

在Cisco IOS XE裝置上為SSH配置證書身份驗證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[部署注意事項](#)

[組態](#)

[IOS-XE裝置 \(SSH伺服器 \)](#)

[Pragma Fortress CL \(安裝在使用者機器上的SSH客戶端 \)](#)

[驗證](#)

[疑難排解](#)

[常見問題](#)

[組態錯誤](#)

[相關資訊](#)

簡介

本檔案概述了根據RFC 6187中定義的准則，在Cisco IOS® XE裝置上使用X.509v3證書進行身份驗證的安全外殼(SSH)配置。

必要條件

需求

思科建議您瞭解公開金鑰基礎架構(PKI)基礎架構。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行Cisco IOS XE 17.3.5版的C9200L交換器
- 雜訊堡壘SSH使用者端

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

背景資訊

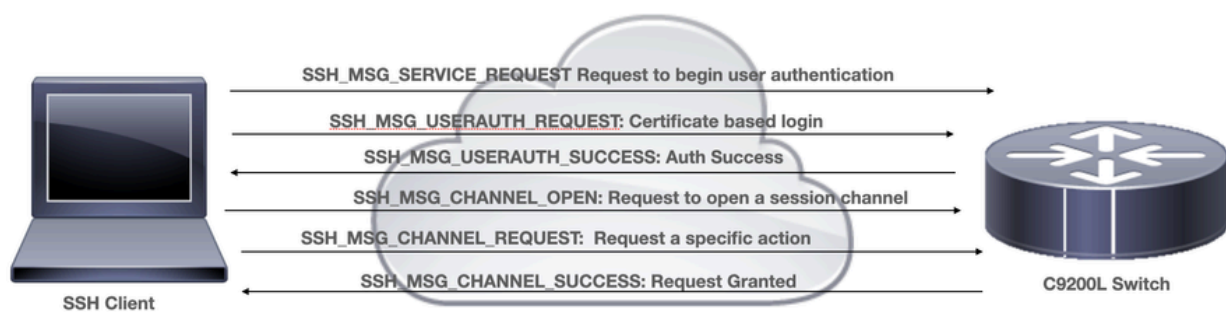
該方法通過啟用基於證書的身份驗證，增強了SSH安全性，從而使SSH金鑰管理實踐與傳輸層安全(TLS)中使用的那些實踐更緊密地保持一致。

SSH提供相互身份驗證，以便在客戶端和伺服器之間建立安全連線。傳統上，伺服器使用Rivest-Shamir-Addleman(RSA)金鑰對進行身份驗證。客戶端計算伺服器的公鑰的指紋，並提示管理員對其進行驗證——理想的做法是將其與通過安全的帶外方法獲得的已知值進行比較。但是，由於其複雜性，這種手動驗證經常被跳過，增加了中間人(MitM)攻擊的風險並削弱了SSH信任模型。

RFC 6187通過啟用X.509v3基於證書的身份驗證（將SSH與PKI整合）來解決這些問題。此方法通過允許通過可信證書頒發機構(CA)建立信任，提供類似於TLS的使用者體驗和信任模型，從而提高安全性和可擴充性。

設定

網路圖表



部署注意事項

- 要利用此功能，需要與RFC6187相容的SSH客戶端。
- 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。
- 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的CA。這意味著只有簽署路由器證書的CA證書才必須安裝在客戶端裝置受信任證書庫上。
- 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）。客戶端必須將作為管理員輸入而提供的伺服器的主機名或IP地址名稱與所提供的證書中的可用身份資料進行比較。它嚴重限制了MitM或其他模擬攻擊的機會。

組態

IOS-XE裝置（SSH伺服器）

配置儲存CA證書和路由器證書 (可選) 的信任點。

```
crypto pki trustpoint pki-server
```

```
enrollment pkcs12
```

```
subject-name cn=RTR-DC01.cisco.com
```

```
revocation-check none
```

```
rsakeypair ssh-cert
```

! The username has to be fetched from the certificate for accounting and authorization purposes. Multip

```
authorization username subjectname commonname
```

配置在SSH隧道協商期間使用的允許身份驗證機制。

```
! 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
```

