Nessus Agent Cheatsheet

Last Updated: October 04, 2018

Table of Contents

Nessus Agent Cheatsheet

Benefits and Limitations of Using 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). 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 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 Nessus Agents on all major operating systems.
  - You can install Nessus Agents anywhere, including transient endpoints like laptops.
  - You can deploy 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 plugins 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 Nessus Agents

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

Hardware

Nessus Agents are designed to be lightweight and to use only minimal system resources. Generally, a Nessus Agent uses 40 MB of RAM (all pageable). A 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 Nessus Agent resource usage, refer to Software Footprint and Host System Utilization.

The following table outlines the minimum recommended hardware for operating a Nessus Agent. 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	< 1 GB
Disk Speed	15-50 IOPS

Software

Operating System	Supported Versions
Linux	Debian 7, 8, and 9- i386 Debian 7, 8, and 9 - AMD64 Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - i386 Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - x86_64 Red Hat ES 7 / CentOS 7 / Oracle Linux 7 - x86_64

Operating System	Supported Versions
	Fedora 24 and 25 - x86_64 Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04, and 16.04 - i386 Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04, and 16.04 - AMD64
Windows	Windows 7, 8, and 10 - i386 Windows Server 2008, Server 2008 R2, Server 2012, Server 2012 R2, Server 2016, 7, 8, and 10 - x86-64
Mac OS X	Mac OS X 10.8 - 10.13

Installing and Linking Nessus Agents

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

Linux

Install the package:

Red Hat, CentOS, and Oracle Linux

rpm -ivh NessusAgent-<version number>-es6.i386.rpm
rpm -ivh NessusAgent-<version number>-es5.x86_64.rpm

Fedora

rpm -ivh NessusAgent-<version number>-fc20.x86_64.rpm

Ubuntu

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

Debian

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

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

Link Agent to Nessus Manager or Tenable.io:

At the command prompt, use the 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 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
```

Mac OS X

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:

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

Link Agent to Nessus Manager or Tenable.io:

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

   For example:

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