Table of Contents

Welcome to Log Correlation Engine ................................................................. 9
  Get Started ..................................................................................................... 10
Components of the Log Correlation Engine .................................................. 12
Hardware and Software Requirements ......................................................... 15
Install the LCE Server ....................................................................................... 21
  LCE Server Installation ................................................................................ 23
    Quick Setup ................................................................................................ 24
  Offline Activation and Plugin Updates ......................................................... 27
  Shortcuts for Running SQL Commands and Scripts ................................... 30
  SQL Scripts ................................................................................................... 32
    dimension-occurrence-stats.sql ............................................................. 40
    throughput--kilo-eps.sql ......................................................................... 42
Files and Layout .............................................................................................. 43
Location of PostgreSQL Files in an LCE Installation ..................................... 45
Tenable.sc CV Integration ............................................................................... 46
  Add LCE to Tenable.sc ................................................................................ 47
Configure Organizations .................................................................................. 49
Using Tenable.sc with LCE ............................................................................ 50
  Analyzing Events ......................................................................................... 51
Full Text Searches .......................................................................................... 53
Queries Against Archived Snapshots .......................................................... 58
Health and Status ............................................................................................ 59
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feed</td>
<td>60</td>
</tr>
<tr>
<td>Statistics</td>
<td>61</td>
</tr>
<tr>
<td>Data Sensors</td>
<td>63</td>
</tr>
<tr>
<td>Alerts</td>
<td>64</td>
</tr>
<tr>
<td>Advanced</td>
<td>66</td>
</tr>
<tr>
<td>System Configuration</td>
<td>67</td>
</tr>
<tr>
<td>Basic Configuration</td>
<td>68</td>
</tr>
<tr>
<td>Storage Configuration</td>
<td>70</td>
</tr>
<tr>
<td>IDS Configuration</td>
<td>72</td>
</tr>
<tr>
<td>High Availability</td>
<td>74</td>
</tr>
<tr>
<td>Configure High Availability</td>
<td>76</td>
</tr>
<tr>
<td>Migrate Your High Availability Configuration to LCE 6.0.4 or Later</td>
<td>80</td>
</tr>
<tr>
<td>Migrate Your High Availability Configuration to LCE 6.0.5 or Later</td>
<td>82</td>
</tr>
<tr>
<td>Monitor Your High Availability Configuration</td>
<td>84</td>
</tr>
<tr>
<td>Disable High Availability</td>
<td>87</td>
</tr>
<tr>
<td>Advanced Configuration</td>
<td>88</td>
</tr>
<tr>
<td>Data Forwarding</td>
<td>100</td>
</tr>
<tr>
<td>Receiving Encrypted Syslog</td>
<td>104</td>
</tr>
<tr>
<td>Example Encrypted TCP Syslog Configuration</td>
<td>106</td>
</tr>
<tr>
<td>TASL and Plugins</td>
<td>110</td>
</tr>
<tr>
<td>Event Rules</td>
<td>111</td>
</tr>
<tr>
<td>Event Rules Examples</td>
<td>118</td>
</tr>
<tr>
<td>Service Control</td>
<td>120</td>
</tr>
<tr>
<td>Feed Settings</td>
<td>121</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>LCE Windows Client Features</td>
<td>203</td>
</tr>
<tr>
<td>Configure the Windows Client Policy</td>
<td>204</td>
</tr>
<tr>
<td>LCE Client for Linux</td>
<td>205</td>
</tr>
<tr>
<td>OPSEC Client</td>
<td>206</td>
</tr>
<tr>
<td>Get Started with the LCE Splunk Client</td>
<td>207</td>
</tr>
<tr>
<td>Install, Configure, and Remove</td>
<td>208</td>
</tr>
<tr>
<td>Install the LCE Splunk Client</td>
<td>209</td>
</tr>
<tr>
<td>Configure the LCE Splunk Client</td>
<td>210</td>
</tr>
<tr>
<td>Remove the LCE Splunk Client</td>
<td>212</td>
</tr>
<tr>
<td>LCE Splunk Client Features</td>
<td>213</td>
</tr>
<tr>
<td>Data Comparison</td>
<td>214</td>
</tr>
<tr>
<td>Configure Splunk</td>
<td>216</td>
</tr>
<tr>
<td>Configure Splunk to Forward Data</td>
<td>217</td>
</tr>
<tr>
<td>Configure the Splunk Client Policy</td>
<td>218</td>
</tr>
<tr>
<td>Additional Resources</td>
<td>219</td>
</tr>
<tr>
<td>Splunk Client Policy Configuration Items</td>
<td>220</td>
</tr>
<tr>
<td>Delimiters</td>
<td>226</td>
</tr>
<tr>
<td>Tenable NetFlow Monitor</td>
<td>228</td>
</tr>
<tr>
<td>Tenable Network Monitor</td>
<td>229</td>
</tr>
<tr>
<td>Tenable RDEP Monitor</td>
<td>230</td>
</tr>
<tr>
<td>Tenable SDEE Monitor</td>
<td>231</td>
</tr>
<tr>
<td>Get Started with the LCE Web Query Client</td>
<td>232</td>
</tr>
<tr>
<td>Hardware Requirements</td>
<td>233</td>
</tr>
<tr>
<td>Software Requirements</td>
<td>234</td>
</tr>
</tbody>
</table>
Additional Resources .................................................................................................................. 266

Web Query Client Policy Configuration Items ........................................................................... 267

Correcting AWS Configuration Issues ....................................................................................... 276

Correcting Network Time Protocol Issues .................................................................................. 278

WMI Monitor Client ..................................................................................................................... 280

**Additional Resources** ........................................................................................................... 281

Tools ......................................................................................................................................... 282

install-PostgreSQL-man-pages ................................................................................................. 293

ts-test ...................................................................................................................................... 294

validate-prm-regex .................................................................................................................... 297

Perform an Online PostgreSQL Backup .................................................................................... 299

Restore an Online PostgreSQL Backup .................................................................................... 300

Site Policies .................................................................................................................................. 301

Rotate Web UI Credentials ......................................................................................................... 305

Encryption Strength ..................................................................................................................... 306

Configure TLS Strong Encryption ............................................................................................... 307

Configure LCE for NIAP Compliance .......................................................................................... 308

File and Process Allow List ........................................................................................................... 310

Refresh or Replace the Vulnerability Reporter SSL Certificate .............................................. 316

Import LCE Data Manually .......................................................................................................... 317

Manual Key Exchange with Tenable.sc .................................................................................... 318

User Tracking ............................................................................................................................... 320

Non-Tenable License Declarations ............................................................................................. 322

Silo Archiving ............................................................................................................................... 323
Welcome to Log Correlation Engine

This document describes the installation, configuration, and administration of the Tenable Log Correlation Engine® (LCE®) LCE 6.0.x for use as a part of Tenable.sc+.

Tip: Tenable rebranded Tenable.sc Continuous View as Tenable.sc+.

LCE is used with Tenable.sc, which is installed separately. This documentation assumes that you already have an operational instance of Tenable.sc. Knowledge of Tenable.sc operation and architecture is also assumed, along with a familiarity with system log formats from various operating systems, network devices, and applications and a basic understanding of Linux and Unix command line syntax. For more information, see the Tenable.sc User Guide.

In addition to the LCE server, Tenable provides the following clients:

- **LCE Client**
- **OPSEC Client**
- **Splunk Client**
- **Tenable NetFlow Monitor**
- **Tenable Network Monitor**
- **Tenable RDEP Monitor**
- **Tenable SDEE Monitor**
- **Web Query Client**
- **WMI Monitor Client**

Note: While you may still manage clients and policies using an account with Administrator privileges in Tenable.sc, LCE (versions 4.8 and later) is now the preferred method, as it provides additional validation to client management and policy modification. Additionally, organizations with a centralized instance of Tenable.sc can better delegate the administration of LCE by utilizing the new features, rather than channeling all LCE administration through Tenable.sc users with the necessary privileges.

For assistance with LCE, contact Tenable Support.
Get Started

Use the following getting started sequence to configure and maintain your LCE deployment.

Prepare

- Components
- Hardware and Software Requirements

Install

- Install LCE Server
- Run Quick Setup Wizard
- Offline Configuration & Plugin Updates

Configure

- Configure LCE server
  - Basic
  - Storage
  - IDS
  - Advanced
  - Control
  - Feed Setting
- Files & Layout
- Configure Organizations

Refine
• Create, Modify, and Assign Policies
• Manage Users
• Manage Clients

Expand

• Upgrade the LCE Server
• Upgrade your LCE License
• Additional Resources
Components of the Log Correlation Engine

The Log Correlation Engine (LCE) has three main components:

- **The LCE server**
  
  The LCE server is a set of cooperating daemons for Red Hat Enterprise Linux (RHEL) or CentOS Linux or Oracle Enterprise Linux (OEL) that collects data from the LCE clients, and then normalizes that data. The normalized data is then analyzed using Tenable.sc. Tenable.sc makes both the raw and normalized event data available to the user for event analysis and mitigation. Depending on the scale and requirements of your organization, you may utilize multiple LCE server instances to collect and normalize data.

- **The LCE interface**
  
  Each LCE server provides a web-based application interface, referred to throughout this documentation as the **LCE interface**. Using the LCE interface, you can monitor the health and status of the LCE server and clients, configure the LCE server, manage clients, create and assign policies, and manage users.

- **LCE clients**
  
  LCE clients are installed on hosts to monitor and collect events. The event data is then communicated to the LCE server. Events are both stored as raw logs and normalized and correlated with vulnerabilities (if applicable).

LCE users work with log data from a wide variety of sources. Each organization can make queries to one or more LCE servers that process events from devices including firewalls, servers, routers, honeypots, mobile device managers, applications, and many other sources. LCE can collect event data from many sources, including:

- **Windows Event Logs** (collected locally or remotely via a WMI client)
- **Windows, Linux, and 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
- Encrypted syslog
- File monitoring for the following operating systems:
  - RHEL
  - Tenable Appliance
  - FreeBSD
  - Debian
  - OS X
  - AIX
  - Solaris
  - HP-UX
  - Dragon
  - Fedora
  - Ubuntu
  - SuSE
  - Windows
- Salesforce
- Amazon Web Services, via CloudTrail
- Google Cloud Platform

Intrusion Detection and Prevention Systems
LCE has many signature processing libraries to parse logs and can normalize and correlate most network intrusion detection (IDS) and intrusion protection systems (IPS), as well as messages from Tenable.sc.

LCE supports event collection and vulnerability correlation for the following systems:

- Bro
- Cisco IDS
- Enterasys Dragon
- IBM Proventia (SNMP)
- Juniper NetScreen IDP
- McAfee IntruShield
- Fortinet IDS events
- Snort (and Snort-based products)
- HP TippingPoint

**Note:** TippingPoint’s syslog event format must be modified to use a comma delimiter rather than a tab delimiter before it can be processed by the LCE.

LCE supports only event collection for the following systems:

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

There are thousands of normalization rules that support most operating systems, firewalls, network routers, intrusion detection systems, honeypots, and other network devices. The list of officially supported log sources is frequently updated on the Tenable website.
Hardware and Software Requirements

Before deploying LCE, confirm that the prerequisite software and hardware requirements have been met and that you have an operational instance of Tenable.sc. Depending on the size of your organization and the way you deploy LCE, the hardware requirements for LCE change. All deployments have a common set of minimum software requirements.

This section contains the following:

- **Software Requirements**
- **Hardware Requirements**
- **System Specifications**
- **Licenses**
- **File System Recommendations**

Software Requirements

All deployments of LCE require the following:

- An active LCE license
- One of the following operating systems:
  - RHEL/CentOS/OEL 6.x, 64-bit
  - RHEL/CentOS/OEL 7.x, 64-bit
  - RHEL/CentOS/OEL 8.x, 64-bit

Additionally, while LCE is active, it requires exclusive access to certain ports. The only services that are required to support remote users are SSH and the LCE interface (`lce_wwwd`). If other services are active on the system, conflicts should be avoided on the following default ports:

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>162/UDP</td>
<td>SNMP</td>
</tr>
<tr>
<td>Port</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>514/UDP</td>
<td>Syslog (forwarded)</td>
</tr>
<tr>
<td>22/TCP</td>
<td>SSH, for requests from Tenable.sc</td>
</tr>
<tr>
<td>601/TCP</td>
<td>Syslog</td>
</tr>
<tr>
<td>1243/TCP</td>
<td>Vulnerability detection, if enabled in Tenable.sc</td>
</tr>
<tr>
<td>6514/TCP</td>
<td>Encrypted syslog</td>
</tr>
<tr>
<td>8836/TCP</td>
<td>LCE Administrative Web UI</td>
</tr>
<tr>
<td>31300/TCP</td>
<td>Events from LCE Clients</td>
</tr>
<tr>
<td>5432/TCP</td>
<td>PostgreSQL replication from the master node or the standby node in a high availability configuration. For more information, see <a href="#">High Availability</a>.</td>
</tr>
<tr>
<td>7091/TCP</td>
<td><code>showids</code> commands forwarded from the master node to the standby node in a high availability configuration. For more information, see <a href="#">High Availability</a>.</td>
</tr>
<tr>
<td>VRRP</td>
<td>Keepalived virtual IP management in a high availability configuration. For more information, see <a href="#">High Availability</a>.</td>
</tr>
<tr>
<td>Ports LCE Uses Over Loopback Interface</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Port 7091/TCP</td>
<td>Internal communication, <code>showids</code> to <code>lce_queryd</code></td>
</tr>
<tr>
<td>Port 7092/TCP</td>
<td>Internal communication, <code>lce_tasld</code> to <code>1ced</code></td>
</tr>
<tr>
<td>Port 7093/TCP</td>
<td>Internal communication, <code>showids</code> to <code>lce_queryd</code></td>
</tr>
</tbody>
</table>

**Caution:** The system running the LCE can operate a syslog daemon, but the syslog daemon must not be listening on the same port(s) that the LCE server is listening on.

**Hardware Requirements**

The hardware requirements for LCE change based on the number of events being processed.

**Estimating Events**

The following table provides the estimated average number of events from various sources.

<table>
<thead>
<tr>
<th>Devices</th>
<th>Number of Estimated Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 workstation/laptop</td>
<td>0.5 events/sec</td>
</tr>
<tr>
<td>1 web-facing app server</td>
<td>20 events/sec</td>
</tr>
<tr>
<td>1 web-facing firewall/IDS/IPS</td>
<td>75 events/sec</td>
</tr>
<tr>
<td>1 internal application server (low volume)</td>
<td>5 events/sec</td>
</tr>
<tr>
<td>1 internal application server (high volume: IIS, Exchange, AD)</td>
<td>20 events/sec</td>
</tr>
<tr>
<td>1 internal network device</td>
<td>2 events/sec</td>
</tr>
</tbody>
</table>

To convert your event rate to bytes per day, it is recommended that you multiply your total events/second by 250 bytes/event and multiply by 86,400 seconds/day. For example, assume 100 events per second: 100 events/second * 250 bytes/event * 86,400 seconds/day = 2,160,000,000 bytes/day.

**System Specification**
The following table specifies the system requirements based on the number of events the LCE server is processing.

<table>
<thead>
<tr>
<th>Installation scenario</th>
<th>RAM</th>
<th>Processor</th>
<th>Hard disk</th>
<th>Hard disk space</th>
</tr>
</thead>
<tbody>
<tr>
<td>One LCE server with PostgreSQL processing</td>
<td>22 GB</td>
<td>8 cores</td>
<td>10,000 RPM HD, or SSD of equiv. IOPS capability; RAID 0/10</td>
<td>2.4x Licensed</td>
</tr>
<tr>
<td>less than 5,000 events per seconds</td>
<td></td>
<td></td>
<td>configuration</td>
<td>storage size</td>
</tr>
<tr>
<td>One LCE server with PostgreSQL processing</td>
<td>30 GB</td>
<td>16 cores</td>
<td>15,000 RPM HD, or SSD of equiv. IOPS capability; RAID 0/10</td>
<td></td>
</tr>
<tr>
<td>between 5,000 and 20,000 events per second</td>
<td></td>
<td></td>
<td>configuration</td>
<td></td>
</tr>
<tr>
<td>One LCE server with PostgreSQL processing</td>
<td>58 GB</td>
<td>24 cores</td>
<td>SSD of IOPS capability at least equiv. to a 15,000 RPM HD;</td>
<td></td>
</tr>
<tr>
<td>greater than 20,000 events per second</td>
<td>or more</td>
<td>or more</td>
<td>RAID 0/10 configuration</td>
<td></td>
</tr>
</tbody>
</table>

The LCE server requires a minimum of 20 GB of storage space to continue running and storing logs. The current system disk space is visible on the [Health and Status page](#) of the LCE interface.

To ensure LCE can take full advantage of the host's RAM and CPU resources, Tenable recommends configuring a dedicated swap partition. If the host has $N$ GB of RAM, you will need at least $1.6 \times N$ GB of swap space for best performance.

**High Availability Requirements**

Tenable strongly recommends using the same system specifications on the master and standby nodes in your high availability configuration, including the following:

- Operating system version, to the patch level
- Layout and size of disk partitions
• File system choice and mount options
• RAM size
• Swap size

For optimal stability and performance, the master and standby nodes should be connected by a fast and reliable network link. For more information about high availability configurations, see High Availability.

File System Recommendations

Placing your activeDb on a networked file system (e.g. NFS) results in inadequate system performance. Tenable recommends that you use EXT3, EXT4, XFS, or ZFS and that you pay close attention to the mount options.

Placing your archiveDb on a networked file system does not impact system performance.

<table>
<thead>
<tr>
<th>If your file system is:</th>
<th>Tenable recommends:</th>
<th>Tenable does not recommend:</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXT3, EXT4, XFS</td>
<td>noatime</td>
<td>atime or strictatime or relatime or diratime or No *atime at all.</td>
</tr>
<tr>
<td>EXT3</td>
<td>barrier=0</td>
<td>barrier=1</td>
</tr>
<tr>
<td>EXT4</td>
<td>barrier=0 or nobarrier</td>
<td>barrier=1 or barrier</td>
</tr>
<tr>
<td>XFS</td>
<td>nobarrier</td>
<td>barrier</td>
</tr>
<tr>
<td>EXT3, EXT4</td>
<td>data=writeback</td>
<td>data=journal or data=ordered or No data=* at all.</td>
</tr>
<tr>
<td>ZFS</td>
<td>atime=off</td>
<td>atime=on or relatime=on or No *atime at all.</td>
</tr>
<tr>
<td>ZFS</td>
<td>Hardware-dependent</td>
<td>compression=gzip or compression=gzip-N or compression=zle or compress=gzip or compress=gzip-N or compress=zle</td>
</tr>
<tr>
<td>ZFS</td>
<td>logbias=throughput</td>
<td>logbias=latency or No logbias at all.</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>ZFS</td>
<td>primarycache=metadata</td>
<td>primarycache=all or primarycache=none or No primarycache=* at all.</td>
</tr>
<tr>
<td>ZFS</td>
<td>Hardware-dependent</td>
<td>recordsize=512 or recordsize=1024 or recordsize=2048 or recordsize=4096</td>
</tr>
</tbody>
</table>

**Licenses**

There is no licensed limit to the number of events or IPs that the LCE can be configured to monitor.

There are different licenses available for LCE based on the total amount of storage used by LCE. The licenses are based on 1 TB, 5 TB, and 10 TB storage sizes. A license for LCE is provided as a part of Tenable.sc Continuous View. There is no difference in the LCE software that is installed, just the maximum storage size that can be used by LCE. Data that exceeds your license limit will be off-lined.
Install the LCE Server

Before You Begin:

- Download the LCE server package from the Tenable downloads page.
- Install the software the LCE server is dependent on.

Installation Location

Caution: /opt/lce/ must not contain any symbolic links.

Installing the Package

**Note:** To ensure consistency of audit record time stamps between the LCE and Tenable.sc, make sure that the underlying OS makes use of the Network Time Protocol (NTP) as described at http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/sect-Date_and_Time_Configuration-Command_Line_Configuration-Network_Time_Protocol.html

If you are upgrading from a previous version of LCE, please skip this section and see Upgrade the LCE Server. Please follow the instructions in this section for new installations.

To install the LCE RPM, enter the following command: `rpm -ivh <package name>`, where `<package name>` is the name of the LCE server package you downloaded from the Tenable downloads page.

For example:

Preparing... #COMPLETE
[100%]
1:lce #COMPLETE
[100%]
The installation process is complete.
Please refer to /var/log/lce_upgrade.log to review installation messages.
This is a new installation. To configure LCE, please direct your browser to:
https://192.168.1.101:8836

The installation process will create a user and group named lce and install the LCE server to the /opt/lce directory. All files will be installed with the user and group of lce except for the majority of LCE daemons, which are set-user-id root. An LCE daemon is started by the root user; once the appropriate port(s) are bound, it will drop root privileges.
LCE Server Installation

The following procedure must be performed as the root user:

1. **Download the LCE server package.**

   **Tip:** After downloading the LCE server package, you can view information about the software the server is dependent on by using the following command:

   ```
   # rpm -qRp <LCE rpm>
   ```

   ...where `<LCE rpm>` is the path to and filename of the package you downloaded. For example, `/tmp/lce-6.0.2-el6.x86_64.rpm`.

2. Confirm the integrity of the package by comparing the MD5 checksum with the one listed in the **product release notes**.

3. **Install the LCE server.**

4. Copy the activation code from the [Tenable Community site](https://tenable.com/community), as described in the Tenable Community Guide.

5. Using a web browser, navigate to the address or hostname of the LCE server on port 8836 (https://<ip or hostname>:8836).

   **Tip:** Ensure that the firewall on the system allows TCP traffic through port 8836, otherwise the web UI will be inaccessible. For example, iptables or firewalls may be blocking port 8836 by default. A full list of required ports is included in the **Software Requirements**.

6. **Complete the Quick Setup wizard.**

7. **Add the LCE server to Tenable.sc.**
Quick Setup

Before You Begin:

- Complete the LCE server installation.

Tip: If you need to correct a value during the Quick Setup, you can click the Previous Step button.

To complete the quick setup:

1. In a browser, navigate to the LCE interface for the server (https://<hostname or IP address>:8836).
   The sign-in page appears.

2. In both the Username and Password boxes, type admin.

3. Click the Sign In To Continue button.
   The Quick Setup Change Default Password dialog box appears.

4. In the New Password and Confirm Password boxes, type a password that is a minimum of four alphanumeric characters.
   Note: Required password complexity can be configured later.

5. Click the Next Step button.
   The Quick Setup Proxy Configuration dialog box appears.

6. (Optional) if a proxy is utilized in the environment where LCE is deployed, select Yes, and then enter the required information into the Proxy Address, Proxy Username, Proxy Password, and Confirm Proxy Password boxes.

7. Click the Next Step button.
   The Quick Setup Set Activation Code dialog box appears.

Caution: If the LCE server instance you are trying to activate is not connected to the Internet, you will need to perform the Offline Activation procedure. Complete that procedure, then continue this procedure from step 9.
8. In a separate browser, find your activation code on the Tenable Community site, as described in the Tenable Community Guide.

9. In the LCE browser, in the Activation Code box, type the corresponding activation code from the Tenable Community site.

10. Click the Apply button.

11. Click the Next Step button.

   The Quick Setup Port Configuration dialog box appears.

   The boxes are populated with the default ports for each type of communication.

12. (Optional) modify the values, and then click the Apply button.

   **Note:** It is recommended that you use the default ports unless a conflict is identified.

13. Click the Next Step button.

   The Quick Setup Database Directory dialog box appears.

   By default, the Database Directory box is set to /opt/lce/db/. The Database Directory box specifies the location on the host where the LCE server will create and maintain silos.

14. Confirm that the available space in the directory is sufficient for your LCE license.

15. Click the Next Step button.

   The Quick Setup Network Ranges dialog box appears.

16. In the Monitored Network box, type the network range that LCE will monitor. The network range must be entered in either CIDR notation, or <IP>/<netmask> format. For example, 192.168.0.0/24 or 192.168.0.0/255.255.255.0.

17. In the Excluded Network box, type a network range that you do not want to be monitored by LCE. The network range must be entered in either CIDR notation, or <IP>/<netmask> format.

18. Click the Next Step button.

   The Quick Setup Tenable.io dialog box appears.
19. (Optional) to send vulnerability reports to Tenable.io, select Yes, and then enter the required information into the Cloud Address, Cloud Port, Cloud Scanner Key, and Scanner Name boxes.

When the LCE server is configured to send vulnerability reports to Tenable.io, the LCE server will query Tenable.io for jobs. The Job Queue Check Rate specifies the amount of time that will elapse between each query.

20. In the Job Queue Check Rate Min and Sec boxes, specify the amount of time that you want to elapse between each query.

21. Click the Next Step button.

The Quick Setup Complete dialog box appears.

22. Click the Restart button.

Quick Setup is completed, and the LCE server and services restart. When the restart is complete, you can sign in to the LCE interface to complete any additional configuration your organization requires, including syslog forwarding, load balancing configuration, and NAT setup for LCE clients, among other configuration items.
Offline Activation and Plugin Updates

Offline Activation

To activate LCE and update LCE plugins on an air-gapped network:

1. Obtain your LCE activation code from the Tenable Community site, as described in the Tenable Community Guide.
2. Copy the activation code to be used with the offline LCE server.
3. Log in to the offline LCE terminal as the root user.
4. In the CLI in LCE, run the following command:

```
# /opt/lce/daemons/lce_wwwd --challenge
Challenge:
  e1e02d38a48603467fb8728b13ada3e29e5e9fd4
Copy the challenge above and paste it (with your Activation Code) into:
  https://plugins.nessus.org/v2/offline-lce.php
```

5. Copy the challenge code to be used with the offline LCE server.
6. Go to https://plugins.nessus.org/v2/offline-lce.php and enter the activation code and challenge code obtained in the previous steps.
7. Select the generated link to download the current plugin set. Make a copy of the link that is returned. The link provided will be valid until the LCE subscription expires.
8. Save the link, as it will be needed each time the plugins are manually updated.
9. Select the link to download the license key, lce.license, or create an lce.license file by copying the license into a text file from -----BEGIN TENABLE LICENSE----- to -----END TENABLE LICENSE-----.
10. On the LCE server host, copy the lce.license file to /opt/lce/daemons, and run the following command:

```
# /opt/lce/daemons/lce_wwwd --register-offline lce.license
```
11. Go to https://<ip address of your lce>:8836 and complete the Quick Setup.

12. To verify the license has been loaded successfully, on the top navigation bar, click **Health and Status**.

13. On the left pane, click **Plugins**.

   The **Activation Status** should be **Licensed**.

---

**Offline Plugin Updates**

**Before you begin:**

- Complete step 5 of the **Offline Activation** procedure to obtain a link to download the latest lce-combined.tar.gz file.

  You will use this link to obtain the latest plugins for the duration of your LCE subscription. The lce-combined.tar.gz file contains updates for LCE PRM(s), TASL(s), discoveries, client policies, the web client, and the web server.

**To perform an offline plugin update:**

1. Download the latest lce-combined.tar.gz file.

2. Log in to the LCE interface (https://<ip address of your lce>:8836).

3. Click **Configuration** on the top navigation bar.

   The **Configuration** page appears, displaying the **Basic** section.

4. Click **Feed Settings** on the left pane.

   The **Feed Settings** section appears.

5. Under **Offline Plugin Update**, click the **Add Plugins** button, and then select the lce-combined.tar.gz file you downloaded in step 1.

6. After the file is successfully uploaded, click the **Process Plugins** button. The process may take a short time to complete.

7. To verify the plugins have been successfully loaded, on the top navigation bar, click **Health and Status**, and then, on the left pane, click **Feed**. The **Plugin Set** and the **Plugin Set Loaded**
should now reflect the latest set of plugins. For example, a value of 201907222231 is interpreted as 2019-07-22 22:31.
Shortcuts for Running SQL Commands and Scripts

For more information about the individual SQL scripts relevant to administration and to troubleshooting or performance tuning, see [Tools](#).

After logging in to a console window and invoking:

```
source /opt/lce/tools/source-for-psql-shortcuts.sh
```

A reminder banner will appear:

```
USAGE of the enabled shortcuts:

psqlc  "<a SQL command>"

psqlf  <path to script with SQL commands>  [arg1] [arg2] [...]]

psqli

Invokes interactive prompt. Note that you can also invoke SQL scripts from within the interactive prompt, like so:   \i <path to script>

; you will then be prompted for script args.
```

**psqlf**

You can use the `psqlf` shortcut to run the various SQL scripts packaged with LCE that are found under `/opt/lce/tools/pg-helper-sql/`.

Here is an example of running a SQL script that takes no arguments:

```
psqlf pg-helper-sql/recent-alerts-24hours.sql
```

And here is an example of running a SQL script that takes an argument:

```
psqlf pg-helper-sql/disk-usage-one-silo.sql 0
```

To quickly locate and run a script:
1. Log in to LCE via the command line interface (CLI).

2. Type `psqlf` followed by a space.

3. Type the first few letters of the name of the script you want to run. For example, to run `wal-activity.sql`, you can type `wa`.

4. Press Tab.
   
   `psqlf` automatically completes the name of the script.

5. To run the script, press Enter.
   
   LCE runs the selected script.
**Caution:** You must run `source /opt/lce/tools/source-for-pgsql-shortcuts` once in a console, before you can run `psqlf <someScript.sql>` commands in that console.

<table>
<thead>
<tr>
<th>File</th>
<th>Usage/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration: Disk Usage</td>
<td></td>
</tr>
<tr>
<td>activeDb-size.sql</td>
<td>Breaks down datastore's disk usage by major categories.</td>
</tr>
<tr>
<td>disk-usage-one-silo.sql</td>
<td>States how much disk is being used by this table and associated database objects.</td>
</tr>
<tr>
<td></td>
<td>&lt;silo#&gt;</td>
</tr>
<tr>
<td>disk-usage-summary.sql</td>
<td>Gives a concise summary of disk usage by table category (tables which store events, tables which maintain filter pointers, rollup counts tables, etc.) Output of this script has been added to diag report to facilitate troubleshooting.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>drop-indexes-on-older-silos.sql</td>
<td>Allows operator to easily free up disk space by dropping indexes on silos which have not yet been archived or trimmed out of activeDb, but are no longer queried.</td>
</tr>
<tr>
<td></td>
<td>[how old, in whole days, must a silo be to have its indexes dropped]</td>
</tr>
<tr>
<td>Administration: PostgreSQL Processes</td>
<td></td>
</tr>
<tr>
<td>breve-processes.sql</td>
<td>Shows the SQL command (up to available screen width) being executed by each process. Automatically refreshes display every N (defaults to 10) seconds.</td>
</tr>
<tr>
<td></td>
<td>[refreshInterval_seconds, defaults to 10; 0 to only show once]</td>
</tr>
<tr>
<td>Script Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>expand-processes.sql</td>
<td>Shows complete SQL command (up to 2048 characters) being executed by each process.</td>
</tr>
<tr>
<td>progress-analyze.sql</td>
<td>Lists processes running ANALYZE commands, names the target tables and/or indexes, and estimates progress.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;refreshInterval_seconds, defaults to 15; 0 to only show once&gt;</code></td>
</tr>
<tr>
<td>progress--bulk-load.sql</td>
<td>Lists processes inserting rows into the siloN tables, and estimates progress; can also track the progress of creating archiveDb snapshots.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;refreshInterval_seconds, defaults to 5; 0 to only show once&gt;</code></td>
</tr>
<tr>
<td>progress--index-or-reindex.sql</td>
<td>Lists processes running CREATE INDEX or REINDEX commands, names the target objects, and estimates progress.</td>
</tr>
<tr>
<td>progress--rebuild-table.sql</td>
<td>Lists processes running CLUSTER commands, names the target objects, and estimates progress.</td>
</tr>
<tr>
<td>progress--stream-backup.sql</td>
<td>Lists processes taking a backup (see Perform an Online PostgreSQL Backup) and estimates progress.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;refreshInterval_seconds, defaults to 60; 0 to only show once&gt;</code></td>
</tr>
<tr>
<td>progress--vacuum.sql</td>
<td>Lists processes running VACUUM commands, names the target objects, and estimates progress.</td>
</tr>
<tr>
<td>Administration: LCE Configuration and Alerts</td>
<td></td>
</tr>
<tr>
<td>alerts-by-day.sql</td>
<td>For more information, see Alerts.</td>
</tr>
<tr>
<td>alerts-by-month.sql</td>
<td>For more information, see Alerts.</td>
</tr>
<tr>
<td><strong>recent-alerts-24hours.sql</strong></td>
<td>For more information, see <a href="#">Alerts</a>.</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------</td>
</tr>
</tbody>
</table>
| **show-config--changed-since-rpm-install.sql** | Shows the following for each configuration attribute changed since the LCE RPM was installed:  
  - Name  
  - Current value  
  - Date of last modification |
| **show-config--mv--event_rules.sql** | For clearly displaying the configured event rules. You may find this presentation preferable to the one in Web UI. For more information, see [Show All Event Rules](#). |
| **Administration: License and Utilization Counting Toward License Limits** |  |
| **show-status.sql** | Displays information which had formerly been available in command-line environment by invoking 
 `/opt/lce/tools/lce_cfg_utils --display-status`: daily syslog counts, syslog sources, LCE daemons’ latest start time, etc. Normally an operator will not need this utility, because all that information is also available in LCE Web UI. |
| **silos.sql** | Lists silos ordered by timestamp of oldest event. For each silo, shows:  
  - how many events are inside  
  - how much rawlog those events collectively contain  
  - that silo’s provenance (whether it had been recorded live, migrated in from an earlier LCE version, or imported from a plain-text file)  
  - presence in activeDb: N if not, Y if yes, P if present but only temporarily to satisfy “archive-peek” queries. |
- presence in archiveDb: N if not, Y if yes.
- TASL %: what percentage of this silo has been scanned for processing by TASL scripts.

Statistics About Stored Events and Event Normalization

**dimension-occurrence-stats.sql**
Permits insight into distribution of the normalized dimensions (event1, event2, sensor, type, user) among stored events.

For additional information, see **dimension-occurrence-stats.sql**.

```
event1|event2|sensor|type|user
[--long]
```

**ip-occurrence-stats.sql**
Reports how many stored events are covered by each configured include_networks range. Also, shows top 100 srcIP by event volume (only including IPs recorded in least 5 events/minute on average): this can help you make a better-informed decisions about what range(s) to configured in include_networks.

**normalization-percentages.sql**
For each dimension (event1, event2, sensor, type, user) reports for what percentage of stored events the respective dimension is known. The numbers are broken down by silo: this lets you quickly gauge extent of event normalization achieved, as well as track progress over time.

**throughput--kilo-eps.sql**
Shows volume of event influx, by the hour, in units of 1000 events per second.

For additional information, see **throughput--kilo-eps.sql**.
useful-and-idle--plugins.sql | Helps you make an informed decision about which PRM and TASL plugins can be disabled without decreasing your event normalization levels; lets you immediately identify any custom plugins which are not working.

rawlog-storage.sql | Shows percentile statistics for rawlog length in a given silo's events.

Tip: To disable any of the plugins, run the command provided in the output.

