Nessus Agent Cheatsheet

Last Updated: July 25, 2023

Table of Contents

Tenable Nessus Agent Cheatsheet

Benefits and Limitations of Using Tenable Nessus Agents

Benefits

- Provides extended scan coverage and continuous security:
    - Can deploy where it's not practical or possible to run network-based scans.
    - Can assess off-network assets and endpoints that intermittently connect to the internet (such as laptops). Tenable Nessus Agents can scan the devices regardless of network location and report results back to the manager.
- Eliminates the need for credential management:
    - Doesn't require host credentials to run, so you don't need to manually update credentials in scan configurations when credentials change, or share credentials among administrators, scanning teams, or organizations.
    - Can deploy where remote credentialed access is undesirable, such as Domain Controllers, DMZs, or Certificate Authority (CA) networks.
- Efficient:
    - Can reduce your overall network scanning overhead.
    - Relies on local host resources, where performance overhead is minimal.
    - Reduces network bandwidth need, which is important for remote facilities connected by slow networks.
    - Removes the challenge of scanning systems over segmented or complex networks.
    - Minimizes maintenance, because Tenable Nessus Agents can update automatically without a reboot or end-user interaction.
    - Large-scale concurrent agent scans can run with little network impact.
- Easy deployment and installation:
    - You can install and operate Tenable Nessus Agents on all major operating systems.
    - You can install Tenable Nessus Agents anywhere, including transient endpoints like laptops.

    - You can deploy Tenable Nessus Agents using software management systems such as Microsoft's System Center Configuration Manager (SCCM).

Limitations

- Network checks — Agents are not designed to perform network checks, so certain plugin items cannot be checked or obtained if you deploy only agent scans. Combining traditional scans with agent-based scanning eliminates this gap.
- Remote connectivity — Agents miss things that can only specifically be performed through remote connectivity, such as logging into a DB server, trying default credentials (brute force), traffic-related enumeration, etc.

System Requirements for Tenable Nessus Agents

For dataflow and licensing requirements, refer to the System Requirements section.

Hardware

Tenable Nessus Agents are lightweight and only use minimal system resources. Generally, a Tenable Nessus Agent uses 40 MB of RAM (all pageable). A Tenable Nessus Agent uses almost no CPU while idle, but is designed to use up to 100% of CPU when available during jobs.

For more information on Tenable Nessus Agent resource usage, refer to Software Footprint and Host System Utilization.

The following table outlines the minimum recommended hardware for operating a Tenable Nessus Agent. Tenable Nessus Agents can be installed on a virtual machine that meets the same requirements specified.

Hardware	Minimum Requirement
Processor	1 Dual-core CPU
Processor Speed	> 1 GHz
RAM	> 1 GB
Disk Space	• Agents 8.0.x and later: > 3 GB, not including space used by the host operating system • Agents 10.0.x and later: > 2 GB, not including space used by the host operating system The agent may require more space during certain processes, such as a `plugins-code.db` defragmentation operation.
Disk Speed	15-50 IOPS

Software

To view the Tenable Nessus Agent software requirements, see Tenable Nessus Agent Software Requirements.

Installing and Linking Tenable Nessus Agents

The following installation instructions are for the command line. To install using the user interface, see Install Tenable Nessus Agents.

Linux

Install the package:

Red Hat, CentOS, and Oracle Linux

dnf install NessusAgent-10.3.1-es8.x86_64.rpm

Fedora

dnf install NessusAgent-10.3.1-fc34.x86_64.rpm

Ubuntu

dpkg -i NessusAgent-<version number>-ubuntu1110_i386.deb

Debian

dpkg -i NessusAgent-<version number>-debian6_amd64.deb

> **Note:** After installing an agent, you must manually start the service using the command **`/sbin/service nessusagent start`**.

Link Agent to Tenable Nessus Manager or Tenable Vulnerability Management:

At the command prompt, use the`nessuscli agent link` command. For example:

```
/opt/nessus_agent/sbin/nessuscli agent link
--key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
--name=MyOSXAgent --groups="All" --host=yourcompany.com --port=8834
```

Windows

You can deploy and link Tenable Nessus Agents via the command line. For example:

```
msiexec /i NessusAgent-<version number>-x64.msi NESSUS_GROUPS="Agent Group Name"
NESSUS_SERVER="192.168.0.1:8834" NESSUS_
KEY=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00 /qn
```

macOS

Install the package:

1. Extract `Install Nessus Agent.pkg` and `.NessusAgent.pkg` from `NessusAgent-<version number>.dmg`.

   > **Note:** The `.NessusAgent.pkg` file is normally invisible in macOS Finder.

2. Open Terminal.
3. At the command prompt, enter the following command:

   ```
   # sudo installer -pkg /<path-to>/Install Nessus Agent.pkg -target /
   ```

Link Agent to Tenable Nessus Manager or Tenable Vulnerability Management:

1. Open Terminal.
2. At the command prompt, use the `nessuscli agent link` command.

   For example:

   ```
   # sudo /Library/NessusAgent/run/sbin/nessuscli agent link
   --key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
   --name=MyOSXAgent --groups=All --host=yourcompany.com --port=8834
   ```