Dell CEE

Using the Common Event Enabler on Linux Platforms

Version 9.x

March 2025
Rev. 11

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Additional resources

As part of an improvement effort, revisions of the software are periodically released. Therefore, some functions described in this document might not be supported by all versions of the software currently in use. The product release notes provide the most up-to-date information on product features. If a product does not function properly or does not function as described in this document, contact your Customer Support representative.

Where to get help

Support, product, and licensing information can be obtained as described below.

Product information

For product and feature documentation or release notes, go to Online Support at dell.com/support.

Troubleshooting

For information about products, software updates, licensing, and service, go to Online Support (registration required) at: dell.com/support. After logging in, locate the appropriate product page.

Dell E-Lab Interoperability Navigator

The Dell E-Lab Interoperability Navigator is a searchable, web-based application that provides access to product interoperability support matrices. It is available on Online Support at dell.com/support. After logging in:

- Click **Diagnostics & Tools**.
- Under **Dell Data Center Tools**, click **E-Lab Navigator**.

1

Introduction

Topics:

About CEE

The Dell Common Event Enabler (CEE) framework is used to provide a working environment for the Common Event Publishing Agent (CEPA) facility, which includes subfacilities for anti-ransomware, auditing, backup, content/quota management (CQM), Common Asynchronous Publishing Service (VCAPS), and indexing.

CEPA is a mechanism whereby applications can register to receive event notification and context from sources such as Dell PowerStore systems. The event publishing agent delivers to the application both event notification and associated context in one message. Context may consist of file metadata or directory metadata that is needed to decide business policy.

The CEPA subfacilities include:

- Auditing—A mechanism for delivering post-events to registered consumer applications in a synchronous manner. Events are delivered individually in real-time.
- Backup—A mechanism for delivering post-events in bulk mode to backup applications. A backup-specific delivery cadence is based on either a time period or a number of events.
- CARA—A mechanism for delivering post-events in bulk mode to anti-ransomware applications. A specific delivery cadence is based on either a time period or a number of events.
- CQM—A mechanism for delivering pre-events to registered consumer applications in a synchronous manner. Events are delivered individually in real-time, allowing the consumer application to exercise business policy on the event.
- Index—A mechanism for delivering events to Splunk Enterprise or the Splunk Cloud in asynchronous mode. The delivery cadence is based on either a time period or a number of events.
- VCAPS—A mechanism for delivering post-events in asynchronous mode. The delivery cadence is based on either a time period or a number of events.

> **NOTE:** If both CQM events and Auditing events are present, CEPA delivers events to the CQM application first, and then delivers events to the Auditing application.

This document is intended for use by customers who want to use CEE with consumer applications (such as for quotas or content type) to manage content stored on file systems.

System requirements

System requirements describes the Dell software, hardware, network, and storage configurations.

Table 1. System requirements

Type	Requirement
Software	One of the following: ● Mainstream supported SUSE Enterprise Linux versions for 32-bit and 64-bit operating systems. ● Mainstream supported Red Hat Enterprise Linux versions for 64-bit operating systems. Three kits are available: ● `emc_cee_SLES-yyy.i386.rpm` for installation on 32-bit SUSE platforms ● `emc_cee_SLES-yyy.x86_64.rpm` for installation on 64-bit SUSE platforms ● `emc_cee_RHEL-yyy.x86_64.rpm` for installation on 64-bit Red Hat Enterprise platforms

Table 1. System requirements (continued)

Type	Requirement
	where *yyy* = software version number Search the Dell E-Lab™ Interoperability Navigator for consumer applications supported when using CEE and CEPA.
Hardware	Recommend using 16 GB Memory with two core processors.
Network	No specific network requirements.
Storage	No specific storage requirements.

Support for third-party applications

CEPA provides event notifications and contexts to consumer applications that monitor the SMB/CIFS and NFS file system activity on the NAS Server. The consumer applications require event notifications from the NAS server to organize the access of information that is stored on the file systems. To provide this functionality, the CEPA API allows the consumer applications to obtain the required event information.

The consumer applications must register for notifications by using the CEPA API. The CEPA API consists of an IDL file, when using XML/MSRPC, and an XML DTD file. These files contain information that is required by an application to interact with the event publishing agent. The consumer application can co-exist with the CEE framework on the same client or on the remote client. CEE facilitates the use of selected third-party applications with file systems. It provides events that contain the required context as defined by the consumer applications for each class. As more applications are added to each class, the events and associated contexts are modified to accommodate the applications.