Performance Tuning

buffer-cache--cat- | Summarizes the current allocation of the PostgreSQL buffer
<table>
<thead>
<tr>
<th>Categories.sql</th>
<th>Shows which indexes have been used in queries and how often.</th>
</tr>
</thead>
<tbody>
<tr>
<td>index-usage-silo.sql</td>
<td>Summarizes some useful information about indexes defined on respective tables.</td>
</tr>
<tr>
<td>indexes-nonsilo.sql</td>
<td>Lists database object locks currently held by user-focused PostgreSQL tasks.</td>
</tr>
<tr>
<td>indexes-silo-fp.sql</td>
<td>Shows estimates that the PostgreSQL query optimizer is now relying on when it generates an access plan for querying the given table. For each column, shows $M$ (defaults to 10) most common values.</td>
</tr>
<tr>
<td>indexes-silo-proper.sql</td>
<td>For each column, shows $M$ (defaults to 10) most common values.</td>
</tr>
<tr>
<td>locks.sql</td>
<td>Lists stored procedures and gives some rudimentary invocation statistics.</td>
</tr>
<tr>
<td>planner-estimates-silo.sql</td>
<td>Rebuilds index on the rawlog column. Required to apply modified text search configuration retroactively to events already stored.</td>
</tr>
<tr>
<td>routines.sql</td>
<td>Shows how many times respective tables had been ANALYZEd and/or VACUUMed, and whether a given table has changed since.</td>
</tr>
<tr>
<td>Table/Script Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>table-access-stats--silo-fp.sql</td>
<td>Shows how much disk is being used by each table along with its indexes.</td>
</tr>
<tr>
<td>table-access-stats--silo-proper.sql</td>
<td></td>
</tr>
<tr>
<td>table-sizes-nonsilo.sql</td>
<td></td>
</tr>
<tr>
<td>top-statements--by--all-exe-time.sql</td>
<td>Tells which SQL commands and stored-procedure calls take the longest to run.</td>
</tr>
<tr>
<td>top-statements--by--n-calls.sql</td>
<td>Tells which SQL commands and stored-procedure calls are called most frequently.</td>
</tr>
</tbody>
</table>

**Troubleshooting**

<table>
<thead>
<tr>
<th>Script Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>identify-currsilo.sql</td>
<td>Prints numeric ID of the silo that incoming new events are now being written to.</td>
</tr>
<tr>
<td>ipfilters-overview.sql</td>
<td>Lists IP filters used in recent queries. Shows the first few IP addresses or IP address ranges of each filter. To see all the IP addresses or IP address ranges belonging to a particular filter, use the reconstitute-ipfilter.sql script.</td>
</tr>
<tr>
<td>lock-blockers.sql</td>
<td>Shows which processes are waiting their turn to access a particular database object.</td>
</tr>
<tr>
<td>migr-full-status.sql</td>
<td>Details migration plan and how far has each of its items been executed.</td>
</tr>
<tr>
<td>n-events--by-hhour--bar-chart.sql</td>
<td>Displays a rudimentary bar chart to give a rough idea of variation in log volume through the day or through the week. Another view of this information is provided by the throughput--kilo-eps.sql script.</td>
</tr>
<tr>
<td>SQL Query</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>presence-dim-by-hhour.sql</code></td>
<td>Displays a concise info-graphic of the presence of a particular type (or user, or sensor, or ...) among the events in a given silo, with half-hourly granularity. This can provide a bare-bones reporting capacity even when a Tenable.sc connection is interrupted.</td>
</tr>
<tr>
<td>`event1</td>
<td>event2</td>
</tr>
<tr>
<td><code>recent-kinds-5minutes.sql</code></td>
<td>Summarizes events most recently added to activeDb by kind.</td>
</tr>
<tr>
<td><code>recent-kinds-60minutes.sql</code></td>
<td></td>
</tr>
<tr>
<td><code>reconstitute-ipfilter.sql</code></td>
<td>Lists all the IP addresses, or IP address ranges, belonging to a particular filter.</td>
</tr>
<tr>
<td></td>
<td>&lt;ipfilterId&gt;</td>
</tr>
</tbody>
</table>
**Usage:**

```
event1|event2|sensor|type|user [--long]
```

If the `--long` option is not given, only basic information is shown. For example, a partial sample output of `psqlf /opt/lce/tools/pg-helper-sql/dimension-occurrence-stats.sql` type is:

<table>
<thead>
<tr>
<th>nickn</th>
<th>name</th>
<th>total #</th>
<th>rank by total #</th>
<th>First Seen</th>
<th>Latest Seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>network</td>
<td>39,234,655</td>
<td>1</td>
<td>2019 Aug23 15:30</td>
<td>2019 Sep19 18:30</td>
</tr>
<tr>
<td>15</td>
<td>database</td>
<td>1,765,733</td>
<td>19</td>
<td>2019 Aug24 16:30</td>
<td>2019 Sep10 19:30</td>
</tr>
<tr>
<td>10</td>
<td>restart</td>
<td>1,679,365</td>
<td>20</td>
<td>2019 Aug24 13:00</td>
<td>2019 Sep17 06:30</td>
</tr>
</tbody>
</table>

This table shows that no events of type=database have been normalized since Sep 10th. Information such as this can be helpful in troubleshooting PRM issues.

If the `--long` option is given, these additional 5 columns (min, 25th %, median, 75th %, and max) are generated. For example, a partial sample output of `psqlf /opt/lce/tools/pg-helper-sql/dimension-occurrence-stats.sql` type `--long` would be:

<table>
<thead>
<tr>
<th>nickn</th>
<th>name</th>
<th>total #</th>
<th>rank by total #</th>
<th>First Seen</th>
<th>Latest Seen</th>
<th>min</th>
<th>25th %</th>
<th>median</th>
<th>75th %</th>
<th>max</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>network</td>
<td>39,234,655</td>
<td>1</td>
<td>2019 Aug-9</td>
<td>201-9 Sep-9</td>
<td>0.00-73</td>
<td>0.97-83</td>
<td>0.99-39</td>
<td>0.99-87</td>
<td>0.99-97</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>database</td>
<td>1,765,733</td>
<td>19</td>
<td>201-9 Aug-24 16:30</td>
<td>201-9 Sep-10 19:30</td>
<td>0.00-93</td>
<td>0.00-94</td>
<td>0.00-94</td>
<td>0.00-94</td>
<td>0.01-02</td>
</tr>
<tr>
<td>10</td>
<td>restart</td>
<td>1,679,365</td>
<td>20</td>
<td>201-9 Aug-24 13:00</td>
<td>201-9 Sep-17 06:30</td>
<td>0.00-01</td>
<td>0.00-02</td>
<td>0.00-87</td>
<td>0.00-92</td>
<td>0.00-98</td>
</tr>
</tbody>
</table>

The last 5 columns on the right show what fraction of events are normalized with respective dimension. For example, `name = network`:

- **0.0073** (equivalent to 0.73%) — minimum, also called 0th percentile
- At some point, events constituted fraction of **0.9997** (equivalent to 99.97%) — maximum, also called 100th percentile
- The fraction of **0.9939** (equivalent to 99.39%) has been the median average, also called 50th percentile. The median is a superior way to measure a dataset's average, because it is not as easily skewed by outliers.
throughput--kilo-eps.sql

**USAGE:** `<daysAgo_max> [<daysAgo_min, default>=0]`

Shows volume of event influx by the hour, in units of 1000 events per second.

**Example Output**

![Example Output Table]
LCE resides in the `/opt/lce` directory, and contains various sub-directories. The contents of each subdirectory are summarized in the table below.

<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin/log</td>
<td>This directory contains all of the LCE tracelog files. Tracelogs with expected higher volume are broken up into monthly files, with names in <code>YYYYMon.log</code> format (e.g. <code>2019Jan.log</code>). Tracelog files for some LCE components are stored in eponymous subdirectories.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Directory <code>/opt/lce/admin/log</code> is the default location of LCE tracelogs. Use <code>change-tracelogs-location</code> to change the tracelogs directory location. For more information, see <code>change-tracelogs-location</code>.</td>
</tr>
<tr>
<td>credentials</td>
<td>This directory contains certificates and keys for LCE modules to authenticate remote connections. For example, the <code>syslog</code> sub-directory contains the default keys and certs to authenticate encrypted TCP syslog senders.</td>
</tr>
<tr>
<td>daemons</td>
<td>This directory contains the <code>lced</code> binary (the log engine) and all other helper daemons in LCE. The LCE Client Manager is also located here. The <code>daemons</code> directory also contains sub-directories for plugins, policies, and other items updated automatically via the LCE plugin feed. When LCE starts, it will load all files in the <code>plugins</code> sub-directory unless they are disabled via the configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> To verify which version of LCE you are running, run the following command:</td>
</tr>
<tr>
<td></td>
<td><code>lced -v</code></td>
</tr>
<tr>
<td>db</td>
<td>LCE stores all event data in the <code>db</code> directory.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Directory <code>/opt/lce/db</code> is the default location of LCE activeDb. Use <code>change-activeDb-location</code> to change the activeDb directory location. For more information, see <code>change-activeDb-location</code>.</td>
</tr>
<tr>
<td>Directory</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>docs</td>
<td>This directory contains the LCE Software License Agreement.</td>
</tr>
<tr>
<td>ids</td>
<td>IDS signature mappings and host vulnerability information from Tenable.sc is stored here for correlation.</td>
</tr>
<tr>
<td>postgresql</td>
<td>Bundled with LCE. For more information, see <a href="#">Location of PostgreSQL Files in an LCE Installation</a>.</td>
</tr>
<tr>
<td>reporter</td>
<td>This directory and its sub-directories contain certs and keys for the Nessus Transport Protocol interface for Tenable.sc to retrieve report information.</td>
</tr>
<tr>
<td>reports</td>
<td>This directory contains host vulnerability information LCE has discovered by scanning logs.</td>
</tr>
<tr>
<td>tmp</td>
<td>Directory used for temporary data that is utilized by LCE.</td>
</tr>
<tr>
<td>tools</td>
<td>This directory contains various tools that are utilized by LCE, and some can be utilized via the command line if required.</td>
</tr>
<tr>
<td>var</td>
<td>The www directory contains the web client, and web server information. The users subdirectory contains a directory for each user configured in the LCE interface.</td>
</tr>
</tbody>
</table>
## Location of PostgreSQL Files in an LCE Installation

<table>
<thead>
<tr>
<th>File</th>
<th>Location</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data files</td>
<td><em>tracelogs directory/postgresql</em></td>
<td>None.</td>
</tr>
<tr>
<td>Persistent configuration</td>
<td><em>tracelogs directory/postgresql</em></td>
<td>Primary config file is postgresql.conf.</td>
</tr>
<tr>
<td>Tracelog</td>
<td><em>tracelogs directory/postgresql</em></td>
<td>None. Expect two tracelog files: startup.log and server.log.</td>
</tr>
<tr>
<td>Binaries</td>
<td>/opt/lce/postgresql/bin</td>
<td></td>
</tr>
<tr>
<td>Dynamic libraries</td>
<td>/opt/lce/postgresql/lib</td>
<td>To run any of the PostgreSQL binaries (see directly above), your LD_LIBRARY_PATH environment variable must include this directory. The source-for-psql-shortcuts.sh script will do this for you. For more information, see <a href="#">Shortcuts for Running SQL Commands and Scripts</a>.</td>
</tr>
<tr>
<td>Setup scripts, timezone rule files, text-search (TS) support files</td>
<td>/opt/lce/postgresql/share</td>
<td>None.</td>
</tr>
</tbody>
</table>
**Tenable.sc CV Integration**

Tenable.sc is used to view events obtained from all of your LCE servers and clients. This section includes:

- Add LCE to Tenable.sc
- Configure Organizations
- Analyzing Events
- Full Text Searches

**SSH (Secure Shell) Public Keys**

LCE analysis is provided to Tenable.sc through the use of command execution across a Secure Shell (SSH) network session. When Tenable.sc queries an LCE server, it invokes an SSH session to the configured LCE server. All execution and analysis of LCE data occurs on the LCE server.

SSH public keys are configured such that Tenable.sc can invoke commands on the LCE server. Non system-administrator accounts are used to perform these queries. The trust relationship is only needed from Tenable.sc to the LCE server.
## Add LCE to Tenable.sc

To add your LCE server to Tenable.sc, see [Add a Log Correlation Engine Server](#) in the [Tenable.sc User Guide](#).

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name that this LCE server will be known as.</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive text for the LCE server.</td>
</tr>
<tr>
<td>Host</td>
<td>The IP address of the LCE server.</td>
</tr>
<tr>
<td><strong>Note:</strong> When the Tenable.sc resides on the same host as the LCE server, it is recommended to use the localhost IP address of 127.0.0.1.</td>
<td></td>
</tr>
<tr>
<td>Organizations</td>
<td>Select the customer that this LCE is assigned to from the drop down menu.</td>
</tr>
</tbody>
</table>

### Event Vulnerability Data

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import Vulnerabilities</td>
<td>Selecting this box will allow you to configure your LCE use Event data to detect vulnerabilities.</td>
</tr>
<tr>
<td>Repositories</td>
<td>This will allow you to select which repository you would like to keep the vulnerability data collected from LCE events.</td>
</tr>
</tbody>
</table>

### Event Vulnerability Host

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>This allows you to configure the port used for communication between Tenable.sc and LCE. The default port is 1243. In the LCE interface this is known as the <strong>Reporter Port</strong>.</td>
</tr>
<tr>
<td>Username</td>
<td>This is the <strong>Reporter Username</strong> that was set in the LCE interface under the <strong>Configuration, Advanced, Host Discovery and Vulnerabilities</strong> section.</td>
</tr>
<tr>
<td>Password</td>
<td>This is known as the <strong>Reporter Password</strong> which is found in the <strong>Configuration, Advanced, Host Discovery and Vulnerabilities</strong> section.</td>
</tr>
</tbody>
</table>
After clicking on Submit, the LCE admin credentials ("root" user or equivalent) are requested to establish an authenticated session between Tenable.sc and the LCE. After the LCE server is successfully added, highlight the new LCE server to display options pertinent to that server.

**Note:** If you are using DNS in your environment, make sure it is configured for reverse DNS resolution to facilitate query speeds. If you are not using DNS, modify the /etc/hosts file to include your Tenable.sc IP address and hostname. For example: 192.0.2.22  SecurityCenter4.example.com  SecurityCenter4
Configure Organizations

Through the web interface, Tenable.sc can be configured such that users of specific organizations can make queries to each LCE server. For more information, see Organizations in the Tenable.sc User Guide.
Using Tenable.sc with LCE

Tenable.sc is used to visualize data from your LCE servers. The following section includes:

- [Analyzing Events](#)
- [Full Text Searches](#)
- [Queries Against Archived Snapshots](#)
Analyzing Events

A wide variety of LCE analysis and reporting tools are available to Tenable.sc users. These users can make use of any LCE event that intersects with their range of managed IP addresses. All analysis and reporting options are described in the Tenable.sc User Guide.

Identifying Vulnerabilities

LCE can leverage log data to find vulnerabilities. The Tenable plugins that report this information will have the plugin ID range of 800,000 - 899,999.

You can filter for the vulnerabilities identified by LCE in Tenable.sc by using the “Filters” and selecting “Plugin ID”, then selecting “≥” and then entering “800000.” The filter setting is pictured below:
TASL Scripts

After PRM processing normalizes an event, the event is submitted to the LCE TASL engine for advanced processing by TASL scripts. TASL scripts are used for many types of detection events such as thresholds, successful attack detection, and alerting. By default, all TASL scripts are enabled in the LCE server; however they can be disabled manually in the “TASL and Plugins” section of the LCE interface described in detail earlier in this document. For more information regarding TASL scripts review the LCE TASL Reference Guide.
Full Text Searches

Full text searches may be performed on the data stored within the attached LCE servers. When viewing the events page the Search field will accept text strings as valid search criteria. Search terms are not case sensitive and a Boolean search may be utilized to further enhance search results. This enables searching the raw logs for details contained in the events.

LCE can search for compound groups of full text tokens.

Tokens

A token in a full text search is a full word (three or more characters) separated by punctuation or whitespace. For example, if you want to search for logs containing "Microsoft," then Microsoft would be the example of the token.

Operators

Operators are case sensitive, and must be capitalized. For example, a search for mike or miked will actually yield mike AND or AND miked. Multiple operators can be used in a single query.

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AND</td>
<td>Finds logs both directly preceding token and the directly following token.</td>
</tr>
<tr>
<td>OR</td>
<td>Finds logs containing the directly preceding token, the directly following token, or both.</td>
</tr>
<tr>
<td>NOT</td>
<td>Finds logs that do not include the subsequent token.</td>
</tr>
</tbody>
</table>

Wildcards

The * wildcard metacharacter can be used to search for log entries that begin with the token preceding the wildcard in your query. For example, if a wildcard immediately follows a token T, then LCE will match logs containing a token that starts with T. So, the query text='atten*' will match logs containing "attention," "attenuate," or "Attenborough."

Grouping
Parentheses may be used to group conditionals together to show evaluation precedence just as in mathematics. This is useful in compound conditionals. Without grouping, the query `text='blocked AND denied AND dropped OR firewall'` would return any log with just “firewall” in it because it satisfies the entire query.

The following query would provide a more accurate result: `text='blocked AND denied AND (dropped OR firewall)'`

This requires that the log contains `blocked`, `denied`, and either `dropped` or `firewall`, because it has additional constraints.

**Token Adjacency**

The relative position of tokens in a log does not normally impact the query results. For example, the query `text='video upload'` will match both "video staging upload success" and "failed to upload video." If you wish to only match immediately adjacent tokens, surround them with quotation characters "". The query `text='"video upload"'` will not match "video staging upload success" or "failed to upload video," but it will match "video upload complete."

If only some of the tokens in your query need to be adjacent, you can surround those tokens with parentheses. For example, if you want to search for logs where "upload" immediately follows "video," while "studio" can be anywhere, you can query `text='studio ("video upload")'` or `text='("video upload") studio'`.

Token-adjacent search is disabled by default. Enabling token-adjacent search results in a 10\% to 15\% increase in disk space needed for the database indexes on event log text.

To enable token-adjacent search, run the following command:

```
/opt/lce/tools/cfg-utils --set-sv position_sensitive_text_search true
```

**Punctuation**

Punctuation characters are normally treated as if they were spaces, separating tokens. The `ts-test` utility, when invoked as `ts-test 'bunnies?possibly!'`, tells us that two asciiword tokens are extracted: `bunnies` and `possibly`.

However, if a string looks like a `protocol prefix`, `email address`, `network name`, `URL fragment`, or `file system path`, it will be parsed specially.
For more information about the ts-test utility, see ts-test.

<table>
<thead>
<tr>
<th>Input</th>
<th>Output You May Have Expected</th>
<th>Actual Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>bunnies://</td>
<td>1 token: bunnies, of type asciiword</td>
<td>1 token: bunnies://, of type protocol</td>
</tr>
<tr>
<td>mystery.localhost</td>
<td>2 tokens: mystery and localhost, both of type asciiword</td>
<td>1 token: mystery.localhost, of type host</td>
</tr>
<tr>
<td><a href="mailto:bunnies@mystery.localhost">bunnies@mystery.localhost</a></td>
<td>3 tokens: bunnies and mystery and localhost, all of type asciiword</td>
<td>1token: <a href="mailto:bunnies@mystery.localhost">bunnies@mystery.localhost</a>, of type email</td>
</tr>
<tr>
<td>I forget which chapter-/page.Hmm!</td>
<td>4 tokens: forget and chapter and page and hmm, all of type asciiword</td>
<td>2 tokens: forget, of type asciiword; and chapter-/page.hmm, of type file</td>
</tr>
</tbody>
</table>

Search Query Examples:

<table>
<thead>
<tr>
<th>Query String</th>
<th>What It Means</th>
<th>Example Result</th>
<th>Example Non-Result</th>
<th>Why It Didn’t Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>text='Heartbeat'</td>
<td>Show me logs with the term &quot;Heartbeat&quot;</td>
<td>LCE Client Heartbeat</td>
<td>07/23/2014</td>
<td>Heart</td>
</tr>
<tr>
<td>Query String</td>
<td>What It Means</td>
<td>Example Result</td>
<td>Example Non-Result</td>
<td>Why It Didn't Match</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>text='linux process'</td>
<td>Show me logs with the term &quot;linux&quot; and the term &quot;process&quot;</td>
<td>00:25:00 AM Hostname: lce_demo IP: 192.0.2.106 Revision: LCE Client 4.2.0 build 20131004</td>
<td>This linux host executed process &quot;ls&quot;</td>
<td>beat&quot; by itself, only as a sub-string</td>
</tr>
<tr>
<td>text='linux NOT process'</td>
<td>Show me logs with the term &quot;linux&quot; but NOT the term &quot;process&quot;</td>
<td>This linux host executed nothing.</td>
<td>This linux host executed process &quot;ls&quot;</td>
<td>contains &quot;process&quot;</td>
</tr>
<tr>
<td>text='linux OR nothing'</td>
<td>Show me logs with either term &quot;linux&quot; or term &quot;nothing&quot;</td>
<td>This linux host executed process &quot;ls&quot;</td>
<td>This nix host did everything.</td>
<td>does not contain &quot;linux&quot; and does not contain &quot;nothing&quot;</td>
</tr>
<tr>
<td>text='(linux OR nothing) AND process'</td>
<td>Show me logs that have terms &quot;linux&quot;</td>
<td>This linux host executed process &quot;ls&quot;</td>
<td>This process did everything.</td>
<td>contains &quot;process&quot; but not &quot;linux&quot; and not</td>
</tr>
<tr>
<td>Query String</td>
<td>What It Means</td>
<td>Example Result</td>
<td>Example Non-Result</td>
<td>Why It Didn't Match</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------</td>
<td>----------------</td>
<td>--------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>and &quot;process&quot; or &quot;nothing&quot; and &quot;process&quot;</td>
<td>The process did nothing.</td>
<td>This Linux host did nothing.</td>
<td>&quot;nothing&quot; contains &quot;linux&quot; and &quot;nothing&quot; but not &quot;process&quot;</td>
<td></td>
</tr>
</tbody>
</table>
Queries Against Archived Snapshots

You can query events from a silo in archiveDb if it was archived by LCE Server 6.0.6 or later. For more information, see Silo Archiving.

Tip: Use the output of archival-manager --list-snapshots to determine which LCE Server version archived the snapshot. For more information about archival-manager, see Tools.

When you select a date range in Tenable.sc using the Archived view, LCE Server temporarily restores the archived silo into activeDb. This automated process can take several minutes. Therefore, expect a higher than usual latency for the first query against a particular archived silo. Subsequent queries should exhibit normal latency.

Switching between the Active view and Archived view in Tenable.sc does not remove the archived silo currently occupying the temporary restore slot. For best performance, complete all desired queries against one archived silo before selecting another. For more information about event analysis in Tenable.sc, see Event Analysis in the Tenable.sc User Guide.
Health and Status

Included in the LCE interface is **Health and Status** information. In the **Service Status** section, the name of the service of each daemon is shown along with its status. It also includes when the daemon was last started, and the version of the daemon. The version of the `lced` daemon indicates the version of LCE you are currently running.

<table>
<thead>
<tr>
<th>Service</th>
<th>Status</th>
<th>Last Started</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Engine</td>
<td>Stopped</td>
<td>2019 Jan 09 10:37:53</td>
<td>6.0.0</td>
</tr>
<tr>
<td>Query Interface</td>
<td>OK</td>
<td>2019 Jan 09 11:10:19</td>
<td>6.0.0</td>
</tr>
<tr>
<td>Vulnerability Reporter</td>
<td>OK</td>
<td>2019 Jan 09 11:10:25</td>
<td>6.0.0</td>
</tr>
<tr>
<td>Statistics Engine</td>
<td>OK</td>
<td>2019 Jan 09 11:10:27</td>
<td>6.0.0</td>
</tr>
<tr>
<td>TASL Engine</td>
<td>OK</td>
<td>2019 Jan 09 11:10:33</td>
<td>6.0.0</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>OK</td>
<td>2019 Jan 09 10:36:49</td>
<td>11.1</td>
</tr>
</tbody>
</table>

Last Updated: 2019 Jan 09 11:34:00
The **Feed** section displays the LCE Server Version, Web Server Version, HTML Client Version, Activation Status, Plugin Set, Plugin Set Loaded, the Feed Expiration information, and the date of the Last Report Uploaded to Cloud.

<table>
<thead>
<tr>
<th>Information</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Version:</td>
<td>6.0.0</td>
</tr>
<tr>
<td>Web Server Version:</td>
<td>1.2.5 (Build ID: 20190109)</td>
</tr>
<tr>
<td>HTML Client Version:</td>
<td>1.2.5 (Build ID: 20190109)</td>
</tr>
<tr>
<td>Activation Status:</td>
<td>Licensed</td>
</tr>
<tr>
<td>Plugin Set:</td>
<td>201901041429</td>
</tr>
<tr>
<td>Plugin Set Loaded:</td>
<td>201901041429</td>
</tr>
<tr>
<td>Feed Expiration:</td>
<td>27 day(s)</td>
</tr>
<tr>
<td>Last Report Uploaded to Cloud:</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

Last Updated: 2019 Jan 11 11:33:32
In the **Statistics** section the amount of events are displayed by each source of event data. The LCE source shows the number of internally generated events from the LCE being administered. The TCP Syslog, and UDP syslog source displays the number of events received on the configured TCP syslog or UDP syslog listening port. Likewise the Clients source is the total amount of event data that all LCE clients produce. The IDS event source type is the total amount of event data from all IDS sources. The TASL source type is all the event data created by the LCE TASL scripts.

The source data is displayed in Average Events / Second and Average Bytes / Second since the LCE server was last started. The source data also displays the Total Events (today) for the day, and the Total Events (since startup) is the total number of events since the LCE server was last started.

Runtime statistics pertaining to logging and correlation are collected, including:

- Logs/bytes per second
- Number/percentage of logs matched/unmatched
- Number of events correlating with vulnerabilities
- Number/percentage of logs from clients, syslog, and IDS

- Number of TASL alerts generated

This information is logged once per hour and is written both to the application log and to the normalized database under the event name **LCE-Server_Statistics** (type “Ice”).

Example Correlation Statistics Output found in the LCE admin logs (e.g., /opt/lce/admin/log/2022Jul.log):

```
An average of 50 logs are being received each second.
A total of 5,778 logs (521,046 bytes) have been received.
2,232 logs have been matched by plugins (38.63%). 3,546 logs did not match (61.37%)
Log source breakdown: 5,774 from clients (99.93%), 2 via syslog (0.07%), 0 from IDS devices (0.00%)
No log events have correlated with vulnerabilities.
2 TASL alerts have been generated.
```
Data Sensors

In the Data Sensors section there is a drop-down box, Select Data Source, to select the type of data sources to be displayed. The Clients option is selected by default, and each client that has sent events to LCE is displayed. The Source column will display the IP address of the client. The Logs Today column will show the total number of logs collected by that client in the current day. The Client Type column will display the type of client. The Last Timestamp column will show when the client last sent an event.

The second option under Select Data Source is Syslog Sources, which will display all hosts that are forwarding syslog to the LCE server. The Source column displays the IP address of the syslog server, and the Logs Today column displays the total number of logs sent in the last day for each syslog server. The Encrypted column shows if the logs being forwarded are encrypted. The Last Timestamp column shows the last time each syslog server sent logs to the LCE server.
**Alerts**

The **Alerts** section is a simple way to see when a condition on the LCE server requires attention from the LCE administrator. It includes informational alerts, such as when a new LCE client requests authorization to send events to LCE. It also includes warnings, such as login failures to the LCE interface, or license expiration warnings. Finally, it includes error conditions that could prevent LCE from working properly.

**Alert Occasions**

For every alert created, LCE Server stores a corresponding *occasion* code, such as `cannot_DNS_resolve`, `client__too_long_inactive`, `license_expired`, or `silo_archival_error`. These codes summarize recent LCE activity, with help of the following scripts under `/opt/lce/tools/pg-helper-sql`:

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>recent-alerts-24hours.sql</td>
<td>Shows alert counts by occasion grouped by hour for the past 24 hours. Hours without alerts are omitted, and alert occasions with zero occurrences are omitted.</td>
</tr>
<tr>
<td>alerts-by-day.sql</td>
<td>Shows alert counts by occasion grouped by day for the past 14 days. Days without alerts are shown, and occasions with zero occurrences are shown. This script can be used for comparing the behavior of multiple LCE instances monitoring the same LCE instance over successive weeks.</td>
</tr>
<tr>
<td>alerts-by-month.sql</td>
<td>Shows alert counts by occasion grouped by month for the past 12 months.</td>
</tr>
</tbody>
</table>

Example alerts-by-day.sql output:
<table>
<thead>
<tr>
<th>occasion</th>
<th>Sep 09</th>
<th>Sep 10</th>
<th>Sep 11</th>
<th>Sep 12</th>
<th>Sep 13</th>
<th>Sep 14</th>
<th>Sep 15</th>
<th>Sep 16</th>
<th>Sep 17</th>
<th>Sep 18</th>
<th>Sep 19</th>
<th>Sep 20</th>
<th>Sep 21</th>
<th>Sep 22</th>
<th>Sep 23</th>
<th>Sep 24</th>
</tr>
</thead>
<tbody>
<tr>
<td>active_db_disk_capacity_saturated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bad_config</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bad_policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bad_fkm_plugin</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bad_query</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bad_runtime_state</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>badSaved_control_state</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cannot_DNS_resolv</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cannot_forward_syslog</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cannot_listen_for_SNMP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cannot_listen_for_syslog</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>client_asked_authorization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>client_authorization_explicitly</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>client_error_connecting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>client_error_provisioning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>client_error_receiving</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>client_logout_involuntary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>client太久没 inactive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>events_persist_error</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>follower</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>license_expired_or_bad</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>load_balance_irregularity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>login_acct_administration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>login_acct_end_session_forced</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>login_acct_end_session_willed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>login_acct_new_session_allowed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>login_acct_new_session_forbade</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>login_acct_session_tokens_ngat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>migration_irregularity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>misc_alert</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>misc_fatal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>plugins_update_done</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>plugins_update_irregularity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>reached_license_limit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>reached_operating_limit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>silo archival_error</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>silo_create_or_roll_error</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>trimming_activeDb</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>trimming_archiveDb</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ui_in_report_upload_error</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The **Advanced** section displays information about the LCE database. The **Active DB File System Usage** row displays the current amount of disk space being used by the active database, as well as the number of inodes. The **Active DB Oldest Event Time** row displays the timestamp of the earliest event available in the active database. If archiving is enabled, the amount of disk space being used by the archive database and the timestamp of the earliest available event in that database will be included.

<table>
<thead>
<tr>
<th>Silo / Database Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active DB File System Usage</td>
<td>11.40 GB / 49.98 GB (22.81%) and 271,772 inodes / 26,214,400 inodes (1.04%)</td>
</tr>
<tr>
<td>Active On Disk Bytes</td>
<td>1.26 KB</td>
</tr>
<tr>
<td>Archive DB File System Usage</td>
<td>Archiving Disabled</td>
</tr>
<tr>
<td>Estimated Time To Fill Disk</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

Last Updated: 2019 Jan 9 17:07:38
To configure the LCE server

1. Log in to LCE via the user interface.
2. On the top navigation bar, click **Configuration**.

   The **System Configuration** page appears.

3. Modify your configuration settings. For more information about the sections on the **System Configuration** page, see:

   - **Basic**
   - **Storage**
   - **IDS**
   - **Advanced**
   - **Control**
   - **Feed Settings**

4. Click **Update**.

   LCE saves your configuration.

---

**Note:** Updates are applied while the LCE server is operational. You do not need to restart the LCE services.
Basic Configuration

The Basic Configuration section comprises the essential configuration needed for an LCE server to function. The items in this section are addressed in the initial Quick Setup, but can be changed in this section at a later time if the need arises.

Each menu option for the Basic section is covered in detail below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Address</td>
<td>The IP address of the network interface(s) that the LCE server listens on. More than one interface may be specified on separate lines:</td>
</tr>
<tr>
<td></td>
<td>127.0.0.1</td>
</tr>
<tr>
<td></td>
<td>192.0.2.2</td>
</tr>
<tr>
<td></td>
<td>By default, or if left blank the above LCE services will listen on all available network addresses.</td>
</tr>
<tr>
<td>Client Port</td>
<td>The port number that the LCE server listens on. By default, port 31300.</td>
</tr>
<tr>
<td>UDP Syslog Port</td>
<td>By default, the LCE server listens for UDP syslog traffic on port 514. If the environment requires the LCE server to listen on a different port, this setting may be changed.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Only ASCII-encoded syslog is accepted.</td>
</tr>
<tr>
<td>TCP Syslog Port</td>
<td>By default, the LCE server listens for TCP syslog traffic on port 601. If the environment requires the LCE server to listen on a different port, this setting may be changed.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Only ASCII-encoded syslog is accepted.</td>
</tr>
<tr>
<td>Encrypted TCP Syslog</td>
<td>By default, the LCE server listens for encrypted TCP syslog traffic on port 6514. If the environment requires the LCE server to listen on a different port, this setting may be changed.</td>
</tr>
<tr>
<td>Listen Port</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SNMP Port</td>
<td>By default, the LCE server listens for SNMP traffic on port 162. If the environment requires the LCE server to listen on a different port, this setting may be changed.</td>
</tr>
<tr>
<td>Include Networks</td>
<td>Defines the internal network range. All networks specified in the first section are included.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Make sure this range matches IP addresses that are considered <em>internal</em> from an event perspective. This range is used by a number of TASL scripts and the stats daemon to define inbound, outbound, and internal specifications for LCE events. This is different from the Directions filter on the Tenable.sc events page, which uses the managed ranges of the active user to determine event direction.</td>
</tr>
<tr>
<td>Exclude Networks</td>
<td>Defines networks that should be excluded from the ranges specified for Include Networks.</td>
</tr>
<tr>
<td>Allow only TLSv1.2</td>
<td>Disables all SSL/TLS support prior to TLS 1.2 for all SSL interfaces for PCI DSS compliance.</td>
</tr>
</tbody>
</table>
Storage Configuration

The Storage section includes information about the database, including disk space limits for both the active and archive databases.

When your active database reaches the limit you have specified in your configuration, data in that database is moved to the archive database. When the archive limit is exceeded, the oldest archive database is deleted. If you do not want the archive databases to be deleted, set the value for the **Archived Database Limit** option to 0. In that case, storage should be regularly monitored to ensure that enough disk space is available for the active database. If the active database exceeds your license limit, that data will still be archived.

The following table describes the options that are available.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archiving</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Archive Directory</td>
<td>The directory that stores data that exceeds your license or active database limit.</td>
</tr>
</tbody>
</table>
IDS Configuration

LCE has the ability to receive IDS events from multiple sources. In addition to being normalized and stored in the log database, each event will be checked against any Tenable.sc vulnerability databases. If a host is vulnerable to attack, the event is marked as such, allowing rules to trigger on this scenario so that the information can be distributed to the affected administrators.

For each IDS sensor, a sensor name and type must be defined as in the example below. The following sensor types are supported:

- Snort
- Bro
- RealSecure
- Dragon
- IntruVert
- IntruShield
The following table describes the options that are available.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDS IP</td>
<td>The IP address of the IDS.</td>
</tr>
<tr>
<td>Sensor Name</td>
<td>Name to be used within the Tenable.sc logs.</td>
</tr>
<tr>
<td>Sensor Type</td>
<td>IDS sensor type.</td>
</tr>
</tbody>
</table>
High Availability

When high availability is required, LCE can be configured for two-node replication. A single virtual IP is always bound to the real IP of whichever node is currently the master node. You use the virtual IP in your high availability configuration for all of the following:

- LCE web UI
- LCE clients
- Syslog and SMTP inputs
- Tenable.sc

The two-node high availability configuration allows you to keep log collection and analysis in the event of a hardware or network failure. High availability works by monitoring services on both configured hosts. At any time, the servers in your configuration are assigned either the active (or master) or the standby role. The role of each node is determined by service status, which is monitored at a high frequency. Example timeline:

1. Initial boot
   - Node A initializes in the master role; Node A binds the virtual IP to its primary network interface
   - Node B initializes in the standby role

2. Node A’s network connection fails
   - Node B detects Node A’s loss of connectivity and takes over the master role

3. Node A’s network connection is restored
   - Node A transitions to the standby role
   - Node B maintains the master role

4. Node B’s electrical power supply fails
   - Node A takes over the master role

5. Node B’s electrical power supply is restored
   - Node B resumes in the standby role
Database synchronization occurs continuously. If a node goes offline and then is restored, ample time is required to re-sync the database. In the event of hardware or network instability that requires the nodes to switch roles more frequently than every 5 minutes, high availability behavior may become unpredictable and may result in missing log data.

**Note:** If you configure high availability for LCE, use the virtual IP address when configuring LCE in Tenable.sc.

**Note:** On the standby node, LCE will run only the following services: `keepalived`, `postgresql`, and `lce_queryd`. Do not manually start, restart, or stop LCE services on the standby node.

**Note:** On both the master and the standby node, `ha-manager` will start and stop the `keepalived` service automatically as needed. Do not manually start, restart, or stop the `keepalived` service on either node.

For more information, see:

- [Configure High Availability](#)
- [Monitor Your High Availability Configuration](#)
- [Disable High Availability](#)

**Health and Status**

You can view status information about your high availability configuration in the LCE web UI or by running `ha-manager --status`.

For more information, see [Monitor Your High Availability Configuration](#).

**Migrating Existing High Availability Configurations**

If you previously configured high availability on your LCE 4.8.4 deployment and want to migrate to LCE 6.0.4 or later, you can upgrade and then re-configure your high availability configuration, as described in [Migrate Your High Availability Configuration to LCE 6.0.4 or Later](#).

**ha-manager Utility**

The `ha-manager` utility configures, disables, and provides status details of high availability configurations. For more information about the `ha-manager` utility and its usage, see [ha-manager](#).
Configure High Availability

You can create a high availability configuration by setting up two-node replication with the `ha-manager` utility. If you encounter issues during setup, before restarting the configuration process, use `-disconnect` to disconnect your master and standby nodes without erasing any LCE or PostgreSQL configuration related to high availability.

If you previously configured high availability on your LCE 4.8.4 deployment and want to migrate to LCE 6.0.4 or later, you can upgrade and then re-configure your high availability configuration, as described in [Migrate Your High Availability Configuration to LCE 6.0.4 or Later](#).

For more information about high availability configurations, see [High Availability](#).

Before you begin:

- Confirm the two nodes you intend to use in your high availability configuration have IP addresses in the same broadcast subnet. For example:
  - Standby node 192.0.2.10/24, with non-loopback interface `bond0`
  - Master node 192.0.2.11/24 with non-loopback interface `eth0`
- Consider the following when selecting your virtual IP address:
  - If you are converting a single-node LCE deployment to two-node high availability, use the IP address of your current LCE server as the virtual IP address and assign a new native IP address to your existing server. This enables Tenable.sc and LCE clients to continue operations without reconfiguration.
  - If you are migrating an LCE deployment with high availability configured, use the same virtual IP address you used in your previous configuration.

To configure high availability:

1. At the master node, run:

   ```bash
   ha-manager --initialize-as-master
   <standby IP address> eth0 <virtual IP address>
   ```
The ha-manager utility initializes setup on the master node.

The ha-manager utility prints the estimated size of the base-backup, a full copy of the master node's activeDb.

2. At the standby node, run:

```
ha-manager --initialize-as-standby
<master IP address> bond0 <virtual IP address>
```

The ha-manager utility initializes setup on the standby node.

The ha-manager utility sends the base-backup of the master node to the standby node.

The ha-manager utility prints the step_2_token.

The master node prompts you for the step_2_token.

**Note:** The time to complete this step depends on the size of the base-backup. During the transfer, the ha-manager utility will print and update the total file size transferred so far.

3. At the master node, type the step_2_token and press Enter.

   The ha-manager utility runs.

   The ha-manager utility prints the step_3_token.

   The standby node prompts you for the step_3_token.

4. At the standby node, type the step_3_token and press Enter.

   The ha-manager utility runs.