配置SSH伺服器，以便在身份驗證過程中使用正確的證書。

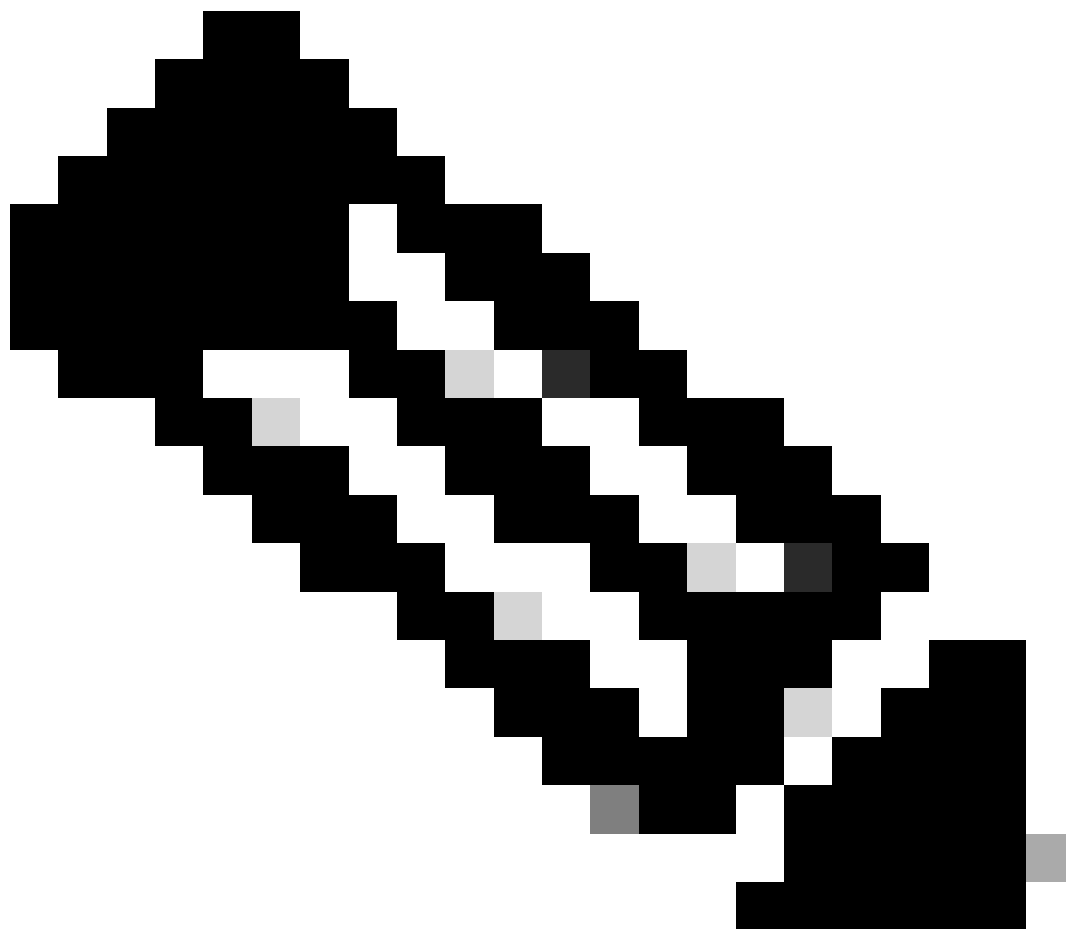
```
ip ssh server certificate profile
```

```
server
```

