Log Correlation Engine 4.2 Quick Start Guide

September 4, 2014

(Revision 3)

Table of Contents

Introduction

This document provides basic instructions for installing and configuring Tenable Network Security's Log Correlation Engine (LCE) version 4.2 or newer. This is not intended to be a comprehensive document on the product and is only focused on essential steps needed to get the product up and running. Please refer to additional documentation available on the Tenable Support Portal for more information. Please email any comments and suggestions to support@tenable.com.

Familiarity with system log formats from various operating systems, network devices, and applications and a basic understanding of Linux/Unix command line syntax is also assumed.

Standards and Conventions

Throughout the documentation, filenames, daemons and executables are indicated with a **courier bold** font such as **gunzip**, **httpd**, and **/etc/passwd**.

Command line options and keywords are also indicated with the **courier bold** font. Command line examples may or may not include the command line prompt and output text from the results of the command. Command line examples will display the command being run in **courier bold** to indicate what the user typed while the sample output generated by the system will be indicated in courier (not bold). Following is an example running of the Linux/Unix **pwd** command:

```
# pwd
/opt/lce/daemons
#
```

Important notes and considerations are highlighted with this symbol and grey text boxes.

Tips, examples, and best practices are highlighted with this symbol and white on blue text.

Product Overview

Tenable's Log Correlation Engine helps organizations find and respond to security threats and demonstrate compliance with policies and regulatory requirements.

The Log Correlation Engine collects, normalizes, and analyzes logs from devices throughout your network. It analyzes and correlates data from firewalls, intrusion detection and prevention systems, and data loss prevention solutions, as well as raw network traffic, application logs and user activity logs.

Prerequisites

Tenable recommends a minimum of 2GB of memory, and a Dual-Core 3.0GHz processor along with 1TB of disk space to operate LCE. A storage configuration of SAS 3 Gb/s, RAID 0 striping is recommended. LCE is available for Red Hat Enterprise Server 5 (32/64-bit) and 6 (32/64-bit). CentOS 5 (32/64-bit) and 6 (32/64-bit) are also officially supported. For more information on hardware requirements for your environment, please review Log Correlation Engine 4.2 High Availability Large Scale Deployment Guide.

LCE Quick Start

This document refers to three primary LCE components: the LCE Client (the device that initially collects data and sends it on to the LCE server); the LCE server (or daemon), which is installed on Red Hat/CentOS and performs the bulk of the processing; and SecurityCenter, which provides a graphical user interface to view and report on the LCE data.

Installation

System Prerequisites

- A RHEL/CentOS 5 or 6 platform with all unnecessary services disabled
- LCE license file (you will need the output of the "**hostname**" command to obtain a license file)
- SecurityCenter (optional purchase). For more information, visit: http://www.tenable.com/products/securitycenter.
- Firewall configuration:
  - Open 514/UDP for standard syslog
  - Open 601/TCP for reliable syslog
  - Open 443/TCP for remote access to the LCE Manager web console if installed on the same server
  - Open 31300/TCP for LCE client/server communications
  - Open 31302/TCP for LCE server load balancing (when used)

These ports cannot be used by any other processes. For example, the **syslogd** service on 514/UDP or 601/TCP must be disabled, or set to listen on different ports.

Prepare the License

The free, demo, or commercial license key file for LCE must be placed on the system running LCE. After the LCE RPM is installed, a configuration script must be run and during that process the full path and name of the **.key** file. For this example, we will assume the key (**lce.key**) and RPM files are in the **/home/root** directory.

Dependencies

Although it is possible to force the installation without all required dependencies, if your version of Red Hat or CentOS is missing certain dependencies, this will cause problems that are not readily apparent with a wide variety of functions. Tenable's Support team has observed different types of failure modes for SecurityCenter when dependencies to the installation RPM are missing. If you require assistance or guidance in obtaining these dependencies, please contact Tenable's Support team at support@tenable.com.

The following programs must be installed on the system prior to installing the Tenable software.

