FORSCHUNGSZENTRUM JÜLICH GmbH

Jülich Supercomputing Centre

Beratung und Betrieb, ☎ (02461) 61-6440

Technische Kurzinformation

FZJ-JSC-TKI-0420

P. Matzerath
E. Gerzen

16.09.2024

Installation und Konfiguration des Nessus-Agents

Einleitung

Für eine Freischaltung an der zentralen JuNet-Firewall muss der Sicherheitszustand des Rechnersystems in regelmäßigen Abständen geprüft werden (vgl. https://go.fzj.de/fw). Im Rahmen seiner Aufgaben im IT-Sicherheitsprozess des Forschungszentrums nutzt das JSC dazu Produkte der Firma Tenable, unter anderem den Nessus Schwachstellen Scanner. Die vorliegende Kurzinformation beschreibt die Installation und Konfiguration des Nessus Agents, der als lokaler Schwachstellen Scanner eingesetzt wird.

Beschreibung des Nessus Agent

Nessus Agents sind lokale Schwachstellenscanner, die direkt auf einem System installiert werden und dort die notwendigen Tests ausführen. Die aktuelle Version des Nessus Agents ist 10.7.3. Tabelle 1 im Anhang listet die unterstützten Betriebssysteme.
Der Ressourcenverbrauch des Scanners auf einem lokalen System ist eher gering einzuschätzen. Der Nessus Agent nutzt 0% der CPU-Leistung, außerhalb der Scan Zeiten. Während eines Scans kann er aber durchaus die volle Leistung beanspruchen, sofern die Systemauslastung es erlaubt. Die Plugins belegen 300 MB Festplattenspeicher. Die Festplattennutzung kann auf 2 GB anwachsen, wenn unter bestimmten Bedingungen Plugin-Quellcode dekomprimiert gespeichert werden muss. Minimale Anforderungen an die unterstützte Hardware sind in Tabelle 2 des Anhangs dokumentiert.
Weitere Leistungsdaten des Agents können auf den folgenden Webseiten eingesehen werden:
Tenable - Software Footprint
Tenable - Host System Utilization

Installation

Laden Sie zur Installation das passende Paket entweder vom PCSRV[1] direkt von der Herstellerseite[2].

Die verschiedenen Linux Derivate nutzen zur Installation das systemeigene Paketverwaltungssystem.

Linux-Derivat	Installationsbefehl
Ubuntu, Debian	dpkg -i NessusAgent-<version>-<os>.deb
Red Hat, CentOS, etc.	rpm -ivh NessusAgent-<version>-<os>.rpm

Windows und macOS Betriebssysteme installieren über die graphischen Installations Wizzards.

Konfiguration

Die Konfiguration des Nessus Agents erfolgt automatisch über den Nessus-Manager. Dazu muss sich jeder Agent an den Manager binden. Die notwendigen Details, hier in spitzen Klammern angegeben, werden Ihnen per E-Mail gesondert mitgeteilt.

Betriebssystem	Kommando
Linux	/opt/nessus_agent/sbin/nessuscli agent link --key=<k> --name=<n> --groups=<g> --host=<h> --port=<p>
macOS	sudo /Library/NessusAgent/run/sbin/nessuscli agent link --key=<k> --name=<n> --groups=<g> --host=<h> --port=<p>

Bei einer Installation unter einem Microsoft Windows Betriebssystem werden die Informationen direkt nach der Installation abgefragt.
Nachdem Nessus Agent und Nessus Manager erfolgreich miteinander verbunden sind, erfolgt ein Update der Schwachstellendefinitionen. Die Schwachstellenprüfung erfolgt einmal wöchentlich, außerhalb der typischen Bürozeiten und sollte binnen 24 Stunden abgeschlossen sein. Aufgrund der gewählten Startzeit sollte der tägliche Serverbetrieb nahezu nicht beeinflusst sein.

FAQ

Welche Vorteile bietet der Einsatz des Nessus Agents?

Nessus Agents bieten für Standardschwachstellenscans verschiedene Vorteile:

- Eine Benutzerverwaltung für Credentialed Scans entfällt
- Nessus Agents können per Orchestrierung ausgerollt werden
- Scans können auch offline laufen
- Konfiguration einer lokalen Firewall entfällt
- Agent nutzt nur eine geringe Netzwerkbandbreite
- sehr einfache Installation und Nutzung

[1] \\pcsrv.zam.kfa-juelich.de/public/Nessus-Agent
[2] https://www.tenable.com/downloads/nessus-agents

Anhang

Tabelle 1: Unterstützte Betriebssysteme

Betriebssystem	Unterstützte Versionen
Linux	Amazon Linux 2 (x86_64, AArch64) Amazon Linux 2023 CentOS Stream 9 (x86_64) Kali Linux 2017, 2018, 2019, and 2020 (i386) Debian 11 and 12 / Kali Linux 2017, 2018, 2019, and 2020 (x86_64) Fedora 38 and 39 (x86_64) Red Hat ES 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) (x86_64) Red Hat ES 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) (AArch64, Graviton2) Red Hat ES 8 and 9 / AlmaLinux 8 and 9 / Oracle Linux 8 and 9 (including Unbreakable Enterprise Kernel) / Rocky Linux 8 and 9 (x86_64) Red Hat ES 8 and 9 / AlmaLinux 8 and 9 / Oracle Linux 8 and 9 (including Unbreakable Enterprise Kernel) / Rocky Linux 8 and 9 (AArch64, Graviton2) SUSE Enterprise 12 SP5, 15 SP2 and later (x86_64) TencentOS (x86_64) Ubuntu 16.04, 18.04, 20.04, 22.04, and 24.04 (x86_64) Ubuntu 18.04, 20.04, 22.04, and 24.04 (AArch64, Graviton2)
Windows[3]	Windows 10 (x86) Windows 10 and 11 (x86_64) Windows Server 2012, 2012 R2, 2016, 2019, and 2022 (x86_64)
macOS	macOS 12, 13, and 14 (x86_64) macOS 12, 13, and 14 (Apple Silicon)

[3] Nessus Agent ab Version 8.2.0 benötigt das Microsoft Universal C Runtime Library (UCRT) auf allen Microsoft Betriebssystemen.

Tabelle 2 Minimale Hardware Anforderungen

Hardware	**Min. Anforderung**
Prozessor	1 Dual Core CPU
Taktfrequenz	> 1 GHz
RAM	> 1 GB
Festplattenkapazität	> 2GB
Festplattengeschwindigkeit	15 – 50 IOPs