

Grunderna i SSH

Samuel Åkesson, Isac Bruce

Vad är SSH?

Vad är SSH?

Köra kommandon i skal/"terminal" på fjärrdator.

Vad är SSH?

Köra kommandon i skal/"terminal" på fjärrdator.

DEMO

Varför SSH (och inte ThinLinc, etc...)?

1. Beror på vad du behöver. Ibland räcker skalet.

Varför SSH (och inte ThinLinc, etc...)?

1. Beror på vad du behöver. Ibland räcker skalet.
2. Fjärrmaskinen har **ingen grafik** ("headless").

SSH-protokollet

- Använder port 22.
- Data som skickas är krypterad (därav *secure* shell).

Funktioner med SSH (utöver fjärrskal!)

- X-vidarebefordring (vi ljög!)

Funktioner med SSH (utöver fjärrskal!)

- X-vidarebefordring (vi ljög!)
- Filsystemsmontering

Funktioner med SSH (utöver fjärrskal!)

- X-vidarebefordring (vi ljög!)
- Filsystemsmontering
- Nätverkstunnling

Funktioner med SSH (utöver fjärrskal!)

- X-vidarebefordring (vi ljög!)
- Filsystemsmontering
- Nätverkstunnling
 - Portvidarebefordring

Funktioner med SSH (utöver fjärrskal!)

- X-vidarebefordring (vi ljög!)
- Filsystemsmontering
- Nätverkstunnling
 - Portvidarebefordring
 - SOCKS-tunnling

Funktioner med SSH (utöver fjärrskal!)

- X-vidarebefordring (vi ljög!)
- Filsystemsmontering
- Nätverkstunnling
 - Portvidarebefordring
 - SOCKS-tunnling
- Filöverföring

Hur sätter jag upp SSH på en fjärrdator?

OpenSSH!



Vad är OpenSSH?



- Mest populär SSH-server
- Öppen-källkod implementation av SSH-protokollet
- Kommer från OpenBSD

Demonstration!

Ansluta

- `ssh <användarnamn>@<fjärrdator>`

Ansluta

- `ssh <användarnamn>@<fjärrdator>`
- Validera fingeravtrycket!

Slipp lösenord- använd nyckelautentisering

1. Generera ssh-nyckel:

```
ssh-keygen
```

Slipp lösenord- använd nyckelautentisering

1. Generera ssh-nyckel:

```
ssh-keygen
```

2. Kopiera **publik**-nyckel till fjärrdator:

```
ssh-copy-id <användarnamn>@<fjärrdator>
```

Galna saker som kan göras med ssh

Reläad SSH-anslutning

Studsas via en annan dator

- `ssh -J <jumphost> <fjärrdator>`

Filöverföring

Överför enstaka filer:

- `scp <källa> <destination>` (Käll- och destinationsfil kan ligga antingen på lokal- eller fjärrdator!)

Filöverföring

Överför enstaka filer:

- `scp <källa> <destination>` (Käll- och destinationsfil kan ligga antingen på lokal- eller fjärrdator!)

Interaktiv filöverföring:

- `sftp <fjärrdator>`

Filöverföring

Överför enstaka filer:

- `scp <källa> <destination>` (Käll- och destinationsfil kan ligga antingen på lokal- eller fjärrdator!)

Interaktiv filöverföring:

- `sftp <fjärrdator>`

Montera filsystem:

- `sshfs <fjärrkatalog> <lokal_katalog>`

rsync

”Bättre” än scp. Varför?

rsync

”Bättre” än scp. Varför?

- Kan göra ”inkrementell överföring”. Överför endast det som har ändrats!

rsync

”Bättre” än scp. Varför?

- Kan göra ”inkrementell överföring”. Överför endast det som har ändrats!
- Tål att avbrytas, kan återuppta en halvfärdig överföring

rsync

”Bättre” än scp. Varför?

- Kan göra ”inkrementell överföring”. Överför endast det som har ändrats!
- Tål att avbrytas, kan återuppta en halvfärdig överföring

Överlag bättre lämpad att ”synka” strukturer, som namnet föreslår.

X-vidarebefordring

ssh -XC <fjärrdator>

- -X : grafisk vidarebefordring
- -C : komprimera data

Portvidarebefordring

Lokal- till fjärrport:

- `ssh -L <lokal_port>:localhost:<fjärr_port> <fjärrdator>`

Portvidarebefordring

Lokal- till fjärrport:

- `ssh -L <lokal_port>:localhost:<fjärr_port> <fjärrdator>`

Fjärr- till lokal port:

- `ssh -R <fjärr_port>:localhost:<lokal_port> <fjärrdator>`

Portvidarebefordring

Lokal- till fjärrport:

- `ssh -L <lokal_port>:localhost:<fjärr_port> <fjärrdator>`

Fjärr- till lokal port:

- `ssh -R <fjärr_port>:localhost:<lokal_port> <fjärrdator>`

Vidarebefordra port från en fjärr dator till en annan:

- `ssh -L <lokal_port>:<fjärrdator2>:<fjärr_port>
<fjärrdator1>`

Tunnling med SOCKS

Öppna en SOCKS-proxy till fjärrdatorn, på vald port i den lokala datorn.

- `ssh -D <port> <fjärrdator>`

Tunnling med SOCKS

Öppna en SOCKS-proxy till fjärrdatorn, på vald port i den lokala datorn.

- `ssh -D <port> <fjärrdator>`

I webbläsare kan man ange manuell proxy, och därmed tunnla **all trafik** i webbläsaren genom denna proxy.

Tunnling med SOCKS

Öppna en SOCKS-proxy till fjärrdatorn, på vald port i den lokala datorn.

- `ssh -D <port> <fjärrdator>`

I webbläsare kan man ange manuell proxy, och därmed tunnla **all trafik** i webbläsaren genom denna proxy.

(Fattigmans-VPN)

Köra enstaka fjärrkommandon

```
ssh <fjärrdator> -- <kommando>
```