5. When the standby node's ha-manager utility finishes running, at the master node, press Enter.
6. When the master node’s `ha-manager` utility finishes running, at the standby node, press Enter:

```
(Reminder: the standby must also have
    broadcast IP=172.26.103.255], activeDb_directory=/home/bunnies], and tracelogs_directory=/opt/ice/admin/log]
)
--------------[ STEP_1: Done ]--------------
Size of base-backup to copy - 28G
Now run
    /opt/ice/tools/ha-manager --initialize-as-standby
at the standby host.
Please type in the step_2_token value which will have been printed at standby node:
    788d
--------------[ STEP_2: Done ]--------------
The step_2_token is a86f; enter that value at the standby node, when asked.
Hit <ENTER> to proceed, once step_4 has completed at standby
--------------[ STEP_5: Done ]--------------
```

7. If only one node has a copy of your SSH keys, run the following command:
LCE copies the SSH keys to the peer node.

**Note:** To ensure both the master node and standby node can respond to requests from Tenable.sc, both nodes must have the same SSH keys. If both nodes already have a copy of your SSH keys, skip this step.

What to do next:

- Monitor your high availability status, as described in [Monitor Your High Availability Configuration](#).
Migrate Your High Availability Configuration to LCE 6.0.4 or Later

You can use this method to upgrade your LCE 4.8.4 deployment with high availability to LCE 6.0.4 or later, then re-configure high availability. To configure high availability for the first time in LCE 6.0.4 or later, see Configure High Availability. For more information about high availability configurations, see High Availability.

**Note:** If you are upgrading from a version of LCE earlier than 4.8.4, upgrade to LCE 4.8.4 before upgrading to LCE 6.0.4 or later.

**Tip:** If you have another node available, you can keep the former standby node offline to use as an emergency backup in case you encounter issues after migration. If you want to keep your former standby node as a backup:

- Skip step three in the procedure below to keep LCE installed on the former standby node.
- Use the third node as the standby node in your new high availability configuration after upgrading to LCE 6.0.4 or later.

To upgrade from LCE 4.8.4 to LCE 6.0.4 or later and re-configure high availability:

1. Log in to LCE via the command line interface (CLI).

2. In the CLI in LCE, run the following commands on both the master node and the standby node to stop LCE:

```
    service stats stop
    /opt/lce/tools/stop_lce
    pkill -KILL keepalived 2>/dev/null
```

LCE stops.

3. (Optional) Make a copy of the master node activeDb.

4. To remove LCE from the standby node, do the following:

   a. In the CLI in LCE, run the following commands:

```
    rpm -e lce
    rm -rf /opt/lce/
```
b. If you configured archiveDb, run the following command:

   `rm -rf <archiveDb directory>`

c. If you moved activeDb from the default directory /opt/lce/db/, run the following command:

   `rm -rf <activeDb directory>`

d. If you moved tracelogsDir from the default directory /opt/lce/admin/log, run the following command:

   `rm -rf <tracelogsDir directory>`

5. At the standby node, run the following command:

   `rpm -ivh lce-6.0.4-.....`

6. At the master node, run the following command:

   `rpm -Uvh lce-6.0.4-.....`

7. Configure high availability on the master node and the standby node, as described in Configure High Availability.

8. At the master node, run the following command:

   `nohup /opt/lce/tools/migrateDB-overseer --migrate-all --clear-source-on-success &`

   LCE migrates silos to the master node's activeDb and copies them to the standby node's activeDb.

What to do next:

- Monitor your high availability status, as described in Monitor Your High Availability Configuration.
Migrate Your High Availability Configuration to LCE 6.0.5 or Later

You can use this method to upgrade your LCE 6.0.4 deployment with high availability to LCE 6.0.5 or later, then re-configure high availability. To configure high availability for the first time in LCE 6.0.4 or later, see Configure High Availability. For more information about high availability configurations, see High Availability.

To upgrade from LCE 6.0.4 to LCE 6.0.5 or later and re-configure high availability:

1. Log in to LCE via the command line interface (CLI).

2. In the CLI in LCE, run the following command on the standby node to make it a standalone node:

   ```bash
   /opt/lce/tools/ha-manager --disconnect
   ```

3. Run the following command on the master node to make it a standalone node:

   ```bash
   /opt/lce/tools/ha-manager --disconnect
   ```

4. Run the following commands to remove LCE from the standby node:
   a. 
   ```bash
   /opt/lce/tools/stop-all
   rpm -e lce
   rm -rf /opt/lce/
   ```
   b. If you moved activeDb from the default directory /opt/lice/db/, run the following command:

   ```bash
   rm -rf <activeDb directory>
   ```
   c. If you moved tracelogsDir from the default directory /opt/lce/admin/log, run the following command:

   ```bash
   rm -rf <tracelongsDir directory>
   ```
5. (Optional) Backup the activeDb of the master node using `/opt/lce/tools/online-pg-backup`.

6. On the master node, run the following command:

   ```bash
   rpm -Uvh lce-6.0.x-......
   ```

7. On the standby node, run the following command:

   ```bash
   rpm -ivh lce-6.0.y-......
   ```

8. Configure high availability on the master and standby nodes, as described in Configure High Availability.

What to do next:

- Monitor your high availability status, as described in Monitor Your High Availability Configuration.
Monitor Your High Availability Configuration

You can view status information about your high availability configuration in the LCE web UI or by running `ha-manager --status`. For more information about high availability and the `ha-manager` utility, see [High Availability](#).

To view the status of your high availability configuration in the LCE web UI:

1. In the top navigation bar, click **Health and Status**.
   
   The **Health and Status** page appears.

2. In the left navigation bar, click **Advanced**.

   The **Advanced** tab appears.

3. View the following information about your high availability configuration:

   - Last HA Replication Ping — the date and time of the last data transmission from the master node to the standby node

   - High Availability Status — shows the results of `ha-manager --status`
To view the status of the Keepalived service:

<table>
<thead>
<tr>
<th>Silo / Database Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active DB File System Usage</td>
<td>3.03 GB / 57.38 GB (5.28%) and 73,821 inodes / 30,091,264 inodes (0.25%)</td>
</tr>
<tr>
<td>Active On Disk Bytes</td>
<td>18.29 MB</td>
</tr>
<tr>
<td>Archive DB File System Usage</td>
<td>Archiving Disabled</td>
</tr>
<tr>
<td>Last HA Replication Ping</td>
<td>2020-05-05 15:29:58</td>
</tr>
</tbody>
</table>

**High Availability Status**

```
pertinent LCE config:
    failover_peer_physical_IP = 172.26.101.244
    failover_virtual_bind_interface = ens192
    failover_virtual_IP = 172.26.101.242
    queries_percent_forward_to_standby = 60

virtual IP: Bound to [ens192]

open and reachable ports:
  PostgreSQL, this node: listening like a HA-capable node should
  lce_queryd, this node: not listening
  PostgreSQL, peer node: listening like a HA-capable node should
  lce_queryd, peer node: listening like HA standby should

commands received during latest run:
  [May05, 20:35:26.629124] --notify-master

Keepalived config and status:

<table>
<thead>
<tr>
<th>PID</th>
<th>%MEM</th>
<th>ELAPSED</th>
</tr>
</thead>
<tbody>
<tr>
<td>7411</td>
<td>0.0</td>
<td>01:13:06</td>
</tr>
<tr>
<td>7412</td>
<td>0.0</td>
<td>01:13:06</td>
</tr>
</tbody>
</table>

Advertisements: VRRP Instance = haLCE
  Received: 0
  Sent: 4380
  Became master: 1
  Released master: 0
  Packet Errors: 0
  Length: 0
  TTL: 0
  Invalid Type: 0

State = MASTER
  Last transition = 1588725326 (Tue May  5 20:35:26 2020)
  Listening device = ens192
  Using src_ip = 172.26.101.245
  Virtual Router ID = 164
  Priority = 50
  Effective priority = 60
  Preempt = disabled
```
1. In the top navigation bar, click **Health and Status**.

   The **Health and Status** page appears.

2. In the left navigation bar, click **Service Status**.

   The **Service Status** tab appears.

3. In the **Keep Alive** row, view the current status.

<table>
<thead>
<tr>
<th>Service</th>
<th>Status</th>
<th>Last Started</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Engine</td>
<td>OK</td>
<td>2020 May 05 20:35:28</td>
<td>6.0.4</td>
</tr>
<tr>
<td>Query Interface</td>
<td>OK</td>
<td>2020 May 05 20:35:28</td>
<td>6.0.4</td>
</tr>
<tr>
<td>Vulnerability Reporter</td>
<td>OK</td>
<td>2020 May 05 20:38:09</td>
<td>6.0.4</td>
</tr>
<tr>
<td>Statistics Engine</td>
<td>OK</td>
<td>2020 May 05 20:35:34</td>
<td>6.0.4</td>
</tr>
<tr>
<td>TASL Engine</td>
<td>OK</td>
<td>2020 May 05 20:35:33</td>
<td>6.0.4</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>OK</td>
<td>2020 May 05 20:35:04</td>
<td>12.1</td>
</tr>
<tr>
<td>Keep Alive</td>
<td>OK</td>
<td>2020 May 05 20:35:27</td>
<td>1.3.9</td>
</tr>
</tbody>
</table>
**Disable High Availability**

For more information about high availability, see [High Availability](#). For more information about the `ha-manager` utility, see [ha-manager](#).

To disable high availability and convert a node into a standalone node:

1. At the node you want to convert into a standalone node, run:

   ```bash
   ha-manager --disconnect
   ```

   The `ha-manager` utility disconnects the master and standby nodes.

2. Run:

   ```bash
   ha-manager --de-configure
   ```

   The `ha-manager` utility erases your high availability configuration.

---
Advanced Configuration

The **Advanced** configuration section is used to fine tune your LCE server configuration. Each section that is changed in the **Advanced** section will require that the **Update** button is selected before the updates are completed. Select **Cancel** to clear any unwanted updates.

The **Advanced** configuration section includes the following groups of settings:

- **Storage**
- **LCE Web Server**
- **Sensor Names**
- **Clients**
- **User Tracking**
- **Host Discovery and Vulnerabilities**
- **Statistical Alerts**
- **Resource Usage and Performance**
- **DNS Caching**
- **Data Forwarding**
- **TCP Syslog**
- **Encrypted TCP Syslog**
- **Correlation**
- **TASL and Plugins**
- **Event Rules**

**Storage**

The options available under the **Storage** subsection are **Store Unnormalized Logs** and **Disk Alert Percentage**. These options are described in the table below.
Option Description

Store Unnormalized Logs If enabled, then LCE will store logs that cannot be normalized by existing LCE plugins. These logs will have the type and event set to unnormalized and will still be available for text, IP, and sensor-based searches.

Disk Alert Percentage When filesystem usage exceeds the specified percentage (from 1 to 99 percent), an alert is generated so that you can take action to ensure the LCE server does not exhaust disk space for log storage. The default value is 75 percent.

LCE Web Server

The LCE Web Server section allows you to specify parameters governing login parameters for user access. These options are described in the table below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Banner</td>
<td>Banner to display prior to login, requiring users to positively acknowledge a customized statement or warning. Up to 1300 characters.</td>
</tr>
<tr>
<td>Enforce Complex Passwords</td>
<td>Require web server user passwords to have at least 1 uppercase, 1 lowercase, 1 number, and 1 special character.</td>
</tr>
<tr>
<td>Min Password Length</td>
<td>Minimum length of a password for a web server user login. This limit only applies to passwords that are created after this option is modified.</td>
</tr>
<tr>
<td>Idle Session Timeout</td>
<td>Idle login sessions will be logged out after the amount of time specified in minutes. To disable the timeout, set the value to 0.</td>
</tr>
<tr>
<td>Web Server Port</td>
<td>Specifies the port used to access the LCE interface. By default, port 8836.</td>
</tr>
<tr>
<td>Enable SSL for Web Server</td>
<td>When enabled, the engine will require SSL protection for connections to the web server. If this setting is changed, users are disconnected and must log back into the server again.</td>
</tr>
<tr>
<td>Enable SSL Client Certificate</td>
<td>If the web_UI__login__client_CA_cert_path configuration attribute is set, the web server will only accept SSL client certificates for user authen-</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Authentication</td>
<td>By default, this option is disabled and the web server allows login only with a username and password.</td>
</tr>
</tbody>
</table>

**Sensor Names**

This option allows you to override the discovered name of a syslog sensor with a name that is more identifiable in the environment. For example if the host is `syslogserver06.example.com` but that server resides in the research area of the environment, you can set a name that is more identifiable, such as `research_syslog`.

Normally, the sensor name is set to one of the following:

- The source of the log
- The sensor name set on the client itself
- The syslog source
- The plugin that normalizes the log

If you specify a sensor name using the LCE interface, that name will always be applied to the sensor that corresponds to the IP address. When creating new sensor names, values must be set for both the **Sensor Name** and **IP Address**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor Name</td>
<td>Sensor name to be used within the Tenable.sc logs.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The sensor name can be a maximum of 128 characters.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the configured client or syslog source.</td>
</tr>
</tbody>
</table>

**Clients**

This section of the Advanced Configuration is used to further define how clients are able to connect to the LCE, and how they are named when viewed in the **Event** section of Tenable.sc. The con-
figurations are **Public Server Address**, **Auto Authorize Clients**, **Use Client Network Address**, and **Override Sensor Name**, described in the table below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Server Address</td>
<td>If the server is run from behind a device performing Network Address Translation (NAT), and the LCE clients that the server manages are on the public side of the device, the <strong>Public Server Address</strong> box must be set to the NAT address so that the managed clients can communicate with the server. The LCE server will listen for clients based on, in order of preference, the <strong>Public Server Address</strong> setting, the <strong>Server Address</strong> setting, or the first IP that it finds LCE using that is not 127.0.0.1.</td>
</tr>
<tr>
<td>Caution: When a Public Server Address is specified, all clients on either side of the NAT device must use this address to connect.</td>
<td></td>
</tr>
<tr>
<td>Auto Authorize Clients</td>
<td>Specifies the number of minutes after the LCE server starts that clients will be automatically authorized. For example, if the value is set to 10, any clients that attempt to connect to the server within ten minutes of it starting will be automatically authorized.</td>
</tr>
<tr>
<td>Use Client Network Address</td>
<td>Override private client IP in events with the NAT / public network peer IP.</td>
</tr>
<tr>
<td>Override Sensor Name</td>
<td>Prefer configured name over discovered name.</td>
</tr>
</tbody>
</table>

The **Client Assignment Rules** section allows for specific policies to be applied to specific client ranges. When a client assignment rule is created, a text box appears in the **Policies** column. In the text box, specify the filenames of the policies that you want applied to clients that fall in the range defined by the rule.

Policies are matched by operating system. If there are multiple policies for a particular operating system, the first applicable policy that is specified for that operating system will be assigned. If none of the specified policies are applicable to a client in the network, the default policy for that operating system will be used.
If **Auto Authorize** is enabled, clients that are discovered in the range defined by the rule will be automatically authorized.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Network</td>
<td>A network range in CIDR notation</td>
</tr>
<tr>
<td>Auto Authorize</td>
<td>If enabled, clients discovered in the network range are automatically authorized.</td>
</tr>
</tbody>
</table>

**User Tracking**

Users of the LCE server are tracked by their username. These options set restrictions on which usernames are considered valid. Any usernames failing to match the specified criteria are disregarded and the user is reported as invalid for the associated log entries.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| User Tracking Plugins      | Only Plugin IDs in this list are used to apply user tracking. Other plugins will normalize usernames, but no tracking is performed based on the source and destination IP addresses. Only usernames normalized by these plugins are subject to the additional user tracking restrictions in this section. If a username is normalized by these plugins but does not meet the additional restrictions it will not be associated with the log and will not be associated with the subsequent logs from that IP address. Some IDs of plugins that can be specified for **User Tracking Plugins** are:<br>  
  - 4770 (tenable_pvs.prm)<br>  - 5450 (mail_imaps.prm)<br>  - 1708 (mail_wuimap.prm)<br>  - 7293 (os_win2008_sec.prm)<br>  - 3260, 3262, 3294 (os_win2k_sec.prm)<br> **Note:** LCE login-failure plugins do not normalize usernames because those logs are not assured to provide a valid username, and it would contaminate the username database. Additionally, it is advised never to add a login-failure plugin ID into the list of User Tracking Plugins. Doing so would invalidate user tracking for hosts that triggered the plugin. |
| Accept Letters             | If enabled, the LCE server will allow usernames to contain letters.                                                                                                                                          |
| Accept Numbers             | If enabled, the LCE server will allow usernames to contain numbers.                                                                                                                                         |
| Valid Username Characters  | Specifies which special characters are considered valid for usernames. By default, the following characters are considered valid: - _ . @ $. For example, the following username would be considered valid based on the default value:<br>  
  b.j-smith@a_b.com<br> **Note:** You cannot specify the semicolon character, ";" for this option.                                               |
<table>
<thead>
<tr>
<th><strong>Option</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Username Length</td>
<td>The maximum number of characters considered valid for usernames normalized by the server.</td>
</tr>
</tbody>
</table>
| Untracked Usernames | These users are not tracked. The usernames are normalized and will appear with their associated logs, but no alert is generated when the username switches from one IP to another.  
Example:  
- root  
- Ice  
- admin  
- administrator  
- Administrator  
- SYSTEM  
- INTERACTIVE  
- NETWORKSERVICE  
- LOCALSERVICE  
- ANONYMOUSLOGON  
- Nobody  
- NTAUTHORITY  
- DIALUP  
- NETWORK  
- BATCH  
- NO_USER_NAME |

**Host Discovery and Vulnerabilities**
This section defines the parameters used by LCE to send vulnerability information to Tenable.sc, as described in the table below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Host Discovery</td>
<td>This option enables or disables host discovery. When set to yes, new hosts on the network will be discovered and reported based on log data.</td>
</tr>
<tr>
<td>Report Interval</td>
<td>The interval, in minutes, in which the report file will be generated and updated on disk. The default is 60 minutes.</td>
</tr>
<tr>
<td>Report Lifetime</td>
<td>The lifetime of a report in days. The report will be cleared after this amount of time. The default is 7 days.</td>
</tr>
<tr>
<td>Learning Period</td>
<td>This option determines how many days a host has not been seen before an alert will be generated. A setting of at least 1 or 2 days is recommended. After that, any host that was not discovered during the period will be alerted on as new. Without this setting, LCE will repeatedly discover all of your hosts that are currently running, and not accurately identify hosts that are actually new.</td>
</tr>
<tr>
<td>Reporter Port</td>
<td>The port used by Tenable.sc to retrieve host and vulnerability reports from LCE.</td>
</tr>
<tr>
<td>Reporter Username</td>
<td>The username used by both Tenable.sc, and LCE to exchange vulnerability information.</td>
</tr>
<tr>
<td>Reporter Password</td>
<td>The password used by Tenable.sc and LCE to exchange vulnerability information.</td>
</tr>
<tr>
<td>Verify Reporter Password</td>
<td>This field is used for password verification.</td>
</tr>
</tbody>
</table>

**Statistical Alerts**

Each statistical anomaly is triggered based on a number of deviations. There are multiple Statistical anomalies that can occur on a network. Some examples are Social Network, Login Failure, DNS, Virus, and Database anomalies. The LCE stats daemon can track these anomalies, and provide feedback when a specific threshold is reached.
Each statistical anomaly is triggered based on a number of deviations. The table below shows what number of standard deviations needs to occur before a statistical anomaly is triggered along with an example event name as it would be seen in the Events section of Tenable.sc.

<table>
<thead>
<tr>
<th>Type</th>
<th>Minimum number of standard deviations from the mean</th>
<th>Maximum number of standard deviations from the mean</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minor Anomaly</td>
<td>1.0</td>
<td>5.99</td>
<td>Statistics-Login_Minor_Anomaly</td>
</tr>
<tr>
<td>Anomaly</td>
<td>6.0</td>
<td>9.99</td>
<td>Statistics-USB_Anomaly</td>
</tr>
<tr>
<td>Medium Anomaly</td>
<td>10.0</td>
<td>99.99</td>
<td>Statistics-SPAM_Medium_Anomaly</td>
</tr>
<tr>
<td>Large Anomaly</td>
<td>100.00</td>
<td>999999.99</td>
<td>Statistics-Intrusion_Large_Anomaly</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min Standard Deviation</td>
<td>This specifies the minimum standard deviation that must occur for an event before an alert will be generated for it. The higher this number, the more statistically significant a sequence of events needs to be before an alert is raised.</td>
</tr>
<tr>
<td>Min Number of Standard Deviations</td>
<td>If an event occurs more or less than 5.0 standard deviation units, an alert will be generated. Setting this value higher will cut down on any sequence of events that occur close to the standard deviation.</td>
</tr>
<tr>
<td>Min Statistical History</td>
<td>This specifies the number of iterations (days) per-event are required before alerts will be generated. If a large amount of LCE data is already present, set this number to a low value or even to zero. The stats daemon can be started</td>
</tr>
</tbody>
</table>
Option | Description
--- | ---
to read in all or just part of the existing LCE data. If you have no LCE data, leave this value around 7 so the stats daemon will not alert on anything until it has 7 days of event data.

Max Occurrence Frequency | If an event occurs more or less than 5.0 standard deviation units, an alert will be generated. Setting this value higher will cut down on any sequence of events that occur close to the standard deviation.

Syslog Alerts | The statistics engine will send anomaly alerts to the syslog servers in this list. It is recommended to include 127.0.0.1 for the local LCE service.

Resource Usage and Performance
This section of the LCE Advanced Configuration is used to tune the performance of the LCE server.

Option | Description
--- | ---
Log Processors | This option leverages multicore processors and determines how many threads will be dedicated to log processing.

It is recommended that this setting be no higher than the number of CPU cores in the LCE host system.

Sampleable TASLs | Sampleable TASL scripts may be skipped to alleviate processor load when the TASL queue is full.

DNS Caching
When a log message is defined in a plugin, LCE provides the option to specify a hostname instead of an IP address for the srcip and dstip fields. In this case, LCE automatically attempts to resolve the provided hostname to an IP address using DNS. Since the same hostname is typically
encountered multiple times, caching the results of lookups can greatly increase performance. These options configure DNS caching in LCE.

A particular hostname or all domain names with a certain extension can be excluded using the **Always Resolve** section. In this case, the matching hosts are looked up at every occurrence. The **Always Resolve** section can be used to maintain a more extensive list of domains to exclude when DNS caching is utilized. The host contained in the **Always Resolve** section of DNS Caching is read when LCE starts up, but changes to the list can be made at any time. If changes are made to the section the **Update** button at the bottom of the **Advanced Configuration** section of the LCE interface will need to be selected.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Memory for DNS Cache</td>
<td>LCE will maintain a cache of hostname-to-IP addresses rather than performing the lookup repeatedly, limited to this amount of memory [MB]. The <strong>Max Memory for DNS Cache</strong> option can go up to 360K domain names.</td>
</tr>
<tr>
<td>DNS Cache Period</td>
<td>The <strong>DNS Cache Period</strong> option specifies the number of days to cache a host-name-to-IP mapping before updating the result with a new lookup. This value can be set between 1 and 30 days.</td>
</tr>
<tr>
<td>Always Resolve</td>
<td>If a host ends with an extension listed here, it will be resolved each time it is encountered rather than being cached. List each host or extension on a new line. A particular hostname or all domain names with a certain extension can be excluded using the <strong>Always Resolve</strong> section. In this case, the matching hosts are looked up at every occurrence. The <strong>Always Resolve</strong> section can be used to maintain a more extensive list of domains to exclude when DNS caching is utilized. The hosts contained in the <strong>Always Resolve</strong> section of DNS Caching are read when LCE starts up, but changes to the list can be made at any time. If changes are made to the section the <strong>Update</strong> button at the bottom of the <strong>Advanced Configuration</strong> section of the LCE interface will need to be selected.</td>
</tr>
<tr>
<td>Cache at Startup</td>
<td>Hosts listed in the <strong>Cache at Startup</strong> are resolved at startup and cached immediately to reduce runtime DNS resolutions and improve performance. The format for these entries is one hostname per line.</td>
</tr>
</tbody>
</table>

**Data Forwarding**
See **Data Forwarding**.

**TCP Syslog and Encrypted TCP Syslog**

See **Receiving Encrypted Syslog**.

**Correlation**

LCE normally matches the vulnerability port with the port given in the normalized event to correlate an event with vulnerability. If this option is disabled, LCE will ignore this requirement if the vulnerability port is 0, 22, or 445.

To correlate an event with a vulnerability, the engine requires that the vulnerability port and event port match; except for vulnerability ports 0, 22, and 445. If this option is enabled, the engine will always require the ports to match.

**TASL and Plugins**

See **TASL and Plugins**.

**Event Rules**

See **Event Rules**.
Data Forwarding

Sending Syslog Messages to Other Hosts

The LCE can be the focal point of your entire log aggregation strategy. If a Storage Area Network, syslog server, or some other type of log aggregation solution is deployed in your network, the LCE can be configured to send a copy of any received message to one or more syslog servers. These messages include any message received from any client.

To configure the LCE to forward these messages:

1. Log in to LCE via the user interface.
2. Click on the Configuration section of the LCE interface.
3. Then select Advanced, and in that section locate Data Forwarding.
4. In the Syslog Forwarding section of Data Forwarding, enter a line for each syslog server.

The actual syslog service is not used to forward the messages. All packet generation is handled by the lced process.

The format of each entry into the Syslog Forwarding section is IP:port,exclude-header as shown below. The IP is the address of the syslog server to which the messages are sent. The port indicates the UDP port in which the receiving syslog server is listening. The exclude-header option determines if the LCE append a custom header to indicate if the messages are sent from the LCE server or not. When omitted or set to 0, the header is appended. When set to 1, the header is not added and only the original log message is sent without indication that it was forwarded from the LCE server. If 2 is used the log will be sent in CEF (Common Event Format) format.

The following is an example of the Syslog Forwarding section that forwards messages to multiple syslog servers utilizing UDP. The first line forwards to UDP port 1234 and appends an LCE server header to each entry. The second forwards to UDP port 514, and an LCE server header is not appended to each entry. The third forwards to UDP port 514 and the log will be sent in CEF format.
The following is an example section of the **TCP Syslog Forwarding** section that forwards messages to multiple **syslog** servers. The first line forwards to TCP port 601 and appends a LCE server header to each entry with an ASCII 10 (Line Feed) delimiter. The second forwards to TCP port 601, and a LCE server header is not appended to each entry. The third forwards to TCP port 1234 and the log will be sent in CEF (Common Event Format) format.

LCE has the ability to forward logs in CEF format. However, the log is received by LCE whether it is a log message from an LCE Client, Syslog server, IDS or any other compatible log format LCE will convert the original log generated into CEF format. Shown below is a normal syslog message received by an LCE server followed by the forwarded CEF formatted message.

Syslog Compliant Messages
Logs forwarded by the LCE will retain the original syslog alert level and facility, if one was present. If one was not present, the LCE assigns a log level of auth.warning.

Typically, LCE clients do not send syslog compliant messages. If a LCE client were configured to monitor a log file that retained an original message's syslog alert level and facility, then this would be retained if forwarded by the LCE.

This allows for a remote syslog server that is receiving events from the LCE to process the received messages and place them in specific files. Depending on the type of syslog server, it may be possible to place logs from a router into one file, operating system logs into another and so on.

**Content of Forwarded syslog Messages**

When the LCE forwards a message, it also adds any matched information to the log file as shown below if configured to do so:

```
Jun 30 17:45:36 lce: [not-matched] 0.0.0.0:0 -o- 192.0.2.1:0 ::
<37>sshd(pam_unix)[15322]: authentication failure; logname= uid=0 euid=0 tty=NODEVsshruser= rhost=192.0.2.1
```

The “::” characters are used to separate LCE's heading from the original message. In this case, the message would also have been sent with a syslog facility/severity of <37> since that was the facility of the original message.

Additionally, notice that the LCE tagged the example event above with a not-matched keyword. This means that the LCE did not possess a .prm file to process the log. If it did, the matched event name would be present in the same location.

If configured to strip the LCE headers from the forwarded syslog messages, only the original log message is sent to the remote syslog server.

**TCP Syslog Server Reconnect Interval**

The **TCP Syslog Server Reconnect Interval** sets the interval that the LCE will wait before making a reconnection attempt to the TCP syslog server that lost its connection.

**Time allowed to pass before the server will attempt to reconnect, if connection to a TCP syslog server is lost.**
TCP Syslog

This list of decimal ASCII character codes tells LCE how to delimit TCP syslogs. By default only the standard linefeed character (ASCII decimal 10) is recognized but other products may use special characters.

<table>
<thead>
<tr>
<th>ASCII Delimiters</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>This list of decimal ASCII character codes tells the server how to delimit TCP syslogs. By default only the standard linefeed character (ASCII decimal 10) is recognized. [0-255]</td>
</tr>
</tbody>
</table>
Receiving Encrypted Syslog

Encrypted TCP Syslog

LCE can be configured to receive encrypted syslog. The configuration to enable this functionality is located in two places. The Encrypted TCP Syslog Listen Port can be found by selecting Configuration followed by Basic, and by default is configured to port 6514. To locate the Encrypted TCP Syslog section, select Configuration followed by Advanced, and scroll down until the Encrypted TCP Syslog section is displayed.

The “Encrypted TCP Syslog” functionality requires an rsyslog server configured to send encrypted syslog to the LCE server. A self-signed certificate can be used, but it is recommended to use a signed certificate from a trusted CA (Certificate Authority). The only configuration requirement in the “Encrypted TCP Syslog” is the “Senders’ CA Cert. PEM-encoded Path”, and the suggested path is /opt/lce/credentials/syslog/<filename.pem>.

A fingerprint can be generated, and used for authentication if it is placed in the “Authorized Fingerprints” section of the “Encrypted TCP Syslog” configuration. It is also suggested to include the IP address or DNS name of authorized hosts that will be forwarding encrypted syslog into the “Authorized Hosts” section of “Encrypted TCP Syslog”.

An example configuration is shown below:

<table>
<thead>
<tr>
<th>Encrypted TCP Syslog</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senders’ CA Cert, PEM-encoded Path</td>
</tr>
<tr>
<td>Authorized Hosts</td>
</tr>
<tr>
<td>Option</td>
</tr>
<tr>
<td>------------------------------</td>
</tr>
<tr>
<td>Senders’ CA Cert PEM-encoded Path</td>
</tr>
<tr>
<td>Authorized Fingerprints</td>
</tr>
<tr>
<td>Note:</td>
</tr>
<tr>
<td>Authorized Hosts</td>
</tr>
<tr>
<td>Note:</td>
</tr>
</tbody>
</table>
Example Encrypted TCP Syslog Configuration

How the Encrypted TCP syslog is configured depends on the implementation of the rsyslog server that is forwarding the logs to LCE. For this example, certificates generated by the openssl-utils script contained in the /opt/lce/tools directory will be used. The certificates generated by the openssl-utils script are X509v3 certificates that will require the FQDN (fully qualified domain name) of each host. The OS used for this example is CentOS 6 64-bit.

To configure the TCP syslog:


   ```
   # ./openssl-utils.sh --generate-CA-creds 'C=US,st=MD,CN=lce01.example.com' /tmp/foo-creds/ca/
   ```

   Generate the certificates for the rsyslog server.

   ```
   # ./openssl-utils.sh --generate-creds devsyslog1.example.com 192.0.2.157 'C=US,st=MD,CN=syslog1.example.com' /tmp/foo-creds/client// /tmp/foo-creds/ca/
   ```

   Generate a client certificate to revoke. This is done to create a certificate revocation list. This is optional.

   ```
   # ./openssl-utils.sh --generate-creds revoke.example.com 192.0.2.47 'C=US,st=MD,CN=revoke.example.com' /tmp/foo-creds/revoked// /tmp/foo-creds/ca/
   ```

   Generate the revocation list certificate. This is only required if you completed the previous step.

   ```
   # ./openssl-utils.sh --revoke /tmp/foo-creds/revoked/cert.pem /tmp/foo-creds/ca/ /tmp/foo-creds/crl.pem
   ```

2. Copy credentials to /opt/lce/credentials/syslog, and to a directory on the remote rsyslog server. Copy the cert.pem certificates to the /opt/lce/credentials/syslog directory on your LCE server.
The certificate will need to be renamed to `rsyslog-ca.pem` so it does not overwrite the LCE `cert.pem` file that already exists in the same location.

**Caution:** Make sure when copying the files to the `/opt/lce/credentials` directory that you do not overwrite the SSL credentials that were generated at the time of installation. The credentials are `CA-cert.pem`, `CA-privkey.pem`, `server-cert.pem`, and `server-privkey.pem`.

```
[root@test01 ca]# cp /tmp/foo-creds/ca/cert.pem /opt/lce/credentials/syslog/rsyslog-ca.pem
```

Copy the certification revocation list (`crl.pem`) to `/opt/lce/credentials/syslog` directory on your LCE server.

```
[root@test01 ca]# cp /tmp/foo-creds/crl.pem /opt/lce/credentials/syslog/crl.pem
```

Copy these certificates to a directory on the server running rsyslog. For this example they will be placed in the `/root/selfsigned` directory of the rsyslog server.

```
/tmp/foo-creds/client/privkey.pem
/tmp/foo-creds/client/cert.pem
/tmp/foo-creds/ca/cert.pem
```

Notice that two of these certificates have the same name. It is suggested the certificate from the `/tmp/foo-creds/ca/` directory be renamed to `rsyslog-ca.pem`.

3. Set file permissions on the certificates.

Verify the file permissions, and ownership on the certificates that were moved to `/opt/lce/credentials/syslog`. Each file should be read only by user, and group. They should be owned by `lce`. Use the following commands to change ownership and permissions.

```
# chmod 440 crl.pem
# chown lce:lce crl.pem

# chmod 440 rsyslog-ca.pem
# chown lce:lce ca.pem
```
The files moved to the rsyslog server should have the same file permissions, but should be owned by the root user.

```bash
# chmod 440 rsyslog-ca.pem
# chmod 440 privkey.pem
# chmod 440 cert.pem
```

4. Use your preferred text editor to add the following lines to the rsyslog server configuration (rsyslog.conf) file if they are not already present.

```bash
#$MainMsgQueueType Direct
# set up the action
$DefaultNetstreamDriver gtls # use gtls netstream driver
$ActionSendStreamDriverMode 1 # require TLS for the connection
#$ActionSendStreamDriverAuthMode anon # server is NOT authenticated
$ActionSendStreamDriverAuthMode x509/certvalid

# rsyslog v5 configuration file
# certificate files - just CA for a client
$DefaultNetstreamDriverKeyFile /root/self-signed/privkey.pem
$DefaultNetstreamDriverCertFile /root/self-signed/cert.pem
$DefaultNetstreamDriverCAFile /root/self-signed/rsyslog-ca.pem

# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
*.* @@lce01.example.com:6514
```

Restart the rsyslog service.

```bash
# service rsyslog restart
```

The following items will need to be included in the LCE interface configuration of Encrypted TCP Syslog. The path for the Senders’ CA Cert, PEM-encoded Path will need to be given, which would be /opt/lce/credentials/syslog/rsyslog-ca.pem.

The certificates were generated using X509v3 extensions, which means the FQDN (Fully Qualified Domain Name) will need to be entered into Authorized Hosts. After the information has been entered scroll to the bottom of the page, and select Update.
5. Configure the “Encrypted TCP Syslog” settings in the LCE interface under **Configuration > Advanced**, and update the configuration.
TASL and Plugins

Excluding TASL Files

TASLs may be disabled selectively by adding the TASL script file name (e.g., program_accounting.tasl) to the **Disabled TASL Scripts** section. This option is located under the **TASL and Plugins** portion of the **Advanced** section of the LCE interface. This is useful for cases where a particular TASL script is not needed by an organization or where the TASL might be causing performance issues and needs to be disabled either temporarily or permanently.

Any disabled TASLs, if removed from the **Disabled TASL Scripts** section, can be re-enabled.

Excluding PRM Files

In some cases, a user may wish to allow the global updates of PRM files, but specifically exclude some from being run. This can be facilitated by using the **Disabled PRM Scripts** section of the LCE interface. The PRM files to be processed but not loaded can be specified in this location, one per line.

If there is a need to customize a plugin or plugins, rename the original file before making modifications. Once done, include the name of the original plugin in the **Disabled PRM Scripts** section. If an existing PRM file is modified and not renamed, it will be overwritten on the next PRM update. If the original is not disabled, and the Multiple Matches option is not enabled, only one of the two PRM files will match. This option is located under the **TASL and Plugins** portion of the **Advanced** section of the LCE interface.
Event Rules

This section is used to configure active response operations used by the LCE daemon. LCE rules are configured to analyze LCE event content and fire if preset conditions are met. Active responses include the ability to send automatic emails (msmtp, sendmail), syslog alerts (syslog, cef), or run custom commands on the LCE system.

Creating Event Rules

To add a new event rule to your configuration, in the Advanced section of Configuration, under Event Rules, click the Add a New Rule button. The Create an event rule window appears. Using this window, you can specify a name, filters, and an action to be taken.
The following table outlines the syntax that can be applied to filters and actions. Some examples are also available.

### Rule Filters

In the **Filter** drop-down box, select a filter that you want to use for the event rule. The values in the **Type** box are contextual, based on the filter you select. In some cases, you may not need to specify a type. Generally, you will need to specify whether you want to filter data that includes or excludes the values you specify. You can specify multiple filters.

