Nessus Agent
Large Scale Deployment Guide

Last Revised: July 11, 2018

Table of Contents

Introduction

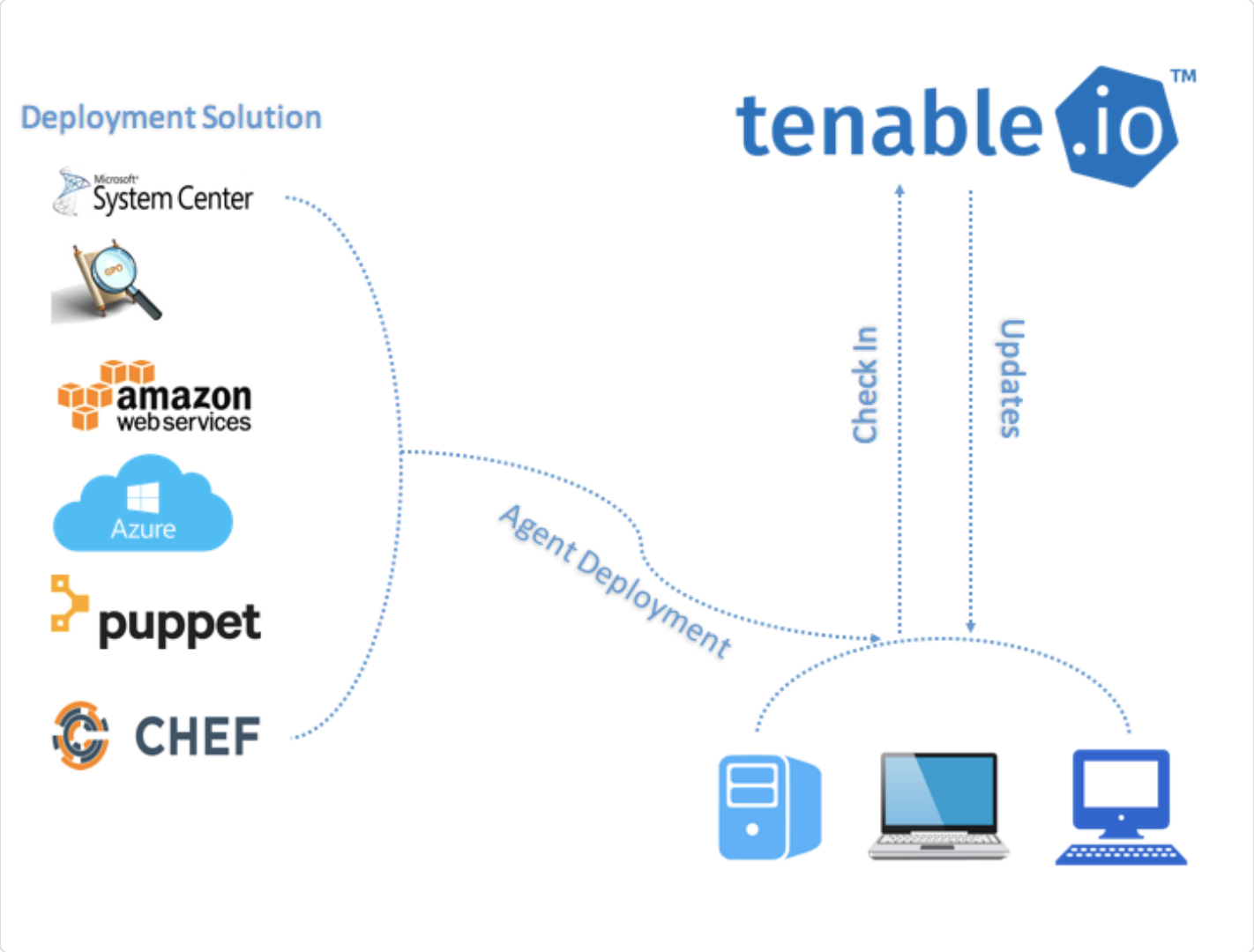
For customers that plan on deploying a multitude of Nessus Agents across their environment, a large scale deployment strategy is required to ensure all Nessus Agents are continuously active and stay connected to Tenable.io or Nessus Manager.

System Requirements

Document Name
Nessus Agent Hardware Requirements
Nessus Agent Software Requirements
Dataflow Requirements

Deployment Strategy

It is possible to deploy agents utilizing software capable of pushing agents through the network. The following diagram illustrates the architecture of a large scale deployment using third-party software:



Additionally, you should deploy batches of agents over a period of 24 hours when deploying a large amount of agents. This prevents the agents from attempting a full plugin set update at the same time. After an agent is initially installed and gets its first plugin update, it sets its timer to attempt the next update 24 hours from that time. As a result, if you deploy 10,000 agents all at once, all of those agents would attempt a full plugin set download at the same time each day, resulting in an excessive amount of bandwidth utilization.

