Log Correlation Engine 4.0 Client Guide

February 20, 2013

(Revision 5)

Table of Contents

Introduction

This document describes various different clients that are available for Tenable Network Security's **Log Correlation Engine 4.0**. Please email any comments and suggestions to support@tenable.com.

A working knowledge of Secure Shell (SSH), regular expressions, and SecurityCenter operation and architecture is assumed. Familiarity with general log formats from various operating systems, network devices and applications, as well as a basic understanding of Linux/Unix is also assumed.

This document describes the current LCE server (daemon) version of 4.0.x. The LCE Clients described are all version 4.0.x. Please refer to the Tenable Support Portal for the latest version of the LCE Client.

LCE 4.0.x clients are designed to connect to LCE 4.0.x servers. While some LCE 4.0.x clients may successfully be configured to work with LCE 3.x, this is not an officially supported configuration and some or all features may not work as expected.

This document is intended to be used with LCE Clients 4.0 and greater, however many of the concepts, with the prominent exception of those relating to the LCE Client Manager, apply to legacy versions of the LCE Clients. Clients prior to version 4.0 may connect to a LCE 4.0.x server using legacy configurations. Some of those legacy clients are alluded to in this document and will be detailed here as 4.x versions become available.

Standards and Conventions

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

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

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

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

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

Log Correlation Engine Client Overview

Throughout this document we will continually refer to three primary LCE components: the LCE Client (the end host that initially collects data and sends it on to the LCE server); the LCE server (or daemon), which is installed on Red Hat/CentOS and performs the bulk of the processing; and the LCE host (LCE Manager or SecurityCenter), which provides a graphical user interface to view and report on the LCE data.

The Log Correlation Engine (LCE) Clients are agents that 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. Once an LCE is installed and configured, one or more LCE Clients can be used to send information back for normalization and correlation.

This document details available LCE 4.0 Clients along with their installation and configuration.

Various versions of LCE Clients can be configured to gather information and events from the following sources:

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

Many of these agents are required to take advantage of the LCE's power. For example, to perform "Blacklist" correlation, the LCE Clients that monitor network traffic via sniffing or NetFlow can be used to identify connections with known hostile IP addresses even if you do not have firewall or proxy logs.

Running LCE Clients Directly on the LCE Server

LCE Clients can be run directly on the LCE server. They must be configured to connect to either the localhost (127.0.0.1) or the IP address of the LCE server. Multiple LCE Client types (such as a LCE Log Agent and a Tenable NetFlow Monitor) can be run at the same time as well. See the section titled "LCE Client Types and Platforms" for a list of available clients.

While using LCE Log Agents to watch LCE log files, be extremely careful to avoid feedback loops. For example, choosing to tail the **`lce.log`** file would cause any log saved by the **`lced`** process to be grabbed by the LCE Log Agent, sent back to **`lced`**, and repeated indefinitely.

Running Multiple LCE Clients on One Host

Remote systems can run multiple LCE Clients. When using the LCE Client Manager and LCE 4.0 clients, each client type is identified and managed appropriately upon connection to the LCE server.

Maximum Number of LCE Clients

A maximum of 8,192 individual LCE Clients can be connected simultaneously to the LCE server. Once 8,192 clients have connected, the LCE server will stop accepting new connections.

LCE Client Types and Platforms

There are a number of different LCE Client types available. All LCE Clients report performance statistics (memory, disk space, and CPU usage) on their host regardless of the platform.

The LCE Clients written for 32-bit platforms will run on 64-bit systems as long as the 32-bit libraries are installed. However, native 64-bit support is only available for certain platforms. See the table below for more details.

<table>
<tr><th>LCE Client</th><th>Platform</th><th>Architecture</th><th>Function</th></tr>
<tr><td rowspan="4">LCE Client (Log Agent)</td><td>RHEL/CentOS 5, 6</td><td>32/64-bit</td><td rowspan="4">Linux and Mac OS X Client:
Events sent encrypted to the LCE
Process accounting event monitoring
Directory and file tailing
File integrity and directory change monitoring
CPU, memory and disk statistics collection
Heartbeats
Windows Client:
Events sent encrypted to the LCE
Configurable Windows event log collection
Remote collection of Windows event logs via WMI
Collection of process execution through event log
Directory and file tailing
File integrity and directory change monitoring
USB insert and remove events
CD-ROM/DVD insert and remove events
CPU, memory and disk statistics collection
Heartbeats
The LCE Clients are designed to send log data to the LCE server. Accepted log data is normally in ASCII text format and will not include binary files (with the exception of process accounting data). The LCE Log Agents will check all data before sending, specifically omitting binary files such as <code>.zip</code>, <code>.gz</code>, <code>.tar</code>, <code>.lzh</code>, <code>.bz2</code>, etc. If a binary file is sent to the LCE, it has the potential to corrupt the database. This filtering is automatically performed by the LCE Client software.</td></tr>
<tr><td>Mac OS X</td><td>32/64-bit</td></tr>
<tr><td>MS Windows XP Professional, Server 2003</td><td>32-bit</td></tr>
<tr><td>MS Windows Server 2008, Vista, and Windows 7 Ultimate</td><td>32/64-bit</td></tr>
<tr><td>LCE WMI Monitor</td><td>RHEL/CentOS 5, 6</td><td>32/64-bit</td><td>Retrieves Windows Event Logs (e.g., System, Application, Security, All, etc.) from one or more Windows hosts using the Windows Management Instrumentation (WMI) protocol.</td></tr>
<tr><td rowspan="2">Tenable NetFlow Monitor</td><td>RHEL/CentOS 5, 6</td><td>32/64-bit</td><td rowspan="2">Receives NetFlow messages for logging to the LCE. Messages can be sent from multiple NetFlow sources to a single TNS_Netflow client. The client supports NetFlow versions 5 and 9.</td></tr>
<tr><td>FreeBSD 7, 8</td><td>32-bit</td></tr>
</table>

Tenable Network Monitor	RHEL/CentOS 5, 6	32/64-bit	Designed to monitor network traffic and send session information to the LCE server. Sniffs network traffic to identify TCP sessions as well as UDP, ICMP and IGMP activity. The Tenable Network Monitor also has a very useful feature of sniffing live **syslog** traffic in motion and sending it to the LCE as if the traffic were originally destined for it. This makes it very easy to centralize logs and not rely on forwarding of events from a different log server.
	FreeBSD 7, 8	32-bit	

Quick Start Summary

Use these steps to get your LCE Clients up and running quickly:

1. Install and configure the clients with the IP address or hostname and port of the LCE server as per the instructions in the Installing the LCE Linux Clients or Installing the Windows Client sections of this document. Make sure the client is started.

2. Using SecurityCenter or LCE Manager 4.6, or the LCE client manager on the LCE server, grant authorization and apply the appropriate configurations for the newly configured clients.

3. Exit the LCE Client Manager to save and apply the settings to the Policy Map.

Diagnosing Connection Problems

If the LCE Client cannot connect:

- View the most recent LCE Client log file located in **/opt/lce_client/** (or appropriate directory for the client in question) to determine if any error messages exist. The log has a file name in the following format: "**YearMon.log**".

- Check that the LCE server daemon is running and correctly licensed by running "**service lce status**". If the process is running, output similar to the following is displayed:

```
# service lce status
lced (pid 26868 26864) is running...
lce_queryd (pid 26876 26874) is running...
lce_indexerd (pid 26892) is running...
```

- Check to see if there is a local firewall, network firewall, or other network issue that would prevent connection from the LCE Client to the LCE server. To test this, run a sniffer on the LCE server monitoring TCP port 31300 (default port). If no connections are observed from the system running the LCE Client, something is blocking the connection. Running a sniffer on the system of the LCE Client may also help determine if something is blocking.

- If the LCE Client manager is being used to manage the affected client(s), confirm that the server has authorized the client(s) to connect.

- Verify that the passwords are correct. Both the LCE Client and LCE server will log failed authentication errors (pre-4.0 clients).

- Verify that the IP addresses of the LCE Client and LCE server are correct. The client will not connect to the LCE server if it has the wrong IP address or cannot correctly resolve the hostname, and the LCE server will not accept a random client unless it is specifically configured in the LCE Client Manager or **lce.conf** file (pre-4.0 clients).

LCE Manager and SecurityCenter Client Management

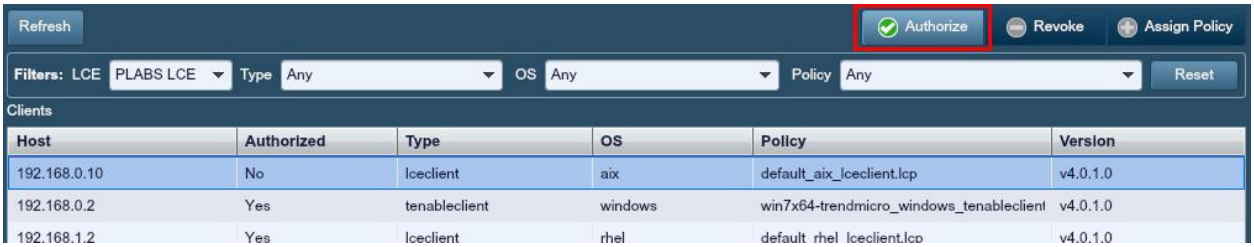
Starting with LCE Manager and SecurityCenter versions 4.6, authorization and revocation of client policies can be performed within the management GUIs. Support for policy creation and change is planned for future releases.

For example, if you have multiple LCE Clients installed on our network, the configuration files were set to point to one LCE Server when they were initially installed. The following screenshot shows that all LCE Clients have been authorized but one:

Host	Authorized	Type	OS	Policy	Version
192.168.0.10	No	lceclient	aix	default_aix_lceclient.lcp	v4.0.1.0
192.168.0.2	Yes	tenableclient	windows	win7x64-trendmicro_windows_tenableclient	v4.0.1.0
192.168.1.2	Yes	lceclient	rhel	default_rhel_lceclient.lcp	v4.0.1.0
192.168.2.2	Yes	lceclient	rhel	default_rhel_lceclient.lcp	v4.0.1.0
192.168.3.6	Yes	3.x Client	-	-	v3.x.x.x
192.168.7.9	Yes	3.x Client	-	-	v3.x.x.x

Default LCE policies are included in the LCE content feed. For information on how to customize policies for use within your organization, see the LCE Client Manager Command Line Options section later in this document.

To authorize a new client, highlight the entry and then click “Authorize”. Once a client has been authorized, the LCE Server can accept data from that client using the policy listed.



Host	Authorized	Type	OS	Policy	Version
192.168.0.10	No	lceclient	aix	default_aix_lceclient.lcp	v4.0.1.0
192.168.0.2	Yes	tenableclient	windows	win7x64-trendmicro_windows_tenableclient	v4.0.1.0
192.168.1.2	Yes	lceclient	rhel	default_rhel_lceclient.lcp	v4.0.1.0

To change a policy or revoke authorization, click on the appropriate buttons after highlighting the client(s) you wish to configure.

LCE Client Manager

The LCE Client Manger is used to manage clients of version 4.0 and higher to a LCE server 4.0 or higher. Previous clients may connect to the LCE server 4.0 and higher using the previous configuration method via the `lce.conf` configuration file.

The LCE Client Manager is a feature introduced in LCE 4.0 for use with all clients of version 4.0 and higher. This command line tool is used on the LCE server to manage the LCE Client access to the server and to manage the configuration files of the attached clients via policy files. The tool may be used in an interactive method or using command line options to facilitate scripting of some routine tasks that do not require a response.

The configurations are managed through the use of the Policy Map. The Policy Map contains a list of the managed clients and key information about them such as the IP address, assigned policy, client OS, and client type (log client, NetFlow, Network Monitor, WMI Monitor, etc.). When changes are made with the LCE Client Manager utility and saved, the Policy Map is reloaded with the new information and is ready for the LCE server to use without restarting the LCE server process.

All policy files (*.lcp) are stored on the LCE server in XML format in the **/opt/lce/daemons/policies** directory.

If clients are being upgraded, their configuration files may be imported as a policy file after conversion by the LCE Conf Converter.

Details for configuring policy files are included in their respective client type sections, described later in this document.

