How to Configure SSH on Catalyst Switches Running CatOS (SSH configureren op Catalyst-switches die CatOS gebruiken)

Inhoud

Inleiding

Dit document geeft stap-voor-stap instructies om Secure Shell (SSH) versie 1 te configureren op Catalyst switches waarop Catalyst OS (CatOS) wordt uitgevoerd. De geteste versie is cat6000-**supk9**.6-1-1c.bin.

Voorwaarden

Vereisten

Deze tabel toont de status van SSH-ondersteuning in de switches. Geregistreerde gebruikers kunnen deze softwareafbeeldingen openen door naar het Software Center te gaan.

CatOS SSH	
Apparaat	**Ondersteuning van SSH**
Kat 4000/4500/2948G/2980G (CatOS)	K9 beelden vanaf 6.1
Kat 5000/5500 (CatOS)	K9 beelden vanaf 6.1
Kat 6000/6500 (CatOS)	K9 beelden vanaf 6.1
IOS-SSH	
Apparaat	**Ondersteuning van SSH**
Kat 2950*	12.1(12c)EA1 en hoger
Kat 3550*	12.1(11)EA1 en hoger
Kat 4000/4500 (geïntegreerde Cisco IOS-software)*	12.1(13)EW en later **
Kat 6000/5500 (geïntegreerde Cisco IOS-software)*	12.1(11b)E en hoger
Kat 8540/8510	12.1(12c)EY en hoger, 12.1(14)E1 en hoger
Geen SSH	
Apparaat	**Ondersteuning van SSH**
Kat 1900	nee
Kat 2800	nee
Kat 2948G-L3	nee
Kat 2900XL	nee
Cat 3500XL	nee
Cat 4840G-L3	nee
Cat 4908G-L3	nee

* Configuration wordt meegeleverd bij het configureren van Secure Shell op routers en Switches waarop Cisco IOS wordt uitgevoerd.

** Er is geen ondersteuning voor SSH in 12.1E trein voor Catalyst 4000 met geïntegreerde Cisco IOS-software.

Raadpleeg het autorisatieformulier voor export van encryptiesoftware om 3DES aan te vragen.

Dit document veronderstelt dat de authentificatie voorafgaand aan implementatie van SSH (door het wachtwoord van Telnet, TACACS+) of RADIUS werkt. SSH met Kerberos wordt niet ondersteund voorafgaand aan de implementatie van SSH.

Gebruikte componenten

Dit document is alleen bestemd voor Catalyst 2948G, Catalyst 2980G, Catalyst 4000/4500 Series, Catalyst 5000/5500 Series en Catalyst 6000/6500 Series met het CatOS K9-beeld. Raadpleeg voor meer informatie het gedeelte Vereisten van dit document.