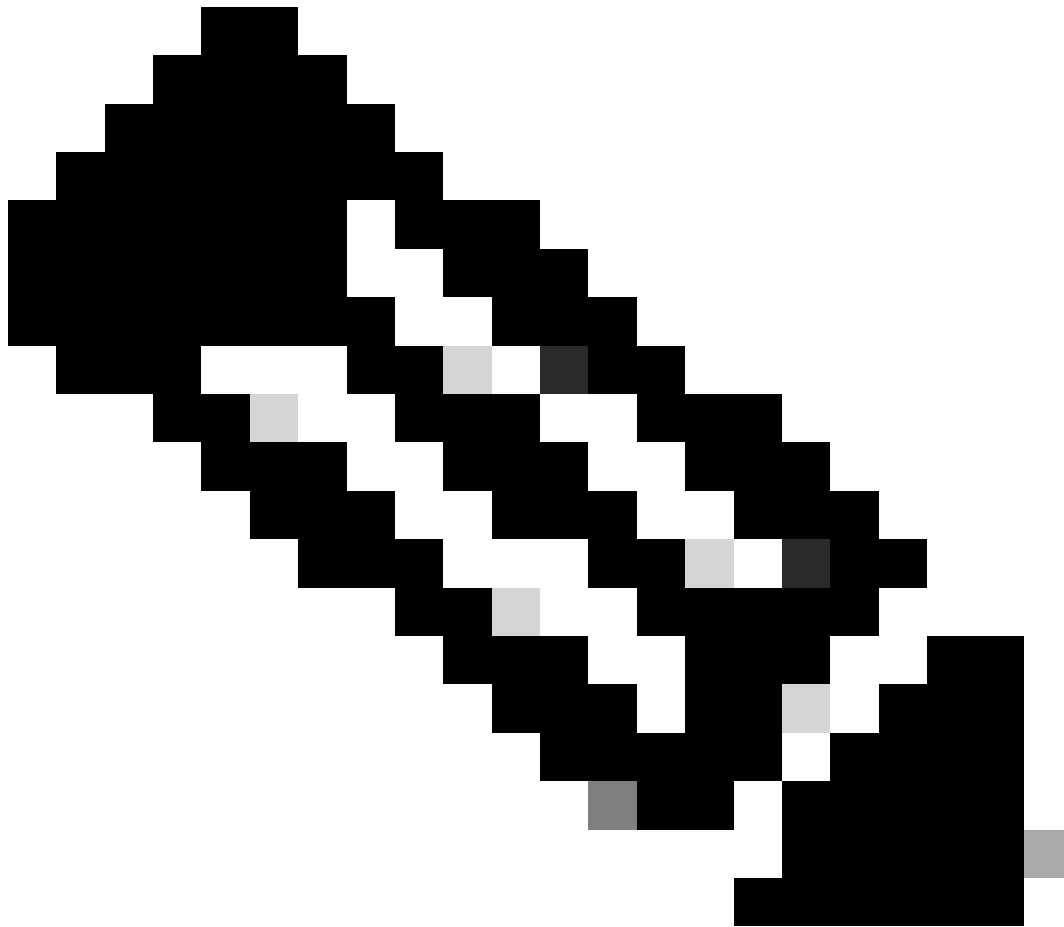
```
trustpoint sign
```

```
user
```

```
trustpoint verify
```



附註：確保SSH伺服器 and SSH客戶端具有由同一CA伺服器頒發的ID證書。



附註：如果SSH客戶端（如Windows電腦）具有由其他某個CA頒發的ID證書，則將其匯入到SSH伺服器（即Cisco交換機）上，並將該Trustpoint對映到使用者部分下的SSH伺服器證書配置檔案之上。

Pragma Fortress CL（安裝在使用者機器上的SSH客戶端）

RTR-DC01.cisco.com

Authentication

Logging

Keyboard

Proxy

Serial

Telnet

Terminal

+ Ssh

+ Window

RTR-DC01.cisco.com

Site name:

RTR-DC01.cisco.com

Host address:

RTR-DC01.cisco.com

Host Alias:

Protocol:

ssh2

Port:

22

Comment:

Host address is the Hostname of the Cisco Device mentioned in the ID certificate issued to it by the CA server

