How do I set up my VM for authenticated vulnerability scanning?

03.07.2024 14:17:24

FAQ-Artikel-Ausdruck

Kategorie:	Server-Dienste::Enterprise Cloud	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	en	**Letzte Aktualisierung:**	10:59:56 - 26.03.2024

Lösung (öffentlich)

How do I set up my VM for authenticated vulnerability scanning?

On Linux systems, a normal user login (without root privileges) is required. The authentication is done with a SSH key stored on the GSM server. All VMs of the service level PaaS, as well as VMs of the service level IaaS provided after 11.05.2018, already have the necessary user login since the time of their creation: zih-gsm. On Linux VMs of the IaaS service level that were created before May 11, 2018, the login can be set up subsequently by simply installing an additional software package:

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

Alternatively, the login can also be created manually - for example with the command adduser zih-gsm. Then the following SSH public key must be stored in the user's HOME directory under ~/.ssh/authorized_keys:

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

ZIH recommends that this check be set up on all self-administered IaaS VMs. For Windows VMs, an authenticated vulnerability scan is currently not yet possible.

[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