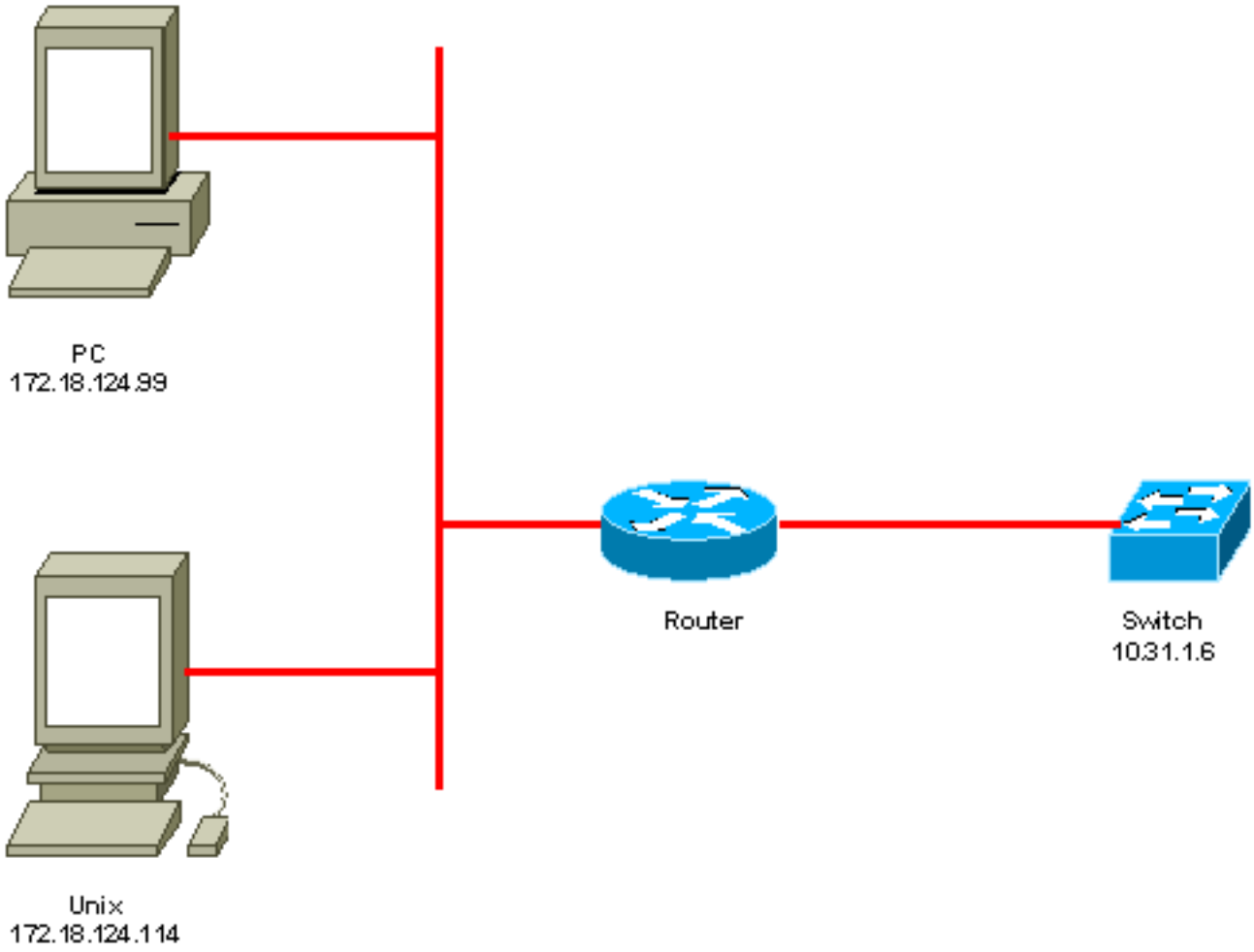
De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een live netwerk werkt, zorg er dan voor dat u de potentiële

impact van iedere opdracht begrijpt voor u deze gebruikt.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Netwerkdiagram



Switchconfiguratie

```
!--- Generate and verify RSA key. sec-cat6000> (enable) set crypto key rsa 1024
Generating RSA keys..... [OK]
sec-cat6000> (enable) ssh_key_process: host/server key size: 1024/768
 !--- Display the RSA key. sec-cat6000> (enable) show crypto key
RSA keys were generated at: Mon Jul 23 2001, 15:03:30 1024 65537 1514414695360
577332853671704785709850606634768746869716963940352440620678575338701550888525
699691478330537840066956987610207810959498648179965330018010844785863472773067
697185256418386243001881008830561241137381692820078674376058275573133448529332
199668201930132947097826805906337821547938540549819306165 1
!--- Restrict which host/subnets are allowed to use SSH to the switch. !--- Note: If you do not
do this, the switch will display the message !--- "WARNING!! IP permit list has no entries!"
```

```
sec-cat6000> set ip permit 172.18.124.0 255.255.255.0
172.18.124.0 with mask 255.255.255.0 added to IP permit list.
!--- Turn on SSH. sec-cat6000> (enable) set ip permit enable ssh
SSH permit list enabled.
!--- Verity SSH permit list. sec-cat6000> (enable) show ip permit
Telnet permit list disabled.
Ssh permit list enabled.
Snmp permit list disabled.
Permit List Mask Access-Type
---------------- ---------------- -------------
172.18.124.0 255.255.255.0 telnet ssh snmp

Denied IP Address Last Accessed Time Type
----------------- ------------------ ------
```

SSH uitschakelen

In bepaalde situaties kan het nodig zijn om SSH uit te schakelen op de switch. U moet verifiëren of SSH op de switch is geconfigureerd en als dat het geval is, uitschakelen.

