

Configurazione di SSH con l'autenticazione x509 nei dispositivi IOS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Considerazioni sulla distribuzione](#)

[Configurazioni](#)

[\(Facoltativo\) Integrazione con il server TACACS](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare il server SSH con l'uso dei certificati x509v3 sui dispositivi IOS in conformità allo standard RFC6187.

Il protocollo SSH (Secure Shell Protocol) fornisce l'autenticazione reciproca, ossia vengono autenticati sia il client sia il server. In genere, il server utilizza la coppia di chiavi privata e pubblica RSA per l'autenticazione. Il client SSH calcola il checksum della chiave pubblica e chiede all'amministratore se è attendibile. L'amministratore deve esportare la chiave pubblica dal router utilizzando il metodo fuori banda e confrontare i valori. In pratica, si tratta di un metodo ingombrante e spesso la chiave pubblica viene accettata senza verifica, il che porta a un potenziale rischio di attacchi da parte dell'uomo nel mezzo.

Lo standard RFC6187 è una soluzione a questo problema in quanto fornisce un livello di sicurezza e un'esperienza utente simile al protocollo TLS (Transport Layer Security) comunemente utilizzato per proteggere le trasmissioni basate sul Web.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Infrastruttura PKI

Componenti usati

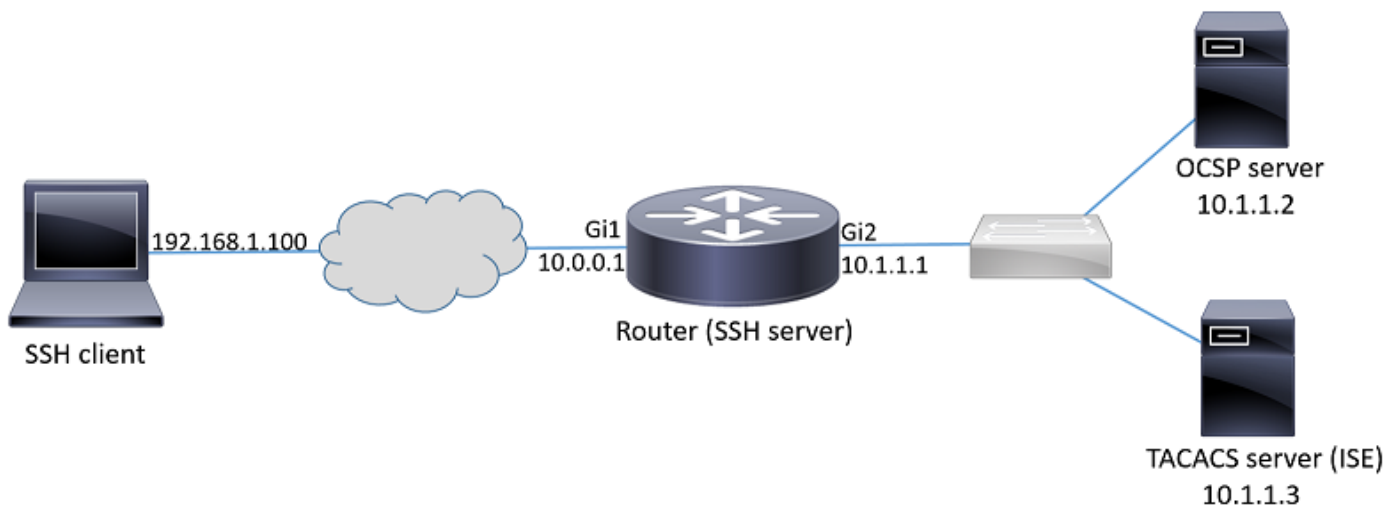
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Router CSR 1000v con IOS-XE versione 16.6.1
- Client SSH Pragma Fortress
- Server OCSP Windows Server 2016
- Identity Services Engine versione 2.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Considerazioni sulla distribuzione

- Un Per utilizzare questa funzione, è necessario un client SSH compatibile con RFC6187.
- Questa funzione è stata implementata in IOS versione 15.5(2)T e IOS-XE versione 15.5(2)S.
- Il client SSH e il server negoziano i meccanismi di autenticazione supportati. Tutti i meccanismi di autenticazione supportati in precedenza nel dispositivo possono continuare a funzionare contemporaneamente ai meccanismi di autenticazione basati su x509 per garantire una transizione senza problemi.
- L'amministratore può scegliere di utilizzare il metodo di autenticazione basato su x509 solo per server, solo client o entrambi.
- Il server IOS può verificare se il certificato presentato dal client non è stato revocato. A tale scopo, la banca dati dei certificati revocati viene consultata per ogni connessione. In questo modo è possibile revocare l'accesso senza dover riconfigurare altri dispositivi, nel caso in cui la chiave privata del certificato sia compromessa o se l'accesso per un utente specifico debba

essere revocato.