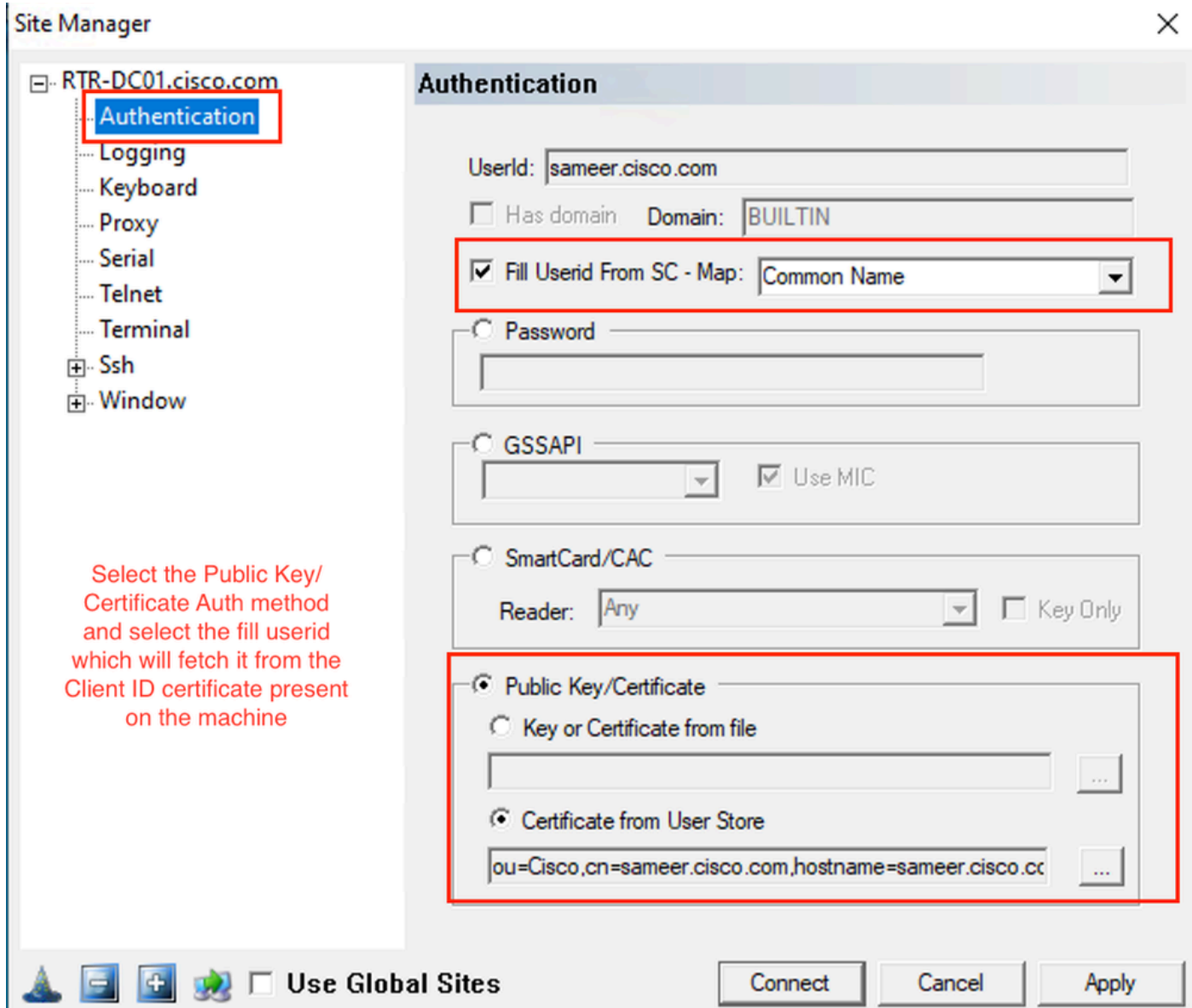


Use Global Sites

Connect

Cancel

Apply



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 sameer.cisco.com 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

Mar 27 15:35:40.103: SSH1: starting SSH control process

! Server identifies itself

Mar 27 15:35:40.103: SSH1: sent protocol version id SSH-1.99-Cisco-1.25

! Client identifies itself

Mar 27 15:35:40.106: SSH1: protocol version id is - SSH-2.0-Pragma FortressCL 5.0.10.4176

! Authentication algorithms supported by server

Mar 27 15:35:40.106: SSH2 1: kexinit sent: kex algo = diffie-hellman-group-exchange-sha1,diffie-hellman

Mar 27 15:35:40.106: SSH2 1: kexinit sent: hostkey algo = x509v3-ssh-rsa,ssh-rsa

Mar 27 15:35:40.106: SSH2 1: kexinit sent: encryption algo = aes128-ctr,aes192-ctr,aes256-ctr

Mar 27 15:35:40.106: SSH2 1: kexinit sent: mac algo = hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-96

Mar 27 15:35:40.106: SSH2 1: SSH2_MSG_KEXINIT sent

Mar 27 15:35:40.109: SSH2 1: SSH2_MSG_KEXINIT received

Mar 27 15:35:40.109: SSH2 1: kex: client->server enc:aes256-ctr mac:hmac-sha2-256

Mar 27 15:35:40.109: SSH2 1: kex: server->client enc:aes256-ctr mac:hmac-sha2-256