<table>
<thead>
<tr>
<th>Filters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP (SrcIPS)</td>
<td>This filter will search for source IP addresses that are or are not present. The following five formats are supported:</td>
</tr>
<tr>
<td></td>
<td>- 192.0.2.1/255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>- 192.0.2.1/32</td>
</tr>
<tr>
<td></td>
<td>- 192.0.2.1-255</td>
</tr>
<tr>
<td></td>
<td>- 192.0.2.1-192.0.2.255</td>
</tr>
<tr>
<td></td>
<td>- 192.0.2.1</td>
</tr>
<tr>
<td></td>
<td>Each of these formats represent a single value. You can include a comma-delimited list of values using one or a mix of these formats.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>192.0.2.1/32, 192.0.2.1-255, 192.0.2..10</td>
</tr>
<tr>
<td>Destination IP (DstIPS)</td>
<td>This filter will search for destination IP addresses that are or are not present. The following five formats are supported:</td>
</tr>
<tr>
<td></td>
<td>- 192.0.2.1/255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>- 192.0.2.1/32</td>
</tr>
<tr>
<td></td>
<td>- 192.0.2.1-255</td>
</tr>
<tr>
<td></td>
<td>- 192.0.2.1-192.0.2.255</td>
</tr>
<tr>
<td>Filters</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| IP (IPS) | This filter allows for the search of IP addresses that are or are not present as either source or destination. The following five formats are supported:  
- 192.0.2.1/255.255.255.0  
- 192.0.2.1/32  
- 192.0.2.1-255  
- 192.0.2.1-192.0.2.255  
- 192.0.2.1  
Each of these formats represent a single value. You can include a comma-delimited list of values using one or a mix of these formats.  
Example: `192.0.2.1/32, 192.0.2.1-255, 192.0.2..10` |
| Events | Filter on LCE normalized event name. Considers both the primary and secondary event names.  
Example: `Cisco-IDS_Command_Execution, Windows-Successful_Network_Login, Linux-User_Added` |
| Sensors | Filter on sensor name (available in the LCE sensor summary view or under Sensor Names) or LCE client name.  
Example: `XPmarketing01, Win7payroll02` |
| Types | Filter on LCE event type.  
Example: `login, login-failure, intrusion` |
<p>| Ports | Filter on the source or destination port. |</p>
<table>
<thead>
<tr>
<th>Filters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filters</td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Example: 80, 443</td>
<td></td>
</tr>
<tr>
<td>Protocols</td>
<td>Filter on the protocol of the event. Note that this means the protocol number as defined by IPv4 (1 for ICMP, 6 for TCP, etc.)</td>
</tr>
<tr>
<td>Example: 1, 6</td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td>Filter on the username in a log.</td>
</tr>
<tr>
<td>Example: bobt, johnc</td>
<td></td>
</tr>
<tr>
<td>Text</td>
<td>Filter on any string in the log (strings can include spaces and punctuation, but not commas).</td>
</tr>
<tr>
<td>Example: Tenable Network Security</td>
<td></td>
</tr>
<tr>
<td>Text, caseless (IText)</td>
<td>Filter on any string in the log, but the text considered would be case insensitive (strings can include spaces and punctuation, but not commas).</td>
</tr>
<tr>
<td>Example: Tenable Network Security</td>
<td></td>
</tr>
<tr>
<td>Vulnerable</td>
<td>Only accepts yes or no. Specify yes if you want to only match logs that correlate to vulnerable hosts.</td>
</tr>
<tr>
<td>Threshold</td>
<td>The number of events required over a specified length of time to trigger the rule. The timeframe is expressed using the following format:</td>
</tr>
<tr>
<td>Example: 600 in a minute</td>
<td></td>
</tr>
<tr>
<td>MaxQueue</td>
<td>The number of events that will be placed into the event processing queue before being dropped from rule evaluation.</td>
</tr>
<tr>
<td>Ratelimit</td>
<td>The maximum number of triggers that will occur over a specified length of time regardless of the number of triggering events. The timeframe is expressed using the following format:</td>
</tr>
<tr>
<td>Example: 1 per hour</td>
<td></td>
</tr>
</tbody>
</table>
Rule Actions

In the **Action** drop-down box, specify an action that you want to take based on the filters you created. The following table describes the actions that are available.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shell command</td>
<td>Runs the given command at the command line as user lce. Examples of the syntax and variables you can use with the shell command follow this table.</td>
</tr>
<tr>
<td>Syslog</td>
<td>Forward logs triggered by this rule to the given syslog server. Examples of the syslog syntax follow this table.</td>
</tr>
<tr>
<td>CEF</td>
<td>Forward logs triggered by this rule to the given syslog server in CEF format. An example of the CEF syntax follows this table.</td>
</tr>
<tr>
<td>Ignore</td>
<td>Causes all events matching the filters to be ignored by LCE. If an event is ignored in this manner there will be no LCE database entry written for it, no other matching event rules will fire, and no TASLs will process this event for alerts. You cannot enter a value for this action.</td>
</tr>
</tbody>
</table>

**Email Syntax**

Command: `echo "body: $log" | sendmail rgula@example.com "subject: $event1 from $sip"

Command: `echo "This is a test message." | /opt/lce/tools/msmtp -C /opt/lce/tools/msmtp.conf bob@example.com`

**Syslog Syntax**

The following syslog line would forward any log that triggered the rule to the remote syslog server 10.10.10.10, port 514, with the default priority of 36 (severity=4, facility=4):

```
syslog: 10.10.10.10 "Possible password guessing evidence: $log"
```

The following syslog line would forward any log that triggered the rule to two remote syslog servers, 10.10.10.9, and 10.10.10.10, on port 515, with the specified priority of 116 (severity=4, facility=14):
syslog: 10.10.10.9, 10.10.10.10 "Your message goes here: $log" -priority 116 -port 515

CEF Syntax
The following value would forward any log that triggered the rule to two remote syslog servers, 10.10.10.9, and 10.10.10.10, on port 515:

10.10.10.9, 10.10.10.10 -port 515

Custom Command Syntax
Command: /path/to/scripts/my_custom_firewall_reconfig_command.sh -block $sip

Shell Command Variables
The following case sensitive variables may be included in the shell command string. Any commands using one or more the of shell command variables below need to be encapsulated in double quotations ("").

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$sip</td>
<td>Source IP of event</td>
</tr>
<tr>
<td>$dip</td>
<td>Destination IP of event</td>
</tr>
<tr>
<td>$sport</td>
<td>Source port of event</td>
</tr>
<tr>
<td>$dport</td>
<td>Destination port of event</td>
</tr>
<tr>
<td>$proto</td>
<td>Protocol of event, displayed as N/A, TCP, UDP, ICMP, or a number for other protocols</td>
</tr>
<tr>
<td>$vuln</td>
<td>&quot;no&quot; if the event was not correlated with a vulnerability, &quot;yes&quot; otherwise.</td>
</tr>
<tr>
<td>$sensor</td>
<td>Name of sensor generating the event</td>
</tr>
<tr>
<td>$event1</td>
<td>Primary event name</td>
</tr>
<tr>
<td>$event2</td>
<td>Secondary event name</td>
</tr>
<tr>
<td>$type</td>
<td>Type name of event</td>
</tr>
</tbody>
</table>
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>$time</code></td>
<td>Time event was recorded at LCE (format: Mon MM, YYYY H:M:S)</td>
</tr>
<tr>
<td><code>$user</code></td>
<td>Username associated with the event</td>
</tr>
<tr>
<td><code>$log</code></td>
<td>Raw text of log</td>
</tr>
<tr>
<td><code>queued_logs</code></td>
<td>All logs currently in the event rules queue. Use of this variable has the effect of emptying the rule's queue</td>
</tr>
</tbody>
</table>

### Show All Event Rules

You can display all configured event rules ordered by descending time of creation or modification with `psqlf show-config--mv--event_rules.sql`.

Example output:

```sql
added  val
2020 Dec22 14:59:44 | Save the English knights
                          | *SrcIP: 172.0.0.1
                          | -SrcIP: 8.0.8.8-9.9.9.9
                          | Command: /sbin/bunnies/chain-the-attack-rabbit
2020 Oct22 14:53:51 | [Ignore] Cisco - Events (General)
                          | *Events: Cisco-Adj_Failed_ToResolve
                          | *Events: Cisco-Line_Down
                          | *Events: Cisco-Line_Up
                          | *Events: Catalyst-Line_Down
                          | *Events: Catalyst-Line_Up
                          | *Events: CiscoSE-Radius_Accounting
                          | *Events: CiscoASA-Duplicate_ICP_Syn
                          | *Events: CiscoASA-Translation_Creation_Failed
                          | *Events: CiscoASA-No_Matching_Connection
                          | *Events: CiscoASA-Deny_Reverse_Path_Check
                          | Ignore
                          | *Events: Paloalto-System-Critical_Msg
                          | Command: printf "%Subject: [Alert] [Alert] Paloalto-System-Critical_Msg
                          | Paloalto - Critical System Message\n\n\nTime: \n\nSensor: \n\nType: \n\nUser: 
\nVulnerability: \n\nEvent Details: \n\n\nLog: " /opt/ice/tools/msmt -c /opt/ice/tools/msmtp.conf Joe.Q.Customer@someplace.com
```
Event Rules Examples

LCE can be configured with the ability to interpret received log events based on log content and use configurable rules to generate active responses from the LCE server. These rules are configured in the LCE interface in the Event Rules section and can perform three primary responses:

- email alerting
- syslog alerting
- command execution

**Note:** The LCE server will generate email alerts using the settings found in the /opt/lce/tools/ directory on the LCE server. This file will need to include your email server information for alerting to function correctly.

Example: Sample msmt.conf File

```bash
# Example smtp configuration file
#
# Please replace the following with the desired settings for mail server, encryption
# and authentication. The full
# smtp documentation is located at http://msmt.sourceforge.net/doc/msmt.html.
#
# smtp usage example: echo "This is a test message." | /opt/lce/tools/smtp -C
# /opt/lce/tools/smtp.conf your_name@your_address.com
account provider
host smtp.gmail.com
  tls on
tls_certcheck off
tls_starttls off
from your_username@your_domain.com
auth on
user your_username
password your_password
port 465
logfile /opt/lce/tools/msmt.log
# Set the above account to be the default when the -a flag is not used
account default : provider
```
Examples of practical applications include configuring rules to rate limit certain types of log events, email administrators immediately when an attack is detected, and send customized commands to a firewall when an inbound attack is detected and firewall reconfiguration needs to take place.

Various fields within the received log alert are automatically placed in variables that may be used as parameters within the active response. For example, consider the following Event Rules entry:

<table>
<thead>
<tr>
<th>Name: DMZ Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>+IPS: 192.168.20.15,192.168.20.100,192.168.20.110-112</td>
</tr>
<tr>
<td>Event: SC4-Login</td>
</tr>
<tr>
<td>Command: echo &quot;body: $log&quot;</td>
</tr>
<tr>
<td>RateLimit: 5m</td>
</tr>
</tbody>
</table>

This rule takes LCE events labeled “SC4-Login” to the specified IP addresses and automatically generates an email alert to the specified administrator email addresses. In addition, a rate limit is applied such that only one email would be sent every five minutes to prevent the LCE server from overwhelming the email server system. Configuration possibilities are limited only by the imagination of the LCE server administrator.
Service Control

The **Control** section of **System Configuration** is used to verify the status of an LCE service. This section can also be used to start and stop each service that is related to LCE if needed.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Processes</td>
<td>Stop or Start all LCE daemons</td>
</tr>
<tr>
<td>Log Engine</td>
<td>Stop or Start the LCE daemon</td>
</tr>
<tr>
<td>Query Interface</td>
<td>Stop or Start the LCE query daemon</td>
</tr>
<tr>
<td>Vulnerability Reporter</td>
<td>Stop or Start the LCE Vulnerability Reporter daemon</td>
</tr>
<tr>
<td>Statistics Engine</td>
<td>Stop or Start the Statistics daemon</td>
</tr>
<tr>
<td>TASL Engine</td>
<td>Stop or Start the TASL Engine daemon.</td>
</tr>
</tbody>
</table>
Feed Settings

The Feed Settings section contains the following groups of settings:

- Feed Registration
- Plugin Update
- Offline Plugin Update
- Web Proxy
- Tenable.io Configuration
Feed Registration

The Feed Registration section is where the activation code is entered. Once a new code is entered, click the Apply button.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation Code</td>
<td>Your activation code is obtained from the <a href="https://community.tenable.com">Tenable Community site</a>, as described in the <a href="https://community.tenable.com">Tenable Community Guide</a>. If a new code is required, type it in the field and click the Apply button.</td>
</tr>
</tbody>
</table>
Plugin Update

Updating Plugins (PRM Files) and TASL Scripts

This section describes the method for updating LCE plugins (files with a .prm extension) and TASL scripts. Plugin updates occur over a HTTPS connection at a set interval. The default update interval is set to 3 days, but can be increased or reduced if required. The LCE interface Plugin Update section, which is found in the Configuration section under Feed Settings, can be easily used to update all plugins along by clicking the Update Plugins button.

The directories containing the PRM files and TASL scripts are specified in the /opt/lce/daemons/plugins directory. When you update plugins, the files contained in the /opt/lce/daemons/plugins directory, which are plugins and correlation scripts (TASL) will be archived to the /opt/lce/daemons/plugins_archive directory. The backups of the files in the TASL directory will appear in the plugins_archive directory as a file such as tasls.tar.gz, and the backups of the files in the plugins directory will appear in the plugins_archive directory as a file such as lce.tar.gz. The backup is only kept until the next plugin update.

Offline Updates

The Offline Plugin Update section can be found in the Configuration section of the LCE interface under Feed Settings. It allows for a .tar file of the LCE plugins to be uploaded by browsing to the file, and then clicking the Process Plugins button.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline Update File</td>
<td>Used to upload a new set of plugins to the LCE. This is only required if an LCE server does not have internet access.</td>
</tr>
<tr>
<td>Process Update</td>
<td>Clicking this button will complete the update process using the plugins file that was uploaded.</td>
</tr>
</tbody>
</table>
# Web Proxy

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Address</td>
<td>The IP address of the proxy server to be used with LCE</td>
</tr>
<tr>
<td>Proxy Username</td>
<td>The username for the proxy if it is required</td>
</tr>
<tr>
<td>Proxy Password</td>
<td>The password for the proxy if it is required</td>
</tr>
<tr>
<td>Verify Proxy Password</td>
<td>The password entered again for verification</td>
</tr>
<tr>
<td>Custom Plugin Feed Host</td>
<td>If a custom plugin feed is used with the LCE server, that host information is entered here.</td>
</tr>
<tr>
<td>Custom User Agent</td>
<td>Custom user agent string used during plugin update requests.</td>
</tr>
</tbody>
</table>
## Tenable.io Configuration

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Address</td>
<td>The IPv4 address or hostname of Tenable.io, usually cloud.tenable.com.</td>
</tr>
<tr>
<td>Cloud Port</td>
<td>[1-65535] Usually 443</td>
</tr>
<tr>
<td>Cloud Scanner Key</td>
<td>User-specified key to connect to Tenable.io.</td>
</tr>
<tr>
<td>Scanner Name</td>
<td>User-specified LCE scanner name when connects to Tenable.io.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The scanner name can be a maximum of 128 characters.</td>
</tr>
<tr>
<td>Job Queue Check Rate</td>
<td>A value between 5 seconds and 60 minutes. By default, 15 seconds</td>
</tr>
</tbody>
</table>
Refresh or Replace the Vulnerability Reporter SSL Certificate

**Required User Role:** Administrator

To update the self-signed SSL certificate used to upload vulnerability reports to Tenable.sc, do one of the following:

- Rotate the self-signed SSL certificate, replacing it with a fresh self-signed certificate.
- Replace the self-signed SSL certificate packaged with LCE with an SSL certificate from your organization.

To rotate the self-signed SSL certificate and replace it with a fresh self-signed certificate:

1. Log in to LCE via the command line interface (CLI).
2. In the CLI in LCE, run the following command to refresh the SSL certificate:

   ```bash
   /opt/lce/tools/lce_crypto_utils --generate-creds-vulnReporter -q
   ```

   LCE regenerates the SSL certificate locally.

3. Re-add the LCE to Tenable.sc, as described in Add a Log Correlation Engine Server in the Tenable.sc User Guide.

To replace the SSL certificate used to upload vulnerability reports to Tenable.sc:

1. Copy the following files from your CA to `/opt/lce/reporter/ssl/`.
   - cacert.pem
   - servercert.pem
   - cakey.pem
   - serverkey.pem

   **Note:** Do not change the certificate file names.

2. Add the LCE to Tenable.sc, as described in Add a Log Correlation Engine Server in the Tenable.sc User Guide.
Upgrade the LCE Server

**Required User Role:** Root user

For information about new features, resolved issues, third-party product updates, and supported upgrade paths, see the [release notes](#) for LCE.

**Note:** All LCE server installations are compatible with Client versions 4.0.0 and later. Older LCE clients will not be able to log in and send event data to LCE 4.4 - 5.1.

Before You Begin

- Download the LCE server package from the [Tenable Downloads](#) page.

**Note:** The complete PostgreSQL 11.1 is bundled inside the LCE RPM.

To upgrade the LCE server:

1. Log in to LCE via the command line interface (CLI).

2. In the CLI in LCE, run the following command, where `<package name>` is the name of the LCE server package you downloaded from the Tenable Downloads page:

   ```bash
   rpm -Uvh <package name>
   ```

   The upgrade begins.

   ```bash
   # rpm -Uvh lce-6.0.0-el6.x86_64.rpm
   Preparing... #===============================================================================
   [100%]
   1:lce warning: /opt/lce/.ssh/authorized_keys
   created as /opt/lce/.ssh/authorized_keys.rpmnew
   #=============================================================================== [100%]
   The installation process is complete.
   Please refer to /var/log/lce_upgrade.log to review installation messages.

   To configure LCE, please direct your browser to:
   https://192.168.0.123:8836
   ```
3. (Optional) Migrate your silos using the `/opt/lce/tools/migrateDB-overseer` utility. The utility supports the following operations:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--estimate-required-disk-space</td>
<td>Estimates how much disk space your 5X silos will need, once migrated into 6X datastore; note, this estimate does not account for events created &quot;live&quot; by LCE in the course of its normal operation while migration is running. If needed it will remind you to give the --clear-source-on-success option to --migrate-all operation.</td>
</tr>
<tr>
<td>--estimate-total-duration</td>
<td>Shows conservative estimates for how long the migration will take for each plausible nParallelWorkers value. Also shows what nParallelWorkers value will be chosen by default.</td>
</tr>
<tr>
<td>--migrate-all [--clear-source-on-success] [&lt;nondefault_nParallelWorkers&gt;]</td>
<td>If you do not specify --clear-source-on-success, the LCE 5X silos will be left as they were, after LCE 6.0.0 silos with the same contents are built. This could lead to running out of disk space.</td>
</tr>
<tr>
<td>--status</td>
<td>Use this option at any time, from another shell console, to see how migration is progressing.</td>
</tr>
</tbody>
</table>

**Caution:** Prior to beginning an event silo migration, you should take precautions to ensure there will be sufficient disk space. A silo in the LCE 6.0.x PostgreSQL format will require more disk space than the same silo in the LCE 5.x Elasticsearch format.

**Note:** While a higher value means a faster migration, it also means less resources will remain for normal LCE operation.

**Note:** Tenable strongly recommends running the `/opt/lce/tools/migrateDB-overseer` --migrate-all command instead of migrating one silo at a time with --migrate-one. With the --migrate-all option, the silos with the most recent events will be migrated first, followed by older silos. With --migrate-one, you cannot automatically undo in event of failure. Using --migrate-one does not guard against event loss or progress bookmarking for correct resumption after premature termination.
**Note:** If your SSH console session times out after you start `migrateDB-overseer`, the migration will stop (and you need to start it again later). To avoid this issue, start `migrateDB-overseer` in console-detached mode:

```bash
nohup /opt/lce/tools/migrateDB-overseer &
```

or

```bash
nohup /opt/lce/tools/migrateDB-overseer --migrate-all --clear-source-on-success &
```
Upgrade your LCE License

You can upgrade your LCE license to a license with higher capacity (e.g., 1 TB to 10 TB). Upgrading your LCE license requires a new license key.

To upgrade your LCE license:

1. Log in to the LCE interface.
2. In the top navigation bar, click Configuration.
   The Configuration page appears, displaying the Basic section.
3. In the left navigation bar, click Feed Settings.
   The Feed Settings section appears.
4. In the Activation Code box, type your new activation code, and then click the Apply button.
5. At the bottom of the Feed Settings section, click the Update button.
   LCE applies the new license.

Tip: To confirm the license upgraded successfully, navigate to Health and Status, and select Plugins to verify the Activation status is Licensed and the Feed Expiration does not show Expired.
Users

The LCE interface can be accessed by two user types: Administrator and Read Only. An Administrator user has the ability to perform all administration of the LCE interface. The Read Only user can only view the Health and Status page. A user's privilege can be seen under User Type.

**Note:** Generally, when this documentation refers to a user, it means a user with Administrator privileges. Otherwise, the documentation will specify a Read Only user.

For more information, see:

- Add Users
- Edit Users
- Delete Users
- Change a User's Password
- Lock a User Account
- Unlock a User Account
- View User Accounts
- Certificate-Authenticated Web UI Logins

Locked User Accounts

Users with locked accounts cannot login until an administrator unlocks their account. User accounts may be automatically locked if they do not follow the password reuse or login session policies an administrator configured. For more information about site policies, see [Site Policies](#).
If a user’s account becomes locked while that user is logged in, LCE immediately terminates the locked user's session.

You can unlock a user's account by doing one of the following:

- Resetting their password, as described in Change a User's Password.
- Using the user-utils utility, as described in Unlock a User Account.

You can check to see if a user's account is locked via the LCE web UI or the CLI, as described in View User Accounts. To lock a user's account, see Lock a User Account.
Add Users

For more information, see Users.

To add a new user:

1. Log in to LCE via the user interface.
2. In the top navigation bar, click Users.
   The Users page appears.
3. Click +New User.
   The +New User window appears.
4. In the Username box, type a username that meets the following criteria:
   - Uses only ASCII alphanumeric characters, at signs, periods, underscores, or hyphens
   - Begins with an alphanumeric character or an underscore
   - Does not contain multiple consecutive periods, underscores, or hyphens
   - Uses fewer than 127 characters
5. In the Password box, type a temporary password for the user.
6. In the Confirm Password box, type the temporary password again.
7. (Optional) To make this user an administrator, select the Administrator check box.
8. Click Create User.
   LCE saves your configuration.
**View User Accounts**

**Required User Role:** Administrator

For more information, see [Users](#).

To view a list of users via the LCE web UI:

1. Log in to LCE via the user interface.
2. In the top navigation bar, click [Users](#).
   
   The Users page appears.
3. View details about each user account:
   
   - **Name** — The username for the user.
   
   - **Last Login** — The date and time the user last logged in to LCE.
   
   - **Status** — The status of the user's account.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ok</td>
<td>The user's account is working normally.</td>
</tr>
<tr>
<td>Locked</td>
<td>The user cannot log in to LCE. To allow this user to log in to LCE, unlock their account, as described in <a href="#">Unlock a User Account</a>.</td>
</tr>
</tbody>
</table>

- **User Type** — The user's role: [Administrator](#) or [Read Only](#).

To view a list of user accounts via the CLI:

1. In the command line interface (CLI), run the following command:

   ```bash
   /opt/lce/tools/user-utils --list-all
   ```

   The `user-utils` utility prints a table of users with the following details:
- **Purpose** — The user's role.

  **Note:** In the printed table, **Administrators** are labeled **WebUI admin** and **Read Only** users are labeled **WebUI readonly**.

- **Username** — The user's username.

- **Locked acct?** — Indicates whether the user's account is locked (yes or no). For more information, see [Locked User Accounts](#).

- **Temp. passw?** — Indicates whether the user has a temporary password (yes or no).

- **Last Reset** — The date and time of the user’s most recent password reset.

- **Last Auth Success** — The date and time of the user's most recent login.

- **Last Activity** — The date and time the user interacted with the LCE web UI.
Edit Users

For more information, see Users.

**Note:** After you set a temporary password for a user, the user must change their password the next time they log in to LCE.

To edit a user via the LCE web UI:

1. Log in to LCE via the user interface.
2. In the top navigation bar, click **Users**.
   - The **Users** page appears.
3. Click the row for the user.
   - The **Edit User** window appears.
4. Modify the user details.
5. Click **Update**.
   - LCE saves your configuration.

To edit a user via the CLI:

- To lock a user's account, run:
  ```
  user-utils --lock--WebUI-acct <username>
  ```

- To unlock a user's account, run:
  ```
  user-utils --unlock--WebUI-acct <username>
  ```

- To change a user's password, run:
  ```
  user-utils --set-password--WebUI-acct <username>
  ```
Change a User's Password

Required User Role: Administrator

For more information, see Users.

Note: After you set a temporary password for a user, the user must change their password the next time they log in to LCE.

To change a user's password via the LCE web UI:

1. Log in to LCE via the user interface.
2. In the top navigation bar, click Users.
   
   The Users page appears.
3. Click the row for the user.
   
   The Edit User window appears.
4. In the New Password field, type a temporary password for the user.
5. In the Confirm Password field, type the temporary password again.
6. Click Update.
   
   LCE saves your configuration.

To change a user's password via the CLI:

1. Log in to LCE via the command line interface (CLI).
2. In the CLI in LCE, run the following command:

   ```
   user-utils --set-password--WebUI-acct <username>
   ```

   The user-utils utility prompts you for a temporary password.
3. Type a temporary password for the user and press Enter.
   
   The user-utils utility sets the temporary password for the user.
Delete Users

For more information, see Users.

To delete a single user:

1. Log in to LCE via the user interface.
2. In the top navigation bar, click Users.
   The Users page appears.
3. In the row for the user you want to delete, click x.
   The Delete User window appears.
4. Click Delete.
   LCE deletes the user account and immediately terminates the deleted user's session.

To delete multiple users at once:

1. Log in to LCE via the user interface.
2. In the top navigation bar, click Users.
   The Users page appears.
3. In the row for each user you want to delete, select the check box.
4. In the Actions drop-down box, click Delete Users.
   The Delete User window appears.
5. Click Delete.
   LCE deletes the user accounts and immediately terminates the deleted users' sessions.
Unlock a User Account

**Required User Role:** Administrator

Users with locked accounts cannot login until an administrator unlocks their account. User accounts may be automatically locked if they do not follow the password reuse or login session policies an administrator configured. For more information about site policies, see [Site Policies](#).

For more information about user accounts, see [Users](#).

**Tip:** Resetting a locked user's password unlocks their account. For more information, see [Change a User's Password](#).

Before you begin:

- (Optional) Determine if a user account is locked by viewing their account status, as described in [View User Accounts](#).

To unlock a locked user account via the CLI:

1. In the command line interface (CLI) in LCE, run the following command:

   ```
   /opt/lce/tools/user-utils --unlock--WebUI-acct <username>
   ```

   LCE unlocks the user account.
Lock a User Account

**Required User Role:** Administrator

Users with locked accounts cannot login until an administrator unlocks their account. User accounts may be automatically locked if they do not follow the password reuse or login session policies an administrator configured. For more information about site policies, see [Site Policies](#).

For more information about user accounts, see [Users](#).

To lock a user account via the CLI:

1. Log in to LCE via the command line interface (CLI).
2. In the CLI in LCE, run the following command:

   ```
   user-utils --lock--WebUI-acct <username>
   ```

   LCE locks the user account.
Certificate-Authenticated Web UI Logins

You can configure the LCE server to allow certificate-authenticated connections for users logging in to the LCE web UI. When enabled, LCE requires certificate authentication for all users.

When you configure certificate-authenticated web UI logins:

- Users cannot log in to LCE using a username and password.
- Users cannot change their passwords.
- LCE continues to enforce the following site policy configuration attributes:
  - `web_UI__password__enforce_complexity`
  - `web_UI__password__minimum_length`
- LCE ignores the following site policy configuration attributes:
  - `web_UI__password__fewest_changes_eve_reuse`
  - `web_UI__password__minimum_edit_distance`
  - `web_UI__password__max_lifetime_days`
  - `web_UI__password__minimum_lifetime_hours`

For more information about site policy configuration attributes, see [Site Policies](#).

To fully configure certificate-authenticated web UI logins:

1. Configure the LCE server for certificate-authenticated logins, as described in [Configure Certificate-Authenticated Web UI Logins](#).
2. Configure certificate authentication for individual user accounts, as described in [Enable Certificate-Authenticated Web UI Logins for a User](#).
Configure Certificate-Authenticated Web UI Logins

**Required User Role:** Administrator

You can configure the LCE server to allow certificate-authenticated connections for users logging in to the LCE web UI. When enabled, LCE requires certificate authentication for all users.

To configure certificate-authenticated logins for the LCE web UI, you will need a certificate file representing one or more certificate authority (CA) entities you trust to sign certificates for your users. Typically, this is a .pem file.

For more information, see Certificate-Authenticated Web UI Logins.

To configure certificate-authenticated web UI logins:

1. Log in to LCE via the command line interface (CLI).
2. In the CLI in LCE, run the following command:

   ```bash
   /opt/lce/tools/cfg-utils --set-sv web_UI__login__client_CA_cert_path <the CA certificate>
   ```

   LCE saves your configuration.

What to do next:

- Configure certificate authentication for individual user accounts, as described in Enable Certificate-Authenticated Web UI Logins for a User.
Enable Certificate-Authenticated Web UI Logins for a User

Required User Role: Administrator

After you configure the LCE server for certificate-authenticated web UI logins, configure certificate authentication for each LCE user account. For more information, see Certificate-Authenticated Web UI Logins.

Before you begin:

- Configure the LCE server to allow certificate-authenticated logins, as described in Configure Certificate-Authenticated Web UI Logins.

To configure certificate authentication for a user account:

1. Log in to LCE via the command line interface (CLI).
2. In the CLI in LCE, run the following command:

   ```
   /opt/lce/tools/cfg-utils --set-sv web_UI_login_client_CA_cert_path <the CA certificate>
   ```

   LCE saves your configuration.
Disable Certificate-Authenticated WebUI Logins

**Required User Role:** Administrator

For more information, see [Certificate-Authenticated Web UI Logins](#).

To disable certificate-authenticated web UI logins:

1. Log in to LCE via the command line interface (CLI).
2. In the CLI in LCE, run the following command:

   ```bash
   /opt/lce/tools/cfg-utils --set-sv web_UI_login_client_CA_cert_path ''
   ```

   LCE saves your configuration.
Manage Clients in LCE

To access the Clients page:

- In the top navigation bar, click Clients.
- The Clients page displays a table of authorized clients and clients requesting permission to communicate with the LCE server.

This table is referred to throughout this documentation as the client table.

Caution: The LCE Client Manager Interactive Mode is deprecated. Clients should be managed using the Clients page.

Additionally, the controls above the client table allow you to search the entries in the client table, apply filters, and show or hide table columns.

Client operations in LCE are performed using the client table that is displayed on this page. Certain operations can be performed on one or more clients simultaneously by selecting the check boxes in the rows corresponding to the clients with which you want to interact.

The following table lists the columns that appear on the Clients page, and provides a brief description of each. Only certain columns are visible by default.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>The IP address of the LCE client host. If you have more than one client installed on a host, the same IP address will appear multiple times.</td>
</tr>
</tbody>
</table>
| Name   | The value in the name column will be one of the following, ordered by priority:  
- The name you have assigned. |
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• The hostname of the LCE client host, if resolved by the LCE server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unknown</strong>, only if a name is not assigned, and the LCE server cannot resolve the hostname.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of LCE client. For example, <strong>LCE Splunk</strong> or <strong>LCE Client</strong>.</td>
</tr>
<tr>
<td>OS</td>
<td>The operating system supported by the installed LCE client package.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: While it may correspond, this value does not reflect the operating system installed on the host.</td>
</tr>
<tr>
<td>Policy</td>
<td>The file name of the policy currently assigned to the LCE client.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the installed LCE client package.</td>
</tr>
<tr>
<td>Last Heartbeat</td>
<td>The last time the LCE server received a heartbeat from an authorized LCE client.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong>: If you hover your cursor over this value, the exact timestamp appears.</td>
</tr>
<tr>
<td></td>
<td>Unauthorized clients do not send heartbeats. This can be used to identify LCE clients that are not reporting to the LCE server correctly.</td>
</tr>
<tr>
<td>Server</td>
<td>The IP address or hostname of the LCE server to which that LCE client is assigned. If the LCE client is installed on the same host as the LCE server, the IP addresses will be the same. By default, this column is not visible.</td>
</tr>
<tr>
<td>Authorized</td>
<td>Whether that LCE client is authorized to communicate with the LCE server. By default, this column is not visible.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong>: This can be used to identify LCE clients that are not be reporting to the LCE server correctly.</td>
</tr>
<tr>
<td>Alive</td>
<td>Whether a heartbeat or log was last received within the 5 minute reporting period from that client. By default, this column is not visible.</td>
</tr>
<tr>
<td>Logs today</td>
<td>The number of events received from that client today, including heartbeats.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>By default, this column is not visible.</td>
<td></td>
</tr>
<tr>
<td>UUID</td>
<td>The UUID of the client, if the client version supports UUIDs. The UUID is used to identify unique instances of LCE clients. By default, this column is not visible.</td>
</tr>
</tbody>
</table>
Clients Page Tasks

On the Clients page, you can do the following:

- Authorize an LCE Client
- Revoke an LCE Client Authorization
- Delete an LCE Client
- Rename an LCE Client
- Assign a Policy to an LCE Client
- Assign an LCE Client to a Server
Authorize an LCE Client

In order for an LCE client to communicate with an LCE server, it must first be authorized. LCE clients that have requested authorization appear in the client table.

**Note:** Client authorization is completed in the web-based LCE Interface on the Clients page.

To authorize a client to communicate with an LCE server:

1. Log in to LCE via the user interface.
2. In the top navigation bar, click **Clients**.

   The **Clients** page appears, displaying the client table.
3. In the client table, in the rows corresponding to the LCE clients that you want to authorize, select the check boxes.

   **Tip:** You can use filters or sort by the **Authorized** column to quickly find LCE clients that need to be authorized.
4. Above the client table, in the upper-left corner, click the **Actions** button, and then click **Authorize**.

   The **Authorize** dialog box appears.
5. Review the list of LCE clients that will be authorized, and then click the **Authorize** button.

   The LCE clients are authorized and will immediately send a heartbeat.
Additional Clients Page Tasks

This section details common tasks that are performed using the Clients page.

This section includes:

- View Details About an LCE Client
- Select Multiple Client Table Entries
- Search the Client Table
- Add a Client Table Filter
- Clear Client Table Filters
- Limit the Client Table Entries Shown
- Show and Hide Client Table Columns

View Details About an LCE Client

1. In the client table, click the row that corresponds to the LCE client for which you want to view details.

   The Detailed view window appears, displaying a list of details about that LCE client. You can modify values in the Name, Policy, and LCE server boxes.

2. If you make changes to the LCE client details, click the Update button.

   LCE saves your configuration.

Select Multiple Client Table Entries

There are two methods to select multiple entries in the client table:

- Above the client table, in the upper-left corner of the page, click the Select all button.

- In the rows corresponding to the LCE clients you want to select, click the check boxes.

Search the Client Table
• In the **Search** box, type a plain text search term. The **Search** box does not accept Boolean operators.

As you type, the client table will be filtered by your search term. The client table will search the text in all columns, regardless of whether they are shown or hidden.

**Tip:** If you are using the desktop version of Safari, you may need to disable the Correct SpellingAutomatically function to prevent the browser from rewriting search terms.

---

**Add a Client Table Filter**

1. Above the client table, in the upper-left corner, click the **Actions** button, and then click **Add filter**.

   The **Add new filter** dialog box appears.

2. In the **Filter on** box, select the column that contains the values you want to filter.

   Depending on the column you select, the **Filter** box will appear as a text box or a list. For example, if you select **Authorized**, the **Filter** box is a list with the values Yes and No. If you select **Name**, you can type directly into the **Filter** box.

3. In the **Filter** box, type or select a value.

4. Click the **Add** button.

   A new filter appears above the client table, and the client table is filtered based on the value.

---

**Clear Client Table Filters**

There are two methods you can use to clear filters:

• Above the client table, in the box that represents the filter you want to clear, click the **x**.

  Repeat this process for each filter you want to clear.

  **Example:**
• Above the client table, in the upper-right corner, click the Basic filter link. All filters that you have applied to the client table are cleared.

Limit the Client Table Entries Shown

• Above the client table, in the upper-right corner, in the Show box, select the number of entries you want to show per client table page. By default, the Show box is set to 10.

Show and Hide Client Table Columns

1. Above the client table, in the upper-right corner, click the Show / hide columns button.

   A list of columns appears.

   By default, the Name, Type, OS, Policy, Version, and Last Heartbeat columns are visible.

2. In the list of columns, select or clear the check boxes corresponding to the columns that you want to show or hide, respectively.

   As you select and clear check boxes, the corresponding columns are either shown or hidden on the client table.
Rename an LCE Client

Naming an LCE client makes it easier to locate in the client table in the future. Initially, an LCE client is given one of the following names, ordered by priority:

- The hostname of the LCE client host, if resolved by the LCE server.
- Unknown, if a name is not assigned and the LCE server cannot resolve the hostname.

To rename an LCE Client:

1. Log in to LCE via the user interface.
2. In the top navigation bar, click Clients.

   The Clients page appears, displaying the client table.

3. In the client table, in the row corresponding to the LCE client that you want to rename, select the check box.

   Note: You can rename multiple LCE clients by selecting the corresponding check boxes. The selected clients will be assigned the same name.

4. Above the client table, in the upper-left corner, click the Actions button, and then click Rename.

   The Rename client(s) dialog box appears.