Om te verifiëren of SSH op de switch is geconfigureerd, geeft u de opdracht **show crypto key uit**. Als de uitvoer de RSA-toets weergeeft, is SSH geconfigureerd en ingeschakeld op de switch. Hier wordt een voorbeeld gegeven.

```
sec-cat6000> (enable) show crypto key
RSA keys were generated at: Mon Jul 23 2001, 15:03:30 1024 65537 1514414695360
577332853671704785709850606634768746869716963940352440620678575338701550888525
699691478330537840066956987610207810959498648179965330018010844785863472773067
697185256418386243001881008830561241137381692820078674376058275573133448529332
199668201930132947097826805906337821547938540549819306165 1
```

Om de crypto sleutel te verwijderen, geef de **duidelijke crypto sleutel rsa** bevel uit om SSH op de switch onbruikbaar te maken. Hier wordt een voorbeeld gegeven.

```
sec-cat6000> (enable) clear crypto key rsa
Do you really want to clear RSA keys (y/n) [n]? y
RSA keys has been cleared.
sec-cat6000> (enable)
```

debug in de Catalyst

Als u debugs wilt inschakelen, geeft u de opdracht **trace ssh 4 uit**.

Om debugs uit te schakelen, geef het **vastgestelde** bevel **van spoor ssh 0 uit**.

Opdracht voorbeelden van een goede verbinding debuggen

Solaris naar Catalyst, standaard voor drievoudige gegevensversleuteling (3DES), Telnet-wachtwoord

Solaris

```
rtp-evergreen# ssh -c 3des -v 10.31.1.6
```

```
SSH Version 1.2.26 [sparc-sun-solaris2.5.1], protocol version 1.5.
Compiled with RSAREF.
rtp-evergreen: Reading configuration data /opt/CISssh/etc/ssh_config
rtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0
rtp-evergreen: Allocated local port 1023.
rtp-evergreen: Connecting to 10.31.1.6 port 22.
rtp-evergreen: Connection established.
rtp-evergreen: Remote protocol version 1.5, remote software version 1.2.26
rtp-evergreen: Waiting for server public key.
rtp-evergreen: Received server public key (768 bits) and host key (1024 bits).
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes
Host '10.31.1.6' added to the list of known hosts.
rtp-evergreen: Initializing random; seed file //.ssh/random_seed
rtp-evergreen: Encryption type: 3des
rtp-evergreen: Sent encrypted session key.
rtp-evergreen: Installing crc compensation attack detector.
rtp-evergreen: Received encrypted confirmation.
rtp-evergreen: Doing password authentication.
root@10.31.1.6's password:
rtp-evergreen: Requesting pty.
rtp-evergreen: Failed to get local xauth data.
rtp-evergreen: Requesting X11 forwarding with authentication spoofing.
Warning: Remote host denied X11 forwarding, perhaps xauth program
   could not be run on the server side.
rtp-evergreen: Requesting shell.
rtp-evergreen: Entering interactive session.

Cisco Systems Console

sec-cat6000>
```

Catalyst

```
sec-cat6000> (enable) debug: _proc->tty = 0x8298a494, socket_index = 3
debug: version: SSH-1.5-1.2.26

debug: Client protocol version 1.5; client software version 1.2.26
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: 3des
debug: Received session key; encryption turned on.
debug: ssh login by user: root
debug: Trying Local Login
Password authentication for root accepted.
debug: ssh received packet type: 10
debug: ssh received packet type: 34
Unknown packet type received after authentication: 34
debug: ssh received packet type: 12
debug: ssh88: starting exec shell
debug: Entering interactive session.
```

PC naar Catalyst, 3DES, Telnet wachtwoord

Catalyst

```
debug: Client protocol version 1.5; client software version W1.0
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: des
debug: Received session key; encryption turned on.
debug: ssh login by user:
```

```
debug: Trying Local Login
Password authentication for accepted.
debug: ssh received packet type: 10
debug: ssh received packet type: 37
Unknown packet type received after authentication: 37
debug: ssh received packet type: 12
debug: ssh89: starting exec shell
debug: Entering interactive session.
```

Solaris naar Catalyst, 3DES, verificatie, autorisatie en accounting (AAA) verificatie

