Nessus Agent
Large Scale Deployment Guide

Last Revised: July 25, 2023

Table of Contents

Introduction

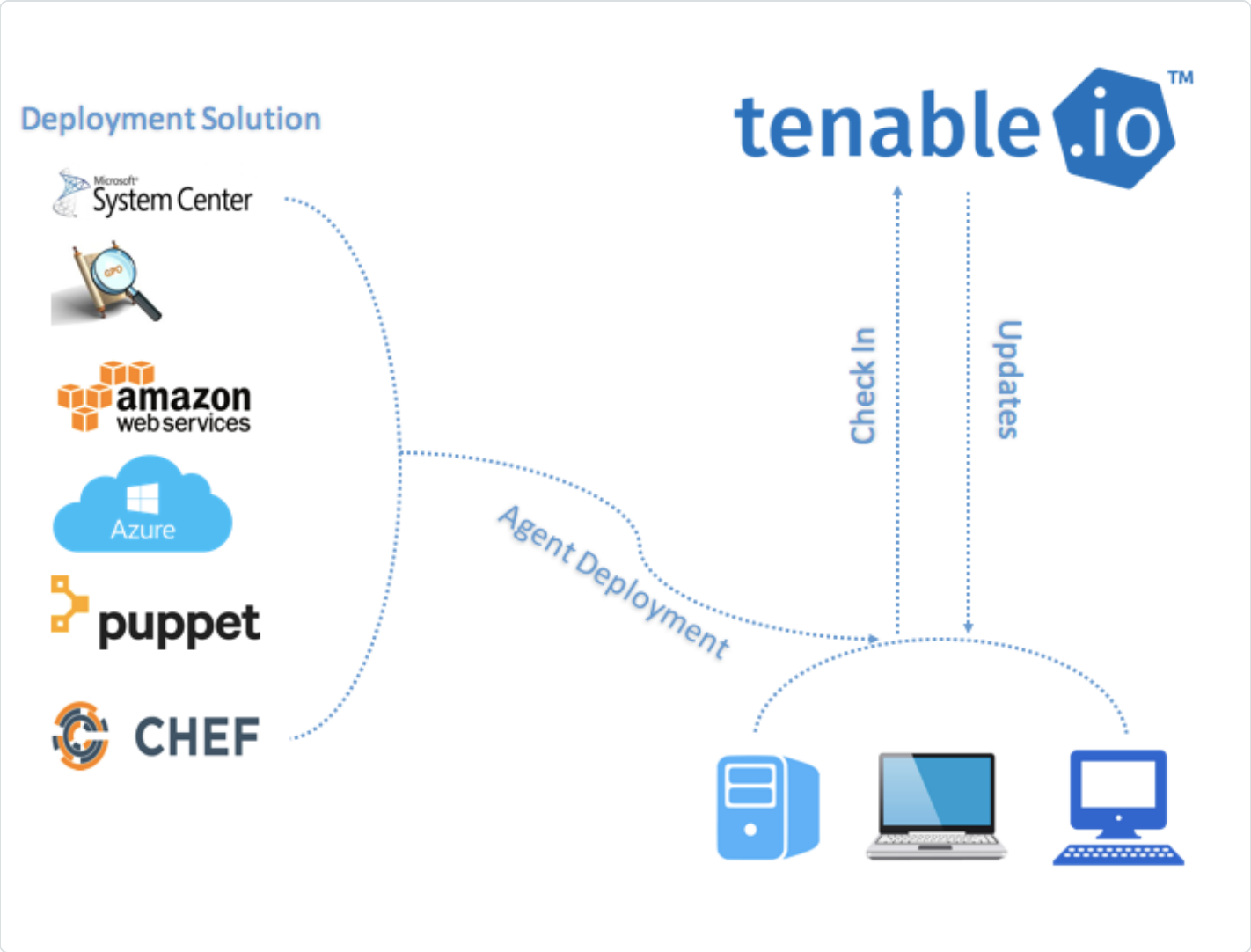
For customers that plan on deploying a multitude of Tenable Nessus Agents across their environment, a large scale deployment strategy is required to ensure all Tenable Nessus Agents are continuously active and stay connected to Tenable Vulnerability Management or Tenable Nessus Manager.

System Requirements

Document Name
Tenable Nessus Agent Hardware Requirements
Tenable 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:



Tenable recommends that you deploy batches of agents over a 24-hour period when deploying a large number of agents. This is especially helpful if you have a limited network bandwidth and need to limit the amount of data your network is downloading at one time.