For LCE server:

- coreutils
- initscripts
- perl
- gawk
- net-tools
- procps
- openssh-clients
- gzip
- findutils
- openssl
- bind-utils
- wget
- rsync

Always use the latest stable production version of each package approved by your IT department. Depending on initial OS installation options, other packages may be requested during product installation.

To determine which version is on your system, run the following command for each of the packages (replace "**libxslt**" with the appropriate package):

```
# rpm -qa | grep libxslt
```

If one of the prerequisite packages is missing, it can be installed using the "yum" or "rpm" package managers. For example, to install Java 1.7.0 and answer "yes" to all questions, use "yum" with the command below:

```
# yum -y install java-1.7.0-openjdk.i386
```

Install the LCE Server Package

As the root user, install the LCE Server RPM using the following command:

```
# rpm -ivh lce-4.x.x-es6.i386.rpm
```

LCE 4.2 introduces a post-install script to facilitate basic configuration. Once the installer completes, the post-install script will need to be executed, which is described in the section "Basic LCE Server Configuration".

Basic LCE Server Configuration

The following is an example of the post-install script that needs to be run after the initial install package has completed. Note that this utility is only available in LCE version 4.2 and higher. Actions you will need to perform are shown as **bold**.

```
# /opt/lce/tools/lce-post-install.sh

------------------------------------------------------------------------------
                                LCE CONFIGURATION
------------------------------------------------------------------------------

                              TENABLE NETWORK SECURITY
                               http://www.tenable.com
                                support@tenable.com
                                Copyright 2003-2013


    Welcome to the LCE configuration!

    This will assist you in configuring your newly installed LCE.
    It should take about a minute to complete.

Press ENTER to continue

The configuration script has detected that LCE is currently running.
It is being shut down so that the configuration can be completed...

Stopping LCE Indexer                                        [  OK  ]
Stopping LCE Report Proxy                                   [  OK  ]

------------------------------------------------------------------------------
```

```
                          LCE CONFIGURATION : Key File
--------------------------------------------------------------------------------

    We will now check /opt/lce/daemons/lce.key for validity...

    The key in /opt/lce/daemons/lce.key is valid!

--------------------------------------------------------------------------------
                        LCE CONFIGURATION : Activation
--------------------------------------------------------------------------------

    In order to receive plugin updates, the Log Correlation Engine
    must be activated.

Please enter your activation code: XXXX-XXXX-XXXX-XXXX-XXXX
Registering activation code XXXX-XXXX-XXXX-XXXX-XXXX...

The activation code has been accepted.
--------------------------------------------------------------------------------
                     LCE CONFIGURATION : Interface Ports
--------------------------------------------------------------------------------

    LCE listens for data on a number of ports.
    LCE will check now to be sure that none of those ports are in use.
    If any of the ports are in use, you may reconfigure LCE to use a different port,
    or stop the service using the port.

    The LCE ports will now be checked for validity...

Press ENTER to continue

    ...checking the syslog port (udp port 514)...

    ...checking the reliable syslog port (tcp port 601)...

    ...checking the LCE client-server communications port (tcp port 31300)...

    ...checking the snmp port (udp port 162)...

    ...checking the LCE load balancing port (tcp port 31302)...

    ...checking the Vulnerability reporting port (tcp port 1243)...

--------------------------------------------------------------------------------
                        LCE CONFIGURATION : Networks
--------------------------------------------------------------------------------

    LCE contains a vulnerability detection engine, a statistics engine for
    anomaly detection, and a correlation engine for advanced alerting.
```

```
    For best performance, these engines need to know what internal network ranges
    to track in your log data, as well as what network ranges NOT to track.

    First, please configure the networks you wish to INCLUDE in analysis.

Press ENTER to continue

--------------------------------------------------------------------------------
                 LCE CONFIGURATION : Networks to include
--------------------------------------------------------------------------------

   Current include-networks:

--------------------

--------------------

   Network ranges may be specified in two ways:
   1.  IP/Netmask - for example, 192.168.0.0/255.255.0.0
   2.  IP/CIDR    - for example, 192.168.0.0/16

   Please enter a network range to include (or press ENTER to quit).

>>xxx.xxx.xxx.xxx/xx

--------------------------------------------------------------------------------
                 LCE CONFIGURATION : Networks to include
--------------------------------------------------------------------------------

   Current include-networks:

--------------------
XXX.XXX.XXX.XXX/XX
--------------------

   Network ranges may be specified in two ways:
   1.  IP/Netmask - for example, 192.168.0.0/255.255.0.0