Installing the Common Event Enabler Framework

Topics:

Install CEE

About this task

Steps

1. Download the CEE framework software from Online Support:
    a. Open a browser window, and go to Online Support.
    b. Perform a search for **`Common Event Enabler`**.
    c. In the **Downloads** list, look for the **Common Event Enabler**<*version number*>**for Linux** program file.
    d. Click the program file name, and save the file.
2. From the program file that you downloaded, install the RPM that corresponds to your operating system:
    a. SUSE: `rpm -i emc_cee_SLES-`*`yyy`*`.x86_64.rpm` (64-bit) OR `rpm -i emc_cee_sles-`*`yyy`*`.i386.rpm` (32-bit)

       Where *yyy* = software version number

    b. Red Hat Enterprise: `rpm -i emc_cee_RHEL-`*`yyy`*`.x86_64.rpm`

       Where *yyy* = software version number

3. Once the installation is complete, go to the directory where the CEE software was installed (the default location is `/opt/CEEPack`). Edit the `emc_cee_config.xml` file based on the instructions in Update the emc_cee_config.xml file.
4. After editing the configuration file, ensure that the CEE daemon is running. If not, Managing the Event Publishing Agent contains instructions.

Verifying the CEE installation package

Starting with the CEE v8.9.4.x release, all CEE RPM installers are signed with a **Dell Technologies Inc.** key.

Instructions for verifying the CEE Installation package are found in the *Common Event Enabler Security Configuration Guide*.

Uninstall CEE

About this task

To remove the CEE software and perform a clean uninstall:

Steps

1. Run the `rpm -e emc_cee` command.
2. Delete the directory where the CEE software was installed (the default location is `/opt/CEEPack`).

3

Configuring the Event Publishing Agent

The CEPA facility is responsible for:

- Creating event notifications (event and its associated context)
- Sending the event package into the CEPA pool

The CEPA pool is responsible for:

- Maintaining a topology and state mapping of all consumer applications
- Delivering event type and associated event metadata through the publishing agent API

Topics:

Update the emc_cee_config.xml file

The emc_cee_config.xml file contains information that is necessary to connect to the Linux systems that contain the CEE software. Update the specified options for each configuration that you use.

Steps

1. Open the `emc_cee_config.xml` file.
2. Update the options for the configuration or configurations that you use, as follows:
   a. For each auditing vendor that you are using, edit the **EndPoint** option with the audit partner name, HTTP address, and port number. You can designate multiple HTTP addresses by separating them with semicolons (;).

      CEE monitors the state of the first audit partner that is defined in the list to determine whether to publish events. If the first partner in the list is not available, events are also not published to subsequent partners in the list. The availability of the first partner also determines whether the event is re-sent later.

      Auditing configuration example:

      This example shows a configuration file that is enabled for an auditing configuration. `auditpartner` designates the value that is supplied by the partner vendor for the application.

```
<CEEConfig version="8.9.8.0">
  <CEPP>
    <Audit>
      <Configuration>
        <Enabled>1</Enabled>
        <EndPoint>auditpartner@http://10.2.3.4:8050;auditpartner@1.2.3.5:8080
           </Endpoint>
      </Configuration>
    </Audit>
    <CQM>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
      </Configuration>
    </CQM>
    <Backup>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
        <FeedInterval>60</FeedInterval>
        <MaxEventsPerFeed>100</MaxEventsPerFeed>
      </Configuration>
    </Backup>
    <CARA>
      <Configuration>
```

```
        <Enabled>0</Enabled>
        <EndPoint/>
        <FeedInterval>60</FeedInterval>
        <MaxEventsPerFeed>100</MaxEventsPerFeed>
      </Configuration>
    </CARA>
    <Index>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
        <FeedInterval>60</FeedInterval>
        <MaxEventsPerFeed>100</MaxEventsPerFeed>
        <SplunkHEC>
          <Index/>
          <Host server="" token=""/>
        </SplunkHEC>
      </Configuration>
    </Index>
    <VCAPS>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
        <FeedInterval>60</FeedInterval>
        <MaxEventsPerFeed>100</MaxEventsPerFeed>
      </Configuration>
    </VCAPS>
  </CEPP>
  <Configuration>
    <CacheSize>100</CacheSize>
    <Debug>0</Debug>
    <HeartBeatIntervalSecs>10</HeartBeatIntervalSecs>
    <InstrIntervalSecs>10</InstrIntervalSecs>
    <NumberOfThreads>20</NumberOfThreads>
    <Verbose>0</Verbose>
    <HttpPort>12228</HttpPort>
    <WatchDog>
      <RestartCount>2</RestartCount>
      <RestartDelay>5</RestartDelay>
      <ResetRestartCountAfter>86400</ResetRestartCountAfter>
    </WatchDog>
    <LogFile>
      <Path>/opt/CEEPack/</Path>
      <MaxSize>100</MaxSize>
    </LogFile>
    <Security>
      <Access>
        <AccessListEnabled>0</AccessListEnabled>
        <AccessList/>
      </Access>
    </Security>
  </Configuration>
</CEEConfig>
```