! Client chooses authentication algorithm

Mar 27 15:35:40.109: SSH2 1: Using hostkey algo = x509v3-ssh-rsa

Mar 27 15:35:40.109: SSH2 1: Using kex_algo = diffie-hellman-group-exchange-sha1

Mar 27 15:35:40.109: SSH2 1: SSH2_MSG_KEX_DH_GEX_REQUEST received

Mar 27 15:35:40.109: SSH2 1: Range sent by client is - 1024 < 2048 < 8192

Mar 27 15:35:40.109: SSH2 1: Modulus size established : 2048 bits

Mar 27 15:35:40.121: SSH2 1: expecting SSH2_MSG_KEX_DH_GEX_INIT

Mar 27 15:35:40.121: SSH2 1: SSH2_MSG_KEXDH_INIT received

! SSH Server sends certificate associated with trustpoint "pki-server"

Mar 27 15:35:40.133: SSH2 1: Sending Server certificate associated with PKI trustpoint "pki-server"

Mar 27 15:35:40.133: SSH2 1: Got 2 certificate(s) on certificate chain

Mar 27 15:35:40.135: SSH2: kex_derive_keys complete

Mar 27 15:35:40.135: SSH2 1: SSH2_MSG_NEWKEYS sent

Mar 27 15:35:40.135: SSH2 1: waiting for SSH2_MSG_NEWKEYS

Mar 27 15:35:40.214: SSH2 0: channel window adjust message received 49926

Mar 27 15:35:41.417: SSH2 1: SSH2_MSG_NEWKEYS received

Mar 27 15:35:41.436: SSH2 1: Authentications that can continue = publickey,password,keyboard-interactive

Mar 27 15:35:41.437: SSH2 1: Using method = none

Mar 27 15:35:41.437: SSH2 1: Authentications that can continue = publickey,password,keyboard-interactive

Mar 27 15:35:41.438: SSH2 1: Using method = publickey

! Client sends certificate

Mar 27 15:35:41.438: SSH2 1: Received publickey algo = x509v3-ssh-rsa

Mar 27 15:35:41.438: SSH2 1: Verifying certificate for user 'sameer.cisco.com' in SSH2_MSG_USERAUTH_REQUEST

Mar 27 15:35:41.439: SSH2 1: Verifying certificate for user 'sameer.cisco.com'

Mar 27 15:35:41.439: SSH2 1: Received a chain of 2 certificate

Mar 27 15:35:41.439: SSH2 1: Received 0 ocsp-response

Mar 27 15:35:41.439: SSH2 1: Starting PKI session for certificate verification

! Client certificate is verified by the SSH-Server

Mar 27 15:35:41.444: SSH2 1: Verifying certificate for user 'sameer.cisco.com'

Mar 27 15:35:41.444: SSH2 1: Received a chain of 2 certificate

Mar 27 15:35:41.444: SSH2 1: Received 0 ocsp-response

Mar 27 15:35:41.444: SSH2 1: Starting PKI session for certificate verification

Mar 27 15:35:41.445: SSH2 1: Verifying signature for user 'sameer.cisco.com' in SSH2_MSG_USERAUTH_REQUEST

Mar 27 15:35:41.445: SSH2 1: Received a chain of 2 certificate

Mar 27 15:35:41.445: SSH2 1: Received 0 ocsp-response

! Certificate status verified successfully


```
Mar 27 15:35:41.446: SSH2 1: Client Signature verification PASSED
Mar 27 15:35:41.446: SSH2 1: Certificate authentication passed for user 'sameer.cisco.com'
Mar 27 15:35:41.446: SSH2 1: authentication successful for sameer.cisco.com
Mar 27 15:35:41.448: SSH2 1: channel open request
Mar 27 15:35:41.451: SSH2 1: pty-req request
Mar 27 15:35:41.451: SSH2 1: setting TTY - requested: height 25, width 80; set: height 25, width 80
Mar 27 15:35:41.452: SSH2 1: shell request
Mar 27 15:35:41.452: SSH2 1: shell message received
Mar 27 15:35:41.452: SSH2 1: starting shell for vty
Mar 27 15:35:41.464: SSH2 1: channel window adjust message received 9
Aug 21 20:07:32.311: CRYPTO_PKI: ip-ext-val: IP extension validation not required
```