   2.  IP/CIDR    - for example, 192.168.0.0/16

   Please enter a network range to include (or press ENTER to quit).

>>

--------------------------------------------------------------------------------
                        LCE CONFIGURATION : Networks
--------------------------------------------------------------------------------

    Next, please configure the networks you wish to EXCLUDE in analysis.

Press ENTER to continue

--------------------------------------------------------------------------------
                 LCE CONFIGURATION : Networks to exclude
--------------------------------------------------------------------------------
```

```
   Current exclude-networks:

--------------------

--------------------

   Network ranges may be specified in two ways:
   1.  IP/Netmask - for example, 192.168.0.0/255.255.0.0
   2.  IP/CIDR    - for example, 192.168.0.0/16

   Please enter a network range to exclude (or press ENTER to quit).

>>

--------------------------------------------------------------------------------
                     LCE CONFIGURATION : Vulnerability Reporting
--------------------------------------------------------------------------------


    LCE will provide reports to SecurityCenter containing vulnerability
    information.  This is done over a secure connection requiring a
    username and password.  Default ones are provided, but it is recommended
    that you choose your own now if you have not done so already.

    The username and password will be the same as the ones you enter into
    SecurityCenter when you add this LCE as a passive scanner for
    vulnerability information.


    The current USERNAME is "username"

    Press ENTER to use this name, or enter a new one now.

>>


    The current PASSWORD is "passwd"

    Press ENTER to use this password, or enter a new one now.

>>

--------------------------------------------------------------------------------
                     LCE CONFIGURATION : Database Directory
--------------------------------------------------------------------------------


    Depending on your license, each LCE may store anywhere from 250 GB to
    10 TB of data in the event database.

    The database directory will now be checked for validity...

Press ENTER to continue

    The current database directory (/opt/lce/db/) has 500 GB free.
```

```
    If you would like to change the database directory, you may enter it now,
    or simply press enter to continue using the current selection.

>>

--------------------------------------------------------------------------------
                      LCE CONFIGURATION : Syslog Sensors
--------------------------------------------------------------------------------


    All events analyzed and stored by LCE have an associated sensor name.
    For events without a sensor name in the data itself, LCE may still assign
    a sensor name you designate based on the IP address of the sender.

    If you wish to name IP addresses as particular sensor names, you may do
    so now.
    This can also be updated later by modifying /opt/lce/admin/syslog_sensors.txt.

    The current configured Sensors are:

---------------------------------------

---------------------------------------


    IP Address  = ""
    Sensor Name = ""

    Please enter the IP address of the next Syslog Sensor,
    or press ENTER to quit entering Syslog Sensors:

>>

Done entering Syslog Sensors.

The Log Correlation Engine will now be updated with the latest plugins.
[LCE-Updater]: Disabling LCE Client update - there are no new changes.
[LCE-Updater]: The following files changed:

[LCE-Updater]: The following new files were added:
[LCE-Updater]: The following policy files changed:
[LCE-Updater]: The following new policy files were added:
[LCE-Updater]: Update complete.

--------------------------------------------------------------------------------
                      LCE CONFIGURATION : Complete
--------------------------------------------------------------------------------


    Congratulations!  LCE configuration has been completed.

    To begin collecting and analyzing data from your network in just minutes,
    please refer to the LCE Quick Start Guide. The LCE Administration and User
    Guide provides a detailed discussion of advance configuration items in
    /opt/lce/daemons/lce.conf, including:
```

```
      - Database archiving
      - Syslog forwarding
      - Automatic plugin updates
      - Load balancing across multiple LCE servers
      - NAT setup for LCE clients
      - IDS sensors
      - Processing of usernames and hostnames
      - Statistical anomaly parameters

     After you have accumulated a week of data or more, you should
     run the statistical anomaly engine by running:
           "service stats restart"


     Press ENTER to complete the configuration
     LCE Services will be restarted



Starting Log Correlation Engine
Log Correlation Engine Configuration
------------------------------------
       Database directory: /opt/lce/db/
   Silo archive directory:
            Log directory: /opt/lce/admin/log/
        Plugins directory: /opt/lce/daemons/plugins/
    Correlation directory: /opt/lce/daemons/plugins/
    Save unmatched events: no


-------------------------------------------------------
LICENSE: LCE 103-Silo Demo License for support
 EXPIRE: 05-29-2013
 REMAIN: 28
-------------------------------------------------------
License valid.
LCE license successfully updated.
                                                    [  OK  ]
Starting LCE Query Daemon                           [  OK  ]
Starting LCE Indexer                          [  OK  ]
Starting LCE Report Proxy                     [  OK  ]
```