Scan Profile Strategy

Before you deploy agents, develop a scanning strategy that best fits your environment.

Document Name
Tenable Scan Strategy - Tenable Professional Services

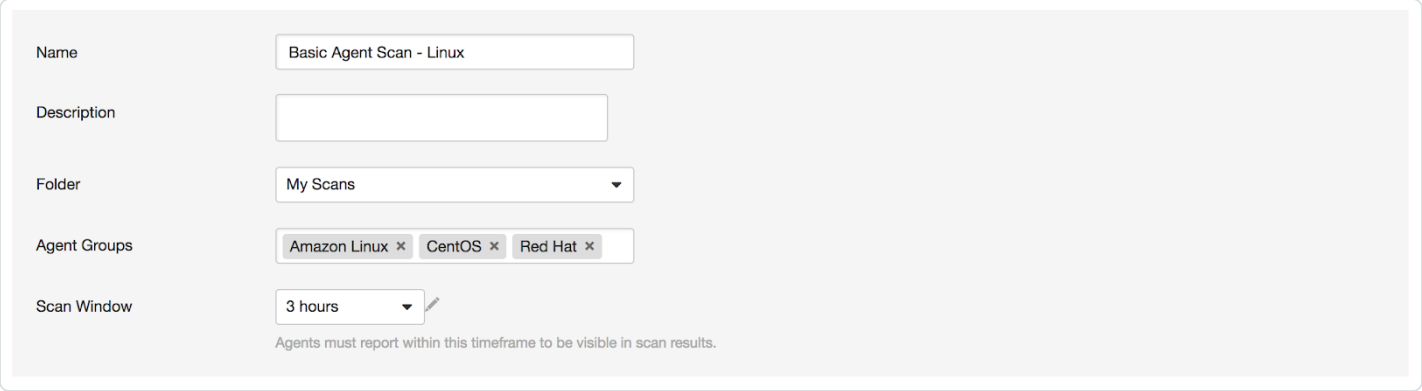
The following are examples on how to build agent scans around an applicable scan strategy.

Operating System Scan strategy

The following strategy is useful if your scanning strategy is based off of the operating system of an asset.

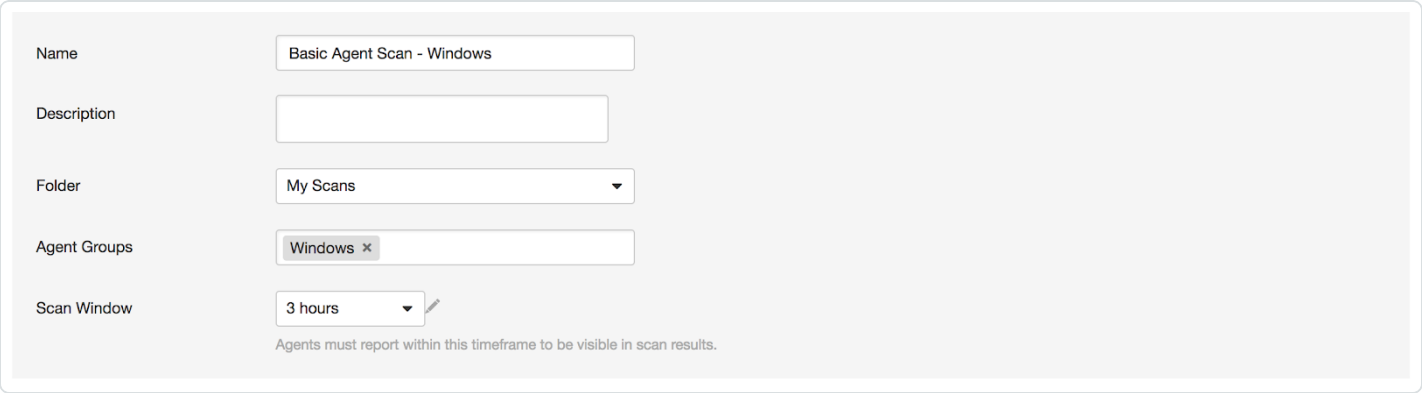
Basic Agent Scan - Linux

In this example, a scan is created based on the **Basic Agent Scan** template, and is assigned the group *Amazon Linux*, *CentOS*, and *Red Hat*. This scan will only scan these assets.



