Tenable Log Correlation Engine Web Query Client 4.8.x User Guide

Last Revised: November 07, 2023

Table of Contents

Get Started with the Log Correlation Engine Web Query Client **4**

Standards and Conventions 5

Hardware Requirements 6

Software Requirements 7

Licensing 8

Install, Configure, and Remove **9**

Download an Log Correlation Engine Client 10

Install the Log Correlation Engine Web Query Client 11

Configure the Log Correlation Engine Web Query Client 12

Remove the Log Correlation Engine Web Query Client 14

Features **15**

Monitor Amazon Web Services (AWS) 16

Monitor Salesforce 17

Monitor Google Cloud Platform (GCP) 18

Monitor and Limit Bandwidth 19

Monitor Client Statistics 20

How To **21**

How to Monitor Amazon Web Services (AWS) 22

Prerequisite Tasks for Integration with AWS 23

Configure the Web Query Client Policy for AWS 24

Review AWS Events in Tenable Security Center 26

How to Monitor Salesforce 28

Prerequisite Tasks for Integration with Salesforce 29

Configure the Web Query Client Policy for Salesforce 30
Review Salesforce Events in Tenable Security Center 32
How to Monitor GCP 33
Prerequisite Tasks for Integration with GCP 34
Configure the Web Query Client Policy for GCP 36
Review GCP Events in Tenable Security Center 39
Additional Resources 40
Authorize an Tenable Log Correlation Engine Client 41
Assign a Policy to an Tenable Log Correlation Engine Client 42
Client Policy Builder 43
Create a Client Policy with the Client Policy Builder 45
Edit a Client Policy with the Client Policy Builder 48
Clone a Client Policy with the Client Policy Builder 51
Web Query Client Policy Configuration Items 54
Correcting AWS Configuration Issues 63
Correcting Network Time Protocol Issues 65

Get Started with the Log Correlation Engine Web Query Client

This document describes the Log Correlation Engine Web Query Client version 4.8.x that is available for the Tenable Tenable Log Correlation Engine.

A working knowledge of Secure Shell (SSH), Tenable Log Correlation Engine (Log Correlation Engine), and Tenable Security Center 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.

Overview

The Log Correlation Engine Web Query Client is used to request event data from RESTful web services. The logs returned from queries are stored and normalized in Log Correlation Engine. Finally, the information may be searched in Tenable Security Center and can be reviewed. The process to setup and configure the Log Correlation Engine Web Query Client begins with the configuration of the RESTful API instances that are to be queried.

The Log Correlation Engine Web Query Client supports:

- Amazon Web Services (AWS)
- Salesforce
- Google Cloud Platform (GCP)

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Standards and Conventions

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Hardware Requirements

Hardware	Minimum Requirement
Processor	Dual Core x86-64
Processor Speed	2 Ghz
Ram	2 GB
Disk Space	100 MB

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Software Requirements

Operating System

The Tenable Log Correlation Engine Web Query Client is compatible with the following operating systems:

- Red Hat Enterprise Linux 6 64-bit
- CentOS 6 64-bit

Tenable Network Security

The Tenable Log Correlation Engine Web Query Client requires the following software:

- Tenable Log Correlation Engine 4.6.1 (Plugin Set 20151120 or later)
- Tenable Security Center 5.1.x or later

Amazon Web Services (AWS)

To monitor AWS, an IAM user account with read-only access to CloudTrail is required.

Salesforce

To monitor Salesforce, a connected app with read permission for the LoginHistory and User objects is required.

Google Cloud Platform (GCP)

To monitor GCP, a user must be created, the Cloud Pub/Sub service must be enabled, and Stackdriver Logging must be configured.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Licensing

Tenable Security Center must be licensed for the Tenable Log Correlation Engine Web Query Client. For more information, see Licenses in the *Tenable Security Center User Guide*.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Install, Configure, and Remove

This section includes the following instructions for installing, configuring, and removing the Log Correlation Engine Web Query Client. With the exception of downloading the Web Query Client, the following procedures must be performed on the command line.

- Download the Tenable Log Correlation Engine Web Query Client
- Install the Log Correlation Engine Web Query Client
- Configure the Log Correlation Engine Web Query Client
- Remove the Log Correlation Engine Web Query Client

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Download an Log Correlation Engine Client

For more information, see Tenable Log Correlation Engine Clients.

To download an Log Correlation Engine Client:

1. Access the Tenable Downloads page.

   The **Tenable Downloads** page appears.

2. Click **Log Correlation Engine**.

3. Select the **Tenable Log Correlation Engine** Client you want to download.

   The **License Agreement** page appears.

4. Review the Software License Agreement. If you agree to the terms, click the **I Agree** button.

   The client package is downloaded.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Install the Log Correlation Engine Web Query Client

Before you begin:

- Download the Log Correlation Engine Web Query Client, as described in Download an Log Correlation Engine Client.

To install the Web Query Client:

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

1. Copy the downloaded client package to the host where it will be installed.
2. Verify the MD5 checksum of the client package against the MD5 checksum found in the release notes.

   Example:

   ```
   # md5sum lce_webquery-4.6.0-el6.x86_64.rpm
   da9f07886a693fb69cba1dbd5c3eba31  lce_webquery-4.6.0-el6.x86_64.rpm
   ```

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

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

   Example:

   ```
   # rpm -ivh lce_webquery-4.6.0-el6.x86_64.rpm
   Preparing...                ########################################### [100%]
      1:lce_webquery           ########################################### [100%]
   Wrote UUID to /opt/tenable/tag
   Please run /opt/lce_webquery/set-server-ip.sh to configure your Tenable Log
   Correlation Engine server's IP and port.
   ```

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Configure the Log Correlation Engine Web Query Client

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

To configure the Web Query Client, you can execute the **set-server-ip.sh** script and include the Log Correlation Engine Server IP address and port number as arguments, or execute the script and, when prompted, enter the IP address and port number individually.

To execute the script using arguments:

1. Type **/opt/lce_webquery/set-server-ip.sh <IP> <Port>**, where *<IP>* is the IP address of an Log Correlation Engine Server and *<Port>* is the port number assigned to the server. By default, the port number is *31300*.

   The Log Correlation Engine Server IP address and port number are updated, and the Tenable Log Correlation Engine Web Query Client daemon is restarted.

   Example:

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

To execute the script without arguments:

1. Type **/opt/lce_webquery/set-server-ip.sh**

   You are prompted to enter the Log Correlation Engine Server IP address or hostname.

2. Type the IP address or hostname of Log Correlation Engine LCE server.

   You are prompted to enter the Log Correlation Engine server port.

3. Type the port number assigned to the server for Log Correlation Engine client communication. By default, the port number is *31300*.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

The Log Correlation Engine Server IP address and port number are updated, and the Log Correlation Engine Web Query Client daemon is restarted.

Example:

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

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


Enter the new desired LCE server port [31300].
>>
31300
Updating LCE Server IP from 203.0.113.1 to 192.168.22.11...
Updating LCE Server Port from 31300 to 31300...
Done
Stopping LCE Webquery daemon                               [  OK  ]
Starting LCE Webquery daemon                               [  OK  ]
```

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Remove the Log Correlation Engine Web Query Client

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

To remove the Log Correlation Engine Web Query Client:

1. To query the rpm database to obtain the name of the currently installed package, type **`rpm -qa |grep lce_`**.

   Example:

   ```
   # rpm -qa |grep lce_
   lce_webquery-4.6.0-el6.x86_64
   ```

2. Type **`rpm -e lce_webquery`**.

   The Web Query Client package is removed.

   Example:

   ```
   # rpm -e lce_webquery
   warning: /opt/lce_webquery/state.json saved as /opt/lce_
   webquery/state.json.rpmsave
   warning: /opt/lce_webquery/server_assignment.xml saved as /opt/lce_
   webquery/server_assignment.xml.rpmsave
   ```

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

   An additional directory, **/opt/tenable**, will be installed with the Web Query Client if it does not already exist. This directory contains a UUID that tracks all events related to the endpoint on which the client is installed. This directory should *only* be removed if no other Tenable products are in use, and no others will be installed on the endpoint in the future.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Features

This section describes the features available in the Tenable Log Correlation Engine Web Query.

- Monitor Amazon Web Services (AWS)
- Monitor Salesforce
- Monitor Google Cloud Platform (GCP)
- Monitor and Limit Bandwidth
- Monitor Client Statistics

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Monitor Amazon Web Services (AWS)

The Tenable Log Correlation Engine Web Query Client queries the AWS CloudTrail API in order to monitor events supported by CloudTrail. These events can be viewed in Tenable Security Center and used to identify irregular activity in AWS. In order to monitor CloudTrail events, you must enable CloudTrail, attach the necessary policy to IAM users or groups, and configure the Web Query Client policy to make calls to the CloudTrail API. Additionally, you can limit the amount of bandwidth the Web Query Client will use when communicating with CloudTrail, and monitor the hardware statistics of the host where the Web Query Client is installed.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Monitor Salesforce

The Tenable Log Correlation Engine Web Query Client queries the Salesforce REST API in order to monitor login events, as well as the creation and modification of user accounts. These events can be viewed in Tenable Security Center and used to identify irregular activity in Salesforce from unexpected sources. In order to monitor Salesforce events, you must create a connected app, and configure the Web Query Client policy to make calls to the Salesforce API. Additionally, you can limit the number of calls the Web Query Client will make to the Salesforce API to respect subscription limits, and monitor the hardware statistics of the host where the Web Query Client is installed.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Monitor Google Cloud Platform (GCP)

The Tenable Log Correlation Engine Web Query Client queries the Google Cloud API and the Google Cloud Pub/Sub service in order to monitor various events that you can specify when configuring logging in GCP. In order to monitor GCP events, you must enable the Pub/Sub API in Google Cloud, set up a topic, and configure the Web Query Client policy to make calls to the Pub/Sub service. Additionally, you can limit the number of calls the Web Query Client will make to the Pub/Sub service, and monitor the hardware statistics of the host where the Web Query Client is installed.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Monitor and Limit Bandwidth

The Tenable Log Correlation Engine Web Query Client monitors the number of calls made and bandwidth used while communicating with the Salesforce and AWS CloudTrail APIs. The monitored data can be viewed in Tenable Security Center. Additionally, when you configure a Web Query Client policy, you may specify limits on the number of calls or the amount of bandwidth the Web Query Client will use over a period of time. This feature can be leveraged to reduce costs related to AWS, or respect the call limit imposed by a Salesforce subscription, among other potential uses. Warnings are generated when usage reaches thresholds of 50%, 75%, and 90% of the defined limit.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Monitor Client Statistics

All Tenable Log Correlation Engine clients monitor the hardware statistics of the host where the client is installed. The hardware statistics can be viewed via the Tenable Log Correlation Engine server interface and Tenable Security Center. These statistics can be used to evaluate the resource and network usage of the host while the Tenable Log Correlation Engine client is operating.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

How To

This section describes how to perform the actions available in Tenable Log Correlation Engine Web Query Client.

You can configure the Web Query Client to query AWS CloudTrail, Salesforce, and Google Cloud Platform in order to track and review events.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

How to Monitor Amazon Web Services (AWS)

This section describes the steps necessary to query AWS with the Tenable Log Correlation Engine Web Query Client.

1. Complete the prerequisite tasks in AWS.
2. Configure the Web Query Client policy.
3. Review AWS events in Tenable Security Center CV.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Prerequisite Tasks for Integration with AWS

Before querying AWS with the Tenable Log Correlation Engine Web Query Client, you must perform the following tasks in AWS:

1. In the AWS console, enable CloudTrail.
2. Create one or more IAM users.
    - Generate an access key for each user.
    - Download the user security credentials.
3. Attach the AWSCloudTrailReadOnlyAccess policy to each user, or the group that contains the users, created in step 2.
4. Configure a Web Query Client policy to query CloudTrail.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Configure the Web Query Client Policy for AWS

Using the Client Policy Builder, you can create and modify policies for your Tenable Log Correlation Engine Web Query Client. The following steps are performed via the web interface on the Tenable Log Correlation Engine server that you configured your Tenable Log Correlation Engine Web Query Client to communicate with.

To configure the Web Query Client Policy for AWS:

1. Using the Client Policy Builder, create a policy for your Tenable Log Correlation Engine Web Query Client. This documentation includes a list of valid configuration items for the client policy.

   A Web Query Client policy for AWS requires you to add an AWS CloudTrail endpoint to the policy. You must provide the following:

   - The User ID and secret key that was created when completing the prerequisite tasks.

   To add the endpoint:

   a. In the **Basic** pane of the Client Policy Builder, click the ⊞ button in Group ⊞⊟ to add a group.

      The **Add a new endpoint group** window appears.

   b. Click the **Add AWS CloudTrail endpoint** button.

      A new AWS CloudTrail endpoint appears.

   c. In the **Endpoint name** box, enter a name that identifies the endpoint.

   d. Select the **Active** check box.

   e. In the **Query interval** box, enter the number of seconds between each query to the Salesforce API.

   f. In the **Region** box, enter the region defined in the AWS account.

   g. In the **Access Key ID** box, enter the Access Key ID for an IAM user.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

h. In the **Secret Access Key** box, enter the IAM Secret Access Key that corresponds to the Access Key ID.

> **Note:** You can add multiple endpoints to a single group. For example, one group could contain three AWS CloudTrail endpoints. Another group could contain a Salesforce endpoint, an AWS CloudTrail endpoint, and a Google Cloud endpoint.

2. Assign the policy to the Tenable Log Correlation Engine Web Query Client.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Review AWS Events in Tenable Security Center

To review AWS Events in Tenable Security Center:

1. Navigate to Tenable Security Center and log on with a user account that has permission to view logs for the organization.

   A dashboard that corresponds to the user role appears.

2. In the top navigation bar, click **Analysis**, and then click the **Events** link.

   The **Event Analysis** page appears, displaying the **Type Summary** section.

3. Click the **Type Summary** button, and then select **Normalized Event Summary**.

   The **Normalized Event Summary** section appears.

4. In the upper-left corner of the page, click » .

   The **Filters** pane appears.

5. Click the **Select Filters** button

6. In the **Add Filter** window, select **Normalized Event**.

7. Click the **Apply** button.

8. Click the **Normalized Event** box.

9. In the **Normalized Event** window, type *AWS-**.

10. Click **OK**.

11. In the **Filters** pane, click the **Apply All** button.

    In the **Normalized Event Summary** section, the list of events is filtered and displays only events that start with *AWS-*.

    The AWS events available will be based on the monitored activity logged by AWS CloudTrail. For a list of specific events, you can click an AWS event type (e. g., AWS-Console_Login) listed in the **Normalized Event Summary** section. You can also click the **Jump to Raw Syslog Events** link to directly view the log data.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

12. At the top of the **Event Analysis** page, click the **Normalized Event Summary** button, and then select **Detailed Event Summary**.

    The **Detailed Event Summary** section appears.

    For a list of specific events, click an AWS event (e. g., ConsoleLogin) listed in the **Detailed Event Summary** section.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

How to Monitor Salesforce

This section describes the steps necessary to query Salesforce with the Tenable Log Correlation Engine Web Query Client.

1. Complete the prerequisite tasks in Salesforce.
2. Configure the Web Query Client policy.
3. Review Salesforce events in Tenable Security Center.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Prerequisite Tasks for Integration with Salesforce

Before completing the procedures to integrate Tenable Log Correlation Engine with Salesforce, you must perform the following tasks in Salesforce:

1. Create a connected app.
    - Give the app read permission for the LoginHistory and User objects.
    - Save the Consumer Secret and Consumer Key.
2. Relax IP restrictions.

    > **Note:** This task is only necessary if you are unable to view Salesforce events in Tenable Security Center.

3. Configure a Web Query Client policy to query the Salesforce REST API.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Configure the Web Query Client Policy for Salesforce

Using the Client Policy Builder, you can create and modify policies for your Tenable Log Correlation Engine Web Query Client. The following steps are performed via the web interface on the Tenable Log Correlation Engine server that you configured your Tenable Log Correlation Engine Web Query Client to communicate with.

To configure the Web Query Client Policy for Salesforce:

1. Using the Client Policy Builder, create a policy for your Tenable Log Correlation Engine Web Query Client. This documentation includes a list of valid configuration items for the client policy.

   A Web Query Client policy for Salesforce requires you to add a Salesforce endpoint to the policy. You must provide the following:

   - The username, password, and security token of a Salesforce user account.
   - The Consumer Secret and Consumer Key you obtained when you created a connected app.

   To add the endpoint:

   a. In the **Basic** pane of the Client Policy Builder, click the button in Group to add a group.

      The **Add a new endpoint group** window appears.

   b. Click the **Add Salesforce endpoint** button.

      A new Salesforce endpoint appears.

   c. In the **Endpoint name** box, enter a name that identifies the endpoint.

   d. Select the **Active** check box.

   e. In the **Query interval** box, enter the number of seconds between each query to the Salesforce API.

   f. In the **Username** box, enter the username for the Salesforce account being queried.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

g. In the **Password** box, enter the password that corresponds to the username, along with that user's security token appended to the end of the password. For example, `passwordsREvNGuKHvuIhLTrS`.

h. In the **Consumer Key** box, enter the Consumer Key for the connected app you created.

i. In the **Consumer Secret** box, enter the Consumer Secret for the connected app you created.

> **Note:** You can add multiple endpoints to a single group. For example, one group could contain three Salesforce endpoints. Another group could contain a Salesforce endpoint, an AWS CloudTrail endpoint, and a Google Cloud endpoint.

2. Assign the policy to the Tenable Log Correlation Engine Web Query Client.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Review Salesforce Events in Tenable Security Center

To review Salesforce Events in Tenable Security Center:

1. Navigate to Tenable Security Center and log on with a user account that has permission to view logs for the organization.

   A dashboard that corresponds to the user role appears.

2. In the top navigation bar, click **Analysis**, and then click the **Events** link.

   The **Event Analysis** page appears, displaying the **Type Summary** section.

3. Click the **Type Summary** button, and then select **Normalized Event Summary**.

   The **Normalized Event Summary** section appears.

4. In the upper-left corner of the page, click » .

   The **Filters** pane appears.

5. Click the **Select Filters** button, and then, in the **Add Filter** popout, select **Normalized Event**.

6. Click the **Apply** button.

7. Click the **Normalized Event** box, and then, in the **Normalized Event** text box, type *Salesforce-*.

8. Click **OK**.

9. In the **Filters** pane, click the **Apply All** button.

   In the **Normalized Event Summary** section, the list of events is filtered and displays only events that start with *Salesforce-*.

   For Salesforce, the Web Query Client monitors login successes and failures, and the creation and modification of user accounts. For a list of specific events, click a Salesforce event type (e. g., Salesforce-Remote_Access_Login) listed in the **Normalized Event Summary** section. You can also click the **Jump to Raw Syslog Events** link to directly view the log data.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

How to Monitor GCP

This section describes the steps necessary to query GCP with the Tenable Log Correlation Engine Web Query Client.

1. Complete the prerequisite tasks in GCP.
2. Configure the Web Query Client policy.
3. Review GCP events in Tenable Security Center CV.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Prerequisite Tasks for Integration with GCP

Before completing the procedures to integrate Tenable Log Correlation Engine with GCP, you must perform the following tasks via the GCP Console:

1. Create a service account for Tenable Log Correlation Engine. When you create the service account:

   - Select **Furnish a new private key**.
   - For **Key type**, select **JSON**.

   A .json file that contains the public/private key pair is downloaded. This key pair is required for the Web Query Client policy.

   > **Note:** The previous link is to the official documentation for GCP. This procedure expects that you will be using the GCP Console to complete the tasks. After viewing the official GCP documentation, to see the instructions for the Console, in the boxes that appear on the page, click **Console**.
   >
   > For example:
   >
   > REST CONSOLE GCLOUD
   >
   > - Open the **Service Accounts** page in the Cloud Platform Console.
   >
   > OPEN THE SERVICE ACCOUNTS PAGE
   >
   > - Click **Select a project**.
   > - Select your project and click **Open**.
   > - Click **Create Service Account**.
   > - Enter a service account name, select a role you wish to grant to the service account and click **Create**.

2. If you have not already, complete the steps required to enable the Pub/Sub API. Then, create a topic and add a subscription.

   - For **Delivery Type**, select **Pull**.

   Note the subscription name. The subscription name is required for the Web Query Client policy.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

> **Note:** The previous links are to the official documentation for the Pub/Sub service. It includes sections about publishing a message to a topic, pulling the message from a subscription, and cleaning up. For the purpose of this procedure, those sections can be ignored.

3. If you want to you want to obtain logs from one or more Google Compute Engine or Amazon EC2 VM instances, install the logging agent on those instances.
4. Configure Stackdriver Logging to export one or more logs to the topic you created in step 2. Those logs will be processed by the Web Query Client.
5. Configure a Web Query Client policy to pull logs from the Pub/Sub service.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Configure the Web Query Client Policy for GCP

Using the Client Policy Builder, you can create and modify policies for your Tenable Log Correlation Engine Web Query Client. The following steps are performed via the web interface on the Tenable Log Correlation Engine server that you configured your Tenable Log Correlation Engine Web Query Client to communicate with.

To configure the Web Query Client Policy for GCP:

1. Using the Client Policy Builder, create a policy for your Tenable Log Correlation Engine Web Query Client. This documentation includes a list of valid configuration items for the client policy.

   A Web Query Client policy for GCP (Google Cloud Platform) requires you to add a Google Cloud endpoint to the policy. You must provide the following:

   - The service account key in the .json file that was downloaded when completing the prerequisite tasks.
   - The subscription name for the Pub/Sub service topic.

   To add the endpoint:

   a. In the **Basic** pane of the Client Policy Builder, click the ⊞ button in Group ⊞⊟ to add a group.

      The **Add a new endpoint group** window appears.

   b. Click the **Add Google Cloud endpoint** button.

      A new Google Cloud endpoint appears.

   c. In the **Endpoint name** box, enter a name that identifies the endpoint.

   d. Select the **Active** check box.

   e. In the **Query interval** box, enter the number of seconds between each query to the Cloud Pub/Sub service.

   f. In the **JSON service account key** box, enter the entire service account key including the braces.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

For example:


```
{
  "type": "service_account",
  "project_id": "blinkum-genovese-011599",
  "private_key_id": "d644c15c7332d29574f0f36ec31659db2e7cdad2",
  "private_key": "-----BEGIN PRIVATE KEY-----
  \nPmxlQ6i3kz/sO7NtLX2lcRuUAzgHiET99UAlqLWGsF2Msqfb38rtvBfFOmTg+NOQH8BkX8Xbh-
  GPN1Ks4xDHxtgKbSvWlUg+Eit3rSp1NuWjSz7YqUuCSgsOwbbRQvXtNKvr2RllbFyyymMpakB6i-
  XT5UnfJqftZa5M6pWlMt2wikmkRQxlmpJTHPmaRr3fyhnYJqM/v\TJL4bjprvuYSqzMiXaWq0\F-
  o0ND28kB30dAhhao5NM6oykq8\OdYc6v534Y+eQfpkpOCN8qRyTTzyYLh0fKm2vEzO/O2n7+jm3-
  1h/zNlLqXf/87HsKE8TwGqw05xii21XlrL3\j8DKrNuYy9UClaxxND/r8ncgK6Cv\AYp1DJ1qLw-
  2aIndYZaN9iXyvVQ5GdpUazj0eHORbibfjMCwP1diOAlnmlXfYMk3hTjT2/+teZtOplDL/4OCzu-
  P\k3foR5\G5aTFKo2+w8N5wmtg5ehvDsmMmvfP2TPxIZia6BPD0uyKdESMOZOfsEgSNSFPoaIUq-
  /qV1IrA7Q2XwtGzWuqDcALJi7x65IxrIivXUrHv379AjgrXW6SnKEFLJ1LtHi9dGBElnI+h3mx+-
  \\z\v0X8d1vJed4tjOMNvWRaAhXhuNouAly7Xt3Eug9OCTX+di9esV7kF++heG/8yQLIQCyeBRM-
  fot4SnDvw7xJ0sKSOKv5MOi8t6HGLsggvFR5R6V6lx3BwqeljYJDNdOYInFYKcI3DUQ8aumNLOJ-
  fEi2st9pR2sH6xb7sKSF5odeSkOoAEPqDBoOrTrYdjMUx/uRTfZBRkhKH3zVGqwR8E4HWLYnuy5-
  vr/yEiJ/xjTS1SfVQ+mw2vVq3UdrGhPOyjEljvGAi6FAccIaJV4LkGrEKjYA6vO6n2Gswt4pR\F-
  Z6IQj9CU8D5rUnmuJ9VP3O2ivHWkXWIBZzUZjFI3TWRZWncZXhQ8ySki6cHW7ng06WsQeN2wfP0-
  UHHPCqkeQo1VOL+5e3POgb0izNCdy3a+ffk9XrMZo91MvyqdwPLOunI6cgcoTLlslDgwrbYvcjU-
  AcYG6iI6/CC5o5ws\5CNlIl/JgE1IQlI48815H+q/67GUaywyR2Sfd\c4nRcNRUMJNWjzzntjra-
  AhBy19NmKaEWKitgSFQIf1o9uatXo4s\OcPzL2ejY2bTF+1Sgo1yatsg5UWZjhb0dPabiAWKQJo-
  Zmilq7jKJ++o\ayooYOVR1kimXuhiX9RrlKLsRy0vL4KjnY3Rg2UTI5zoPyAdr4VFTsLuZ8\0WM-
  F8/BxcASBhPCu9f4YI9hL3Qnhf4sV2+cMDUR71uv7LXIzhsaz9TDDKRvqyEoRGVo1EiNjClCrF4-
  IPzDRwfRoAD7SegAKt5gLF+XkE5PWrVqYD9iTxj7tK\yyOR9nRRswgsz3MW78hVJXKcvSVh06m\-
  2S55MiSBp/Qm4U9Rjtnpy1SwNc8818A6DKQtUfM/R+rR\Nl9pmMo2yPBNRX+5F0KMKRsvYuDWuh-
  gvXmWIV19I8+Aif4kh9XUpJBQtrHrFD1wRDQ2HNV+vgklewhMOiHmSqTc5oZlNQmOH0+dgKwkkN-
  gc12yu/z5FSOxm\bl0b+fZ54KI3lJa45jJyq3+BMyN0pJ\nIWoSRqSIbyD/TlmGsfGzoQLTrUm1-
  SgLh2RKmaCogdBlsGg6hD2C8Uf\n-----END PRIVATE KEY-----\n",
  "client_email": "test-credential-service-acct@blinkum-genovese-
  011599.iam.gserviceaccount.com",
  "client_id": "404842616201342653591",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://accounts.google.com/o/oauth2/token",
```


Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