Solaris

```
Solaris with aaa on:
rtp-evergreen# ssh -c 3des -l abcde123 -v 10.31.1.6
SSH Version 1.2.26 [sparc-sun-solaris2.5.1], protocol version 1.5.
Compiled with RSAREF.
rtp-evergreen: Reading configuration data /opt/CISssh/etc/ssh_config
rtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0
rtp-evergreen: Allocated local port 1023.
rtp-evergreen: Connecting to 10.31.1.6 port 22.
rtp-evergreen: Connection established.
rtp-evergreen: Remote protocol version 1.5, remote software version 1.2.26
rtp-evergreen: Waiting for server public key.
rtp-evergreen: Received server public key (768 bits) and host key (1024 bits).
rtp-evergreen: Host '10.31.1.6' is known and matches the host key.
rtp-evergreen: Initializing random; seed file //.ssh/random_seed
rtp-evergreen: Encryption type: 3des
rtp-evergreen: Sent encrypted session key.
rtp-evergreen: Installing crc compensation attack detector.
rtp-evergreen: Received encrypted confirmation.
rtp-evergreen: Doing password authentication.
abcde123@10.31.1.6's password:
rtp-evergreen: Requesting pty.
rtp-evergreen: Failed to get local xauth data.
rtp-evergreen: Requesting X11 forwarding with authentication spoofing.
Warning: Remote host denied X11 forwarding, perhaps xauth program
   could not be run on the server side.
rtp-evergreen: Requesting shell.
rtp-evergreen: Entering interactive session.

Cisco Systems Console

sec-cat6000>
```

Catalyst

```
sec-cat6000> (enable) debug: _proc->tty = 0x82a07714, socket_index = 3
debug: version: SSH-1.5-1.2.26

debug: Client protocol version 1.5; client software version 1.2.26
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: 3des
debug: Received session key; encryption turned on.
debug: ssh login by user: abcde123
debug: Trying TACACS+ Login
Password authentication for abcde123 accepted.
debug: ssh received packet type: 10
debug: ssh received packet type: 34
Unknown packet type received after authentication: 34
debug: ssh received packet type: 12
```

```
debug: ssh88: starting exec shell
debug: Entering interactive session.
```

Opdracht voorbeelden van wat fout kan gaan

Catalyst-debug met client proberen [niet ondersteund] Blowfish-algoritme

```
debug: Client protocol version 1.5; client software version W1.0
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: blowfish
cipher_set_key: unknown cipher: 6
debug: Calling cleanup
```

Catalyst debug met slecht Telnet-wachtwoord

```
debug: _proc->tty = 0x82897414, socket_index = 4
debug: version: SSH-1.5-1.2.26
debug: Client protocol version 1.5; client software version W1.0
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: 3des
debug: Received session key; encryption turned on.
debug: ssh login by user:
debug: Trying Local Login
debug: Password authentication for failed.
```

Catalyst-debug met slechte AAA-verificatie

```
cat6000> (enable) debug: _proc->tty = 0x829abd94, socket_index = 3
debug: version: SSH-1.5-1.2.26

debug: Client protocol version 1.5; client software version 1.2.26
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: 3des
debug: Received session key; encryption turned on.
debug: ssh login by user: junkuser
debug: Trying TACACS+ Login
debug: Password authentication for junkuser failed.
SSH connection closed by remote host.
debug: Calling cleanup
```

Problemen oplossen

Deze sectie behandelt verschillende het oplossen van probleemscenario's met betrekking tot de configuratie van SSH op Cisco-switches.

Kan geen verbinding met Switch maken via SSH

Probleem:

Kan geen verbinding met de switch maken met SSH.

Het **debug ip sh** commando toont deze uitvoer:

```
Jun 15 20:29:26.207: SSH2 1: RSA_sign: private key not found
```

```
Jun 15 20:29:26.207: SSH2 1: signature creation failed, status -1
```

Oplossing:

Dit probleem doet zich voor om een van de volgende redenen:

- Nieuwe SSH-verbindingen falen na het wijzigen van de hostnaam.
- SSH geconfigureerd met niet-gelabelde toetsen (met de router FQDN).

De mogelijke oorzaken van dit probleem zijn:

- Als de hostname is gewijzigd en SSH niet meer werkt, dan zet u de nieuwe sleutel op nul en maakt u een nieuwe sleutel met het juiste label.
  ```
  crypto key zeroize rsa
  crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
  ```
- Gebruik geen anonieme RSA-toetsen (genoemd naar de FQDN van de switch). Gebruik gelabelde toetsen.
  ```
  crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
  ```

Om dit probleem voor altijd op te lossen, upgrade de IOS software naar een van de versies waarin dit probleem is opgelost.

Er is een fout ingediend over deze kwestie. Raadpleeg voor meer informatie Cisco bug-id CSC4114 **(alleen** geregistreerde **klanten)**.

Gerelateerde informatie

- Ondersteuning van SSH-pagina
- Secure Shell configureren op routers en switches die Cisco IOS draaien
- Bug Toolkit
- Technische ondersteuning – Cisco Systems

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.