After you install an agent, it receives its first plugin update once it receives instructions to run an assessment. The agent sets a timer to attempt the next update 24 hours from the initial plugin update time (and update the plugin update date on subsequent successful plugin downloads).

Deploying your agents in batches also prevents too many agents from checking for product updates at one time and consuming too much bandwidth.

Scan Profile Strategy

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

Document Name
Tenable Scan Strategy - Tenable Professional Services

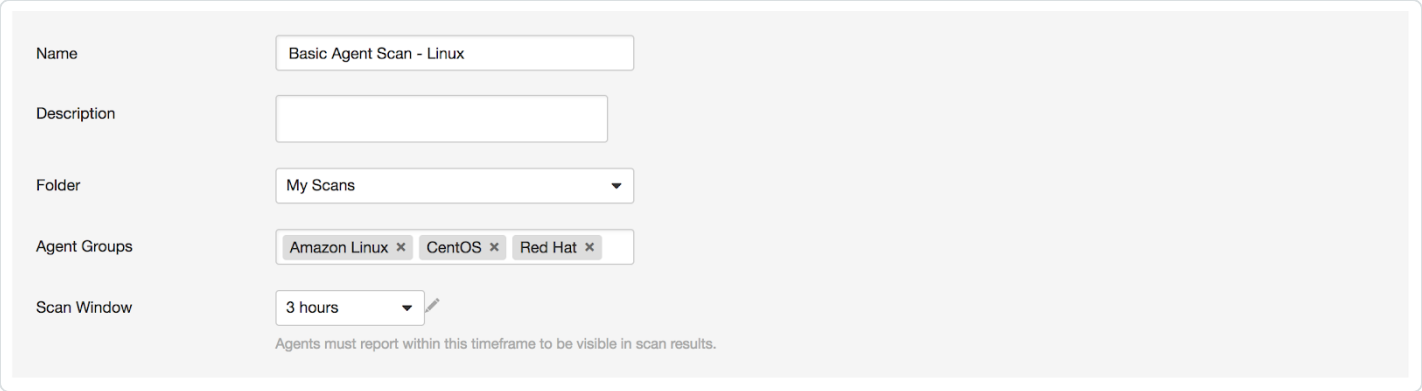
The following are examples on how to build agent scans around an applicable scan strategy.

Operating System Scan strategy

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

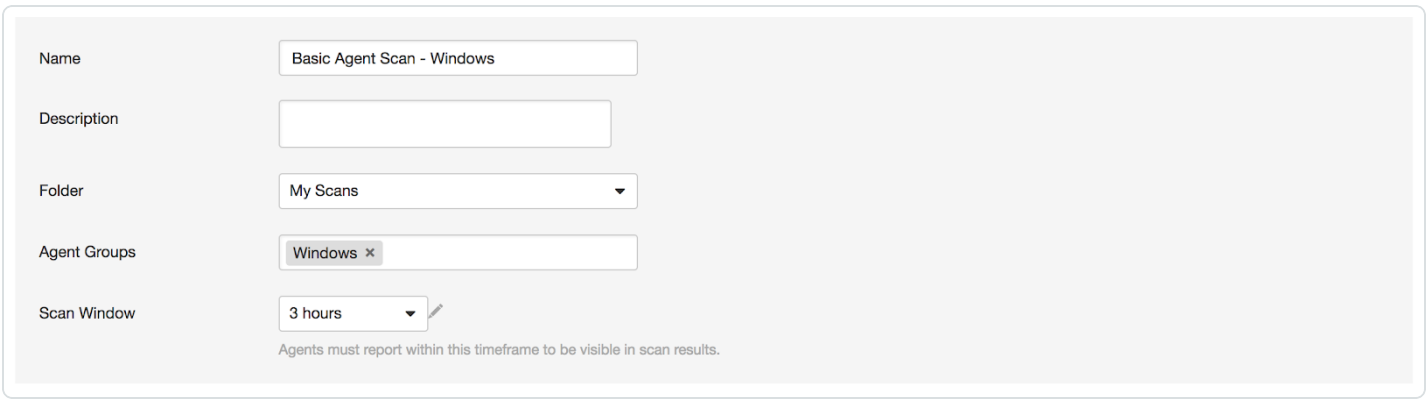
Basic Agent Scan - Linux

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.