```
  "auth_provider_x509_cert_url":
  "https://www.googleapis.com/oauth2/v1/certs",
  "client_x509_cert_url":
  "https://www.googleapis.com/robot/v1/metadata/x509/test-credential-service-
  acct%40blinkum-genovese-011599.iam.gserviceaccount.com"
}
```

g. In the **Subscription** box, enter the subscription name. For example, `projects/my-project-name/subscriptions/my-subscription-name`.

> **Note:** You can add multiple endpoints to a single group. For example, one group could contain three Google Cloud endpoints. Another group could contain a Salesforce endpoint, an AWS CloudTrail endpoint, and a Google Cloud endpoint.

2. Assign the policy to the Tenable Log Correlation Engine Web Query Client.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Review GCP Events in Tenable Security Center

To review GCP Events in Tenable Security Center:

1. Navigate to Tenable Security Center and log on with a user account that has permission to view logs for the organization.

   A dashboard that corresponds to the user role appears.

2. In the top navigation bar, click **Analysis**, and then click the **Events** link.

   The **Event Analysis** page appears, displaying the **Type Summary** section.

3. Click the **Type Summary** button, and then select **Normalized Event Summary**.

   The **Normalized Event Summary** section appears.

4. In the upper-left corner of the page, click » .

   The **Filters** pane appears.

5. Click the **Syslog Text** box, and then, in the **Syslog Text** text box, type *googleapis*.

6. Click **OK**.

7. In the **Filters** pane, click the **Apply All** button.

   In the **Normalized Event Summary** section, the list of events is filtered and displays events that include *googleapis* in the text of the syslog.

   The GCP events available will be based on the logs you specified when you configured Stackdriver Logging. You can click the **Jump to Raw Syslog Events** link to directly view the log data.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Additional Resources

This section contains the following additional resources:

- Authorize an Tenable Log Correlation Engine Client
- Assign a Policy to an Tenable Log Correlation Engine Client
- Client Policy Builder
- Web Query Client Policy Configuration Items
- Correcting AWS Configuration Issues
- Correcting Network Time Protocol Issues

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Authorize an Tenable Log Correlation Engine Client

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

> **Note:** Client authorization is completed in the web-based Tenable Log Correlation Engine Interface on the Clients page.

To authorize a client to communicate with an Tenable Log Correlation Engine server:

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

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

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

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

   The Tenable Log Correlation Engine clients are authorized and will immediately send a heartbeat.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Assign a Policy to an Tenable Log Correlation Engine Client

In addition to using Tenable Security Center and the **Policies** page, you can assign policies to Tenable Log Correlation Engine clients via the **Clients** page.

To assign a policy to a client:

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

   The **Clients** page appears, displaying the client table.
3. In the client table, in the row corresponding to the Tenable Log Correlation Engine client that you want to assign a policy, select the check box.

   > **Note:** You can assign a policy to multiple Tenable Log Correlation Engine clients by selecting the corresponding check boxes. The selected Tenable Log Correlation Engine clients must be the same client type, and support the same operating system. The selected clients will be assigned the same policy.