LCE provides many options that can be fine-tuned to suit a wide variety of environments. Since this document focuses on getting LCE up running as quickly as possible, only the options that are prompted by the installation utility are noted. Please refer to the LCE documentation noted at the end of this document for more information on available options.

The **`/opt/lce/daemons/lce.conf`** file is used to specify all LCE configuration parameters. Any changes to this file must be performed using a text editor. For changes to go into effect, the LCE server process needs to be restarted, as described in the section below.

Basic LCE Server Operations

The RPM installation creates a service called **lce**. This section describes how to start, stop, and restart LCE.

Starting LCE

Use the following command to start the LCE server:

```
# service lce start
```

If the daemon terminates abnormally for any reason, the system will attempt to automatically restart the process and add a warning to the LCE logs.

Halting LCE

Use the following command to stop the LCE server:

```
# service lce stop
```

Restarting LCE

Use the following command to restart the LCE server:

```
# service lce restart
```

Determine LCE Status

Use the following command to acquire the status of the LCE server processes:

```
# service lce status
```

LCE Clients

The LCE Client is installed on hosts to monitor and collect events that are forwarded on to the LCE server daemon. When received by the LCE server, events are stored both as raw logs as well as normalized and correlated with vulnerabilities (if applicable). The SecurityCenter UI makes both the raw and normalized event data available to the user for event and analysis and mitigation.

The LCE supports many types of agents including:

- Windows Event Logs (collected locally or remotely via WMIC)
- Windows/Linux/Unix system and application logs
- Check Point OPSEC events
- Cisco RDEP events
- Cisco SDEE events
- NetFlow
- Splunk
- Sniffed TCP and UDP network traffic (Tenable Network Monitor)
- Sniffed **syslog** messages in motion
- File monitoring (Linux, Unix and Windows)

LCE has many signature processing libraries to parse logs and can normalize and correlate most network Intrusion Detection System (IDS) devices, as well as messages from SecurityCenter. The LCE supports the following IDS sources:

IDS Collection and Correlation

- Bro
- Cisco IDS
- Enterasys Dragon
- HP TippingPoint
- IBM Proventia (SNMP)
- Juniper NetScreen IDP
- McAfee IntruShield
- Fortinet IDS events
- Tenable's Passive Vulnerability Scanner (PVS)
- Snort (and Snort-based products)

TippingPoint's `syslog` event format must be modified to use a comma delimiter instead of a tab delimiter before it can be processed by the LCE.

IDS Collection Only

- AirMagnet
- Check Point (Network Flight Recorder)
- Portaledge
- Toplayer IPS

The list of officially supported log sources is frequently updated on the Tenable web site's LCE product page.

Installing the Linux Clients

To install the LCE Client, obtain the package for your OS platform and desired client and install as the *root* user on the target client system.

The following table provides an installation example for some of the available LCE Clients on supported platforms. Any special installation instructions are provided in a note following the example.

