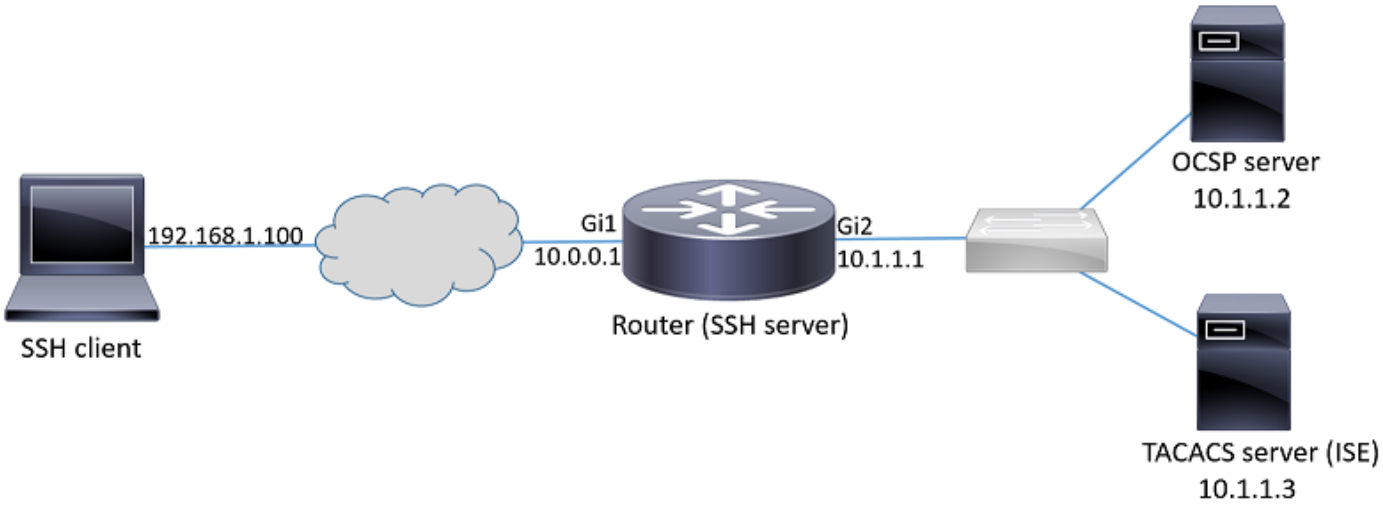
本文档中的信息基于以下软件和硬件版本：

- 运行IOS-XE版本16.6.1的CSR 1000v路由器
- 附注堡垒SSH客户端
- Windows服务器2016 OCSP服务器
- 身份服务引擎版本2.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络实际，请保证您了解所有命令潜在影响。

配置

网络图



部署注意事项

- RFC6187-compatible SSH客户端是必要利用功能。
- 功能在IOS版本15.5(2)T和IOS-XE版本15.5(2)S实现。
- SSH客户端和服务器协商支持的认证机制。以前支持所有authenitcation机制设备可能继续在x509-based认证机制的同时运行为了保证顺利过渡。
- 管理员可能选择使用x509-based认证方法仅服务器，客户端或只有两个。
- 如果客户端提交的证书没有取消， IOS服务器能验证。为了执行那，取消的证书数据库参见在每连接。这允许访问的撤销，不用需要重新配置其它设备，万一，如果证书的专用密钥减弱或，如果特定的访问用户需要取消。
- 撤销检查可选，但是高度推荐的有拒绝的可能性根据折衷的凭证的访问。另一个选项是对执行从在外部终端访问控制器访问控制系统(TACACS)或RADIUS服务器的证书拿来的用户名的授权。万一证书折衷，帐户在外部服务器可以禁用防止与使用的访问该证书。
- 用户的授权可以由外部服务器执行或可以被跳过(有假设的有效证书的所有用户有权限到接入设备)。前面的方法用于为了简化此的示例。
- 为了顺利地验证另一个当事人的身份验证数据，仅客户端和服务器需要委托一普通的Certificate Authority (CA)。这意味着签署路由器证书CA仅的证书在客户端设备信任证书存储需要安装。
- 证书提供关于另一个当事人的标识的信息(公用名称和主题替代方案名称典型地使用该目的)。客户端应该比较带有作为输入由管理员在提交证书的标识数据联机服务器的主机名或IP地址名称

