在 IOS 裝置上設定 SSH 的 x509 驗證

目錄

簡介

本文檔介紹如何根據標準RFC6187在IOS裝置上使用x509v3證書配置SSH伺服器。
安全殼層通訊協定(SSH)提供相互驗證，即使用者端和伺服器都進行驗證。傳統上，伺服器使用RSA專用金鑰對和公用金鑰對進行身份驗證。SSH客戶端會計算公鑰的校驗和，並詢問管理員是否信任它。管理員應使用帶外方法從路由器匯出公鑰並比較其值。在實踐中，這種方法比較麻煩，並且公鑰通常在沒有驗證的情況下被接受，這會導致潛在的中介人攻擊風險。
RFC6187標準是解決此問題的一個解決方案，因為它提供的安全性和使用者體驗與通常用於保護基於Web的傳輸的TLS（傳輸層安全）協定類似。

必要條件

需求

思科建議您瞭解以下主題：

- PKI基礎設施

採用元件

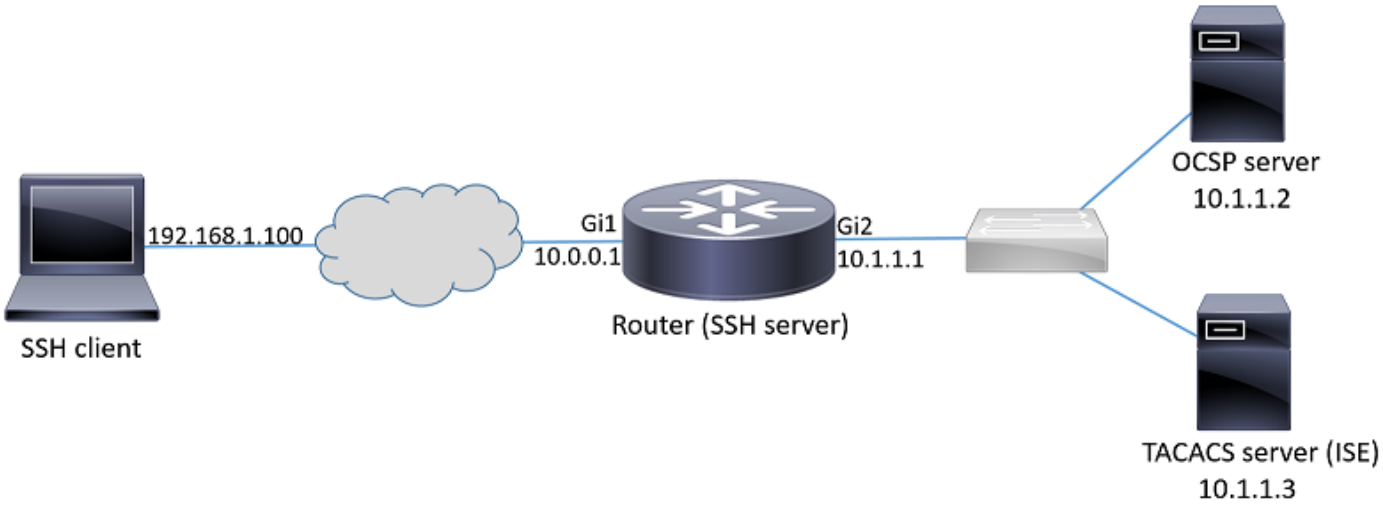
本文中的資訊係根據以下軟體和硬體版本：

- 運行IOS-XE 16.6.1版的CSR 1000v路由器
- 雜訊堡壘SSH使用者端
- Windows Server 2016 OCSP伺服器
- 身分識別服務引擎版本2.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

網路圖表



部署注意事項

- 安 必須使用RFC6187相容的SSH客戶端才能利用此功能。
- 此功能已在IOS版本15.5(2)T和IOS-XE版本15.5(2)S中實施。
- SSH客戶端和伺服器協商支援的身份驗證機制。以前裝置上支援的所有身份驗證機制可以繼續與基於x509的身份驗證機制同時運行，以確保平穩過渡。
- 管理員可以選擇將基於x509的身份驗證方法僅用於伺服器、僅用於客戶端或同時用於兩者。
- IOS伺服器可以驗證客戶端提供的證書是否未被吊銷。為此，會在每個連線上查閱已撤銷證書的資料庫。這樣可撤銷訪問，而無需重新配置其他裝置，以防證書的私鑰受損或需要撤銷特定使用者的訪問。
- 吊銷檢查是可選的，但強烈建議可以根據受損的憑據拒絕訪問。另一種方法是在外部終端存取控制器存取控制系統(TACACS)或RADIUS伺服器上，執行從憑證擷取的使用者名稱的授權。如果證書受到危害，可以在外部伺服器上禁用該帳戶，以防止使用該證書進行訪問。
- 使用者授權可由外部伺服器執行，也可以跳過（假定具有有效證書的所有使用者都具有訪問裝置的許可權）。 為了簡單起見，本示例使用了前一種方法。
- 為了成功驗證另一方的驗證資料，使用者端和伺服器只需信任一個通用憑證授權單位(CA)。 這意味著只有簽署路由器證書的CA證書才需要在客戶端裝置受信任證書儲存區安裝。
- 證書提供有關另一方的身份資訊（通常使用常用名稱和主體替代名稱）。 客戶端應將管理員輸入時提供的伺服器的主機名或IP地址名稱與所提供的證書中可用的身份資料進行比較。它嚴重

