SSH Restricted Access - Sicherheitsimplementierung

Höchste Sicherheit für Traceroute-Ausführung

Kernmerkmale der Lösung:

- **Strikte Zugriffskontrolle:** NUR Ansible Controller (10.1.2.3) erlaubt
- **OpenSSH 7.2+ restrict:** Modernste Sicherheitsmechanismen
- **Keine Admin-Rechte:** Traceroute läuft als eingeschränkter Benutzer
- **Validierung:** Nur 10.x.x.x Ziele erlaubt, CSV-Output
- **Defense-in-Depth:** Mehrschichtige Sicherheitsarchitektur

Berechtigungsmatrix:

Aufgabe	Ansible-Playbook Ausführung	Traceroute-Ausführung
Benutzer	Admin mit sudo-Zugriff	traceuser (eingeschränkt)
Privilegien	Volle sudo (root)	**KEINE Admin-Rechte!**
SSH-Zugriff	Beliebige IP, Passwort/Key	**NUR 10.1.2.3**, nur Key + forced cmd
Zweck	Deployment/Konfiguration	Ausschließlich traceroute/mtr

Sicherheitsprinzipien:

Prinzip	Umsetzung
Root-Besitz verhindert Privilege Escalation	Alle kritischen Dateien gehören root
Gruppenbasierte Zugriffskontrolle	tracegroup für lesenden Zugriff
Principle of Least Privilege	Minimale Rechte für jeden Prozess

OS-Sicherheit mit authorized_keys

authorized_keys Konfiguration

```
# NUR Ansible Controller (10.1.2.3) ist erlaubt!
restrict,no-port-forwarding,no-X11-forwarding,no-agent-forwarding,
no-pty,from="10.1.2.3",command="/usr/local/bin/tracersh" <public-key>
```

OpenSSH Sicherheitsebenen:

Option	Funktion	Sicherheitsvorteil
restrict	Master-Schalter (ab OpenSSH 7.2)	Deaktiviert ALLE gefährlichen Features
from="10.1.2.3"	IP-Whitelist	**Exakte IP-Prüfung, keine Netze!**
command="..."	Forced Command	Überschreibt jeden Client-Befehl
no-pty	Kein Pseudo-Terminal	Verhindert interaktive Sessions
no-port-forwarding	Kein TCP/UDP Forwarding	Verhindert Tunnel/Pivoting
no-X11-forwarding	Kein X11	Keine GUI-Weiterleitung
no-agent-forwarding	Kein SSH-Agent	Verhindert Key-Weitergabe

Dateisystem-Härtung:

Pfad	Besitzer:Gruppe	Rechte	Sicherheitszweck
/home/traceuser	root:tracegroup	750	User kann Home nicht ändern
~/.ssh/	root:tracegroup	750	SSH-Config unveränderlich
~/.ssh/authorized_keys	root:tracegroup	640	Nur lesbar via Gruppe
/usr/local/bin/tracersh	root:root	755	Systemweit, unveränderlich
/var/log/tracersh.log	root:tracegroup	660	Audit-Log (optional)

Bash-Script Sicherheitsimplementierung

Vollständige Sicherheitsanforderungen im tracersh Script:

Anforderung	Implementierung	Zeile
Umgebungssäuberung	LC_ALL=C LANG=C	16
Sicheres IFS	IFS=$'\n\t'	17
Fester PATH	PATH='/usr/sbin:/usr/bin:/sbin:/bin'	18
Variablen-Bereinigung	unset BASH_ENV ENV CDPATH	19
Alias-Entfernung	unalias -a	20
Strict Mode	set -euo pipefail	39
Input-Validierung	Regex ^10\.\d+\.\d+\.\d+$	354
Command Injection Schutz	awk '{print $1}' Extraktion	344
Timeout-Schutz	timeout –kill-after=5s 60s	375
Signal-Behandlung	trap für HUP, INT, TERM	391
Read-only Variablen	readonly Deklarationen	42-98

Zugriffskontroll-Logik:

- Keine SSH_CLIENT → "Nur SSH erlaubt"
- SSH mit TTY ohne Befehl → Verweigert
- SSH ohne ORIGINAL_COMMAND → Verweigert
- Ungültige IP → "# input invalid: <ip>"
- Nur erstes Wort wird verarbeitet
- Keine Shell-Expansion möglich

Sicherheitsarchitektur und Verbindungsablauf

Kompletter Sicherheitsablauf:

Schritt	Komponente	Prüfung	Aktion bei Fehler
1	Ansible Controller	Initiiert SSH-Verbindung	-
2	OpenSSH Server	from="10.1.2.3"prüfen	Connection refused
3	OpenSSH Server	Public-Key Auth	Permission denied
4	OpenSSH Server	restrict + no-* Optionen	Features deaktiviert
5	OpenSSH Server	command=/usr/local/bin/tracersh"	Forced execution
6	tracersh Script	SSH_CLIENT vorhanden?	"Nur SSH erlaubt"
7	tracersh Script	SSH_ORIGINAL_COMMAND?	"Nur traceroute erlaubt"
8	tracersh Script	Target = 10.x.x.x?	"# input invalid: <ip>"
9	tracersh Script	Tool verfügbar?	Fallback oder Error
10	System	traceroute/mtr mit Timeout	Timeout nach 60s
11	tracersh Script	Parse zu CSV	Error message
12	OpenSSH Server	Output an Client	Connection closed

Testabdeckung: ansible-playbook -i "host,"test.yml

Testbereich	Abdeckung	Prüfung
Konnektivität	SSH-Verbindung, Schlüssel-Auth	Nur 10.1.2.3 kann sich verbinden
Befehlsausführung	Gültige/ungültige Targets	Nur 10.x.x.x IPs werden akzeptiert
Sicherheitsrestriktionen	Verbotene Befehle, Shell-Zugriff	Keine interaktive Shell möglich
Fehlerbehandlung	Timeouts, fehlende Tools	60s Timeout, Fallback zu mtr
Idempotenz	Mehrfache Ausführungen	Keine Seiteneffekte bei Wiederholung