How to Configure SSH on Catalyst Switches Running CatOS

Inhalt

Einleitung

Dieses Dokument enthält schrittweise Anweisungen zur Konfiguration von Secure Shell (SSH) Version 1 auf Catalyst-Switches mit Catalyst OS (CatOS). Die getestete Version ist cat6000-**supk9**.6-1-1c.bin.

Voraussetzungen

Anforderungen

Diese Tabelle zeigt den Status der SSH-Unterstützung in den Switches. Registrierte Benutzer können auf diese Software-Images zugreifen, indem sie das Software Center besuchen.

CatOS SSH

"Slot0:"	SSH-Unterstützung
Cat 4000/4500/2948G/2980G (CatOS)	K9 Bilder ab 6.1
Cat 5000/5500 (CatOS)	K9 Bilder ab 6.1
Cat 6000/6500 (CatOS)	K9 Bilder ab 6.1
IOS-SSH	
"Slot0:"	**SSH-Unterstützung**
Cat 2950*	12.1(12c)EA1 und höher
Cat 3550*	12.1(11)EA1 und neuere Versionen
Cat 4000/4500 (integrierte Cisco IOS Software)*	12.1(13)EW und höher **
Cat 6000/5500 (integrierte Cisco IOS Software)*	12.1(11b)E und neuere Versionen
Kat. 8540/8510	12.1(12c)EY und höher, 12.1(14)E1 und höher
Kein SSH	
"Slot0:"	**SSH-Unterstützung**
Cat 1900	nein
Cat 2800	nein
Cat 2948G-L3	nein
Cat 2900XL	nein
Cat 3500XL	nein
Cat 4840G-L3	nein
Cat 4908G-L3	nein

* Die Konfiguration wird unter Konfigurieren von Secure Shell auf Routern und Switches mit Cisco IOS erläutert.

** Im 12.1E-Zug wird SSH für Catalyst 4000 mit integrierter Cisco IOS Software nicht unterstützt.

Informationen zur Beantragung von 3DES finden Sie unter Encryption Software Export Distribution Authorization Form (Formular für die Exportautorisierung der Verschlüsselungssoftware).

In diesem Dokument wird davon ausgegangen, dass die Authentifizierung vor der Implementierung von SSH (über das Telnet-Kennwort, TACACS+) oder RADIUS funktioniert. SSH mit Kerberos wird vor der Implementierung von SSH nicht unterstützt.

Verwendete Komponenten

In diesem Dokument werden nur die Catalyst-Serien 2948G, 2980G, 4000/4500, 5000/5500 und 6000/6500 mit dem CatOS K9-Image behandelt. Weitere Informationen finden Sie im Abschnitt Anforderungen dieses Dokuments.

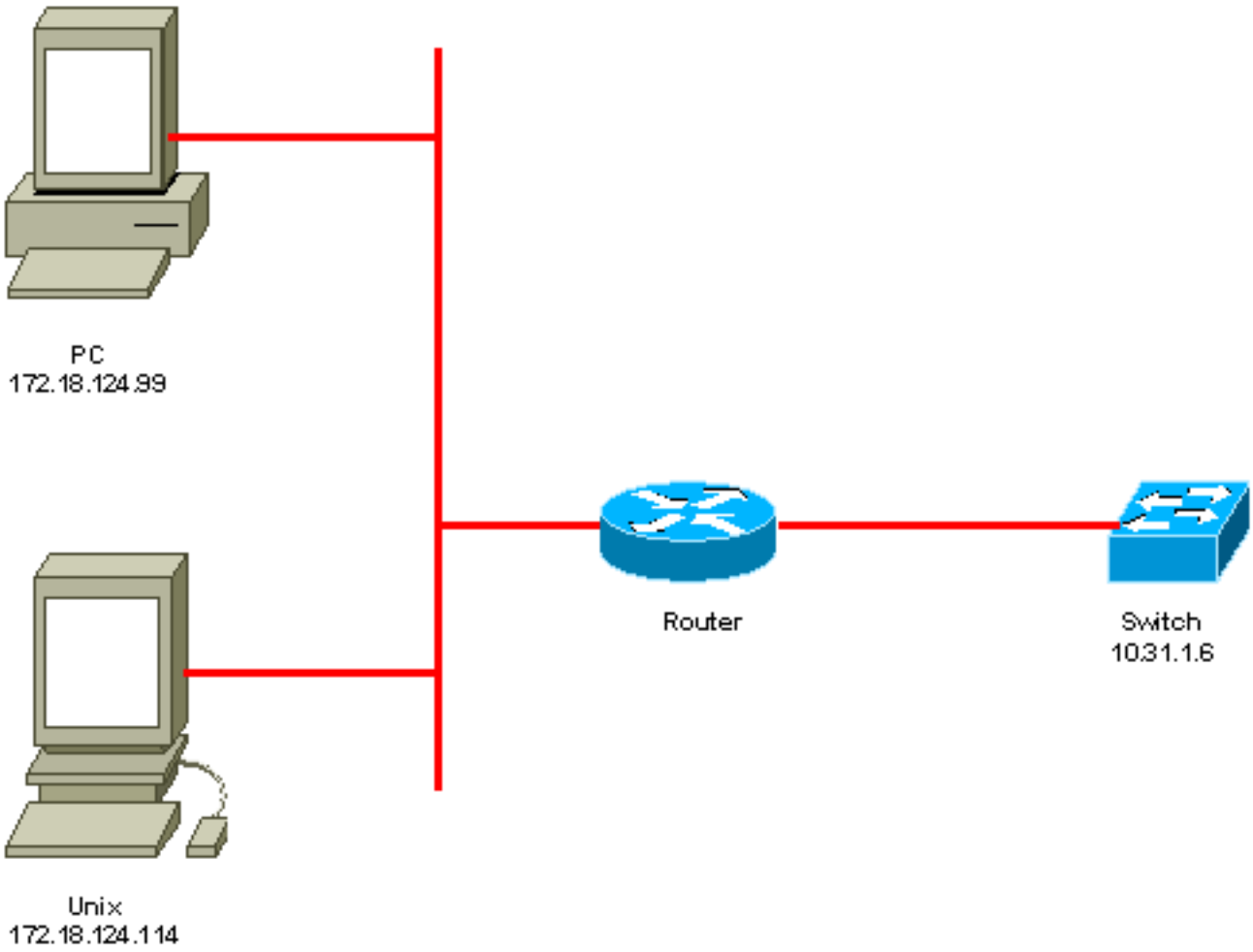
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn sich Ihr Netzwerk in der Produktionsumgebung befindet, müssen Sie sich bei jedem Befehl zunächst dessen potenzielle Auswirkungen vor Augen führen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Netzwerkdiagramm



