OpenSSH

Das neue Zeug

Der Leyrer

Chemnitzer Linux-Tage
22. und 23. März 2025

Trigger-Warnungen

- Österreicher
  - unverständliches Deutsch
  - DEnglisch
  - schwarzer, morbider Humor
  - Ich habe Meinungen
  - nicht markierter Sarkasmus
- Hohe Slide-Frequenz
  - Standardvortrag: 45 Minuten Redezeit + 10 Minuten für Fragen
  - 60 Slides

Leyrer

- Der Leyrer / Dem Leyrer sein …
- „Du Martin“ ist auch OK, Siezen verwirrt mich
- Sammelt alte Hardware (NeXTCube anyone?)
- Kommandozeilen und Linux „Affinität“
- 30+ Jahre in der IT, 40+ Jahre am Gerät
- Erstes Mal auf den CLT

Sven Guckes

Wiederholungs“täter“

(was SSH Talks betrifft)

GPN20: Besser leben mit SSH

https://media.ccc.de/v/gpn20-8-besser-leben-mit-ssh

GPN21: Noch besser leben mit SSH

https://media.ccc.de/v/gpn21-28-noch-besser-leben-mit-ssh

Lyrische Lesung des OpenSSH Changelogs

Chemnitzer Linux-Tage
22. und 23. März 2025

Das neue Zeug

- Dinge, die wegfallen
- Mehr Sicherheit
- Dateien kopieren (scp, sftp, ...)
- Netzwerk
- Config-File Verbesserungen
- Misc ssh(d)

Dinge, die wegfallen

DSA zur Compilezeit deaktiviert

- Digital Signature Algorithm (DSA) – 1991
  - 160 bit private key
  - SHA1 digest
- security level: 80 bits symmetric equivalent

OpenSSH 9.9
2024-09-19


Sun
SPARCstation 20

Kein MD5 Support mehr

- Message-Digest Algorithm 5 (MD5) – 1991
- kryptographische Hashfunktion
- 128-Bit-Hashwert
- keine Kollisionsresistenz seit 2004

OpenSSH 8.9
2022-02-23

Mehr Sicherheit

RequiredRSASize

- Minimum RSA key size (in bits)
- The default is 1024 bits.
- User und host-based authentication keys kleiner als das Limit werden abgelehnt.
- BSI TR-02102-1/2025-01: 3000 bit

OpenSSH 9.1
2022-10-04

Post-Quantum Key Exchange

- sntrup761x25519-sha512@openssh.com
- Hybrid ECDH/x25519 + Streamlined NTRU Prime post-quantum KEX
- Default seit OpenSSH 9.0 (2022-04-08)

OpenSSH 8.9
2022-02-23

ssh-agent: pin-required FIDO keys

- allow pin-required FIDO keys to be added to ssh-agent.
- $SSH_ASKPASS will be used to request the PIN at authentication time.

OpenSSH 8.9
2022-02-23

Besserer FIDO Support

- better handling for FIDO keys on tokens that provide user verification (UV) on the device itself, including biometric keys
- avoiding unnecessary PIN prompts.

OpenSSH 8.9
2022-02-23

RefuseConnection

- connections are terminated immediately after the first failed authentication attempt
- blocks further attempts from the same session
- mitigate brute-force attacks by disconnecting sources that exhibit repeated failed login attempts

OpenSSH 9.9
2024-09-19

RefuseConnection Syntax

```
sshd_config:
    RefuseConnection yes
    PerSourcePenalties refuseconnection:5  # or 5s
```

RefuseConnection Beispiel

```
sshd_config:
    PerSourcePenalties refuseconnection:10
    Match Address 192.168.1.*
        RefuseConnection yes
```

Match invalid-user

- matches when the target username is not valid on the server

OpenSSH 9.9
2024-09-19

Match invalid-user Beispiel

```
sshd_config:
    # Deny access for specific invalid users
    Match invalid-user
        DenyUsers admin wasadmin wpadmin
```

Dateien kopieren

Wechsel von scp/rcp zu SFTP

- scp nutzt nun SFTP anstelle des legacy scp/rcp Protokolls
- Kein „Double-Quoting“ mehr !!!
- Achtung bei Tilde („~“) Pfaden
- „scp -O“ machts wieder „alt“

OpenSSH 9.0
2022-04-08

scp/rcp und SFTP

- **R**emote **C**o**p**y – Remote Shell
- **S**ecure **C**o**p**y – Secure Shell
- **S**ecure **F**ile **T**ransfer **P**rotocol
  - resuming interrupted transfers
  - directory listings
  - remote file removal

Double Quoting in scp

- scp host:* .
- Wildcard wird über eine remote shell aufgelöst
- Shell-metazeichen müssen double-quoted werden, weil sie sonst remote als shell commandos interpretiert werden
- `scp remote.example.com:"\"rm\ -rf\ Datei\ \!\!\ \ \ \ \$USERNAME\ \*.doc\"" .`

No Bug-Compatibility

We consider the removal of the need for double-quoting shell characters in file names to be a benefit and do not intend to introduce bug-compatibility for legacy scp/rcp in scp(1) when using the SFTP protocol.