常見問題

組態錯誤

使用者的證書驗證成功，但是，由於配置中缺少強制命令 `authorization username subjectname commonname`，使用者的證書驗證失敗。

```
Apr 26 01:35:32.222: SSH1: starting SSH control process
Apr 26 01:35:32.222: SSH1: sent protocol version id SSH-1.99-Cisco-1.25
Apr 26 01:35:32.224: SSH1: protocol version id is - SSH-2.0-Pragma FortressCL 5.0.10.4176
Apr 26 01:35:32.224: SSH2 1: kexinit sent: kex algo = diffie-hellman-group-exchange-sha1,diffie-hellman
Apr 26 01:35:32.224: SSH2 1: kexinit sent: hostkey algo = x509v3-ssh-rsa,ssh-rsa
Apr 26 01:35:32.224: SSH2 1: kexinit sent: encryption algo = aes128-ctr,aes192-ctr,aes256-ctr
Apr 26 01:35:32.224: SSH2 1: kexinit sent: mac algo = hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-96
Apr 26 01:35:32.224: SSH2 1: SSH2_MSG_KEXINIT sent
Apr 26 01:35:32.234: SSH2 1: SSH2_MSG_KEXINIT received
Apr 26 01:35:32.234: SSH2 1: kex: client->server enc:aes256-ctr mac:hmac-sha2-256
Apr 26 01:35:32.235: SSH2 1: kex: server->client enc:aes256-ctr mac:hmac-sha2-256
Apr 26 01:35:32.235: SSH2 1: Using hostkey algo = x509v3-ssh-rsa
Apr 26 01:35:32.235: SSH2 1: Using kex_algo = diffie-hellman-group-exchange-sha1
Apr 26 01:35:32.235: SSH2 1: SSH2_MSG_KEX_DH_GEX_REQUEST received
Apr 26 01:35:32.235: SSH2 1: Range sent by client is - 1024 < 2048 < 8192
Apr 26 01:35:32.235: SSH2 1: Modulus size established : 2048 bits
Apr 26 01:35:32.246: SSH2 1: expecting SSH2_MSG_KEX_DH_GEX_INIT
Apr 26 01:35:32.246: SSH2 1: SSH2_MSG_KEXDH_INIT received
Apr 26 01:35:32.259: SSH2 1: Sending Server certificate associated with PKI trustpoint "pki-server"
Apr 26 01:35:32.259: CRYPTO_PKI: (A0049) Session started - identity selected (pki-server)
Apr 26 01:35:32.259: SSH2 1: Got 3 certificate(s) on certificate chain
Apr 26 01:35:32.259: CRYPTO_PKI: Rcvd request to end PKI session A0049.
Apr 26 01:35:32.260: CRYPTO_PKI: PKI session A0049 has ended. Freeing all resources.
Apr 26 01:35:32.260: CRYPTO_PKI: unlocked trustpoint pki-server, refcount is 0
Apr 26 01:35:32.273: SSH2: kex_derive_keys complete
Apr 26 01:35:32.274: SSH2 1: SSH2_MSG_NEWKEYS sent
Apr 26 01:35:32.274: SSH2 1: waiting for SSH2_MSG_NEWKEYS
Apr 26 01:35:45.664: SSH2 1: SSH2_MSG_NEWKEYS received
Apr 26 01:35:45.665: SSH2 1: Authentications that can continue = publickey,password,keyboard-interactive
Apr 26 01:35:45.666: SSH2 1: Using method = none
Apr 26 01:35:45.666: SSH2 1: Authentications that can continue = publickey,password,keyboard-interactive
Apr 26 01:35:45.675: SSH2 1: Using method = publickey
Apr 26 01:35:45.675: SSH2 1: Received publickey algo = x509v3-ssh-rsa
Apr 26 01:35:45.676: SSH2 1: Verifying certificate for user 'sameer.cisco.com' in SSH2_MSG_USERAUTH_REQUEST
Apr 26 01:35:45.676: SSH2 1: Verifying certificate for user 'sameer.cisco.com'
```