b. For each Content/Quota Management vendor that you are using, edit the **EndPoint** option with the partner name, HTTP address, and port number. You can designate multiple HTTP addresses by separating them with semicolons (;).

Content/Quota Management configuration example:

This example shows a configuration file that is enabled for a Content/Quota Management configuration. `cqmpartner` designates the value that is supplied by the partner vendor for the application.

```
<CEEConfig version="8.9.8.0">
  <CEPP>
    <Audit>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
      </Configuration>
    </Audit>
    <CQM>
      <Configuration>
        <Enabled>1</Enabled>
        <EndPoint>cqmpartner@http://10.2.3.10:8050;cqmpartner@http://10.2.3.11:8050
```

```
          </EndPoint>
      </Configuration>
    </CQM>
    <VCAPS>
     <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
        <FeedInterval>60</FeedInterval>
        <MaxEventsPerFeed>100</MaxEventsPerFeed>
      </Configuration>
    </VCAPS>
    <Index>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
        <FeedInterval>60</FeedInterval>
        <MaxEventsPerFeed>100</MaxEventsPerFeed>
        <SplunkHEC>
          <Index></Index>
          <Host server="" token=""/>
        </SplunkHEC>
      </Configuration>
    </Index>
  </CEPP>
  <Configuration>
    <CacheSize>100</CacheSize>
    <Debug>0</Debug>
    <HeartBeatIntervalSecs>10</HeartBeatIntervalSecs>
    <InstrIntervalSecs>10</InstrIntervalSecs>
    <NumberOfThreads>20</NumberOfThreads>
    <Verbose>0</Verbose>
    <HttpPort>12228</HttpPort>
    <WatchDog>
      <RestartCount>2</RestartCount>
      <RestartDelay>5</RestartDelay>
      <ResetRestartCountAfter>86400</ResetRestartCountAfter>
    </WatchDog>
    <LogFile>
      <Path>/opt/CEEPack/</Path>
      <MaxSize>100</MaxSize>
    </LogFile>
    <Security>
      <Access>
        <AccessListEnabled>0</AccessListEnabled>
        <AccessList/>
      </Access>
    </Security>
  </Configuration>
</CEEConfig>
```

c. For each Anti-Ransomware partner that you are using, edit the **EndPoint** option with the partner name, HTTP address, and port number. You can designate multiple HTTP addresses by separating them with semicolons (;). You can also edit the **FeedInterval** and **MaxEventsPerFeed** options or keep the default values.

   Anti-Ransomware configuration example:

   This example shows a configuration file that is enabled for a CARA configuration. `carapartner` designates the value that is supplied by the partner for the application.

```
<CEEConfig version="8.9.8.0">
  <CEPP>
    <Audit>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
      </Configuration>
    </Audit>
    <CQM>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
      </Configuration>
    </CQM>
    <Backup>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
        <FeedInterval>60</FeedInterval>
        <MaxEventsPerFeed>100</MaxEventsPerFeed>
      </Configuration>
    </Backup>
    <CARA>
      <Configuration>
        <Enabled>1</Enabled>
        <EndPoint>carapartner@http://10.2.3.10:8050</EndPoint>
        <FeedInterval>60</FeedInterval>
        <MaxEventsPerFeed>100</MaxEventsPerFeed>
      </Configuration>
    </CARA>
    <Index>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
        <FeedInterval>60</FeedInterval>
        <MaxEventsPerFeed>100</MaxEventsPerFeed>
        <SplunkHEC>
          <Index/>
          <Host server="" token=""/>
        </SplunkHEC>
      </Configuration>
    </Index>
    <VCAPS>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
        <FeedInterval>60</FeedInterval>
        <MaxEventsPerFeed>100</MaxEventsPerFeed>
      </Configuration>
    </VCAPS>
  </CEPP>
  <Configuration>
    <CacheSize>100</CacheSize>
    <Debug>0</Debug>
    <HeartBeatIntervalSecs>10</HeartBeatIntervalSecs>
    <InstrIntervalSecs>10</InstrIntervalSecs>
    <NumberOfThreads>20</NumberOfThreads>
    <Verbose>0</Verbose>
    <HttpPort>12228</HttpPort>
    <WatchDog>
      <RestartCount>2</RestartCount>
      <RestartDelay>5</RestartDelay>
      <ResetRestartCountAfter>86400</ResetRestartCountAfter>
    </WatchDog>
    <LogFile>
      <Path>/opt/CEEPack/</Path>
      <MaxSize>100</MaxSize>
    </LogFile>
    <Security>
      <Access>
        <AccessListEnabled>0</AccessListEnabled>
        <AccessList/>
      </Access>
    </Security>
  </Configuration>
</CEEConfig>
```

d. For each Indexing vendor that you are using, edit the:
   - **EndPoint** option with the software name (`SplunkHEC`), HTTPS address of the computer where the Splunk consumer application is installed, and port number of `8088`. You can designate multiple HTTPS addresses by separating them with semicolons (;).
   - **SplunkHEC Index** option with a user-defined name for the index. Only one index value is allowed.
   - **Host server** option with the IP address of the computer where the Splunk consumer application is installed.
   - **token** option with the GUID generated by Splunk Enterprise or Splunk Cloud application for the index.

NOTE: If the Splunk consumer application is installed on multiple computers, you must create multiple <Host server / token> lines, one for each computer.

Indexing configuration example:

This example shows a configuration file that is enabled for an Indexing configuration.

```
<CEEConfig version="8.9.8.0">
  <CEPP>
    <Audit>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
      </Configuration>
    </Audit>
    <CQM>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
      </Configuration>
    </CQM>
    <Backup>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
        <FeedInterval>60</FeedInterval>
        <MaxEventsPerFeed>100</MaxEventsPerFeed>
      </Configuration>
    </Backup>
    <CARA>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
        <FeedInterval>60</FeedInterval>
        <MaxEventsPerFeed>100</MaxEventsPerFeed>
      </Configuration>
    </CARA>
    <Index>
      <Configuration>
        <Enabled>1</Enabled>
        <EndPoint>SplunkHEC@https://10.3.4.20:8088</EndPoint>
        <FeedInterval>60</FeedInterval>
        <MaxEventsPerFeed>100</MaxEventsPerFeed>
        <SplunkHEC>
          <Index>ceeindex</Index>
          <Host server="10.3.4.20" token="ab962c17-55dc-4516-b3f0-4xyza07bfb22"/>
        </SplunkHEC>
      </Configuration>
    </Index>
    <VCAPS>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
        <FeedInterval>60</FeedInterval>
        <MaxEventsPerFeed>100</MaxEventsPerFeed>
      </Configuration>
    </VCAPS>
  </CEPP>
  <Configuration>
    <CacheSize>100</CacheSize>
    <Debug>0</Debug>
    <HeartBeatIntervalSecs>10</HeartBeatIntervalSecs>
    <InstrIntervalSecs>10</InstrIntervalSecs>
    <NumberOfThreads>20</NumberOfThreads>
    <Verbose>0</Verbose>
    <HttpPort>12228</HttpPort>
    <WatchDog>
      <RestartCount>2</RestartCount>
      <RestartDelay>5</RestartDelay>
      <ResetRestartCountAfter>86400</ResetRestartCountAfter>
    </WatchDog>
    <LogFile>
      <Path>/opt/CEEPack/</Path>
      <MaxSize>100</MaxSize>
    </LogFile>
    <Security>
      <Access>
        <AccessListEnabled>0</AccessListEnabled>
        <AccessList/>
      </Access>
    </Security>
  </Configuration>
</CEEConfig>
```

e. If you want to allow HTTP connections only from specific IP addresses, enable the AccessList option by editing:
   - Set **AccessListEnabled** to 1 (enabled).
   - To **AccessList**, add the list of IP addresses from which CEE will accept messages. You can designate multiple IP addresses by separating them with semicolons (;).

