SSH Basics / Training

SSH prakticky pro začátečníky

Adam Kalisz

adam.kalisz@notnullmakers.com

SSH Components

Client `ssh`   Server `sshd`

Connect

`ssh user@destination`   Like e-mail

Connect

```
ssh root@138.199.197.176
ssh abel@2a01:4f8:1c1b:63f3::1
ssh bob@training.notnullmakers.com
```

```
nnm-101-<user>
```

abel bob carmen dido elias fred gustav
hank ian jules karel luna mia nina
oleg paul quentin richard simon tomas
ursula vit walter xena yale zara adam
bert cameron david eva felix gabriel
hunter ivan jana kevin leo mark nadia
omar pablo qasim rose saul tara uma
vivian wren xavier yael zelda

nnm-101-<user>

Connect

The authenticity of host
'training.notnullmakers.com (138.199.197.176)'
can't be established.
ED25519 key fingerprint is
SHA256:M/kGWOSFAYtwK5qeYHZaxuFBhpGbK6xwXQmE1osyfAQ.
This key is not known by any other names.
Are you sure you want to continue connecting
(yes/no/[fingerprint])?

Keys

```
ssh-keygen -t ed25519 -C "training"
```

```
-> /home/user/.ssh/id_ed25519
-> /home/user/.ssh/id_ed25519.pub
```

More Keys

```
ssh-keygen -t ed25519 -C "training" \
  -f training_key -N ''
```

Authorized Keys

~/.ssh/authorized_keys

ssh-copy-id -i <pubkey> user@host

ssh-copy-id -i .ssh/id_ed25519 \
  <user>@training.notnullmakers.com

Authorized Keys

```
cat ~/.ssh/id_ed25519.pub | \
  ssh user@host "mkdir -p .ssh && \
  cat - >> .ssh/authorized_keys"
```

Known Hosts

~/.ssh/known_hosts
|1|+cerzND2aFOgYWkP2/HT41sQ0Lk=|
aCOFWYM9HhjeZTLif7G5I9Q6OdU= ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAID3JIjt4i+tq2If+QityO8pu+
Qv49VegOAuVtrIWzh7r
|1|OMbjux2v31Jap4mbBZeABYRMo1U=|
fEcByJzGBqFc1YX9eVEHdhQ2CHY= ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC1TLqUZsONda1wXuP98
nFZSuPODZhywuC6dzOVqgd9rrJk8x0+gDgpa8aWBfWP0oxMsA
Zw1mwDwj905L2tO013LTk...

Host Keys

/etc/ssh/ssh_host_ecdsa_key
/etc/ssh/ssh_host_ecdsa_key.pub
/etc/ssh/ssh_host_ed25519_key
/etc/ssh/ssh_host_ed25519_key.pub
/etc/ssh/ssh_host_rsa_key
/etc/ssh/ssh_host_rsa_key.pub

SSH Config

~/.ssh/config or /etc/ssh/ssh_config

```
Host europe
  HostName 138.199.197.176
  User <user>
  IdentityFile %d/.ssh/id_ed25519
  IdentitiesOnly yes
```

Connect Revisited

~~ssh root@162.55.58.201~~
~~ssh abel@2a01:4f8:1c1b:84b8::1~~
~~ssh bob@training.notnullmakers.com~~

`ssh europe`

SSH-Agent

`ssh-add ~/.ssh/id_ed25519`

`ssh-add -d ~/.ssh/id_ed25519`

Copy File To Remote Destination

```
scp <file> europe:~/<file>
```

Copy Files To Remote Destination

```
scp <file1> <file2> europe:~/
```

```
scp -pr <dir> europe:~/
```
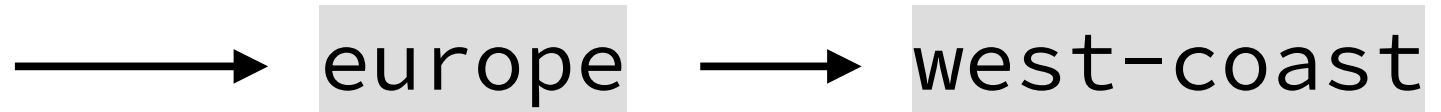
SFTP

Interactive or batched

Rsync

Saving data transfers

Piping Over SSH

```
cat, dd, tar
```

Training Setup

⟶ `europe` ⟶ `west-coast`

ProxyJump - Intermediary Host

```
ssh -J europe <user>@west-coast

-> west-coast in /etc/hosts
```

Tunneling over SOCKS

```
ssh -D 9999 -J europe \
  <user>@west-coast
```

Other Tunneling Options

- Local Port Forwarding (-L)
- Remote Port Forwarding (-R)

Only SFTP Server

In /etc/ssh/sshd_config

Subsystem sftp internal-sftp

Match Group sftponly

     ChrootDirectory /uploads

     ForceCommand internal-sftp

     PermitTunnel no

     X11Forwarding no

     AllowTcpForwarding no

Only SFTP Server Continued

```
groupadd sftponly
useradd -d /uploads -g sftponly \
  -s /sbin/nologin -M upload
mkdir -p /uploads/new
chown upload:sftponly /uploads/new
passwd upload


systemctl restart sshd
```

Forwarding and Reverse Proxying

- nftables - Network Address/ Port Translation
- nginx - Reverse proxy

Thank You

For later questions, feedback:

adam.kalisz@notnullmakers.com

NOT NULL
Makers