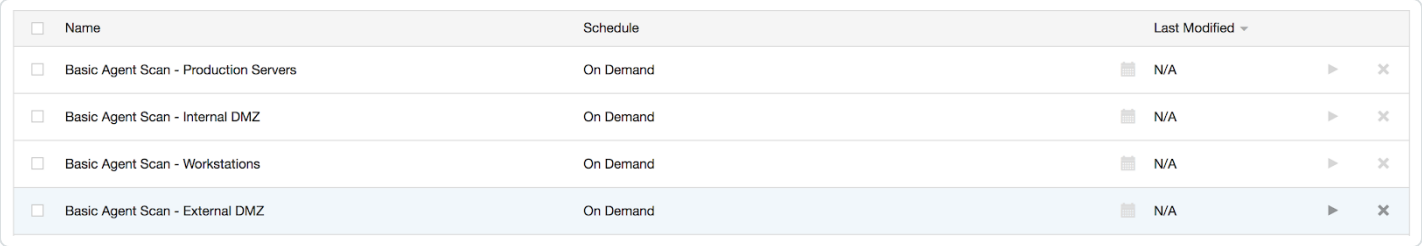
Basic Agent Scan - Windows

In this example, a scan is created based on the **Basic Agent Scan** template, and is assigned the group *Windows*. This scan will only scan Windows assets.



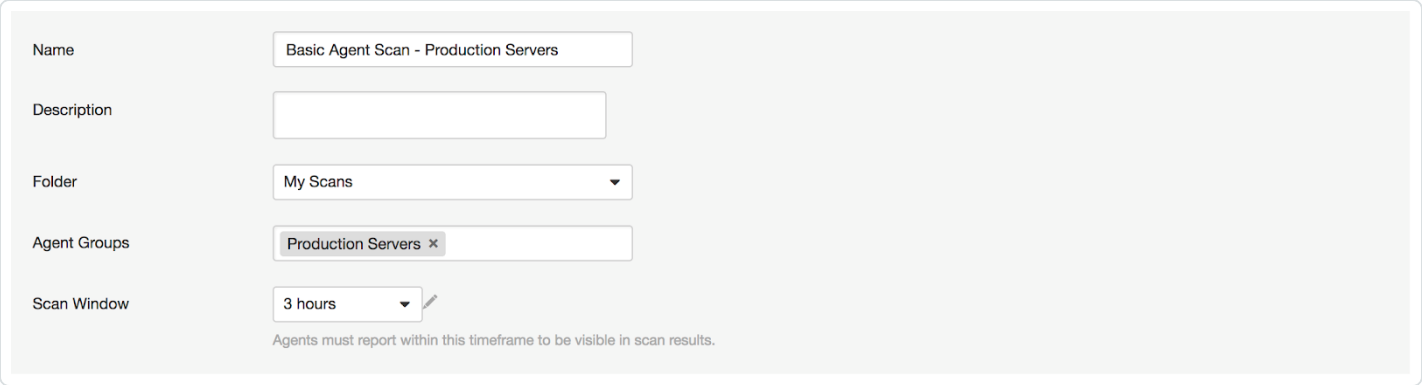
Asset Type or Location Scan Strategy

The following strategy is useful if your scanning strategy is based off of the asset type or location of an asset.



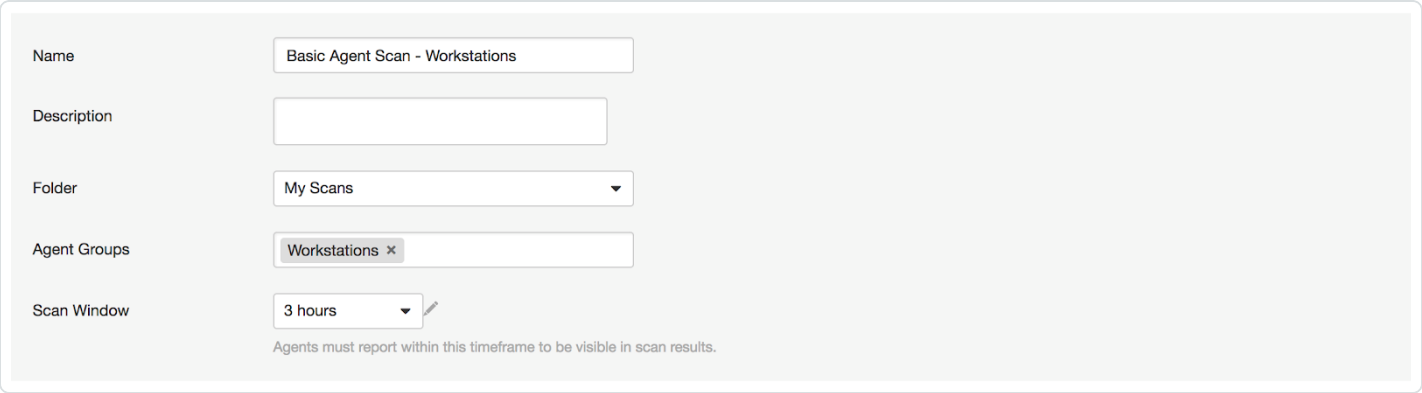
Basic Agent Scan - Production Servers

In this example, a scan is created a scan based on the **Basic Agent Scan** template, and is assigned the group *Production Servers*. This scan will only scan production server assets.