LCE Client Manager Interactive Mode

The tool is launched by an authorized user on the LCE server by running **/opt/lce/daemons/lce_client_manager** from the server command line. When run without any options (interactive mode), a menu is presented to guide the user in managing the clients.

```
# /opt/lce/daemons/lce_client_manager


*******************************************
* LCE Client Manager 1.0
* Please select an option from the menu below
*******************************************
 [g] Grant authorization to a client or clients to connect to LCE
 [r] Revoke a client or clients access to connect to LCE
 [d] Display clients by policy assignment
 [p] Display available policies
 [a] Add a new policy
 [c] Copy a policy
 [m] Modify an existing policy
 [s] Assign a policy to a client or clients
 [v] Assign a client or clients to a new LCE server
 [i] Import a file as a policy
 [n] Assign a custom sensor name to a client or clients
 [x] Remove a client
 [q] Exit


lce_client_manager >>
```

To select an option, enter the letter that corresponds with its description. As each option is selected, a submenu is offered that prompts for further information to complete the selected task.

[g] Grant Authorization to a Client

After a LCE Client is initially installed on a machine, configured to direct traffic to the LCE server, and started, the LCE Client Manager must authorize the connection. This is done by selecting the "**g**" option from the menu.

After selecting the "**g**" option from the menu, the user is asked a yes or no question to authorize all clients or select the client to authorize from a list. Selecting "no" will display a list of all unauthorized clients attempting to make a connection. Entering the IP address or index number (ID number) of the client to authorize will write the information to the Policy Map file upon exiting the LCE Client Manager utility. Select "**0**" to return to the main menu. Selecting "yes" will cause all clients pending authorization to be written to the Policy Map upon exiting the utility. After a confirmation message is written to the terminal, the user is returned to the main menu.

Exit the utility with the "**q**" menu option to save the policy file to disk and activate the changes.

[r] Revoke Authorization to a Client

There are situations where client access to the LCE server needs to be revoked. This is done by selecting the "**r**" option from the menu.

After selecting the "**r**" option from the menu, the user is asked a yes or no question to revoke access to all clients or select the client to revoke access from a list. Selecting "no" will display a list of all authorized clients. Entering the IP address or index number (ID number) of the client to revoke will write the information to the Policy Map file on exiting the LCE Client Manager utility. Select "**0**" to return to the main menu. Selecting "yes" will cause all clients to have their authorization revoked and to be written to the Policy Map on exiting the utility. After a confirmation message is written to the terminal, the user is returned to the main menu.

Exit the utility with the "**q**" menu option to save the policy file to disk and activate the changes.

[d] Display Clients by Policy Assignment

To display a list of clients grouped by the policy assigned to the client, select the "**d**" option from the menu. A list of all clients in the Policy Map file will be displayed sorted by the client policy assigned. Once the list is complete, the user is returned to the main menu.

[p] Display Available Policies

The "**p**" option displays the policies available to assign to clients, which can also be used as a base for developing new policies. A list is displayed with a column for the filename of the policy, client type, and OS.

[a] Add New Policy

Selecting the "**a**" option from the main menu begins the process to add a new policy to the LCE Client Manager. During the creation of a new policy, the user is prompted for information including the policy name, the OS type, the client type, and add the elements and options for the policy file (elements are the valid options for a LCE Client). The policy file contents are displayed on screen during the creation process. When the addition and creation of the elements are completed, the changes may be saved to the new policy file and the user is returned to the main menu.

[c] Copy a Policy

There are times when it is desirable to copy an existing policy, such as when a default policy needs to be modified for use in the environment. Select the "**c**" option from the main menu and a list of policy names will be displayed, ending with **.lcp**. Type the entire policy name at the prompt and press "Enter". Enter the desired name of the policy to be created and press "Enter". The policy will be copied and created under the new name, preserving the original policy file.

[m] Modify an Existing Policy

Selecting the "**m**" option from the main menu allows the user to edit an existing policy. When selected, a list of editable policies is displayed ending with **.lcp**. Enter the filename to be modified followed by the "Enter" key. The policy is displayed, including its values. Select the appropriate option from the available menu to add, delete, or modify an existing key. Once the changes are satisfactorily made, select the "save and exit" option to preserve the changes and return to the main menu.

[s] Assign a Policy to a Client(s)

The "**s**" option from the main menu allows the user to assign a policy to one or more clients. The first step is to select the clients from the presented list via the IP address or ID. The clients selected must be of the same OS and client type. Select "**0**" when all the clients have been selected. Enter the filename of the policy to apply to the clients from the available list and press "Enter". The selected policy will be associated with the selected client(s) and applied on exiting the LCE Client Manager.

[v] Assign Client(s) to a New LCE Server

As organizations grow or devices change location, LCE Clients may need to be modified to report to a different LCE server. In this case, select "**v**" from the main menu. Select the desired clients to change from the list of available clients by IP address or ID and select "**0**" when complete. Enter the IP address and the port of the new LCE server. Once applied, the designated client will have the new server information applied to it. The new LCE server must be configured to authorize the client and configure its policy information.

[i] Import a Policy File

When a policy file has been created outside of the LCE Client Manager, it may be imported to the configuration via the "**i**" option of the main menu. After selecting the option, enter the full path and file name of the policy file to import. Once

entered, answer the questions for the OS type, client type, and descriptive name for the policy. Once that information is entered, it will be imported for use.

[n] Assign a Sensor Name to Client(s)

The "**n**" option allows the user to assign custom sensor names to clients. Sensor names are displayed in SecurityCenter or LCE Manager to identify LCE Client sensors with names identifiable in the organization. By default, the sensor name is set to the DNS hostname if identified from the LCE server, otherwise it is listed as "unknown". This option allows for customization of one or more sensor names to something meaningful for users within the organization.

When selected, a list of available clients is displayed. Select the IP address or ID of the client(s) followed by "**0**". Then enter the sensor name to use for the selected client(s). Once the sensor name is entered, the user is returned to the main menu and the changes will be applied on exit.

[x] Remove a Client

Selecting "**x**" from the main menu begins the process to remove a client. When selected, a list of all available clients is listed. Enter the IP address or ID of the client(s) to remove. Once completed, select "**0**" to save the changes. On exiting the LCE Client Manager, the selected clients will be removed from the Policy Map and no longer be accepted by the LCE server as valid clients.

[q] Exit

The "**q**" command will cleanly exit the LCE Client Manger, apply pending changes to the Policy Map file, and reload the Policy Map to apply the new changes to the running file.

LCE Client Manager Command Line Options

The options for the LCE Client manager can also be invoked on the command line as in, for example: "**/opt/lce/daemons/lce_client_manager --remove-client <client ID>**" (to remove a client). The command **/opt/lce/daemons/lce_client_manager -h** will display all the available options that can be invoked from the command line.

Usage Example (Interactive Mode)

Shown below is an example of how to copy a default policy, customize it, and use it for LCE Client installations. The RHEL LCE Client policy will be copied and customized for use on RHEL systems running the Apache Web server, where it will monitor any file changes (recursively) in the configuration directory (**/etc/https**).

```
# /opt/lce/daemons/lce_client_manager


*******************************************
* LCE Client Manager 1.0
* Please select an option from the menu below
*******************************************
 [g] Grant authorization to a client or clients to connect to LCE
 [r] Revoke a client or clients access to connect to LCE
 [d] Display clients by policy assignment
 [p] Display available policies
 [a] Add a new policy
 [c] Copy a policy
 [m] Modify an existing policy
 [s] Assign a policy to a client or clients
 [v] Assign a client or clients to a new LCE server
 [i] Import a file as a policy
 [n] Assign a custom sensor name to a client or clients
 [x] Remove a client
 [q] Exit
```

```
lce_client_manager >> c

Policy Filename                          Client Type             OS
TNS-MSExchangeServer_windows_tenableclient.lcp
                                         tenableclient           windows
TNS-MSSQLServer_windows_tenableclient.lcp
                                         tenableclient           windows
TNS-NTevents-FileSysMon_windows_tenableclient.lcp
                                         tenableclient           windows
TNS-NTevents_windows_tenableclient.lcp   tenableclient           windows
TNS-WinDesktop_windows_tenableclient.lcp
                                         tenableclient           windows
default_aix_lceclient.lcp                lceclient               aix
default_debian_lceclient.lcp             lceclient               debian
default_dragon_lceclient.lcp             lceclient               dragon
default_fedora_lceclient.lcp             lceclient               fedora
default_freebsd_lceclient.lcp            lceclient               freebsd
default_hpux_lceclient.lcp               lceclient               hpux
default_osx_lceclient.lcp                lceclient               osx
default_rhel_lceclient.lcp               lceclient               rhel
default_rhel_lcesplunk.lcp               lcesplunk               rhel
default_rhel_netflowclient.lcp           netflowclient           rhel
default_rhel_networkmonitor.lcp          networkmonitor          rhel
default_rhel_opsec.lcp                   opsec                   rhel
default_rhel_rdep.lcp                    rdep                    rhel
default_rhel_sdee.lcp                    sdee                    rhel
default_rhel_wmimonitor.lcp              wmimonitor              rhel
default_solaris_lceclient.lcp            lceclient               solaris
default_sun_lceclient.lcp                lceclient               Unknown
default_ubuntu_lceclient.lcp             lceclient               ubuntu
default_windows_tenableclient.lcp        tenableclient           windows

Enter the name of the policy to copy, or 0 to cancel.
lce_client_manager >> default_rhel_lceclient.lcp

Enter a descriptive name for the new policy.
LCE will append the client name and operating system type.
It may not start with "default" and should contain only a-z,A-Z,0-9, and .
For example: corp-desktops-1
             web-servers-2
             lab-machines-3

Enter 0 to cancel.

lce_client_manager >> apache

Full name : /opt/lce/daemons/policies/apache_rhel_lceclient.lcp
Successfully copied policy /opt/lce/daemons/policies/default_rhel_lceclient.lcp to
       /opt/lce/daemons/policies/apache_rhel_lceclient.lcp.

Reminder: policy map changes take effect when you quit the LCE Client Manager through
       the menu option.


*******************************************
```

```
* LCE Client Manager 1.0
* Please select an option from the menu below
*******************************************
 [g] Grant authorization to a client or clients to connect to LCE
 [r] Revoke a client or clients access to connect to LCE
 [d] Display clients by policy assignment
 [p] Display available policies
 [a] Add a new policy
 [c] Copy a policy
 [m] Modify an existing policy
 [s] Assign a policy to a client or clients
 [v] Assign a client or clients to a new LCE server
 [i] Import a file as a policy
 [n] Assign a custom sensor name to a client or clients
 [x] Remove a client
 [q] Exit


lce_client_manager >> m

Policy Filename                          Client Type             OS
apache_rhel_lceclient.lcp                lceclient               rhel

Enter the file name of the policy to modify (0 to cancel):
lce_client_manager >> apache_rhel_lceclient.lcp

Tip: Policies are lists of key-value pairs called elements.  Elements can be nested,
       as follows:
[key0] -> [value0]
[key1]
    [subkey1] -> [value1]
    [subkey2] -> [value2]
[key2] -> [value4]

To reach value2, first ask to modify key1, then modify subkey2.

The current policy key-values being modified:
------ BEGIN POLICY ------
  [log-directory] -> [./]
  [tail-file] -> [/var/log/messages]
  [tail-file] -> [/var/log/secure]
  [scan-frequency] -> [60]
  [report-ownership-changes] -> [yes]
  [report-permissions-changes] -> [yes]
  [modification-check-frequency] -> [30]
  [heartbeat-frequency] -> [300]
  [statistics-frequency] -> [60]
  [compress-events] -> [1]

------- END POLICY -------

Select an option to modify your policy:
[a] Add new key (and values)
[d] Delete existing key/element (and values)
[m] Modify value for existing key
[s] Save and exit
```

```
[q] Exit WITHOUT saving changes

lce_client_manager >> a


Enter the new key to add to your policy:
lce_client_manager >> recursive-directory-changes


Current element being modified:

  [recursive-directory-changes]

Select an option for this element:
[a] Add a nested element
[v] Add a new value
[d] Delete a value
[z] Modify a nested element
[m] Modify a value
[s] Save and complete

lce_client_manager >> v


Enter the new value to add to your element:
lce_client_manager >> /etc/httpd


Current element being modified:

  [recursive-directory-changes] -> [/etc/httpd]


Select an option for this element:
[a] Add a nested element
[v] Add a new value
[d] Delete a value
[z] Modify a nested element
[m] Modify a value
[s] Save and complete

lce_client_manager >> s


Saving element...

The current policy key-values being modified:
------ BEGIN POLICY ------
  [log-directory] -> [./]
  [tail-file] -> [/var/log/messages]
  [tail-file] -> [/var/log/secure]
  [scan-frequency] -> [60]
  [report-ownership-changes] -> [yes]
  [report-permissions-changes] -> [yes]
  [modification-check-frequency] -> [30]
  [heartbeat-frequency] -> [300]
```

```
   [statistics-frequency] -> [60]
   [compress-events] -> [1]
   [recursive-directory-changes] -> [/etc/httpd]

------- END POLICY -------

Select an option to modify your policy:
[a] Add new key (and values)
[d] Delete existing key/element (and values)
[m] Modify value for existing key
[s] Save policy to file and exit
[q] Exit WITHOUT saving changes

lce_client_manager >> s


Successfully saved the modified policy.
Successfully signaled LCE to reload the policy map.


*********************************************
* LCE Client Manager 1.0
* Please select an option from the menu below
*********************************************
 [g] Grant authorization to a client or clients to connect to LCE
 [r] Revoke a client or clients access to connect to LCE
 [d] Display clients by policy assignment
 [p] Display available policies
 [a] Add a new policy
 [c] Copy a policy
 [m] Modify an existing policy
 [s] Assign a policy to a client or clients
 [v] Assign a client or clients to a new LCE server
 [i] Import a file as a policy
 [n] Assign a custom sensor name to a client or clients
 [x] Remove a client
 [q] Exit


lce_client_manager >>
```

The **`*.lcp`** policy files located in **`/opt/lce/daemons/policies`** are in XML format, which can be edited manually.

