OpenSSH server hardening

Effective configuration, access controls, authentication and operational verification

Start with effective configuration

OpenSSH reads sshd_config and any Include files, commonly /etc/ssh/sshd_config.d/*.conf. The first obtained value for many keywords wins, and Match blocks can override settings for selected connections. Editing a file does not prove the daemon uses the value you intended. Inspect the effective result for a representative connection.

Always keep a working administrative session and a console or out-of-band recovery path before changing remote authentication. Validate syntax before reloading; use a second connection to confirm success before closing the original.

```
sudo sshd -t
sudo sshd -T -C user=admin,host=example.net,addr=198.51.100.25
sudo systemctl reload ssh
```

Authentication policy

A typical key-only policy disables password and keyboard-interactive authentication while permitting public keys. If PAM TOTP is deliberately required, keyboard-interactive must be enabled and AuthenticationMethods can require publickey followed by keyboard-interactive:pam. Do not copy a key-only recipe into a TOTP deployment without understanding that distinction.

UsePAM yes is often retained for account and session handling even when password login is disabled. PermitRootLogin no removes direct root SSH login; administrators can use individual accounts with controlled sudo privileges. Verify the actual authentication path rather than relying on individual directive names.

```
PermitRootLogin no
PubkeyAuthentication yes
PasswordAuthentication no
KbdInteractiveAuthentication no
UsePAM yes
# For key-only access, inspect AuthenticationMethods too.
```

Restricting access

AllowUsers, AllowGroups, DenyUsers and DenyGroups can narrow who may connect. A user@host pattern can restrict source hosts, but its syntax and name-resolution behaviour require care. Network firewalls, VPNs and bastion hosts can reduce exposure further. A nondefault port may reduce background scanning but is not a meaningful substitute for authentication and patching.

Limit forwarding features where not needed. AllowTcpForwarding, X11Forwarding, PermitTunnel and AllowAgentForwarding are separate controls. Match blocks allow different restrictions for service accounts and administrators.

```
AllowGroups ssh-admins
X11Forwarding no
AllowAgentForwarding no
PermitTunnel no
# Validate forwarding requirements before disabling them.
```

Logging and rate controls

Monitor successful and failed authentication, unexpected account use and configuration changes. OpenSSH logs via syslog/journald depending on distribution. A firewall or rate limiter can help with noisy scanning, but indiscriminate bans can lock out legitimate administrators.

MaxAuthTries limits authentication attempts within a connection; LoginGraceTime limits the unauthenticated period. Neither replaces an access-control policy. Keep OpenSSH updated through the distribution's security maintenance process.

```
sudo journalctl -u ssh --since today
sudo sshd -T | grep -E "^(maxauthtries|logingracetime|passwordauthentication|permitrootlogin)
     "
```

Safe change procedure

Before changing access rules, record a known-good configuration, check whether cloud-init or configuration management owns any drop-ins, and test with sshd -t. Reload rather than restart where possible, then open a new session using the intended account and method. Confirm sudo still works if administrative access depends on it.

If a Match rule is present, test the precise username and source address using sshd -T -C. Document exceptions for automation; a blanket interactive TOTP requirement can break scheduled tasks unless a separate restricted mechanism is designed.

```
sudo cp -a /etc/ssh/sshd_config /etc/ssh/sshd_config.before-change
sudo sshd -t && sudo systemctl reload ssh
sudo sshd -T -C user=admin,host=example.net,addr=198.51.100.25
```

Reference scope: commands and defaults vary by distribution and software version. Consult the locally installed manual pages for exact syntax and behaviour.