限制了中間人攻擊或其他模擬攻擊的機會。

組態

配置AAA引數。在基本情況下（沒有外部授權伺服器），可以跳過對從證書獲取的使用者名稱的授權。

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

配置儲存CA證書和路由器證書（可選）的信任點。

```
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：如果OCSP伺服器無法訪問，管理員可以選擇使用**revocation-check ocsp**配置禁止所有訪問，或使用**revocation-check ocsp none**（不推薦）允許未經撤銷檢查的訪問。

配置SSH隧道協商期間使用的允許身份驗證機制。

```
! 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伺服器以在身份驗證過程中使用正確的證書。

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

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

（可選）與TACACS伺服器整合

從憑證中擷取使用者名稱后，IOS可以針對TACACS伺服器對該使用者名稱執行授權。如果已部署TACACS伺服器用於裝置管理，則此功能尤其有用。

> **附註**：IOS SSH伺服器當前不支援身份驗證方法連結。這表示如果憑證用於驗證使用者，則TACACS伺服器無法用於密碼驗證。它只能用於授權。

配置TACACS伺服器。

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

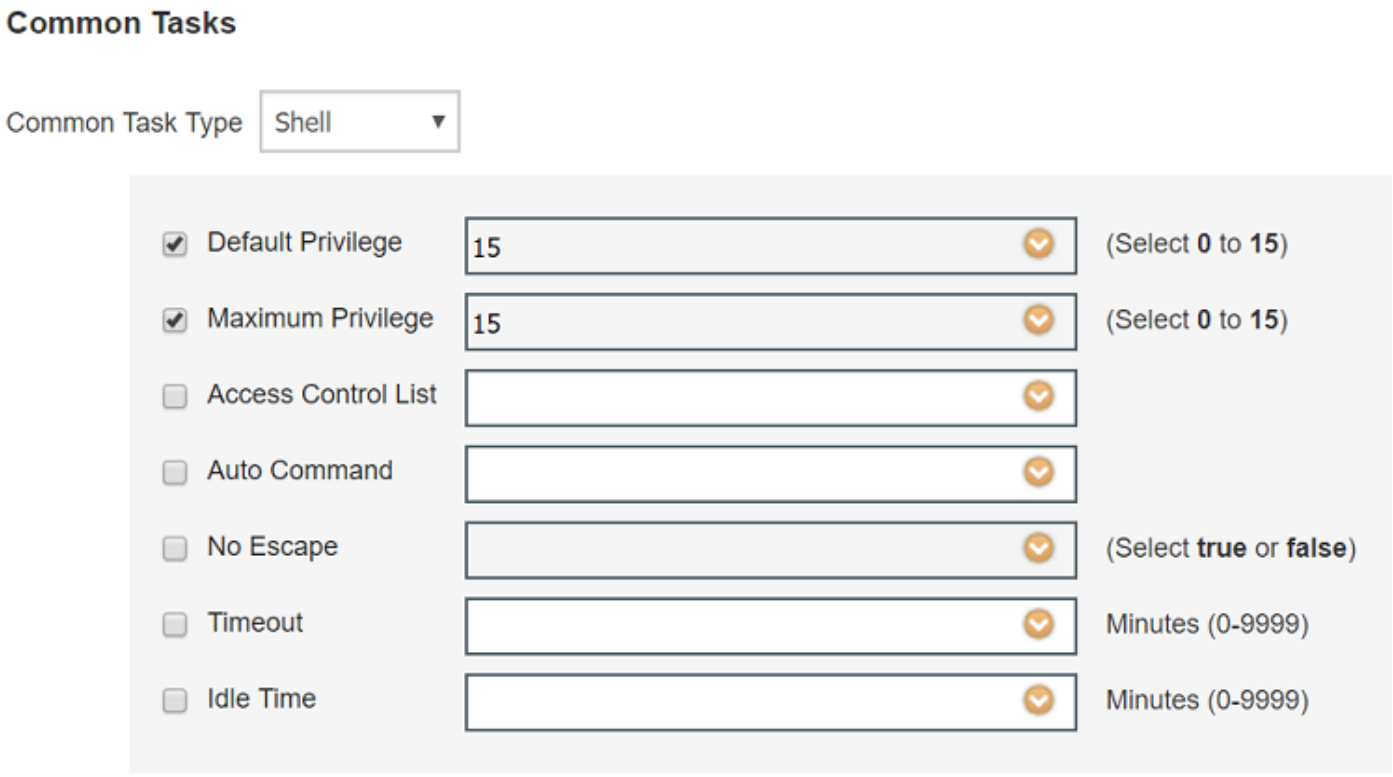