5. In the Name box, type a name for the LCE client.

6. Review the LCE client that will be renamed, and then click the Rename client(s) button.

   The LCE client is renamed. The new name appears in the Name column of the client table.
Assign a Policy to an LCE Client

In addition to using Tenable.sc and the Policies page, you can assign policies to LCE clients via the Clients page.

To assign a policy to a client:

1. Log in to LCE via the user interface.
2. In the top navigation bar, click Clients.
   The Clients page appears, displaying the client table.
3. In the client table, in the row corresponding to the LCE client that you want to assign a policy, select the check box.
   
   **Note:** You can assign a policy to multiple LCE clients by selecting the corresponding check boxes. The selected LCE clients must be the same client type, and support the same operating system. The selected clients will be assigned the same policy.

4. Above the client table, in the upper-left corner, click the Actions button, and then click Change Policy.
   The Change policy dialog box appears.
5. In the Assign the following policy list, select the policy that you want to assign to the LCE client.
6. Review the LCE client that will have a new policy, and then click the Change policy button.
   The specified policy is assigned to the LCE client.
Assign an LCE Client to a Server

To assign a client to a server:

1. Log in to LCE via the user interface.

2. In the top navigation bar, click Clients.

   The Clients page appears, displaying the client table.

3. In the client table, in the rows corresponding to the LCE clients that you want to assign to a different LCE server, select the check boxes.

4. Above the client table, in the upper-left corner, click the Actions button, and then click Assign to.

   The Assign server dialog box appears.

   By default, below the list of LCE clients, the first box is set to IP address.

5. If you want to use a hostname, in the first box, select Hostname, and then type a hostname. Otherwise, type an IP address.

6. In the Port box, type the port number for the LCE server. Unless the LCE server has been configured to use a different port, the default LCE Client port is 31300.

7. Review the list of LCE clients that will be assigned to a new LCE server, and then click the Assign server button.

   The LCE clients are assigned to the specified LCE server.
Revoke an LCE Client Authorization

To revoke a client authorization:

1. Log in to LCE via the user interface.

2. In the top navigation bar, click **Clients**.

   The **Clients** page appears, displaying the client table.

3. In the client table, in the rows corresponding to the LCE clients that have authorizations you want to revoke, select the check boxes.

4. Above the client table, in the upper-left corner, click the **Actions** button, and then click **Revoke**.

   The **Revoke** dialog box appears.

5. Review the list of LCE clients that will have authorizations revoked, and then click the **Revoke** button.

   The authorizations for the LCE clients are revoked. The LCE clients will no longer be able to communicate with the LCE server, except to request authorization.
Delete an LCE Client

When you delete an LCE client on the Clients page, the LCE client is not uninstalled from its host, only removed from the client table. If the LCE client was authorized, the authorization will be revoked when it is deleted.

To delete a client on the Clients page:

1. Log in to LCE via the user interface.
2. In the top navigation bar, click Clients.
   
   The Clients page appears, displaying the client table.
3. In the client table, in the rows corresponding to the LCE clients that you want to delete, select the check boxes.
4. Above the client table, in the upper-left corner, click the Actions button, and then click Delete.
   
   The Delete dialog box appears.
5. Review the list of LCE clients that will be deleted, and then click the Delete button.
   
   The LCE clients are removed from the client table. If any of those clients were authorized, that authorization is revoked.
Client Policies

To access the Policies page, in the top navigation bar, click Policies. The Policies page appears, displaying a table of policies, including the pre-packaged default and TNS policies. This table is referred to throughout this documentation as the policy table.

The Policies page is used to perform the following tasks:

- Create client policies
- Edit client policies
- Clone client policies
- Delete client policies
- Download client policies
- Upload client policies

Creating, editing, and cloning policies is performed using the Client Policy Builder.

Additionally, using the controls above the policy table, you can search the entries in the policy table, and show or hide table columns.

The following table lists the columns that appear on the Policies page, and provides a brief description of each. By default, all columns are visible.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy name</td>
<td>The file name of the policy. The name of a prepackaged policy is prefixed by default or TNS. All policy files for LCE have the .1cp extension.</td>
</tr>
<tr>
<td>OS</td>
<td>The operating system supported by the policy.</td>
</tr>
<tr>
<td>Client Type</td>
<td>The type of LCE client that the policy is for. For example, LCE Splunk or LCE Client.</td>
</tr>
<tr>
<td>Clients using</td>
<td>The number of clients to which the policy is assigned.</td>
</tr>
<tr>
<td>Created by</td>
<td>The user who created the policy. In the case of the prepackaged policies, the value is lce.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last modified by</td>
<td>The user who last modified the policy.</td>
</tr>
<tr>
<td>Created on</td>
<td>The date on which the policy was created, or, if within 24 hours, the time since the policy was created. For example, 16 hours ago.</td>
</tr>
<tr>
<td>Actions</td>
<td>Contains the <strong>Edit</strong>, <strong>Clone</strong>, <strong>Delete</strong>, and <strong>Download</strong> buttons.</td>
</tr>
</tbody>
</table>

**List All Client Policies**

You can list all client policies with `/opt/lce/tools/list-policies`. For more information about the list-policies tool, see [list-policies](#).

Example output:
<table>
<thead>
<tr>
<th>basename</th>
<th>agent</th>
<th>tCreated</th>
<th>fH repellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>TNS-TenableProducts-FVS_rhel_iteclient.lcp</td>
<td>tail_Lnx</td>
<td>2021-01-04 15:43:14</td>
<td>9a926360b5cb888a2b25df35bf90b1138f782</td>
</tr>
<tr>
<td>default_rhel_opsec.lcp</td>
<td>OFSEC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TNS-Mielvents-Filesysmon_windows_tenableclient.lcp</td>
<td>tail_Win</td>
<td>2021-01-04 15:43:14</td>
<td>f294f9d4be6bea228d5f392fe865f95b6</td>
</tr>
<tr>
<td>default_rhel_sudee.lcp</td>
<td>SDEE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TNS-MalwareDetectionOnly_oss ITEclient.lcp</td>
<td>default_appliance_networkmonitor.lcp</td>
<td>2021-01-04 15:43:14</td>
<td>2d958f5f4d70b6756c774f85bb0f9eb77e</td>
</tr>
<tr>
<td>default_appliance_netflowclient.lcp</td>
<td>Netflow</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TNS-ProcessExecutionOnly_rhel ITEclient.lcp</td>
<td>default_networkmonitor.lcp</td>
<td>2021-01-04 15:43:14</td>
<td>2d958f5f4d70b6756c774f85bb0f9eb77e</td>
</tr>
<tr>
<td>TNS-TenableProducts-Nessus_windows_tenableclient.lcp</td>
<td>default_air ITEclient.lcp</td>
<td>2021-01-04 15:43:14</td>
<td>2d958f5f4d70b6756c774f85bb0f9eb77e</td>
</tr>
<tr>
<td>TNS-MiSQLServer_windows_tenableclient.lcp</td>
<td>default_oss ITEclient.lcp</td>
<td>2021-01-04 15:43:14</td>
<td>2d958f5f4d70b6756c774f85bb0f9eb77e</td>
</tr>
<tr>
<td>TNS-MalwareDetectionOnly_oss ITEclient.lcp</td>
<td>default_oss ITEclient.lcp</td>
<td>2021-01-04 15:43:14</td>
<td>2d958f5f4d70b6756c774f85bb0f9eb77e</td>
</tr>
<tr>
<td>TNS-MalwareDetectionOnly_oss ITEclient.lcp</td>
<td>default_oss ITEclient.lcp</td>
<td>2021-01-04 15:43:14</td>
<td>2d958f5f4d70b6756c774f85bb0f9eb77e</td>
</tr>
<tr>
<td>TNS-MiSQLServer_windows_tenableclient.lcp</td>
<td>default_oss ITEclient.lcp</td>
<td>2021-01-04 15:43:14</td>
<td>2d958f5f4d70b6756c774f85bb0f9eb77e</td>
</tr>
<tr>
<td>TNS-MiSQLServer_windows_tenableclient.lcp</td>
<td>default_oss ITEclient.lcp</td>
<td>2021-01-04 15:43:14</td>
<td>2d958f5f4d70b6756c774f85bb0f9eb77e</td>
</tr>
<tr>
<td>TNS-MiSQLServer_windows_tenableclient.lcp</td>
<td>default_oss ITEclient.lcp</td>
<td>2021-01-04 15:43:14</td>
<td>2d958f5f4d70b6756c774f85bb0f9eb77e</td>
</tr>
<tr>
<td>TNS-MiSQLServer_windows_tenableclient.lcp</td>
<td>default_oss ITEclient.lcp</td>
<td>2021-01-04 15:43:14</td>
<td>2d958f5f4d70b6756c774f85bb0f9eb77e</td>
</tr>
<tr>
<td>TNS-MiSQLServer_windows_tenableclient.lcp</td>
<td>default_oss ITEclient.lcp</td>
<td>2021-01-04 15:43:14</td>
<td>2d958f5f4d70b6756c774f85bb0f9eb77e</td>
</tr>
<tr>
<td>TNS-MiSQLServer_windows_tenableclient.lcp</td>
<td>default_oss ITEclient.lcp</td>
<td>2021-01-04 15:43:14</td>
<td>2d958f5f4d70b6756c774f85bb0f9eb77e</td>
</tr>
<tr>
<td>TNS-MiSQLServer_windows_tenableclient.lcp</td>
<td>default_oss ITEclient.lcp</td>
<td>2021-01-04 15:43:14</td>
<td>2d958f5f4d70b6756c774f85bb0f9eb77e</td>
</tr>
<tr>
<td>TNS-MiSQLServer_windows_tenableclient.lcp</td>
<td>default_oss ITEclient.lcp</td>
<td>2021-01-04 15:43:14</td>
<td>2d958f5f4d70b6756c774f85bb0f9eb77e</td>
</tr>
<tr>
<td>TNS-MiSQLServer_windows_tenableclient.lcp</td>
<td>default_oss ITEclient.lcp</td>
<td>2021-01-04 15:43:14</td>
<td>2d958f5f4d70b6756c774f85bb0f9eb77e</td>
</tr>
<tr>
<td>TNS-MiSQLServer_windows_tenableclient.lcp</td>
<td>default_oss ITEclient.lcp</td>
<td>2021-01-04 15:43:14</td>
<td>2d958f5f4d70b6756c774f85bb0f9eb77e</td>
</tr>
<tr>
<td>TNS-MiSQLServer_windows_tenableclient.lcp</td>
<td>default_oss ITEclient.lcp</td>
<td>2021-01-04 15:43:14</td>
<td>2d958f5f4d70b6756c774f85bb0f9eb77e</td>
</tr>
<tr>
<td>TNS-MiSQLServer_windows_tenableclient.lcp</td>
<td>default_oss ITEclient.lcp</td>
<td>2021-01-04 15:43:14</td>
<td>2d958f5f4d70b6756c774f85bb0f9eb77e</td>
</tr>
</tbody>
</table>
Client Policy Builder

The Client Policy Builder is a tool for creating and editing policies directly in the LCE interface. The Builder can be used to create a policy for any supported combination of LCE client and operating system, and will not allow invalid combinations, preventing you from inadvertently creating an invalid policy. Additionally, if upgrading from a previous version of LCE, the Builder can be used to modify any existing policies and will alert you if an existing policy that you modify is invalid.

The Builder is divided into the title bar and the Basic and Advanced panes.

In the Basic pane:

You can add or remove configuration items and specify valid values for those items. All values that you enter for configuration items are validated. If an invalid value is entered, the Builder warns you and prevents the invalid policy from being saved. As you modify the configuration items in the Basic pane, the XML source code in the Advanced pane will be updated to reflect the new values. In the Basic pane, if a check box is empty, the value for that configuration item will be set to false in the Advanced pane.

In the Advanced pane:
You can modify the XML directly. As with the values in the Basic pane, all changes made to the XML are validated, including but not limited to values for the configuration items, element tags, and the file header. You are also alerted if you attempt to add configuration items that do not correspond to the policy type. When changes are made to values in the XML, the Basic pane is updated to reflect the new values.

**Note:** It is recommended that only advanced users utilize the Advanced pane.
Create a Client Policy with the Client Policy Builder

To create a client policy with the client policy builder:

1. Log in to LCE via the user interface.

2. In the top navigation bar, click Policies.

The Policies page appears, displaying the policy table.

3. In the upper-left corner of the policy table, click the Add policy button.

The Client Policy Builder window appears, displaying the Create section.

4. In the OS list, select the operating system of the host for which you want to create a policy.

The Client list is filtered automatically to display only LCE clients that are supported on the select operating system. For example, if you select Windows, the Client list will be limited to just Tenable Client, the only supported LCE client for Windows.

5. In the Client list, select the client for which you want to create a policy, and then click the Start Editing button.

The Client Policy Builder appears. At the top of the Builder, the title bar displays the name of the default policy corresponding to the operating system and LCE client that you selected. A complete list of configuration items that are valid for the type of policy appear in the Basic pane. XML source code with corresponding values appears in the Advanced pane.
6. Using the Basic or Advanced panes, modify values for each configuration item.

**Tip:** In the Basic pane, to modify a configuration item that uses a list of values (e.g., Included networks), click to add items and to remove items from the list. Additionally, to expand and collapse the lists, click and , respectively. If configuration items are visible in the Advanced pane but not in the Basic pane, it is likely that the parent configuration item is currently collapsed.

As you configure the policy, the Builder will validate the configuration items, and alert you if any invalid configuration is found.

7. Click the Save as button.

The Save file as dialog box appears.

8. In the Filename box, type a name for the policy. A valid file name cannot include the phrase default or TNS as a prefix, and cannot include spaces or underscores. Do not include a file extension. The operating system, client, and file extension will be appended to the name when the policy is saved.
For example, if you are saving a policy for the LCE Tenable Network Monitor that supports Red Hat Enterprise Linux, and you type `corpnet` as the name, the policy will be saved with the following complete name: `corpnet_rhel_networkmonitor.lcp`.

**Note:** The policy name can be a maximum of 50 characters.

9. Click **OK**.

   LCE saves your configuration.

   A notification appears, confirming that the policy was saved successfully. The **Save** button is enabled. You can continue to modify the policy and save those changes.

10. At the top of the Builder, in the title bar, click the **Quit** button.

    The **Policies** page appears, displaying a list of default and existing policies.
Edit a Client Policy with the Client Policy Builder

To edit a client policy with the client policy builder:

1. Log in to LCE via the user interface.

2. In the top navigation bar, click **Policies**.

   The **Policies** page appears, displaying the policy table.

3. In the row corresponding to the policy you want to edit, in the **Actions** column, click the **Edit** button.

   The Client Policy Builder appears. At the top of the Builder, the title bar displays the name of the policy that you selected. A complete list of configuration items that are valid for the type of policy appear in the **Basic** pane. XML source code with corresponding values appears in the **Advanced** pane.

   **Caution:** If comments are present in an existing policy, those comments will be removed. Comments will not be saved with the policy.

4. Using the **Basic** or **Advanced** panes, modify values for each configuration item.

   **Tip:** In the **Basic** pane, to modify a configuration item that uses a list of values (e.g., `[ Included networks ]`), click `[ ]` to add items and `[-]` to remove items from the list. Additionally, to expand and collapse the lists, click `[ ]` and `[-]`, respectively. If configuration items are visible in the **Advanced** pane, but not in the **Basic** pane, it is likely that the parent configuration item is currently collapsed.
As you configure the policy, the Builder will validate the configuration items, and alert you if any invalid configuration is found.

5. If you want to keep the existing file name, click the **Save** button, and then proceed to step 7 of this procedure. Otherwise, click the **Save as** button.

   The **Save file as** dialog box appears.

6. In the **Filename** box, type a name for the policy. Do not include a file extension. The operating system, client, and file extension will be appended to the name when the policy is saved.

   For example, if you are saving a policy for the LCE Tenable Network Monitor that supports Red Hat Enterprise Linux, and you type `corpnet` as the name, the policy will be saved with the following complete name: `corpnet_rhel_networkmonitor.lcp`.

7. Click **OK**.

   LCE saves your configuration.

   A notification appears, confirming that the policy was saved successfully.

8. At the top of the Builder, in the title bar, click the **Quit** button.

   The **Policies** page appears, displaying a list of default and existing policies. To confirm that the policy you modified was saved, in the upper-right corner of the list of policies, in the **Search** box, type the name of the policy you created, and then check the value in the **Last modified on** column.
Upload a Client Policy

It is recommended that you create and modify policies using the Client Policy Builder, but if desired, you can still download a policy in order to modify it and then upload the modified policy back into the LCE server.

To upload a client policy or upload a modified client policy:

1. Log in to LCE via the user interface.
2. In the top navigation bar, click Policies.
   The Policies page appears, displaying the policy table.

3. In the upper-left corner of the policy table, click the Add policy button.
   The Client Policy Builder window appears, displaying the Create section.
4. Click the **Upload** tab.

The **Upload** section appears.

5. In the **OS** list, select the operating system corresponding to the client policy you want to upload.

6. In the **Client** list, select the type of LCE client corresponding to the client policy you want to upload.

**Note:** The selected OS and Client must match the policy you want to upload, or the upload will fail and an error message will appear.
7. In the **Policy Name** box, type a name for the policy. A valid policy name cannot include the phrase *default* or *TNS* as a prefix, and cannot include spaces or underscores. Do not include a file extension. The operating system, client, and file extension will be appended to the name when the policy is saved.

For example, if you are uploading a policy for the LCE Tenable Network Monitor that supports Red Hat Enterprise Linux, and you type *corpnet* as the name, the policy will be uploaded with the following complete name: *corpnet_rhel_networkmonitor.lcp*.

8. If you want to overwrite an existing policy that has the same name, select the **Overwrite** check box.

9. Click the **Add Policy** button.

   The policy is uploaded and appears in the policy table.
Download a Client Policy

It is recommended that you create and modify policies using the Client Policy Builder, but if desired, you can still download a policy in order to modify it or transfer it to another LCE server.

To download a client policy:

1. Log in to LCE via the user interface.
2. In the top navigation bar, click Policies.
   
   The Policies page appears, displaying the policy table.

3. In the policy table, in the row corresponding to the policy that you want to download, click the Download button.
   
   The policy is downloaded. If desired, you can make changes, and then upload the policy.
Clone a Client Policy with the Client Policy Builder

To clone a client policy with the client policy builder:

1. Log in to LCE via the user interface.

2. In the top navigation bar, click Policies.

   The Policies page appears, displaying the policy table.

3. In the row corresponding to the policy you want to clone, in the Actions column, click the Clone button.

   -or-

   a. In the upper-left corner of the policy table, click the Add policy button.

      The Client Policy Builder window appears, displaying the Create section.
b. Click the **Clone** tab.

The **Clone** section appears.

c. In the **Policy** list, select the policy that you want to clone, and then click the **Start Editing** button.

The Client Policy Builder appears. At the top of the Builder, the title bar displays the name of the policy that you selected. A complete list of configuration items that are valid for the type of policy appear in the **Basic** pane. XML source code with corresponding values appears in the **Advanced** pane.

4. Using the **Basic** or **Advanced** panes, modify values for each configuration item.

Tip: In the **Basic** pane, to modify a configuration item that uses a list of values (e.g., included networks), click to add items and to remove items from the list. Additionally, to expand and collapse the lists, click and , respectively. If configuration items are visible in the
As you configure the policy, the Builder will validate the configuration items and alert you if any invalid configuration is found.

5. Click the **Save as** button.

The **Save file as** dialog box appears.

6. In the **Filename** box, type a name for the policy. Do not include a file extension. The operating system, client, and file extension will be appended to the name when the policy is saved.

For example, if you are saving a policy for the LCE Tenable Network Monitor that supports Red Hat Enterprise Linux, and you type *corpnet* as the name, the policy will be saved with the following complete name: *corpnet_rhel_networkmonitor.lcp*.

7. Click **OK**.

LCE saves your configuration.

A notification appears, confirming that the policy was saved successfully. The **Save** button is enabled. You can continue to modify the policy and save those changes.

8. At the top of the Builder, in the title bar, click the **Quit** button.

The **Policies** page appears, displaying a list of default and existing policies.
Other Policies Page Tasks

This section details common tasks that are performed using the Policies page.

This section includes:

- Search the Policy Table
- Limit the Policy Table Entries Shown
- Show and Hide Policy Table Columns

Search the Policy Table

- Above the policy table, in the Search box, type a plain text search term. The Search box does not accept Boolean operators.

As you type, the policy table is filtered by your search term. The text in all columns of the policy table is searched, regardless of whether they are shown or hidden.

Tip: If you are using the desktop version of Safari, you may need to disable the Correct Spelling Automatically function to prevent the browser from rewriting search terms.

Limit the Policy Table Entries Shown

- Above the policy table, in the upper-right corner, in the Show box, select the number of entries you want to show per policy table page. By default, the Show box is set to 10.

Show and Hide Policy Table Columns

1. Above the policy table, in the upper-right corner, click the Show / hide columns button.

   A list of columns appears.

   By default, all columns are visible.

2. In the list of columns, select or clear the check boxes corresponding to the columns that you want to show or hide, respectively.

   As you select and clear check boxes, the policy table is updated with the appropriate columns.
Delete a Client Policy

You cannot delete policies that are currently being used by clients, or pre-packaged policies (i.e., *default* and *TNS* policies). Policies are deleted permanently and cannot be recovered.

To delete a client policy:

1. Log in to LCE via the user interface.
2. In the top navigation bar, click **Policies**.
   
   The **Policies** page appears, displaying the policy table.
3. In the policy table, in the row corresponding to the policy that you want to delete, click the **Delete** button.
   
   The **Confirm deletion** dialog box appears.
4. Click **OK**.
   
   The policy is deleted.
Automatically Authorize LCE Clients

In order for an LCE client to communicate with an LCE server, it must first be authorized. Client assignment rules can be used to automatically authorize clients.

To auto authorize an LCE to communicate with an LCE server:

1. Log in to LCE via the user interface.
2. In the top navigation bar, click Configuration.
   The System Configuration page appears, displaying basic configuration settings.
3. In the left side navigation bar, click Advanced.
   The Advanced configuration section appears, displaying options used to fine tune your LCE server configuration.
4. Scroll down to the Clients section, and check the Auto Authorize checkbox.
5. Enter a network range in the Client Network field using CIDR notation.
6. In the LCE IP:port field, enter the LCE server IP address and port that you want the clients to communicate with.
7. Click the Add New Client Rule button.
   The policies text box appears.
8. In the text box, specify the filenames of the policies that you want applied to clients that fall in the range defined by the rule.

   **Note:** Policies are matched by operating system. If there are multiple policies for a particular operating system, the first applicable policy that is specified for that operating system will be assigned. If none of the specified policies are applicable to a client in the network, the default policy for that operating system will be used.

9. Scroll to the bottom of the page and click the Update button.

LCE saves your configuration.

**Tip:** Install the LCE client on your target hosts if you haven't already.
LCE Clients

A key component of LCE, the LCE clients capture event data from a variety of sources and send that data to the LCE server for normalization. The LCE clients are installed on systems whose logs, network traffic, performance and other types of protocols and technologies are to be monitored by forwarding the data securely to the LCE server. Policies are assigned to the LCE clients, which govern the methods by which a client captures event data. For example, the Web Query Client is used to collect events from Salesforce, AWS CloudTrail, and Google Cloud Platform.

The following table lists the LCE clients that Tenable Network Security provides, and the operating systems supported by those clients. This table only lists clients that are compatible with the latest version of LCE.

<table>
<thead>
<tr>
<th>Client</th>
<th>Operating Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>LCE Client for Windows and Linux</td>
<td>RHEL/CentOS</td>
</tr>
<tr>
<td></td>
<td>Tenable Appliance</td>
</tr>
<tr>
<td></td>
<td>FreeBSD</td>
</tr>
<tr>
<td></td>
<td>Debian</td>
</tr>
<tr>
<td></td>
<td>OS X</td>
</tr>
<tr>
<td></td>
<td>AIX</td>
</tr>
<tr>
<td></td>
<td>Solaris</td>
</tr>
<tr>
<td></td>
<td>HP-UX</td>
</tr>
<tr>
<td></td>
<td>Dragon</td>
</tr>
<tr>
<td></td>
<td>Fedora</td>
</tr>
<tr>
<td></td>
<td>Ubuntu</td>
</tr>
<tr>
<td></td>
<td>SuSE</td>
</tr>
<tr>
<td></td>
<td>Windows</td>
</tr>
</tbody>
</table>
## LCE Clients and Operating Systems

<table>
<thead>
<tr>
<th>Client</th>
<th>Operating Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPSEC Client</td>
<td>RHEL/CentOS</td>
</tr>
<tr>
<td>Splunk Client</td>
<td>RHEL/CentOS</td>
</tr>
<tr>
<td>Tenable NetFlow Monitor</td>
<td>RHEL/CentOS</td>
</tr>
<tr>
<td>Tenable Network Monitor</td>
<td>RHEL/CentOS</td>
</tr>
<tr>
<td>Tenable RDEP Monitor</td>
<td>RHEL/CentOS</td>
</tr>
<tr>
<td>Tenable SDEE Monitor</td>
<td>RHEL/CentOS</td>
</tr>
<tr>
<td>Web Query Client</td>
<td>RHEL/CentOS</td>
</tr>
<tr>
<td>WMI Monitor Client</td>
<td>RHEL/CentOS</td>
</tr>
</tbody>
</table>

The LCE clients can be configured to gather information and events from the following sources:

- Windows Event Logs (collected locally or remotely via WMI)
- Windows/Linux/Unix system and application logs
- Check Point OPSEC events
- Cisco RDEP events
- Cisco SDEE events
- Cisco NetFlow
- Splunk
- Sniffed TCP and UDP network traffic (Tenable Network Monitor)
- Sniffed syslog messages in motion
- File monitoring (Linux, Unix, and Windows)
All data transmitted from LCE clients to the LCE server is encrypted using AES-256-CFB.
LCE Client for Windows

The LCE Windows Client monitors events, as well as specific log files or directories, for new event data. Tenable provides 32-bit and 64-bit versions of the LCE Windows Client for Windows Server 2008/2012 R2/2016 and Windows 7/8/10.
**System Requirements**

**Operating System**

The Windows Client is compatible with the following operating systems:


**Additional Software**

The 5.x Windows Client requires the following software:

- [Microsoft Visual C++ 2015 Redistributable Package, Update 2](#)

**Licensing**

Tenable.sc must be licensed for the LCE Windows Client. For more information, see [Licenses](#) in the Tenable.sc User Guide.
Install, Configure, and Remove

This section includes the following instructions for installing, configuring, and removing the LCE Windows Client.

- [Download the LCE Windows Client](#)
- [Install the LCE Windows Client](#)
- [Install the LCE Windows Client Remotely](#)
- [Configure the LCE Windows Client](#)
- [Remove the LCE Windows Client](#)
Download an LCE Client

For more information, see LCE Clients.

To download an LCE Client:

1. Access the Tenable Downloads page.
   
   The Tenable Downloads page appears.

2. Click Log Correlation Engine.

3. Select the Log Correlation Engine Client you want to download.
   
   The License Agreement page appears.

4. Review the Software License Agreement. If you agree to the terms, click the I Agree button.
   
   The client package is downloaded.
Install the LCE Windows Client

In addition to installing the LCE Windows Client locally, you can also install the LCE Windows Client on remote hosts.

Before You Begin

Download the LCE Windows Client.

To install LCE Windows Client on remote hosts:

1. If you are installing the LCE Windows Client on a host where User Account Control is enabled, right-click the LCE Windows Client .msi file and select Run As Administrator. Otherwise, double-click the LCE Windows Client .msi file.

   The LCE Windows Client requires the Microsoft Visual C++ 2015 Redistributable Package. If the package is not installed, an error will appear that instructs you to download and install the package.

   The InstallShield Wizard appears.

2. Complete the installation using the InstallShield Wizard.

   The LCE Client is installed.
Install the LCE Windows Client Remotely

The installation of the LCE Windows Client can be accomplished from a command line or script via the execution of msiexec.exe. This makes it possible to perform remote installations of LCE Windows Clients for multiple hosts.

To facilitate this process, the option exists to set the client’s initial configuration settings at the time of the installation from the same command.

The following table contains a list of PUBLIC properties for the Tenable LCE Windows Client MSI install package. Because all parameters (except LCE server IP address and port) are set using policies on the server, there are only the two options available.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERVERIP</td>
<td>The IP address or hostname of the LCE server. The maximum length of the hostname is 46 characters. If not specified, the value is set to 192.0.2.91.</td>
</tr>
<tr>
<td>SERVERPORT</td>
<td>The port used to communicate with the LCE server. The default port is 31300.</td>
</tr>
</tbody>
</table>

Caution: Versions of the LCE Windows Client earlier than 4.4 also provided the SERVERNAME property. That property is deprecated and should not be used.

Before you begin:

- Download an LCE Client

To install the LCE Windows Client remotely:

1. Using a script or via the command line, execute the following: "<Package File>"
   SERVERIP="<Server IP or Hostname>" SERVERPORT=<Port Number>

   - <Package File> corresponds to the directory location and name of the .msi file. For example, C:\Users\Administrator\Downloads\<LCE Client Installer>.msi, where <LCE Client Installer> is the file name of the .msi file.
- **<Server IP or Hostname>** corresponds to the IP address or hostname of the LCE server that you want the LCE Windows Client to communicate with. The hostname can be a maximum length of 46 characters.

- **<Port Number>** corresponds to the port used to communicate with the LCE server. Specify an integer between 1 and 65535. The default port is 31300.

If a log file of the installation is desired, /I can be used, followed by the path to the log file. For example: /I C:\Users\Administrator\Documents\lce_client_install.txt /passive /i "C:\Users\Administrators\Downloads\<LCE Client Installer>"
SERVERIP="127.0.0.2" SERVERPORT=31300, where **<LCE Client Installer>** is the file name of the .msi file.

If you want the log file to include all installation information including debug information, instead of /I, specify /lvx*. For example: /lvx* "install_log.txt" /passive /i "C:\Users\Administrators\Downloads\<LCE Client Installer>"
SERVERIP="127.0.0.2" SERVERPORT=31300, where **<LCE Client Installer>** is the file name of the file.
Configure the LCE Windows Client

If you did not configure the LCE Windows Client during installation, or if you want to modify the configuration, you can configure the client using the command line.

To configure the LCE Windows Client:

1. Via the command line, go to the directory where you installed the LCE Windows Client, then execute the following command:

   `server_assignment --server-ip "<Server IP or Hostname>" --server-port <Server Port>

   - `<Server IP or Hostname>` corresponds to the IP address or hostname of the LCE server that you want the LCE Windows Client to communicate with. The hostname can be a maximum length of 46 characters.
   - `<Port Number>` corresponds to the port used to communicate with the LCE server. The default port is 31300.

   **Note:** The default installation location is C:\Program Files\Tenable\LCEClient.

2. Type `net stop "Tenable LCE Client"

   The LCE Client service stops.

3. Type `net start "Tenable LCE Client"

   The LCE Client service starts. The LCE Windows Client is configured.

   **Note:** After the client is configured and authorized by the LCE server, a hidden file named .lcufh is created in C:\ProgramData\Tenable\LCE Client. This file contains a cache of process hashes and is used to store hashes that should only be reported once.
# Windows Client Policy Configuration Items

The following table lists the configuration items that are valid for the LCE Windows Client policy, and provides a brief description of each item. These configuration items appear in the Client Policy Builder when you create or modify a policy for the LCE Windows Client.

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Description</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>event-log</td>
<td>The name of a Windows event log to monitor. Each event that appears in event logs monitored by the LCE Windows Client are sent to the LCE server individually. You can specify one or more event logs to monitor. XML Examples:</td>
<td>The name of the Windows event log (for example, Application) that you want to monitor, or the value all. If you specify all, in addition to Windows logs, events from Applications and Services logs will also be monitored.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Events to ignore</td>
<td>A provider name that you want the LCE Windows Client to ignore. Additionally, if you do not want to ignore all events from a log provider, you can add specific event IDs for that provider. XML Example:</td>
<td>The provider name must be a valid log provider. The event ID must be an integer. It cannot include any letters or symbols.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Tip:** To locate event providers that you want to include in your policy, use the Windows Event Viewer.
<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Description</th>
<th>Valid Values</th>
</tr>
</thead>
</table>
| Monitor text files | The full path and file name of a text file to monitor. Each new line is sent to LCE as a new log. If you want to monitor multiple text files in the same folder, you can specify the following parameters to refine which text files are monitored by the client:  
  - **Location:** The full path that contains text files you want to monitor. Each new line in each file is sent to LCE as a new log.  
  - **Include:** Files in the folder specified for Location will only be monitored if they match the Include pattern. Wildcards are allowed.  
  - **Exclude:** Files in the folder specified for Location will NOT be monitored if they match the Exclude pattern. | Any fully qualified path and file name, including the file extension. It is best practice to escape folder separators with a backslash. For example, `C:\Windows`. |
<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Description</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>pattern. Wildcards are allowed.</td>
<td>Maximum file size: Files in the folder specified for Location will be deleted once they reach the size specified in this key (in bytes). Optional letters can be post-fixed to change the multiplier (K for kilobytes, M for megabytes, or G for gigabytes). This option was added specifically for Exchange log files, which can grow unbounded.</td>
<td>Optional letters can be post-fixed to change the multiplier (K for kilobytes, M for megabytes, or G for gigabytes). This option was added specifically for Exchange log files, which can grow unbounded.</td>
</tr>
<tr>
<td>Caution: If you specify a maximum file size, the LCE Windows Client will attempt to delete files in the folder specified for Location when they go above the maximum file size. Do not use this option if you want to retain the files.</td>
<td>XML Examples:</td>
<td>Any absolute path and file name, including the file extension. It is best</td>
</tr>
<tr>
<td>Monitor binary files</td>
<td>The full path and file name of a non-text file to monitor. If the file changes, the old and new SHA256 checksums are sent as an event to the LCE server. The maximum number of files that can be specified is 63. If multiple files in the same folder are being monitored, Any absolute path and file name, including the file extension. It is best</td>
<td></td>
</tr>
</tbody>
</table>

XML Examples:

```
<flat-file>C:\Windows\WindowsUpdate.log</flat-file>
```

```
<flat-file>
    <location>C:\Windows\</location>
    <include>*.log</include>
    <exclude>iis7.log</exclude>
    <delete-on-size-bytes>4096K</delete-on-size-bytes>
</flat-file>
```
you should monitor the folder itself. If you want to monitor multiple files in the same folder, you can specify optional parameters to refine which files are monitored by the client:

- **Location**: The full path that contains files you want to monitor.
- **Include**: Files in the folder specified for Location will only be monitored if they match the Include pattern. Wildcards are allowed.
- **Exclude**: Files in the folder specified for Location will NOT be monitored if they match the Exclude pattern. Wildcards are allowed.

If you want to include or exclude directories in the same folder, you can specify optional parameters to refine which files are monitored by the client:

- **Include-dir**: Included directory path for monitoring files. Wildcards are allowed.
- **Exclude-dir**: Excluded directory path for monitoring files. Wildcards are allowed.

XML Example:

```xml
<monitor-file>C:\Windows\notepad.exe</monitor-file>
<monitor-file>
  <location>C:\Windows\</location>
  <include>*.exe</include>
  <exclude>explorer.exe</exclude>
  <include-dir>C:\Windows\System32</include-dir>
</monitor-file>
```
<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Description</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&lt;exclude-dir&gt;C:\Windows\debug&lt;/exclude-dir&gt; &lt;/monitor-file&gt;</td>
<td></td>
</tr>
<tr>
<td>monitor-sub-directories</td>
<td>Whether to monitor files in subdirectories of the folder specified for Location for Monitor binary files, if those files match the specified pattern. If set to 1, monitoring an extensive folder structure (such as C:\Windows) with no include or exclude filters may impact performance. XML Example:</td>
<td>0 (off) or 1 (on)</td>
</tr>
<tr>
<td>Monitor wait seconds</td>
<td>The number of seconds to wait before monitoring files. The default is 5 seconds. XML Example:</td>
<td>An integer greater than 0.</td>
</tr>
<tr>
<td>Tail sub-directories</td>
<td>Whether to monitor files in subdirectories of the folder specified for Location for Monitor text files, if those files match the specified pattern. If set to 1, monitoring an extensive folder structure (such as C:\Windows) with no include or exclude filters may impact performance. XML Example:</td>
<td>0 (off) or 1 (on)</td>
</tr>
<tr>
<td>Configuration Item</td>
<td>Description</td>
<td>Valid Values</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Seconds between scans of logs and text files</td>
<td>The number of seconds between scanning logs monitored by the LCE Windows Client. XML Example: <code>&lt;interval-log-seconds&gt;30&lt;/interval-log-seconds&gt;</code></td>
<td>An integer greater than 0.</td>
</tr>
<tr>
<td>monitor-wait-seconds</td>
<td><strong>Caution:</strong> This option is not available for the LCE Windows Client versions 4.4 and later.</td>
<td>No valid values</td>
</tr>
<tr>
<td>Send new events only</td>
<td>Whether to only send new events. If set to 0, all data in all monitored logs will be sent to the LCE server every time the client is restarted or when the policy changes. XML Example: <code>&lt;send-new-events-only&gt;1&lt;/send-new-events-only&gt;</code></td>
<td>0 (off) or 1 (on)</td>
</tr>
<tr>
<td>Monitor config</td>
<td><strong>Caution:</strong> This option is not available for the LCE Windows Client versions 4.4 and later.</td>
<td>No valid values</td>
</tr>
<tr>
<td>Report unknown processes</td>
<td>If enabled, the LCE Windows Client will send an LCE_Client_Detected_Uknown_Process event for each unknown process on the monitored host. This event is sent once for each unknown process detected. XML Example: <code>&lt;report-unknown-processes&gt;2&lt;/report-unknown-processes&gt;</code></td>
<td>0 (off), 1, or 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1: A list of LCE_Client_Detected_Uknown_Process events will be sent</td>
</tr>
<tr>
<td>Configuration Item</td>
<td>Description</td>
<td>Valid Values</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>

only once, and subsequently only newly-encountered unknown DLLs and EXEs will be reported.

