Certificaatverificatie configureren voor SSH op Cisco IOS XE-apparaten

Inhoud

Inleiding

Dit document schetst de configuratie van Secure Shell (SSH) op Cisco IOS® XE-apparaten met behulp van X.509v3-certificaten voor verificatie, in overeenstemming met de richtlijnen die zijn gedefinieerd in RFC 6187.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van de Public Key Infrastructure (PKI) infrastructuur.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- C9200L-Switch met Cisco IOS XE versie 17.3.5
- Pragma Fortress SSH-client

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

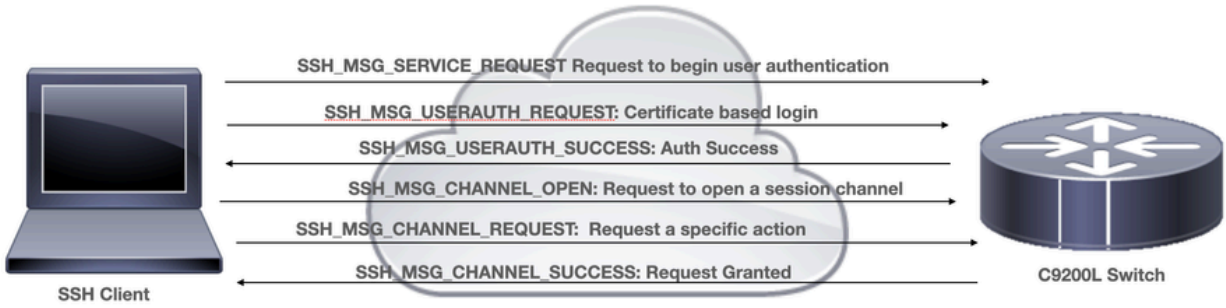
De aanpak verbetert de SSH-beveiliging door op certificaten gebaseerde verificatie mogelijk te maken, waardoor de beheerpraktijken voor SSH-sleutels nauwer worden afgestemd op die welke worden gebruikt in Transport Layer Security (TLS).

SSH biedt wederzijdse authenticatie om een veilige verbinding tussen client en server tot stand te brengen. Traditioneel worden servers geverifieerd met behulp van Rivest-Shamir-Addleman (RSA) sleutelparen. De client berekent een vingerafdruk van de openbare sleutel van de server en vraagt de beheerder om deze te verifiëren - idealiter door deze te vergelijken met een bekende waarde die is verkregen via een veilige, out-of-band methode. Deze handmatige verificatie wordt echter vaak overgeslagen vanwege de complexiteit ervan, waardoor het risico op man-in-the-middle (MitM) -aanvallen toeneemt en het SSH-vertrouwensmodel wordt verzwakt.

RFC 6187 pakt deze problemen aan door X.509v3-certificaatgebaseerde verificatie in te schakelen, waarbij SSH met PKI wordt geïntegreerd. Deze aanpak verbetert de beveiliging en schaalbaarheid doordat vertrouwen kan worden gevestigd via vertrouwde certificeringsinstanties (CA's), die een gebruikerservaring en vertrouwensmodel bieden dat vergelijkbaar is met TLS.

Configureren

Netwerkdiagram



Overwegingen bij implementatie

- Een RFC6187-compatibele SSH-client is nodig om van de functie te profiteren.
- De SSH-client en -server onderhandelen over ondersteunde verificatiemechanismen. Alle verificatiemechanismen die eerder op het apparaat werden ondersteund, kunnen gelijktijdig

blijven werken met op x509 gebaseerde verificatiemechanismen om een soepele overgang te garanderen.
- De beheerder kan ervoor kiezen om de op x509 gebaseerde verificatiemethode alleen te gebruiken voor de server, de client of beide.
- Om de authenticatiegegevens van de andere partij met succes te verifiëren, hoeven de client en server alleen een gemeenschappelijke CA te vertrouwen. Dit betekent dat alleen het certificaat van CA dat het routercertificaat heeft ondertekend, moet worden geïnstalleerd op het vertrouwde certificaatarchief van het clientapparaat.
- Het certificaat bevat informatie over de identiteit van de andere partij (algemene naam en alternatieve naam van het onderwerp worden meestal voor dat doel gebruikt). De client moet de hostnaam of IP-adresnaam van de server die als invoer door de beheerder is opgegeven, vergelijken met de identiteitsgegevens die beschikbaar zijn in het gepresenteerde certificaat. Het beperkt de mogelijkheden van MitM of andere imitatie-aanvallen ernstig.

