Tenable Vulnerability Management Scan Performance at Scale

Last Revised: September 08, 2023

Tenable Vulnerability Management Scan Performance at Scale

Requirement

Use Tenable Vulnerability Management to scan an organization's entire external network to discover 55,000 assets and scan for external vulnerabilities on those assets daily. The daily scan time must be no more than 12 hours.

Contributing Factors

There are a number of variables to consider when running a vulnerability assessment, such as scanner hardware, scanner and scan job configuration, and operating system settings.

Other contributing factors to consider include:

- The targets that scanners are connected to
- Scanner network health
- Global variables
- Local scanner variables
- Scanner hardware and software
- Scan type and scan policy variables (discovery settings, performance settings, authenticated versus unauthenticated scanning)

Study Summary

This study explores the effects that the following four contributing factors have on scan performance:

- Scanner hardware
- Scanner and scan job configuration in Tenable Nessus
- Operating system settings
- Internal Tenable platform tuning

The study was conducted across five iterations, with each iteration building off the previous iteration. This was done to test and demonstrate the overall effect that each of the four factors has on scan performance.

Choices

This study was performed on Tenable Vulnerability Management in AWS for unlimited scalability (the ability to pool scanner resources, manage and configure scanners in a single workspace, and see aggregated data from a holistic view) and computation/control options.

The study was performed with the following hardware:

- **Scanners**

  Managed Tenable Nessus scanners on DigitalOcean Droplets

- **Scanner hardware**

  16 GB RAM, 8 CPU cores, 50 GB disk space

- **Operating system**

  Red Hat Enterprise Linux (RHEL) 7 with kernel, paging size, and other tuned variables

- **Scan configuration**

  An Advanced Scan configuration with default scan settings for speed and simplification of time and management

Results

1. **First iteration: Tune the scanning hardware**

   The first iteration of scan tuning was used to find optimal settings for the scanner hardware resources and total number of scanners. The study began with 10 scanners using the default recommended 16 GB RAM and 8 cores, which finished the required scanning job in 4 days and 20 hours.

   Decreasing to the minimum recommended specifications of 8 GB RAM and 4 cores with 20 scanners yielded a minimal performance improvement of 4 days and 6 hours.

2. **Second iteration: Tune Tenable Nessus (the scan job and scanners)**

By default, Tenable Nessus scanners are configured with the following settings: Advanced Settings. During the second iteration, we set **Max Concurrent Checks Per Host** to 15 and **Global Max Hosts Concurrently Scanned** to 1000. This decreased the scan time to 3 days.

> **Note:** These local settings can override and be overridden by the advanced scan settings in Tenable Vulnerability Management.

3. **Third iteration: Tune the operating system settings**

   For the third iteration, we tuned the RHEL 7 buffer sizing and garbage cleaning intervals on each scanner. At this scale, these changes only reduced the overall scan time by a few hours.

4. **Fourth iteration: Tune Tenable Vulnerability Management (the platform)**

   For the fourth iteration, we made internal platform adjustments in Tenable Vulnerability Management on behalf of the study organization. These adjustments involved settings that only Tenable can configure. These adjustments drastically reduced the overall scan time to 19 hours.

   > **Note:** If your organization wants to learn more about internal adjustments that Tenable can make to improve your scan metrics, contact your Tenable Customer Success Manager.

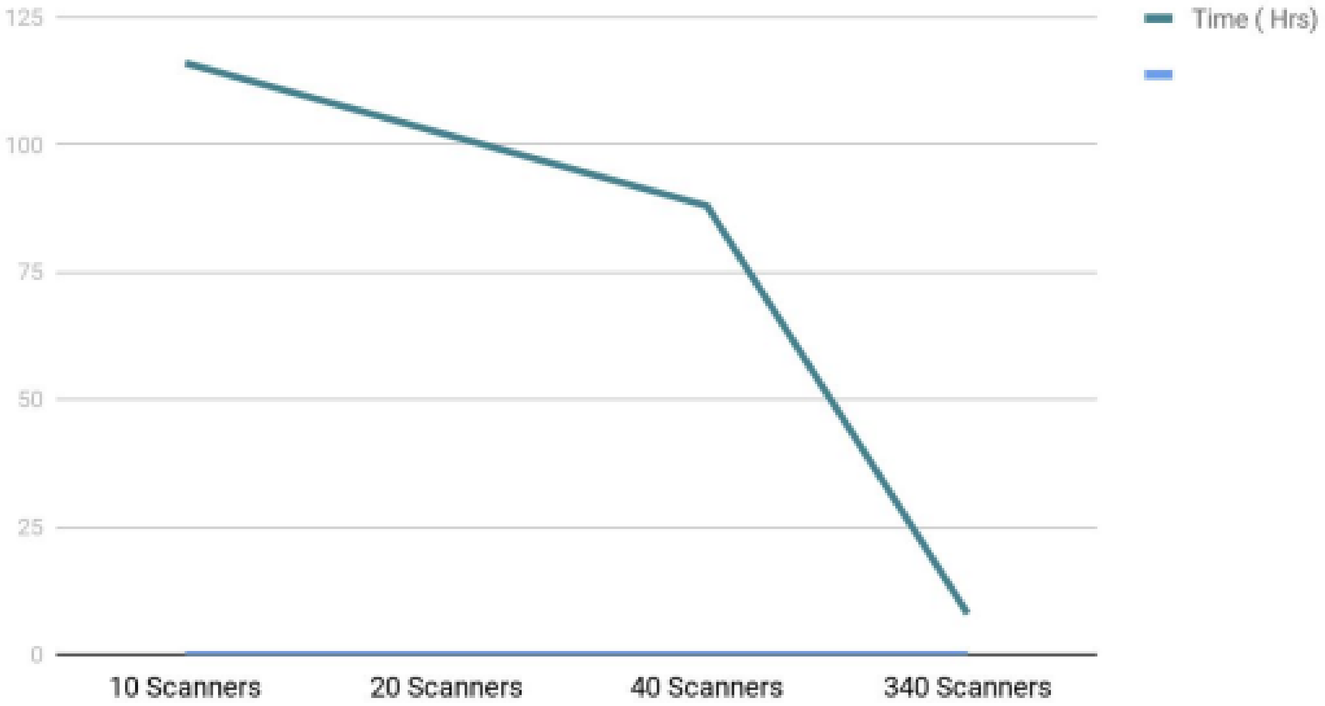
5. **Fifth iteration: Scale hardware for study requirement**