Basic Agent Scan - Workstations

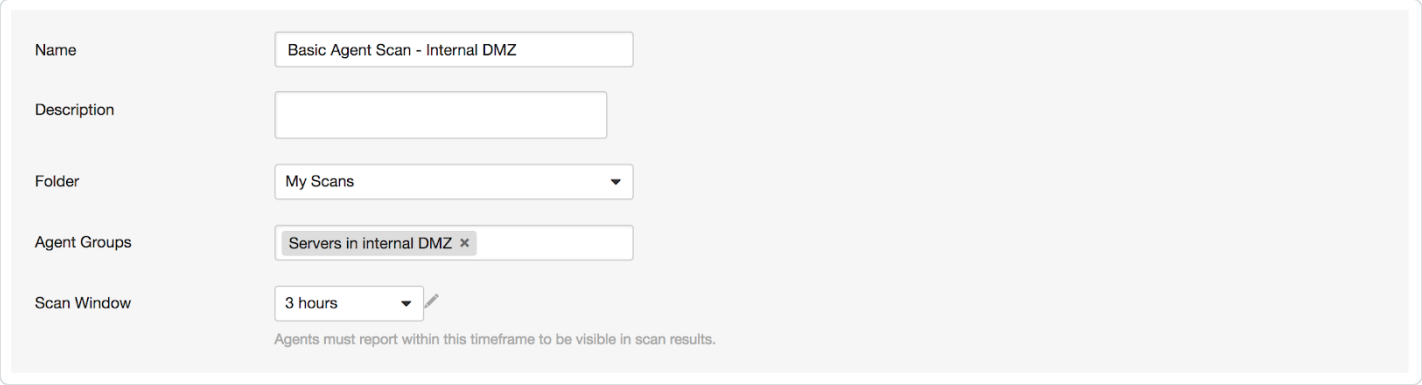
In this example, a scan is created based on the **Basic Agent Scan** template, and is assigned the group *Workstations*. This scan will only scan workstation assets.



Note: Workstation scans may want to be configured for longer scan windows, as most organizations cannot guarantee when these systems will be online (as opposed to servers which are typically on 24/7).

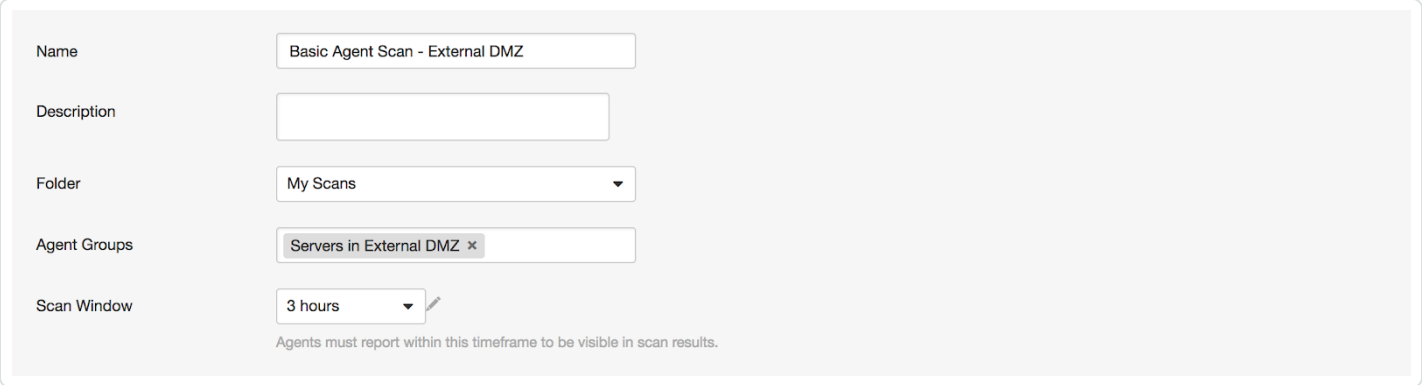
Basic Agent Scan - Internal DMZ

In this example, a scan is created based on the **Basic Agent Scan** template, and is assigned the group *Internal DMZ*. This scan will only scan internal DMZ assets.



Basic Agent Scan - External DMZ

In this example, a scan is created based on the **Basic Agent Scan** template, and is assigned the group *External DMZ*. This scan will only scan external DMZ assets.



Agent Groups

Tenable recommends that you size agent groups appropriately, particularly if you are managing scans in Nessus Manager or Tenable.io and then importing the scan data into SecurityCenter. You can size agent groups when you manage agents in Nessus Manager or Tenable.io.