。它严重地限制man-in-the-middle或其他模拟攻击opportnities。

配置

配置AAA参数。在基本情形中(没有外部授权服务器)，从证书拿来的用户名的授权可以被跳过。

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

配置有CA证书和或者路由器证书的信任点。

```
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
rsakeypair 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
```

> **提示**：万一OCSP服务器是不可得到的，管理员可能选择禁止所有访问通过使用撤销**检查ocsp**配置或允许，不用撤销检查使用撤销**检查ocsp无**(不建议使用)。

configure允许在SSH隧道协商时使用的认证机制。

```
! 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
```

配置SSH服务器使用正确证书在认证过程。

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

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

(可选)集成用TACACS服务器

在用户名从证书后被拿来， IOS可执行该用户名aginst TACACS服务器的授权。如果TACACS服务

器为设备管理，已经部署这是特别有用的。

> **Note**:IOS SSH服务器当前不支持认证方法连锁。这意味着，如果证书用于验证用户，TACACS服务器不可能用于密码验证。它可能只用于授权。

配置TACACS服务器。

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

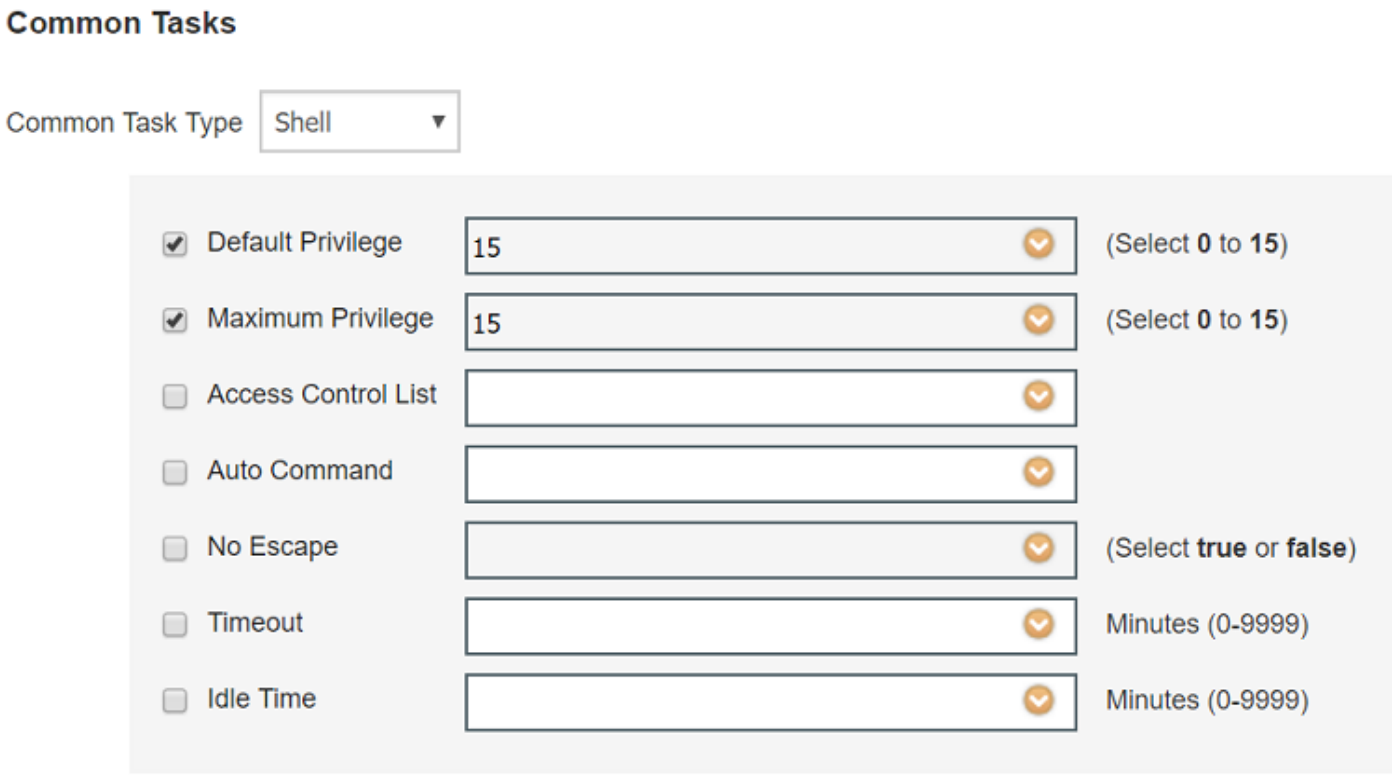
配置authorization list使用TACACS服务器。

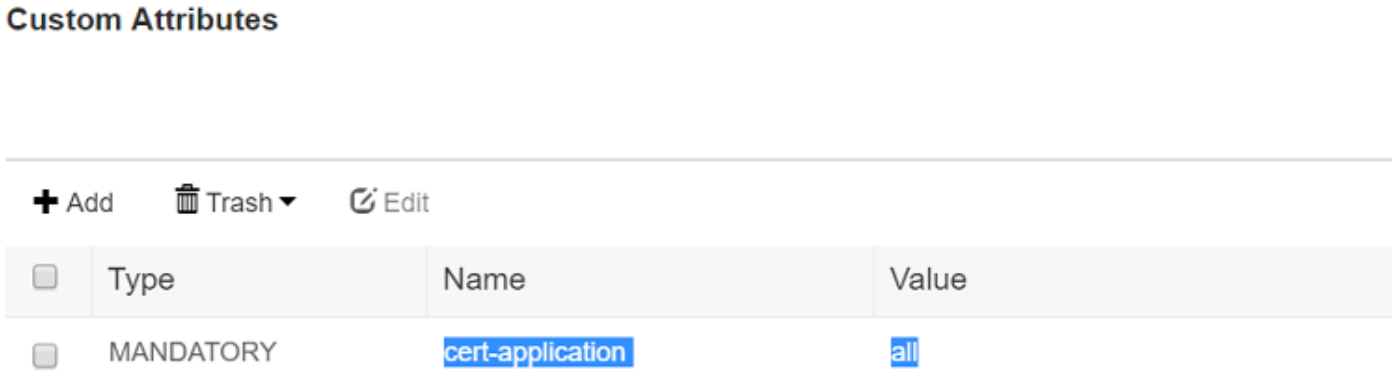
```