Never edit the default policies, as they will be overwritten with future updates.

When using the LCE Client Manager to edit a policy, all comments and white space are removed from the file.

XML Policy Representation of Client Manager Parameters

The following is an example of how the parameters entered using the Client Manager are stored when using the Client Manager:

```
[log-directory] -> [./]
[interface] -> [eth0]
[syslog-only] -> [no]
[include-networks]
    [filter] -> [192.168.20.5/32]
    [filter] -> [127.0.0.1]
    [filter] -> [172.0.0.0/8]
[exclude-networks]
[heartbeat-frequency] -> [300]
[statistics-frequency] -> [60]
[compress-events] -> [1]
[filter-expression] -> [udp or tcp or icmp]
```

This is what the XML policy file contains:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?> <options
       xmlns:xi="http://www.w3.org/2003/XInclude">
    <log-directory>./</log-directory>
    <interface>eth0</interface>
    <syslog-only>no</syslog-only>
    <include-networks>
        <filter>192.168.20.5/32</filter>
        <filter>127.0.0.1</filter>
        <filter>172.0.0.0/8</filter>
    </include-networks>
    <exclude-networks/>
    <heartbeat-frequency>300</heartbeat-frequency>
    <statistics-frequency>60</statistics-frequency>
    <compress-events>1</compress-events>
    <filter-expression>udp or tcp or icmp</filter-expression> </options>
```

LCE Conf Converter

The LCE Conf Converter is a utility to convert LCE configuration files from versions of the LCE Clients prior to 4.0 to new policy files.

The following command run from the command line with no options will display the help file:

```
# /opt/lce/daemons/lce_conf_file_converter
```

There are four valid options to use as described in the table below:

Option	Description
--input-conf-file **-i**	The input configuration file (i.e., **lce_client.conf**)
--output-policy-file **-o**	The output policy file (e.g., **my-new-policy.lcp**)
--help **-h**	Display the help menu
--version **-v**	Display version information

Once saved as a policy file, the converted file may be imported to the LCE Client Manager and assigned to the appropriate client(s).

The following is an example of how to convert an **lce_client.conf** to a policy file (for RHEL):

```
# /opt/lce/daemons/lce_conf_file_converter -i
      /opt/lce_client/lce_client.conf -o ~/lce_client_conf.lcp

Successfully converted /opt/lce_client/lce_client.conf to policy
/root/lce_client_conf.lcp.

# /opt/lce/daemons/lce_client_manager --import-policy
      ~/lce_client_conf.lcp --output-policy my-converted-conf
      --client-type lceclient --os-type rhel
      /opt/lce/daemons/policies/my-converted-conf_rhel_lceclient.lcp
```

If there is an error, a non-zero error code will be displayed.

LCE Linux and Unix-based Clients

The LCE Linux and Unix-based clients are available in a package format appropriate for the platform operating system and include system startup files.

Installing the LCE Linux and Unix-Based Clients

Each client comes with an example client configuration file (e.g., **lce_client.conf** for the LCE Client), the program binary, and is installed into the appropriate client directory that will be created if it does not already exist.

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

The following table provides an installation example for each available LCE Client for RHEL/CentOS and other Unix-based systems. Any special installation instructions are provided in a note following the example.

LCE Client	Installation Example
Red Hat / CentOS	
LCE Client (Log Agent)	`# rpm -ivh lce_client-4.x.x-esX.i386.rpm`
LCE WMI Monitor Agent	`# rpm -ivh wmi_monitor-4.x.x-esX.i386.rpm`
Tenable NetFlow Monitor	`# rpm -ivh TenableNetFlowMonitor-4.x.x-esX.i386.rpm`
Tenable Network Monitor	`# rpm -ivh TenableNetworkMonitor-4.x.x-esX.i386.rpm`
Mac OS X	
LCE Client (Log Agent)	Download **lce_client-4.x.x-osx.pkg.tar.gz** to the client system and click on it to run the Mac Installer.

A successful installation is indicated by the return of the command prompt with no errors. See Appendix 1 for example output of several installations.

Once the client is installed, the **lce-server** and **server-port** options must be configured if it will connect to a LCE 4.0 server. Next, restart the client for it to make an initial connection to the LCE server. Using SecurityCenter, LCE Manager 4.6, or LCE Client Manager on the LCE server, allow the server to accept the connection and configure the client.

After configuration by the LCE Client Manager, the **lce_client.conf** file is no longer used to manage the client. The **server_assignment.xml** file details the connection information from the client to the LCE server. The client policy file is copied to the client with the **.policyf** file instructing the client which policy file to load. It is not recommended to edit these files directly unless instructed to do so by Tenable Support.

Installation Directories

LCE Client	Installation Directory
Red Hat / CentOS	
LCE Client (Log Agent)	`/opt/lce_client`
LCE WMI Monitor Agent	`/opt/wmi_monitor`
Tenable NetFlow Monitor	`/opt/netflow_monitor`
Tenable Network Monitor	`/opt/network_monitor`
Mac OS X	
LCE Client (Log Agent)	`/opt/lce_client`

Upgrading the LCE Clients

LCE Clients 3.4.3 and greater can be upgraded by performing a basic install or upgrade process, depending on the method. During the installation or upgrade process, the original LCE Client is removed automatically and the new one is then added. Follow the instructions above for performing the LCE Client installation, replacing '`-ivh`' with '`-Uvh`'.

After upgrading clients, they must be configured by the LCE Client Manager of the LCE server if they are version 4.0 or higher.

Removing the LCE Clients

To remove the LCE Client, login as the root user or equivalent, stop the client daemon (see the section "Halting the LCE Linux and Unix-Based Clients" for directions) and run the appropriate commands for your client and platform as shown in the following table:

LCE Client	Removal Example
Red Hat / CentOS	
LCE Client (Log Agent)	Determine the name of the installed package:

	# **rpm -qa | grep lce_client** lce_client-4.x.x-esX # Remove the installed package: # **rpm -ev lce_client-4.x.x-esX**
LCE WMI Monitor Agent	Determine the name of the installed package: # **rpm -qa | grep wmi_monitor** wmi_monitor-4.x.x-esX # Remove the installed package: # **rpm -ev wmi_monitor-4.x.x-esX**
Tenable NetFlow Monitor	Determine the name of the installed package: # **rpm -qa | grep TenableNetFlowMonitor** TenableNetFlowMonitor-4.x.x-esX # Remove the installed package: # **rpm -ev TenableNetFlowMonitor-4.x.x-esX**
Tenable Network Monitor	Determine the name of the installed package: # **rpm -qa | grep TenableNetworkMonitor** TenableNetworkMonitor-4.x.x-esX # Remove the installed package: # **rpm -ev TenableNetworkMonitor-4.x.x-esX**
Mac OS X	
LCE Client (Log Agent)	To remove the LCE client on a Mac use a third party de-installation program or run the following commands from the command line prompt: # **rm /opt/lce_client/lce_clientd** # **rm -r /System/Library/StartupItems/LCEClient**

LCE Linux and Unix-Based Client Configuration

This section describes how to configure the LCE Linux and Unix-based clients for communication with the LCE server. The configuration files for each of the clients on the supported operating systems are listed in the table below:

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

If changes must be made to an existing configuration file and the client is already running, make the changes, halt the client, and then restart it. See "Halting the LCE Linux and Unix-Based Client".

Once a 4.x client connects to a 4.x server, the **`.conf`** files are no longer used, and the policy files (provided by the LCE server) will be used. Policy files are sent from the LCE server to the LCE client each time they are changed server-side. Policies are covered in the "LCE Client Manager" section of this document.

LCE Client

LCE's Linux and Unix-based clients can be used to monitor log files that contain events received from other devices. For example, if a Linux server is configured to receive **`syslog`** events from a nearby router, the LCE Client and LCE server will parse all events as if they originally came from the Linux server. If IP address information is in the **`syslog`** message, then the LCE server assigns the source and destination events accordingly.

All that needs to be done for configuration here is to specify the LCE server's IP address, and if needed, change the server port. A default **`lce_client.conf`** configuration file is shown below:

```
# If using an LCE 4.x server, configure this file with the appropriate
# server information. After the first run, the client will be
# configured strictly from the Client Manager.

# If using an LCE 3.x server, replace this file with the
# lce_client.conf.v3_server file, which contains full
# configuration information.

options {
        # LCE client log messages are written to a file named
        # according to the date in the directory specified below.
        log-directory /opt/lce_client/