Switch-Konfiguration

```
!--- 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
57733285367170478570985060663476874686971696394035244062067857533870155088852 5
69969147833053784006695698761020781095949864817996533001801084478586347277306 7
69718525641838624300188100883056124113738169282007867437605827557313344852933 2
19966820193013294709782680590633782154793854054981930616 51
```

```
!--- 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
---------------- ----------------- ------
```

Deaktivieren von SSH

In einigen Situationen kann es notwendig sein, SSH auf dem Switch zu deaktivieren. Sie müssen überprüfen, ob auf dem Switch SSH konfiguriert ist, und ihn deaktivieren, wenn dies der Fall ist.

Um zu überprüfen, ob SSH auf dem Switch konfiguriert wurde, geben Sie den Befehl **show crypto key (Verschlüsselungsschlüssel anzeigen**) ein. Wenn in der Ausgabe der RSA-Schlüssel angezeigt wird, wurde SSH auf dem Switch konfiguriert und aktiviert. Ein Beispiel ist hier dargestellt.

```
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
```

Um den Kryptografieschlüssel zu entfernen, geben Sie den Befehl **clear crypto key rsa** ein, um SSH auf dem Switch zu deaktivieren. Ein Beispiel ist hier dargestellt.

```
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)
```

debuggen im Catalyst

Um Debug-Vorgänge zu aktivieren, geben Sie den Befehl **set trace ssh 4** ein.

Um Debugging-Vorgänge zu deaktivieren, geben Sie den Befehl **set trace ssh 0** ein.

debug-Befehl Beispiele für eine gute Verbindung

Solaris zu Catalyst, Triple Data Encryption Standard (3DES), Telnet-Kennwort

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>
```

Katalysator

```
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 zu Catalyst, 3DES, Telnet-Passwort

Katalysator

```
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.
```

Authentifizierung von Solaris gegenüber Catalyst, 3DES, Authentifizierung, Autorisierung und Abrechnung (AAA)

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>
```

Katalysator

```
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.
```

debug-Befehl Beispiele für mögliche Fehler

Catalyst-Debugging mit Client Attempting [nicht unterstützt] Blowfish Cipher

```
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-Fehlerbehebung mit ungültigem Telnet-Kennwort

```
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-Debugging mit schlechter AAA-Authentifizierung

```
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
```

Fehlerbehebung

In diesem Abschnitt werden verschiedene Fehlerbehebungsszenarien im Zusammenhang mit der SSH-Konfiguration auf Cisco Switches behandelt.

Verbindung zum Switch über SSH nicht möglich

Problem:

Verbindung zum Switch über SSH nicht möglich.

Der Befehl **debug ip ssh** gibt folgende Ausgabe aus:

```
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
```

Lösung:

Dieses Problem tritt aus einem der folgenden Gründe auf:

- Neue SSH-Verbindungen schlagen nach dem Ändern des Hostnamens fehl.
- Für SSH wurden Schlüssel ohne Label (mit dem Router-FQDN) konfiguriert.

Die Lösung für dieses Problem:

- Wenn der Hostname geändert wurde und SSH nicht mehr funktioniert, setzen Sie den neuen Schlüssel auf Null, und erstellen Sie einen neuen Schlüssel mit der richtigen Bezeichnung.
  ```
  crypto key zeroize rsa
  crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
  ```
- Verwenden Sie keine anonymen RSA-Schlüssel (benannt nach dem FQDN des Switches). Verwenden Sie stattdessen beschriftete Tasten.
  ```
  crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
  ```

Um dieses Problem für immer zu beheben, aktualisieren Sie die IOS-Software auf eine der Versionen, in denen dieses Problem behoben ist.

Es wurde ein Fehler bezüglich dieses Problems gemeldet. Weitere Informationen finden Sie unter der Cisco Bug-ID CSCtc4114 **(nur für registrierte Kunden)** .

Zugehörige Informationen

- SSH-Support-Seite
- Konfigurieren von Secure Shell auf Routern und Switches mit Cisco IOS
- Bug-Toolkit
- Technischer Support – Cisco Systems

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.