aaa authorization network ISE group tacacs+
```

1. 配置ISE (身份服务引擎)。配置示例可以找到在：

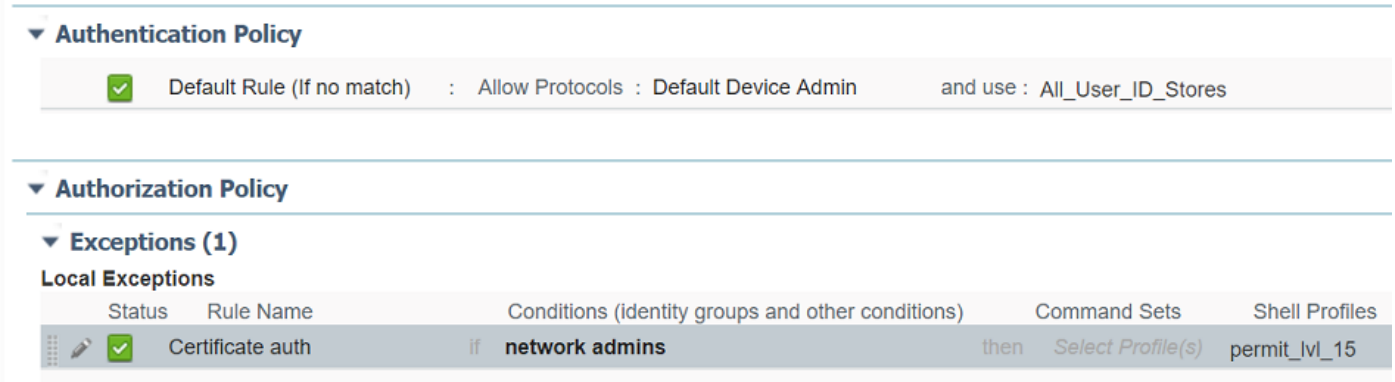
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200208-Configure-ISE-2-0-IOS-TACACS-Authentic.html

2. 配置TACACS配置文件。其它参数**cert-application=all**需要配置为了授权能成功，导航对**工作区>设备管理>Policy元素>结果> TACACS配置文件>Add**。





3. 为了配置策略集，请导航对**工作区>设备Administration >设备Admin策略集>Add。**



验证

```
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

故障排除

这些调试用于跟踪成功的会话：

```
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 ocsp-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 ocsp-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
```

万一admin1的证书取消：

```
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
```

相关信息

- **PKI配置指南：**
  https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mt-book.html
- **在ISE配置示例的TACACS ：**
  https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200208-Configure-ISE-2-0-IOS-TACACS-Authentic.html

- 技术支持和文档 - Cisco Systems