LCE Client	Installation Example
Red Hat	
LCE Log Agent	`# rpm -ivh lce_client-4.x.x-esX.i386.rpm`
LCE WMI Monitor Agent	`# rpm -ivh wmi_monitor-4.x.x-esX.i386.rpm`
Tenable NetFlow Monitor	`# rpm -ivh TenableNetFlowMonitor-4.x.x-esX.i386.rpm`
Tenable Network Monitor	`# rpm -ivh TenableNetworkMonitor-4.x.x-esX.i386.rpm`

A successful installation is indicated by the return of the command prompt with no errors.

Linux Client Configuration

Once the client is installed, the **lce-server** and **server-port** options in the client's **.conf** file must be configured.

LCE Client	Configuration File
Red Hat	
LCE Log Agent	`/opt/lce_client/lce_client.conf`
LCE WMI Monitor Agent	`/opt/wmi_monitor/wmi_monitor.conf`
Tenable NetFlow Monitor	`/opt/netflow_monitor/tfm.conf`
Tenable Network Monitor	`/opt/network_monitor/tnm.conf`

Change the **lce-server** option address to that of your LCE Server. For this example, both are on the same system, so we can use the localhost IP address of 127.0.0.1. After this is done, you will need to restart the LCE Client (see below).

The **.conf** files are no longer used to maintain monitoring options starting with the LCE 4.2.x client. The appropriate default policy will be pushed to the LCE 4.2.x client after it is authorized in the LCE clients section of SecurityCenter. Currently not all LCE clients are version 4.2 so the configuration file may still need to be edited for those clients.

Controlling the Linux Client

Below is a table that displays how to start, stop, and restart the client software on the various platforms:

LCE Client	Methods (start/stop/restart)
Red Hat	
LCE Log Agent	`# service lce_client {start|stop|restart|status}`
LCE WMI Monitor Agent	`# service wmi_monitor {start|stop|restart|status}`
Tenable NetFlow Monitor	`# service netflow_monitor {start|stop|restart|status}`
Tenable Network Monitor	`# service network_monitor {start|stop|restart|status}`

After the client is authorized by SecurityCenter, the local *.conf file is no longer used to manage the client.

Windows Client Configuration

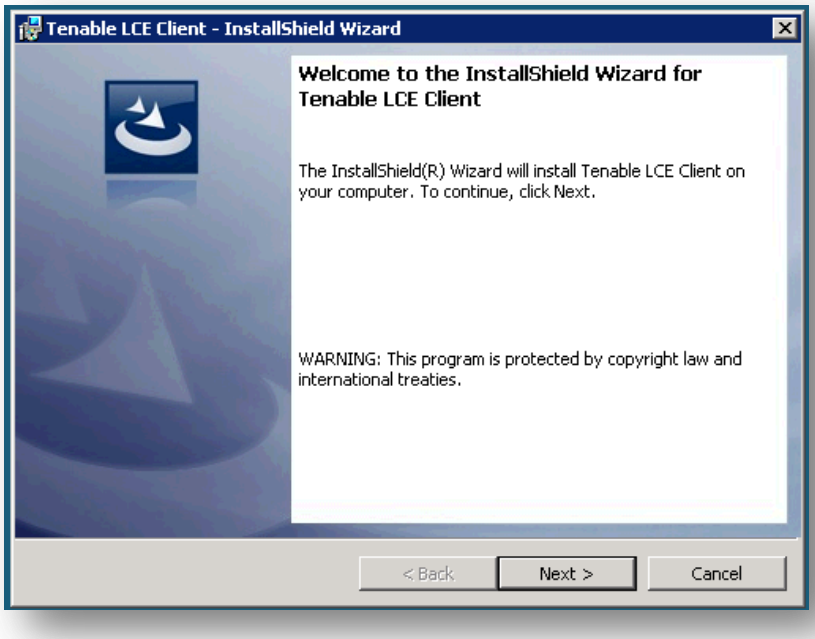
The Log Correlation Engine Windows Log Agent client monitors events, as well as specific log files or directories, for new event data. Tenable currently provides two Windows LCE Log Agents: one for Windows XP/2003 platforms and one for Windows Vista/2008/7 platforms.