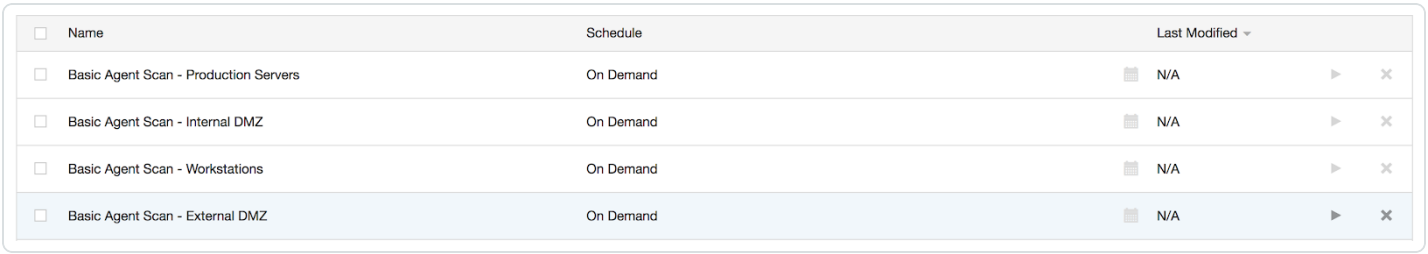
Basic Agent Scan - Windows

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.