The more agents that you scan and include in a single agent group, the more data that the manager must process in a single batch. The size of the agent group determines the size of the `.nessus` file that must be imported into SecurityCenter. The `.nessus` file size affects hard drive space and bandwidth.

Group Sizing

Product	Agents Assigned per Group
Tenable.io	Unlimited agents per group if not sending to SecurityCenter 1,000 agents per group if sending to SecurityCenter
Tenable.io On-prem	Unlimited
Nessus Manager	20,000 agents per group if not sending to SecurityCenter 1,000 agents per group if sending to SecurityCenter

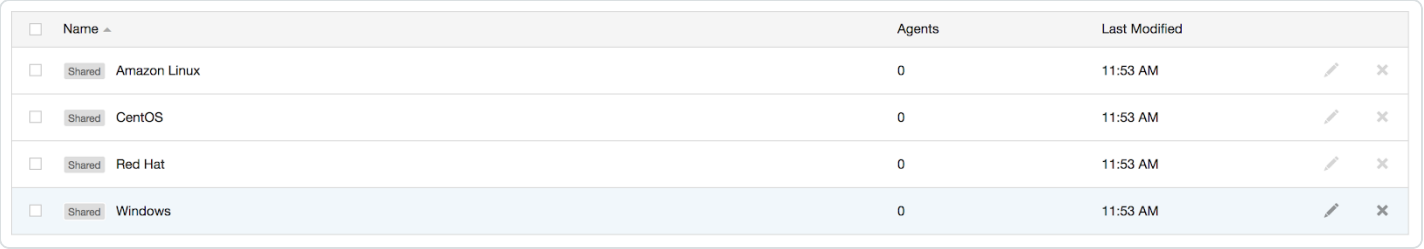
Caution: If you scan multiple groups of agents in a single scan, the total number of agents per scan might not match the total number of agents per group. For example, if you have three groups of 750 agents, all in one scan, then data for 2,250 agents would be imported into SecurityCenter at one time and may overwhelm it.

Group Types

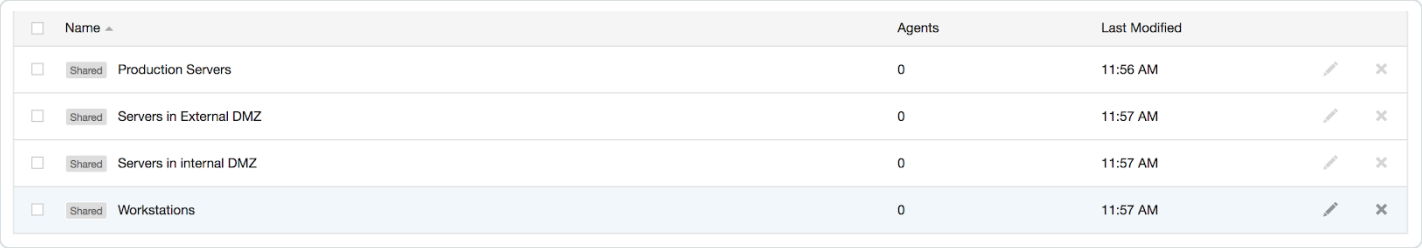
Before you deploy agents to your environment, create groups based on your scanning strategy.

The following are example group types:

Operating System

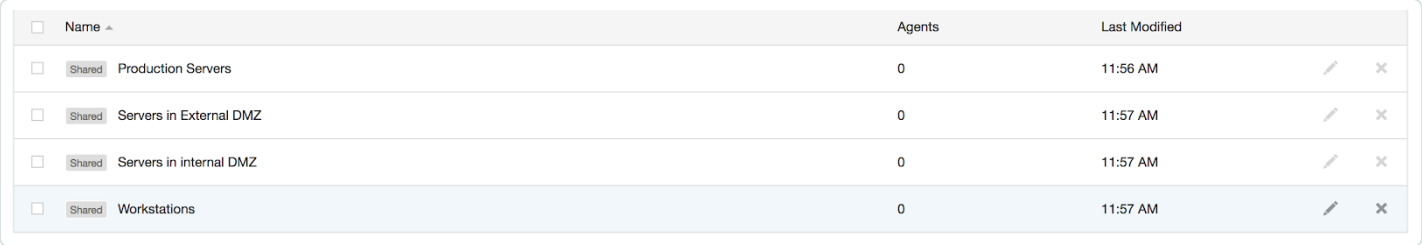


Asset Type or Location



Name	Agents	Last Modified
Shared Production Servers	0	11:56 AM
Shared Servers in External DMZ	0	11:57 AM
Shared Servers in internal DMZ	0	11:57 AM
Shared Workstations	0	11:57 AM

You can also add agents to more than one group if you have multiple scanning strategies.