   To meet the organization's use case, the scan time had to be reduced to 12 hours or less. To accomplish this, the organization used 340 scanners to reduce the scan time to 8 hours total.

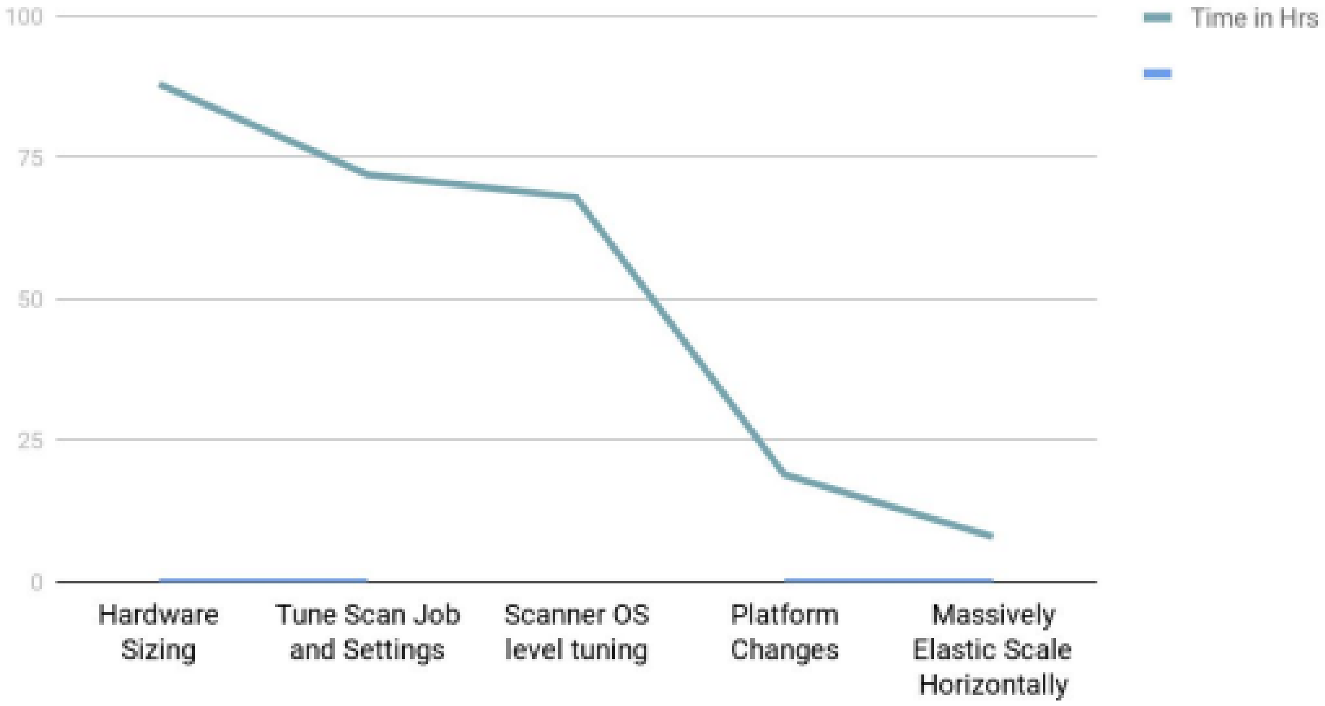
Analysis

The following graphs show the scan duration improvements related to the number of scanners used, and scan time improvements that were observed after each tuning iteration:

Scan Duration by Hardware



Total scan time after each tuning iteration



The vast majority of environments do not allow for dedicated platform testing with this significant number of resources. The purpose of this study is to highlight all scan variables, raise awareness of their impact, and aid in a variety of scenarios.

There are numerous ways to tune scans, but the Tenable development team has done a commendable job in building and exposing control of the Tenable Nessus engine. Efficient use of hardware and operating system resources, along with the ability to adjust resources automatically, allow the vast majority of customers to use Tenable scanning products out of the box and realize immediate value. This study demonstrates that, considering the limited need to scale the individual scanners vertically.

Horizontal scale is powerful and efficient as it allows single resources to become multithreaded and eliminates singular bottlenecks. There are always finite limitations however, and we saw diminishing returns when using 30, 40, and up to 340 scanners connected to Tenable Vulnerability Management.