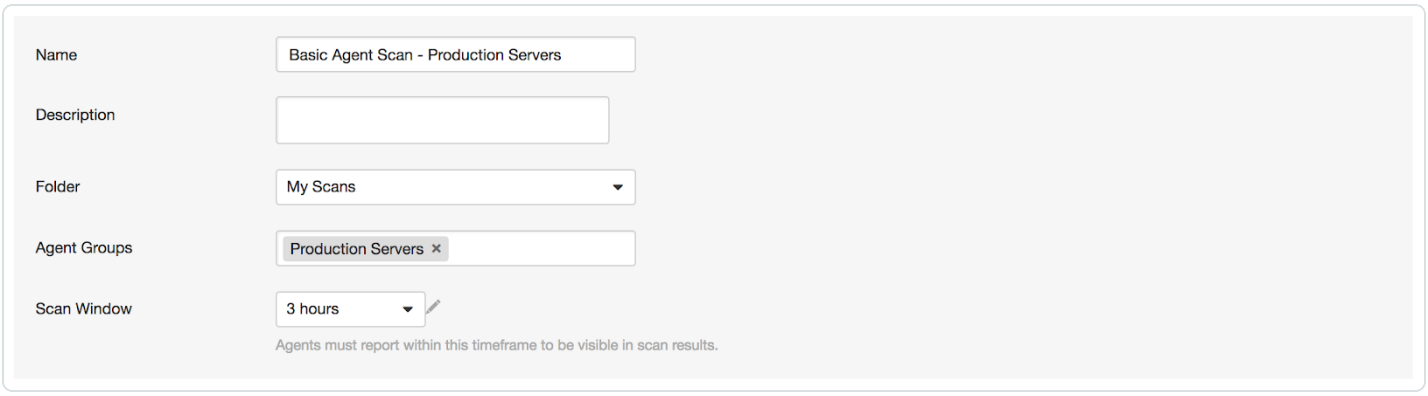
Asset Type or Location Scan Strategy

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



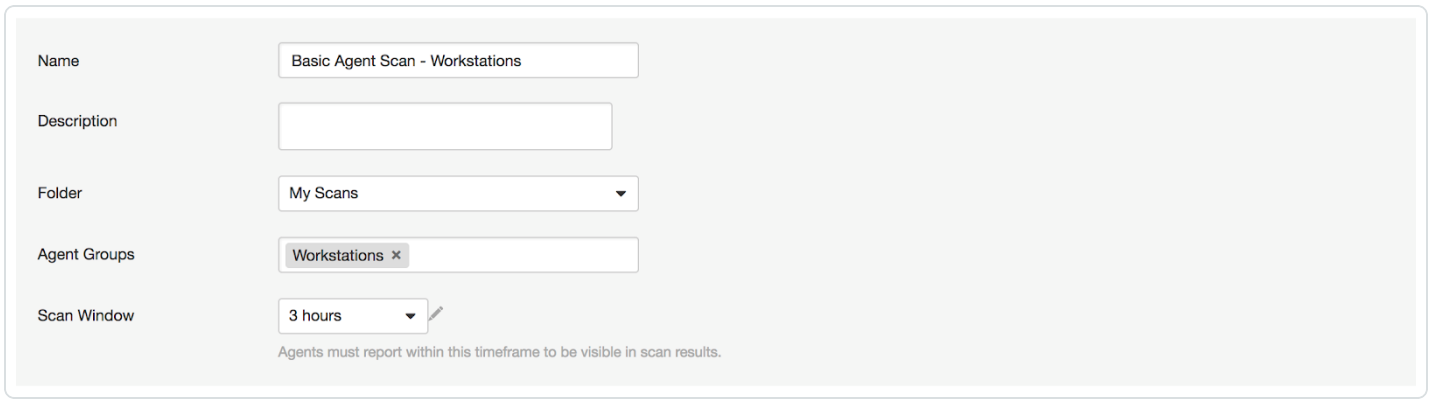
Basic Agent Scan - Production Servers

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

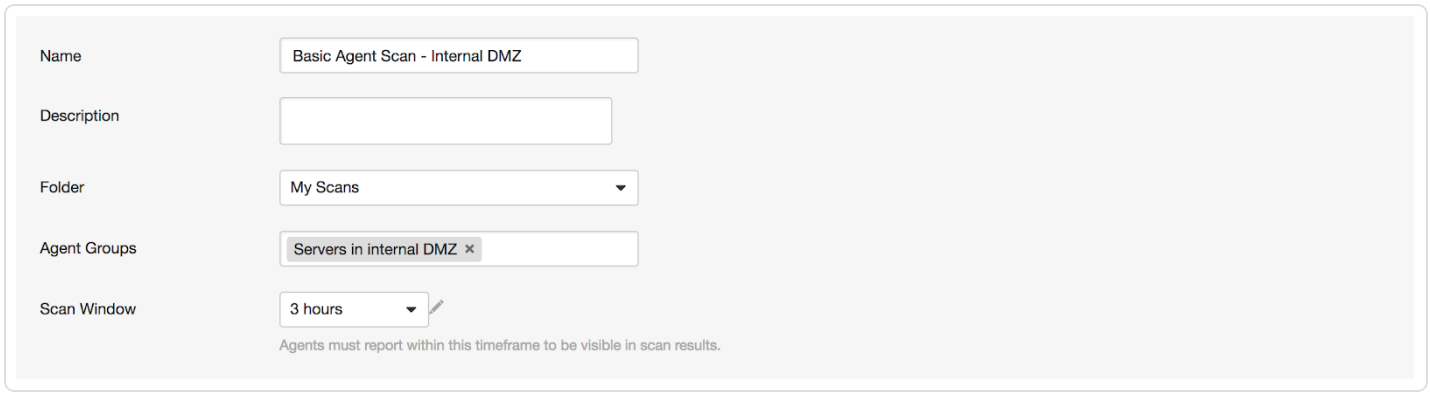
In this example, a scan is created based on the **Basic Agent Scan** template, and is assigned the group *Workstations*. This scan will only scan workstation assets.



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).

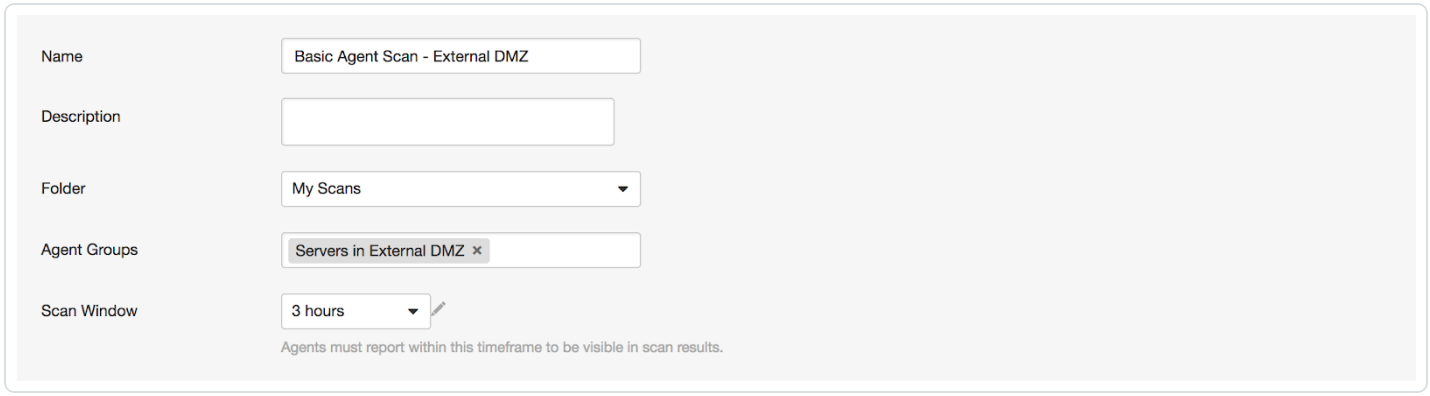
Basic Agent Scan - Internal DMZ

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 Tenable Nessus Manager or Tenable Vulnerability Management and then importing the scan data into Tenable.sc. You can size agent groups when you manage agents in Tenable Nessus Manager or Tenable Vulnerability Management.