4. Above the client table, in the upper-left corner, click the **Actions** button, and then click **Change Policy**.

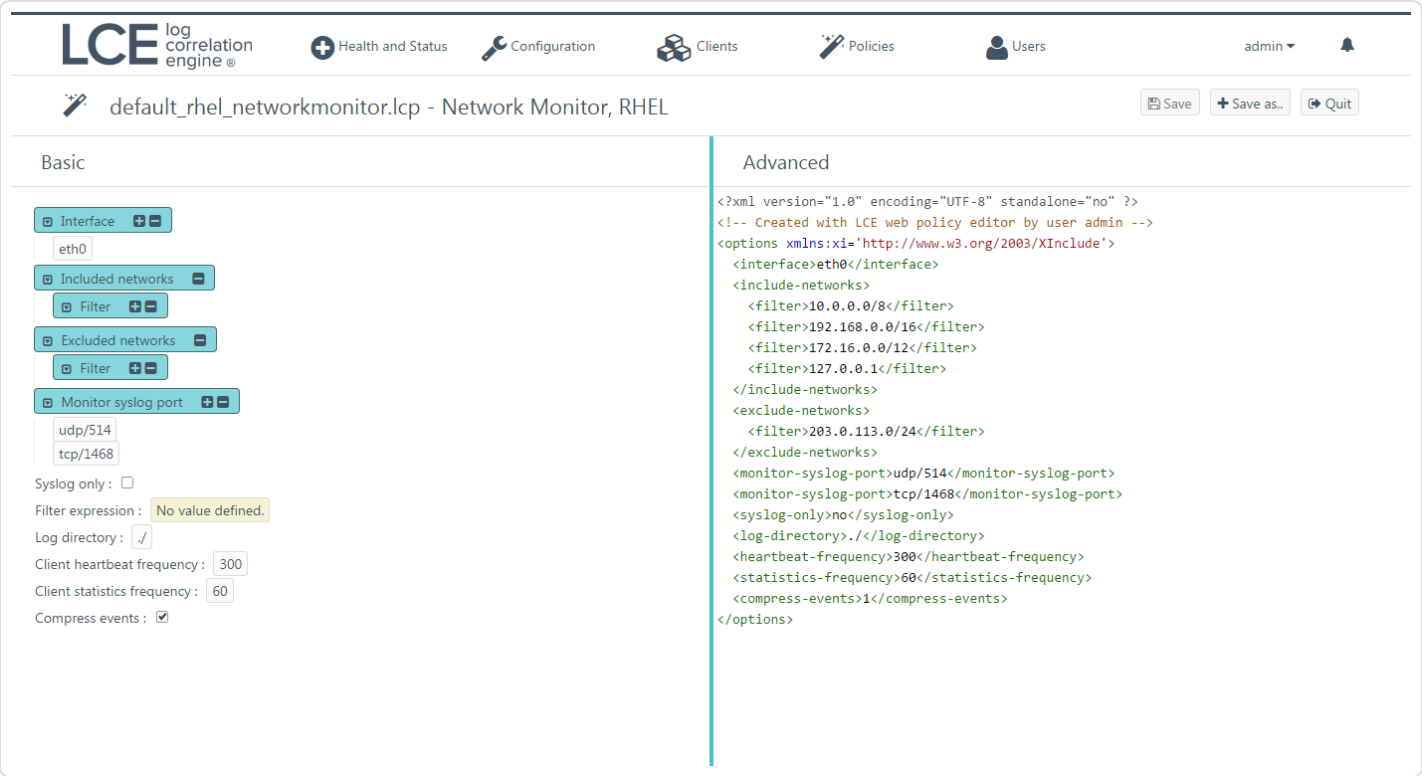
   The **Change policy** dialog box appears.
5. In the **Assign the following policy** list, select the policy that you want to assign to the Tenable Log Correlation Engine client.
6. Review the Tenable Log Correlation Engine client that will have a new policy, and then click the **Change policy** button.

   The specified policy is assigned to the LCE client.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Client Policy Builder

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



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

In the **Basic** pane:

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

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

In the **Advanced** pane:

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

> **Note:** It is recommended that only advanced users utilize the **Advanced** pane.

Primarily, the Builder will be used to:

- Create a Client Policy
- Edit an Existing Client Policy
- Clone an Existing Client Policy

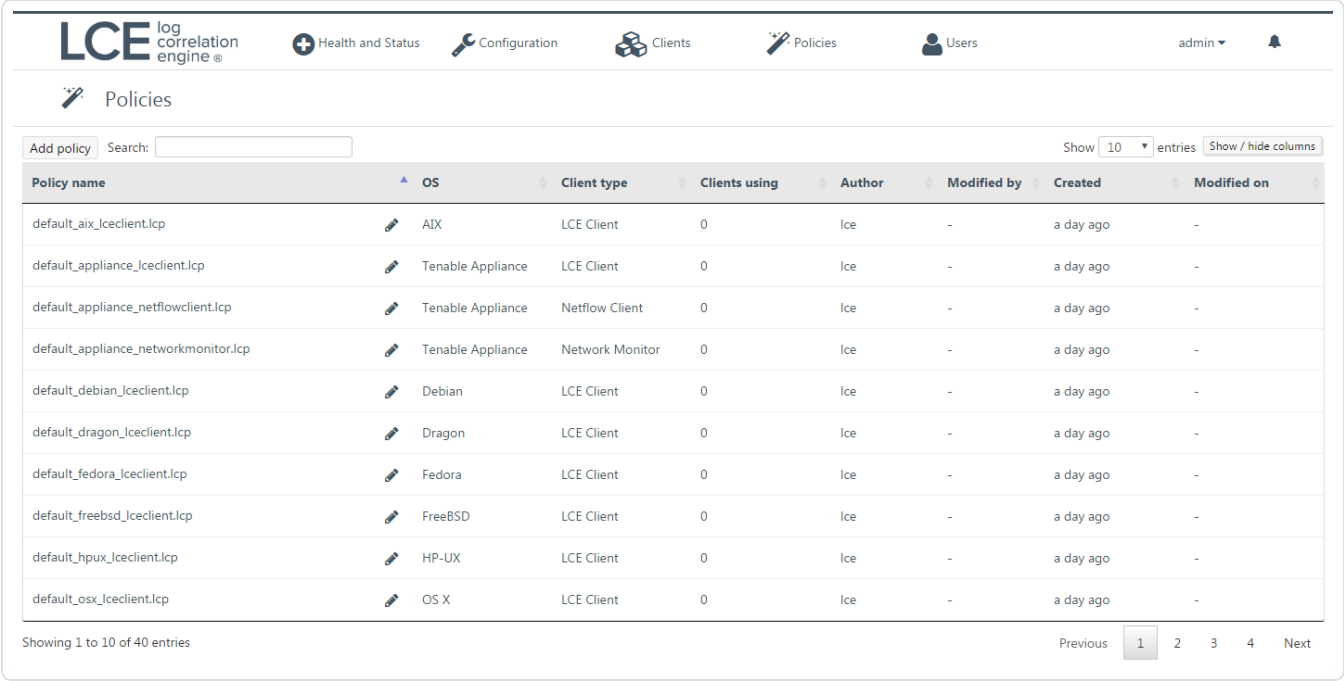
Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

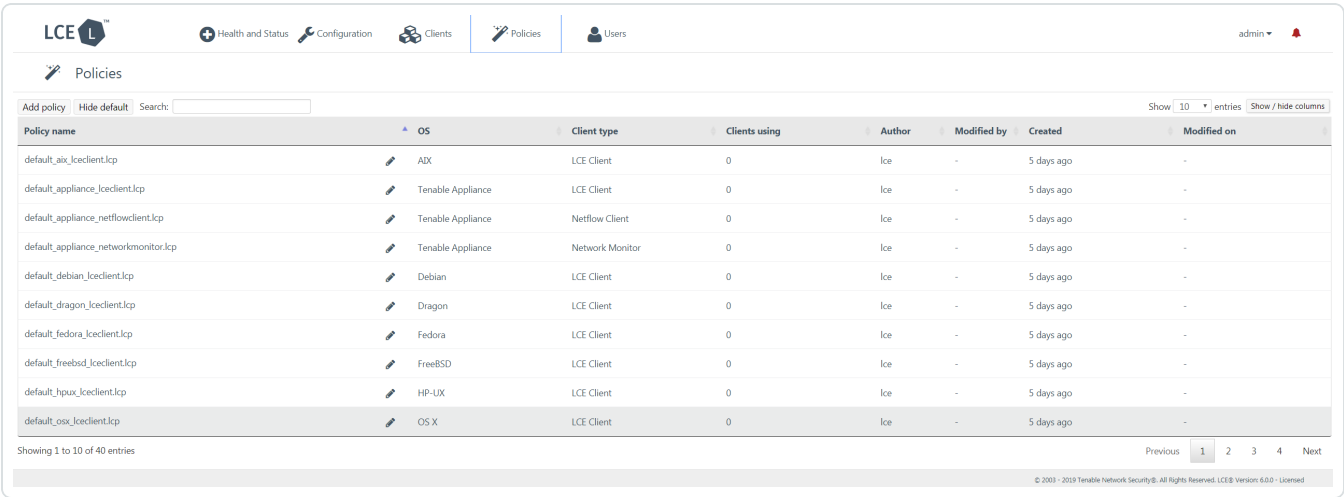
Create a Client Policy with the Client Policy Builder

To create a client policy with the client policy builder:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Policies**.

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





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

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

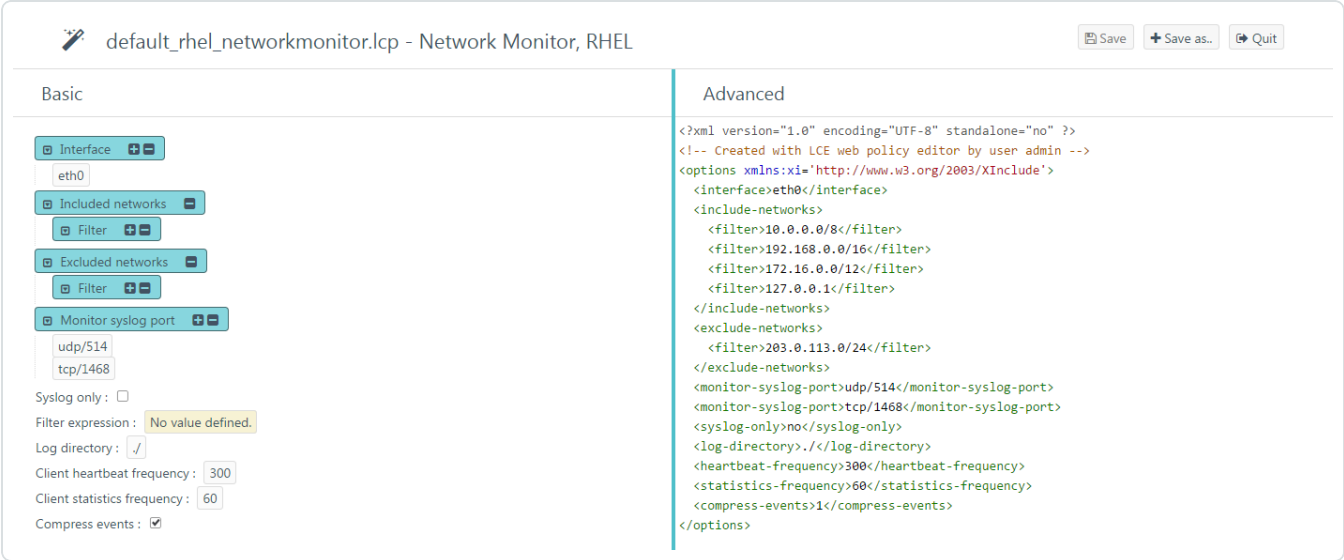
The **Client Policy Builder** window appears, displaying the **Create** section.

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

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

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

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



> **Note:** The list of configuration items in the **Basic** pane includes items that do not yet have a configured value. If the configuration item normally accepts a value, *No value defined* will be displayed. In the case of a group, that group will not contain any items.

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

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

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

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

7. Click the **Save as** button.

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

8. In the **Filename** box, type a name for the policy. A valid file name cannot include the phrase *default* or *TNS* as a prefix, and cannot include spaces or underscores. Do not include a file extension. The operating system, client, and file extension will be appended to the name when the policy is saved.

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

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

9. Click **OK**.

   Log Correlation Engine saves your configuration.

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

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

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

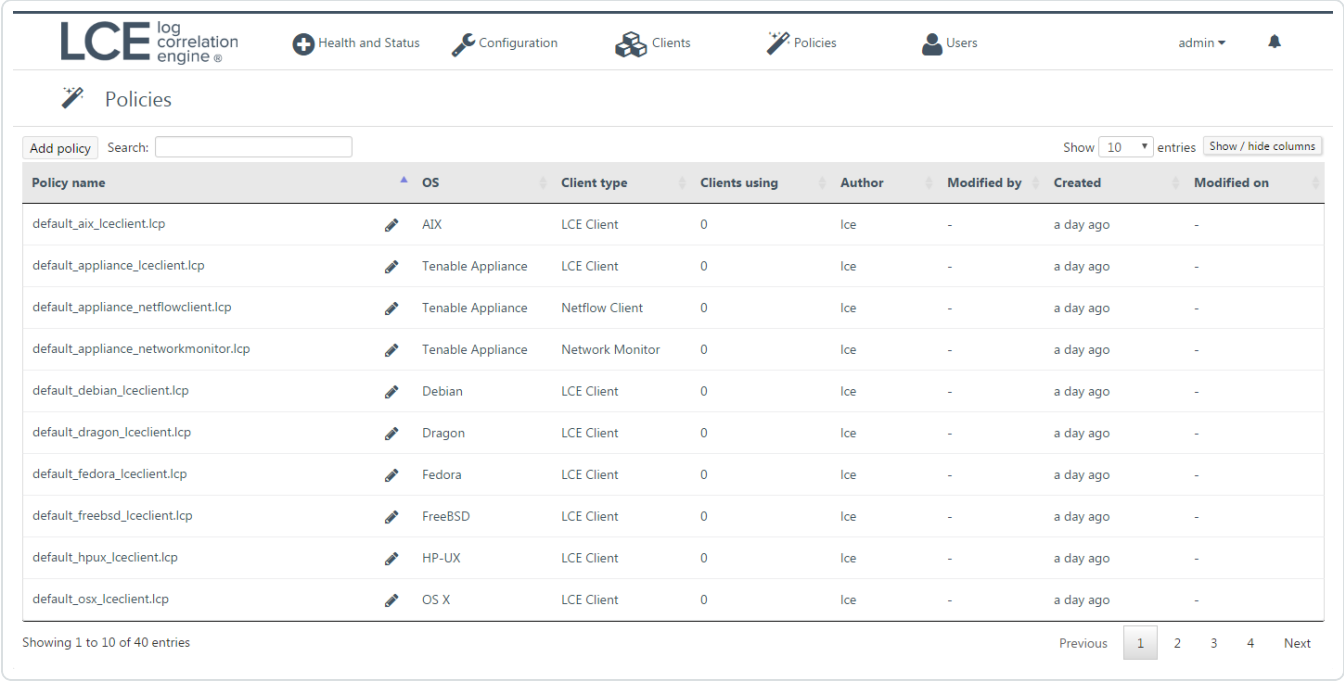
Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

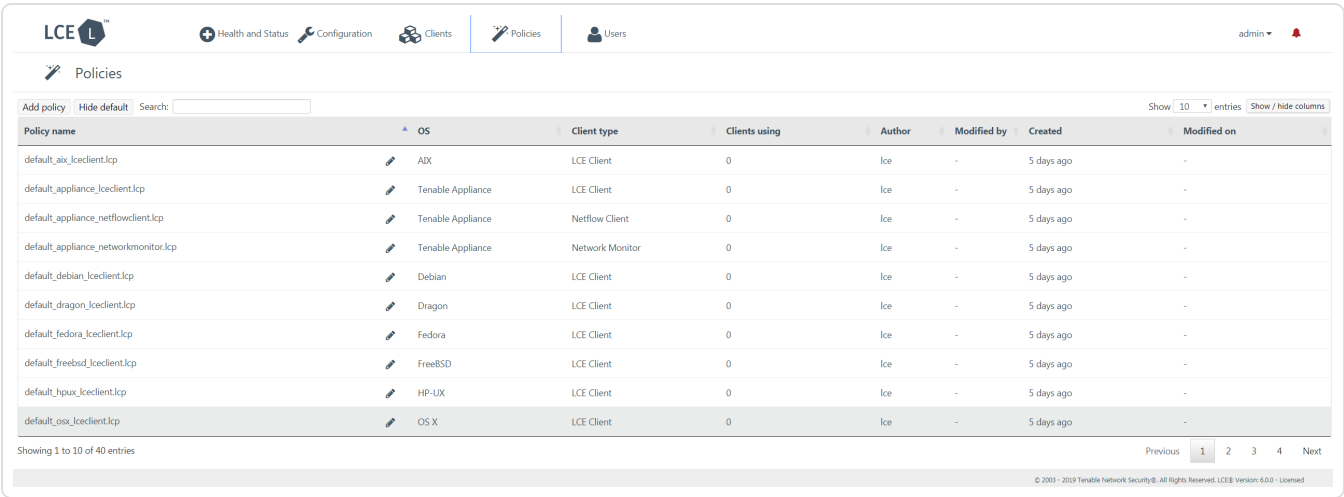
Edit a Client Policy with the Client Policy Builder

To edit a client policy with the client policy builder:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Policies**.

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





Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

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

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

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

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

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