- Il controllo di revoca è facoltativo, ma è consigliabile avere la possibilità di negare l'accesso in base a credenziali compromesse. In alternativa è possibile eseguire l'autorizzazione per il nome utente recuperato dal certificato sul TACACS (Terminal Access Controller Access-Control System) esterno o sul server RADIUS. Se il certificato è compromesso, è possibile disabilitare l'account sul server esterno per impedire l'accesso con l'utilizzo del certificato.
- L'autorizzazione degli utenti può essere eseguita da un server esterno o può essere ignorata (tutti gli utenti con un certificato valido si presume abbiano i privilegi per accedere al dispositivo). In questo esempio, il metodo precedente viene utilizzato per semplificare.
- Per verificare correttamente i dati di autenticazione dell'altra parte, il client e il server devono solo considerare attendibile un'Autorità di certificazione (CA) comune. Ciò significa che solo il certificato della CA che ha firmato il certificato del router deve essere installato nell'archivio certificati attendibili del dispositivo client.
- Il certificato fornisce informazioni sull'identità dell'altra parte (il nome comune e il nome alternativo del soggetto sono in genere utilizzati a tale scopo). Il client deve confrontare il nome host o il nome dell'indirizzo IP del server fornito come input dall'amministratore con i dati di identità disponibili nel certificato presentato. Limita severamente le opportunità di attacchi di tipo man-in-the-middle o di altro tipo.

Configurazioni

Configurare i parametri AAA. In uno scenario di base (senza un server di autorizzazione esterno) è possibile ignorare l'autorizzazione per il nome utente recuperato dal certificato.

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

Configurare un trust point che contenga il certificato CA e, facoltativamente, il certificato del router.

```
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 ocs
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
```

Suggerimento: Se il server OCSP non è raggiungibile, l'amministratore può scegliere di non consentire tutti gli accessi utilizzando la configurazione **ocsp controllo di revoca** o di consentire l'accesso senza controllo di revoca utilizzando **ocsp controllo di revoca nessuno**

(scelta non consigliata).

Configurare i meccanismi di autenticazione consentiti utilizzati durante la negoziazione del tunnel SSH.

```
! 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
```

Configurare il server SSH in modo che usi i certificati corretti nel processo di autenticazione.

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

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

(Facoltativo) Integrazione con il server TACACS

Dopo aver recuperato il nome utente dal certificato, il sistema operativo IOS può autorizzare il nome utente sul server TACACS. Ciò è particolarmente utile se il server TACACS è già stato implementato per l'amministrazione del dispositivo.

Nota: Il server SSH IOS non supporta attualmente il concatenamento del metodo di autenticazione. Ciò significa che se i certificati vengono utilizzati per autenticare l'utente, il server TACACS non può essere utilizzato per l'autenticazione tramite password. Può essere utilizzato solo a scopo di autorizzazione.

Configurare il server TACACS.

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

Configurare l'elenco delle autorizzazioni per l'utilizzo del server TACACS.

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

1. Configurare ISE (Identity Services Engine). L'esempio di configurazione è disponibile all'indirizzo:

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

2. Configurare il profilo TACACS. Il parametro aggiuntivo **cert-application=all** deve essere configurato affinché l'autorizzazione abbia esito positivo, selezionare **Centri di lavoro > Amministrazione dispositivi > Elementi criterio > Risultati > Profili TACACS > Aggiungi**.

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. Per configurare il set di criteri, passare a **Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dispositivi > Aggiungi**.

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

Verifica

```
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
```

Risoluzione dei problemi

Questi debug vengono utilizzati per tenere traccia della sessione completata:

```
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

Se il certificato per admin1 è stato revocato:

```
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
```

Informazioni correlate

- Guida alla configurazione di 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
- Esempio di configurazione di TACACS su ISE:
<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200208-Configure-ISE-2-0-IOI-TACACS-Authentic.html>
- [Documentazione e supporto tecnico – Cisco Systems](#)