

Tenable Log Correlation Engine and Nessus Network Manager

Quick Start Service Specification

Last Revised: September 18, 2018

Quick Start Service Specification

Quick Start Service Overview

The Tenable Quick Start Service provides Tenable customers a fast path to full operational capability of Tenable SecurityCenter™. The service allows your organization to realize several key benefits of SecurityCenter in a short period of time. The Quick Start Service has the following outcomes:

- Install and configure the Log Correlation Engine® and Nessus Network Monitor™. Log Correlation Engine and Nessus Network Monitor will be installed and configured based on requirements captured during the solution design.
- Implement best practices. Experienced Tenable consultants will implement and orient you to Tenable best practices for enterprise deployment and log event management throughout the system.
- Validate operational capabilities. Log Correlation Engine and Nessus Network Monitor will be tested end to end for scanning and other operational capabilities.

Tenable provides this predefined service for the installation and configuration of one Log Correlation Engine instance and one Nessus Network Monitor instance.

Preparing for Quick Start Engagement

In order to receive the services, the customer must ensure that:

1. Customer systems meet or exceed the specifications found in the Tenable General Requirements document, available at <https://docs.tenable.com/generalrequirements/Content/Introduction.htm>.
2. All necessary hardware and appliances are mounted and in place.
3. Tenable appropriate product licenses and activation keys/codes are obtained.
4. SecurityCenter must be installed and properly configured.
5. All required network communication paths are verified. Many customers find that firewall policy exceptions are required for remote scanners.

Tasks

1. **LCE Installation and Configuration.** The Tenable Consultant will install and configure one LCE instance.
2. **NNM Configuration.** The Tenable Consultant will install and configure one NNM instance. The NNM product set install requires a span, tap, or hub port. The Tenable Certified Engineer will assist customers to create Scanning Policies and Asset Lists for a successful SecurityCenter and Nessus/NNM installation.
3. **Recommendations and Knowledge Transfer.** The Tenable Certified Engineer will provide Customer with recommendations on how to capitalize on SecurityCenter capabilities and features for a more proactive and pragmatic approach to vulnerability management and risk remediation procedures. This will address End of Life (EOL) systems, MS bulletin scanning, valid virus scanning data, and 3rd party application information. The Tenable Certified Engineer will provide knowledge transfer of findings and results for each task.

Session Delivery

The Quick Start service is delivered in the following manner:

Kickoff Meeting

- Meet and interview key stakeholders
- Discuss outcomes of Quick Start service
- Introduce Deployment Worksheet
- Initiate architecture discussion – Customer infrastructure & Tenable product placement

Log Correlation Engine and Nessus Network Monitor

- Install and Configure LCE Server
- Install and Configure Nessus Network Monitor
- Enable SYSLOG on Network Devices
- Load LCE Clients

Nessus Network Monitor Event Analysis

- Event Analysis
- Nessus Network Monitor
- Review Client Policy and Events

Log Correlation Event Analysis

- Log Correlation Dashboard Creation
- Log Correlation Reporting
- Log Correlation Event Rule Analysis
- Query Creation and Review
- Query Techniques and Methods

Log Correlation Alerts

- Alerts and Ticketing
- Review PRM Functionality
- Review Operational Procedures

Deliverables

A deliverable with the following components will be completed as part of the engagement:

- Configuration document summarizing the configuration of customer's installation

Out-of-Scope Items

Custom scripts and customer audit files are outside the scope of this engagement.