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 Tenable.sc. The `.nessus` file size affects hard drive space and bandwidth.

Group Sizing

Product	Agents Assigned per Group
Tenable Vulnerability Management	Unlimited agents per group if not sending to Tenable.sc 20,000 agents per group if sending to Tenable.sc
Tenable Nessus Manager	Unlimited agents per group if not sending to Tenable.sc 20,000 agents per group if sending to Tenable.sc
Tenable Nessus Manager Clusters	Unlimited since scans are automatically broken up as appropriate by separate child nodes.

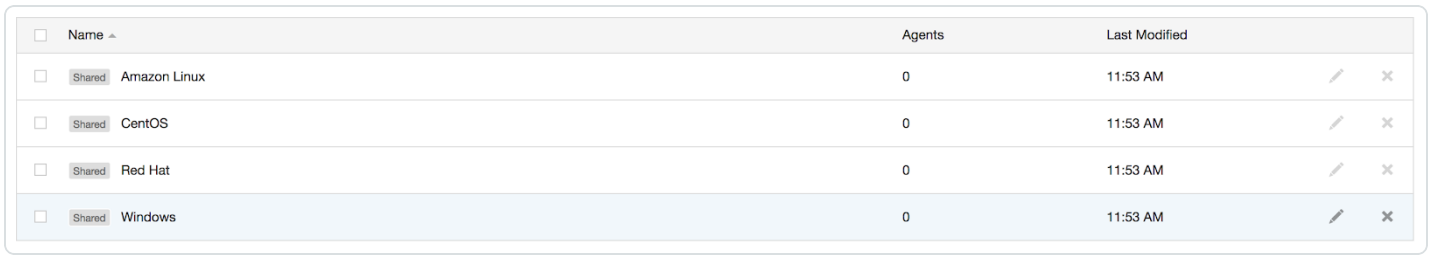
Caution: If you scan multiple groups of agents in a single scan, the total number of agents per scan might not match the total number of agents per group. For example, if you have three groups of 7,500 agents in Tenable Vulnerability Management, all in one scan, then data for 22,500 agents would be imported into Tenable.sc at one time and may overwhelm it.

Group Types

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

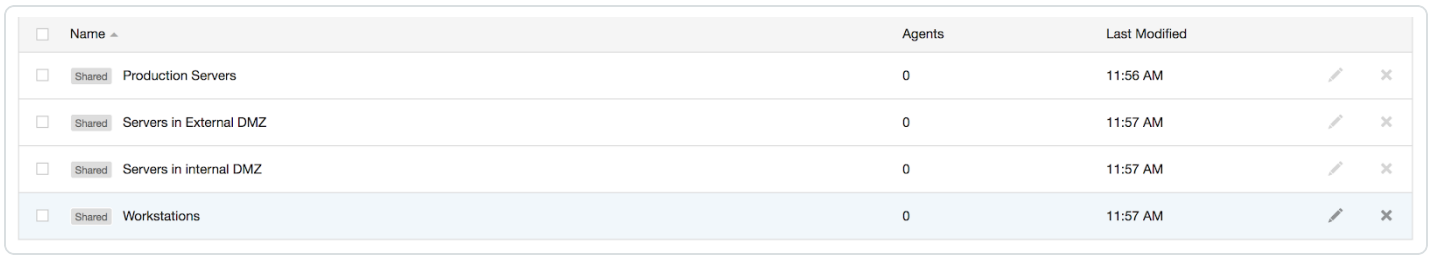
The following are example group types:

Operating System



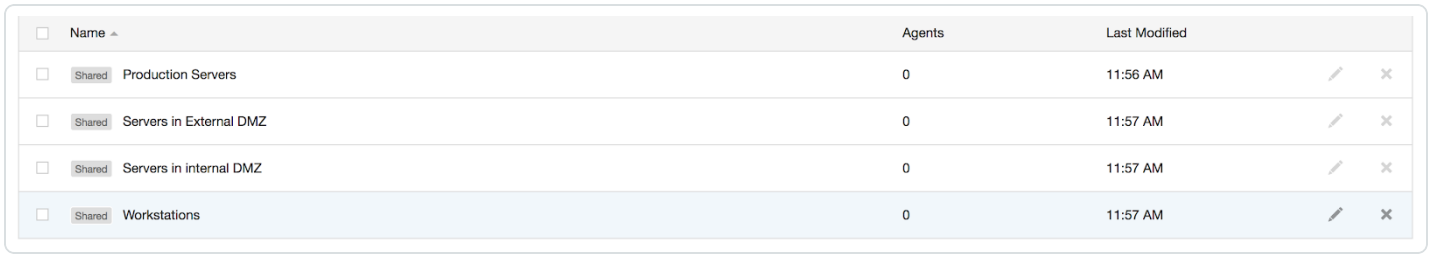
Name	Agents	Last Modified
Shared Amazon Linux	0	11:53 AM
Shared CentOS	0	11:53 AM
Shared Red Hat	0	11:53 AM
Shared Windows	0	11:53 AM