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

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

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

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

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

7. Click **OK**.

   Log Correlation Engine saves your configuration.

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

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

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

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

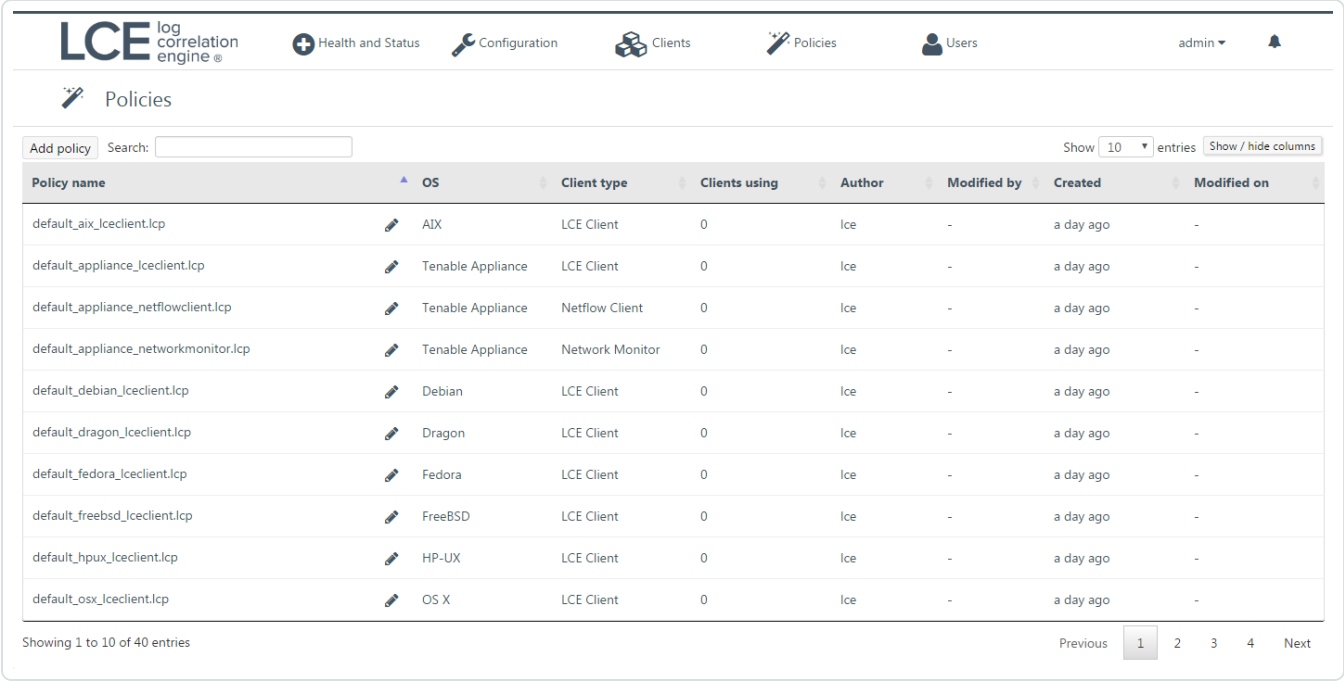
Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

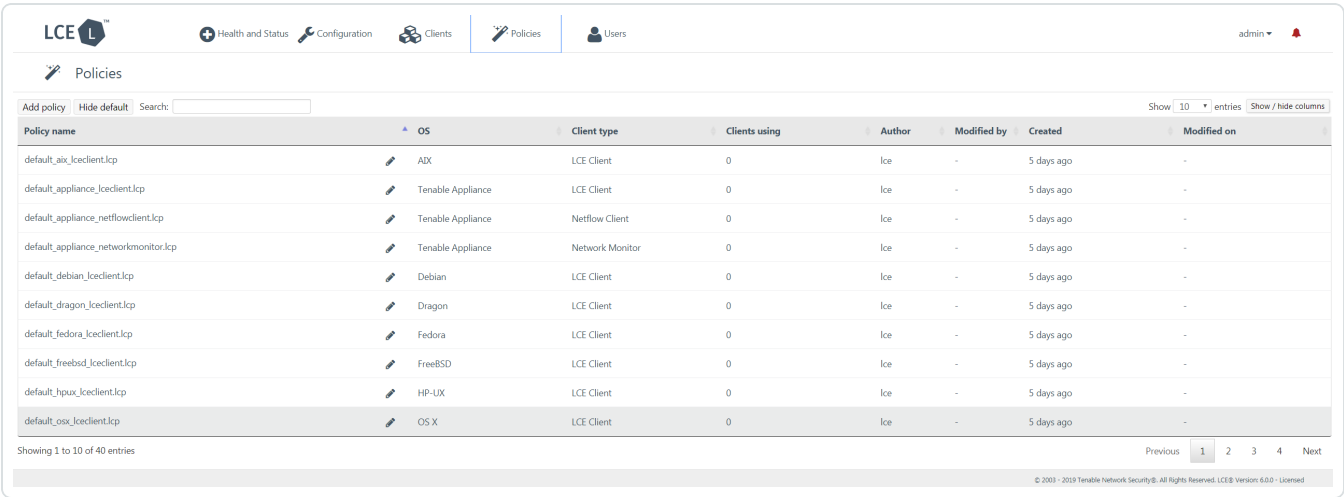
Clone a Client Policy with the Client Policy Builder

To clone a client policy with the client policy builder:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Policies**.

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





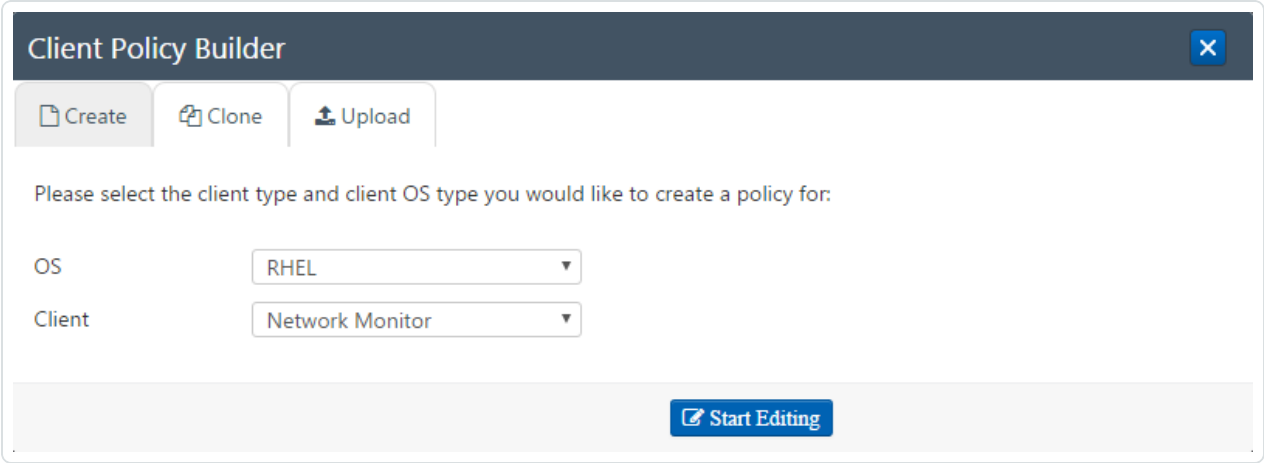
Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

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

   -or-

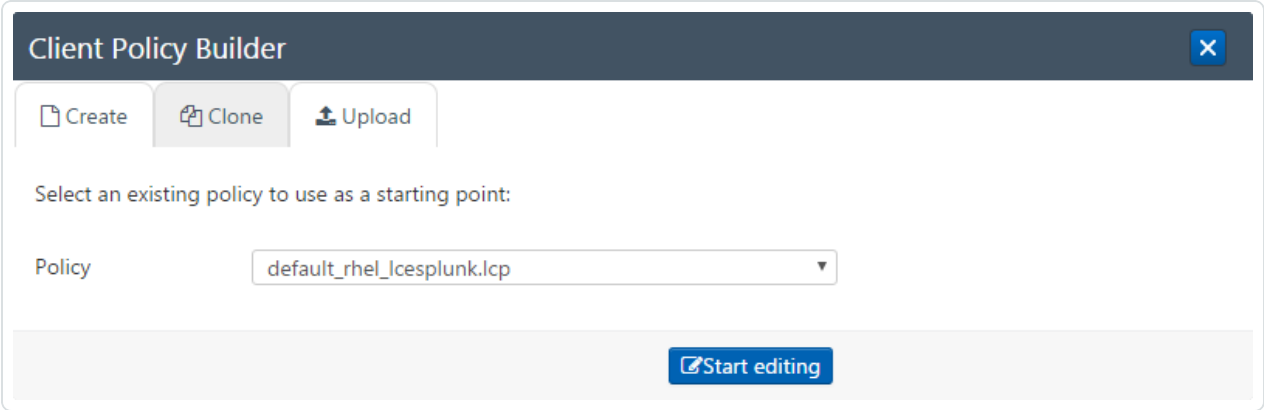
   a. In the upper-left corner of the policy table, click the **Add policy** button.

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



   b. Click the **Clone** tab.

      The **Clone** section appears.



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

   The Client Policy Builder appears. At the top of the Builder, the title bar displays the name of the policy that you selected. A complete list of configuration items that are valid for the type

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

of policy appear in the **Basic** pane. XML source code with corresponding values appears in the **Advanced** pane.

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

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

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

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

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

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

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

7. Click **OK**.

   Log Correlation Engine saves your configuration.

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

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

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

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Web Query Client Policy Configuration Items

The interaction of the Web Query Client with AWS, Salesforce, and GCP is configured by modifying a Web Query Client policy via the Client Policy Builder. The policy is separated into configurable items, represented in the **Advanced** pane of the Client Policy Builder by XML elements of the same name. Certain parameters are common to all Tenable Log Correlation Engine clients and are generally the parameters listed first in a policy.

The usage and application parameters that follow the common client parameters vary based on the client. In the case of the Web Query Client policy, parameters are provided that allow you to limit the bandwidth the Web Query Client will use, as well as specify the credentials required for connecting to AWS, Salesforce, and GCP.

This section includes:

- Example: **default_rhel_web** Policy
- Common Client Parameters
- Usage-Limit Parameters
- CloudTrail Parameters
- Salesforce Parameters
- GCP Parameters

Example: **default_rhel_web** Policy

The following is an example of the contents of a Web Query Client policy file.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<options xmlns:xi="http://www.w3.org/2003/XInclude">
    <log-directory>/opt/lce_webquery/logs</log-directory>
    <debug-level>INFO</debug-level>

    <!--<local-ip-net>192.0.2.0/24</local-ip-net>-->

    <!-- client-debug / -->
    <heartbeat-period>300</heartbeat-period>
    <statistics-period>60</statistics-period>
```