Name	Agents	Last Modified
Shared Production Servers	0	11:56 AM
Shared Servers in External DMZ	0	11:57 AM
Shared Servers in internal DMZ	0	11:57 AM
Shared Workstations	0	11:57 AM

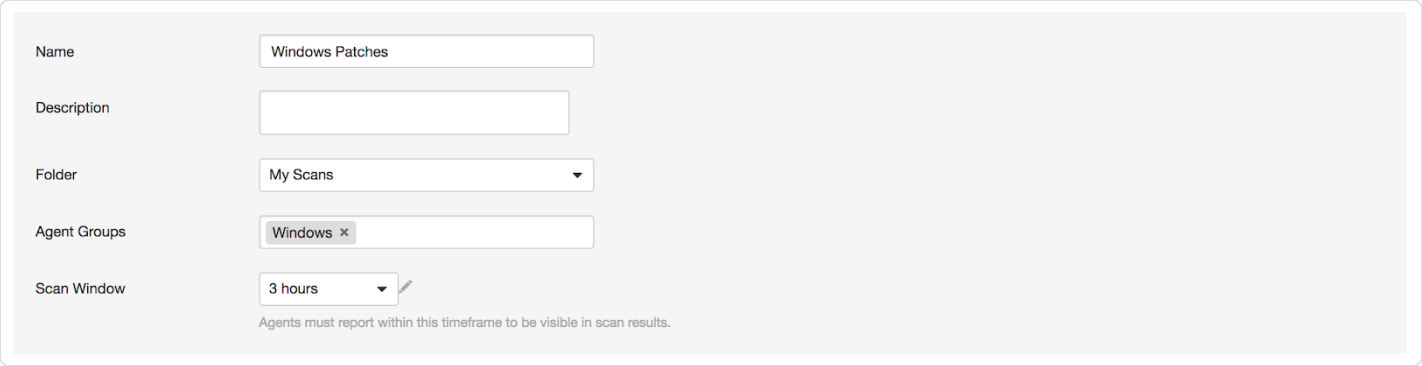
Scan Staggering

Due to the amount of data that goes across your network, it is beneficial to set each scan at different times of the day and week in order to reduce network load and/or bandwidth consumption.

In the following example, your scan runs at the same time on the same day, once a week.

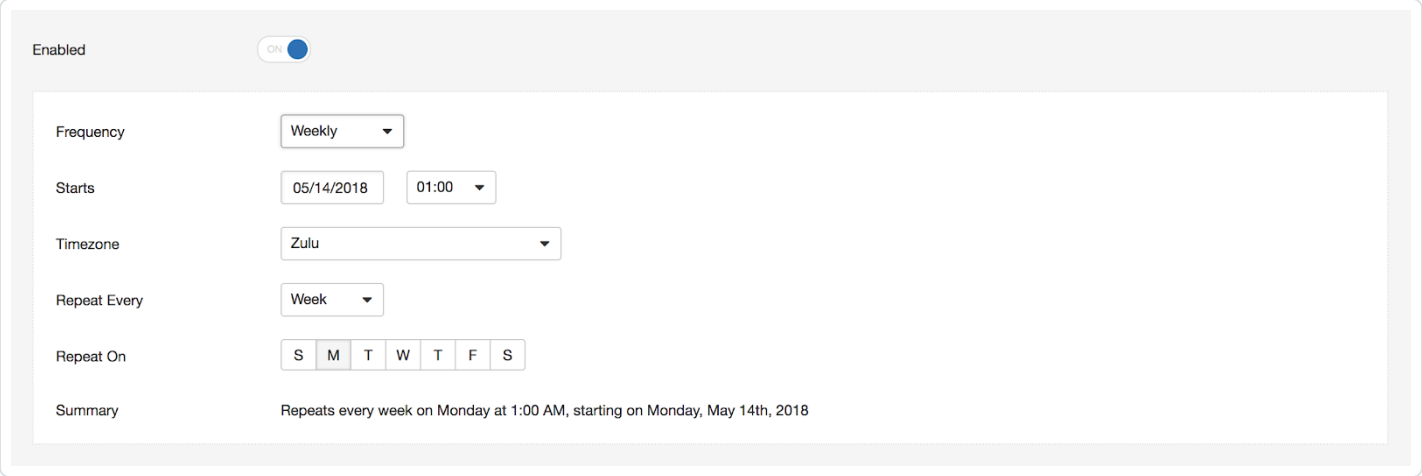
The first thing you should set is a scan window for the scan. A scan window sets the amount of time during which an agent must report.