        # The following block defines the IP address at which the
        # LCE server is located.
        # Replace the below address with the IP address of the LCE server.
        lce-server 203.0.113.250 {
        }
```

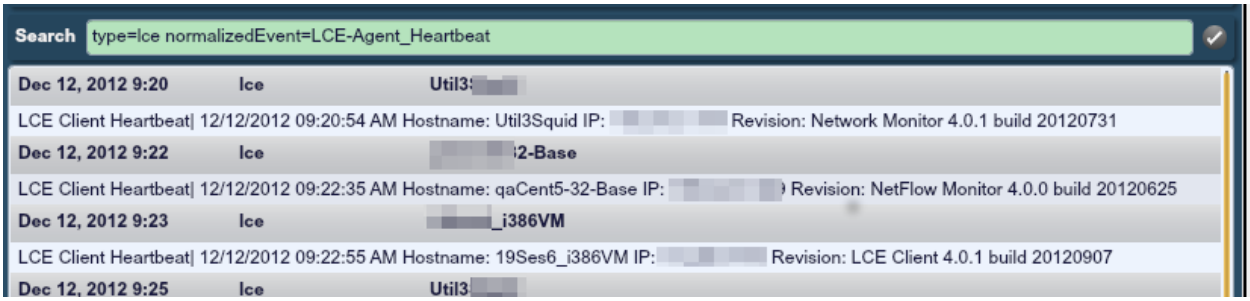
```
        # The LCE server can be configured to listen on a user-specified
        # port. The setting below should match the server setting,
        # which is 31300 by default.
        server-port 31300
}
```

Once the configuration file is updated and applied, check the client log to ensure it is operating properly and to validate that configuration directives were configured correctly.

Policy Parameters
The following is a list of all valid “keys” available for use in with the Linux policies:

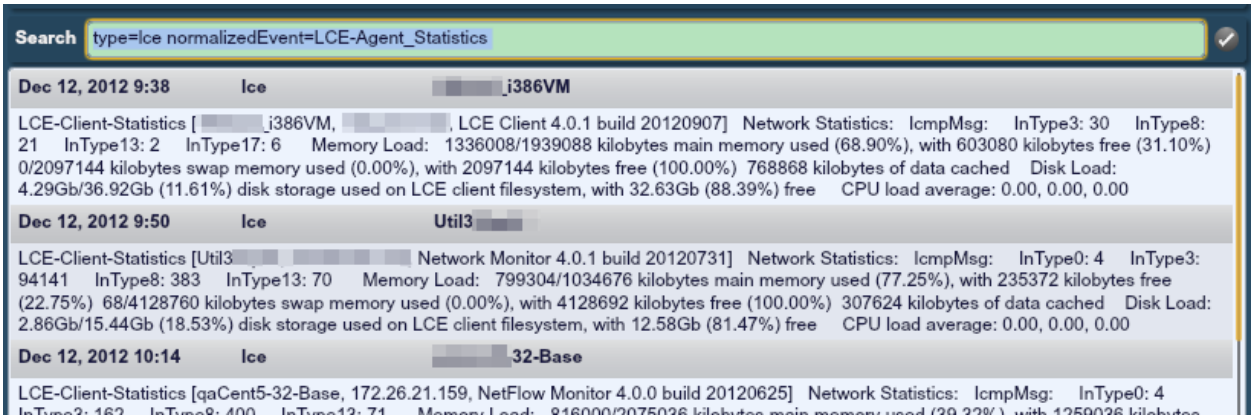
Key Name	Description	Valid Values	Examples
tail-file	Tail a single text log file - each new line will be sent to the LCE server.	Any full path and file name.	/var/log/messages /var/log/secure /root/my_log_file.txt
tail-dir	Tail all text files in a directory, instead of a single file like "tail-file". Wildcards are permitted.	Any full path name with wildcards.	/var/log/*.log /var/log/*
monitor-file-changes	Monitor a single file and send a log if it is added, deleted, or modified. MD5 checksums are sent in each log.	Any full path and file name.	/etc/passwd /root/.bashrc
monitor-directory-changes	Monitor all files in a directory instead of a single file like "monitor-file-changes".	Any full path name with wildcards.	/etc/* /bin/* /usr/bin/*
recursive-directory-changes	Monitor all files in a directory and all files in subdirectories, like "monitor-directory-changes".	Any full path name.	/usr/ /bin/
accounting-file	Monitor a single accounting file (produced by a Unix process accounting daemon).	The full path and file name of the accounting file.	/var/account/acct
audit-dir	Monitor audit files in this directory (produced by a BSM auditing daemon).	The full path name to the audit file directory.	/var/audit/
scan-frequency	The number of seconds between rescanning directories being tailed (keys starting with "tail-").	A positive non-zero integer.	10 60
modification-check-frequency	The number of minutes between rescanning directories being monitored (keys ending with "-changes").	A positive non-zero integer.	10 60
report-ownership-changes	Whether or not to report changes in ownership for monitored files (keys ending with "-changes").	0 or 1 (0=off,1=on)	0 1
report-permission-changes	Whether or not to report changes in permissions for monitored files (keys ending with "-changes").	0 or 1 (0=off,1=on)	0 1

heartbeat-frequency	The number of seconds between each client heartbeat message to the LCE server. If “0”, it will not send heartbeats.	A positive integer.	0 300
statistics-frequency	The number of minutes between each client host performance statistics report to the LCE server. If “0”, it will not send statistics.	A positive integer.	0 60
compress-events	Whether or not to compress events before transmitting them to the LCE server. Marginally saves bandwidth, marginally increases CPU usage.	0 or 1 (0=off,1=on)	0 1
log-directory	The path to which the LCE Client writes its own log file (startup information, errors, warning, and optional debug information).	A full path name.	/opt/lce_client/
client-debug	Reports additional debugging information if this key is present.	There are no values needed here; the key will be empty.	N/A



Performance Reporting

When the LCE Client sends performance statistics to the LCE server, the exact information sent depends on the operating system (e.g., swap and cache data is not available on all platforms). The various performance logs are normalized to the “lce” event type for easy analysis. When viewed using the Raw Syslog Events tool, the data appears similar to the following screen capture:



This data is very useful for troubleshooting performance issues on the remote LCE Client. Used in conjunction with the “process” LCE event type that hourly monitors and reports on system processes, runaway processes can be quickly debugged and resolved before they completely take the LCE client system down.

LCE WMI Monitor Agent

The LCE WMI Monitor Agent is used to automate the collection of Windows Event Logs from remote Windows systems by using WMIC calls from the Linux system running the agent.

This facilitates the collection of Windows logs from many hosts for the purpose of event normalization/searches and performance analysis.

Host network connections occur in parallel, and though very quick, they may cause a temporary spike in network traffic and WMIC processes from the WMI Monitor Agent host while collection is occurring.

For performance reasons, Tenable recommends configuring no more than 100 Windows hosts per WMI Monitor Agent.

All that needs to be done for configuration here is to specify the LCE server's IP address, and if needed, change the server port. A default **`wmi_monitor.conf`** configuration file is shown below:

```
# If using an LCE 4.x server, configure this file with the appropriate
# server information. After the first run, the client will be configured
# strictly from the Client Manager.

# If using an LCE 3.x server, replace this file with the
# wmi_monitor.conf.v3_server file, which contains full configuration
# information.

options {
      # WMI Monitor log messages are written to a file named according to
       # the date in the directory specified below.
      log-directory /opt/wmi_monitor/

       # The following section defines the IP at which the LCE server is
       # located, as well as the authentication required to log in. Only
       # one LCE server is currently supported. For example, use the
       # following to configure an LCE server at 192.168.1.2
       lce-server 192.168.1.2 {
      }

      # The LCE server can be configured to listen on a user-specified port.
       # The setting below should match the server setting, which is 31300 by
       # default.
      server-port 31300
}
```

After the WMI Monitor Agent is installed, log into SecurityCenter or LCE Manger to download a copy of the default wmi_monitor LCP policy file. Open the downloaded file in a text editor to configure the wmi_monitor LCP policy file, and add the list of Windows hosts (one per **`WMI-host`** keyword) to be monitored. An example wmi_monitor LCP policy file is shown below and should not be used in production networks without customizations.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<options xmlns:xi="http://www.w3.org/2003/XInclude">
    <!-- WMI Monitor log messages are written to a file named according to
        the date in the directory specified below. -->
    <log-directory>/opt/wmi_monitor/</log-directory>
```

```
<!-- Each WMI-host block specifies a Windows system to be monitored.
     It is no longer possible to specify username/password in this host
    specification - run ./wmi_config_credentials to add/modify hosts and
    manage host credentials.  Run ./wmi_config_credentials -h for help. -->
<!-- WMI-host -->
    <!-- address>192.168.0.2</address -->
   <!-- domain>HEADQUARTERS</domain -->
   <!-- The "monitor" option below is used to specify which Win32_NTLogEvent
        log files will be tracked. If "All" is specified, the WMI agent will
        automatically query the host to determine which files are available,
         and those files will be tracked. -->
   <!-- monitor>All</monitor -->
   <!-- monitor>System</monitor -->
   <!-- monitor>Windows Powershell</monitor -->
   <!-- monitor>Application</monitor -->
   <!-- monitor>Security</monitor -->
<!-- /WMI-host -->
   <WMI-host>
       <address>192.168.1.65</address>
       <monitor>All</monitor>
   </WMI-host>
   <WMI-host>
       <address>192.168.1.67</address>
       <monitor>All</monitor>
   </WMI-host>
   <WMI-host>
       <address>192.168.1.70</address>
       <monitor>All</monitor>
   </WMI-host>
   <WMI-host>
       <address>192.168.1.71</address>
       <monitor>All</monitor>
   </WMI-host>
   <WMI-host>
       <address>192.168.1.72</address>
       <monitor>All</monitor>
   </WMI-host>
   <WMI-host>
       <address>192.168.1.75</address>
       <monitor>All</monitor>
   </WMI-host>

<!-- In addition to the Log Correlation Engine, events downloaded from the
    security device can also be forwarded to one or more syslog servers.
    The syslog-server keyword defines the address at which each is located. -->
<!-- syslog-server>192.168.1.20</syslog-server -->
<!-- syslog-server>192.168.1.21</syslog-server -->


<!-- When the following line is uncommented, extra debugging information
    is logged. This option should be enabled only temporarily, as it may
    cause the application log file to grow extremely large. Debug mode
    can be toggled during runtime by sending the SIGUSR1 signal to the
    lce_wmid process. -->
<!-- debug>1</debug -->
```

```
    <!-- The heartbeat-frequency option defines the number of seconds between each
       pair
        of client heartbeat messages that are sent to the server. -->
    <heartbeat-frequency>300</heartbeat-frequency>

    <!-- The LCE client provides the option of periodically sending a log file
       containing
        performance statistics to the LCE server. The following option determines the
        number of minutes between each performance statistics report. When the next
       line
        is commented out or removed, performance reporting is disabled. -->
    <statistics-frequency>60</statistics-frequency>

    <!-- LCE clients can compress log data prior to sending it to the LCE server,
       saving bandwidth.
         For debugging purposes, event packet compression may be disabled, but this
       will
        increase the bandwidth required to send data from LCE clients to the LCE
       server.
        Setting the following option to 0 will disable compression only during
       transmission. -->
    <compress-events>1</compress-events>

</options>

}
```

The WMI agent will automatically query the host to determine which files are available, and those files will be tracked. In this example, “All” events are tracked.

WMI monitor LCP policy file

The following table describes the configuration options available in the WMI_monitor LCP policy file:

Option		Description
log-directory		Log directory storage point
lce-server		IP address or hostname of the LCE server
server-port		Port that the LCE server is configured to listen on
WMI-host	**address**	IP address or hostname of a Windows system to be monitored  DNS must be configured properly if a hostname is used in this field.
	domain	The Windows domain in which the credentials used to log into the system belong
	Username	Username that will be used to perform Windows system login

	Password	Password that will be used to perform Windows system login
	Monitor	Specifies which **Win32_NTLogEvent** log files to track. If "All" is specified, the WMI agent will automatically query the host to determine which files are available, and those files will be tracked.
syslog-server	In addition to the Log Correlation Engine, events downloaded from the security device can also be forwarded to one or more **syslog** servers. The **syslog-server** keyword defines the address at which each server is located.	
heartbeat-frequency	The number of seconds between each pair of client heartbeat messages that are sent to the server	
statistics-frequency	The number of minutes between each performance statistics report to the LCE server	
debug	When this line is uncommented, extra debugging information is logged. This option should be enabled only temporarily, as it may cause the application log file to grow extremely large. Debug mode can be toggled during runtime by sending the **SIGUSR1** signal to the **lce_wmid** process.	
compress-events	LCE Clients have the ability to compress log data prior to sending the information to the LCE server. Enabling this feature saves bandwidth. It may be disabled by changing the option to "0". This option is enabled by default.	

WMI Encrypted Credentials

Encrypted credentials are not managed by the LCE Client Manager. If WMI encrypted credentials are used, they must be configured on each individual WMI client machine.

A feature is available through the **/opt/wmi_monitor/wmi_config_credentials** binary to encrypt the WMI credentials to an external file set. This tool has the ability to read the current hosts from the wmi_monitor LCP policy file, and the credentials in that file. Once saved, the cleartext credentials in the policy file may be deleted.

The preferred method to store credentials is to use the **wmi_config_credentials** tool. While cleartext usernames and passwords will currently work, a warning about their use being deprecated will appear in the log files.

Option	Description
-i <wmi_monitor policy file >	When the **-i** option is used, it will read the specified **wmi_monitor LCP policy** file and will read in the data available for the configured host(s).
-o </path/to/credentials>	When used, the **-o** option will instruct the program to write the credential files to the specific directory.
-c </path/to/credentials>	When used, the **-c** option will instruct the program where to read the credential files from the specific directory for modification purposes.
-v	When used, the **-v** option will print the version information to the screen.
-h	When used, the **-h** option will display the help file.

When the **wmi_config_credentials** program is run on its own without options, it will read the default file **/opt/wmi_monitor/wmi_monitor LCP policy file** and the encrypted credentials in the **/opt/wmi_monitor/data/** directory and will save the modifications to the same directory. When run, output similar to the following will be displayed:

```
 [root@wmimonitor wmi_monitor]# ./wmi_config_credentials
WARNING: Plaintext usernames/passwords are deprecated (I found one for 192.168.1.63).
Please run wmi_config_credentials to encrypt your credentials, then remove plaintext
      usernames/passwords from the wmi_monitor.conf file.
The "address", "domain", and "monitor" lines must remain in the wmi_monitor.conf file.
(0):    Domain:
   Address: 192.168.1.63
  Username: *************
  Password: ********
     Files: All

Found 1 host(s) in your configuration.


****************************************
*****  Please select an option below *****
****************************************
*[1] Display current hosts               *
*[2] Add a new host                      *
*[3] Modify an existing host             *
*[4] Delete an existing host             *
*[5] Save hosts and credentials          *
*[Q] Save and quit                       *
*[X] Quit without saving                 *
*                                        *
* >> (3):    Domain: bogusdom
   Address: 192.168.1.63
  Username: ***
  Password: ***
     Files: Security

Found 4 host(s) in your configuration.


****************************************
*****  Please select an option below *****
****************************************
*[1] Display current hosts               *
*[2] Add a new host                      *
*[3] Modify an existing host             *
*[4] Delete an existing host             *
*[5] Save hosts and credentials          *
*[Q] Save and quit                       *
*[X] Quit without saving                 *
*                                        *
* >>
```

At the beginning, in the **Warning:** section, we see that a username and password exists in the configuration file that is being read. This informs us that once encrypted, we may delete the username and password lines from the configuration file for that host.