Configuraties

IOS-XE-apparaat (SSH-server)

Configureer een vertrouwenspunt dat het CA-certificaat en optioneel het routercertificaat bevat.

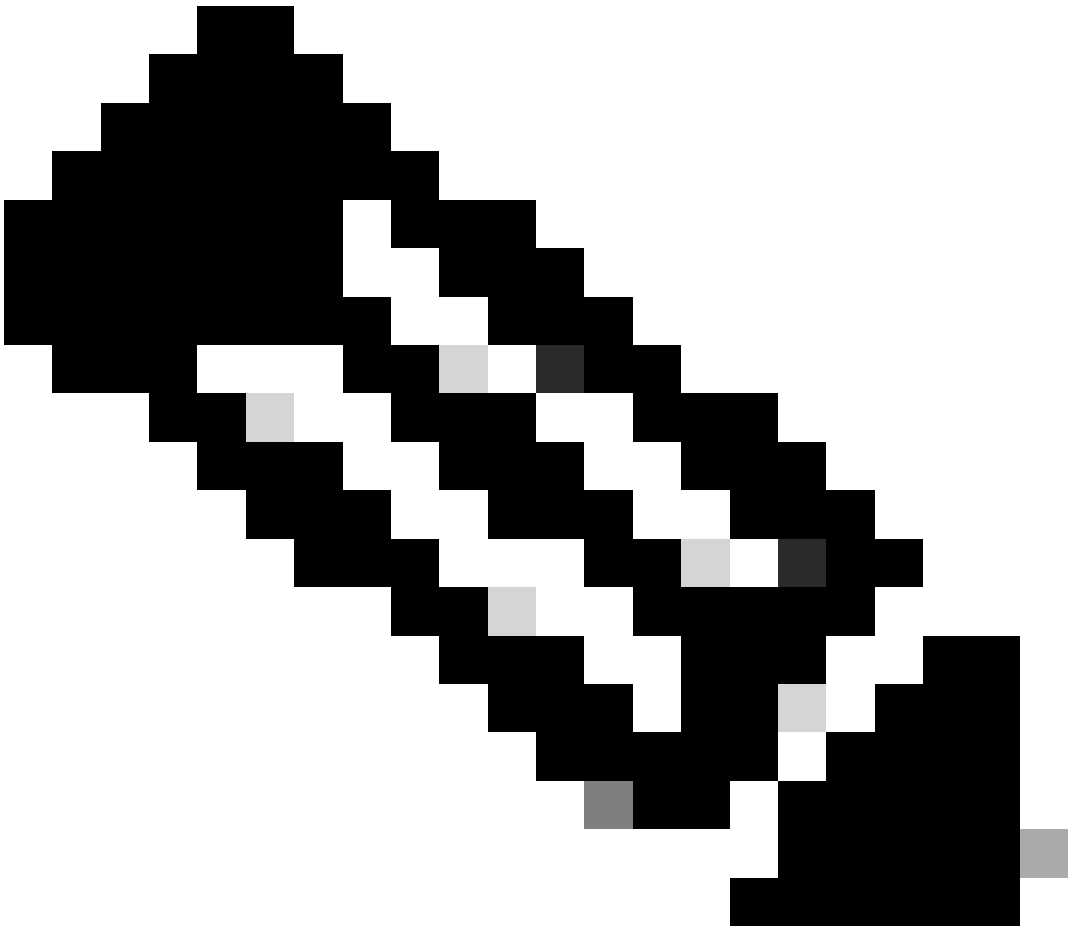
```
crypto pki trustpoint pki-server

 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
```

Configureer toegestane authenticatiemechanismen die worden gebruikt tijdens SSH-tunnelonderhandelingen.