   AccessList configuration example

```
<CEEConfig version="8.9.8.0">
  <CEPP>
    <Audit>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
      </Configuration>
    </Audit>
    <CQM>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
      </Configuration>
    </CQM>
    <Backup>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
        <FeedInterval>60</FeedInterval>
        <MaxEventsPerFeed>100</MaxEventsPerFeed>
      </Configuration>
    </Backup>
    <CARA>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
        <FeedInterval>60</FeedInterval>
        <MaxEventsPerFeed>100</MaxEventsPerFeed>
      </Configuration>
    </CARA>
    <Index>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
        <FeedInterval>60</FeedInterval>
        <MaxEventsPerFeed>100</MaxEventsPerFeed>
        <SplunkHEC>
          <Index/>
          <Host server="" token=""/>
        </SplunkHEC>
      </Configuration>
    </Index>
    <VCAPS>
      <Configuration>
        <Enabled>0</Enabled>
        <EndPoint/>
        <FeedInterval>60</FeedInterval>
        <MaxEventsPerFeed>100</MaxEventsPerFeed>
      </Configuration>
    </VCAPS>
  </CEPP>
  <Configuration>
    <CacheSize>100</CacheSize>
    <Debug>0</Debug>
    <HeartBeatIntervalSecs>10</HeartBeatIntervalSecs>
    <InstrIntervalSecs>10</InstrIntervalSecs>
    <NumberOfThreads>20</NumberOfThreads>
    <Verbose>0</Verbose>
    <HttpPort>12228</HttpPort>
    <WatchDog>
      <RestartCount>2</RestartCount>
      <RestartDelay>5</RestartDelay>
      <ResetRestartCountAfter>86400</ResetRestartCountAfter>
    </WatchDog>
    <LogFile>
      <Path>/opt/CEEPack/</Path>
      <MaxSize>100</MaxSize>
    </LogFile>
    <Security>
      <Access>
        <AccessListEnabled>1</AccessListEnabled>
        <AccessList>10.5.7.9;10.5.7.1</AccessList>
      </Access>
    </Security>
  </Configuration>
</CEEConfig>
```

f. To allow CEE to communicate with the platform via HTTP or HTTPS, set **ServerEnabled** to 1 (enabled).

3. In the information source software that sends events to CEE, ensure that the **HttpPort** option is set to the default port number of **12228**.

4

Managing the Event Publishing Agent

Topics:

Start the CEPA facility

About this task

Steps

To start the CEPA facility, run this CEE daemon command:

```
emc_cee_svc start
```

Stop the CEPA facility

About this task

Steps

To stop the CEPA facility, run this CEE daemon command:

```
emc_cee_svc stop
```

Restart the CEPA facility

About this task

Steps

To restart the CEPA facility, run this CEE daemon command:

```
emc_cee_svc restart
```

5

Managing CARA

Common Anti-Ransomware Agent (CARA) is a mechanism for delivering post-events in asynchronous mode. The delivery cadence is based on a time period or a number of events.

Topics:

Set up access for Linux platforms

About this task

You must define four CARA entries in the configuration file.

Steps

1. Open the emc_cee_config.xml file.
2. In the <CARA> section, do the following:
    a. Set **Enabled** to `1` to enable CARA.
    b. Set **Endpoint** to the IP addresses of the computers where the consumer application is installed, in the following format:

    ```
    <carapartner>@http://<IP address:port>
    ```

    For example, mycarapartner@http://10.2.3.10:8050. When setting multiple computers, you must use a ; (semicolon) to separate the IP addresses.

    c. Set **FeedInterval** to specify how often, in seconds, information is sent from CARA to the consumer application. The default is 60 seconds. The range is from 60 seconds to 600 seconds.
    d. Set **MaxEventsPerFeed** to specify how many modification events must occur before information is sent from CARA to the consumer application. The default is 100 events. The range is from 10 events to 10,000 events.
3. Save the configuration file, and then close it.