- 2: The list of reported unknown processes will be cleared every time the client is restarted or a new policy is received. All existing unknown DLLs and EXEs will


<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Description</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote host to monitor</td>
<td>Using the following parameters, specifies a remote host to monitor:</td>
<td>All parameters require values.</td>
</tr>
<tr>
<td></td>
<td>• IP address: The IP address of the host that you want to monitor.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Namespace: The namespace of the WMI classes being monitored, usually <code>root\cimv2</code>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Domain: The domain of the remote host to monitor.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Username: The user name of the account on the remote machine that should be used for monitoring.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Password: The corresponding password for the specified user name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• File paths to monitor: One or more fully qualified paths with file name and extension that you want to monitor on the remote host.</td>
<td></td>
</tr>
</tbody>
</table>

**XML Example:**

```
<Host>
  <ip>192.0.2.10</ip>
  <namespace>root\cimv2</namespace>
  <domain>?</domain>
  <username>corpnetAdmin</username>
  <password>argus$12</password>
</Host>
```
<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Description</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;logfilename&gt;C:\Windows\WindowsUpdate.log&lt;/logfilename&gt; &lt;/Host&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Info</td>
<td>Enable or disable info-level logging in lce_client.log (the LCE client debugging log).</td>
<td>0 (off) or 1 (on)</td>
</tr>
<tr>
<td></td>
<td>XML Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;info&gt;0&lt;/info&gt;</td>
</tr>
<tr>
<td>Verbose</td>
<td>Enable or disable verbose logging in lce_client.log (the LCE client debugging log).</td>
<td>0 (off), 1, or 2</td>
</tr>
<tr>
<td></td>
<td>XML Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;verbose&gt;0&lt;/verbose&gt;</td>
</tr>
<tr>
<td>Debug</td>
<td>Whether to enable debugging messages in lce_client.log (the LCE Windows Client log). If &lt;debug&gt;1&lt;/debug&gt; is present in the policy, debugging messages are enabled. It is recommended you only enable debugging if directed to do so by Tenable Network Security.</td>
<td>0 (off) or 1 (on)</td>
</tr>
<tr>
<td></td>
<td>XML Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;debug&gt;0&lt;/debug&gt;</td>
</tr>
<tr>
<td>Client heartbeat frequency</td>
<td>The number of seconds between each client heartbeat message to the LCE server. If set to 0, the client will not send heartbeats.</td>
<td>An integer</td>
</tr>
<tr>
<td>Configuration Item</td>
<td>Description</td>
<td>Valid Values</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>XML Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;heartbeat-frequency&gt;600&lt;/heartbeat-frequency&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client statistics frequency</td>
<td>The number of minutes between each client host performance statistics report (CPU, Disk Space, and Physical Memory) to the LCE server. If set to 0, client statistics will not be sent.</td>
<td>An integer</td>
</tr>
<tr>
<td>XML Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;statistics-frequency&gt;60&lt;/statistics-frequency&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compress events</td>
<td>Whether client will compress log data prior to sending it to the LCE server in order to save bandwidth. Recommended except when debugging. If set to 0, events will not be compressed.</td>
<td>0 (off) or 1 (on)</td>
</tr>
<tr>
<td>XML Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;compress-events&gt;1&lt;/compress-events&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compression level</td>
<td>Compression level to use when compressing events for transmission across network using zlib, set on a scale from 1 to 9. 1 provides the least amount of compression, resulting in minimum CPU usage and minimum bandwidth savings; 9 maximizes compression, resulting in increased CPU usage and maximum bandwidth savings. Ignored unless compression is enabled.</td>
<td>An integer from 1 to 9.</td>
</tr>
<tr>
<td>XML Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;compression-level&gt;5&lt;/compression-level&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration Item</td>
<td>Description</td>
<td>Valid Values</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Minimum compression ratio</td>
<td>Defines the minimum acceptable savings ratio for event data being transmitted across the network, in terms of (bytes total) / (bytes compressed). If the client determines a savings ratio of less than this value, then event data will not be compressed before sending. This reduces the effort on the LCE Server decompressing event data when compression benefits are minimal. Ignored unless compression is enabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>XML Example:</td>
<td>A decimal number.</td>
</tr>
<tr>
<td>Minimum compression input size</td>
<td>The minimum number of bytes a packet must have to be compressed. Ignored unless compression is enabled.</td>
<td>An integer greater than 0.</td>
</tr>
<tr>
<td>Event queue timeout</td>
<td>Maximum number of seconds between event messages the client sends to the LCE server.</td>
<td>An integer greater than 0.</td>
</tr>
<tr>
<td>Malware scan period</td>
<td>This option specifies the interval (in seconds) that the LCE Windows Client will scan running processes, and monitored directories.</td>
<td>An integer greater than 0.</td>
</tr>
<tr>
<td>Configuration Item</td>
<td>Description</td>
<td>Valid Values</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Whitelist hashes</td>
<td>MD5 file hashes that will be ignored by LCE Windows Client that may otherwise be considered malware.</td>
<td>An MD5 hash.</td>
</tr>
<tr>
<td></td>
<td>XML Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>&lt;whitelist-hashes&gt;</code>8d1ae0900d461fd593b4daf67ee72e00<code>/whitelist-hashes&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Custom malware hashes</td>
<td>MD5 file hashes that will be identified as malware by the LCE Windows Client if detected.</td>
<td>An MD5 hash.</td>
</tr>
<tr>
<td></td>
<td>XML Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>&lt;custom-malware-hashes&gt;</code>e1112134b6dccc8bed54e0e34d8ac272795e73d74-<code>/custom-malware-hashes&gt;</code></td>
<td></td>
</tr>
</tbody>
</table>
Remove the LCE Windows Client

The LCE Windows Client can be removed in three ways:

- **Using the original .msi file**
- **Using the command line**
- Using the Control Panel for your version of Windows

**Note:** This method will vary based on your operating system. If you are unsure how to remove a program using the Control Panel, consult the documentation for your operating system.

To remove The LCE Windows Client using the LCE Windows Client .msi File

1. If you are removing the LCE Windows Client from a host where User Account Control is enabled, right-click the LCE Windows Client .msi file and select **Run As Administrator**. Otherwise, double-click the LCE Windows Client .msi file.

   The InstallShield Wizard appears.

   On the **Program Maintenance** screen, you are prompted to **Modify**, **Repair**, or **Remove** the installation.

2. Select **Remove**, and then click the **Next** button.

   The **Remove the Program** screen appears. You are prompted to remove all files in program data folders. By default, the **Remove all files in program data folders** check box is selected.

3. If you do not want to remove local files that were created by the LCE Windows Client, clear the **Remove all files in program data folders** check box.

4. Click the **Next** button.

   The **Files in Use** screen appears. The Tenable LCE Client service must be stopped in order for the removal to complete successfully. By default, the Tenable LCE Client service will be stopped.

5. If you do not want to stop the Tenable LCE Client service, select **Do not close applications**. Your computer will need to be restarted before the removal process is completed.

6. Click **OK**, and then complete the InstallShield Wizard.
The LCE Windows Client is removed.

To remove the LCE Windows Client using the CLI

1. Via the command line, execute the following: `/uninstall "<Package File>"

   - `<Package File>` corresponds to the directory location and name of the .msi file. For example, `C:\Users\Administrator\Downloads\lce_client-4.4.0-windows_2008_x64.msi`. The exact package name will vary.
LCE Windows Client Features

The LCE Windows Client is used to monitor events from many different channels on supported Windows platforms, including logs created by applications, and any Windows event logs. Additionally, the client can be configured to monitor text and binary files on a host, report on MD5 hash changes, monitor unknown processes, and scan for malware. Remote hosts can also be monitored.

Event and Text File Monitoring

Whenever a new event appears in a monitored Windows event log, the event is transmitted to the LCE server for normalization. In the case of monitored text files, each new line is transmitted. After the LCE server normalizes the event data, the data can be visualized using Tenable.sc. The LCE Windows Client can process files of all common encoding types, including UTF-8 and UTF-16.

Binary File and Unknown Process Monitoring

When a binary or executable file is monitored, if the MD5 checksum of the file changes, the old and new MD5 hashes are transmitted to the LCE server as an event. When unknown processes are monitored, you can configure the LCE Windows Client to report all unknown processes that are detected every time the client is restarted, or to report only newly-identified unknown processes.

Malware Scan

When the LCE Windows Client is configured to scan for malware, it will check the MD5 checksums of all running processes, as well as any binary file that the LCE Windows Client is monitoring, and compare the checksums to the Tenable database of known malware. Any processes or files that are identified as malware will be reported to the LCE server as events. When malware scanning is enabled, the LCE Windows Client will use DNS queries to compare the MD5 checksums.
Configure the Windows Client Policy

Using the [Client Policy Builder](#), you can create and modify policies for your LCE Windows Client. The following steps are performed via the web interface on the LCE server that you configured your LCE Windows Client to communicate with.

To configure the Windows Client Policy:

1. **Using the Client Policy Builder**, create a policy for your LCE Windows Client. This documentation includes a list of [valid configuration items for the client policy](#).

2. **Assign the policy to the LCE Windows Client.**
The documentation for the most recent version of the LCE Client for Linux is currently available starting on page 18 of the following document: http://static.tenable.com/prod_docs/LCE_4.2_clients.pdf
OPSEC Client

The documentation for the OPSEC Client is currently available here: https://docs.tenable.com/other/lce/LCE_4.5.0_OPSEC_Client_Guide.pdf
Get Started with the LCE Splunk Client

LCE unifies vulnerability collection and event analysis data through Tenable.sc, which provides easy-to-use dashboards to display multiple data points in a centralized view. Organizations that choose to send Splunk logs to the LCE have a unique advantage in that Splunk data is normalized by LCE and can be included for automatic anomaly detection, discovering assets, and additional vulnerability information including botnet and malware detection.

The LCE Splunk Client forwards data that Splunk collects to the LCE server. Once the data reaches the LCE server, the data is reviewed and normalized so it can be queried in Tenable.sc. The scope of this client can vary depending on what data is being forwarded from Splunk to the LCE Splunk Client.

Caution: The LCE Splunk Client can process a maximum of 500 logs per second. Processing more than 500 logs per second can result in a loss of data. This is an absolute limit and cannot be increased by improving the system hardware.
Install, Configure, and Remove

This section includes the following instructions for installing, configuring, and removing the LCE Splunk Client. With the exception of downloading the Splunk Client, the following procedures must be performed on the command line.

- Download the LCE Splunk Client
- Install the LCE Splunk Client
- Configure the LCE Splunk Client
- Remove the LCE Splunk Client
## Install the LCE Splunk Client

To install the LCE Splunk Client:

**Note:** All shell commands need to be executed by a user with root privileges.

1. Copy the downloaded client package to the host where it will be installed. The LCE Splunk Client can be installed directly on a Splunk server.

2. Verify the MD5 checksum of the client package against the MD5 checksum found in the release notes.

   Example:

   ```
   # md5sum lce_splunk-4.6.0-el6.x86_64.rpm
   da9f07886a693fb69c6a1dbd5c3eba31  lce_splunk-4.6.0-el6.x86_64.rpm
   ```

3. To initiate the installation, type the following command:

   ```
   rpm -ivh <package name>, where <package name> is the name of the client package.
   ```

   Example:

   ```
   # rpm -ivh lce_splunk-4.6.0-el6.x86_64.rpm
   Preparing...  ##################################################################### [100%]
   1:lce_splunk  ##################################################################### [100%]
   Checking for existence of TAG file at /etc/tenable_tag ...  
   Writing TAG to /etc/tenable_tag ...
   ```
Configure the LCE Splunk Client

**Note:** All shell commands need to be executed by a user with root privileges.

To configure the Splunk Client, you can execute the `set-server-ip.sh` script and include the LCE Server IP address and port number as arguments, or execute the script and, when prompted, enter the IP address and port number individually.

Finally, you will need to authorize the LCE Splunk Client.

To execute the script using arguments:

1. Type `/opt/lce_splunk/set-server-ip.sh <IP> <Port>`, where `<IP>` is the IP address of an LCE Server and `<Port>` is the port number assigned to the server. By default, the port number is 31300.

   The LCE Server IP address and port number are updated, and the LCE Splunk Client daemon is restarted.

   Example:

   ```
   # /opt/lce_splunk/set-server-ip.sh 192.168.22.11 31300
   Updating LCE Server IP from 192.0.2.66 to 192.0.2...
   Updating LCE Server Port from 31300 to 31300...
   Done
   Stopping LCE Splunk Client daemon [ OK ]
   Starting LCE Splunk Client daemon [ OK ]
   ```

To execute the script without arguments:

1. Type `/opt/lce_splunk/set-server-ip.sh`

   You are prompted to enter the LCE Server IP address or hostname.

2. Type the IP address or hostname of an LCE server.

   You are prompted to enter the LCE server port.

3. Type the port number assigned to the server for LCE client communication. By default, the port number is 31300.
The LCE Server IP address and port number are updated, and the LCE Splunk Client daemon is restarted.

Example:

```
# /opt/lce_splunk/set-server-ip.sh

Enter the new desired LCE server IP or hostname.
>>
192.168.22.11

Enter the new desired LCE server port [31300].
>>
31300

Updating LCE Server IP from 203.0.113.1 to 192.168.22.11...
Updating LCE Server Port from 31300 to 31300...
Done
Stopping LCE Splunk Client daemon [ OK ]
Starting LCE Splunk Client daemon [ OK ]
```
Remove the LCE Splunk Client

Note: All shell commands need to be executed by a user with root privileges.

To remove the LCE Splunk Client:

1. To query the rpm database to obtain the name of the currently installed package, type `rpm -qa |grep lce_`.
   
   Example:
   
   ```
   # rpm -qa |grep lce_
   lceSplunk-4.6.0-el6.x86_64.rpm
   ```

2. Type `rpm -e lce_splunk`.

   The Splunk Client package is removed.

   Example:
   
   ```
   # rpm -e lce_splunk
   warning: /opt/lce_splunk/server_assignment.xml saved as /opt/lce_splunk/server_assignment.xml.rpmsave
   ```

3. Optionally, type `rm -rf /opt/lce_splunk/` to remove the Splunk Client install directory. Configuration and log files will remain unless the directory is removed.

   An additional file, `/etc/tenable_tag`, will be installed with the Splunk Client if it does not already exist. This file contains a UUID that tracks all events related to the endpoint on which the client is installed. This file should only be removed if no other Tenable products are in use, and no others will be installed on the endpoint in the future.
LCE Splunk Client Features

The LCE Splunk Client provides you a way to move data from your Splunk instances into Tenable.sc by way of LCE. Tenable.sc is then used to comprehensively visualize the data from Splunk.

After the LCE Splunk Client is installed and configured, you configure the Splunk Indexer to forward data to the LCE Splunk Client. The client then sends that data to the LCE server, which normalizes it. Finally, that normalized data is sent to Tenable.sc.
Data Comparison

An example of the data shown in Splunk is shown below. The example shown contains search results for a Cisco ASA firewall. The exact search used narrowed the results to sourcetype=syslog, and matched the text string %ASA.

The same type of log information is available in Tenable.sc. When a user logs into Tenable.sc, there can be multiple dashboards available that display pertinent information for that user. It is possible to set a specific collection of dashboards as the default view in Tenable.sc. Examples of dashboards that can be created for events that are collected by the LCE Splunk client.

The Splunk Events dashboard in the previous example contains a component named NormalizedEvent Types Collected by Splunk. Click beside that component to view all the information available.

The NormalizedEvent Types Collected by Splunk component on the Splunk Events dashboard includes the Cisco ASA Firewall events and all event types in a normalized format that is easy to interpret. There are several views that you can select on the Event Analysis page that can be displayed by selecting Normalized Event Summary. A view similar to that in Splunk can be seen by clicking the Raw Syslog Events link.
It is also possible to filter the **Normalized Event Summary** along with any other summary view by clicking » at the top left of the window. The text string `%ASA` used in the Splunk search could be typed in the **Syslog Text** box.
Configure Splunk

This section describes the steps necessary to receive data from Splunk with the LCE Splunk Client.

- Configure the Splunk Indexer to forward data to the LCE Splunk Client.
- Configure and assign the client policy for the LCE Splunk Client.
Configure Splunk to Forward Data

The following procedure is performed on the Splunk Indexer that you want to forward data to the LCE Splunk Client.

To configure the Splunk Client to Forward Data:

1. Access Splunk Web as a user with Administrator privileges.

2. At the top of the Splunk Web interface, click Settings, and then click Forwarding and receiving.

   The Forwarding and receiving page appears.

3. In the Configure forwarding row, in the Actions column, click the Add new link.

   The Add new page appears.

4. In the Host box, type the IP address of the LCE Splunk Client host, and then click the Save button.

   The IP address is saved. On the Splunk Web interface, the IP address appears on the Forward data page.

5. Access the Splunk Indexer as the root user.

6. Edit the outputs.conf file, usually located at /opt/splunk/etc/system/local/outputs.conf. The lines you must add appear in bold.

   ```
   [tcpout]
   defaultGroup = default
   disabled = 0
   indexAndForward = 1
   [tcpout-server://LCE_IP_OR_Hostname:9800]
   [tcpout:default]
   disabled = 0
   server = LCE_IP_OR_Hostname:9800
   sendCookedData = false
   ```

7. Save the file, and then restart the Splunk services.

   Data will now be forwarded to the LCE Splunk Client.
**Configure the Splunk Client Policy**

Using the [Client Policy Builder](#), you can create and modify policies for your LCE Splunk Client. The following steps are performed via the web interface on the LCE server that you configured your LCE Splunk Client to communicate with.

**Caution:** The LCE Splunk Client can process a maximum of 500 logs per second. Processing more than 500 logs per second can result in a loss of data. This is an absolute limit and *cannot* be increased by improving the system hardware.

To configure the Splunk Client:

1. Using the Client Policy Builder, [create a policy for your LCE Splunk Client](#). This documentation includes a list of [valid configuration items for the client policy](#).

   **Note:** The LCE Splunk Client policy requires at least one IP address for a Splunk server. If no IP addresses are provided, the client will not open the Listen port.

   In order for the Splunk Client to function, you will need to edit the Client policy, include the required syntax noted below, and specify your Splunk server.

   XML Example:

   ```xml
   <splunk-server>192.0.2.10</splunk-server>
   ```

2. [Assign the policy to the LCE Splunk Client](#).
Additional Resources

This section contains the following additional resources:

- [Splunk Client Policy Configuration Items](#)
# Splunk Client Policy Configuration Items

In the Client Policy Builder, the following configuration items appear for the LCE Splunk Client.

The following table lists the configuration items that are valid for the LCE Splunk Client, and provides a brief description of each.

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Description</th>
<th>Valid Values</th>
</tr>
</thead>
</table>
| Splunk server      | The IP addresses of one or more Splunk servers that are sending data to the LCE Splunk Client. | One IP address per entry. Note: The LCE Splunk Client requires at least one IP address to be entered in order to receive data. If no Splunk servers are added, the LCE Splunk Client will not open the Listen port. In order for the Splunk Client to function, you will need to edit the Client policy, include the required syntax noted below, and specify your Splunk server. XML Example:  

```
<splunk-server>192.0.2.10</splunk-server>
```

| Listen port        | The port to which the Splunk servers are sending data. | An integer from 1024 to 65535. Privileged ports (lower than 1024) are not valid for this configuration item. | XML Example:  

```
<listen-port>8000</listen-port>
```

| Syslog server      | The IP address or hostname and port number of the syslog server that you want the LCE Splunk Client to forward events to in addition to the LCE server. | `<IP or Hostname>:<Port Number>`, where  

- `<IP or Host-`
<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Description</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>XML Examples:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <code>&lt;syslog-server&gt;</code>192.0.2.10:8000<code>/syslog-server&gt;</code></td>
<td>name&gt; is an IP address, or a hostname that is a maximum length of 46 characters.</td>
<td></td>
</tr>
<tr>
<td>• <code>&lt;syslog-server&gt;</code>corpnet8557:8000<code>/syslog-server&gt;</code></td>
<td>• <code>&lt;Port Number&gt;</code> is an integer from 1 to 65535.</td>
<td></td>
</tr>
<tr>
<td>Delimiter</td>
<td>The custom delimiters that you want to apply to parse events in Splunk logs. You can include multiple Delimiter entries in your policy.</td>
<td>See Delimiters</td>
</tr>
<tr>
<td>Note: By default, the policy includes the delimiter for Windows multiline logs. This delimiter is not required by the policy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>XML Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <code>&lt;delimiters&gt;</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <code>&lt;/delimiters&gt;</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log directory</td>
<td>Directory containing files, named according to the date, that contain LCE Splunk Client log messages.</td>
<td>A path to an existing directory.</td>
</tr>
<tr>
<td>XML Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration Item</td>
<td>Description</td>
<td>Valid Values</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Search path</td>
<td>&lt;log-directory&gt;&lt;/log-directory&gt;</td>
<td></td>
</tr>
<tr>
<td>Client heartbeat frequency</td>
<td><strong>Caution:</strong> This configuration item is deprecated for versions 4.6 and later of the LCE Splunk Client. <strong>Client heartbeat period</strong> should be used instead. XML Example: &lt;heartbeat-frequency&gt;600&lt;/heartbeat-frequency&gt;</td>
<td>No valid values.</td>
</tr>
<tr>
<td>Client heartbeat period</td>
<td>The number of seconds between each client heartbeat message to the LCE server. If not used or set to 0, the client will not send heartbeats. XML Example: &lt;heartbeat-period&gt;600&lt;/heartbeat-period&gt;</td>
<td>An integer.</td>
</tr>
<tr>
<td>Client statistics frequency</td>
<td><strong>Caution:</strong> This configuration item is deprecated for versions 4.6 and later of the LCE Splunk Client. <strong>Client statistics period</strong> should be used instead. XML Example: &lt;statistics-frequency&gt;60&lt;/statistics-frequency&gt;</td>
<td>No valid values.</td>
</tr>
<tr>
<td>Client statistics period</td>
<td>The number of minutes between each client host performance statistics report (CPU, Disk Space, and Physical Memory) to the LCE server. If not used or set to 0, client statistics will not be sent. XML Example:</td>
<td>An integer.</td>
</tr>
<tr>
<td>Configuration Item</td>
<td>Description</td>
<td>Valid Values</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td></td>
<td>&lt;statistics-period&gt;60&lt;/statistics-period&gt;</td>
<td></td>
</tr>
<tr>
<td>Compress events</td>
<td>Whether client will compress log data prior to sending it to the LCE server in order to save bandwidth. Recommended except when debugging. If set to 0, events will not be compressed. XML Example:</td>
<td>0 (off) or 1 (on)</td>
</tr>
<tr>
<td></td>
<td>&lt;compress-events&gt;1&lt;/compress-events&gt;</td>
<td></td>
</tr>
<tr>
<td>Compression level</td>
<td>Compression level to use when compressing events for transmission across network using zlib, set on a scale from 1 to 9. 1 provides the least amount of compression, resulting in minimum CPU usage and minimum bandwidth savings; 9 maximizes compression, resulting in increased CPU usage and maximum bandwidth savings. Ignored unless compression is enabled. XML Example:</td>
<td>An integer from 1 to 9.</td>
</tr>
<tr>
<td></td>
<td>&lt;compression-level&gt;5&lt;/compression-level&gt;</td>
<td></td>
</tr>
<tr>
<td>Minimum compression ratio</td>
<td>Defines the minimum acceptable savings ratio for event data being transmitted across the network, in terms of (bytes total) / (bytes compressed). If the client determines a savings ratio of less than this value, then event data will not be compressed before sending. This reduces the effort on the LCE Server decompressing event data when compression benefits are minimal. Ignored</td>
<td>A decimal number.</td>
</tr>
<tr>
<td>Configuration Item</td>
<td>Description</td>
<td>Valid Values</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>unless compression is enabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>XML Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;minimum-compression-ratio&gt;1.5&lt;/minimum-compression-ratio&gt;</td>
<td></td>
</tr>
<tr>
<td>Minimum compression input size</td>
<td>The minimum number of bytes a packet must have to be compressed. Ignored unless compression is enabled.</td>
<td>An integer greater than 0.</td>
</tr>
<tr>
<td></td>
<td>XML Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;minimum-compression-input-size&gt;2048&lt;/minimum-compression-input-size&gt;</td>
<td></td>
</tr>
<tr>
<td>Debug level</td>
<td>Controls the debugging information that is logged.</td>
<td>One of the following values:</td>
</tr>
<tr>
<td></td>
<td>XML Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;debug-level&gt;NONE&lt;/debug-level&gt;</td>
<td>• NONE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• VERBOSE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• INFO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• WARN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ERROR</td>
</tr>
<tr>
<td>Event queue timeout</td>
<td>Maximum number of seconds between event messages the client sends to the LCE server.</td>
<td>An integer greater than 0.</td>
</tr>
<tr>
<td></td>
<td>XML Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;event-queue-timeout&gt;30&lt;/event-queue-timeout&gt;</td>
<td></td>
</tr>
<tr>
<td>Configuration Item</td>
<td>Description</td>
<td>Valid Values</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Local IP net</td>
<td>If a host has multiple network connections, allows you to specify which network to use. If not set or if the CIDR does not match any networks, the client will use the first network connection detected.</td>
<td>A CIDR.</td>
</tr>
<tr>
<td></td>
<td><strong>XML Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>```xml                                                                                   &lt;local-ip-net&gt;192.0.2.0/8&lt;/local-ip-net&gt;</td>
<td></td>
</tr>
<tr>
<td>Event file</td>
<td>Path to file for receiving events. Relative paths are interpreted to start at the client's installation directory.</td>
<td>A path to an existing file.</td>
</tr>
<tr>
<td></td>
<td><strong>XML Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>```xml                                                                                   &lt;write-events-to-file&gt;&lt;/write-events-to-file&gt;</td>
<td></td>
</tr>
<tr>
<td>Write events to standard output</td>
<td>Whether to write events to standard output (stdout). Any event picked up by the LCE Splunk Client will have the raw log printed to the stdout of the client, the default being a terminal session, before the client sends it to the LCE server to be processed. This configuration item is useful for debugging and troubleshooting.</td>
<td>0 (off) or 1 (on)</td>
</tr>
<tr>
<td></td>
<td><strong>XML Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>```xml                                                                                   &lt;write-events-to-stdout&gt;0&lt;/write-events-to-stdout&gt;</td>
<td></td>
</tr>
</tbody>
</table>
Delimiters

Depending on the needs of your organization and the types of logs coming from your Splunk server, you may want to implement custom delimiters in the client policy for your LCE Splunk Client.

By default, the LCE Splunk Client parses each line in a log as an event. Because not all logs captures events on a single line, delimiters can be implemented that allow the LCE Splunk Client to capture multiple lines and parse them as a single event. If a log had more than one event stored on a single line, you can implement delimiters that allow the LCE Splunk Client to parse multiple events from a single line.

Caution: Delimiters should only be implemented by advanced users with an understanding of ECMA regular expression grammar.

The LCE Splunk Client policy can include zero or more delimiters. Delimiters are not required. In the case that delimiters are included in the policy but do not match in a log, the LCE Splunk Client uses the default behavior of parsing each line in a log as an event.

Because logs from Splunk may come from many different sources, you can include multiple delimiters in your LCE Splunk Client policy to account for the different methods of logging.

There are several considerations when implementing client policy delimiters:

- In the client policy, delimiters consist of Start and End expressions. The Start and End expressions are used to identify the starting and ending strings of the events you want to capture.

  For example, the default Start expression that appears in the policy is \d{1,2}/\d{2}(/\d{4}\d{2}:\d{2}:\d{2}) (A|P)M, which will match an event that starts with a value such as 06/15/2016 05:23:06 AM. The End expression is [^\r]\n, which matches a newline that is not preceded by a carriage return. This delimiter allows the LCE Splunk Client to capture multi-line events from Windows logs.

- Delimiters should be entered in order of priority. In the client policy, delimiters will be tested in the order they appear. If a delimiter is found to be valid for a log (i.e., the Start expression matches), no subsequent delimiters will be applied. Only one delimiter will be applied to a log.

- Delimiters must be entered using ECMA regular expression grammar.
• If a delimiter is used and more than 50,000 bytes of data follows before the End expression is found, the incomplete result will be sent to the LCE server, and the LCE Splunk Client will continue with the next log.

• After an event is captured, if it contains carriage returns or line feeds, they will be converted to spaces.
Tenable NetFlow Monitor

The documentation for the most recent version of the Tenable NetFlow Monitor is currently available starting on page 38 of the following document: http://static.tenable.com/prod_docs/LCE_4.2_clients.pdf
Tenable Network Monitor

The documentation for the most recent version of the Tenable Network Monitor is currently available starting on page 41 of the following document: http://static.tenable.com/prod_docs/LCE_4.2_clients.pdf
Tenable RDEP Monitor

The documentation for the most recent version of the Tenable RDEP Monitor is currently available starting on page 46 of the following document: http://static.tenable.com/prod_docs/LCE_4.2_clients.pdf
Tenable SDEE Monitor

The documentation for the most recent version of the Tenable SDEE Monitor is currently available starting on page 49 of the following document:  http://static.tenable.com/prod_docs/LCE_4.2_clients.pdf#page=49
Get Started with the LCE Web Query Client

The LCE Web Query Client is used to request event data from RESTful web services. The logs returned from queries are stored and normalized in LCE. Finally, the information may be searched in Tenable.sc and can be reviewed. The process to setup and configure the LCE Web Query Client begins with the configuration of the RESTful API instances that are to be queried.

The LCE Web Query Client supports:

- Amazon Web Services (AWS)
- Salesforce
- Google Cloud Platform (GCP)
# Hardware Requirements

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Dual Core x86-64</td>
</tr>
<tr>
<td>Processor Speed</td>
<td>2 Ghz</td>
</tr>
<tr>
<td>Ram</td>
<td>2 GB</td>
</tr>
<tr>
<td>Disk Space</td>
<td>100 MB</td>
</tr>
</tbody>
</table>
Software Requirements

Operating System
The LCE Web Query Client is compatible with the following operating systems:

- Red Hat Enterprise Linux 6 64-bit
- CentOS 6 64-bit

Tenable Network Security
The LCE Web Query Client requires the following software:

- Tenable.sc 5.1.x or later

Amazon Web Services (AWS)
To monitor AWS, an IAM user account with read-only access to CloudTrail is required.

Salesforce
To monitor Salesforce, a connected app with read permission for the LoginHistory and User objects is required.

Google Cloud Platform (GCP)
To monitor GCP, a user must be created, the Cloud Pub/Sub service must be enabled, and Stack-driver Logging must be configured.
Licensing

Tenable.sc must be licensed for the LCE Web Query Client. For more information, see Licenses in the Tenable.sc User Guide.
Install, Configure, and Remove

This section includes the following instructions for installing, configuring, and removing the LCE Web Query Client. With the exception of downloading the Web Query Client, the following procedures must be performed on the command line.

- Download the LCE Web Query Client
- Install the LCE Web Query Client
- Configure the LCE Web Query Client
- Remove the LCE Web Query Client
Install the LCE Web Query Client

Before you begin:

- Download the LCE Web Query Client, as described in Download an LCE Client.

To install the Web Query Client:

**Note:** All shell commands need to be executed by a user with root privileges.

1. Copy the downloaded client package to the host where it will be installed.
2. Verify the MD5 checksum of the client package against the MD5 checksum found in the release notes.
   
   Example:
   
   ```
   # md5sum lce_webquery-4.6.0-el6.x86_64.rpm
   da9f07886a693fb69c1a3b2d53eb31a1 lce_webquery-4.6.0-el6.x86_64.rpm
   ```
   
3. To initiate the installation, type the following command:

   ```
   rpm -ivh <package name>, where <package name> is the name of the client package.
   ```
   
   Example:
   
   ```
   # rpm -ivh lce_webquery-4.6.0-el6.x86_64.rpm
   Preparing... .......................................................... [100%]
   1:1ce_webquery ....................................................... [100%]
   Wrote UUID to /opt/tenable/tag
   Please run /opt/lce_webquery/set-server-ip.sh to configure your LCE server's IP and port.
   ```
Configure the LCE Web Query Client

**Note:** All shell commands need to be executed by a user with root privileges.

To configure the Web Query Client, you can execute the `set-server-ip.sh` script and include the LCE Server IP address and port number as arguments, or execute the script and, when prompted, enter the IP address and port number individually.

To execute the script using arguments:

1. Type `/opt/lce_webquery/set-server-ip.sh <IP> <Port>`, where `<IP>` is the IP address of an LCE Server and `<Port>` is the port number assigned to the server. By default, the port number is 31300.

   The LCE Server IP address and port number are updated, and the LCE Web Query Client daemon is restarted.

   Example:

   ```bash
   # /opt/lce_webquery/set-server-ip.sh 192.168.22.11 31300
   Updating LCE Server IP from 192.0.2.66 to 192.0.2...
   Updating LCE Server Port from 31300 to 31300...
   Done
   Stopping LCE Webquery daemon
   Starting LCE Webquery daemon
   [ OK ]
   ```

To execute the script without arguments:

1. Type `/opt/lce_webquery/set-server-ip.sh`

   You are prompted to enter the LCE Server IP address or hostname.

2. Type the IP address or hostname of LCE LCE server.

   You are prompted to enter the LCE server port.

3. Type the port number assigned to the server for LCE client communication. By default, the port number is 31300.
The LCE Server IP address and port number are updated, and the LCE Web Query Client daemon is restarted.

Example:

```
# /opt/lce_webquery/set-server-ip.sh

Enter the new desired LCE server IP or hostname.
>>
192.168.22.11

Enter the new desired LCE server port [31300].
>>
31300
Updating LCE Server IP from 203.0.113.1 to 192.168.22.11...
Updating LCE Server Port from 31300 to 31300...
Done
Stopping LCE Webquery daemon [ OK ]
Starting LCE Webquery daemon [ OK ]
```
Remove the LCE Web Query Client

**Note:** All shell commands need to be executed by a user with root privileges.

To remove the LCE Web Query Client:

1. To query the rpm database to obtain the name of the currently installed package, type `rpm -qa |grep lce_`.
   
   Example:
   ```
   # rpm -qa |grep lce_
   lce_webquery-4.6.0-el6.x86_64
   ```

2. Type `rpm -e lce_webquery`.
   
   The Web Query Client package is removed.
   
   Example:
   ```
   # rpm -e lce_webquery
   warning: /opt/lce_webquery/state.json saved as /opt/lce_webquery/state.json.rpmsave
   warning: /opt/lce_webquery/server_assignment.xml saved as /opt/lce_webquery/server_assignment.xml.rpmsave
   ```

3. Optionally, type `rm -rf /opt/lce_webquery/` to remove the Web Query Client install directory. Configuration and log files will remain unless the directory is removed.

   An additional directory, `/opt/tenable`, will be installed with the Web Query Client if it does not already exist. This directory contains a UUID that tracks all events related to the endpoint on which the client is installed. This directory should only be removed if no other Tenable products are in use, and no others will be installed on the endpoint in the future.
Features

This section describes the features available in the LCE Web Query.

- Monitor Amazon Web Services (AWS)
- Monitor Salesforce
- Monitor Google Cloud Platform (GCP)
- Monitor and Limit Bandwidth
- Monitor Client Statistics
Monitor Amazon Web Services (AWS)

The LCE Web Query Client queries the AWS CloudTrail API in order to monitor events supported by CloudTrail. These events can be viewed in Tenable.sc and used to identify irregular activity in AWS. In order to monitor CloudTrail events, you must enable CloudTrail, attach the necessary policy to IAM users or groups, and configure the Web Query Client policy to make calls to the CloudTrail API. Additionally, you can limit the amount of bandwidth the Web Query Client will use when communicating with CloudTrail, and monitor the hardware statistics of the host where the Web Query Client is installed.
Monitor Salesforce

The LCE Web Query Client queries the Salesforce REST API in order to monitor login events, as well as the creation and modification of user accounts. These events can be viewed in Tenable.sc and used to identify irregular activity in Salesforce from unexpected sources. In order to monitor Salesforce events, you must create a connected app, and configure the Web Query Client policy to make calls to the Salesforce API. Additionally, you can limit the number of calls the Web Query Client will make to the Salesforce API to respect subscription limits, and monitor the hardware statistics of the host where the Web Query Client is installed.
Monitor Google Cloud Platform (GCP)

The LCE Web Query Client queries the Google Cloud API and the Google Cloud Pub/Sub service in order to monitor various events that you can specify when configuring logging in GCP. In order to monitor GCP events, you must enable the Pub/Sub API in Google Cloud, set up a topic, and configure the Web Query Client policy to make calls to the Pub/Sub service. Additionally, you can limit the number of calls the Web Query Client will make to the Pub/Sub service, and monitor the hardware statistics of the host where the Web Query Client is installed.
Monitor and Limit Bandwidth

The LCE Web Query Client monitors the number of calls made and bandwidth used while communicating with the Salesforce and AWS CloudTrail APIs. The monitored data can be viewed in Tenable.sc. Additionally, when you configure a Web Query Client policy, you may specify limits on the number of calls or the amount of bandwidth the Web Query Client will use over a period of time. This feature can be leveraged to reduce costs related to AWS, or respect the call limit imposed by a Salesforce subscription, among other potential uses. Warnings are generated when usage reaches thresholds of 50%, 75%, and 90% of the defined limit.
Monitor Client Statistics

All LCE clients monitor the hardware statistics of the host where the client is installed. The hardware statistics can be viewed via the LCE server interface and Tenable.sc. These statistics can be used to evaluate the resource and network usage of the host while the LCE client is operating.
How To

This section describes how to perform the actions available in LCE Web Query Client.