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

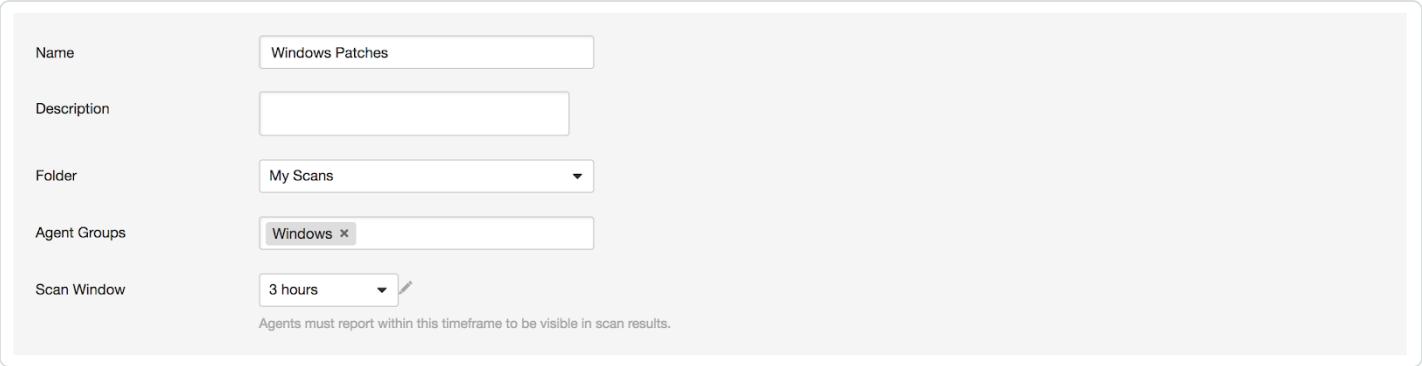
Scan Staggering

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.

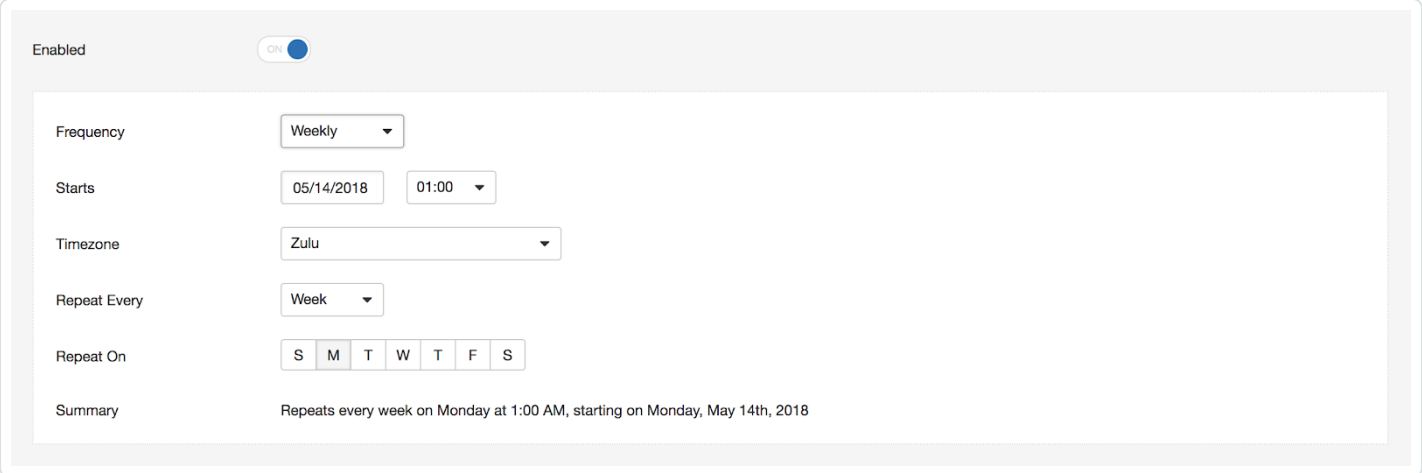
The first thing you should set is a scan window for the scan. A scan window sets the amount of time during which an agent must report.