~ Pfade

- POSIX: ~name will expand to the home directory of user name
- "scp host:~user/file /tmp".
- Das SFTP Protokoll kann ~username pfade nativ nicht auflösen
- sftp-server(8) in OpenSSH 8.7 und neuer unterstützt die Protokollerweiterung "expand-path@openssh.com"

Exkurs: Tilde

- Tilde(~): spanisch tilde, von lateinisch titulus, Überschrift, Überzeichen
- POSIX: ~name will expand to the home directory of user name
- Aber warum?

Lear Siegler ADM-3A terminal

https://vintagecomputer.ca/lear-siegler-adm-3a-terminal/

SFTP: "copy-data" extension

- allow server-side copying of files/data
- Copy data from one handle to another on the server.
- The server SHOULD allow 'read-from-handle' and 'write-to-handle' to be the same handle as long as the range of data is not overlapping.
- https://datatracker.ietf.org/doc/html/draft-ietf-secsh-filexfer-extensions-00#section-7

OpenSSH 9.0
2022-04-08

scp remote-to-remote

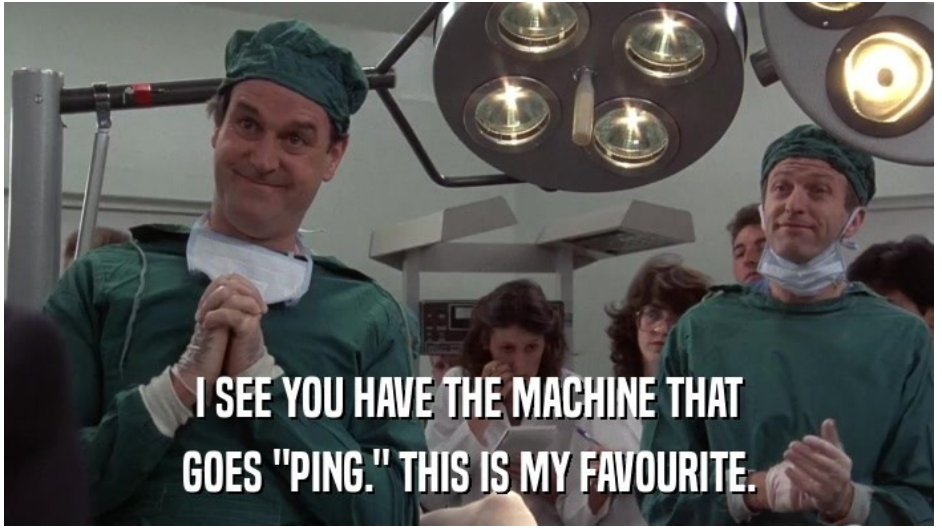
- scp host-a:/path host-b:
- Neuer Default: transfer through the local host
  - avoids the need to expose credentials on the origin hop
  - avoids triplicate interpretation of filenames by the shell
  - allows use of all authentication methods to the remote hosts
- Früher „-3“ Option
- Altes Verhalten: „-R“

OpenSSH 8.8
2021-09-26

Netzwerk

Transport-Level Ping

- SSH2_MSG_PING/ PONG
- advertised using a "ping@openssh.com" ext-info message



OpenSSH 8.8
2021-09-26

Forwarding UNIX Domain Sockets

- `-W host:port`
  - `Requests that standard input and output on the client be forwarded to host on port over the secure channel.`
- OpenSSH 9.4: Allow forwarding Unix Domain sockets via ssh -W

OpenSSH 9.4
2023-08-10

Channel Inactivity Timeouts

- Allows channels that have not seen traffic in a configurable interval to be automatically closed
- Different timeouts for
  - session
  - X11
  - agent
  - TCP forwarding

  channels

OpenSSH 8.8
2021-09-26

Channel Timeout Beispiel

```
sshd_config:
    # Drop Connections after 8 hours
    # monitors all channels separately
    ChannelTimeout *=8h
    # terminate connection after last channel closed
    UnusedConnectionTimeout 1m
```

Channel Timeout Beispiel

```
sshd_config:
    # Drop Connections after 8 hours
    # activity on any channel to reset the timeout
    global=8h
    # terminate connection after last channel closed
    UnusedConnectionTimeout 1m
```