Platform	LCE Client Type	Install File Name and Utility
MS Windows XP Professional, Windows Server 2003	LCE Log Agent	`lce_client-4.x.x-windows_2003_x86.msi`
MS Windows Server 2008, 2012 Windows Vista, Windows 7, 8	LCE Log Agent	`lce_client-4.x.x-windows_2008_x86.msi` `lce_client-4.x.x-windows_2008_x64.msi`

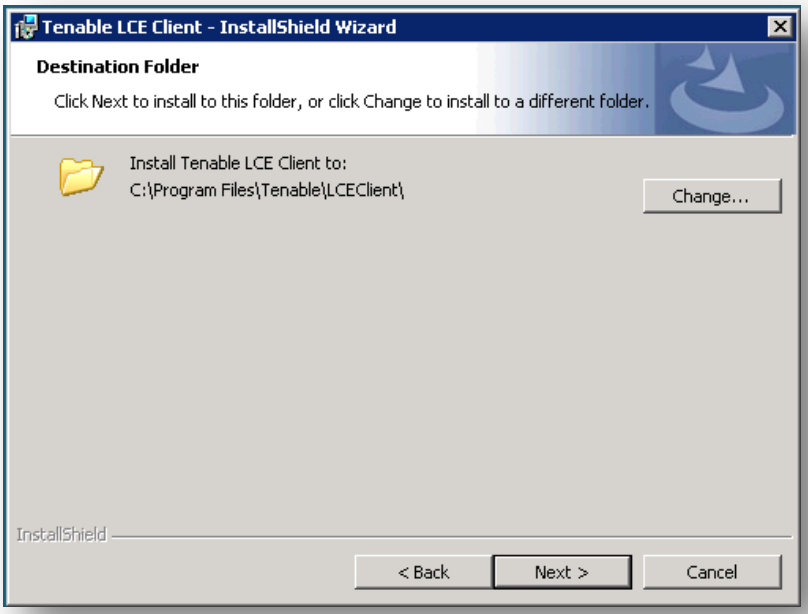
Installing the Windows Client

The LCE Windows Log Agent client is installed by clicking on the `.msi` distribution file, which will launch the InstallShield Wizard. On machines where Universal Access Control (UAC) is enabled, the user must run the installer as an Administrator level user. Right-click the installer icon and select "**Run as Administrator**".

A license agreement will be displayed that must be agreed to before installation can continue. The installer will prompt to choose if the application is to be shared or not, as shown in the following screen:



Click "**Next**".



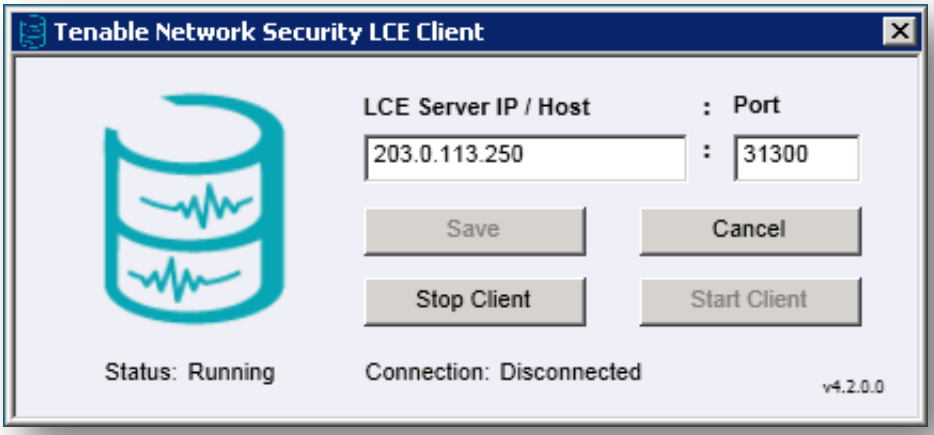
To use the default location, simply click "**Next**" and a screen will be displayed to begin the installation by clicking "**Install**". After a short period, the InstallShield Wizard will display a screen indicating that the installation is complete. Once installation is complete, you may be prompted to restart the system for the configuration changes to take effect.