Scan Window



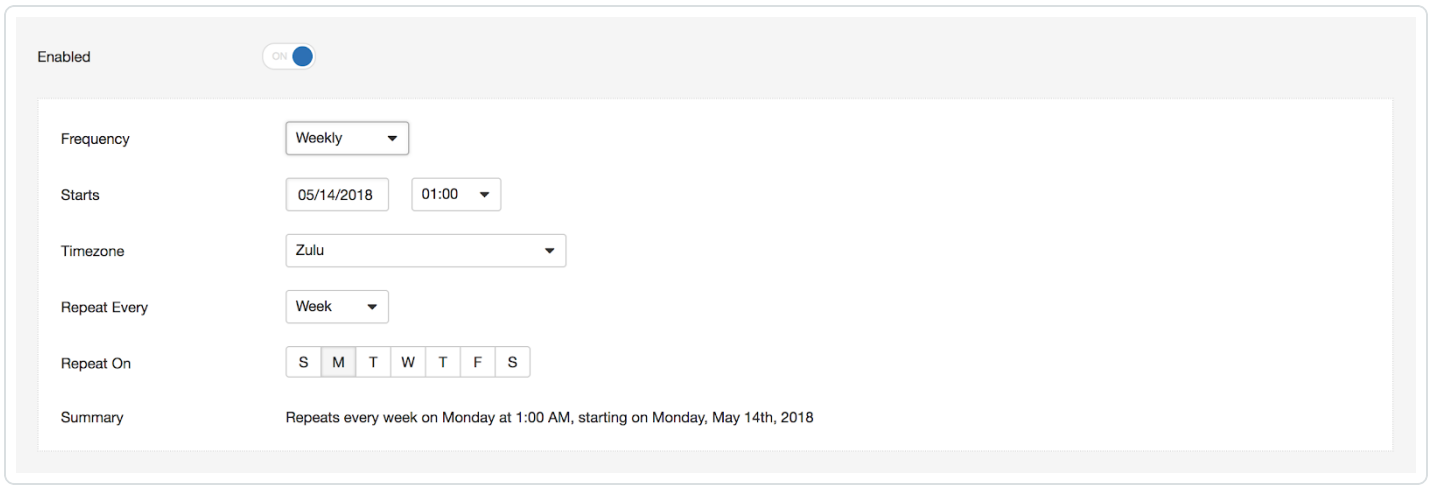
Scan Schedule

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

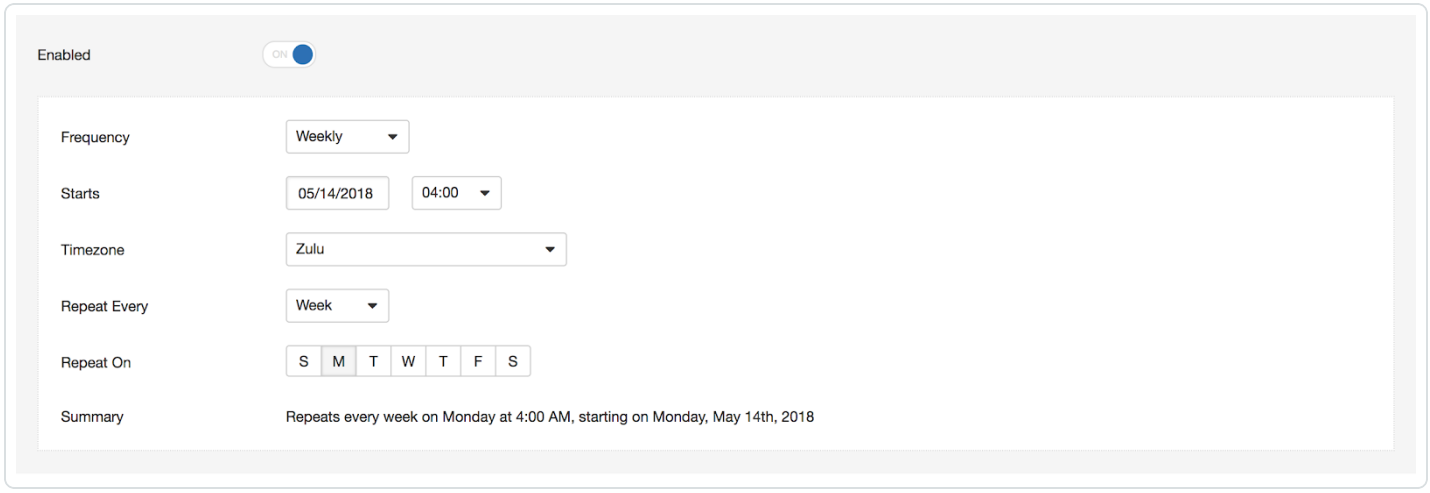


The scan window is set for 3 hours, and the scan starts every Monday at 1:00 a.m. You can now set the second scan for 4:00 a.m.