You can configure the Web Query Client to query AWS CloudTrail, Salesforce, and Google Cloud Platform in order to track and review events.
How to Monitor Amazon Web Services (AWS)

This section describes the steps necessary to query AWS with the LCE Web Query Client.

1. Complete the prerequisite tasks in AWS.
2. Configure the Web Query Client policy.
3. Review AWS events in Tenable.sc CV.
Prerequisite Tasks for Integration with AWS

Before querying AWS with the LCE Web Query Client, you must perform the following tasks in AWS:

1. In the AWS console, enable CloudTrail.
2. Create one or more IAM users.
   - Generate an access key for each user.
   - Download the user security credentials.
3. Attach the AWSCloudTrailReadOnlyAccess policy to each user, or the group that contains the users, created in step 2.
4. Configure a Web Query Client policy to query CloudTrail.
Configure the Web Query Client Policy for AWS

Using the Client Policy Builder, you can create and modify policies for your LCE Web Query Client. The following steps are performed via the web interface on the LCE server that you configured your LCE Web Query Client to communicate with.

To configure the Web Query Client Policy for AWS:

1. Using the Client Policy Builder, create a policy for your LCE Web Query Client. This documentation includes a list of valid configuration items for the client policy.

A Web Query Client policy for AWS requires you to add an AWS CloudTrail endpoint to the policy. You must provide the following:

   • The User ID and secret key that was created when completing the prerequisite tasks.

To add the endpoint:

a. In the Basic pane of the Client Policy Builder, click the button in Group to add a group.

   The Add a new endpoint group window appears.

b. Click the Add AWS CloudTrail endpoint button.

   A new AWS CloudTrail endpoint appears.

c. In the Endpoint name box, enter a name that identifies the endpoint.

d. Select the Active check box.

e. In the Query interval box, enter the number of seconds between each query to the Salesforce API.

f. In the Region box, enter the region defined in the AWS account.

g. In the Access Key ID box, enter the Access Key ID for an IAM user.

h. In the Secret Access Key box, enter the IAM Secret Access Key that corresponds to the Access Key ID.
Note: You can add multiple endpoints to a single group. For example, one group could contain three AWS CloudTrail endpoints. Another group could contain a Salesforce endpoint, an AWS CloudTrail endpoint, and a Google Cloud endpoint.

2. Assign the policy to the LCE Web Query Client.
Review AWS Events in Tenable.sc

To review AWS Events in Tenable.sc:

1. Navigate to Tenable.sc and log on with a user account that has permission to view logs for the organization.
   
   A dashboard that corresponds to the user role appears.

2. In the top navigation bar, click Analysis, and then click the Events link.
   
   The Event Analysis page appears, displaying the Type Summary section.

3. Click the Type Summary button, and then select Normalized Event Summary.
   
   The Normalized Event Summary section appears.

4. In the upper-left corner of the page, click ➤.
   
   The Filters pane appears.

5. Click the Select Filters button

6. In the Add Filter window, select Normalized Event.

7. Click the Apply button.

8. Click the Normalized Event box.

9. In the Normalized Event window, type AWS-*.

10. Click OK.

11. In the Filters pane, click the Apply All button.
   
   In the Normalized Event Summary section, the list of events is filtered and displays only events that start with AWS-.

   The AWS events available will be based on the monitored activity logged by AWS CloudTrail. For a list of specific events, you can click an AWS event type (e.g., AWS-Console_Login) listed in the Normalized Event Summary section. You can also click the Jump to Raw Syslog Events link to directly view the log data.
12. At the top of the Event Analysis page, click the Normalized Event Summary button, and then select Detailed Event Summary.

The Detailed Event Summary section appears.

For a list of specific events, click an AWS event (e.g., ConsoleLogin) listed in the Detailed Event Summary section.
How to Monitor Salesforce

This section describes the steps necessary to query Salesforce with the LCE Web Query Client.

1. Complete the prerequisite tasks in Salesforce.
2. Configure the Web Query Client policy.
3. Review Salesforce events in Tenable.sc.
Prerequisite Tasks for Integration with Salesforce

Before completing the procedures to integrate LCE with Salesforce, you must perform the following tasks in Salesforce:

1. **Create a connected app.**
   - Give the app read permission for the LoginHistory and User objects.
   - Save the Consumer Secret and Consumer Key.

2. **Relax IP restrictions.**
   
   **Note:** This task is only necessary if you are unable to view Salesforce events in Tenable.sc.

3. **Configure a Web Query Client policy to query the Salesforce REST API.**
Configure the Web Query Client Policy for Salesforce

Using the Client Policy Builder, you can create and modify policies for your LCE Web Query Client. The following steps are performed via the web interface on the LCE server that you configured your LCE Web Query Client to communicate with.

To configure the Web Query Client Policy for Salesforce:

1. Using the Client Policy Builder, create a policy for your LCE Web Query Client. This documentation includes a list of valid configuration items for the client policy.

   A Web Query Client policy for Salesforce requires you to add a Salesforce endpoint to the policy. You must provide the following:
   
   - The username, password, and security token of a Salesforce user account.
   - The Consumer Secret and Consumer Key you obtained when you created a connected app.

To add the endpoint:

   a. In the Basic pane of the Client Policy Builder, click the button in Group to add a group.

      The Add a new endpoint group window appears.

   b. Click the Add Salesforce endpoint button.

      A new Salesforce endpoint appears.

   c. In the Endpoint name box, enter a name that identifies the endpoint.

   d. Select the Active check box.

   e. In the Query interval box, enter the number of seconds between each query to the Salesforce API.

   f. In the Username box, enter the username for the Salesforce account being queried.

   g. In the Password box, enter the password that corresponds to the username, along with that user’s security token appended to the end of the password. For example, passwordsREvNGuKHvuIhLTrS.
h. In the **Consumer Key** box, enter the Consumer Key for the connected app you created.

i. In the **Consumer Secret** box, enter the Consumer Secret for the connected app you created.

**Note:** You can add multiple endpoints to a single group. For example, one group could contain three Salesforce endpoints, Another group could contain a Salesforce endpoint, an AWS CloudTrail endpoint, and a Google Cloud endpoint.

2. **Assign the policy to the LCE Web Query Client.**
Review Salesforce Events in Tenable.sc

To review Salesforce Events in Tenable.sc:

1. Navigate to Tenable.sc and log on with a user account that has permission to view logs for the organization.

   A dashboard that corresponds to the user role appears.

2. In the top navigation bar, click Analysis, and then click the Events link.

   The Event Analysis page appears, displaying the Type Summary section.

3. Click the Type Summary button, and then select Normalized Event Summary.

   The Normalized Event Summary section appears.

4. In the upper-left corner of the page, click ».

   The Filters pane appears.

5. Click the Select Filters button, and then, in the Add Filter popout, select Normalized Event.

6. Click the Apply button.

7. Click the Normalized Event box, and then, in the Normalized Event text box, type Salesforce-.

8. Click OK.

9. In the Filters pane, click the Apply All button.

   In the Normalized Event Summary section, the list of events is filtered and displays only events that start with Salesforce-.

For Salesforce, the Web Query Client monitors login successes and failures, and the creation and modification of user accounts. For a list of specific events, click a Salesforce event type (e.g., Salesforce-Remote_Access_Login) listed in the Normalized Event Summary section. You can also click the Jump to Raw Syslog Events link to directly view the log data.
How to Monitor GCP

This section describes the steps necessary to query GCP with the LCE Web Query Client.

1. Complete the prerequisite tasks in GCP.
2. Configure the Web Query Client policy.
3. Review GCP events in Tenable.sc CV.
Prerequisite Tasks for Integration with GCP

Before completing the procedures to integrate LCE with GCP, you must perform the following tasks via the GCP Console:

1. **Create a service account for LCE.** When you create the service account:
   - Select **Furnish a new private key**.
   - For **Key type**, select **JSON**.

   A .json file that contains the public/private key pair is downloaded. This key pair is required for the Web Query Client policy.

   **Note:** The previous link is to the official documentation for GCP. This procedure expects that you will be using the GCP Console to complete the tasks. After viewing the official GCP documentation, to see the instructions for the Console, in the boxes that appear on the page, click **Console**.

   For example:

   ![Console screenshot](image)

2. If you have not already, **complete the steps required to enable the Pub/Sub API**. Then, **create a topic and add a subscription**.
   - For **Delivery Type**, select **Pull**.

   Note the subscription name. The subscription name is required for the Web Query Client policy.
3. If you want to obtain logs from one or more Google Compute Engine or Amazon EC2 VM instances, install the logging agent on those instances.

4. Configure Stackdriver Logging to export one or more logs to the topic you created in step 2. Those logs will be processed by the Web Query Client.

5. Configure a Web Query Client policy to pull logs from the Pub/Sub service.
Configure the Web Query Client Policy for GCP

Using the Client Policy Builder, you can create and modify policies for your LCE Web Query Client. The following steps are performed via the web interface on the LCE server that you configured your LCE Web Query Client to communicate with.

To configure the Web Query Client Policy for GCP:

1. Using the Client Policy Builder, create a policy for your LCE Web Query Client. This documentation includes a list of valid configuration items for the client policy.

   A Web Query Client policy for GCP (Google Cloud Platform) requires you to add a Google Cloud endpoint to the policy. You must provide the following:

   - The service account key in the .json file that was downloaded when completing the pre-requisite tasks.
   - The subscription name for the Pub/Sub service topic.

To add the endpoint:

   a. In the Basic pane of the Client Policy Builder, click the button in  to add a group.

      The Add a new endpoint group window appears.

   b. Click the Add Google Cloud endpoint button.

      A new Google Cloud endpoint appears.

   c. In the Endpoint name box, enter a name that identifies the endpoint.

   d. Select the Active check box.

   e. In the Query interval box, enter the number of seconds between each query to the Cloud Pub/Sub service.

   f. In the JSON service account key box, enter the entire service account key including the braces.

      For example:
{
"type": "service_account",
"project_id": "blinkum-genovese-011599",
"private_key_id": "d644c15c7332d29574f0f36ec31659db2e7cdad2",
"private_key": "-----BEGIN PRIVATE KEY----\nPmxlQ6i3kz/sO7NtLX2lcRuUAzgHiET99UAlqLWGsF2Msqfb38rtvBfFOmTg+NOQH8BkX8XbhGPN1Ks4xDHxtgKbSvWlUg+Eit3rSp1NuWjSz7YqUuCSgsOwbbRQvXtNKvr2RllbFyyymMpakB6iXT5UnfJqftZa5M6pWlMt2wikmkRQxlmpJTHPmaRr3fyhnYJqM/v\TJL4bjprvuYSqzMiXaWq0\Fo0ND28kB30dAhhao5NM6oykq8\OdYc6v534Y+eQfpkpOCN8qRyTTzyYLh0fKm2vEzO/O2n7+jm31h/zNlLqXf/87HsKE8TwGqw05xii21XlrL3\j8DKrNuYy9UClaxxND/r8ncgK6Cv\AYp1DJ1qLw2aIndYZaN9iXyvVQ5GdpUazj0eHORbibfjMCwP1diOAlnmlXfYMk3hTjT2/+teZtOplDL/4OCzuP\k3foR5\G5aTFKo2+w8N5wmtg5ehvDsmMmvfP2TPxIZia6BPD0uyKdESMOZOfsEgSNSFPoaIUq/qV1IrA7Q2XwtGzWuqDcALJi7x65IxrIivXUrHv379AjgrXW6SnKEFLJ1LtHi9dGBElnI+h3mx+\\z\v0X8d1vJed4tjOMNvWRaAhXhuNouAly7Xt3Eug9OCTX+di9esV7kF++heG/8yQLIQCyeBRMfot4SnDvw7xJ0sKSOKv5MOi8t6HGLsggvFR5R6V6lx3BwqeljYJDNdOYInFYKcI3DUQ8aumNLOJfEi2st9pR2sH6xb7sKSF5odeSkOoAEPqDBoOrTrYdjMUx/uRTfZBRkhKH3zVGqwR8E4HWLYnuy5vr/yEiJ/xjTS1SfVQ+mw2vVq3UdrGhPOyjEljvGAi6FAccIaJV4LkGrEKjYA6vO6n2Gswt4pR\FZ6IQj9CU8D5rUnmuJ9VP3O2ivHWkXWIBZzUZjFI3TWRZWncZXhQ8ySki6cHW7ng06WsQeN2wfP0UHHPCqkeQo1VOL+5e3POgb0izNCdy3a+ffk9XrMZo91MvyqdwPLOunI6cgcoTLlslDgwrbYvcjUAcYG6iI6/CC5o5ws\5CNlIl/JgE1IQlI48815H+q/67GUaywyR2Sfd\c4nRcNRUMJNWjzzntjraAhBy19NmKaEWKitgSFQIf1o9uatXo4s\OcPzL2ejY2bTF+1Sgo1yatsg5UWZjhb0dPabiAWKQJoZmilq7jKJ++o\ayooYOVR1kimXuhiX9RrlKLsRy0vL4KjnY3Rg2UTI5zoPyAdr4VFTsLuZ8\0WMF8/BxcASBhPCu9f4YI9hL3Qnhf4sV2+cMDUR71uv7LXIzhsaz9TDDKRvqyEoRGVo1EiNjClCrF4IPzDRwfRoAD7SegAKt5gLF+XkE5PWrVqYD9iTxj7tK\yyOR9nRRswgsz3MW78hVJXKcvSVh06m\2S55MiSBp/Qm4U9Rjtnpy1SwNc8818A6DKQtUfM/R+rR\Nl9pmMo2yPBNRX+5F0KMKRsvYuDWuhgvXmWIV19I8+Aif4kh9XUpJBQtrHrFD1wRDQ2HNV+vgklewhMOiHmSqTc5oZlNQmOH0+dgKwkkNgc12yu/z5FSOxm\bl0b+fZ54KI3lJa45jJyq3+BMyN0pJ\nIWoSRqSIbyD/TlmGsfGzoQLTrUm1SgLh2RKmaCogdBlsGg6hD2C8Uf\n-----END PRIVATE KEY-----\n",
"client_email": "test-credential-service-acct@blinkum-genovese011599.iam.gserviceaccount.com",
"client_id": "404842616201342653591",
"auth_uri": "https://accounts.google.com/o/oauth2/auth",
"token_uri": "https://accounts.google.com/o/oauth2/token",
"auth_provider_x509_cert_url":
"https://www.googleapis.com/oauth2/v1/certs",

Copyright © 2022 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable,Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective


g. In the Subscription box, enter the subscription name. For example, `projects/my-project-name/subscriptions/my-subscription-name`.

**Note:** You can add multiple endpoints to a single group. For example, one group could contain three Google Cloud endpoints. Another group could contain a Salesforce endpoint, an AWS CloudTrail endpoint, and a Google Cloud endpoint.

2. Assign the policy to the LCE Web Query Client.
Review GCP Events in Tenable.sc

To review GCP Events in Tenable.sc:

1. Navigate to Tenable.sc and log on with a user account that has permission to view logs for the organization.

   A dashboard that corresponds to the user role appears.

2. In the top navigation bar, click Analysis, and then click the Events link.

   The Event Analysis page appears, displaying the Type Summary section.

3. Click the Type Summary button, and then select Normalized Event Summary.

   The Normalized Event Summary section appears.

4. In the upper-left corner of the page, click ».

   The Filters pane appears.

5. Click the Syslog Text box, and then, in the Syslog Text text box, type googleapis.

6. Click OK.

7. In the Filters pane, click the Apply All button.

   In the Normalized Event Summary section, the list of events is filtered and displays events that include googleapis in the text of the syslog.

   The GCP events available will be based on the logs you specified when you configured Stack-driver Logging. You can click the Jump to Raw Syslog Events link to directly view the log data.
Additional Resources

This section contains the following additional resources:

- Web Query Client Policy Configuration Items
- Correcting AWS Configuration Issues
- Correcting Network Time Protocol Issues
Web Query Client Policy Configuration Items

The interaction of the Web Query Client with AWS, Salesforce, and GCP is configured by modifying a Web Query Client policy via the Client Policy Builder. The policy is separated into configurable items, represented in the Advanced pane of the Client Policy Builder by XML elements of the same name. Certain parameters are common to all LCE clients and are generally the parameters listed first in a policy.

The usage and application parameters that follow the common client parameters vary based on the client. In the case of the Web Query Client policy, parameters are provided that allow you to limit the bandwidth the Web Query Client will use, as well as specify the credentials required for connecting to AWS, Salesforce, and GCP.

This section includes:

- **Example**: default_rhel_web Policy
- Common Client Parameters
- Usage-Limit Parameters
- CloudTrail Parameters
- Salesforce Parameters
- GCP Parameters

Example: default_rhel_web Policy

The following is an example of the contents of a Web Query Client policy file.

```xml
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<options xmlns:xi="http://www.w3.org/2003/XInclude">
  <log-directory>/opt/lce_webquery/logs</log-directory>
  <debug-level>INFO</debug-level>

  <!--local-ip-net>192.0.2.0/24</local-ip-net-->  

  <!-- client-debug / -->
  <heartbeat-period>300</heartbeat-period>
  <statistics-period>60</statistics-period>
</options>
```
<compress-events>1</compress-events>
<group>
</group>

<!-- Group Setup Example
<group>
  <name>ByteRestrictedGroup</name>
  <usage-limit>
    <type>BYTES</type>
    <value>35M</value>
    <time>MONTH</time>
    <start-day>5</start-day>
  </usage-limit>
  <cloudtrail>
    <name>CloudTrail1</name>
    <active>yes</active>
    <query-interval-seconds>600</query-interval-seconds>
    <region>us-east-1</region>
    <id>AWSId</id>
    <key>MySecretKey</key>
  </cloudtrail>
</group>

<group>
  <name>CallRestrictedGroup</name>
  <usage-limit>
    <type>CALLS</type>
    <value>10000</value>
    <time.DAY</time>
  </usage-limit>
  <salesforce>
    <name>Salesforce_1</name>
    <active>No</active>
    <query-interval-seconds>300</query-interval-seconds>
    <username>MyUsername</username>
    <password>MyPassword</password>
    <consumer-key>MyKey</consumer-key>
    <consumer-secret>MySecret</consumer-secret>
  </salesforce>
</group>
Common Configuration Items

The following table lists the policy configuration items in the order they appear in the default Web Query Client policy. These parameters are defined when configuring the Web Query Client policy for AWS, Salesforce, and GCP.

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>log-directory</td>
<td>The path to which to write the Web Query Client operational logs.</td>
<td>/opt/ice_webquery/logs</td>
</tr>
<tr>
<td>debug-level</td>
<td>Minimum debugging level that is printed to the log. The options supported are as follows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• INFO</td>
<td>INFO</td>
</tr>
<tr>
<td></td>
<td>• WARN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ERROR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NONE</td>
<td></td>
</tr>
<tr>
<td>local-ip-net</td>
<td>If a host has multiple network connections, allows you to specify which network to use. If not set or if the CIDR does not match any networks, the client will use the first network connection detected.</td>
<td>192.0.2.0/24</td>
</tr>
<tr>
<td>Configuration Item</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>heartbeat-frequency</td>
<td>The number of seconds between each client heartbeat message to the LCE server. If set to 0, the client will not send heartbeats.</td>
<td>A positive integer. 300</td>
</tr>
<tr>
<td>statistics-frequency</td>
<td>The number of minutes between each client host performance statistics report (CPU, Disk Space, and Physical Memory) to the LCE server. If set to 0, client statistics will not be sent.</td>
<td>A positive integer. 60</td>
</tr>
<tr>
<td>compress-events</td>
<td>Defines whether to compress events before transmitting them to the LCE server. If set to 1, provides a marginal savings for bandwidth in exchange for a marginal increase in CPU usage.</td>
<td>0 (off) or 1 (on)</td>
</tr>
<tr>
<td>Write events to standard output</td>
<td>Whether to write events to standard output (stdout). Any event picked up by the LCE Splunk Client will have the raw log printed to the stdout of the client, the default being a terminal session, before the client sends it to the LCE server to be processed. This configuration item is useful for debugging and troubleshooting.</td>
<td>0 (off) or 1 (on)</td>
</tr>
</tbody>
</table>

**Usage-Limit Configuration Items**

The configuration of the usage-limit items is usually based on the API being queried. The AWS CloudTrail API measures the amount of bandwidth utilized by the queries made to the API. The Salesforce API measures the number of calls. Because CloudTrail and Salesforce monitor usage differently, generally groups will be limited by bytes or calls based on the API. However, the Web Query Client can be configured to support many use cases, such as limiting usage of the Salesforce API by bytes. The usage limit parameters are in place to help control excess bandwidth charges, and respect call limitations that are applied by the API vendor.
The following table lists the usage-limit parameters in the order they appear in the Client Policy Builder. These parameters are defined when configuring a Web Query Client policy for AWS, Salesforce, or GCP.

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>An alphanumeric name for the connection group.</td>
<td>ByteRestrictedGroup</td>
</tr>
<tr>
<td>type</td>
<td>Groups can either be limited byBYTES or CALLS.</td>
<td>BYTES</td>
</tr>
<tr>
<td>value</td>
<td>This is the numeric value given toBYTES or CALLS.</td>
<td>100M</td>
</tr>
<tr>
<td>time</td>
<td>The period of time by which usage is limited. For example, if a group is limited to 1000 calls, and this parameter is set to DAY, usage is limited to 1000 calls every 24 hours.</td>
<td>MONTH, DAY, HOUR, MINUTE</td>
</tr>
<tr>
<td>start-day</td>
<td>Defines the starting day when the time parameter is set to MONTH. The value can be an integer from 1 to 28.</td>
<td>14</td>
</tr>
</tbody>
</table>

**Note:** Bytes can be represented by a number followed by K(Kilobyte), M(Megabyte) G(Gigabyte), or T(Terabyte).

CloudTrail Parameters

The following table lists the CloudTrail parameters in the order they appear in the Client Policy Builder. These parameters are defined when configuring a Web Query Client policy for AWS.

<table>
<thead>
<tr>
<th>Policy Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>An alphanumeric name for the</td>
<td>AWSgroup</td>
</tr>
<tr>
<td>Policy Parameter</td>
<td>Description</td>
<td>Example Value</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>active</td>
<td>Defines whether to query the instance. If set to yes, the Web Query Client</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>will make queries using the parameters defined in that CloudTrail sub-section.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can have multiple sub-sections that are configured to be active.</td>
<td></td>
</tr>
<tr>
<td>query-interval-seconds</td>
<td>The number of seconds between each query to the endpoint.</td>
<td>300</td>
</tr>
<tr>
<td>region</td>
<td>The region defined in the AWS account.</td>
<td>us-east-1</td>
</tr>
<tr>
<td>id</td>
<td>An IAM Access Key ID.</td>
<td>IKADIY6VH42HTKTQl4OA</td>
</tr>
<tr>
<td>key</td>
<td>The IAM Secret Access Key that corresponds to the Access Key ID.</td>
<td>koN/ByNBZB5S7/tOrT3WBr6D9d0jDvT98bU9qpyH</td>
</tr>
</tbody>
</table>
The following table lists the Salesforce parameters in the order they appear in the Client Policy Builder. These parameters are defined when configuring a Web Query Client policy for Salesforce.

<table>
<thead>
<tr>
<th>Policy Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>An alphanumeric name for the Salesforce connection.</td>
<td>SalesforceGroup</td>
</tr>
<tr>
<td>active</td>
<td>Defines whether to query the instance. If set to yes, the Web Query Client will make queries using the parameters defined in that Salesforce subsection. You can have one or more sub-sections in multiple groups that are configured to be active.</td>
<td>yes</td>
</tr>
<tr>
<td>query-interval-seconds</td>
<td>The number of seconds between each query to the endpoint.</td>
<td>300</td>
</tr>
<tr>
<td>Policy Parameter</td>
<td>Description</td>
<td>Example Value</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>---------------</td>
</tr>
<tr>
<td>username</td>
<td>The username for the Sales-force account being queried.</td>
<td><a href="mailto:user@example.com">user@example.com</a></td>
</tr>
<tr>
<td>password</td>
<td>The password that corresponds to the username, and that user’s security token appended to the end of the password.</td>
<td>passwordsREvNGuKHvuLTrS</td>
</tr>
<tr>
<td>consumer-key</td>
<td>The Consumer Key for a connected app.</td>
<td>1MVG7KI2HHAq08RzmvrJMFaXELNe_ Tbg1vJf.xUyRK7f5Hyso2bZrW.TobC9X0.jqzNVP0ytuD_1XrKKFsku</td>
</tr>
<tr>
<td>consumer-secret</td>
<td>The Consumer Secret for a connected app.</td>
<td>8675309731701479235</td>
</tr>
</tbody>
</table>

**GCP Parameters**

The following table lists the GCP parameters in the order they appear in the Client Policy Builder. These parameters are defined when configuring a Web Query Client policy for GCP.

<table>
<thead>
<tr>
<th>Policy Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>An alphanumeric name for the GCP group.</td>
<td>GCP</td>
</tr>
<tr>
<td>active</td>
<td>Defines whether to query the</td>
<td>yes</td>
</tr>
<tr>
<td>Policy Parameter</td>
<td>Description</td>
<td>Example Value</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>---------------</td>
</tr>
<tr>
<td>instance. If set to yes, the Web Query Client will make queries using the parameters defined in that GCP subsection. You can have one or more subsections in multiple groups that are configured to be active.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>query-interval-seconds</td>
<td>The number of seconds between each query to the end-point.</td>
<td>300</td>
</tr>
<tr>
<td>json-service-account-key</td>
<td>The service account key for a GCP user.</td>
<td>The contents of a .json file downloaded from GCP.</td>
</tr>
<tr>
<td>Subscription</td>
<td>The subscription name for the Google Pub/Sub service topic.</td>
<td>projects/example-project080116/subscriptions/logging-feed-topic</td>
</tr>
</tbody>
</table>
Correcting AWS Configuration Issues

The AWS command line interface (CLI) can be installed to troubleshoot AWS connection and configuration issues. Information about installation of AWS CLI can be found here.

To correct AWS configuration issues:

1. The first command will configure the AWS CLI. If it was previously ran the AWS Access Key ID, AWS Secret Access Key, and region name will already be populated. This information is also found in the policy file. An example of the output from this command is shown below.

   ```bash
   C:\>aws configure
   AWS Access Key ID [***************JSQJ]:
   AWS Secret Access Key [***************yaGQ]:
   Default region name [us-west-2]:
   Default output format [None]:
   ```

2. The second command will describe trails that are available if the configuration criterion was entered correctly in the previous step. It will also provide the names of the trails that are available to be queried. An example of the output from this command is shown below.

   ```json
   C:\>aws cloudtrail describe-trails
   }
   ```
3. Using the name of the trail you can query the trails status. From the output, you can tell if the trail is logging and the start and stop logging time in Epoch time of the trail. An example of the output from this command is shown below.

```bash
C:\>aws cloudtrail get-trail-status --name test_trail {
   "LatestNotificationAttemptSucceeded": "",
   "LatestDeliveryAttemptTime": "2015-11-02T05:04:50Z",
   "LatestDeliveryTime": 1446440690.306,
   "TimeLoggingStarted": "2015-10-26T21:43:08Z",
   "LatestDeliveryAttemptSucceeded": "2015-11-02T05:04:50Z",
   "IsLogging": true,
   "LatestCloudWatchLogsDeliveryTime": 1446243728.775,
   "StartLoggingTime": 1445895788.299,
   "StopLoggingTime": 1444418827.475,
   "LatestNotificationAttemptTime": "",
   "TimeLoggingStopped": "2015-10-09T19:27:07Z"
}
```
Correcting Network Time Protocol Issues

If you are not receiving any AWS events, and the message below is found in the logs Network Time Protocol (NTP), it should be checked to ensure it is configured correctly.

Oct 28, 15 14:38:26.898556 (endpoint_0) INFO (webquery_endpoint.cpp:168,sendHealthStatus) - LCE Web Client Status: Alert: Endpoint Demo/CloudTrail-test-Cloud: CloudTrail query signature was invalid, and no further queries will be submitted. Check your system clock and timezone. To resume querying, update the system clock or restart the client.

To correct Network Time Protocol issues:

1. Running the clock or date command will show the current time of the server.

   ```
   # clock
   Wed 04 Nov 2015 04:33:29 PM EST -0.266432 seconds
   # date
   Wed Nov 4 16:33:32 EST 2015
   ```

2. The following command can be run to re-sync the time with the configured NTP servers if the time is found to be incorrect.

   ```
   # ntpd -qg
   ntpd: time set -6.953726s
   ```

3. After the time is has been re-synced stop the LCE Web Query Client using the command below.

   ```
   # service lce_webquery stop
   ```

4. Remove the state.json file from the /opt/lce/webquery directory.

   ```
   # rm -rf /opt/lce_webquery/state.json
   ```
5. Start the LCE Web Query Client.

```
# service lce_webquery start
```
WMI Monitor Client

The documentation for the most recent version of the WMI Monitor Client is currently available starting on page 30 of the following document: http://static.tenable.com/prod_docs/LCE_4.2_clients.pdf
Additional Resources

This section includes the following:

- **Tools**
- **Encryption Strength**
- **File and Process Allow List**
- **Import LCE Data Manually**
- **Manual Key Exchange with Tenable.sc**
- **User Tracking**
- **Non-Tenable License Declarations**
- **Silo Archiving**
Tools

When LCE is installed, it includes a number of tools and utilities. All tools are installed in the
/opt/lce/tools/ directory.

General Tools

The following table lists in alphabetical order each tool and describes its function.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>archival-manager</td>
<td>Performs tasks relating to archiveDb.</td>
<td>--list-snapshots [&lt;siloName&gt;</td>
</tr>
</tbody>
</table>
|                    |                                                                            | --enum-snapshots [<siloName>]
<p>|                    |                                                                            | (Faster but less informative than --list-snapshots.)                  |
|                    |                                                                            | --archive &lt;siloName&gt;                                                  |
|                    |                                                                            | --restore &lt;snapshotId&gt;                                                |
|                    |                                                                            | [into_siloName&gt;]                                                      |
|                    |                                                                            | --remove-active &lt;siloName&gt;                                             |
|                    |                                                                            | --remove-archived &lt;snapshotId&gt;                                        |
|                    |                                                                            | --archive--range [--dry-run] &lt;from_ date&gt; &lt;to_date&gt;                   |
|                    |                                                                            | --restore--range [--dry-run] &lt;from_ date&gt; &lt;to_date&gt;                   |
|                    |                                                                            | --remove-active--range [--dry-run] &lt;from_ date&gt; &lt;to_date&gt;             |
|                    |                                                                            | --remove-archived--range [--dry-run] &lt;from_ date&gt; &lt;to_date&gt;          |
|                    |                                                                            | (Each date must be given in YYYYMmmDD format.                        |
|                    |                                                                            | A range includes both &quot;to&quot; and &quot;from&quot; dates.                         |
|                    |                                                                            | Dates refer to tOrigin of contained events.)                         |
|                    |                                                                            | --identify-currsilo                                                  |
|                    |                                                                            | --roll-currsilo-now                                                  |</p>
<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
</table>
| **cfg-utils** | Used to manipulate LCE Server configuration attributes that do not appear in the web UI. Tenable Support may ask you to perform administrative tasks with this utility. | **Note:** Each date must be given in YYYYMmmDD format. A range includes both “to” and “from” dates. Dates refer to tOrigin of contained events. The most commonly used actions are:  

- --help  
- --list-all  
- --like <case-ignored substring of K>  
- --describe <K>  
- --get <K>  
- --vlike <case-ignored substring of K>  
- --set-sv <K> <V>

To see the complete list of available actions, run:
```
cfg-utils --help
```

For information about configuring site policies related to user activity, see [Site Policies](#).

**Tip:** You can use `cfg-utils` to configure certificate-authenticated web UI logins. For more information, see [Certificate-Authenticated Web UI Logins](#). |
<p>| <strong>change-activeDb-location</strong> | Changes the root directory of the operational LCE datastore from the default. | <code>&lt;absolute path of new location&gt;</code> |
| <strong>change-tracelogs-location</strong> | Changes the root directory of the LCE tracelogs from the default. | <code>&lt;absolute path of new location&gt;</code> |</p>
<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>create--make-current--silo</td>
<td>If silo rolling is inoperable, this utility can be used (with all LCE daemons stopped) to switch to a new silo.</td>
<td>&lt;siloNumber&gt;</td>
</tr>
<tr>
<td>check_fix_file_accessibility</td>
<td>Detects and fixes file accessibility problems like wrong ownership, wrong permissions, and inadvertently set immutable (“i”) extended file attribute. Normally, invoke with --normal.</td>
<td>--check-only</td>
</tr>
</tbody>
</table>
| ha-manager           | Configures, manages, or disables high availability. For more information about high availability configurations, see [High Availability](). | --initialize-as-master <standbyIP> <i/f> <virtualIP>  
--initialize-as-standby <masterIP> <i/f> <virtualIP>  
--copy-SSH-keys-to-peer  
--status  
--disconnect  
--de-configure |

For more information, see:

- Configure High Availability
- Monitor Your High Availability Configuration
- Disable High Availability
<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
</table>
| import_logs                 | Imports a directory of log files or a list of one or more logs on disk into the active database on the LCE server. You must specify whether the logs you are importing are encoded as ASCII (--ASCII) or UTF-8 (--UTF8). | --ASCII | --UTF8  
|--now-as-timestamp | --may-guess-timestamp | [--minimum-timestamp-epoch <N>]  
|--maximum-timestamp-epoch <N>]  
|--no-eval-event-rules]  
<inputFileAbsolutePath> |
|                            | For more information about import_logs usage, see Import LCE Data Manually. |                                                                      |
| install-PostgreSQL-man-pages | For the description and usage, see install-PostgreSQL-man-pages.             |                                                                      |
| lce_crypto_utils            | Used to generate and manipulate SSL credential files in the /opt/lce/credentials/syslog and /opt/lce/credentials/web_UI directories. | --generate-creds-cryptSyslog [CA_dnSpec>[endEntity_dnSpec>]  
(NB: any prior contents of /opt/lce/credentials/syslog/ will be erased.)  
--generate-creds-vulnReporter [-q]  
(Will prompt for cert generation parameters, unless -q.)  
(NB: any prior contents of /opt/lce/reporter/ssl/ will be erased.)  
--generate-creds-webUI [-q]  
(Will prompt for cert generation parameters, unless -q.)  
(NB: any prior contents of /opt/lce/credentials/web_UI/ will be erased.)  
--is-signed-by <endEntity_cert_path>.pem <CA_cert_path>.pem |
<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>--is-revoked-per &lt;endEntity_cert_path&gt;.pem &lt;CRL_path&gt;.pem</td>
</tr>
<tr>
<td></td>
<td></td>
<td>--save-as-PKCS12 &lt;endEntity_cert_path&gt;.pem &lt;endEntity_privkey&gt;.pem &lt;into_path&gt;.pfx (Will prompt for password, and again to confirm.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>--print-cert &lt;endEntity_cert_path&gt;.pem</td>
</tr>
<tr>
<td></td>
<td></td>
<td>--print-CRL &lt;CRL_path&gt;.pem</td>
</tr>
<tr>
<td></td>
<td></td>
<td>--print-privkey &lt;privkey_path&gt;.pem</td>
</tr>
<tr>
<td></td>
<td></td>
<td>--print-PKCS12 &lt;PKCS12_path&gt;.pfx (Will prompt for password.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>--what-is &lt;path&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A &lt;dnSpec&gt; is a ,,-separated list of K=V pairs, all optional save the last; \escape as needed: 'C=&lt;country&gt;,ST=&lt;state&gt;,L=&lt;city&gt;,O=&lt;org&gt;,OU=&lt;-orgUnit&gt;,CN=&lt;name&gt;'</td>
</tr>
<tr>
<td>Tool</td>
<td>Description</td>
<td>Usage</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>sendmail</td>
<td>a sendmail compatible interface.</td>
<td>an smtp host, username, password, and port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td># msmt <a href="mailto:recipient@domain.com">recipient@domain.com</a></td>
</tr>
<tr>
<td>online-pg-backup</td>
<td>Allows you to take an online backup of the PostgreSQL database that contains LCE events and part of the LCE control state.</td>
<td>For more information about online-pg-backup, see:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <a href="#">Perform an Online PostgreSQL Backup</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <a href="#">Restore an Online PostgreSQL Backup</a></td>
</tr>
<tr>
<td>openssl-utils.sh</td>
<td>Used to generate and view self signed CA certificates in .pem format when troubleshooting issues with Tenable Support.</td>
<td>--generate-CA-creds <code>&lt;CA_dnSpec&gt;</code> <code>&lt;into_dir&gt;</code> <code>[&lt;certSpec&gt;]</code> (NB: any prior contents of <code>&lt;into_dir&gt;</code> will be erased!!)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>--generate-creds <code>&lt;hostSpec&gt;</code> <code>&lt;dnSpec&gt;</code> <code>&lt;into_dir&gt;</code> <code>&lt;CAcreds_dir&gt;</code> <code>[&lt;certSpec&gt;]</code> (NB: any prior contents of <code>&lt;into_dir&gt;</code> will be erased!!)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>--is-signed-by <code>&lt;cert_path&gt;.pem</code> <code>&lt;CA_cert_path&gt;.pem</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>--revoke <code>&lt;cert_path&gt;.pem</code> <code>&lt;CAcreds_dir&gt;</code> <code>&lt;CRL_path&gt;.pem</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>--save-as-PKCS12 <code>&lt;endEntity_cert_path&gt;.pem</code> <code>&lt;endEntity_privkey&gt;.pem</code> <code>&lt;into_path&gt;.pem</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>--print-cert <code>&lt;cert_path&gt;.pem</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>--print-CRL <code>&lt;CRL_path&gt;.pem</code> <code>[&lt;CA_cert_path&gt;.pem]</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>--print-PKCS12 <code>&lt;PKCS12_path&gt;.pfx</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>A <code>&lt;hostSpec&gt;</code> is: <code>&lt;host_DNS_name&gt;</code> <code>&lt;host_IP&gt;</code>; IP can be IPv4 or IPv6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A <code>&lt;dnSpec&gt;</code> is: ,,-separated list of K=V pairs, all optional save the last; \-escape as needed:</td>
</tr>
</tbody>
</table>

**Note:** This tool relies on the external openssl binary, not distributed with LCE but available as part of the OpenSSL RPM.