Scan Window



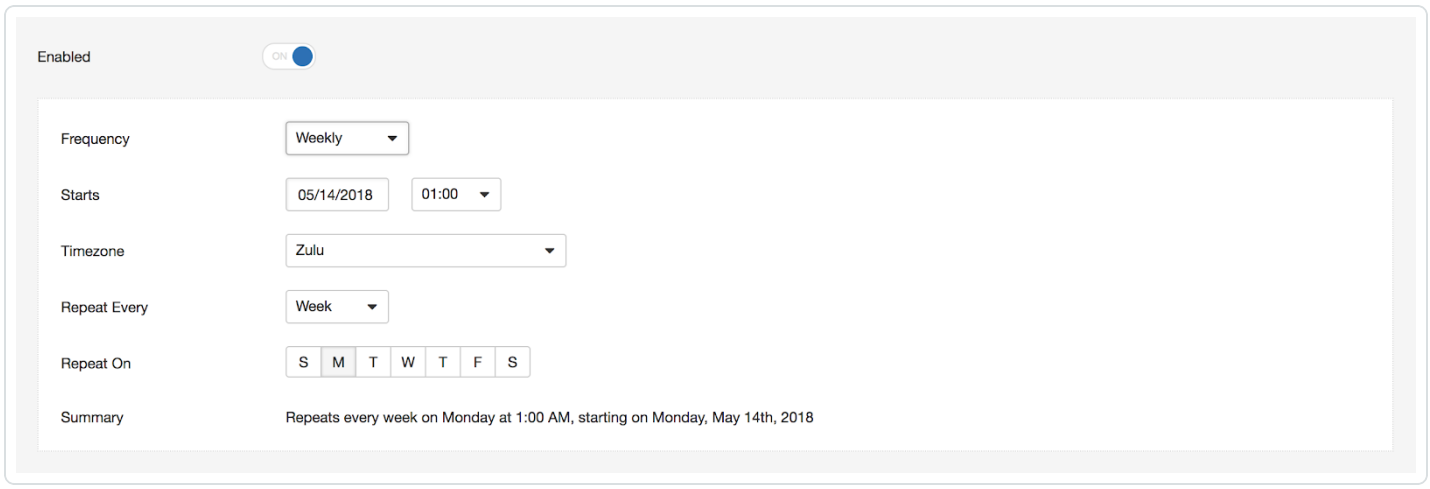
Scan Schedule

Set the scan frequency, start time, timezone, and day. For example, this scan is scheduled to run every Monday at 1:00 a.m.

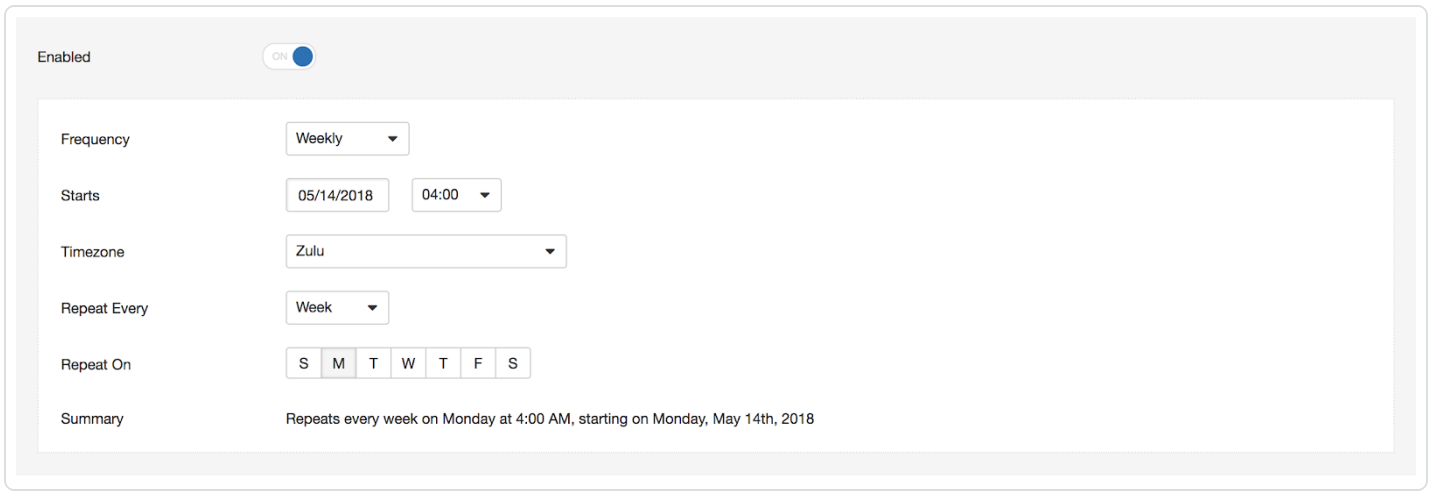


The scan window is set for 3 hours, and the scan starts every Monday at 1:00 a.m. You can now set the second scan for 4:00 a.m.