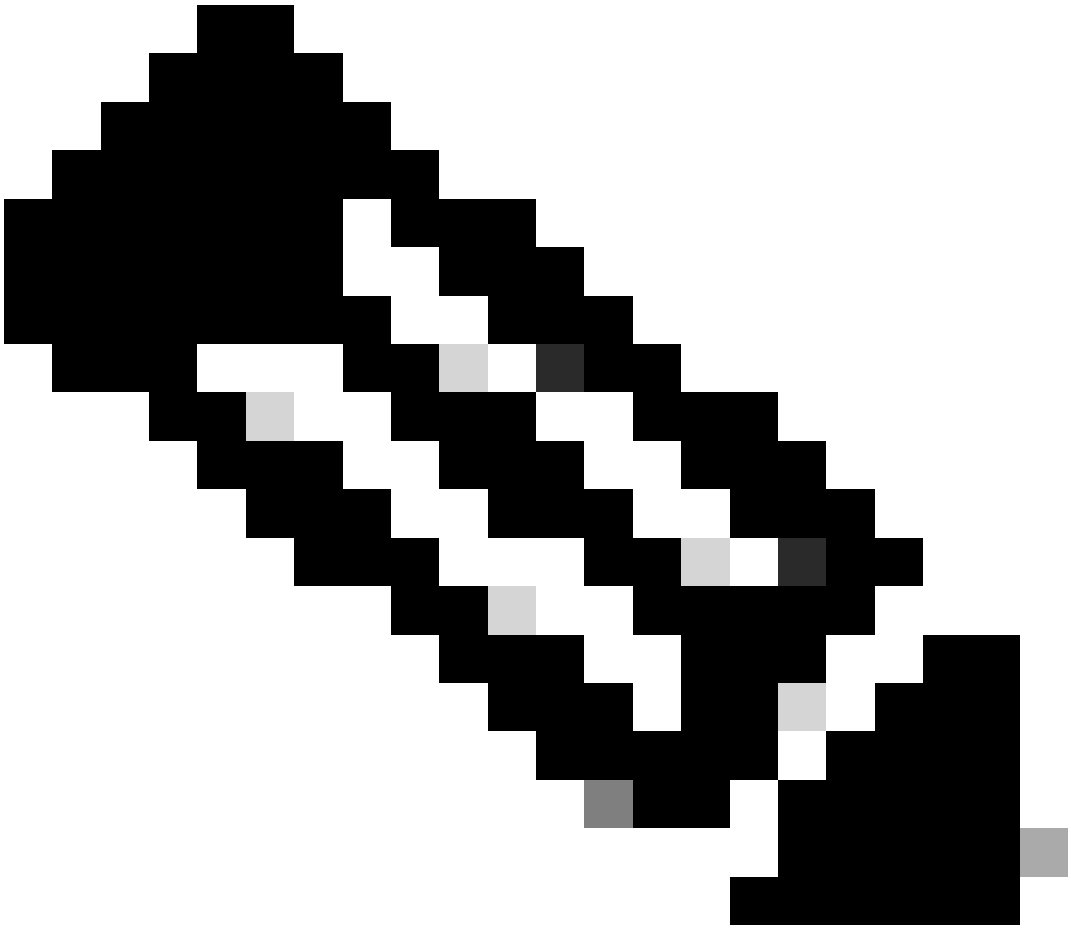
```
! Alorithms used to authenticate server
ip ssh server algorithm hostkey x509v3-ssh-rsa ssh-rsa

! 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
```

Configureer de SSH-server om de juiste certificaten te gebruiken in het verificatieproces.

```
ip ssh server certificate profile
server
  trustpoint sign



user
  trustpoint verify
```

