SSH

Flaggor

-v = Verbose, använd vid felsökning
-O exit host.jehrlander.net = stänga master session mot hosten

error in libcrypto mot nätverksutrustning (Cisco)

Får man ex. `ssh_dispatch_run_fatal: Connection to 1.2.3.4 port 22: error in libcrypto` vid försök att SSHa kan det betyda att OS:et (i det här fallet Red Hat) inte längre accepterar SSH-koppel gentemot utrustning som har SSH-nycklar med gamla protokoll, ex. RSA.

För att komma runt problemet, generera istället nya SSH-nycklar. På ASA kan man göra det med ex. `crypto key generate ecdsa elliptic-curve 256` för att då istället använda ECDSA som krypteringsprotokoll. Verifiera med `show crypto key mypubkey ecdsa`.

SSH-Nyckel

SSH nycklar kan användas för att inte behöva slå användarnamn och lösenord. Man genererar ett nyckelpar, en privat och en publik nyckel. Den publika nyckeln distribuerar man till enheter man vill logga in på och den privata har man kvar på sin maskin och använder för autentisering. Det är viktigt att man skyddar den privata nyckeln med exempelvis lösenord.

Man skapar en ny nyckel med

```
ssh-keygen -t rsa -C "förnamn.efternamn@jehrlander.net"
```

Under skapande av nyckeln sätter man ett lösenord. Man kan sedan skicka den publika nyckeln till mottagande server med:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub jehrlander@10.0.0.5
```

Uppdatera sedan .ssh/config med IdentityFile (exempel finns nedan under config) eller SSH:a och specifisera nyckelfil genom `ssh -i ~/.ssh/<nyckelfil> <användarnamn>@<server>`.

Önskar man byta lösenord på sin SSH-nyckeln kan man göra det med `ssh-keygen -p -f ~/.ssh/id_rsa`.

config

SSH-konfig finns i filen `~/.ssh/config`. Redigera med textredigerare. Se exempelkonfiguration:

```
Match Host "rt-*,sw-*
 ! Matchar olika hostnamn

Host router
 Hostname router.jehrlander.net
 ! För att specifisera specifikt hostname
 User jehrlander
 ! Specifisera användare som används vid SSH-anrop
 IdentityFile ~/.ssh/ida_rsa
 ! Används SSH-nyckel för inlogg så pekar man ut den här
 KexAlgorithms +ssh-rsa
 ! Specifisera SSH-krypteringsalgoritmer. Använd + för att lägga till, använder man = så hårdkodar man istället och accepterar inget annat
 Ciphers=aes256-cbc,aes256-ctr
 Specifisera specifika cipher. Hårdkodat med =
 ProxyJump jumpserver.jehrlander.net
 ! Ska man använda en server som jumphost specifiserar man det man ProxyJump
 GSSAPIClientIdentity user@AD.JERHLANDER.NET
 ! Används kerberos för inloggning kan man specifisera det här. Kräver att man har en kerberosbiljett vid inloggning
```

Revision #6
Created 14 November 2025 11:28:24 by Jehrlander
Updated 9 March 2026 10:39:31 by Jehrlander