Windows Client Configuration

To configure the LCE Windows Log Agent client, launch the LCE Configuration tool located at "**`C:\Program Files\Tenable\LCEClient\LCE_Server_Assignment.exe`**". Depending on options selected during installation, a shortcut icon(s) is created on the Desktop and the "**Start**" menu under "**Tenable Network Security**" called "**LCE Client Configuration**".

The only configuration required is the LCE server IP address or DNS name and the port (if the server is configured for one other than the default of 31300). All other configuration options will be managed by the LCE Client Manager upon connection.

An example screen for the LCE Client Configuration tool is shown below:



By default, the LCE Log Agent client is configured using a non-routable documentation IP address (203.0.113.250) and LCE Server Port 31300. These settings must be changed to the IP address or hostname and listening port of the actual LCE server. No further local configuration is required. Once set, select the "**Save**" button followed by "**Start Client**".

Once the client connects to the LCE server and is authorized by the LCE Client Manager, the appropriate configuration file will be pushed to the client.

Security Center Configuration

Please refer to the "Log Correlation Engines" section of the "SecurityCenter 4.7 Administration Guide" for details on how to add LCE to SecurityCenter.

For More Information

Tenable has produced a variety of additional documents detailing the LCE's deployment, configuration, user operation, and overall testing. These documents are listed here:

- Log Correlation Engine Architecture Guide – provides a high-level view of LCE architecture and supported platforms/environments.
- Log Correlation Engine Administrator and User Guide – describes installation, configuration, and operation of the LCE.
- Log Correlation Engine Client Guide – how to configure, operate, and manage the various Linux, Unix, Windows, NetFlow, OPSEC, and other clients.
- LCE High Availability Large Scale Deployment Guide – details various configuration methods, architecture examples, and hardware specifications for performance and high availability of large scale deployments of Tenable's Log Correlation Engine (LCE).
- LCE Best Practices – Learn how to best leverage the Log Correlation Engine in your enterprise.
- Tenable Event Correlation – outlines various methods of event correlation provided by Tenable products and describes the type of information leveraged by the correlation, and how this can be used to monitor security and compliance on enterprise networks.
- Tenable Products Plugin Families – provides a description and summary of the plugin families for Nessus, Log Correlation Engine, and the Passive Vulnerability Scanner.

- Log Correlation Engine Log Normalization Guide – explanation of the LCE's log parsing syntax with extensive examples of log parsing and manipulating the LCE's `.prm` libraries.
- TASL Reference Guide – explanation of the Tenable Application Scripting Language with extensive examples of a variety of correlation rules.
- Log Correlation Engine Statistics Daemon Guide – configuration, operation, and theory of the LCE's statistic daemon used to discover behavioral anomalies.
- Log Correlation Engine Large Disk Array Install Guide – configuration, operation, and theory for using the LCE in large disk array environments.
- Example Custom LCE Log Parsing - Minecraft Server Logs – describes how to create a custom log parser using Minecraft as an example.

Documentation is also available for Nessus, the Passive Vulnerability Scanner, and SecurityCenter through the Tenable Support Portal located at https://support.tenable.com/.

There are also some relevant postings at Tenable's blog located at http://blog.tenable.com/ and at the Tenable Discussion Forums located at https://discussions.nessus.org/community/lce.

For further information, please contact Tenable at support@tenable.com, sales@tenable.com, or visit our web site at http://www.tenable.com/.

About Tenable Network Security

Tenable Network Security is relied upon by more than 20,000 organizations, including the entire U.S. Department of Defense and many of the world's largest companies and governments, to stay ahead of emerging vulnerabilities, threats and compliance-related risks. Its Nessus and SecurityCenter solutions continue to set the standard to identify vulnerabilities, prevent attacks and comply with a multitude of regulatory requirements. For more information, please visit www.tenable.com.

GLOBAL HEADQUARTERS

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com