Following the **Warning:** section, we have a list of the hosts within the configuration file followed by the total number of hosts in the configuration. Each host is prefaced with the number in the order it was found in the configuration file (starting with 0). The **Domain**, **Address**, **Username**, **Password**, and **Files** fields are contained in the description:

Field	Description
Domain	This is the Windows domain that the credentials will attempt to login to when the program is executed. This is stored in the **wmi_monitor** LCP policy file.
Address	This is the IP address of the host that will attempt to be logged into when the program is executed. This is stored in the **wmi_monitor** LCP policy file.
Username	This field indicates if a **Username** is saved or not. If there are asterisks in the field, the username is set in the encrypted file. If <Not Set> is shown, then the host does not have a corresponding encrypted credential saved.
Password	This field indicates if a **Password** is saved or not. If there are asterisks in the field, the username is set in the encrypted file. If <Not Set> is shown, then the host does not have a corresponding encrypted credential saved.
Files	This field indicates the files that are monitored by the WMI monitor on the targeted host. This is stored in the **wmi_monitor** LCP policy file.

The following section shows the menu of actions that may be performed:

```
****************************************
*****  Please select an option below *****
****************************************
*[1] Display current hosts               *
*[2] Add a new host                      *
*[3] Modify an existing host             *
*[4] Delete an existing host             *
*[5] Save hosts and credentials          *
*[Q] Save and quit                       *
*[X] Quit without saving                 *
*                                        *
* >>
```

Selecting **1** will display a list of the hosts currently available within the encrypted host credential directory.

Selecting **2** allows for adding a new host to the credential directory. When selected, a series of questions will be asked beginning with the new host address and followed by the username and password to use. Once entered, a list of available hosts will be shown on the screen followed by a success or failure message. When successful, a reminder will be given to enter the host's address, domain, and monitor lines to the **wmi_monitor** LCP policy file.

Note that when you are entering the Username and Password there is nothing echoed to the screen.

Selecting **3** will allow the user to make changes to the credentials of an existing host. A list of all hosts will be displayed. Select the host to modify by selecting the number next to the host information. The user is then prompted to enter the updated username and password to be used with the host.

Selecting **4** will allow the user to delete an existing host from the records. After selecting the option, enter the number of the host to delete. If successful, the list of menu options will be displayed. If there is an issue, an error message will be displayed indicating what has gone wrong.

Selecting **5** will save the current state of hosts and passwords. This allows the user to save their work without exiting the program.

Selecting **Q** (case insensitive) will save the changes that have been made since the last save and quit the program.

Selecting **X** (case insensitive) will quit the program and not save any of the changes that were entered.

When running the **wmi_config_credentials** program, ensure that the **wmi_monitor** LCP policy file used contains at least the hosts that have been previously encrypted. Otherwise, a warning will be issued and credentials will be lost if you continue.

For more information about configuring remote hosts for remote WMIC connectivity or troubleshooting connectivity issues, please refer to the following helpful links:

- http://msdn.microsoft.com/en-us/library/aa389290%28v=vs.85%29.aspx#configuring_a_computer_for_a_remote_connection
- http://support.microsoft.com/kb/875605

Tenable NetFlow Monitor

The Tenable NetFlow Monitor Client currently only supports NetFlow versions 5 and 9.

A list of decimal protocol enumerations is found here:
http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml

The Tenable NetFlow Monitor (TFM) client takes advantage of the ability in most modern routers to use the “NetFlow” protocol to send network session statistics to remote collectors for processing and reporting. This enables you to monitor network traffic without having to install a sniffer on a hub or switched span port.

To configure, specify the LCE server’s IP address, and if needed, change the server port. A default **tfm.conf** configuration file is shown below:

```
# If using an LCE 4.x server, configure this file with the appropriate server
      information.
# After the first run, the client will be configured strictly from the Client Manager.

# If using an LCE 3.x server, replace this file with the tfm.conf.v3_server file,
# which contains full configuration information.

options {
        # Log messages will be stored in a file named according to date in the
       following
        # directory.
        log-directory "/opt/netflow monitor/";

        # This section defines the login information for the LCE server. Only one
```

```
        server
         # is currently supported.
         lce-server 192.168.1.160 {
         }

         # The LCE server can be configured to listen on a user-specified port. The
        setting
         # below should match the server setting, which is 31300 by default.
         server-port 31300;
 }      server-port 31300;
 }
```

Default Netflow Policy

The following table describes the configuration options available in the **default_rhel_netflowclient.lcp** file:

Option	Description
log-directory	Directory where LCE Client logs are stored. If the **log-directory** keyword is commented out, then the client install directory will be used. Otherwise, ISO9000 compliant log files will be saved in the specified directory.
lce-server	Directs the TFM client to the IP address or hostname of the LCE, and specifies the password used to connect. Note: Each client can only connect to one server, and will connect to the first available server specified if multiple **lce-server** directives exist.
server-port	The port that the LCE server, as designated by the **lce-server** directive, listens on.
netflow-server-port	Specifies the NetFlow port to monitor. Do not change the **netflow-server-port** keyword unless you have specifically modified the configuration of your networking devices to report NetFlow data on non-standard ports.
heartbeat-frequency	The TFM client can be configured to send a “heartbeat” message to the LCE. This message indicates that the client is still alive and performing normally.
statistics-frequency	The frequency with which the LCE Client sends a log entry containing performance statistics to the LCE.
compress-events	LCE Clients have the ability to compress log data prior to sending the information to the LCE server. Enabling this feature saves bandwidth. It may be disabled by changing the option to “0”. This option is enabled by default.
include-filter **exclude-filter**	The filtering section is used to limit the amount of data logged. Unlike the TNM that has command line filtering courtesy of the **libcap** packet capture library, TFM filtering is specified inside the **tfm.conf** file.
Debug	NetFlow data reported by the NetFlow agent, along with other verbose output, may be printed to the NetFlow agent log if desired primarily for troubleshooting purposes. By default this option is disabled because it can generate very large agent logs.

Filtering is accomplished by specifying one or more protocol, network, or port combinations. In the provided default netflow policy file, several examples are given that look for generic matches. The filtering logic works such that any reported NetFlow session must match at least one of the specified filters in each section.

Negative filtering can also be used. Consider the following section from a **tfm.conf** file:

```
          include-filter {
              proto 6;
          }

          exclude-filter {
            port 20;
            port 21;
            port 22;
            port 25;
            port 80;
            port 53;
            port 110;
            port 123;
            port 161;
            port 143;
            port 443;
            port 1434;
            port 1863;
            port 5050;
            port 5190;
            port 8200;
         }
```

In this example, the **tfm** would look for all TCP traffic, but would also ignore any sessions occurring on the ports listed in the exclude filter.

Tenable NetFlow Monitor Event Types
These are the event types that the Tenable NetFlow Monitor can currently generate:

- TFM-TCP_Session_Whole
- TFM-TCP_Session_Partial
- TFM-UDP_Activity
- TFM-TCP_Session_Whole_1MB
- TFM-TCP_Session_Whole_10MB
- TFM-TCP_Session_Whole_100MB
- TFM-TCP_Session_Whole_1000MB
- TFM-TCP_Session_Whole_Long
- TFM-TCP_Session_Partial_Long

Usage
Once the policy is configured correctly, simply invoke the **tfmd** binary from the command line.

Traffic from NetFlow version 9 will produce records that will have a trailing “0”. This will be seen in the LCE host when viewing log data from the LCE. An example of these records is shown below:

```
Tue Jul 18 13:30:27 - TFM-TCP_Session_Partial[46|0]:192.168.1.6:5190 ->
       192.168.1.7:2958|1153243797|1153243797|0
```

```
Tue Jul 18 13:30:39 - TFM-TCP_Session_Partial[9492|0]:192.168.1.4:21766 ->
      192.168.1.5:2832|1153243809|1153243809|0

Tue Jul 18 13:31:05 - TFM-TCP_Session_Partial[0|757]:192.168.1.2:4136 ->
      192.168.1.3:80|1153243835|1153243835|0
```

Available fields within this raw output include (from left to right):

- Alert date/time
- Alert name
- [Bytes downloaded|Bytes uploaded]
- Source IP:port
- Destination IP:port
- Start time (Unix timestamp)
- End time (Unix timestamp)
- Length of session (in seconds)

Running the **`tfmd`** binary with the **`-h`** switch will provide a list of the available command line options as shown here:

```
 [root@linux]# /opt/netflow_monitor/tfmd -h
usage: ./tfmd [ -v ] [ -e ] [ -f <pcap file> ] [ -p <port> ]

  -v            Display version information and exit

  -e            Enable event reporting on the terminal.
                All events reported to the LCE server are also printed to the screen.

  -f            Allows the user to feed a pcap file to the agent as the event source,
      in lieu of using live NetFlow data.

  -p            Allows the user to specify the live NetFlow traffic port on the
      command line.
                This is the same as, and will override, netflow-server-port in the
      tfm.conf file.

  -h            Display this help information and exit.
```

Tenable Network Monitor

The Tenable Network Monitor (TNM) is designed to monitor network traffic and send session information to the LCE server. It can also sniff **`syslog`** messages sent from one point to another and treat them as if they were originally sent directly to the LCE. The following is an example of the **`tnm.conf`** configuration file:

```
# If using an LCE 4.x server, configure this file with the appropriate server
      information.
# After the first run, the client will be configured strictly from the Client Manager.

# If using an LCE 3.x server, replace this file with the tnm.conf.v3_server file,
```

```
# which contains full configuration information.

options {
        # Network Monitor log messages are stored in files named according to the date
        # in the following directory.
        log-directory "/opt/network_monitor/";

        # This section defines the IP address for connections to the
        # Log Correlation Engine server. In the example, the server is located at
       203.0.113.250
        # Only one LCE server is currently supported.
        lce-server 172.26.34.167 { }

        # The LCE server can be configured to listen on a user-specified port. The
       setting
        # below should match the server setting, which is 31300 by default.
        server-port "31300";

}
```

Default TNM XML Policy

The following is taken from the **default_rhel_networkmonitor.lcp** policy file. These settings can be changed using the LCE Client Manager. Remember to never edit the XML file directly; instead, download and edit any of the policy files from SecurityCenter or LCE Manager, and import the new file to assign it to the proper client.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<options xmlns:xi="http://www.w3.org/2003/XInclude">

    <!-- Network Monitor log messages are stored in files named according to the date
        in the following directory. -->
    <log-directory>./</log-directory>

    <!-- The Network Monitor automatically generates a tcpdump filter expression that
       selects
        which network packets will be processed. This expression is based on the
       syslog
        monitoring settings below. The following option allows the default filter to
       be
        overridden with a custom expression.  -->
    <!-- filter-expression>tcp or icmp or udp port 514</filter-expression -->

    <!-- The network monitor will report traffic from only the interfaces listed
       below. -->
    <!-- interface>eth0</interface -->
    <interface>eth0</interface>

    <!-- Traffic containing syslog messages is forwarded to the LCE server for the
       hosts
        matching the filtering criteria in the final section. The following specifies
       the
        protocol/port pairs for which all traffic will be processed as syslog
       messages.
        These settings should match the syslog or syslog-ng configuration.  -->
    <monitor-syslog-port>udp/514</monitor-syslog-port>
    <monitor-syslog-port>tcp/1468</monitor-syslog-port>
```

```
    <!-- When the below option is set to yes, only syslog messages are reported, and
       all
        all other traffic is ignored.  -->
    <syslog-only>no</syslog-only>

    <!-- The following section defines the networks on which syslog will be monitored.
         The network monitor will report syslog messages received at the above
       specified
         ports for any IP address matching the filter criteria. -->
    <include-networks>
        <filter>192.168.20.5/32</filter>
        <filter>127.0.0.1</filter>
    </include-networks>
    <exclude-networks>
    </exclude-networks>

    <!-- The heartbeat-frequency option defines the number of seconds between each
       pair
        of client heartbeat messages that are sent to the server. -->
    <heartbeat-frequency>300</heartbeat-frequency>

    <!-- The LCE client provides the option of periodically sending a log file
       containing
        performance statistics to the LCE server. The following option determines the
        number of minutes between each performance statistics report. When the next
       line
        is commented out or removed, performance reporting is disabled. -->
    <statistics-frequency>60</statistics-frequency>

    <!-- LCE clients can compress log data prior to sending it to the LCE server,
       saving bandwidth.
         For debugging purposes, event packet compression may be disabled, but this
       will
        increase the bandwidth required to send data from LCE clients to the LCE
       server.
        Setting the following option to 0 will disable compression only during
       transmission. -->
    <compress-events>1</compress-events>