Config-File Verbesserungen

SetEnv: „first-match-wins“

- Erinnerung: ssh(d)_config: Spezifisches zuerst, generisches am Ende

- first-match-wins wie auch andere Direktiven
- Früher: Letzter Wert gewinnt

OpenSSH 9.1
2022-10-04

Quotes in Match

- Processing of the arguments to the "Match" configuration directive now follows more shell-like rules for quoted strings
- including allowing nested quotes and \-escaped Characters

OpenSSH 9.9
2024-09-19

Match host Beispiel

```
Match host web exec "hostname -I | grep -qF 10.10.11."
    ForwardAgent yes
    ProxyCommand ssh -p 110 -q relay.example.com nc %h %p

Host web
    HostName web.example.com
    Port 1111
```

Include mit Environment Vars

- "Include" directive can now expand environment as well as the same set of %-tokens "Match Exec" supports.

OpenSSH 9.9
2024-09-19

Beispiele für Tokens und Env

- %h The remote hostname.
- %i The local user ID.
- %L The local hostname.
- %l The local hostname, including the domain name.
- %n The original remote hostname, as given on the command line.
- %p The remote port.
- %r The remote username.

- Arguments to some keywords can be expanded at runtime from environment variables on the client by enclosing them in ${}, for example ${HOME}/.ssh would refer to the user's .ssh directory.

Jump Host Token

- %j
- expands to the configured ProxyJump hostname
- empty string if not used
- CertificateFile, ControlPath, IdentityAgent, IdentityFile, Include, KnownHostsCommand, LocalForward, Match exec, RemoteCommand, RemoteForward, RevokedHostKeys, UserKnownHostsFile, VersionAddendum

OpenSSH 9.6
2023-12-18

Match localnetwork

- allows matching on the addresses of available network interfaces
- may be used to vary the effective client configuration based on network location

OpenSSH 9.4
2023-08-10

Match localnetwork Beispiel

```
Match Host ctf localnetwork 10.10.12.0/24
    HostName 10.10.12.4


Host ctf
    # External VPN address
    HostName 134.109.72.67
    User clt2025
    Identityfile ~/.ssh/id_cltctf
```

@-Parsing

- Make parsing user@host consistently **look for the last '@'** in the string rather than the first.
- This makes it possible to more consistently use usernames that contain '@' characters.

OpenSSH 9.9
2024-09-19

Identity Managment „Lösungen“

```
ssh pvwauser@account#xyz.com@target host
```

Tags

- Support for configuration tags "Tag" directive and corresponding "Match tag"
- used to select blocks of configuration

OpenSSH 9.4
2023-08-10

Tags Beispiel

```
#  For data center hosts
Match tagged ed_key
  Identityfile ~/.ssh/id_ed25519

# For AWS hosts
Match tagged aws_key
  IdentityFile ~/.ssh/aws_key

# force IPv4
Match tagged ip4
  AddressFamily inet
```

```
Host webserver
     Hostname web1.lan
     User mario
    Tag ed_key
    Tag ip4

Host ec2
    Hostname myec2.example.com
    Tag aws_key
```

Misc ssh(d)

sshd -G

- parses and prints the effective configuration
- **without** attempting to load private keys and perform other checks

OpenSSH 9.3
2023-03-15

sshd -V

- version option for sshd like the ssh client has

OpenSSH 9.2
2023-02-02

Exoten

- WAYLAND_DISPLAY environment variable (analog X11-DISPLAY)
- Notifying systemd on server listen and reload without using libsystemd

OpenSSH 9.8
2024-07-01

Exoten

- WAYLAND_DISPLAY environment variable (analog X11-DISPLAY)
- Notifying systemd on server listen and reload without using libsystemd

sshd: Zwei Binaries

- the server has been split into a listener binary, sshd(8), and a per-session binary "sshd-session"
- smaller listener binary
- support for disabling privilege separation and disabling re-execution of sshd(8) has been removed
- log messages will be tagged with "sshd-session" rather than "sshd"

OpenSSH 9.8
2024-07-01

Versionsüberblick

Linux Distribution	OpenSSH Version
Alpine Linux 3.21	9.9
Debian 11	8.4
Debian 12	9.2
Debian Unstable	9.9
Fedora 41	9.8
Ubuntu 25.04	9.9
OpenSuSE Leap 16.0	9.9
RHEL	8.7 (?)
NixOS	9.9

Fragen ?

- Martin Leyrer
- https://martin.leyrer.priv.at
- leyrer@23.social

Solange man selbst redet, erfährt man nichts.

– Marie Freifrau Ebner von Eschenbach, österreichische Schriftstellerin