Results

The FeedInterval and MaxEventsPerFeed delivery cadences are used simultaneously.

CARA sends a list of modified events to the consumer application, not the actual content.

6

Managing VCAPS

Common Asynchronous Publishing Service (VCAPS) is a mechanism for delivering post-events in asynchronous mode. The delivery cadence is based on a time period or a number of events.

Topics:

Set up access

About this task

You must define four VCAPS entries in the configuration file.

Steps

1. Open the emc_cee_config.xml file.
2. In the <VCAPS> section, do the following:
    a. Set **Enabled** to **1** to enable VCAPS.
    b. Set **Endpoint** to the IP addresses of the computers where the consumer application is installed, in the following format:

    ```
    <vendorname>@http://<IP address:port>
    ```

    For example, myvendor@http://10.1.2.1:8200. When setting multiple computers, you must use a ; (semicolon) to separate the IP addresses.

    c. Set **FeedInterval** to specify how often, in seconds, information is sent from VCAPS to the consumer application. The default is 60 seconds. The range is from 60 seconds to 600 seconds.
    d. Set **MaxEventsPerFeed** to specify how many modification events must occur before information is sent from VCAPS to the consumer application. The default is 100 events. The range is from 10 events to 10,000 events.
3. Save the configuration file, and then close it.

Results

The FeedInterval and MaxEventsPerFeed delivery cadences are used simultaneously.

VCAPS sends a list of modified events to the consumer application, not the actual content.

7

Managing Indexing

The Index subfacility of CEPA is a mechanism for delivering bulk events in asynchronous mode to partner applications. The delivery cadence is based on either a time period or a number of events. You can use this Index facility to deliver bulk events to Splunk Enterprise or Splunk Cloud. CEE uses the Splunk HTTP Event Collector (HEC) to send events to a Splunk deployment over the Secure HTTP (HTTPS) protocol. The index that is used in Splunk Enterprise or Splunk Cloud to receive the CEE events must be configured in Splunk for structured messaging in the JSON format.

Topics:

Set up access for Splunk

About this task

Use the Index facility to deliver events to Splunk Enterprise or Splunk Cloud by performing the following steps.

You must define Index entries in the configuration file.

Steps

1. From the `/opt/CEEpack` directory, open the `emc_cee_config.xml` file.
2. In the <Index> section, do the following:
   a. In the <Configuration> section, do the following:
      i. Set **Enabled** to **1** to enable Index.
      ii. Set **EndPoint** and specify the host and port, or hosts and ports, of the instances where the Splunk consumer application is installed, in the following format:

         ```
         SplunkHEC@https://<host>:<port>
         ```

         where `<host>` is the URI, IP address, or FQDN of Splunk Enterprise or Splunk Cloud. For example, `SplunkHEC@https://10.3.4.20:8088`.

         When setting multiple entries, you must use a ; (semicolon) to separate the individual entries. For example, `SplunkHEC@https://10.3.4.20:8088;SplunkHEC@https://10.3.4.40:8088`.

      iii. (Optional) **FeedInterval** specifies how often, in seconds, information is sent from the Index application to the Splunk consumer application. The default is 60 seconds. The range is from 60 to 600 seconds . Update this value only if necessary.
      iv. (Optional) **MaxEventsPerFeed** specifies how many events are accumulated before information is sent from the Index application to the Splunk consumer application. The default is 100 events. The range is from 10 events to 10,000 events. Update this value only if necessary.
   b. In the <SplunkHEC> subsection, do the following:
      i. Specify **Index**, which is a user-defined name for the index being used on Splunk Enterprise or Splunk Cloud. Only one index value is allowed.
      ii. Set **Host server** to the name of the URI or IP address of Splunk Enterprise or Splunk Cloud.
      iii. Set **token** by copying the token value that is defined in the HTTP Event Collector in Splunk Enterprise or Splunk Cloud to here.

      NOTE: To use multiple instances of the Splunk consumer application, you must create multiple `<Host server=""token="">` values - one for each location.

3. Save the configuration file, and then close it.

Results

The **FeedInterval** and **MaxEventsPerFeed** delivery cadences are used simultaneously.

The Index application sends a list of events to the Splunk consumer application, not the content of files.

Index