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

```
    <compress-events>1</compress-events>
    <group>
    </group>

    <!-- Group Setup Example
    <group>
        <name>ByteRestrictedGroup</name>
        <usage-limit>
            <type>BYTES</type>
            <value>35M</value>
            <time>MONTH</time>
            <start-day>5</start-day>
        </usage-limit>
        <cloudtrail>
            <name>CloudTrail1</name>
            <active>yes</active>
            <query-interval-seconds>600</query-interval-seconds>
            <region>us-east-1</region>
            <id>AWSId</id>
            <key>MySecretKey</key>
        </cloudtrail>
    </group>
    <group>
        <name>CallRestrictedGroup</name>
        <usage-limit>
            <type>CALLS</type>
            <value>10000</value>
            <time>DAY</time>
        </usage-limit>
        <salesforce>
            <name>Salesforce_1</name>
            <active>no</active>
            <query-interval-seconds>300</query-interval-seconds>
            <username>MyUsername</username>
            <password>MyPassword</password>
            <consumer-key>MyKey</consumer-key>
            <consumer-secret>MySecret</consumer-secret>
        </salesforce>
        <salesforce>
```

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

```
            <name>Salesforce_2</name>
            <active>yes</active>
            <query-interval-seconds>450</query-interval-seconds>
            <username>MyUsername</username>
            <password>MyPassword</password>
            <consumer-key>MyKey</consumer-key>
            <consumer-secret>MySecret</consumer-secret>
        </salesforce>
    </group>
    -->
</options>
```