Scan Window



Scan Schedule



Agent Check-in

Each agent checks in during the scan window between 1 minute and 1 hour. Once checked in, the agent will begin its scan job. After the scan job completes, the agent starts uploading its results. If the agent does not finish its scan and upload the results within the scan window, Tenable.io and/or Nessus Manager does not receive the scan results.

Deployment Mechanism

For automation purposes, it is possible to assign agents to groups during the deployment phase by using the following arguments:

Sample Commands (single group)

These commands are for assigning agents to only one group.

Operating System	Command
Linux	`/opt/nessus_agent/sbin/nessuscli agent link --key=apikey --groups="Group Name" --host=hostname --port=443`
Windows	`msiexec /i NessusAgent-<version number>-x64.msi NESSUS_GROUPS-S="Group Name" NESSUS_SERVER="hostname:443" NESSUS_KEY=apikey /qn`

Sample Commands (multiple groups)

These commands are for assigning agents to multiple groups.

Operating System	Command
Linux	`/opt/nessus_agent/sbin/nessuscli agent link --key=apikey --groups="group 1, group 2, group 3" --host=hostname --port=443`
Windows	`msiexec /i NessusAgent-<version number>-x64.msi NESSUS_GROUPS-S="group 1, group 2, group 3" NESSUS_SERVER="hostname:443" NESSUS_KEY=apikey /qn`

You can use these arguments with third-party agent deployment software such as SCCM, Powershell, Group Policy, Python, etc. to fully automate the deployment of Nessus Agents.

Note: Each agent has an initial plugin update size requirement of 44 MB. Afterward, the agent gets plugin updates regularly in increments.

Logging

Logs for a Nessus Agent can be located at the following locations per operating system.

Operating System	Log Location
Windows	`C:\ProgramData\Tenable\Nessus Agent\nessus\logs`
Linux	`/opt/nessus_agent/var/nessus/logs`
macOS	`/Library/NessusAgent/run/var/nessus/logs`

Agent Deployment Checklist

Before deploying Nessus Agents to production networks, deploy using the following checklist to test devices and networks:

1. Identify the operating systems where you will be deploying agents.
2. Download the agent installation files for each operating system from https://www.tenable.com/downloads.
3. Deploy agents in small test groups to assets using third-party software.
4. During agent deployment, monitor the bandwidth utilization for the network and internet using third-party software. Use this information to avoid times of high bandwidth utilization during agent deployments.
5. Log in to Tenable.io or Nessus Manager and ensure each agent is connected and showing the status **Online**.
6. If your automated deployment solution put each agent in agent groups during the deployment process, ensure each agent is in the appropriate agent group.
7. Set up test scans with the **Basic Agent Scan** policy and target the scans toward your test deployment assets.
8. While the scan is running, monitor your bandwidth utilization using third-party software.
9. After tests are complete, use this checklist and the information you gathered to determine the best strategy to deploy agents to production networks.

Appendix

- Troubleshooting
- Additional Documentation

Troubleshooting

Agent linking key has changed.

If the Agent linking key has been changed, use the following instructions to relink each agent with the new key:

https://docs.tenable.com/nessus/commandlinereference/Content/LocalAgentsCommands.htm

Agent shows offline in Tenable.io and/or Nessus Manager, but the agent is installed on the asset.

1. Ensure the Nessus Agent service is started.
2. Ensure the linked key has not changed.
3. Ensure all firewalls in between the asset and Tenable.io and/or Nessus Manager are allowing port 443.

Agent install is reporting an error during install.

1. Ensure that virus protection software is not preventing the Nessus Agent from installing.
2. Ensure that no permission issues are preventing the install from occurring.

Dataflow Requirements

Port	Traffic from	Traffic to	Purpose
TCP 443	Standalone Nessus or Nessus Manager	Tenable (plugins.nessus.org, plugins-customers.nessus.org, or plugins-us.nessus.org)	Update plugins **Note:** Offline updates are also available if Nessus Manager does not have internet access.
TCP 443	Nessus Agents	Tenable.io (cloud.tenable.com)	Pull plugin updates and scan configurations; push scan results
TCP 443	SecurityCenter	Tenable.io (cloud.tenable.com)	Push scan configurations and pull scan results
TCP 8834 (customizable)	Management Workstation	Nessus or Nessus Manager	Nessus or Nessus Manager Administrative GUI
TCP 8834 (customizable)	Nessus Agents	Nessus Manager	Pull plugin updates and scan configurations; push scan results
TCP 8834 (customizable)	SecurityCenter	Nessus	Push plugin updates and scan configurations; pull scan results
TCP 8834 (customizable)	SecurityCenter	Nessus Manager	Pull scan results
UDP/TCP 53	Nessus	Organization DNS Servers	DNS lookups

Additional Documentation

Document
Nessus Agent Hardware Requirements
Nessus Agent Software Requirements
Nessus Agent Groups
Nessuscli Agent Syntax