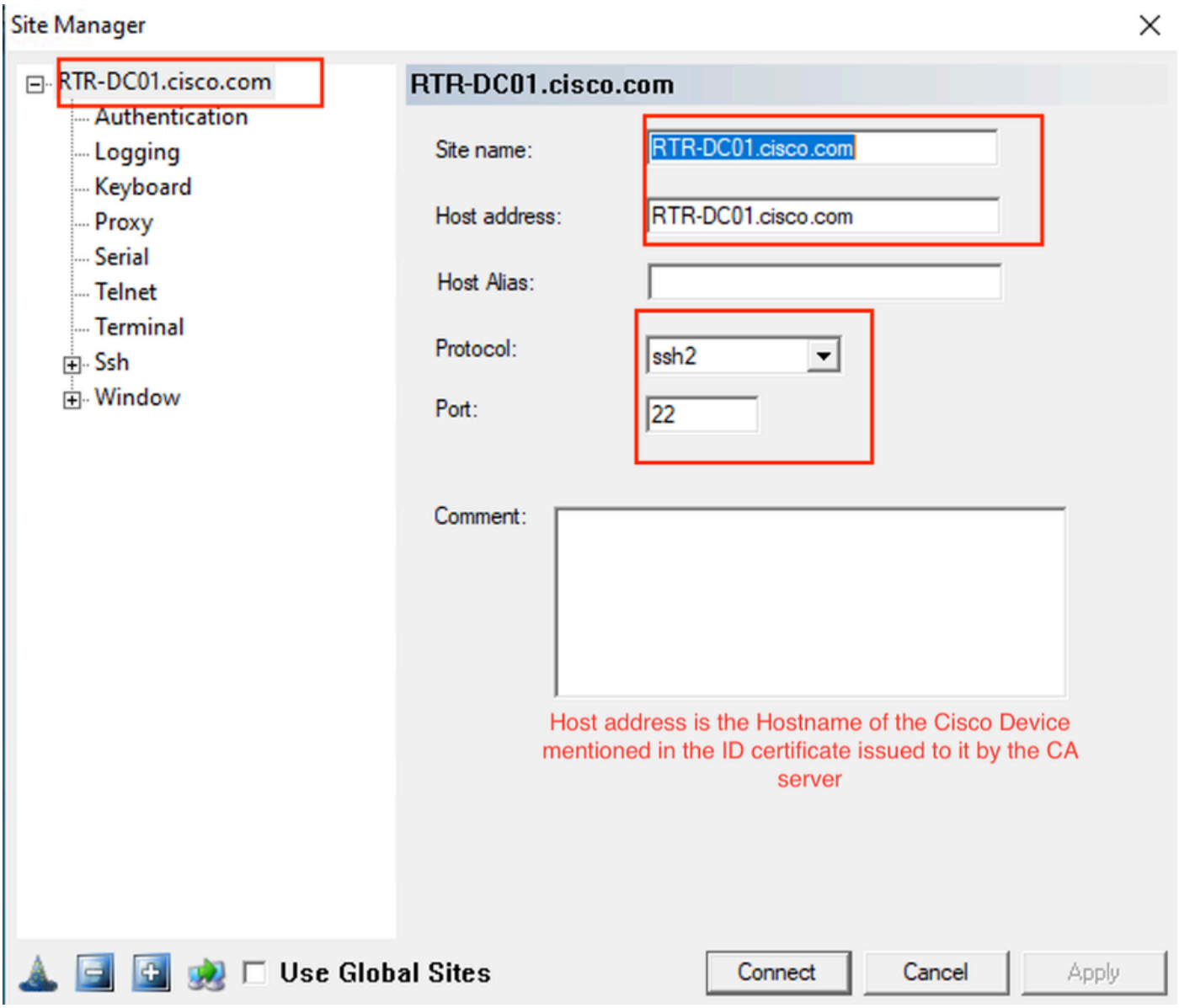


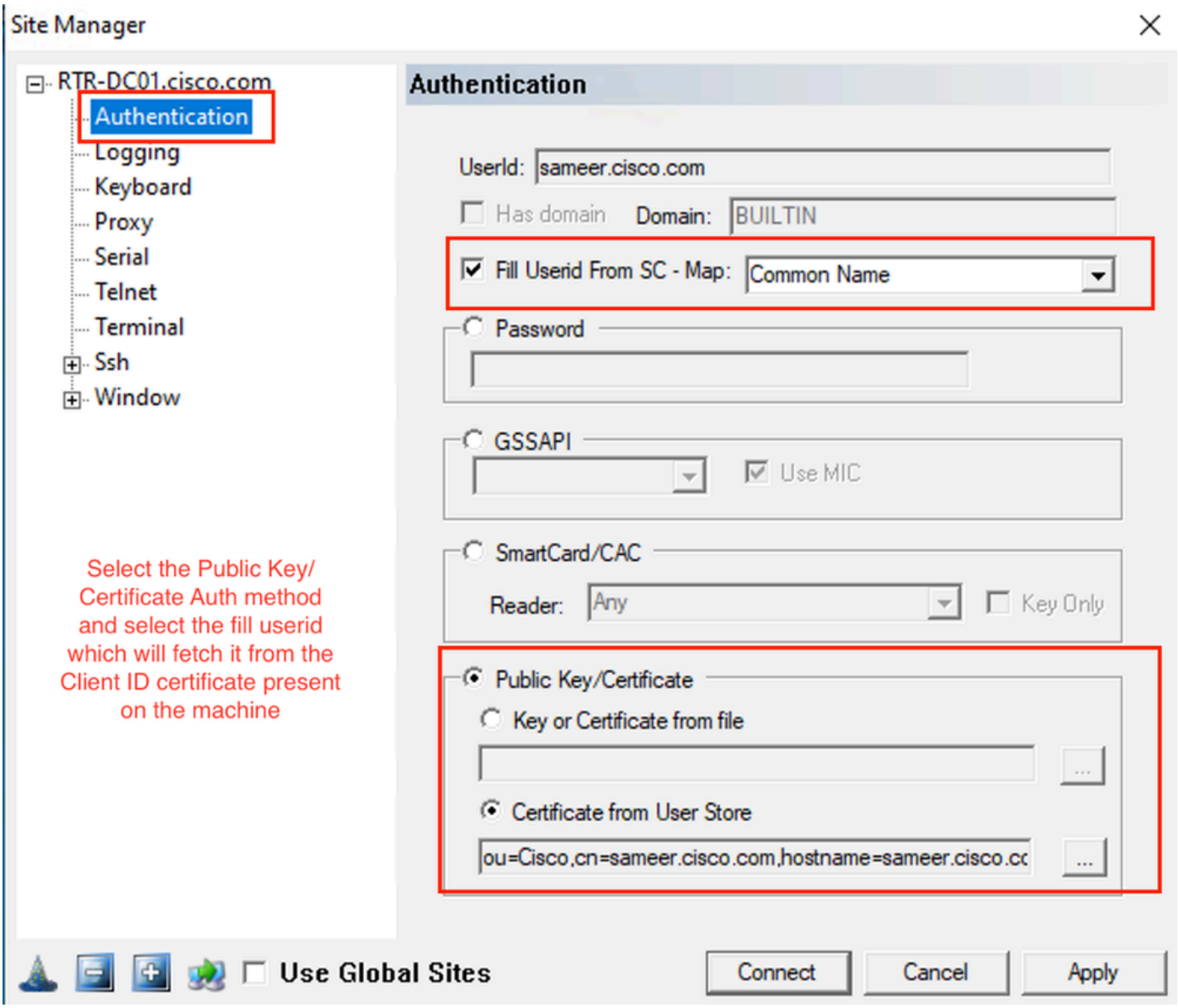
Opmerking: Zorg ervoor dat de SSH-server en de SSH-client het ID-certificaat hebben dat is afgegeven door dezelfde CA-server.



Opmerking: Als een SSH-client zoals een Windows-systeem een ID-certificaat heeft dat is afgegeven door een andere CA, moet u het importeren op de SSH-server, dat wil zeggen Cisco Switch, en dat Trustpoint toewijzen aan het bovenstaande SSH-servercertificaatprofiel onder gebruikersgedeelte.

Pragma Fortress CL (SSH-client geïnstalleerd op gebruikersmachine)


Site Manager
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



Verifiëren

```
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
```

Problemen oplossen

Deze debugs worden gebruikt om succesvolle sessies bij te houden:

```
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-sha1-9
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-interactiv
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-interactiv
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_REQ
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_REQUE
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
```

Veelvoorkomende problemen

Configuratiefouten

Certificaatvalidatie is succesvol voor de gebruiker, maar vanwege het ontbreken van de verplichte opdracht autorisatie gebruikersnaam gebruikersnaam gebruikersnaam gemeenschappelijke naam in de configuratie, het certificaat authenticatie voor de gebruiker mislukt.

```
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-sha1-9
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-interactiv
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-interactiv
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_REQ
```

```
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 ocsp-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: EKU 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'
```

Gerelateerde informatie

- PKI-configuratiehandleiding
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.