配置授權清單以使用TACACS伺服器。

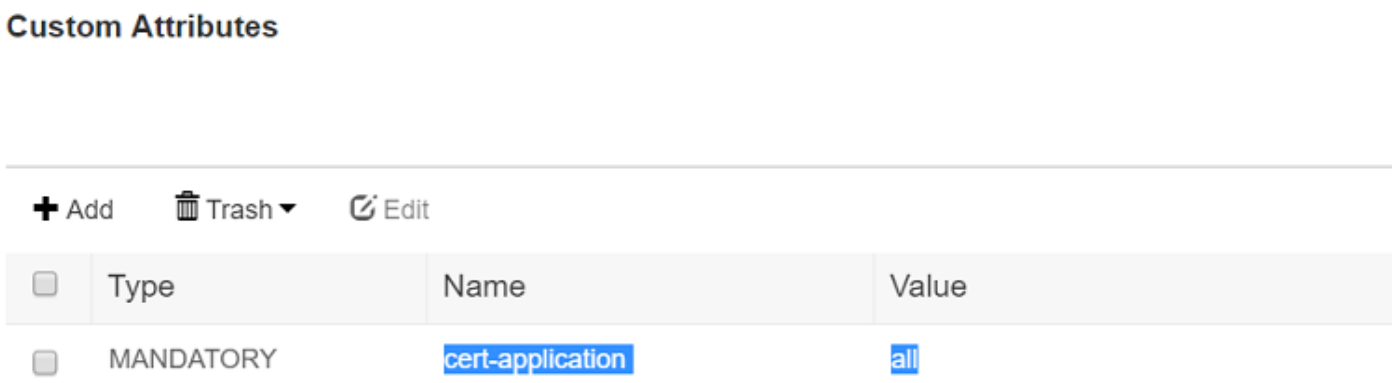
```
aaa authorization network ISE group tacacs+
```

1.配置ISE（身份服務引擎）。 配置示例位於：

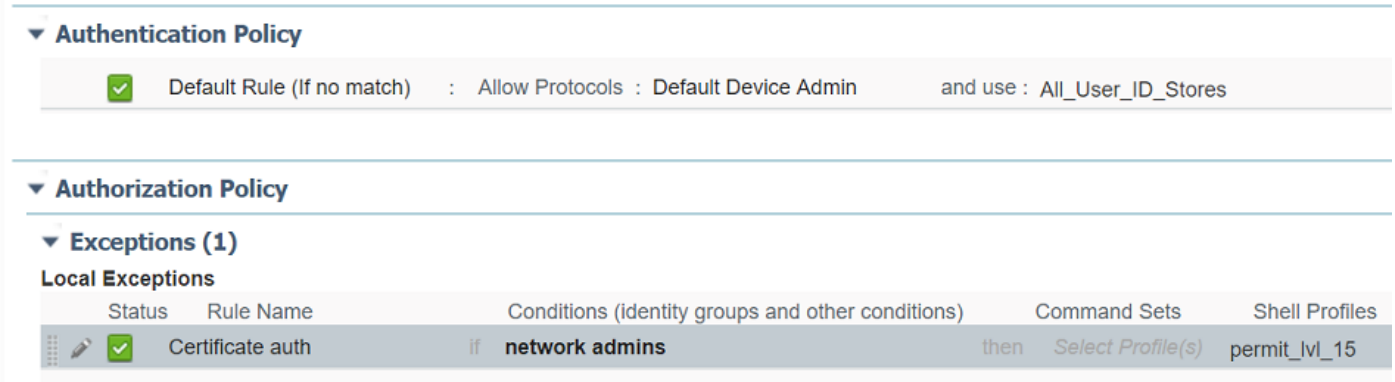
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200208-Configure-ISE-2-0-IOS-TACACS-Authentic.html

2.配置TACACS配置檔案。需要配置其他引數 **cert-application=all**才能成功完成授權，請導航到 **Work Centers > Device Administration > Policy Elements > Results > TACACS profiles > Add**。





3.要配置策略集，請導航至**工作中心>裝置管理>裝置管理策略集>新增**。



驗證

```
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
```

疑難排解

以下調試用於跟蹤成功的會話：

```
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
```

如果admin1的證書被吊銷：

```
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
```

相關資訊

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

- **技術支援與文件 - Cisco Systems**