**Tip:** This tool is intended for troubleshooting with Tenable Support. Otherwise, use the lce_crypto_utils tool.
<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>C=&lt;country&gt;,ST=&lt;state&gt;,L=&lt;city&gt;,O=&lt;org&gt;,OU=&lt;-orgUnit&gt;,CN=&lt;name&gt;</td>
<td></td>
<td>'A &lt;certSpec&gt; is: &lt;days_to_expiry&gt; --rsa</td>
</tr>
<tr>
<td>Tool</td>
<td>Description</td>
<td>Usage</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>policies</td>
<td></td>
</tr>
<tr>
<td></td>
<td>plugins</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IDS signatures</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cronjob definitions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSH keys</td>
<td></td>
</tr>
<tr>
<td></td>
<td>daemon initscripts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Text search stopwords</td>
<td></td>
</tr>
<tr>
<td>port-controlfiles</td>
<td>can be used to assist in moving an LCE instance from one host to another.</td>
<td></td>
</tr>
</tbody>
</table>
| query-plan-explainer | A convenient wrapper around the PostgreSQL EXPLAIN command, making its output both more concise and better readable. | ```bash
[--estimate-only] <sqlFile> | "SQL query"
``` |
| send_syslog           | Sends syslog messages to one or more servers.                                | ```bash
# /opt/lce/tools/send_syslog (server address 1) [...] [server address N] -message "(message)"
[ -port <port num>]  
[ -priority #]
``` |
<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>start-all</td>
<td>Starts PostgreSQL daemon and all LCE daemons.</td>
<td><code># /opt/lce/tools/start-all</code></td>
</tr>
<tr>
<td>restart-all</td>
<td>Without <code>bar-pg</code>, restarts the LCE daemons and PostgreSQL.</td>
<td><code># /opt/lce/tools/restart-all [bar-pg]</code></td>
</tr>
<tr>
<td></td>
<td>With <code>bar-pg</code>, only restarts the LCE daemons.</td>
<td></td>
</tr>
<tr>
<td>stop-all</td>
<td>Without <code>bar-pg</code>, stops the LCE daemons and PostgreSQL.</td>
<td><code># /opt/lce/tools/stop-all [bar-pg]</code></td>
</tr>
<tr>
<td></td>
<td>With <code>bar-pg</code>, only stops the LCE daemons.</td>
<td></td>
</tr>
<tr>
<td>timestamp Formats.txt</td>
<td>Used to identify the timestamp formats that appear for event timestamps in logs imported by <code>import_logs</code>. By default, this file includes a list of date formats.</td>
<td>If you are importing logs with timestamps in formats that are not included in this file, you can append the new formats to the list.</td>
</tr>
<tr>
<td>Tool</td>
<td>Description</td>
<td>Usage</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>toggle-augmented-event-lookups</td>
<td>LCE Server maintains several special database lookups to improve query performance. These lookups incur a cost in [a] computing resources to build, and [b] disk space once built. If your queries involve the database column(s) to which a particular lookup is devoted, the benefit is well worth the cost; if not, disabling that lookup will save disk space.</td>
<td>--add-lookup</td>
</tr>
<tr>
<td>ts-test</td>
<td>Used to check how a particular log would be tokenized for the purpose of text search indexing and whether a particular text search phrase would match it.</td>
<td>[--detail-spaces] &lt;rawDocument&gt; [&lt;tsQuery_inclStopwords&gt;] or &lt;path to file with rawDocument&gt; [&lt;tsQuery_inclStopwords&gt;]</td>
</tr>
</tbody>
</table>

Note: Use only at direction of Tenable Support.

To translate a showids +text search expression to a tsQuery expression, use /opt/lce/daemons/lce_queryd --translate-
<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>Usage</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter-on-rawlog</td>
<td></td>
<td>filter-on-rawlog &lt;showidsSearchExpr&gt;</td>
<td>For more information, see ts-test.</td>
</tr>
<tr>
<td>validate-PRM-regex</td>
<td>To test matching, using exactly the same regex matching package, version, and settings, as used by the LCE engine.</td>
<td>&lt;PRM_reg.ex._line&gt; &lt;sample_log&gt;</td>
<td>For more information, see validate-prm-regex.</td>
</tr>
<tr>
<td>user-utils</td>
<td>Reset the password for one of the secured accounts used to login to an LCE Server instance from outside the instance's host, if the LCE UI is for some reason unavailable or an operator simply prefers a console interaction for the purpose.</td>
<td>--list-all</td>
<td><strong>Note:</strong> --set-password--WebUI-acct sets a temporary password and, if the user account was locked, unlocks the account. For more information about changing user passwords, see Change a User's Password. For more information about locked user accounts, see Locked User Accounts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>--lock--WebUI-acct &lt;username&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>--unlock--WebUI-acct &lt;username&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>--set-password--WebUI-acct &lt;username&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>--replace--vuln_reporter-acct &lt;username&gt;</td>
<td><strong>Note:</strong> --replace--vuln_reporter-acct removes an existing account and sets a temporary password for the user. For more information about changing user passwords, see Change a User's Password.</td>
</tr>
</tbody>
</table>
install-PostgreSQL-man-pages

This utility leverages the Linux man-page facility to provide a full local copy of official documentation for all PostgreSQL utilities and SQL commands; in the same format as native GNU/Linux utilities. They need to run only once, and then can issue commands such as:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>man 1 pg_dump, man 1 pg_restore</td>
<td>Displays information about the PostgreSQL utilities for, respectively, export and import; these exact utilities are used by LCE’s archival-manager utility.</td>
</tr>
<tr>
<td>man 1 psql</td>
<td>Displays information about the PostgreSQL command-line client (see also source-for-psql-shortcuts.sh.)</td>
</tr>
<tr>
<td>man 1 pg_receivewal, man 1 pg_resetwal</td>
<td>Displays information about PostgreSQL built-in clustering/replication facilities.</td>
</tr>
<tr>
<td>man 7 SELECT</td>
<td>Displays information about the complete syntax of the SQL SELECT command, including any PostgreSQL extensions to the SQL: 2011 (ISO/IEC 9075:2011) standard.</td>
</tr>
<tr>
<td>man 7 CREATE_MATERIALIZED_VIEW</td>
<td>Displays information about the complete syntax of the DDL CREATE MATERIALIZED VIEW command, including any PostgreSQL extensions to the SQL: 2011 (ISO/IEC 9075:2011) standard.</td>
</tr>
<tr>
<td>man 7 CREATE_TEXT_SEARCH_CONFIGURATION, man 7 CREATE_TEXT_SEARCH_DICTIONARY, man 7 CREATE_TEXT_SEARCH_TEMPLATE</td>
<td>Displays information about syntax of commands used to configure the PostgreSQL full-text search feature.</td>
</tr>
</tbody>
</table>
The `ts-test` utility can tell you how PostgreSQL would parse a log and whether a given text search query matches that log.

Usage:

```text
<rawDocument> [<tsQuery_inclStopwords>]
```

or

```text
<path to file with rawDocument> [<tsQuery_inclStopwords>]
```

Example Output

If you invoke `ts-test` with a sample rawlog as the 1 arg, `ts-test` outputs a list of extracted terms and a detailed term extraction report table.

```text
'The LCE agent at 192.0.2.10 [sensor: unknown] [type: networkmonitor v4.2.0.0] has been manually granted authorization to log in and send events to this LCE.'
```
In this example output, the top two rows indicate the following:

- Token "The" was rejected by the human_language_rejecter.
- Token "" was rejected because our config rejects the entire "Space symbols" category.

**Tip:** Use the `--detail-spaces` option to show this information in the `ts-test` report.

- Token "LCE" was rejected by whole_word_rejecter.

If you provide a query string (for example, 'Authorization'), `ts-test` indicates whether that query string matches the sample rawlog:
The LCE agent at 192.0.2.10 [sensor: unknown] [type: networkmonitor v4.2.0.0] has been manually granted authorization to log in and send events to this LCE. 'Authorization'

To see an example of match failure, provide a nonsense query string (for example, 'Bunnies?').

The LCE agent at 192.0.2.10 [sensor: unknown] [type: networkmonitor v4.2.0.0] has been manually granted authorization to log in and send events to this LCE. 'Bunnies?'
validate-prm-regex

The /opt/lce/tools/validate-PRM-regex utility uses the same pattern matching library and parameters as the LCE engine. Tenable recommends using this tool to test your plugins.

validate-PRM-regex takes two arguments:

```plaintext
<PRM_reg.ex._line> <sample_log>
```

**Note:** As the regex argument, validate-PRM-regex accepts either an entire directive line (i.e. `regex=regexExpression` or `regexi=regexExpression`) exactly as it would appear in a .prm file; or just the `regexExpression`. In the latter case, it behaves as if `regexExpression` were prefixed by `regex=.`.

**Note:** While you can and should feed validate-PRM-regex complete sample logs for final testing, log fragments are fine when developing.

**Note:** Enclose each argument in single quotes to protect from shell interpretation.

Example Output

Log Matched, Extracted 1 or More Substrings

```plaintext
validate-PRM-regex 'DstPort \{d\{1,5\} } ' with DstPort 55555 %'
```

Log matched, extracted 1 substring:

```
$1: [55555]
```

Log Matched, No Substrings Extracted

```plaintext
validate-PRM-regex 'DstPort \d\{1,5\} ' with DstPort 55555 %'
```

Log matched, no substrings extracted.

**Tip:** Enclose the subpattern you want to extract in parentheses to make it a capturing subpattern.

Log Not Matched
validate-PRM-regex 'DstPort (\d{1,5})' 'with DstPort % 55555'

Log not matched.

Invalid Regex

validate-PRM-regex 'DstPort (\d{1,5})' 'with DstPort 55555 %'

Tip: The error message printed above may help to figure out what is wrong with the regex. In this example, exactly as the error message says, the closing delimiter ) was missing.
Perform an Online PostgreSQL Backup

**Caution:** If you have configured high availability, do not perform an online backup at the standby node. For more information about high availability configurations, see [High Availability](#).

You can use the `online-pg-backup` utility to perform an online backup of the PostgreSQL that contains LCE events and part of the LCE control state. Online backups can be created while LCE and PostgreSQL are running.

The control state `online-pg-backup` saves does not include all control files, such as policies or plugins. To save all control files, use the `port-controlfiles` utility.

Before you begin:

- If this is the first time you are using the `online-pg-backup` utility, in the command line interface (CLI) in LCE, run the following command to restart PostgreSQL and all LCE daemons:

  ```
  online-pg-backup --one-time-backup-prep
  ```

  PostgreSQL and all LCE daemons restart.

To create an online PostgreSQL backup:

1. Log in to LCE via the command line interface (CLI).
2. In the CLI in LCE, run the following command:

   ```
   online-pg-backup --backup-to <full path of directory>
   ```

   PostgreSQL creates the backup files.

   **Note:** This step may take 10-45 minutes to run, depending on the size of the backup file (10-20% of activeDb's size at the time backup was taken). Creating online backup files does not cause LCE or PostgreSQL downtime.

What to do next:

- (Optional) Restore the backup file, as described in [Restore an Online PostgreSQL Backup](#).
**Restore an Online PostgreSQL Backup**

**Caution:** If you have configured high availability, do not restore an online backup to the master node or the standby node. For more information about high availability configurations, see [High Availability](#).

You can use the `online-pg-backup` utility to restore an online PostgreSQL backup to a standalone LCE server node.

**Note:** Restoring an online backup completely replaces the PostgreSQL database. This may result in 10-45 minutes of downtime, depending on the size of the backup files.

Before you begin:

- Perform an online PostgreSQL backup, as described in [Perform an Online PostgreSQL Backup](#).

To restore an online PostgreSQL backup to a standalone LCE node:

1. Log in to LCE via the command line interface (CLI).
2. In the CLI in LCE, run the following command:
   
   ```
   online-pg-backup --restore-from <full path of directory>
   ```

   LCE restores the backup file.
   
   PostgreSQL restarts.
Site Policies

You can specify the following site policies related to user activity using the `cfg-utils` utility:

- **Audit Log Policy**
- **Password Format Policy**
- **Password Reuse Policy**
- **Login Session Policy**

To configure a setting for any of the following policies, run:

```
/opt/lce/tools/cfg-utils --set-sv <configuration attribute> '<value>'
```

For more information about the `cfg-utils` utility and its usage, see `cfg-utils`.

Audit Log Policy

You can configure the audit log policy to choose what user activities are logged, how often audit log backups are created, and whether the audit log is updated in real time.

You can view the complete audit log at any time by running `user-utils --print-audit-log`. For more information about the `user-utils` utility, see `user-utils`.

By default, LCE tracks the following user activities in the audit log:

- account administration, such as adding and unlocking accounts
- session-scope actions with failure outcome, such as login failures or users logged out involuntarily

<table>
<thead>
<tr>
<th>Configuration Attribute</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| web_UI_account__audit_session_everything | false | If enabled, LCE tracks the following additional activities:  
- session-scope actions with success outcome (logged in, logged out) |
• session tokens management actions (created token, destroyed token, ...)

<table>
<thead>
<tr>
<th>Configuration Attribute</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>audit_log__backup_destination_directory</td>
<td>none</td>
<td>If a directory is specified, LCE saves the entire audit log to a file every audit_log_backup__interval__days days.</td>
</tr>
<tr>
<td>audit_log__backup_interval__days</td>
<td>7</td>
<td>In days, sets how frequently LCE saves the audit file to the directory you specify using audit_log__backup_destination_directory.</td>
</tr>
<tr>
<td>audit_log__notify_updates</td>
<td>false</td>
<td>If enabled, LCE writes each audit log entry to the host’s syslog as it is created in real time. Site administrators can use this setting to receive notifications of new audit log entries.</td>
</tr>
</tbody>
</table>

Password Format Policy

You can configure the password format policy to customize user password requirements.

<table>
<thead>
<tr>
<th>Configuration Attribute</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>web_UI__password__minimum_length</td>
<td>4</td>
<td>Specifies the minimum number of characters that must be used when creating user passwords.</td>
</tr>
<tr>
<td>web_UI__password__enforce_complexity</td>
<td>false</td>
<td>When enabled, user passwords must contain at least one of each of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• An uppercase letter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A lowercase letter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A numerical character</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A special character</td>
</tr>
</tbody>
</table>
Password Reuse Policy

You can configure the password reuse policy to specify how long passwords can be used, how frequently the same password can be reused, and how much new passwords must differ from previously-used passwords.

<table>
<thead>
<tr>
<th>Configuration Attribute</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>web_UI__password__min-imum__lifetime__hours</td>
<td>0</td>
<td>Specifies the number of hours a user must wait before changing their password after the last non-administrative password change.</td>
</tr>
<tr>
<td>web_UI__password__max__lifetime__days</td>
<td>0</td>
<td>Specifies how frequently users must change their passwords. If a user has not changed their password before the specified number of days, the user account locks automatically. For more information, see Locked User Accounts.</td>
</tr>
<tr>
<td>web_UI__password__fewest__changes__ere__reuse</td>
<td>1</td>
<td>Specifies how frequently users can re-use the same password. By default, users cannot use the same password twice in a row. For example, if the value is set to 2, the user must use two other unique passwords before using the same password again.</td>
</tr>
<tr>
<td>web_UI__password__minimum__edit__distance</td>
<td>0</td>
<td>When set, requires new passwords to differ from previous passwords based on the edit distance value specified. New passwords must have at least x characters that differ from the previous password.</td>
</tr>
</tbody>
</table>

Login Session Policy

You can configure the login session policy to specify when user accounts are locked due to failed login attempts, set the maximum number of concurrent sessions per user, and set user accounts to be locked or logged out following a period of inactivity.
For more information about locked user accounts, see [Locked User Accounts](#).

<table>
<thead>
<tr>
<th>Configuration Attribute</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>web_UI__login__max_failures_during_window</td>
<td>0</td>
<td>Specifies the number of times a user can attempt to log in during the window specified by <code>web_UI__login__failure_window_size__minutes</code> before their account is locked.</td>
</tr>
<tr>
<td>web_UI__login__failure_window_size__minutes</td>
<td>15</td>
<td>Specifies the login window during which users will have <code>web_UI__login__max_failures_during_window</code> chances to try logging in before their account is locked.</td>
</tr>
<tr>
<td>web_UI__login__max_concurrent_sessions</td>
<td>5</td>
<td>Specifies the maximum number of concurrent login sessions per user.</td>
</tr>
<tr>
<td>web_UI__account__lock__if_inactive__hours</td>
<td>0</td>
<td>When set, LCE locks the account of any user who has not been active (logged in an interacting with the LCE web UI) in the specified number of hours.</td>
</tr>
<tr>
<td>webserver__idle_session_timeout__minutes</td>
<td>60</td>
<td>Specifies the number of minutes a user can be idle before being automatically logged out.</td>
</tr>
</tbody>
</table>

If `web_UI__login__max_failures_during_window > 0`, LCE will automatically lock (see [About Locked Accounts section](#)) the account of any user who has attempted but failed to log in `web_UI__login__max_failures_during_window` times in a `web_UI__login__failure_window_size__minutes` period.
Rotate Web UI Credentials

You can use the `lce_crypto_utils` utility to rotate your user credentials for the LCE web UI. For more information about the `lce_crypto_utils` utility, see `lce_crypto_utils`.

**Note:** These credentials only apply to users logging in the LCE web UI and not to uploading of vulnerability reports to Tenable.sc.

To rotate web UI credentials:

1. Log in to LCE via the command line interface (CLI).
2. In the CLI in LCE, run the following command:

   ```
   /opt/lce/credentials/web_UI/opt/lce/tools/lce_crypto_utils --generate-creds-webUI
   ```

   LCE rotates your web UI credentials.
Encryption Strength

LCE uses the following default encryption for storage and communications.

<table>
<thead>
<tr>
<th>Function</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storing user account passwords</td>
<td>SHA-512 and the PBKDF2 function</td>
</tr>
</tbody>
</table>
Configure TLS Strong Encryption

You can configure TLS strong encryption for LCE-client communications to meet the security needs of your organization. LCE uses TLS 1.2 to encrypt LCE-client communications. For more information about LCE encryption, see Encryption Strength.

To configure TLS strong encryption for LCE communications:

1. Log in to LCE via the command line interface (CLI).
2. In the CLI in LCE, run the following command to specify the cipher you want to use for TLS encryption:

```
source /opt/lce/tools/exigent-sessions.bashrc
undoc-config --set lced cryptSyslog_ciphersuiteSelector <cipher you want to use for TLS encryption>
```

For example:

```
source /opt/lce/tools/exigent-sessions.bashrc
```

3. Run the following command to restart all LCE daemons:

```
restart-all bar-pg
```

All LCE daemons restart.
Configure LCE for NIAP Compliance

If your organization requires your instance of LCE to meet National Information Assurance Partnership (NIAP) standards, you can configure relevant settings to be compliant with NIAP standards.

You must run LCE 6.0.6 to configure LCE for NIAP compliance.

For more information about LCE storage and communications encryption, see Encryption Strength. For more information about data gathered by the LCE Client, see LCE Clients.

Before you begin:

- Confirm you have enabled the full disk encryption capabilities provided by the operating system on the host where LCE is installed.
- Contact Tenable Support for access to the following required script file:
  - LCE-NIAPcompliance-Oct29-fixerPkg.tgz

To configure LCE for NIAP compliance:

1. As the root user, in the command line interface (CLI) in LCE, run the following command to create a new directory for the script file:

   ```
   mkdir /path/to/fixer29/
   ```

2. Run the following commands to download the script file into the directory you created:

   ```
   cp /path/to/download/LCE-NIAPcompliance-Oct29-fixerPkg.tgz /path/to/fixer29
   ```

3. Run the following command to navigate to the fixer29 directory:

   ```
   cd /path/to/fixer29
   ```

4. Run the following command to extract the script:

   ```
   tar zxf LCE-NIAPcompliance-Oct29-fixerPkg.tgz
   ```
5. Run the following command to start LCE-NIAPcompliance-Oct29-fixer:

```
./LCE-NIAPcompliance-Oct29-fixer
```

6. Run the following commands to enable NIAP-compliant settings:

```
./opt/lce/tools/exigent-sessions.bashrc
enable_NIAP_Mode
```

LCE restarts.

LCE secures communications with TLS 1.2 and the following cipher suites: ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-SHA384, or ECDHE-RSA-AES256-GCM-SHA384.

**Note:** Enabling NIAP mode encrypts communications for the following:
- Receiving the encrypted TCP syslog. For more information, see [Receiving Encrypted Syslog](#).
- Sending vulnerability reports to Tenable.sc.
- Downloading plugin updates.
- Web UI server and desktop browser.

7. (Optional) Run the following commands to view your NIAP settings and enabled cipher suites:

```
undoc-config --get wwwd NIAP_COMPLIANT
```

8. If you connect LCE to Tenable.sc, you must use certificates to authenticate the connection.
   For more information, see [Manual Key Exchange with Tenable.sc](#).
**File and Process Allow List**

If you use third-party endpoint security products such as anti-virus applications and host-based intrusion and prevention systems, you should add LCE to the allow list.

The following tables list the LCE Server and LCE Client folders, files, and processes that should be allowed.

### LCE Server

<table>
<thead>
<tr>
<th>LCE Server</th>
<th>Folders</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>/opt/lce/*</td>
</tr>
<tr>
<td></td>
<td>/opt/lce/admin/log/*</td>
</tr>
<tr>
<td></td>
<td>/opt/lce/db/*</td>
</tr>
<tr>
<td></td>
<td>/tmp/*</td>
</tr>
<tr>
<td></td>
<td>/tmp/download surge_domains</td>
</tr>
<tr>
<td></td>
<td>/tmp/download surge_files</td>
</tr>
<tr>
<td></td>
<td>/tmp/user_tracking_day</td>
</tr>
<tr>
<td></td>
<td>/tmp/sw_tracking_day</td>
</tr>
<tr>
<td></td>
<td>/tmp/threatlist.tmp</td>
</tr>
<tr>
<td></td>
<td>/tmp/threaturl.tmp</td>
</tr>
<tr>
<td></td>
<td>/tmp/usb_tracking_day</td>
</tr>
<tr>
<td></td>
<td>/etc/logrotate.d/lce</td>
</tr>
<tr>
<td></td>
<td>/etc/keepalived/keepalived.conf</td>
</tr>
<tr>
<td></td>
<td>/etc/sysconfig/keepalived</td>
</tr>
<tr>
<td>Directory</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>/etc/systemd/system/keepalived.service</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/systemd/system/keepalived.service</td>
<td></td>
</tr>
<tr>
<td>/var/run/keepalived</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/firewalld/services/lce-server.xml</td>
<td></td>
</tr>
<tr>
<td>/etc/init.d/</td>
<td></td>
</tr>
<tr>
<td>/var/log/subsys/</td>
<td></td>
</tr>
<tr>
<td><strong>Files</strong></td>
<td></td>
</tr>
<tr>
<td>/opt/lce/tools/optimize-datastore</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/tools/cache-filter-pointers</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/diag</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/showids</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/tasl</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/daemons/lce_client_manager</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/postgresql/bin/pg_basebackup</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/postgresql/bin/pg_ctl</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/postgresql/bin/pg_dump</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/postgresql/bin/pg_isready</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/postgresql/bin/pg_restore</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/postgresql/bin/pg_rewind</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/postgresql/bin/psql</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/tools/archival-manager</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/tools/check_fix-file_accessibility</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/tools/cfg-utils</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/tools/fwd-silo-cksum</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/tools/ha-manager</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/tools/msmtp</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/tools/restart-all</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/tools/send_syslog</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/tools/start-all</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/tools/stop-all</td>
<td></td>
</tr>
<tr>
<td>/opt/lce/tools/user-utils</td>
<td></td>
</tr>
</tbody>
</table>

### Processes

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt/lce/daemons/lced</td>
</tr>
<tr>
<td>/opt/lce/daemons/ice_queryd</td>
</tr>
<tr>
<td>/opt/lce/daemons/ice_report_proxyd</td>
</tr>
<tr>
<td>/opt/lce/daemons/ice_wwwd</td>
</tr>
<tr>
<td>/opt/lce/daemons/ice_tasld</td>
</tr>
<tr>
<td>/opt/lce/daemons/stats</td>
</tr>
<tr>
<td>/opt/lce/postgresql/bin/postgres</td>
</tr>
<tr>
<td>/opt/lce/ha/keepalived</td>
</tr>
</tbody>
</table>

### LCE Clients

#### Tenable NetFlow Monitor

<table>
<thead>
<tr>
<th>Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt/netflow_monitor/</td>
</tr>
<tr>
<td>/etc/init.d/netflow_monitor</td>
</tr>
<tr>
<td>Processes</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td><strong>Tenable Network Monitor</strong></td>
</tr>
<tr>
<td>Folders</td>
</tr>
<tr>
<td>(Linux only) /opt/network_monitor/</td>
</tr>
<tr>
<td>(FreeBSD only) /usr/local/network_monitor</td>
</tr>
<tr>
<td>/etc/init.d/network_monitor</td>
</tr>
<tr>
<td>Processes</td>
</tr>
<tr>
<td>tnmd</td>
</tr>
<tr>
<td><strong>OPSEC Client</strong></td>
</tr>
<tr>
<td>Folders</td>
</tr>
<tr>
<td>/opt/lce_opsec/*</td>
</tr>
<tr>
<td>/etc/init.d/lce_opsec</td>
</tr>
<tr>
<td>Files</td>
</tr>
<tr>
<td>lce_query_opsec</td>
</tr>
<tr>
<td>Processes</td>
</tr>
<tr>
<td>lce_opsed</td>
</tr>
<tr>
<td><strong>Tenable RDEP Monitor</strong></td>
</tr>
<tr>
<td>Folders</td>
</tr>
<tr>
<td>/opt/rdep_monitor/</td>
</tr>
<tr>
<td>/etc/init.d/rdep_monitor</td>
</tr>
<tr>
<td>Processes</td>
</tr>
<tr>
<td>Service</td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td><strong>Tenable SDEE Monitor</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Splunk Client</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>LCE Client for Linux</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### Ice_clientd

<table>
<thead>
<tr>
<th><strong>LCE Client for Windows</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Folders</strong></td>
</tr>
<tr>
<td>C:\Program Data\Tenable\LCEClient</td>
</tr>
<tr>
<td>C:\Program Files\Tenable\LCEClient</td>
</tr>
<tr>
<td><strong>Files</strong></td>
</tr>
<tr>
<td>server_assignment.exe</td>
</tr>
<tr>
<td><strong>Processes</strong></td>
</tr>
<tr>
<td>Ice_client.exe</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Web Query Client</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Folders</strong></td>
</tr>
<tr>
<td>/opt/ice_webquery/*</td>
</tr>
<tr>
<td>/etc/init.d/ice_webquery</td>
</tr>
<tr>
<td><strong>Processes</strong></td>
</tr>
<tr>
<td>ice_webqueryd</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>WMI Monitor Agent</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Folders</strong></td>
</tr>
<tr>
<td>/opt/wmi_monitor/*</td>
</tr>
<tr>
<td>/etc/init.d/wmi_monitor</td>
</tr>
<tr>
<td><strong>Files</strong></td>
</tr>
<tr>
<td>wmi_config_credentials wmic</td>
</tr>
<tr>
<td><strong>Processes</strong></td>
</tr>
<tr>
<td>ice_wmid</td>
</tr>
</tbody>
</table>
Refresh or Replace the Vulnerability Reporter SSL Certificate

**Required User Role:** Administrator

To update the self-signed SSL certificate used to upload vulnerability reports to Tenable.sc, do one of the following:

- Rotate the self-signed SSL certificate, replacing it with a fresh self-signed certificate.
- Replace the self-signed SSL certificate packaged with LCE with an SSL certificate from your organization.

To rotate the self-signed SSL certificate and replace it with a fresh self-signed certificate:

1. Log in to LCE via the command line interface (CLI).
2. In the CLI in LCE, run the following command to refresh the SSL certificate:
   ```
   /opt/lce/tools/lce_crypto_utils --generate-creds-vulnReporter -q
   ```
   LCE regenerates the SSL certificate locally.
3. Re-add the LCE to Tenable.sc, as described in Add a Log Correlation Engine Server in the Tenable.sc User Guide.

To replace the SSL certificate used to upload vulnerability reports to Tenable.sc:

1. Copy the following files from your CA to /opt/lce/reporter/ssl/.
   - cacert.pem
   - servercert.pem
   - cakey.pem
   - serverkey.pem
   **Note:** Do not change the certificate file names.
2. Add the LCE to Tenable.sc, as described in Add a Log Correlation Engine Server in the Tenable.sc User Guide.
Import LCE Data Manually

LCE data can be collected both via real-time logging and manually in batch mode using the `import_logs` tool. These events will show up in the normalized event view along with events collected in real-time. This command-line tool allows data to be imported into the LCE that may not be available in real-time, but is still important for correlation of vulnerability data and for analysis of security posture and events.

Log files must be in ASCII format or UTF8, not binary, and each log must be delimited by a single newline.

**Note:** Event silos in the LCE activeDb may not overlap in respective time spans of contained events.

Usage:

```bash
# /opt/lce/tools/import_logs
--ASCII | --UTF8
[--now-as-timestamp | --may-guess-timestamps]
[--minimum-timestamp-epoch <N>]
[--maximum-timestamp-epoch <N>]
[--no-eval-event-rules]
<inputFileAbsolutePath>
```

The following table describes the options available for `import_logs`:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--no-eval-event-rules</td>
<td>Do not apply LCE event rules to imported logs.</td>
</tr>
<tr>
<td>--may-guess-timestamps</td>
<td>If no timestamp can be determined for an event, assign the most recent known timestamp.</td>
</tr>
<tr>
<td>--now-as-timestamp</td>
<td>Use the current system time for all imported logs rather than the timestamps contained within the event text.</td>
</tr>
</tbody>
</table>
Manual Key Exchange with Tenable.sc

A manual key exchange between Tenable.sc and the LCE is normally not required; however, in some cases where remote root login is prohibited or key exchange debugging is required, you will need to manually exchange the keys.

For the remote LCE to recognize Tenable.sc, you need to copy the SSH public key of Tenable.sc and append it to the `/opt/lce/.ssh/authorized_keys` file on the LCE server. The `/opt/lce/daemons/lce-install-key.sh` script performs this function.

**Note:** The LCE server must have a valid license key installed and the LCE daemon must be running before performing the steps below.

To manually exchange the keys with Tenable.sc:

1. In Tenable.sc, download the Tenable.sc key, as described in [Download the Tenable.sc SSH Key](#) in the *Tenable.sc User Guide*. Both DSA and RSA formats work for this process.

2. Save the key file (SSHKey.pub) to your local workstation. Do not edit the file or save it to any specific file type.

3. From the workstation where you downloaded the key file, use a secure copy program, such as “scp” or “WinSCP” to copy the SSHKey.pub file to the LCE system. You will need to have the credentials of an authorized user on the LCE server to perform this step. For example, if you have a user “bob” configured on the LCE server (hostname "lceserver") whose home directory is `/home/bob`, the command on a Linux or Unix system would be as follows:

   ```
   # scp SSHKey.pub bob@lceserver:/home/bob
   ```

4. After the file is copied to the LCE server, in the command line interface (CLI), run the following command to move the file to `/opt/lce/daemons`:

   ```
   # mv /home/bob/SSHKey.pub /opt/lce/daemons
   ```

5. On the LCE server, as the root user, run the following command to change the ownership of the SSH key file to "Ice":

   ```
   # chown lce /opt/lce/daemons/SSHKey.pub
   ```
6. Run the following command to append the SSH public key to the "/opt/lce/.ssh/authorized_keys" file:

```bash
# su lce
# /opt/lce/daemons/lce-install-key.sh /opt/lce/daemons/SSHKey.pub
```

7. To test the communication, as tns user on the Tenable.sc system, attempt to run the id command:

```bash
# su tns
# ssh -C -o PreferredAuthentications=publickey lce@<LCE-IP> id
```

- If a connection has not been previously established, you will see a warning similar to the following:

```
The authenticity of host '192.168.15.82 (192.168.15.82)' can't be established. RSA key fingerprint is 86:63:b6:c3:b4:3b:ba:96:5c:b6:d4:42:b5:45:37:7f. Are you sure you want to continue connecting (yes/no)?
```

Answer “yes” to this prompt.

- If the key exchange worked correctly, a message similar to the following will be displayed:

```
# uid=251(lce) gid=251(lce) groups=251(lce)
```

8. You can add the IP address of Tenable.sc to the LCE system’s /etc/hosts file. This prevents the SSH daemon from performing a DNS lookup that can add seconds to your query times.

9. Add the LCE to Tenable.sc, as described in Add a Log Correlation Engine Server in the Tenable.sc User Guide.
User Tracking

The LCE server has a feature that is designed to track users. User tracking can be applied to any event coming into the LCE server, regardless of the source of the event. Events correlated from Windows, Linux, Unix, or other network devices can be monitored.

When LCE encounters a log that has no username field, it will assign the username of the user most recently associated with the source IP of the incoming log, or associated with the destination IP of the log if a destination IP (dstip) is provided but a source IP (srcip) is not. If no user was previously tracked at either of the IPs, or if no IP is provided, an "(unknown)" entry is assigned.

When a user changes IP addresses (i.e., a LCE receives a log where the user’s srcip differs from the srcip in the previous log tagged with the username), the new IP address is also associated with the user. The last three IP addresses per user are stored for the user, allowing for cases where a single user logs into multiple systems at the same time. For example, the following event shows a user becoming active at a new IP address:

| Network user IP address change: user someguy94 became active at 169.254.96.232 with event login (169.254.96.232:0) |

The data used to track usernames is stored in the files usernames.txt, ip_user.dat, and user_ip.dat in the LCE database directory. The .dat files are written when the LCE service is shut down gracefully. In case of a server crash, the data is automatically backed up every 10 minutes.

A maximum of 65,534 unique usernames can be stored. If the maximum is reached, incoming logs with new users will have the user fields marked with the "(unknown)" entry.

User tracking in LCE will function if the following conditions are met:

- The LCE server has plugins that can match the events and pull usernames from the events. For example, plugin 3209 in os_win2k_sec.prm has the following line:

  `log-event:Windows-Account_Used_For_Login sensor:$1 dstip:$2 type:login user:$4 event2:WindowsEvent-680`

  The user:$4 directive tells the plugin to add the username to the available event searchable fields. As a result, searches that query this event based on the username will return results.
• The plugin IDs have been added to the **User Tracking Plugins** in the **User Tracking** section in the configuration section of the LCE interface (one plugin ID per line).

  **Note:** A list of the plugins provided by Tenable that include user information is found at the end of `/opt/lce/daemons/plugins/prm_map.prm`.

• The user tracking settings have been properly configured in the LCE interface under “User Tracking”. Please refer to the Advanced Configuration Options section of this document for a description of the following applicable keywords:

  - `accept-letters`
  - `accept-numbers`
  - `additional-valid-characters`
  - `max-username-characters`

If these conditions are not met, usernames may still be stored in normalized events; however, they cannot be searched using the event filter `username` parameter. Another way to search for usernames in logs is through the raw log search feature of Tenable.sc.
Non-Tenable License Declarations

Below you will find the command that will list all the third-party software packages that Tenable provides for use with the Log Correlation Engine. This command may be run at the command line interface by users with permissions to the lced binary.

```
# /opt/lce/daemons/lced -l
```

For a list of third-party software packages that Tenable utilizes with LCE, see Log Correlation Engine Third-Party Licenses.
Silo Archiving

Configuration

- Total size of activeDb is limited by config attribute `active-size` (default: 20 TB).
- Total size of archiveDb is limited by config attribute `archive-size` (default: 20 TB).

Control Flow

Every 2.5 minutes, LCE will:

1. Read in the results of the last-executed action, from LCE status database.
2. Choose the next action to take based on the last-executed action.
3. Perform the next action and store results in LCE status database.

Storing the state in this manner has the following advantages:

- simplicity (no separate logic to handle reloads/restarts is needed)
- transparency (to see exactly where the archival algorithm is, just query the LCE status database.)
- available emergency override (can alter the control flow by updating the LCE status database.)

**Note:** This is not standard operating procedure and should only be performed in very rare cases.

LCE waits a maximum of 60 minutes for an archive job to complete in order to avoid being stuck in the CheckArchiveDone state indefinitely in the rare case that PostgreSQL fails to report an archive job as complete.

**Note:** Archiving a silo normally takes 6 to 8 minutes.

Example `archival-manager --list-snapshots` Output
null