</options>
```

Option	Description
log-directory	Directory where LCE Client logs are stored. If the **log-directory** keyword is commented out, then the client install directory will be used. Otherwise, ISO 9000 compliant log files will be saved in the specified directory.
heartbeat-frequency	The Tenable Network Monitor can be configured to send a "heartbeat" message to the LCE. This message indicates that the client is still alive and performing normally.
statistics-frequency	The frequency with which the Tenable Network Monitor sends a log entry containing performance statistics to the LCE.
filter-expression	The network monitor automatically generates a TCPDUMP filter expression that

	selects which network packets will be processed. This expression relies on the **syslog** monitoring settings being enabled.
lce-server	Directs the Tenable Network Monitor to the IP address or hostname of the LCE, and specifies the password used to connect.
server-port	The port the LCE listens to as designated by the **lce-server** directive.
interface	The network interface(s) from which the Tenable Network Monitor will report traffic.
monitor-syslog-port	The protocol/port designation that is used to forward **syslog** messages to the LCE server.
syslog-only	Directive to only report **syslog** messages; yes or no.
include-networks	Specify which networks are to be included in monitoring activity.
exclude-networks	Designate specific networks to exclude from monitoring activity.

Functionality

The **tnmd** tool will report on TCP sessions it sees. For example, if there is an FTP session, it will report when the session starts and when it is completed. If the session has no activity for a certain amount of time, **tnmd** will "time out" the session and log it as complete. For UDP and ICMP protocols, **tnmd** will log the individual packets. An example TNM alert is included in the screen capture below:

Time	Type	Sensor	Message
Jul 26, 2011 18:04	network	unknown	Tue Jul 26 18:02:35 - TNM-Long_TCP_Session_5_Minutes[554]: :49229 -> :80 [u:123 d:431]|1311717640|1311717755|115
Jul 26, 2011 18:09	network	unknown	Tue Jul 26 18:09:00 - TNM-Long_TCP_Session_5_Minutes[4685]: :49228 -> :80 [u:115 d:4570]|1311717640|1311718140|500
Jul 26, 2011 18:09	network	unknown	Tue Jul 26 18:09:00 - TNM-Long_TCP_Session_5_Minutes[8487]: :49230 -> :80 [u:326 d:8161]|1311717640|1311718140|500
Jul 26, 2011 18:14	network	unknown	Tue Jul 26 18:14:43 - TNM-Long_TCP_Session_5_Minutes[3837697]: :49981 -> :993 [u:42490 d:3795207]|1311718377|1311718483|106
Jul 26, 2011 18:14	network	unknown	Tue Jul 26 18:14:43 - TNM-Long_TCP_Session_5_Minutes[8688]: :49980 -> :993 [u:1576 d:7112]|1311718376|1311718483|107
Jul 26, 2011 18:23	network	unknown	Tue Jul 26 18:23:06 - TNM-Long_TCP_Session_5_Minutes[5103]: :50054 -> :80 [u:2891 d:2212]|1311718872|1311718986|114
Jul 26, 2011 18:23	network	unknown	Tue Jul 26 18:23:06 - TNM-Long_TCP_Session_5_Minutes[1852]: :50051 -> :80 [u:976 d:876]|1311718871|1311718986|115
Jul 26, 2011 18:24	network	unknown	Tue Jul 26 18:24:09 - TNM-Long_TCP_Session_5_Minutes[40372]: :45478 -> :22 [u:2452 d:37920]|1311718932|1311719049|117
Jul 26, 2011 18:24	network	unknown	Tue Jul 26 18:24:52 - TNM-Long_TCP_Session_5_Minutes[47802]: :55325 -> :22 [u:2909 d:44893]|1311718904|1311719092|188
Jul 26, 2011 18:29	network	unknown	Tue Jul 26 18:29:31 - TNM-Long_TCP_Session_5_Minutes[1027]: :50052 -> :80 [u:505 d:522]|1311718871|1311719371|500

Available fields within this raw output include (from left to right within the "Message" field):

- Alert date/time
- Alert name
- Amount of traffic captured
- Source IP:port
- Destination IP:port

- Uploaded bytes
- Downloaded bytes
- Start time (Unix timestamp)
- End time (Unix timestamp)
- Length of session (in seconds)

Alerts can indicate many traffic anomalies including TCP data flows that occurred where more than a gigabyte of traffic was detected within the flow, an unusual traffic pattern that could indicate malicious or non-compliant activity. Using this information within the raw output enables the user to get a better picture of what actually happened during the session and increases network traffic visibility.

When sending network traffic activity to the LCE, it is important to carefully consider the traffic source to monitor. The amount of network logs generated while monitoring a busy T3, 100 Mb, or even Gigabit link can vastly outweigh the total amount of firewall, web log and IDS logs. However, monitoring activity on key servers, key protocols, or even known malicious IP addresses is extremely useful.

When used to aggregate **syslog** messages from another set of servers, make sure to specify the correct destination IP addresses for the **syslog** messages. Otherwise, the Tenable Network Monitor may ignore **syslog** messages you actually want gathered. Tenable also recommends deploying the TNM directly in front of or on any **syslog** gathering servers.

The advantage of this is to work with the logs directly as they arrive from their source servers. **syslog** servers that forward messages often add additional data in front of the log, which increases the overall log size. In addition, logs that are forwarded often include source names for systems they may not be resolvable via DNS, making it harder to understand which system generated a log file. Using the TNM to sniff logs in motion preserves the source IP address of the original log.

Command Line Options

The **tnmd** binary has several command line options that are printed out when it is invoked with the **–help** option. Here is a list of the current options:

```
usage: ./tnmd [ -v ] [ -e ] [ -r <pcap file> ] [ -t <TCP timeout> ] [ expression ]
```

The **–v** option displays the version of the TNM. The **–e** will display the logs sent to the LCE on the local console via **stderr**. The **–r** option specifies a TCPDUMP binary file that can be used to send older logs to the LCE. The **–t** option specifies the amount of time of inactivity to be used by **tnm** before considering a TCP session dead. The last part of the command line allows for specification of a specific packet filter. Command line filtering options must be enclosed in quotation marks.

For example, the following command line can be used to run **tnmd** and log all network data except for UDP packets and ports 80 and 6346.

```
# ./tnmd "not proto 17 and not port 80 and not port 6346" &
```

A list of decimal protocol enumerations is found here:
http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml

The **tnmd** is usually started via the **network_monitor** RC script in the system startup directory (for example, **/etc/rc.d/init.d** on Red Hat Linux systems). To change the default packet filter in the startup script, edit this script and go to the following entry on or about line 21:

```
$NETWORK_MONITOR_DIR/$NETWORK_MONITOR_BIN &> /dev/null &
```

To modify this default setting, add your filter statement after the command statement such as this:

```
$NETWORK_MONITOR_DIR/$NETWORK_MONITOR_BIN tcp or icmp or udp port 514 &> /dev/null
```

This particular statement matches on any TCP or ICMP traffic and also collects any UDP based **syslog** traffic.

Performance Considerations
When running the TNM, it is important to consider how much data you are collecting and what you are doing with the data. If you are not doing anything with a certain set of data and you do not have a requirement to collect it, you can improve the performance of your LCE and the total useful storage capacity by not collecting it.

Consider these strategies when collecting logs:

- Ignoring UDP traffic in general, or at least UDP protocols to your basic services, can save you many records. For example, ignoring DNS lookups to your DNS servers will save you logging events that are repetitious.
- If you have acceptable logs from your email, web, and other services, consider ignoring port 80, port 443, and port 25 to these servers.
- If you have a long-term requirement to store logs but not necessarily network traffic, consider deploying a single LCE for log aggregation and then add a secondary LCE to gather network traffic. You might be able to store your logs much longer than your network traffic. With two LCEs, the LCE host can also query both of these and unify their results in a user-friendly graphical display.

LCE Linux Client Operations

This section describes the administrative functions of the LCE Linux clients including starting, halting and monitoring.

Starting the LCE Linux Clients

As noted earlier in this document, the LCE Client packages include start-up scripts that are installed in the system start-up directory (e.g., **/etc/init.d)** on the respective platform.

The provided start-up scripts are designed to check if the LCE Client is already running and will not start a second instance. Although it is possible to manually start the LCE Client without using the provided script, it is not recommended to do so as it could result in multiple instances of the LCE Client daemon running.

If there are errors in the configuration file, they will be displayed in the LCE Client log, which is under the appropriate client directory (e.g., **/opt/lce_client** for the LCE Log Agent, **/opt/network_monitor** for the Tenable Network Monitor client, etc. by default) in the format of **YEARMon.log**. At the LCE server, using the "**netstat -pan | grep 31300**" command will list all of the established LCE Client connections.

At any time, the version of the LCE Client can be determined by running it with the **-v** option, as follows:

```
# /opt/lce_client/lce_clientd -v
LCE Client 4.0.1
#
```

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

LCE Client	Starting Methods
Red Hat / CentOS	
LCE Client (Log Agent)	# service lce_client start or # /etc/init.d/lce_client start
LCE WMI Monitor Agent	# service wmi_monitor start or # /etc/init.d/wmi_monitor start
Tenable NetFlow Monitor	# service netflow_monitor start or # /etc/init.d/netflow_monitor start
Tenable Network Monitor	# service network_monitor start or # /etc/init.d/network_monitor start
Mac OS X	
LCE Client (Log Agent)	# SystemStarter start LCEClient

Halting the LCE Linux and Unix-Based Clients

LCE Client software can be halted using any one of three methods; Use the **kill** command to cause the process of the **lce_client** program to stop running, use the **service** command or use the **init.d** script. The following table demonstrates how to halt the various client software:

LCE Client	Halting Methods
Red Hat / CentOS	
LCE Client (Log Agent)	# service lce_client stop or # /etc/init.d/lce_client stop
LCE WMI Monitor Agent	# service wmi_monitor stop or # /etc/init.d/wmi_monitor stop
Tenable NetFlow Monitor	# service netflow_monitor stop or # /etc/init.d/netflow_monitor stop
Tenable Network Monitor	# service network_monitor stop or # /etc/init.d/network_monitor stop
Mac OS X	
LCE Client (Log Agent)	# SystemStarter stop LCEClient

On most Unix or Linux systems, running the command "**ps -e | grep lce_clientd**" will provide output similar to "32321 ? 00:00:15 lce_clientd". The first set of numbers is the process ID. Once the process ID is known, the command "**kill 32321**" can be used to kill the client process.

Monitoring Log Correlation Engine Client Status

While running, the **lced** process will keep track of LCE Client status in a file named **client.status** located in the **/opt/lce/admin/log** directory. Below is an example listing:

```
# cat /opt/lce/admin/log/client.status
Client[192.168.14.9]: Not logged in (state: PREVIOUSLY_CONNECTED status:Alive), LCE
       Client 4.0.0.0 20120620 0
Client[192.168.14.42]: Not logged in (state: PREVIOUSLY_CONNECTED status:Alive),
       NetFlow Monitor 4.0.0.0 20120620 0
Client[192.168.14.55]: Not logged in (state: PREVIOUSLY_CONNECTED status:Alive), WMI
       Monitor 4.0.0.0 20120615 0
Client[192.168.14.157]: Not logged in (state: PREVIOUSLY_CONNECTED status:Alive), LCE
       Client 4.0.0.0 20120615 0
```

For each configured LCE Client, the IP address specified in the LCE Client Manager or the **lce.conf** file will be displayed as well as if it is logged in, the type of client, version of client and if it is "alive" or "dead".

The **tail -f** command is not effective on this log file since it is completely re-written each time the **lced** process detects a change in a client's status.

Log Correlation Engine Client Reconnection Attempts

The LCE Client will attempt to reconnect every minute until it can re-establish a connection with the server if the following conditions occur:

- The LCE server **lced** process stops
- The network connection between the client and the server breaks
- The client is removed from the LCE Client Manager or server's configuration file (changing the server's configuration file requires a restart of the service to take affect)

Log Correlation Engine Windows Client

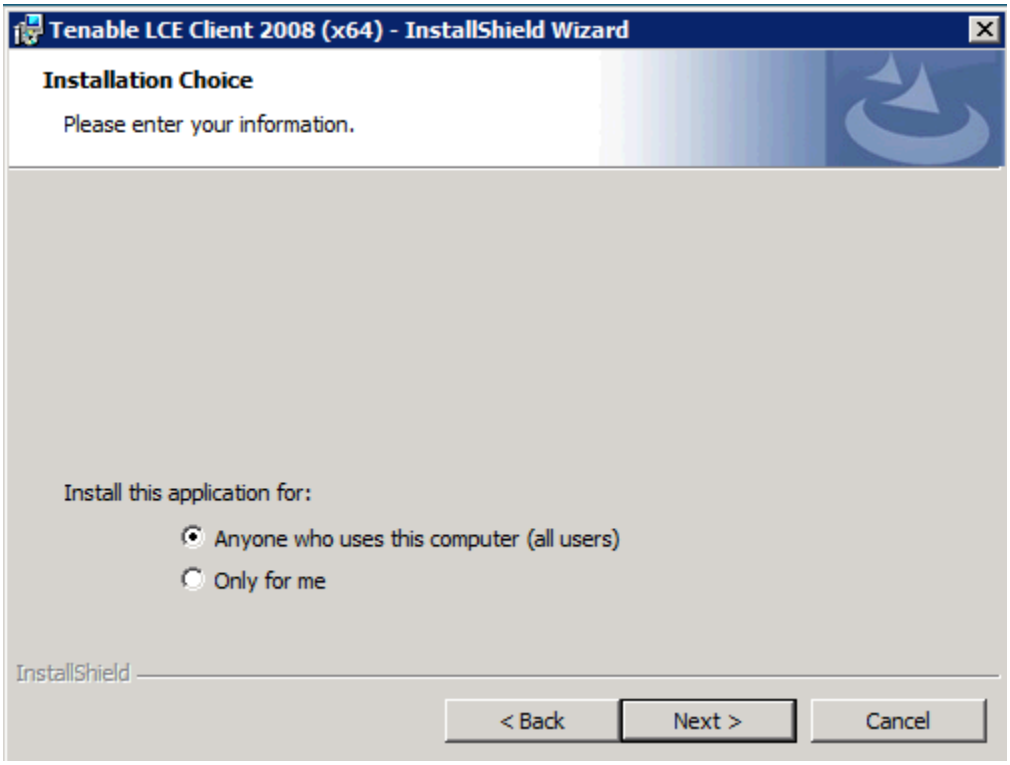
The Log Correlation Engine Windows Client monitors events, as well as specific log files or directories, for new event data. Tenable currently has two Windows LCE Clients: one for Windows XP/2003 platforms and one for Windows Vista/2008/7 platforms.

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

Installing the Windows Client

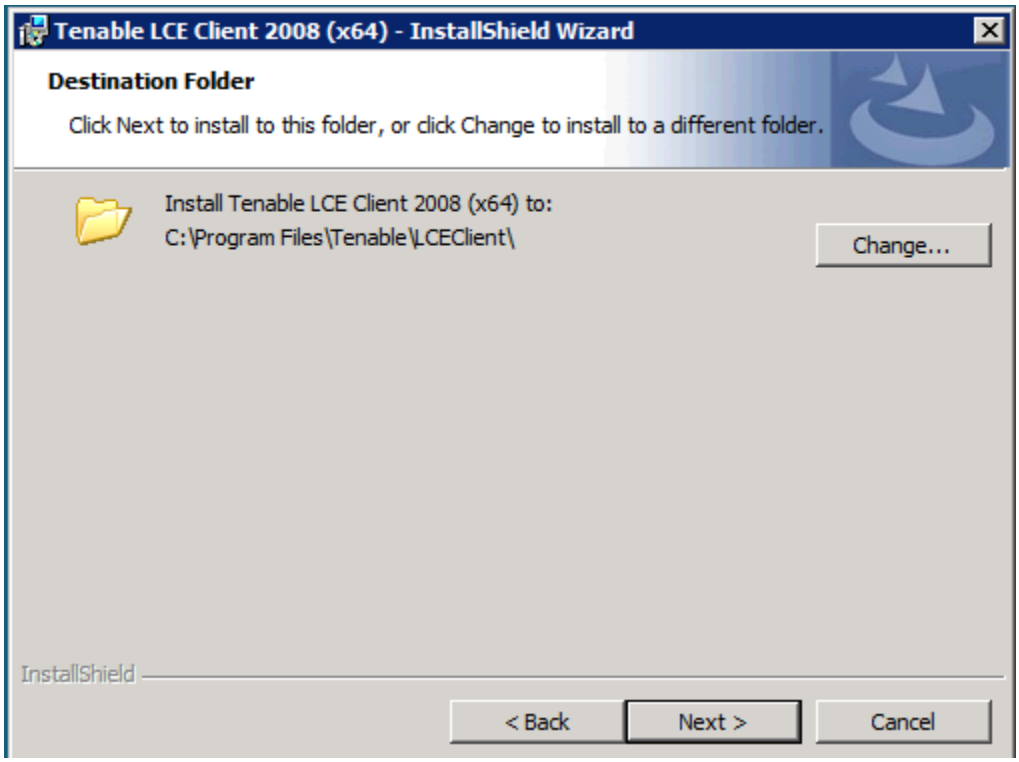
The LCE Windows Log Agent client is installed by clicking on the `.msi` distribution file, which will launch the InstallShield Wizard. On machines where Universal Access Control (UAC) is enabled, the user must run the installer as an Administrator level user. Right click on the installer icon and select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

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



Installation Location

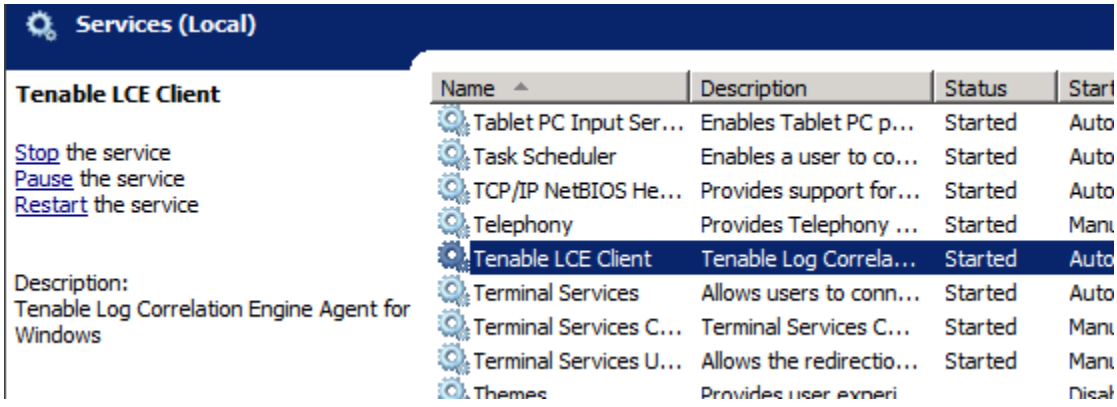
The next screen allows the user to change the default installation location:



Click the "Change…" button and select a new location if the application is to be installed in an alternate location. To use the default location, simply click "**Next**" and a screen will be displayed to begin the installation by clicking "**Install**". If this is an upgrade and a previous version of LCE Client is running, you may be prompted to either automatically close and restart the application or not close the running application and restart it at a later time for the new version to be applied. After a short period, the InstallShield Wizard will display a screen indicating that the installation is complete. Once installation is complete, you may be prompted to restart the system for the configuration changes to take effect.

Service Location

Once installation is complete, a new Windows Service named the "**Tenable LCE Client**" will be added that can be viewed through Control Panel -> Administrative Tools -> Services window as shown below:



Remote Installation/Configuration for Multiple Hosts

The installation of the LCE Windows Client can be accomplished from a command line or script via the execution of the "msiexec.exe" program. 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 Log Agent client MSI install package. Because all parameters (except LCE server IP address and port) are set using policies on the server, there are only a few options available.

Property	Description
ALLUSERS	1 = Installer tries to install for all users, fails if user rights are insufficient 2 = Tries all users first, then tries single user if that fails
PATH	The path that the program will be installed in. Specify the full path including the drive letter, and include the slash at the end of the path. Defaults to: "**`C:\Program Files\Tenable\LCEClient\`**"
SERVERIP	The IP address of the LCE server Defaults to: "203.0.113.250"
SERVERNAME	Designates the hostname of the LCE server for the client to use.
USERIP	Tells the client to use an IP address or hostname for its connection to the LCE server. A value of "0" will use the hostname and a value of "1" will use the IP address. Defaults to: "1"
VERBOSE	Controls the verbosity of the LCE Windows Log Agent client's own log. A value of "1" is the normal higher level of verbosity and a value of "0" is the reduced level. Defaults to: "1"

The following demonstrates an installation of the LCE Windows Log Agent client from the command line:

```
msiexec.exe /q /I "lce_client-4.0.1-windows_2008_x64.msi" SERVERIP="127.0.0.2"
```

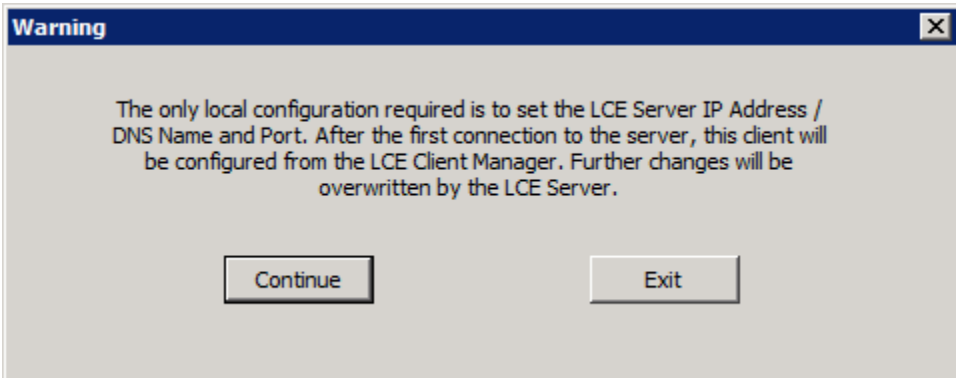
The "**`/q`**" on the above line instructs the installer to run with no user feedback. When performing an installation from the command line, the "**`/q`**" (or "**`/quiet`**" or "**`/qn`**") option can be used to keep the installation program from stopping the process to ask if previous settings should be applied. The "**`/i`**" is the operative parameter that specifies the name of the file to be installed.

Removing the LCE Windows Client

To remove the LCE Windows Log Agent client, under Control Panel, open "**Add or Remove Programs**" or "**Programs and Features**" depending on the version of Windows. Select "**Tenable LCE Client**" and then click the "**Change/Remove**" button. This will open the InstallShield Wizard. Follow the directions in this wizard to completely remove the LCE client.

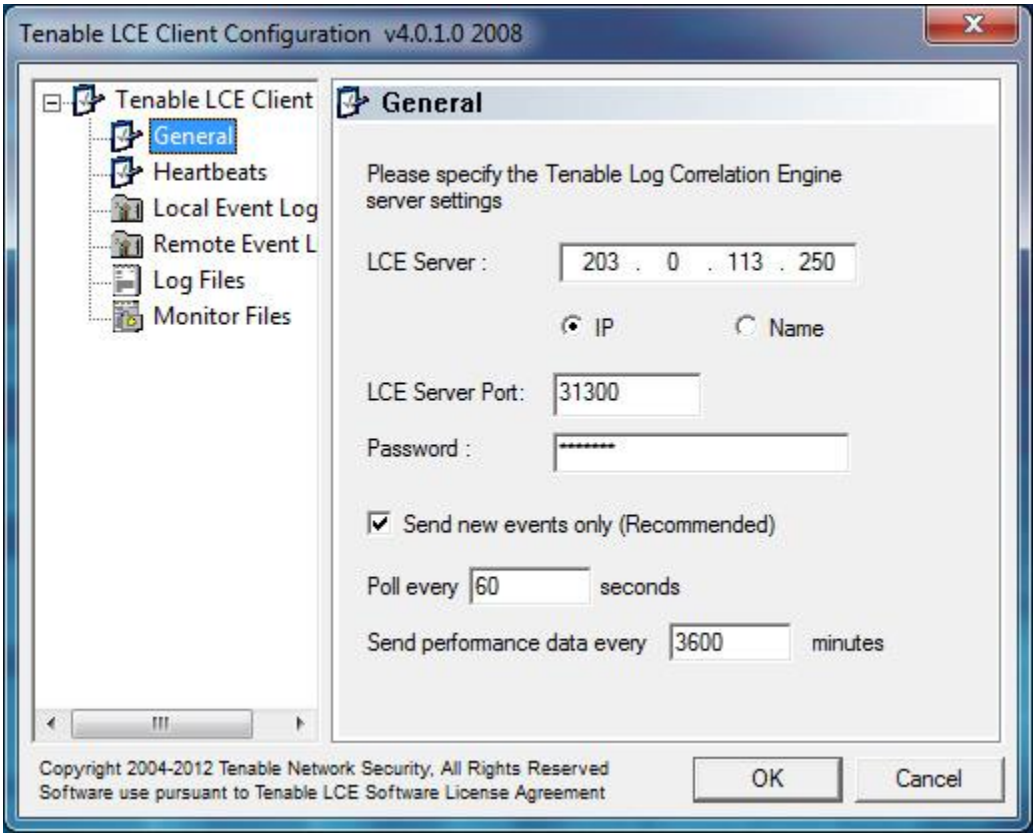
Windows Client Configuration

To configure the LCE Windows Log Agent client, launch the LCE Configuration tool located at "**C:\Program Files\Tenable\LCEClient\LCEConfig.exe**". Depending on options selected during installation, a shortcut icon(s) is created on the Desktop and the "**Start**" menu under "**Tenable Network Security**" called "LCEConfig". Once the configuration tool is launched, a warning message is displayed as follows:



When connecting to a LCE 4.x server, the only configuration required is the LCE server IP address or DNS name and the port (if the server is configured for one other than the default of 31300). All other configuration options will be managed by the LCE Client Manager upon connection.

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



By default, the LCE Log Agent client is configured using a non-routable documentation IP address (203.0.113.250) and LCE Server Port 31300. These settings must be changed to the IP address or hostname and listening port of the actual LCE server. No further local configuration is needed. Once set, select the “OK” button. The configuration window will close and will prompt to restart the LCE Client Service. Settings will not be applied until the service is restarted.

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

Policy Parameters
The following is a list of all valid “keys” available for use in with the Windows policies:

<table>
<tr><th>Key Name</th><th>Description</th><th>Valid Values</th></tr>
<tr><td>event-log</td><td>The name of a Windows NT Event log to monitor. Each event is sent to LCE as a new log.</td><td>Any NT event log name, or, “all” will monitor all NT event logs at the time the client is started.</td></tr>
<tr><td>flat-file</td><td>The full path and name of a text file to monitor. Each new line is sent to LCE as a new log.</td><td>Any fully qualified path and file name, with the file extension. It is best practice to escape folder separators with a backslash.</td></tr>
<tr><td>flat-file</td><td colspan="2">
<table>
<tr><th>Sub Key</th><th>Description</th></tr>
<tr><td>location</td><td>The full path of which to monitor text files. Each new line in each file is sent to LCE as a new log.</td></tr>
<tr><td>include</td><td>Optional sub key. Files at “location” will only be monitored if they match this pattern. Wildcards are allowed.</td></tr>
<tr><td>exclude</td><td>Optional sub key. Files at “location” will NOT be monitored if they match this pattern. Wildcards are allowed.</td></tr>
<tr><td>delete-on-size-bytes</td><td>Optional sub key. Files at “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.

EXERCISE CAUTION AND DISCRETION with this option - the LCE Client will attempt to delete log files above a certain size with this option.</td></tr>
</table>
If “flat-file” holds sub-keys, then “location” is the fully qualified path and file name. The other sub keys apply ONLY to the files monitored at this specified location.
</td></tr>
<tr><td>interval-log-seconds</td><td>The number of seconds between scanning logs watched with “flat-file”.</td><td>A non-zero integer</td></tr>
<tr><td>tail-subdirectories</td><td>Whether or not to follow subdirectories given in “flat-file” and “flat-file” “location” values. Setting this to “1” when watching large directories with no include/exclude filters (like C:\\Windows) may impact performance.</td><td>0 or 1
(0=off,1=on)</td></tr>
<tr><td>monitor-file</td><td>The full path and name of a file to monitor. If the file changes, the old and new MD5 checksums are sent in an event to the LCE server.</td><td>Any fully qualified path and file name, with the file extension. It is best practice to escape folder separators with a backslash.</td></tr>
<tr><td>monitor-file</td><td colspan="2">
<table>
<tr><th>Sub Key</th><th>Description</th><th>Valid Values</th></tr>
<tr><td>location</td><td>The full path at which to monitor binary files. For each file that changes, the old and new MD5 checksums are sent in an event to the LCE server.</td><td>Any fully qualified path and file name, with the file extension. It is best practice to escape folder separators with a backslash.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td><table>
<tr><td>include</td><td>Optional sub key. Files at “location” will only be monitored if they match this pattern. Wildcards are allowed.</td><td>Optional sub key. Files at “location” will only be monitored if they match this pattern. Wildcards are allowed.</td></tr>
<tr><td>exclude</td><td>Optional sub key. Files at “location” will NOT be monitored if they match this pattern. Wildcards are allowed.</td><td>Optional sub key. Files at “location” will NOT be monitored if they match this pattern. Wildcards are allowed.</td></tr>
</table></td></tr>
<tr><td>interval-monitor-seconds</td><td>The number of seconds between scanning files watched with “monitor-file”.</td><td>A non-zero integer.</td></tr>
<tr><td>monitor-subdirectories</td><td>Whether or not to follow subdirectories given in “monitor-file” and “monitor-file” “location” values. Setting this to “1” when watching large directories with no include/exclude filters (like C:\\Windows) may impact performance.</td><td>0 or 1
(0=off,1=on)</td></tr>
<tr><td>send-new-events-only</td><td>Whether to only send new events encountered. Setting this to “0” results in sending all data in all logs every time they are scanned, and thus it is NOT recommended unless specifically directed by Tenable Network Security.</td><td>0 or 1
(0=off,1=on)</td></tr>
<tr><td>heartbeat-frequency</td><td>The number of seconds between each client heartbeat message to the LCE server. If “0”, it will not send heartbeats.</td><td>A positive integer.</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) sent to the LCE server. If “0”, it will not send stats.</td><td>A positive integer.</td></tr>
<tr><td>compress-events</td><td>Whether or not to compress events before transmitting them to the LCE server. Marginally saves bandwidth, marginally increases CPU usage.</td><td>0 or 1
(0=off,1=on)</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 or 1
(0=off,1=on)</td></tr>
<tr><td>verbose</td><td>Enable or disable verbose logging in lce_client.log (the LCE client debugging log).</td><td>0 or 1
(0=off,1=on)</td></tr>
<tr><td>debug</td><td>Enable or disable debugging messages in lce_client.log (the LCE client debugging log). This is NOT recommended to be set to 1 unless specifically directed by Tenable Network Security.</td><td>0 or 1
(0=off,1=on)</td></tr>
<tr><td>host</td><td>Host contains sub keys describing a remote machine on which this LCE Client will perform monitoring via the WMI interface.
<table>
<tr><th>Sub Key</th><th>Description</th><th>Valid Values</th></tr>
<tr><td>ip</td><td>The IP address of the remote machine to monitor</td><td>A valid IPv4 address.</td></tr>
<tr><td>namespace</td><td>The namespace of the WMI classes being monitored (almost always root\cimv2)</td><td>A valid WMI namespace.</td></tr>
</table></td><td></td></tr>
</table>

domain	The domain of the remote machine to monitor	A valid domain name.
user	The username of the account on the remote machine that should be used for monitoring	A valid user account.
password	The password to use to login to the user account	A valid password. Be sure to escape special XML characters.
logfilename	A remote NT Log file to monitor	The name of a remote NT Log file.

For More Information

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

- Log Correlation Engine Architecture Guide – provides a high-level view of LCE architecture and supported platforms/environments.
- Log Correlation Engine Administrator and User Guide – describes installation, configuration, and operation of the LCE.
- Log Correlation Engine Quick Start Guide – provides basic instructions to quickly install and configure an LCE server. A more detailed description of configuration and management of an LCE server is provided in the "LCE Administration and User Guide" document.
- Log Correlation Engine Client Guide – how to configure, operate, and manage the various Unix, Windows, NetFlow, OPSEC, and other clients.
- LCE High Performance Configuration Guide – details various configuration methods, architecture examples, and hardware specifications for achieving high performance with Tenable's Log Correlation Engine, specifically for organizations with logging requirements in the tens of thousands of Events Per Second (EPS).
- LCE Best Practices – Learn how to best leverage the Log Correlation Engine in your enterprise.
- Tenable Event Correlation – outlines various methods of event correlation provided by Tenable products and describes the type of information leveraged by the correlation, and how this can be used to monitor security and compliance on enterprise networks.
- Tenable Products Plugin Families – provides a description and summary of the plugin families for Nessus, Log Correlation Engine, and the Passive Vulnerability Scanner.
- Log Correlation Engine Log Normalization Guide – explanation of the LCE's log parsing syntax with extensive examples of log parsing and manipulating the LCE's .prm libraries.
- TASL Reference Guide – explanation of the Tenable Application Scripting Language with extensive examples of a variety of correlation rules.
- Log Correlation Engine Statistics Daemon Guide – configuration, operation, and theory of the LCE's statistic daemon used to discover behavioral anomalies.
- Log Correlation Engine Large Disk Array Install Guide – configuration, operation, and theory for using the LCE in large disk array environments.

- Example Custom LCE Log Parsing - Minecraft Server Logs – describes how to create a custom log parser using Minecraft as an example.

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

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

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

Appendix 1: Sample Installation Output

Red Hat

The Red Hat distributions are in RPM format, similar to the following (the exact name of the client will depend on the client you are installing and target platform):

```
-rw-rw-r-- 1 user user 1.2M Nov 29 19:42 lce_client-4.0.1-es6.x86_64.rpm
```

To install the package, use the **rpm** command as shown in the following example:

```
 [root@europa src]# rpm -ivh lce_client-4.0.1-es6.x86_64.rpm
Preparing...                ########################################### [100%]

   1:lce_client             ########################################### [100%]
[root@europa src]#
```

Appendix 2: Sample Remove Output

Red Hat

To uninstall the LCE Log Agent client on a Red Hat platform, use the **rpm** command to first determine the installed package name, and then to remove it as shown in the following example:

```
 [root@europa src]# rpm -qa | grep lce_client
lce_client-4.0.1-es6.x86_64
[root@europa src]# rpm -ev lce_client-4.0.1-es6
[root@europa src]#
```

Appendix 3: Non-Tenable License Declarations

Below you will find third party software packages that Tenable provides for use with the Log Correlation Engine.

Section 1 (b) (ii) of the Log Correlation Engine License Agreement reads:

(ii) The Software may include code or other intellectual property provided to Tenable by third parties (collectively, "Third Party Components"). Any Third Party Component that is not marked as copyrighted by Tenable is subject to other license terms that are specified in the Documentation. By using the Software, you hereby agree to be bound by such other license terms as specified in the Documentation.

The Log Correlation Engine's Software License Agreement can be found on the machine in the top-level directory for the LCE application, `/opt/lce`.

Related 3rd Party and Open-Source Licenses

blowfish.h

This product includes cryptographic software written by Eric Young (eay@mincom.oz.au).
This product includes software written by Tim Hudson (tjh@mincom.oz.au).

crypto/bf/blowfish.h
Copyright (C) 1995-1998 Eric Young (eay@mincom.oz.au)
All rights reserved.

This package is an SSL implementation written by Eric Young (eay@mincom.oz.au).
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@mincom.oz.au).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
   "This product includes cryptographic software written by Eric Young (eay@mincom.oz.au)"
   The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
   "This product includes software written by Tim Hudson (tjh@mincom.oz.au)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

libCURL

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2011, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

OpenSSL

Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project
for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young
(eay@cryptsoft.com). This product includes software written by Tim
Hudson (tjh@cryptsoft.com).

zlib

(C) 1995-2010 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied
warranty. In no event will the authors be held liable for any damages
arising from the use of this software.

Permission is granted to anyone to use this software for any purpose,
including commercial applications, and to alter it and redistribute it
freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not
   claim that you wrote the original software. If you use this software
   in a product, an acknowledgment in the product documentation would be
   appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be
   misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly Mark Adler
jloup@gzip.org madler@alumni.caltech.edu

Hash functions

'Hash functions' is Copyright 2004-2008 by Paul Hsieh, and distributed under the LGPL 2.1 license.

OpenBSM

OpenBSM is covered by a number of copyrights, with licenses being either two or three clause BSD licenses. Individual file headers should be consulted for specific copyrights on specific components.

libpcap

License: BSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

libmcrypt

libmcrypt (part of the mcrypt project) is distributed under the LGPL 2.1 license.

libxml2

Libxml2 is the XML C parser and toolkit developed for the Gnome project (but usable outside of the Gnome platform), it is free software available under the MIT License.

About Tenable Network Security

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management, and compromise detection to help ensure network security and FDCC, FISMA, SANS CAG, and PCI compliance. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit http://www.tenable.com/.

GLOBAL HEADQUARTERS

Tenable Network Security
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
410.872.0555
www.tenable.com