Common Configuration Items

The following table lists the policy configuration items in the order they appear in the default Web Query Client policy. These parameters are defined when configuring the Web Query Client policy for AWS, Salesforce, and GCP.

Configuration Item	Description	Example
log-directory	The path to which to write the Web Query Client operational logs.	/opt/lce_webquery/logs
debug-level	Minimum debugging level that is printed to the log. The options supported are as follows: • INFO • WARN • ERROR • NONE	INFO
local-ip-net	If a host has multiple network connections, allows you to specify which network to use. If not set or if the CIDR does not match any networks, the client will use the first network connection detected.	192.0.2.0/24

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Configuration Item	Description	Example
heartbeat-frequency	The number of seconds between each client heartbeat message to the Tenable Log Correlation Engine server. If set to *0*, the client will not send heartbeats.	A positive integer. 300
statistics-frequency	The number of minutes between each client host performance statistics report (CPU, Disk Space, and Physical Memory) to the Tenable Log Correlation Engine server. If set to *0*, client statistics will not be sent.	A positive integer. 60
compress-events	Defines whether to compress events before transmitting them to the Tenable Log Correlation Engine server. If set to *1*, provides a marginal savings for bandwidth in exchange for a marginal increase in CPU usage.	0 (off) or 1 (on)
Write events to standard output	Whether to write events to standard output (stdout). Any event picked up by the Tenable Log Correlation Engine Splunk Client will have the raw log printed to the stdout of the client, the default being a terminal session, before the client sends it to the Tenable Log Correlation Engine server to be processed. This configuration item is useful for debugging and troubleshooting.	0 (off) or 1 (on)

Usage-Limit Configuration Items

The configuration of the usage-limit items is usually based on the API being queried. The AWS CloudTrail API measures the amount of bandwidth utilized by the queries made to the API. The Salesforce API measures the number of calls. Because CloudTrail and Salesforce monitor usage differently, generally groups will be limited by bytes or calls based on the API. However, the Web Query Client can be configured to support many use cases, such as limiting usage of the Salesforce API by bytes. The usage limit parameters are in place to help control excess bandwidth charges, and

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

respect call limitations that are applied by the API vendor.

The following table lists the usage-limit parameters in the order they appear in the Client Policy Builder. These parameters are defined when configuring a Web Query Client policy for AWS, Salesforce, or GCP.

Configuration Item	Description	Example Value
name	An alphanumeric name for the connection group.	ByteRestrictedGroup
type	Groups can either be limited by BYTES or CALLS	BYTES
value	This is the numeric value given to BYTES or CALLS. **Note:** Bytes can be represented by a number followed by K(Kilobyte), M(Megabyte) G (Gigabyte), or T(Terabyte).	100M
time	The period of time by which usage is limited. For example, if a group is limited to 1000 calls, and this parameter is set to DAY, usage is limited to 1000 calls every 24 hours.	MONTH, DAY, HOUR, MINUTE
start-day	Defines the starting day when the *time* parameter is set to *MONTH*. The value can be an integer from 1 to 28.	14

CloudTrail Parameters

The following table lists the CloudTrail parameters in the order they appear in the Client Policy Builder. These parameters are defined when configuring a Web Query Client policy for AWS.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Policy Parameter	Description	Example Value
name	An alphanumeric name for the CloudTrail connection.	AWSgroup
active	Defines whether to query the instance. If set to *yes*, the Web Query Client will make queries using the parameters defined in that CloudTrail subsection. You can have multiple subsections that are configured to be active.	yes
query-interval-seconds	The number of seconds between each query to the endpoint.	300
region	The region defined in the AWS account.	us-east-1
id	An IAM Access Key ID.	IKADIY6VH42HTKTQI4OA
key	The IAM Secret Access Key that corresponds to the Access Key ID.	koN/ByNBZB5S7/tOrT3WBrGD9dQjDvT98bU9qpyH

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Salesforce Parameters

The following table lists the Salesforce parameters in the order they appear in the Client Policy Builder. These parameters are defined when configuring a Web Query Client policy for Salesforce.

Policy Parameter	Description	Example Value
name	An alphanumeric name for the Salesforce connection.	SalesforceGroup
active	Defines whether to query the instance. If set to *yes*, the Web Query Client will make queries using the parameters defined in that Salesforce subsection. You can have one or more subsections in multiple groups that are configured to be active.	yes
query-interval-seconds	The number of seconds between each	300

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Policy Parameter	Description	Example Value
	query to the endpoint.	
username	The username for the Salesforce account being queried.	user@example.com
password	The password that corresponds to the username, and that user's security token appended to the end of the password.	passwordsREvNGuKHvulhLTrS
consumer-key	The Consumer Key for a connected app.	1MVG7KI2HHAq08RzmvrJMfFaXELNe_Tbg1vJf.xUyRK7f5Hyso2bZrW.TobC9XQ.jqzNVP0ytuD_1XrKKFsku
consumer-secret	The Consumer Secret for a connected app.	8675309731701479235

GCP Parameters

The following table lists the GCP parameters in the order they appear in the Client Policy Builder. These parameters are defined when configuring a Web Query Client policy for GCP.

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Policy Parameter	Description	Example Value
name	An alphanumeric name for the GCP group.	GCP
active	Defines whether to query the instance. If set to *yes*, the Web Query Client will make queries using the parameters defined in that GCP subsection. You can have one or more subsections in multiple groups that are configured to be active.	yes
query-interval-seconds	The number of seconds between each query to the endpoint.	300
json-service-account-key	The service account key for a GCP user.	The contents of a .json file downloaded from GCP.
Subscription	The subscription name for the Google Pub/Sub service topic.	projects/example-project080116/subscriptions/logging-feed-topic

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Correcting AWS Configuration Issues

The AWS command line interface (CLI) can be installed to troubleshoot AWS connection and configuration issues. Information about installation of AWS CLI can be found here.

To correct AWS configuration issues:

1. The first command will configure the AWS CLI. If it was previously ran the AWS Access Key ID, AWS Secret Access Key, and region name will already be populated. This information is also found in the policy file. An example of the output from this command is shown below.

```
C:\>aws configure
AWSAccess Key ID [****************JSQJ]:
AWS SecretAccess Key [****************yaGQ]:
Default region name [us-west-2]:
Default output format [None]:
```

2. The second command will describe trails that are available if the configuration criterion was entered correctly in the previous step. It will also provide the names of the trails that are available to be queried. An example of the output from this command is shown below.

```
C:\>aws cloudtrail describe-trails
{
    "trailList": [
        {
            "IncludeGlobalServiceEvents": true,
            "Name": "test_trail",
            "TrailARN": "arn:aws:cloudtrail:us-west-2:920172477660:trail/test_tr
ail",
            "LogFileValidationEnabled": false,
            "S3BucketName": "client-api-test-bucket",
            "CloudWatchLogsRoleArn": "arn:aws:iam::920172477660:role/CloudTrail_
CloudWatchLogs_Role",
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-west-2:920172477660:lo
g-group:CloudTrail/DefaultLogGroup:*"
        }
    ]
}
```

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

3. Using the name of the trail you can query the trails status. From the output, you can tell if the trail is logging and the start and stop logging time in Epoch time of the trail. An example of the output from this command is shown below.

```
C:\>aws cloudtrail get-trail-status --name test_trail {
    "LatestNotificationAttemptSucceeded": "",
    "LatestDeliveryAttemptTime": "2015-11-02T05:04:50Z",
    "LatestDeliveryTime": 1446440690.306,
    "TimeLoggingStarted": "2015-10-26T21:43:08Z",
    "LatestDeliveryAttemptSucceeded": "2015-11-02T05:04:50Z",
    "IsLogging": true,
    "LatestCloudWatchLogsDeliveryTime": 1446243728.775,
    "StartLoggingTime": 1445895788.299,
    "StopLoggingTime": 1444418827.475,
    "LatestNotificationAttemptTime": "",
    "TimeLoggingStopped": "2015-10-09T19:27:07Z"
}
```

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Correcting Network Time Protocol Issues

If you are not receiving any AWS events, and the message below is found in the logs Network Time Protocol (NTP), it should be checked to ensure it is configured correctly.

```
Oct 28, 15 14:38:26.898556 (endpoint_0) INFO (webquery_
endpoint.cpp:168,sendHealthStatus) - LCE Web Client Status: Alert: Endpoint
Demo/CloudTrail-test-Cloud: CloudTrail query signature was invalid, and no further
queries will be submitted.  Check your system clock and timezone.  To resume querying,
update the system clock or restart the client.
```

To correct Network Time Protocol issues:

1. Running the clock or date command will show the current time of the server.

   ```
   # clock
   Wed 04 Nov 2015 04:33:29 PM EST  -0.266432 seconds
   # date
   Wed Nov  4 16:33:32 EST 2015
   ```

2. The following command can be run to re-sync the time with the configured NTP servers if the time is found to be incorrect.

   ```
   # ntpd -qg
   ntpd: time set -6.953726s
   ```

3. After the time is has been re-synced stop the Log Correlation Engine Web Query Client using the command below.

   ```
   # service lce_webquery stop
   ```

4. Remove the state.json file from the /opt/lce/webquery directory.

   ```
   # rm -rf /opt/lce_webquery/state.json
   ```

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

5. Start the Log Correlation Engine Web Query Client.

```
# service lce_webquery start
```

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.