Wie richte ich meine VM für authentifizierte Schwachestellenscans ein?

03.07.2024 14:17:14

FAQ-Artikel-Ausdruck

Kategorie:	Server-Dienste::Enterprise Cloud	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	en	**Letzte Aktualisierung:**	10:57:22 - 26.03.2024

Lösung (öffentlich)

Wie richte ich meine VM für authentifizierte Schwachestellenscans ein?

Auf Linux-Systemen ist dazu ein normales Nutzer-Login (ohne root-Rechte) erforderlich. Die Authentifizierung erfolgt mit einem auf dem GSM Server gespeicherten SSH-Schlüssel. Alle VMs des Service Levels PaaS, sowie nach dem 11.05.2018 bereitgestellte VMs des Service Levels IaaS, verfügen bereits seit dem Zeitpunkt ihrer Erstellung über das nötige Benutzer-Login: zih-gsm. Auf Linux-VMs des Service Levels IaaS, die vor dem 11.05.2018 erstellt worden sind, kann durch einfache Installation eines zusätzlichen Softwarepakets das Login nachträglich eingerichtet werden:

- Debian/Ubuntu: [1]credential-zih-gsm.deb
SHA256 Checksum:
1abf6cb7ec7648c513e928b294fa744a5bac71e8cd2c0560c3840cdf8d010555
- SUSE / RedHat / CentOS: [2]credential-zih-gsm.rpm
SHA256 Checksum:
c3d197429f81c8587adb36d2911072a023327bf54b42bf101e37e94d13cb3414

Alternativ kann das Login auch manuell erstellt werden - bspw. durch das Kommando adduser zih-gsm. Anschließend muss der folgende öffentliche SSH-Schlüssel im HOME-Verzeichnis des Nutzers unter ~/.ssh/authorized_keys gespeichert werden:

[3]credential-zih-gsm.pub
SHA256 Checksum:
8d0edcef351bf767a4bdf62c7b589fdc1f0b97e3c8fb02bf03d7908b2b0f454a

Das ZIH empfiehlt, diesen Check auf allen selbst verwalteten IaaS-VMs einzurichten. Für Windows VMs ist ein authentifizierter Schwachstellenscan derzeit noch nicht möglich.

[1] https://wwwpub.zih.tu-dresden.de/~jurenz/pub/faq/downloads/credential-zih-gsm.deb
[2] https://wwwpub.zih.tu-dresden.de/~jurenz/pub/faq/downloads/credential-zih-gsm.rpm
[3] https://wwwpub.zih.tu-dresden.de/~jurenz/pub/faq/downloads/credential-zih-gsm.pub