Apr 26 01:35:45.676: SSH2 1: Received a chain of 3 certificate
Apr 26 01:35:45.676: SSH2 1: Received 0 ocsrp-response
Apr 26 01:35:45.676: SSH2 1: Starting PKI session for certificate verification
Apr 26 01:35:45.676: CRYPTO_PKI: (A004A) Session started - identity not specified
Apr 26 01:35:45.676: CRYPTO_PKI: (A004A) Adding peer certificate
Apr 26 01:35:45.676: CRYPTO_PKI: Added x509 peer certificate - (1249) bytes
Apr 26 01:35:45.676: CRYPTO_PKI: (A004A) Adding peer certificate
Apr 26 01:35:45.676: CRYPTO_PKI: Added x509 peer certificate - (1215) bytes
Apr 26 01:35:45.676: CRYPTO_PKI: (A004A) Adding peer certificate
Apr 26 01:35:45.676: CRYPTO_PKI: Added x509 peer certificate - (921) bytes
Apr 26 01:35:45.676: CRYPTO_PKI: ip-ext-val: IP extension validation not required
Apr 26 01:35:45.677: CRYPTO_PKI: create new ca_req_context type PKI_VERIFY_CHAIN_CONTEXT, ident 37
Apr 26 01:35:45.677: CRYPTO_PKI: (A004A) validation path has 1 certs
Apr 26 01:35:45.677: CRYPTO_PKI: (A004A) Check for identical certs
Apr 26 01:35:45.677: CRYPTO_PKI : (A004A) Validating non-trusted cert
Apr 26 01:35:45.677: CRYPTO_PKI: (A004A) Create a list of suitable trustpoints
Apr 26 01:35:45.677: CRYPTO_PKI: Found a issuer match
Apr 26 01:35:45.677: CRYPTO_PKI: (A004A) Suitable trustpoints are: pki-server,
Apr 26 01:35:45.677: CRYPTO_PKI: (A004A) Attempting to validate certificate using pki-server policy
Apr 26 01:35:45.677: CRYPTO_PKI: ECU validation successful. Cert matches configuration.
Apr 26 01:35:45.677: CRYPTO_PKI: (A004A) Using pki-server to validate certificate
Apr 26 01:35:45.677: CRYPTO_PKI: Added 1 certs to trusted chain.
Apr 26 01:35:45.677: CRYPTO_PKI: Prepare session revocation service providers
Apr 26 01:35:45.677: CRYPTO_PKI: Deleting cached key having key id 50
Apr 26 01:35:45.677: CRYPTO_PKI: Attempting to insert the peer's public key into cache
Apr 26 01:35:45.677: CRYPTO_PKI: Peer's public inserted successfully with key id 51
Apr 26 01:35:45.678: CRYPTO_PKI: Expiring peer's cached key with key id 51
Apr 26 01:35:45.678: CRYPTO_PKI: (A004A) Certificate is verified
Apr 26 01:35:45.678: CRYPTO_PKI: Remove session revocation service providers
Apr 26 01:35:45.678: CRYPTO_PKI: Remove session revocation service providers
Apr 26 01:35:45.678: CRYPTO_PKI: (A004A) Certificate validated without revocation check
Apr 26 01:35:45.678: CRYPTO_PKI: Populate AAA auth data
Apr 26 01:35:45.678: CRYPTO_PKI: Unable to get configured attribute for primary AAA list authorization.
Apr 26 01:35:45.678: CRYPTO_PKI: (A004A) chain cert was anchored to trustpoint pki-server, and chain val
Apr 26 01:35:45.678: CRYPTO_PKI: destroying ca_req_context type PKI_VERIFY_CHAIN_CONTEXT, ident 37, ref
Apr 26 01:35:45.678: CRYPTO_PKI: ca_req_context released
Apr 26 01:35:45.678: CRYPTO_PKI: (A004A) Validation TP is pki-server
Apr 26 01:35:45.678: CRYPTO_PKI: (A004A) Certificate validation succeeded
Apr 26 01:35:45.678: SSH2 1: Could not find username field configured for certificate in trustpoint Err
Apr 26 01:35:45.678: CRYPTO_PKI: Rcvd request to end PKI session A004A.
Apr 26 01:35:45.678: CRYPTO_PKI: PKI session A004A has ended. Freeing all resources.
Apr 26 01:35:45.679: SSH2 1: Can not decode the certificate Err code = 7
Apr 26 01:35:45.679: SSH2 1: Certificate authentication failed for user 'sameer.cisco.com'

相關資訊

- [PKI配置指南](#)
- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。