Scan Window



Scan Schedule



Agent Check-in

Agents check in every 30 seconds to 2,000 seconds (~33 minutes) for jobs. Agents also check in no less than 24 hours since their last job check-in for version and plugin updates. 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 Vulnerability Management and/or Tenable 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>-x64.msi NESSUS_GROUPS="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>-x64.msi NESSUS_GROUPS="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 Tenable 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 Tenable 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 Tenable 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 Vulnerability Management or Tenable 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/command-line-reference/Content/LocalAgentsCommands.htm

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

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

Agent install is reporting an error during install.

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

Port Requirements

Tenable Nessus Agent port requirements include Tenable Nessus Agent-specific requirements and manager-specific requirements. Depending on your deployment setup, see the Tenable Nessus Manager and Tenable.sc port requirements.

Tenable Nessus Agent

Your Tenable Nessus Agents require access to specific ports for outbound traffic.

Outbound Traffic

You must allow outbound traffic to the following ports.

Port	Traffic
TCP 443	Communicating with Tenable Vulnerability Management.
TCP 8834	Communicating with Tenable Nessus Manager. **Note:** The default Tenable Nessus Manager port is TCP 8834. However, this port is configurable and may be different for your organization.
UDP 53	Performing DNS resolution.

Tenable Nessus Manager

Your Tenable Nessus instances require access to specific ports for inbound and outbound traffic.

Inbound Traffic

You must allow inbound traffic to the following ports.

Port	Traffic
TCP 8834	Accessing the Tenable Nessus interface. Communicating with Tenable.sc. Interacting with the API.

Outbound Traffic

You must allow outbound traffic to the following ports.

Port	Traffic
TCP 25	Sending SMTP email notifications.
TCP 443	Communicating with Tenable Vulnerability Management. Communicating with the `plugins.nessus.org` server for plugin updates.
UDP 53	Performing DNS resolution.

Tenable.sc

Your Tenable.sc instances require access to specific ports for inbound and outbound traffic.

Inbound Traffic

You must allow inbound traffic to the following ports.

Port	Traffic
TCP 22	Performing remote repository synchronization with another Tenable.sc.
TCP 443	Accessing the Tenable.sc interface. Communicating with Tenable Security Center Director instances. Communicating with Tenable OT Security instances. Performing the initial key push for remote repository synchronization with another Tenable.sc. Interacting with the API.

Outbound Traffic

You must allow outbound traffic to the following ports.

Port	Traffic
TCP 22	Communicating with Log Correlation Engine for event query.
TCP 25	Sending SMTP email notifications.
TCP 443	Communicating with Tenable Vulnerability Management. Communicating with Tenable Lumin for synchronization. Communicating with the `plugins.nessus.org` server for plugin updates.
TCP 1243	Communicating with Tenable Log Correlation Engine.
TCP 8834	Communicating with Tenable Nessus.
TCP 8835	Communicating with Tenable Nessus Network Monitor.

Port	Traffic
UDP 53	Performing DNS resolution.

Agent Content Distribution Network (CDN)

Dependent on rule logic in place, you may need to adjust your firewall or proxy rules in order to utilize the Agent Content Distribution Network (CDN) introduced with Tenable Nessus Agent 7.1.2.

FQDN Updates

The CDN leverages `downloads-agent.cloud.tenable.com` for downloading plugins and binary updates, `uploads-agent.cloud.tenable.com` for uploading scan results, and `sensor.cloud.tenable.com` for linking and communicating with Tenable Vulnerability Management. If you have a firewall or proxy rule configured for `*.cloud.tenable.com` then you should not encounter issues. However, if there are stricter rules in place then you need to update your rule set.

IP Allowlisting

The IP addresses associated with `downloads-agent.cloud.tenable.com` and `uploads-agent.cloud.tenable.com` are dynamic and dependent on the locale of the agent and its connectivity to the internet. If you currently have IP-based rules configured for proxies and firewalls you must update the rules based on IP ranges utilized by Amazon CloudFront. Amazon's documentation Locations and IP Address Ranges of CloudFront Edge Servers has a list of the IP ranges available for download.

Additional Documentation

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